Virtual University of Pakistan
FEDERAL GOVERNMENT UNIVERSITY

COMPLETE SLIDES

Cyber Security

CS627

Order Your VU Books Now

Get all Virtual University books in high-quality hard copy, delivered right to your doorstep. Visit vubookshoppk.com

Order Now

Importance of Cyber Security

- Mobile Phones
- Total population of Pakistan (2020) → **219,067,896**
- Number of **mobile phone users in Pakistan** has reached 161.183 million, as of May **2019**.
  - Smart phones
  - Traditional phones:
    - SMS / Call Scams

Importance of Cyber Security

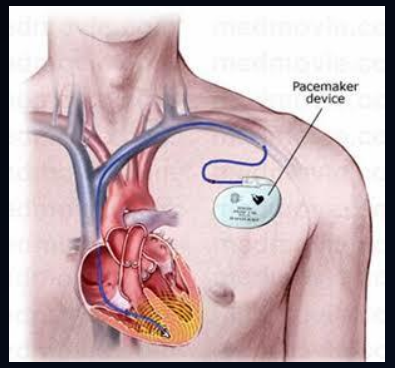
- Drones
  - **Here's How Hackers Could Have Spied On Your DJI Drone Account**
    - https://thehackernews.com/2018/11/dji-drone-hack_8.html





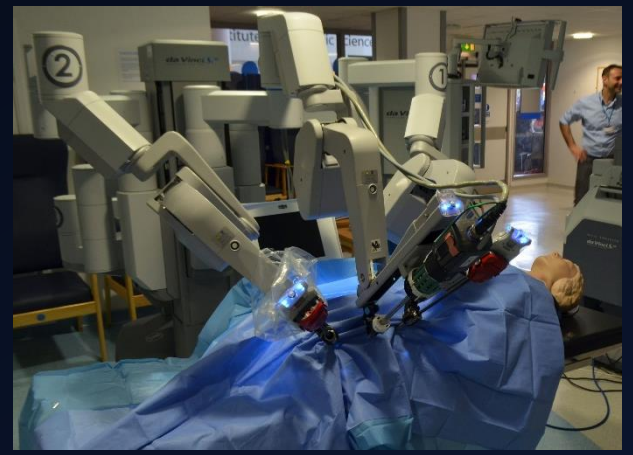


Importance of Cyber Security



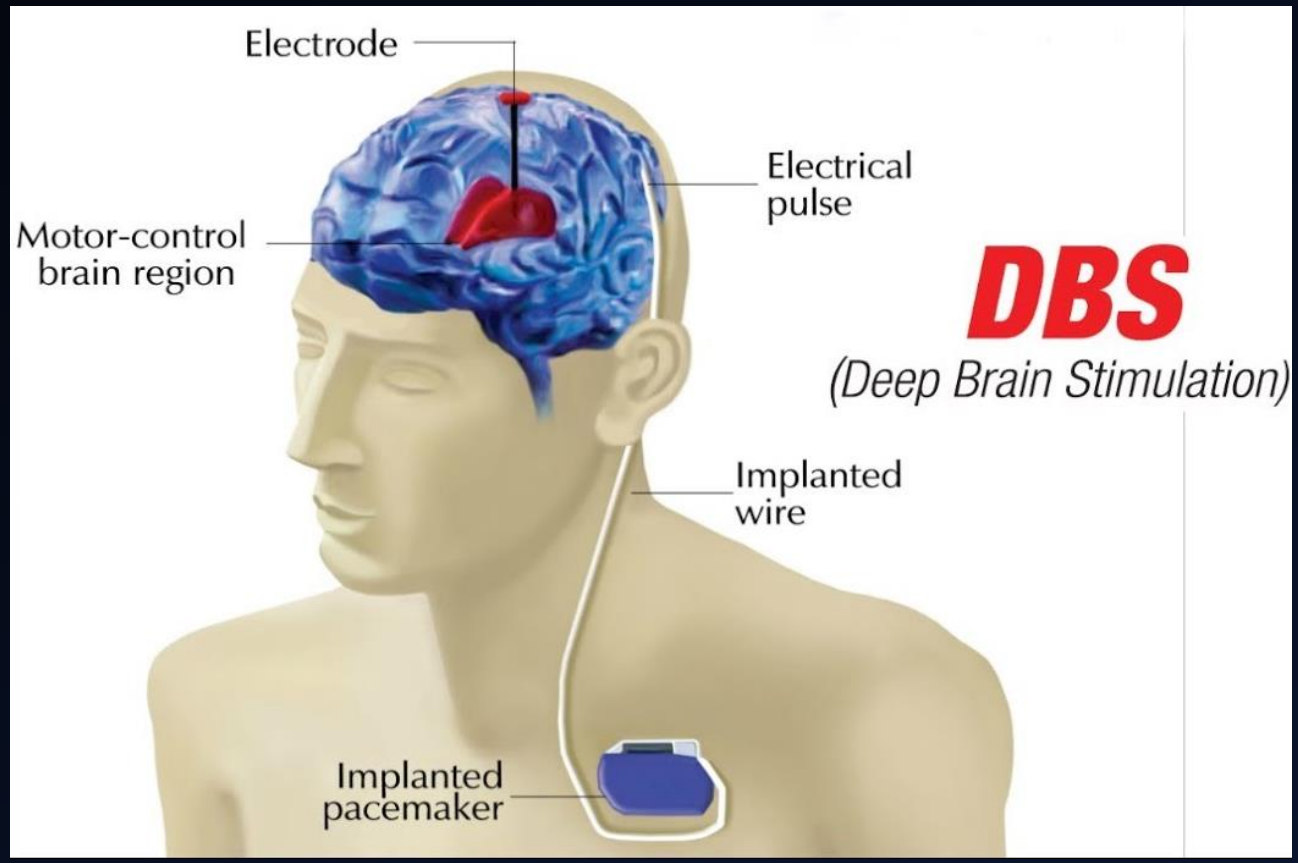


- Health / Medical
  - Pacemaker: a device for stimulating the heart muscle and regulating its contractions.
  - Robotic Surgeons
    - 5 Medical Robots Making a Difference in Healthcare
      - https://online-engineering.case.edu/blog/medical-robots-making-a-difference
  - Remote Surgery
    - China completes world's first 5G remote surgery in test on animal
      - https://www.youtube.com/watch?v=yFR61jjL1vo
    - Robot Helps Perform First Long-Distance Heart Surgery
      - **A surgeon in India performed the first remote heart operation on a patient 20 miles away.**
        - https://www.popularmechanics.com/technology/robots/a28941179/robot-performs-first-long-distance-heart-surgery/



Bluetooth in health





- The field of ‘Cyber Security’ is becoming more important due to increased reliance on
  - computer systems
  - the Internet
  - wireless network standards
    - such as Bluetooth and Wi-Fi
  - due to the growth of "smart" devices
    - including smartphones, televisions, and the "Internet of things".
- Owing to its complexity, both in terms of politics and technology, cybersecurity is also one of the major challenges in the contemporary world.
  - Ease of use results in increasing underlying complexity

What is Cyber Security?

- Cyber
  - Relating to or characteristic of the culture of computers, information technology, and virtual reality.
  - **Cyberspace** is a term for virtual reality coined by William Gibson.
    - https://en.wikipedia.org/wiki/Cyberspace
  - *Cyber-* is derived from "cybernetic", [https://en.wikipedia.org/wiki/Cybernetics] which comes from the Greek word κυβερνητικός meaning *'skilled in steering or governing'.*
    - Pronunciation: [https://forvo.com/word/%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%B7%CF%84%CE%B9%CE%BA%CF%8C%CF%82/]
  - Cybernetics: the science of communications and automatic control systems in both machines and living things.
  - Used to describe policies and politics regarding computer systems and networks.
  - Term used in Information Technology industry and the Internet era.
    - https://en.wikipedia.org/wiki/Internet-related_prefixes#.22Cyber-.22
    - https://en.wikipedia.org/wiki/Cyber

What is Cyber Security?

- Security
  - Degree of ‘protection’ [safe & secure].
  - The state of being free from danger or threat.
  - **Security** is freedom from, or resilience against, potential harm caused by others. [Wikipedia]
    - https://en.wikipedia.org/wiki/Security

What is Cyber Security?

- **Computer security**, **cybersecurity** or **information technology security** (**IT security**) is the protection of computer systems from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.
  - https://en.wikipedia.org/wiki/Computer_security

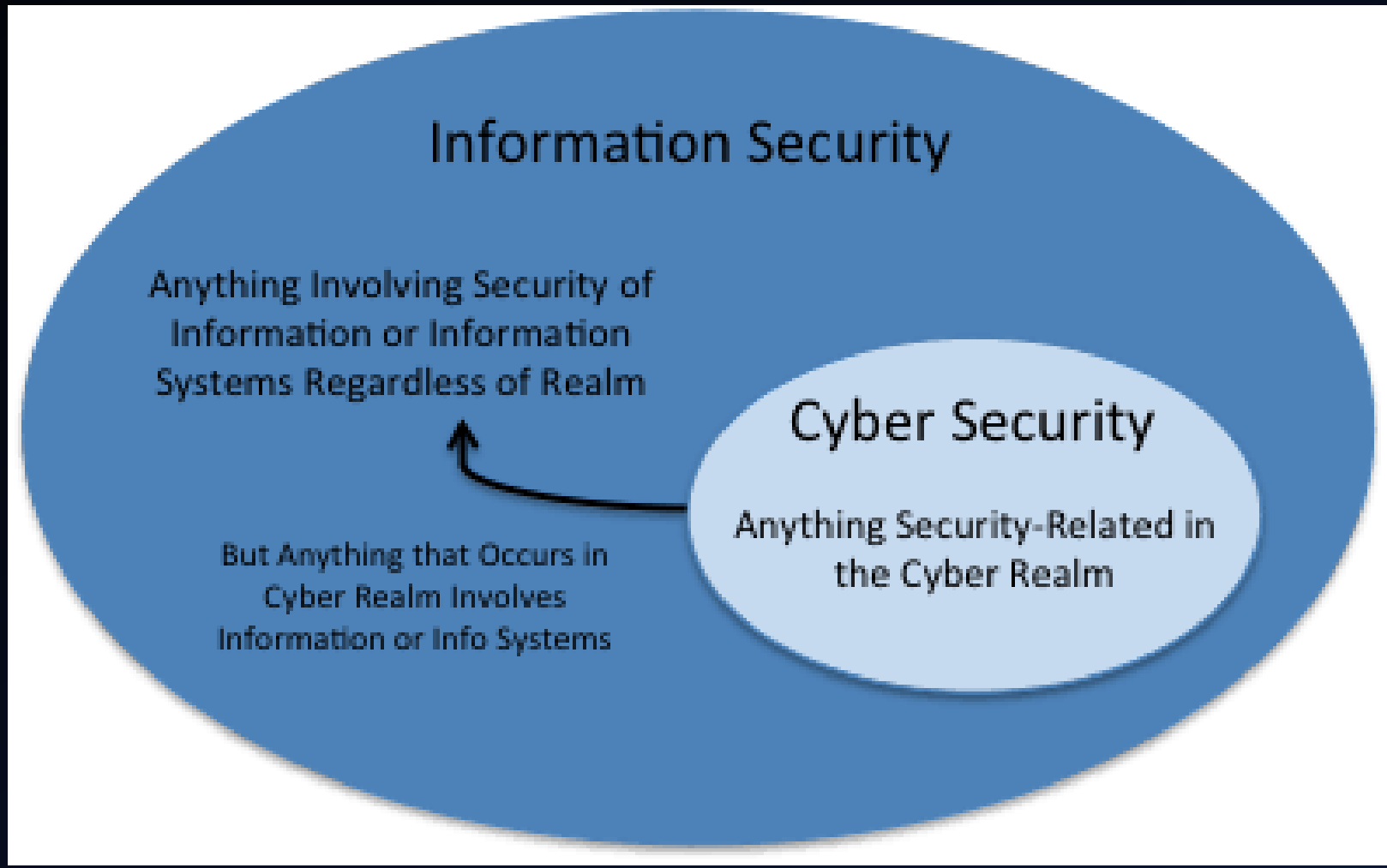
Security Realms

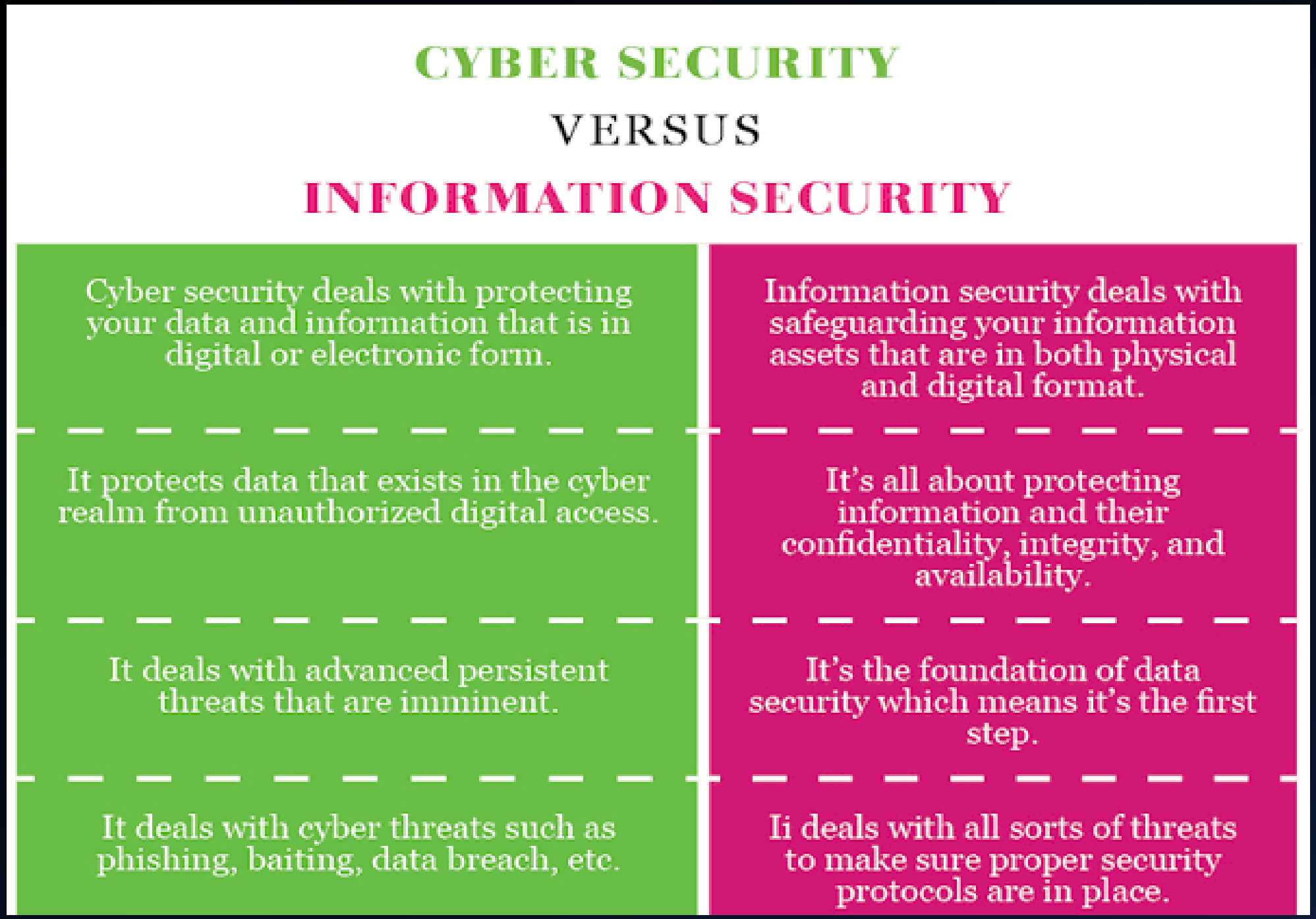
- Information Security
- IT Security
- Cyber Security
- Network Security
- System Security
- Data Security
- Operating System Security
- Physical Security

Information Security

- **Information security**, sometimes shortened to **infosec**, is the 'practice of protecting information' by mitigating information risks.
- It is part of information risk management.
- It typically involves preventing or at least reducing the probability of unauthorized/inappropriate access, use, disclosure, disruption, deletion/destruction, corruption, modification, inspection (monitor), recording or devaluation of data and/or systems.
- Information may take any form, e.g. electronic or physical.

Cyber Security vs InfoSec




CYBER SECURITY
VERSUS
INFORMATION SECURITY
Cyber security deals with protecting your data and information that is in digital or electronic form.
Information security deals with safeguarding your information assets that are in both physical and digital format.
It protects data that exists in the cyber realm from unauthorized digital access.
It's all about protecting information and their confidentiality, integrity, and availability.
It deals with advanced persistent threats that are imminent.
It's the foundation of data security which means it's the first step.
It deals with cyber threats such as phishing, baiting, data breach, etc.
Ii deals with all sorts of threats to make sure proper security protocols are in place.

Cyber Security Jobs & Careers

https://www.cybersecurityeducation.org/careers/

- Start at any point in your life / career.
- Wide range of responsibilities.
- Crux of the job is to protect online data and systems form being compromised.
- Cyber security careers are complex.
- Many roles can be found with banks, retailers and government organizations.
- On the job, you can expect to:
  - safeguard an organization's files and network
  - install / configure firewalls
  - create security plans
  - monitor activity
  - If a breach occurs, you'll be responsible for identifying the problem and finding a solution quickly.
- Because of the frequency of cyber attacks, careers are varied and qualified professionals are in demand.
- If you're ready to get started in this fast-growing career, start exploring cyber careers now.

Job Titles

- Cyber Security Vendor
  - Solution Provider
  - Services
- Security Auditor
- PenTester / Ethical Hacker
- Security Analyst
- InfoSec Engineer
- InfoSec Consultant
- Malware Analyst
- Forensic Analyst/Expert/Investigator
- Incident Handler / Manager
- InfoSec / Cyber Security Specialist
- InfoSec Manager
- CISO

*TOP 10 CYBER SECURITY JOB TITLES

- Security Engineer
- Security Analyst
- Information Security Analyst
- Information Security Engineer
- Network Security Engineer
- Information Technology Security Analyst
- Information Security Manager
- Information Assurance Engineer
- Senior IT Auditor
- Security Administrator

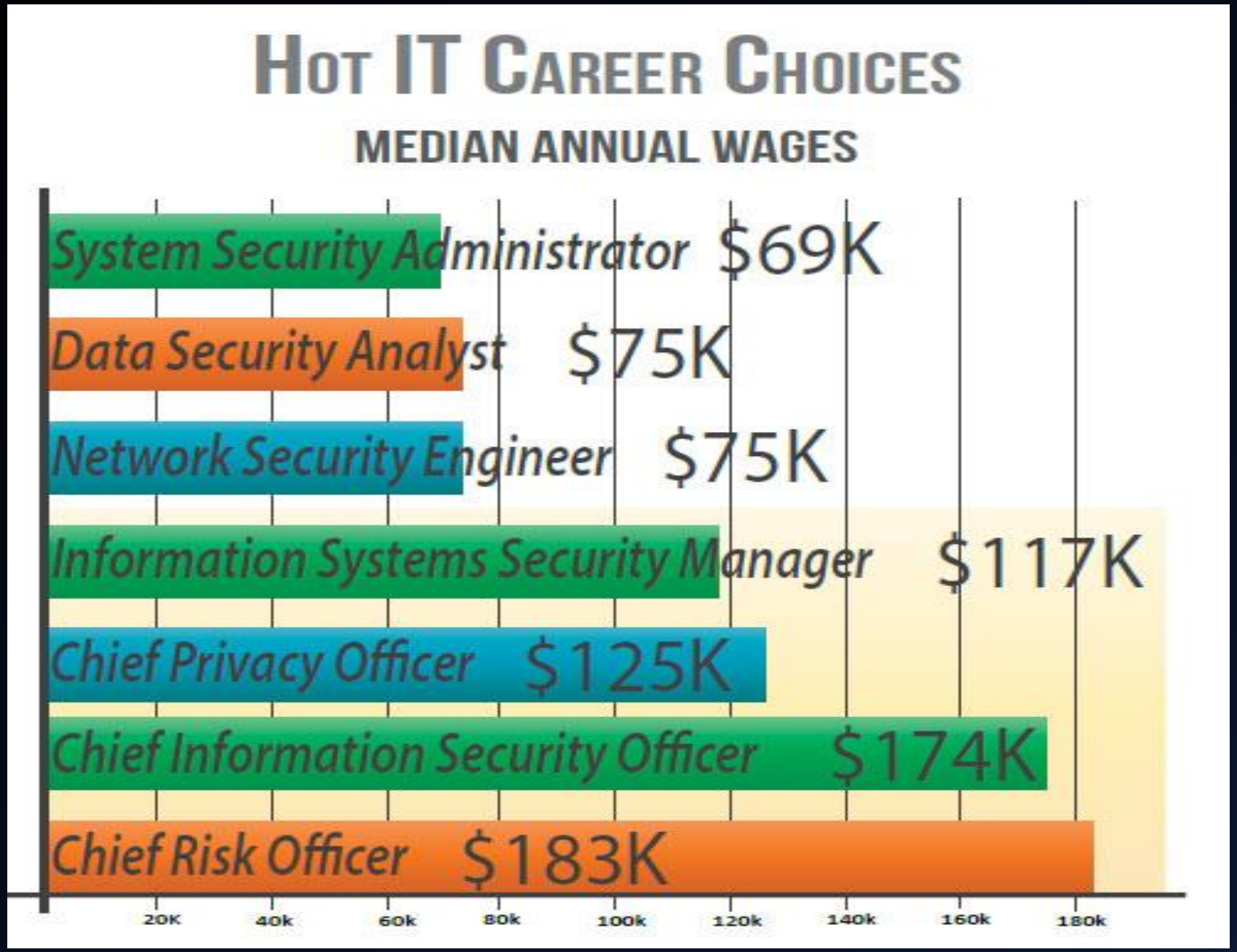
*UMUC.edu study

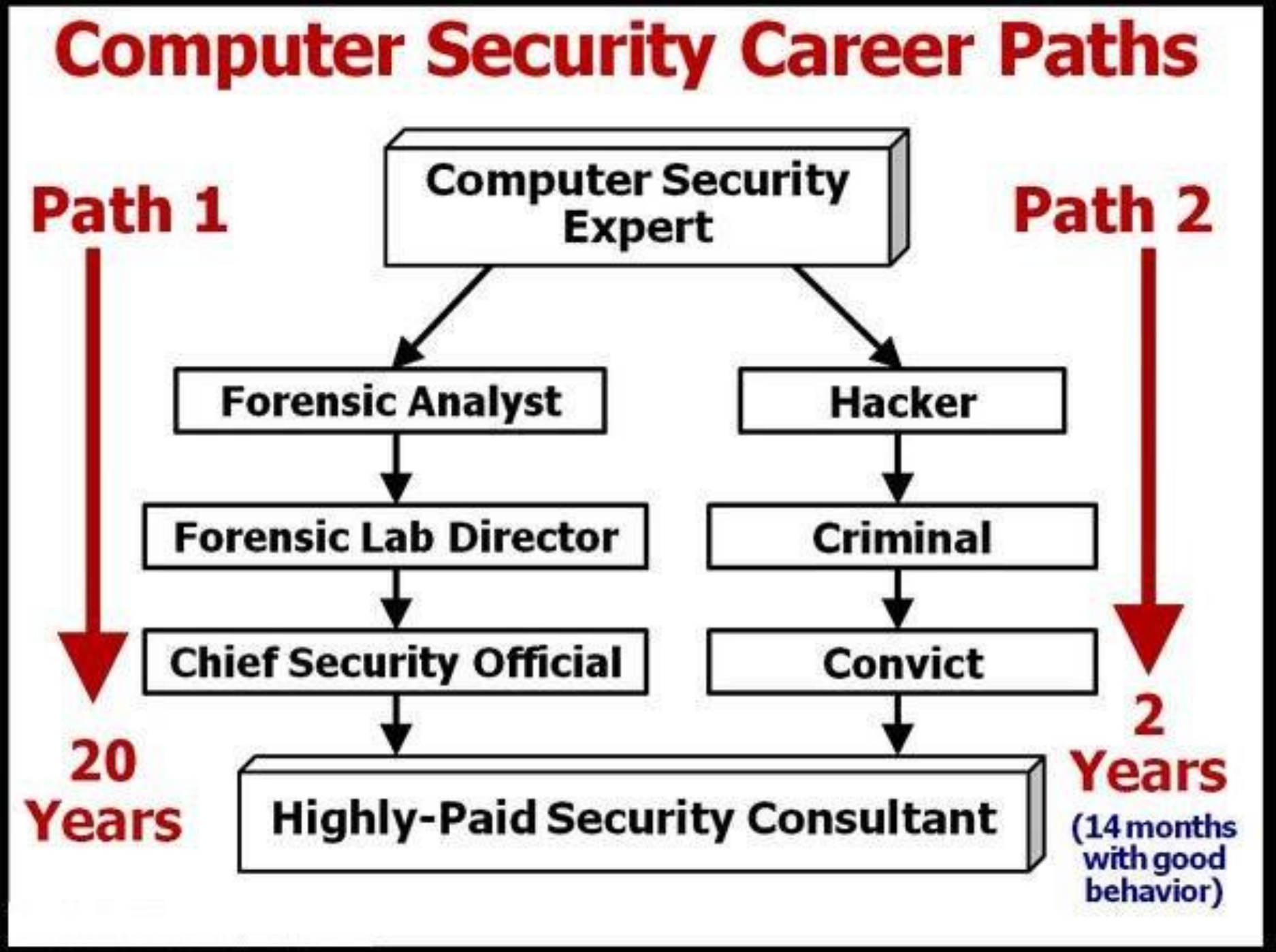
Here are the 10 highest-paying job titles in cybersecurity in the US.

- Application security engineer
- Director of information security
- Senior security consultant
- Cloud engineer
- Software architect
- Penetration tester
- Risk manager
- Chief information officer
- Security engineer
- Information manager



Source - Indeed.com


HOT IT CAREER CHOICES
MEDIAN ANNUAL WAGES
System Security Administrator $69K
Data Security Analyst $75K
Network Security Engineer $75K
Information Systems Security Manager $117K
Chief Privacy Officer $125K
Chief Information Security Officer $174K
Chief Risk Officer $183K
20K
40k
60k
80k
100k
120k
140k
160k
180k


Computer Security Career Paths
Computer Security Expert
Path 1
Path 2
Forensic Analyst
Hacker
Forensic Lab Director
Criminal
Chief Security Official
Convict
20 Years
2 Years
(14 months with good behavior)
Highly-Paid Security Consultant

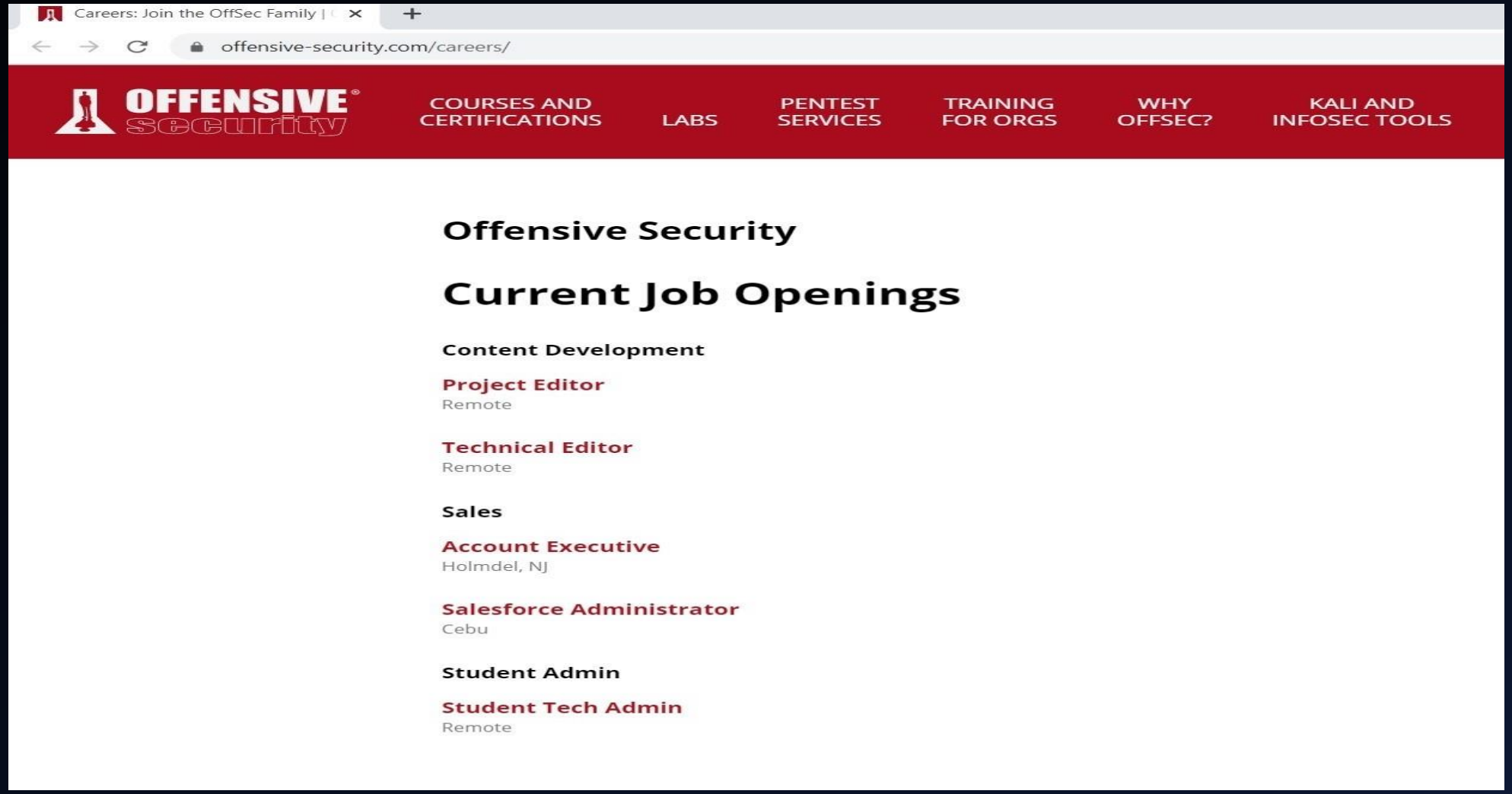
Job Sectors

- Internships
- Education
  - Teaching / Training
  - Universities / Certs
- CERTs
- Private Organizations
- Government Institutes
- Financial Sector
- Law Enforcement & Military
- Freelancing
- Independent Consultant



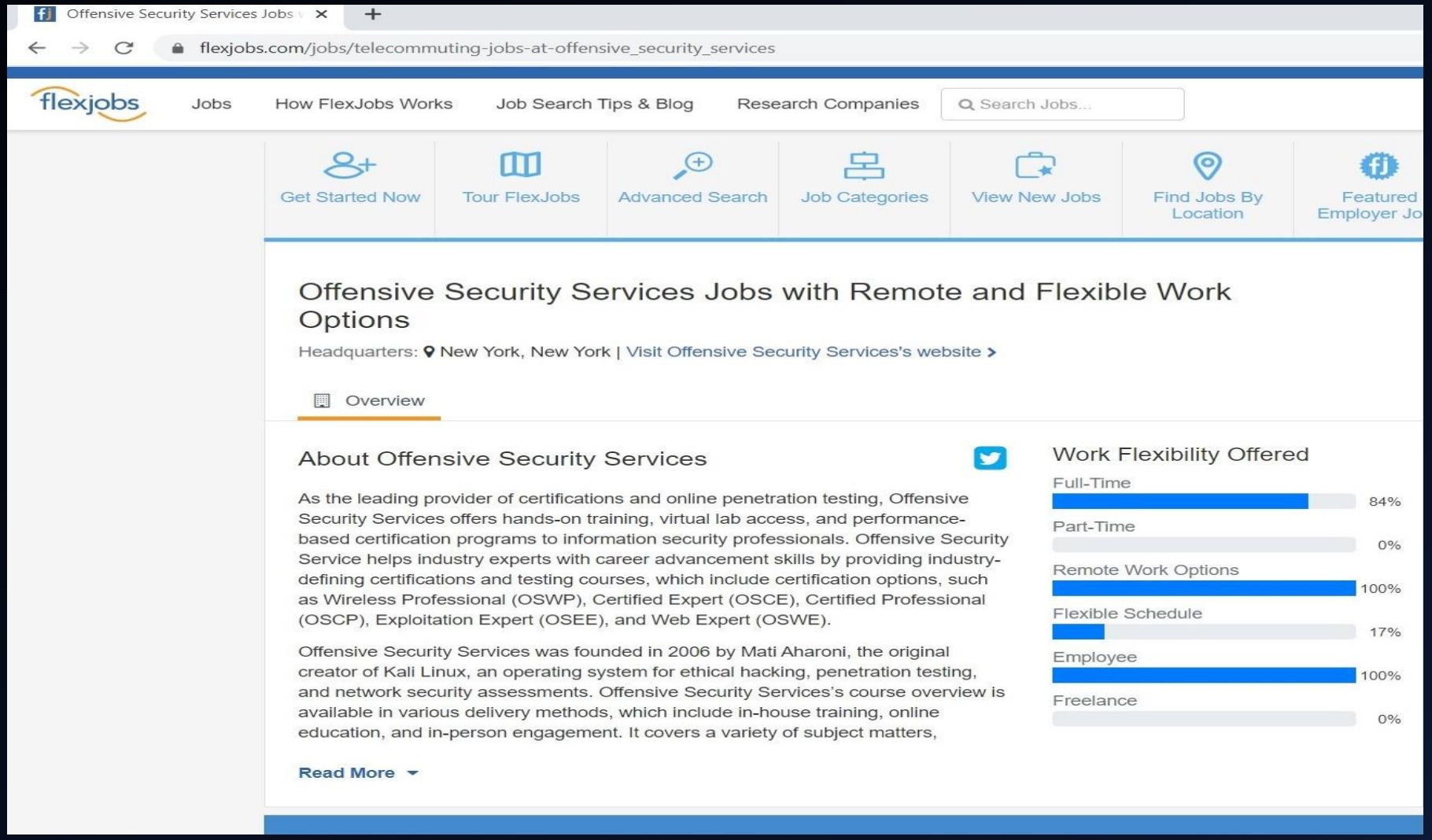
Offensive Security – Jobs

https://www.offensive-security.com/careers/



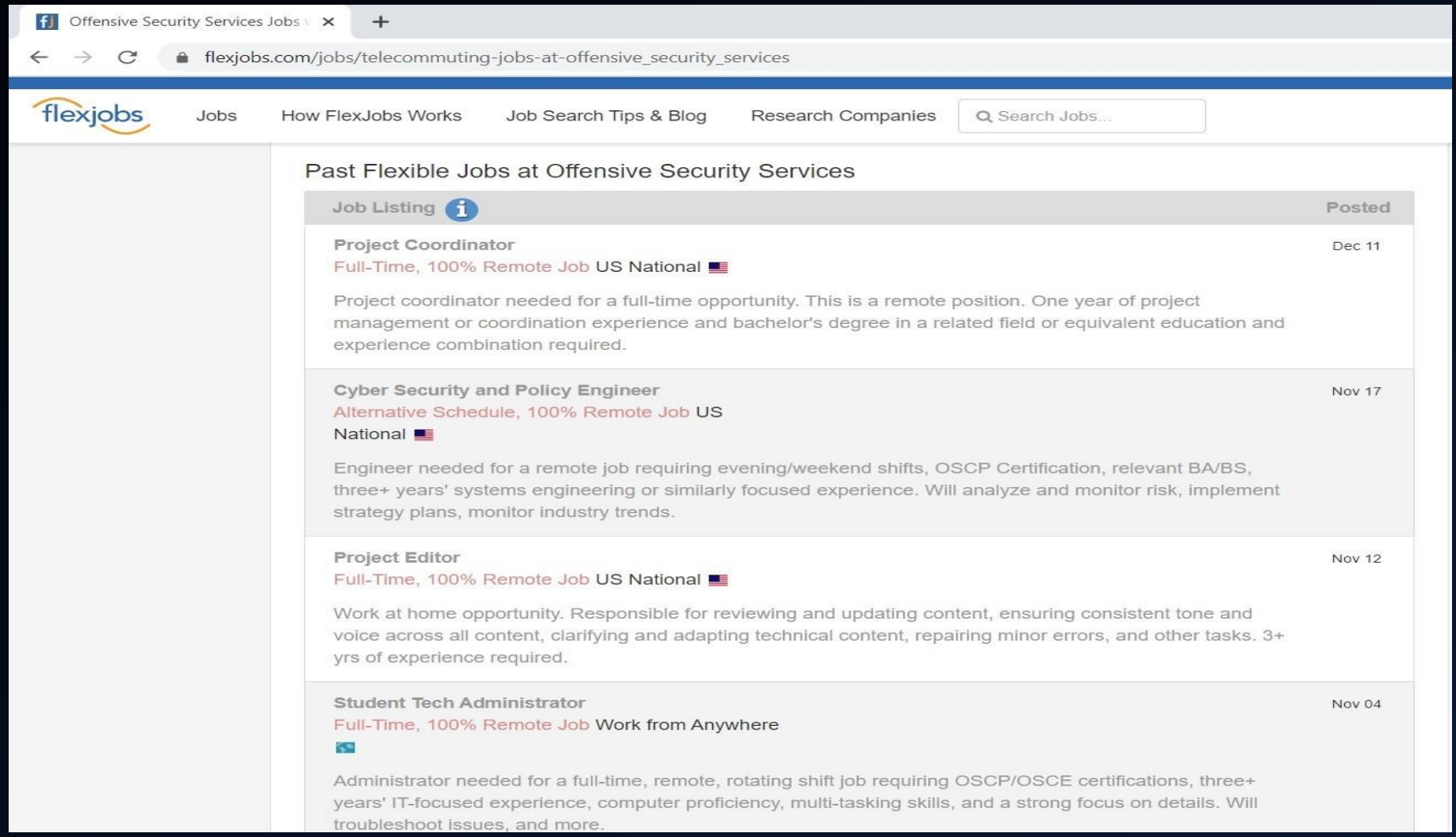
Offensive Security – Jobs

https://www.flexjobs.com/jobs/telecommuting-jobs-at-offensive_security_services



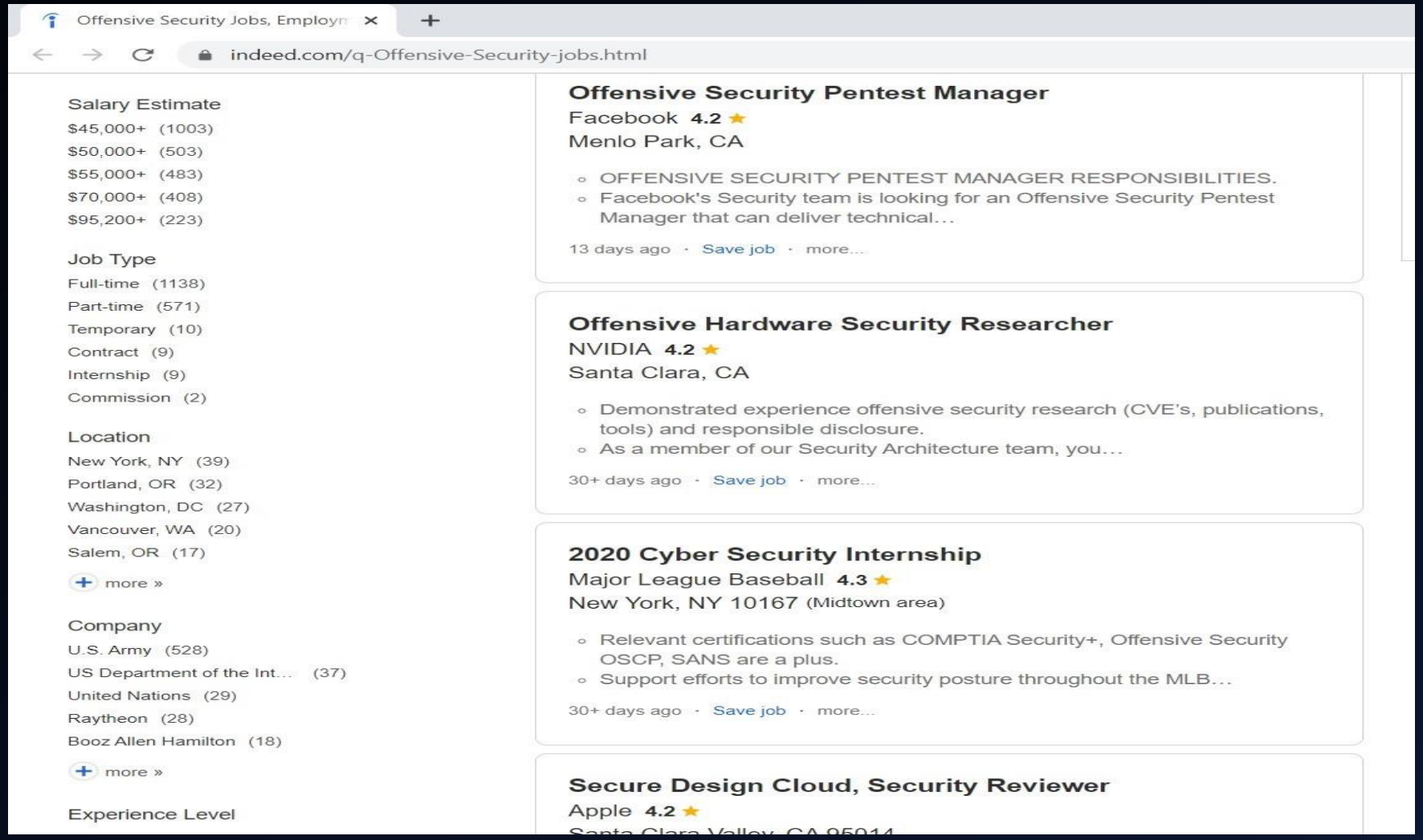
Offensive Security – Jobs

https://www.flexjobs.com/jobs/telecommuting-jobs-at-offensive_security_services



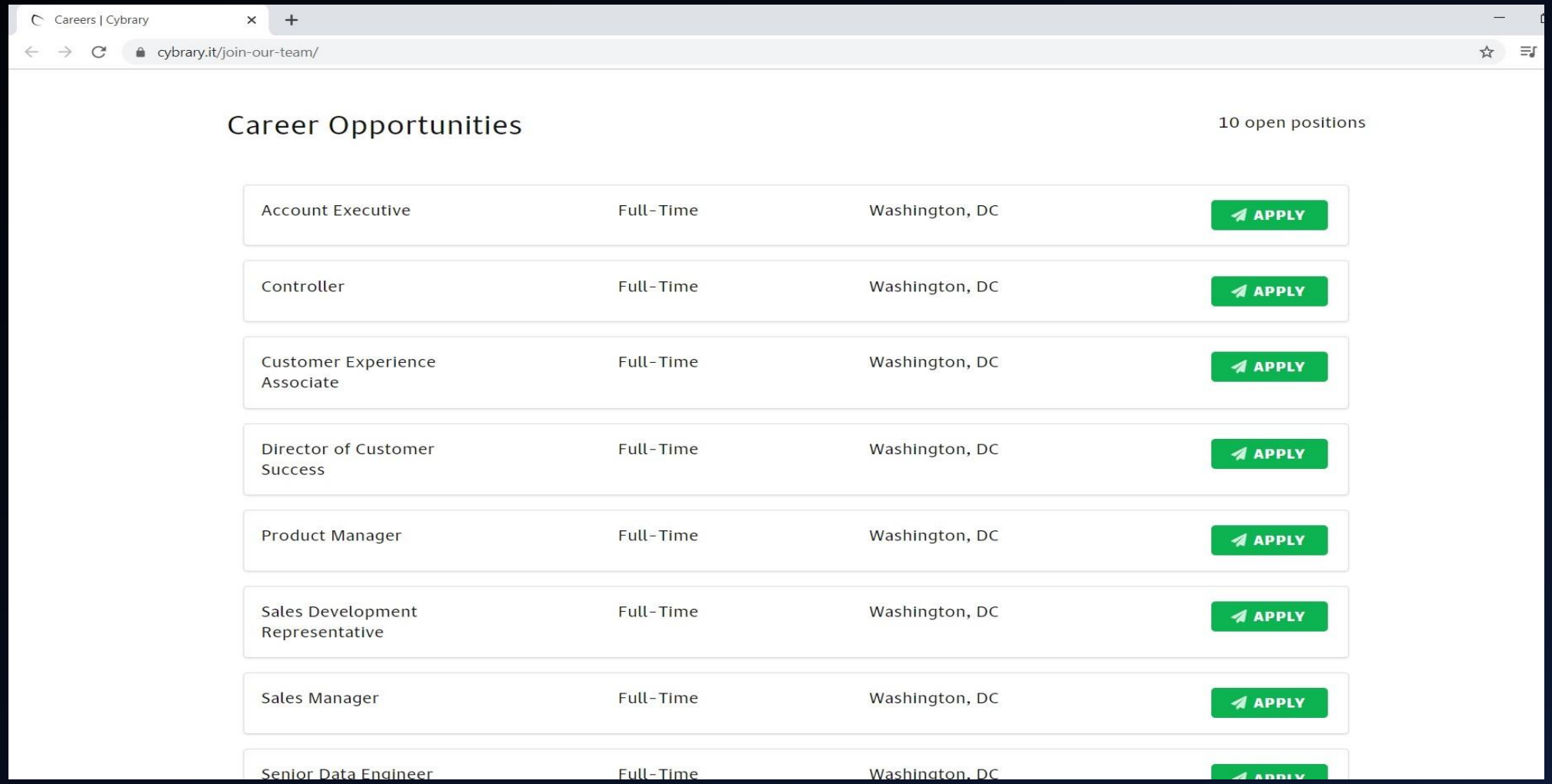
Offensive Security – Jobs

https://www.indeed.com/q-Offensive-Security-jobs.html



CYBRARY Career Opportunities

https://www.cybrary.it/join-our-team/



CYBRARY Career Opportunities

https://www.cybrary.it/contribute/



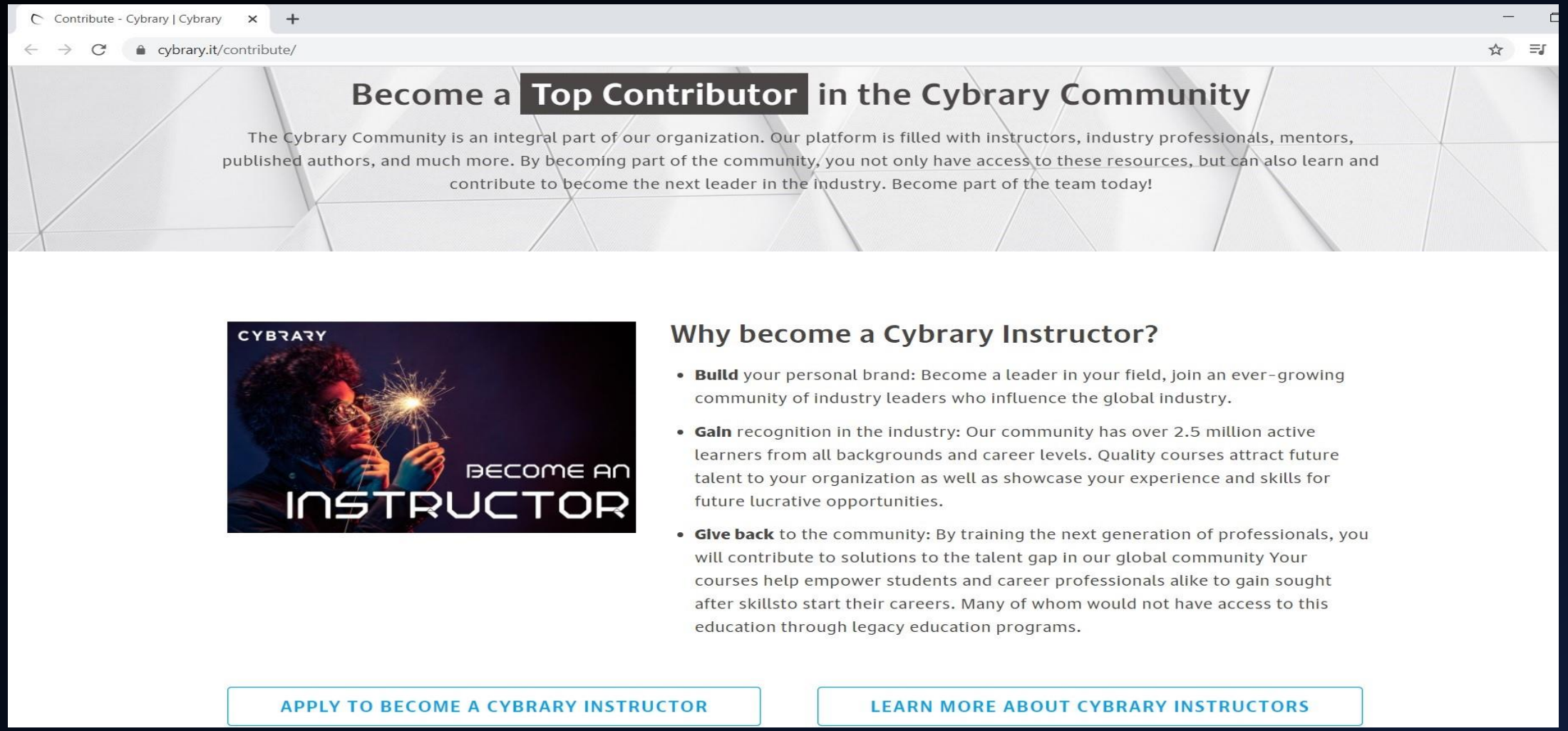






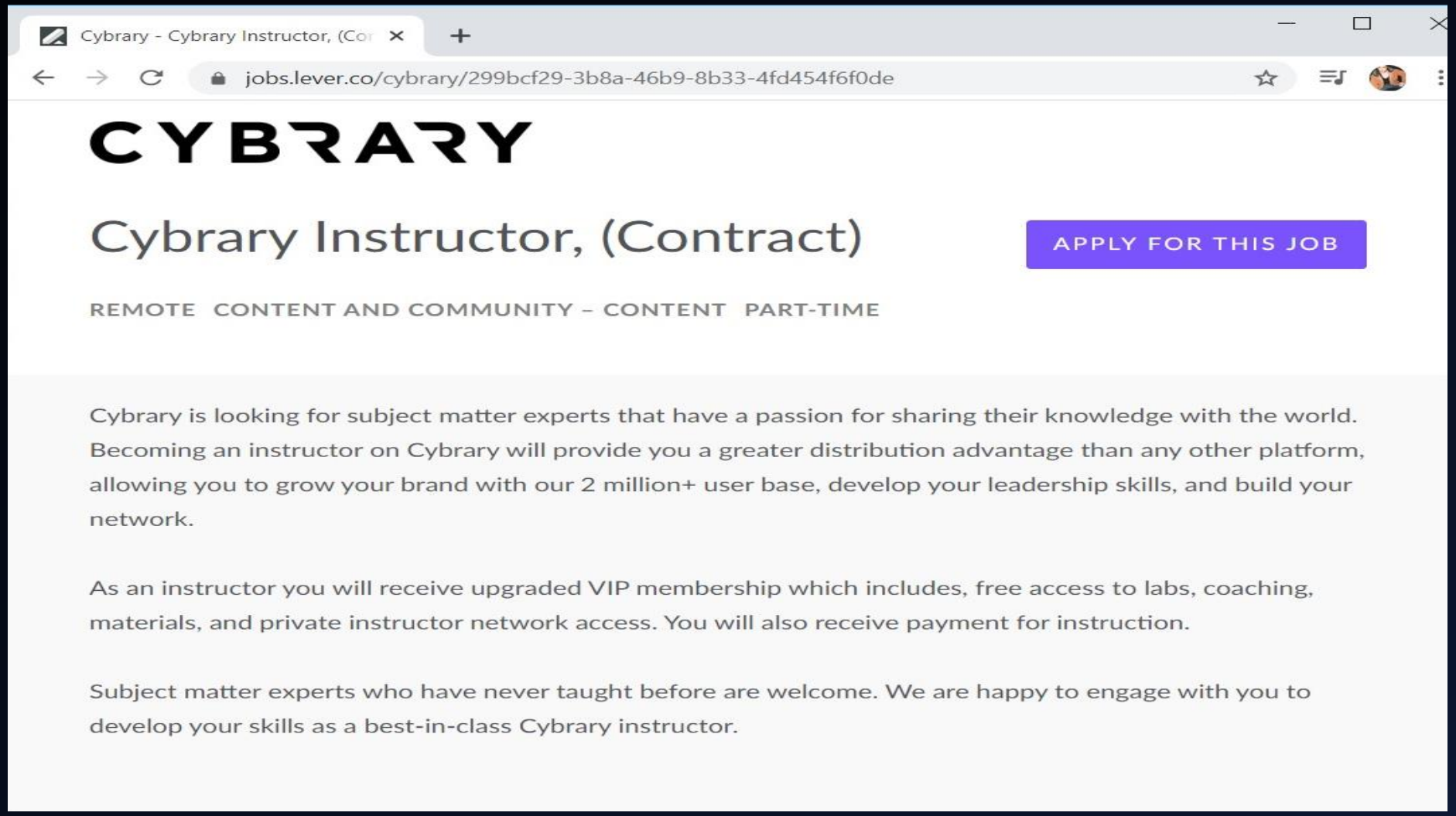
CYBRARY Career Opportunities

https://www.cybrary.it/contribute/



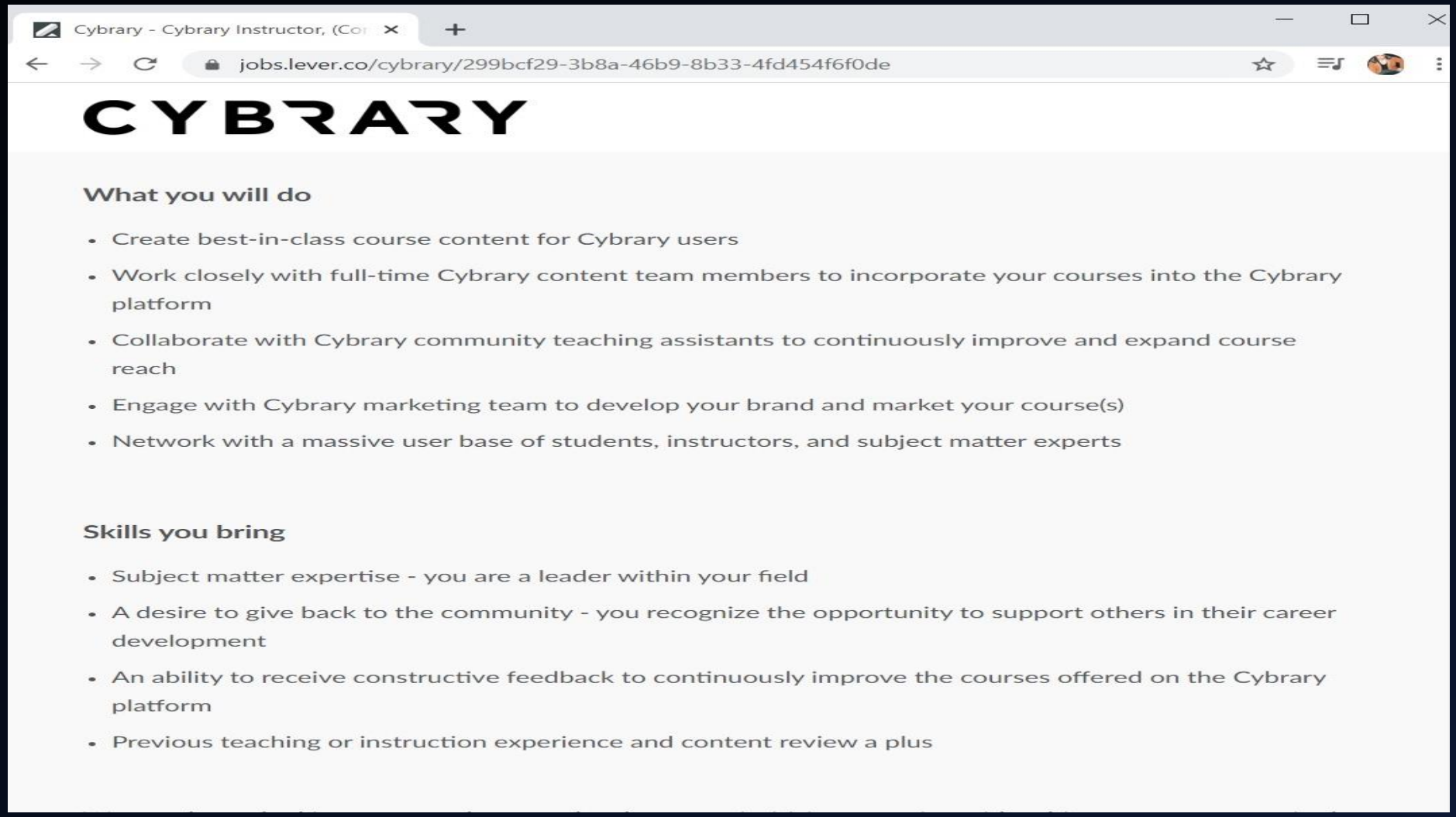
CYBRARY Instructor

https://jobs.lever.co/cybrary/299bcf29-3b8a-46b9-8b33-4fd454f6f0de



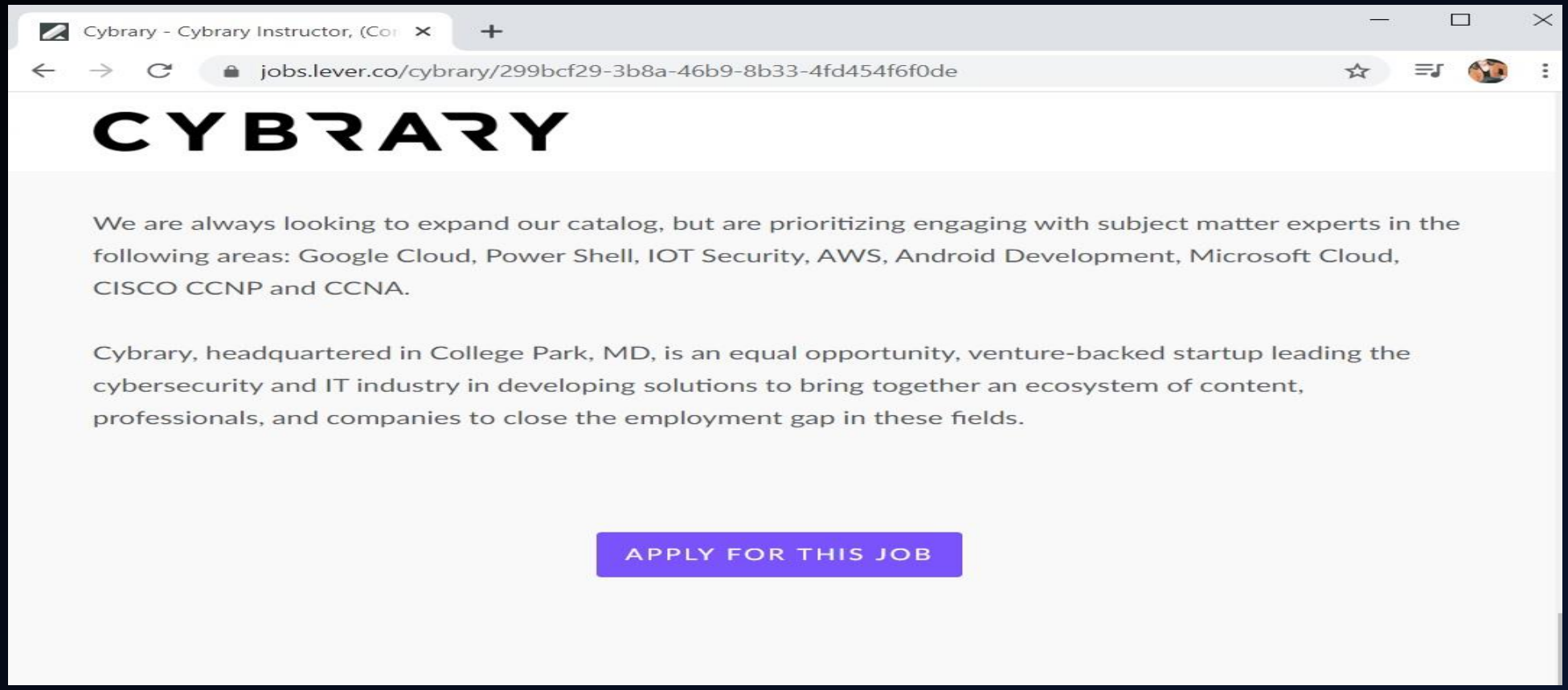
CYBRARY Instructor

https://jobs.lever.co/cybrary/299bcf29-3b8a-46b9-8b33-4fd454f6f0de



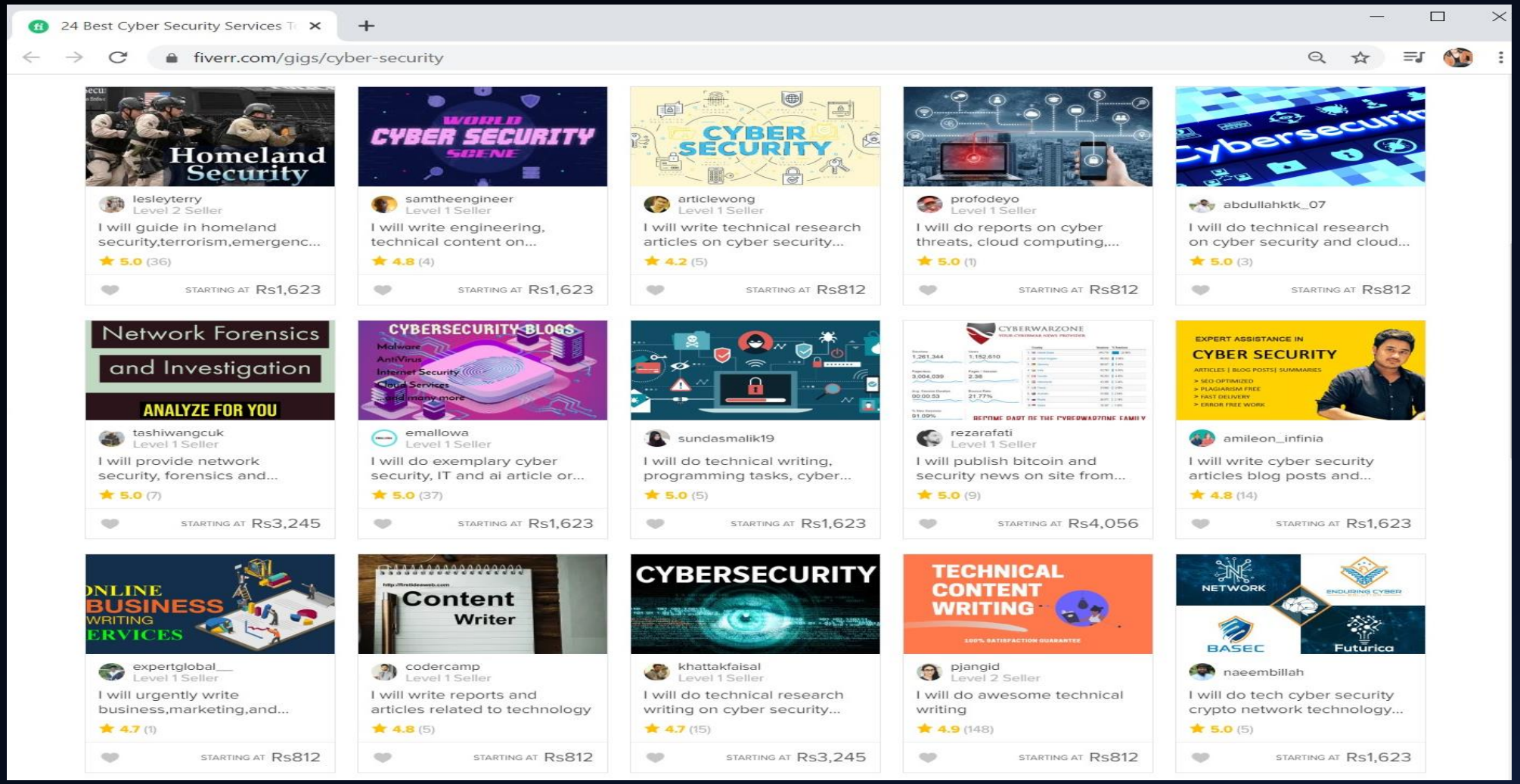
CYBRARY Instructor

https://jobs.lever.co/cybrary/299bcf29-3b8a-46b9-8b33-4fd454f6f0de



Fiverr Security Projects

https://www.fiverr.com/gigs/cyber-security



Online Job Application / Search Sources

- Job Websites / Online Career Portals
- Social Media
  - Facebook
  - LinkedIn
- Company Websites
- InfoSec Organization’s career portals

Other Ways

- Search for company contact, submit CV’s, turn up in-person.
- Word of mouth
  - Increase your social circle
- Attend InfoSec/IT related meetups, seminars, workshops & conferences.

Where the cybersecurity jobs are

Metros with the most job postings for cybersecurity roles

Rank	Metro area	Rank	Metro area
1	Washington, DC	6	Atlanta, GA
2	New York, NY	7	Boston, MA
3	Dallas-Fort Worth, TX	8	San Francisco, CA
4	Baltimore, MD	9	Los Angeles, CA
5	Chicago, IL	10	San Jose, CA

Source: Indeed

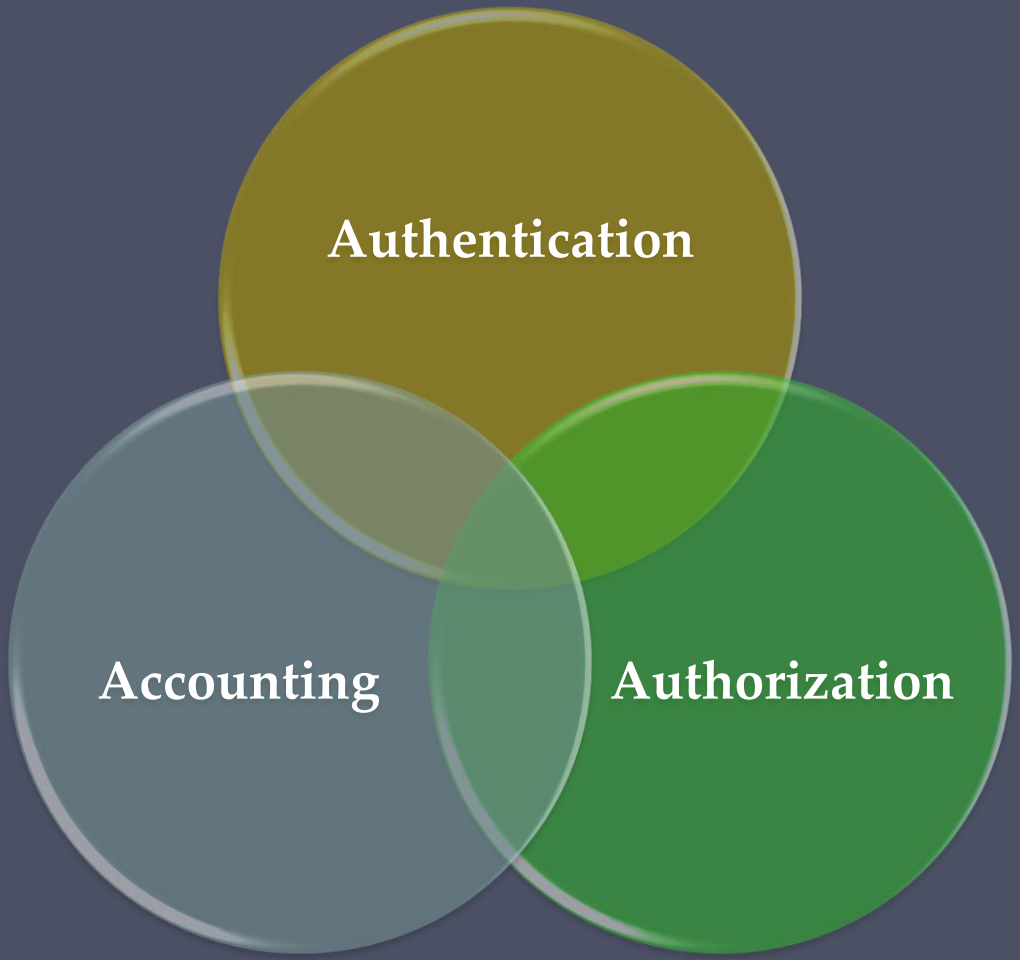
indeed

Pre-requisites / Previous Knowledge

- Hardware
  - PC, Server, DC
  - Network Devices: Router, Switch, Load Balancer
- Operating Systems
  - Microsoft Windows, Apple Mac, Unix, Linux
- Networking
  - OSI, TCP/IP, Ports, Protocols, Devices
- Virtualization / Cloud Computing
- Programming / Scripting



User Authentication and Access Control



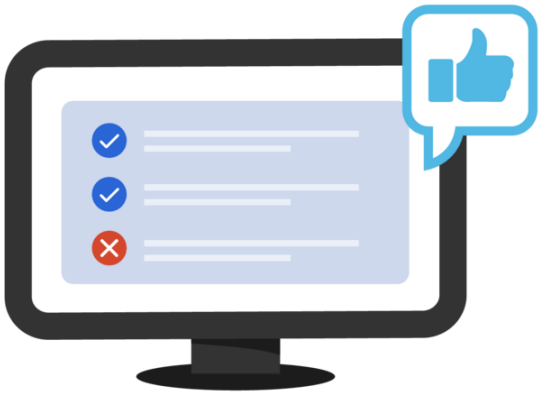
Authentication, Authorization, and Accounting (AAA)

Authentication



Confirms users
are who they say they are.

Authorization



Gives users permission
to access a resource.

Accounting



Measures the resources a user
consumes during access

Authentication, **Authorization, and Accounting** (**AAA**)

AAA is a term referred to the framework for

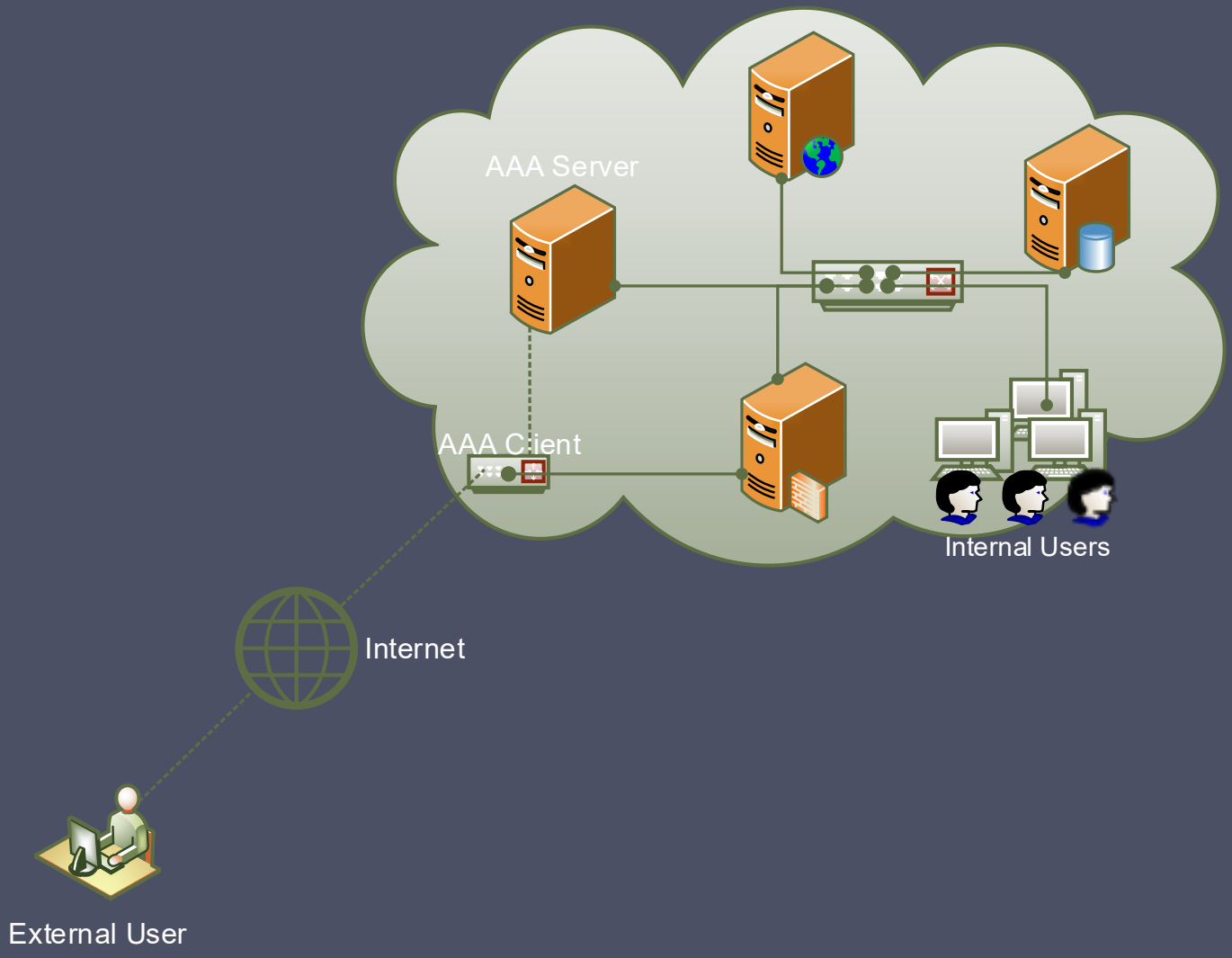
- Intelligently controlling access to the systems and resources
- Enforcing polices
- Auditing usage…

Source: https://www.okta.com/identity-101/authentication-vs-authorization/

Illustration – Physical World



Illustration – Cyber World




IDENTITY & ACCESS MANAGEMENT
Adobe Stock | #112340342

AAA vs. IAM

AAA

- AAA (Authentication, Authorization, and Accounting) is a general term that refers to a set of security processes that control access to computer resources.
- AAA servers are primarily used for network infrastructure.

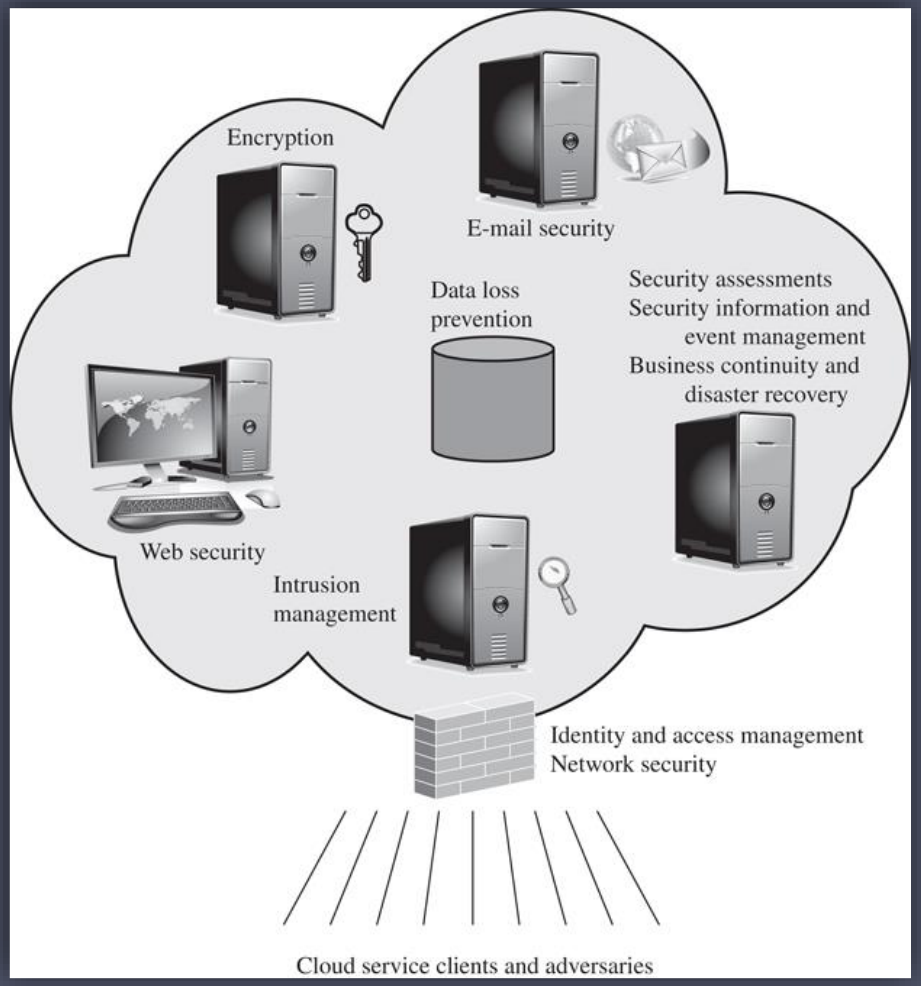
IAM

- IAM (Identity and Access Management) is a specific set of technologies and policies used to manage access to an organization's IT resources.
- IAM systems are used for managing access to enterprise applications and data.

Identity and Access Management (IAM)

To ensure that the right people and things have
- the right access to
- the right resources
- at the right time.

IAM include establishing trusted user profile and policy information, using it to control access within the cloud service, and doing this in an auditable way.



Elements of Cloud Security as a Service

Identity Theft

- Consumers lost $56 billion to identity fraud in America during 2021 [CNBC]
- The COVID-19 pandemic has created more points of vulnerability
- Identity theft scams - criminals interact directly with consumers to steal their information through methods such as robocalls and phishing emails.
- Three common red flags to watch
  - **Unsolicited calls or emails**
  - **High-pressure tactics**
  - **Outdated passwords**

Source https://www.cnbc.com/2021/03/23/consumers-lost-56-billion-dollars-to-identity-fraud-last-year.html



MEANS OF USER AUTHENTICATION

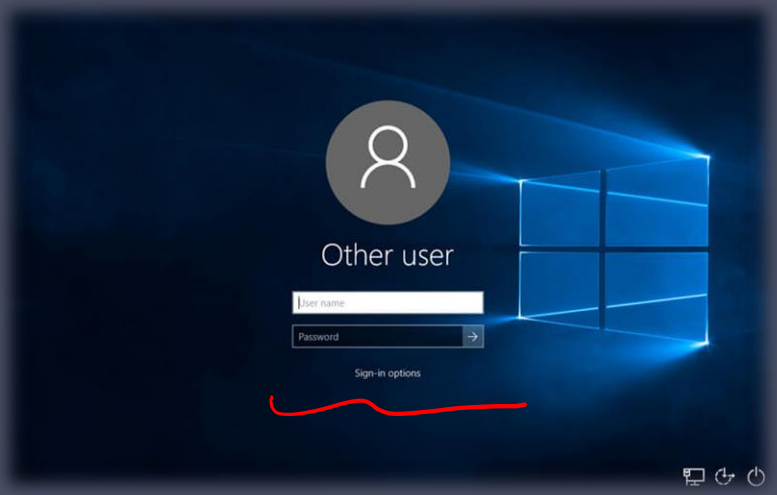
Recap


Authentication
USER NAME
******
login
Confirms users are who they say they are.
Authorization
Gives users permission to access a resource.
Accounting
Measures the resources a user consumes during access

The four means of authenticating user identity are based on:

1/4 Something the individual knows

- Password, PIN, answers to prearranged questions





The four means of authenticating user identity are based on:

2/4

Something the individual possesses (token)

- Smartcard, electronic keycard, physical key



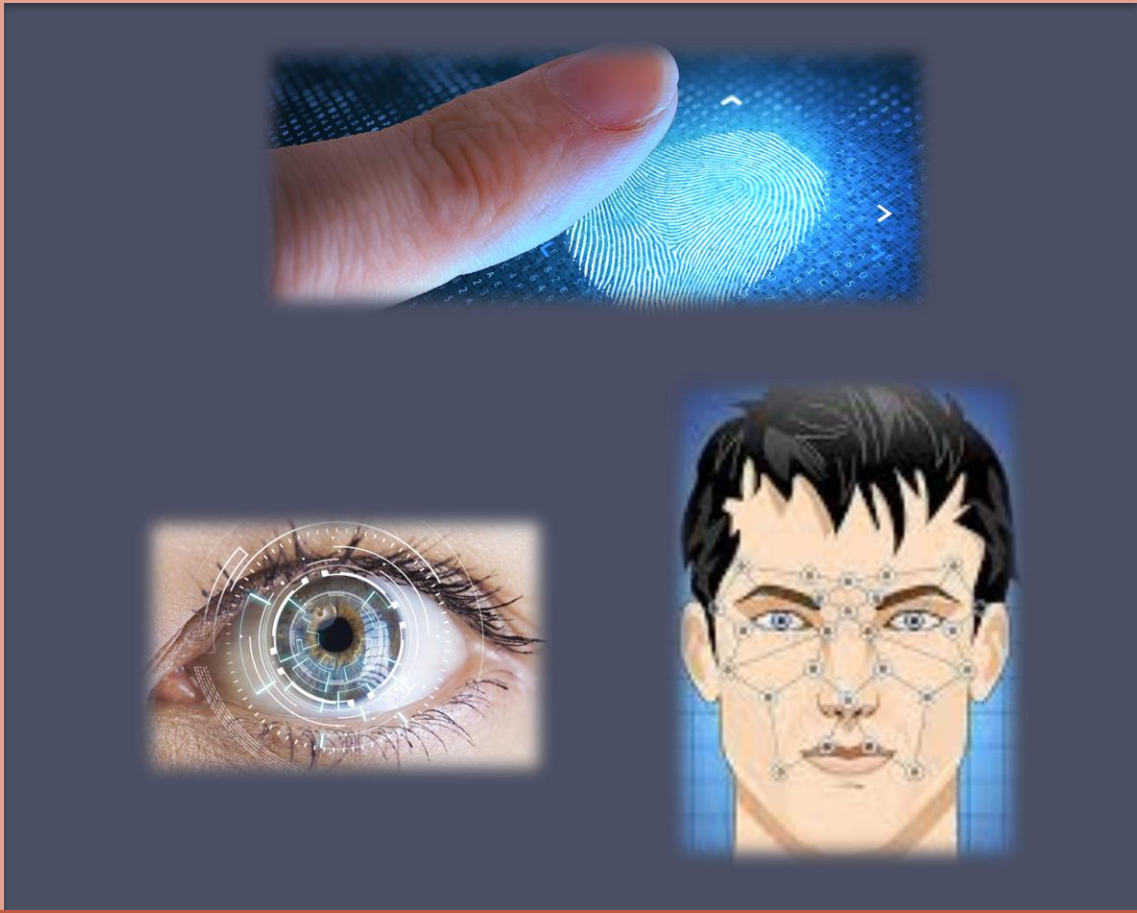


The four means of authenticating user identity are based on:

3/4

Something the individual is (static biometrics)

- Fingerprint, retina, face



The four means of authenticating user identity are based on:

4/4

Something the individual does (dynamic biometrics)

- Voice pattern, handwriting, typing rhythm





Summary

The four means of authenticating user identity are based on:

Something the individual knows

- Password, PIN, answers to prearranged questions

Something the individual possesses (token)

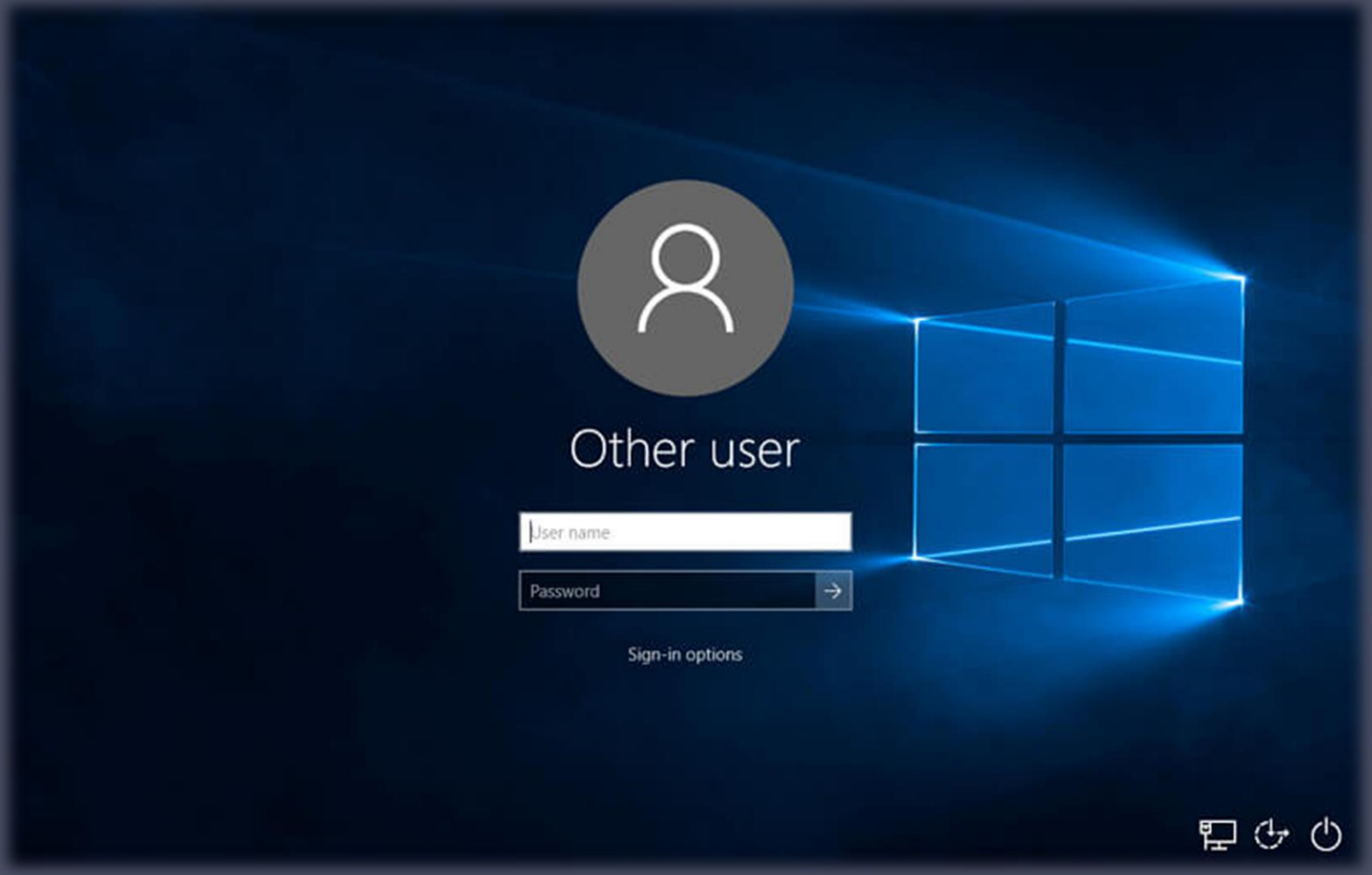
- Smartcard, electronic keycard, physical key

Something the individual is (static biometrics)

- Fingerprint, retina, face

Something the individual does (dynamic biometrics)

- Voice pattern, handwriting, typing rhythm



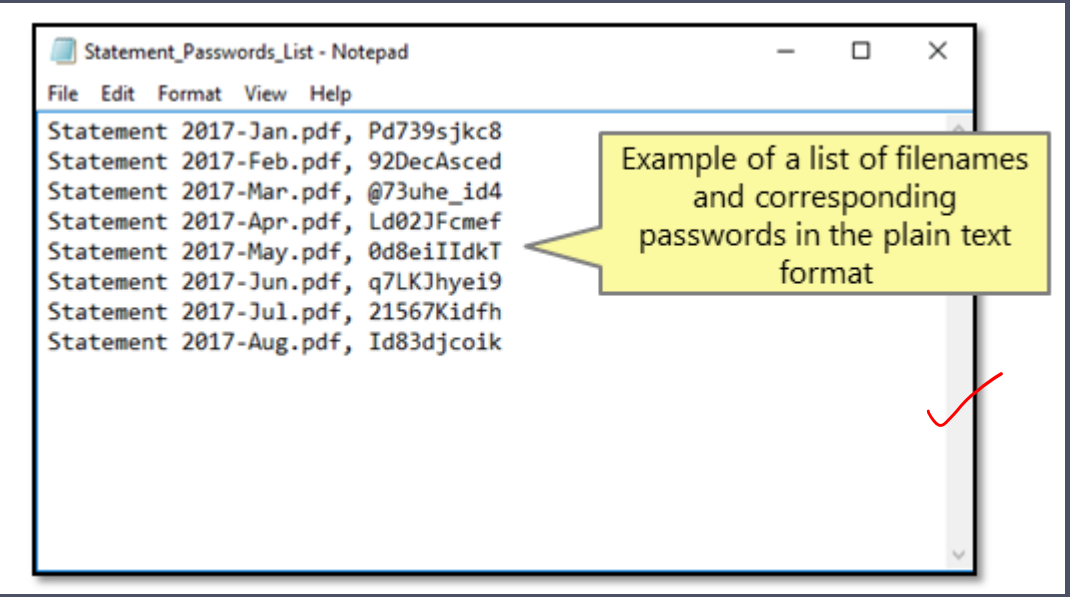
PASSWORD-BASED AUTHENTICATION

Password-Based Authentication



- Widely used line of defense against intruders
  - User provides name/login and password
  - System compares password with the one stored for that specified login
- The user ID:
  - Determines that the user is authorized to access the system
  - Determines the user's privileges
  - Is used in discretionary access control

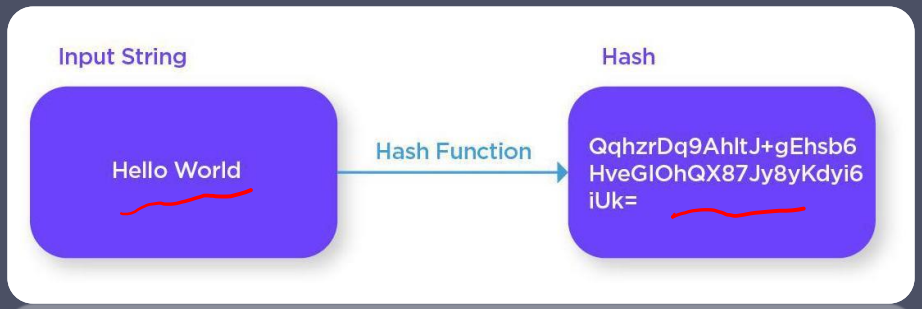
PASSWORD STORAGE
Plain Text



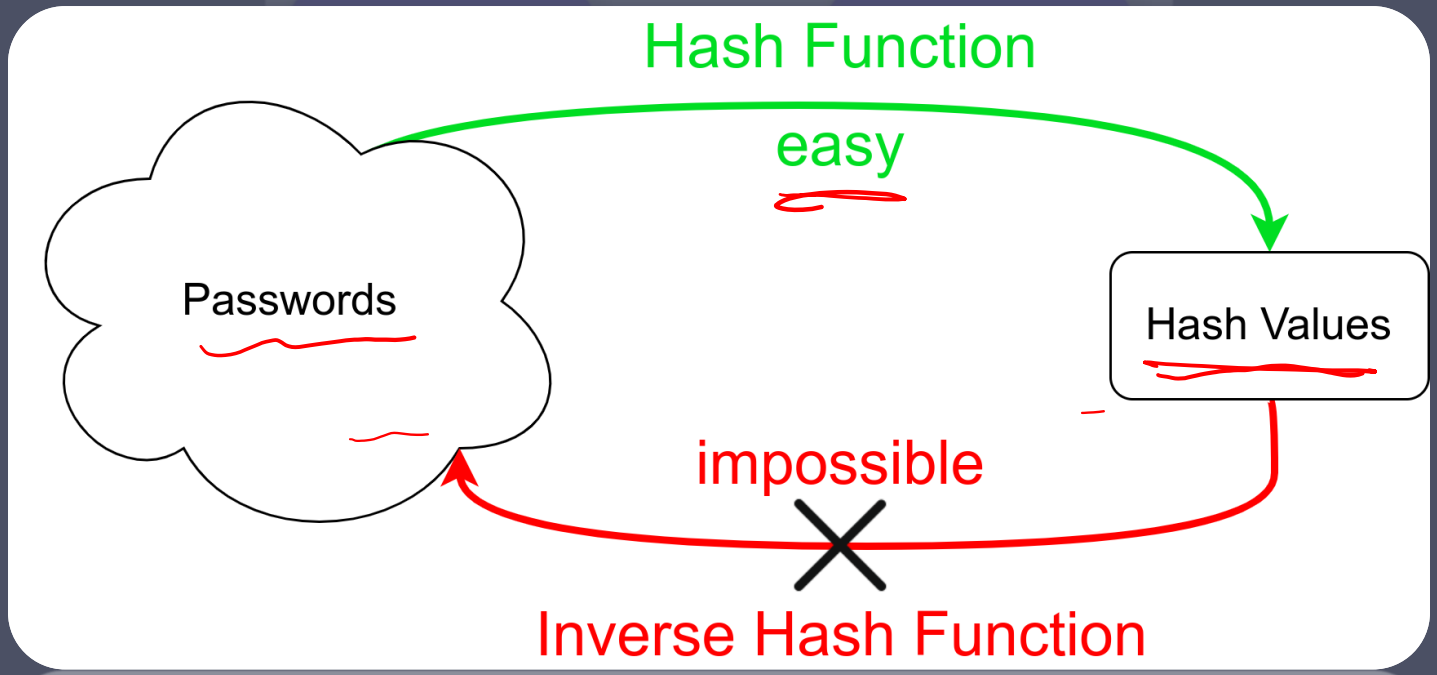
- Storing passwords in plaintext dangerous
  - because it puts both the system and users at risk.

PASSWORD STORAGE

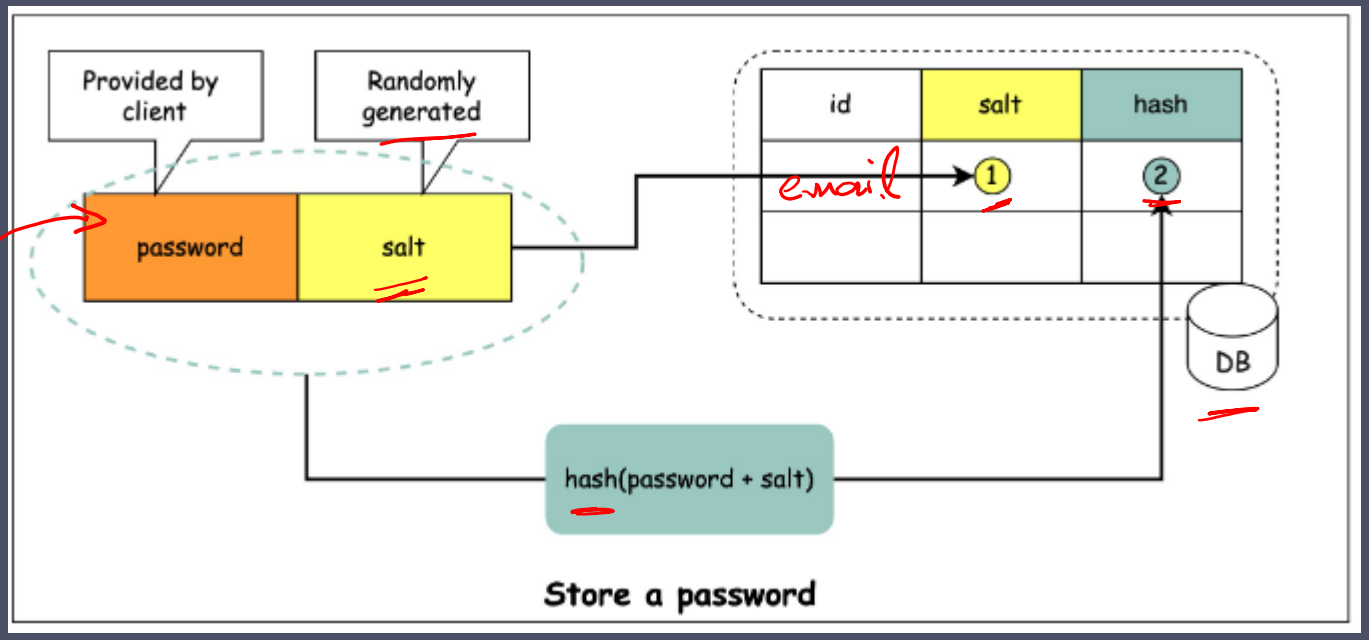
Hash Function



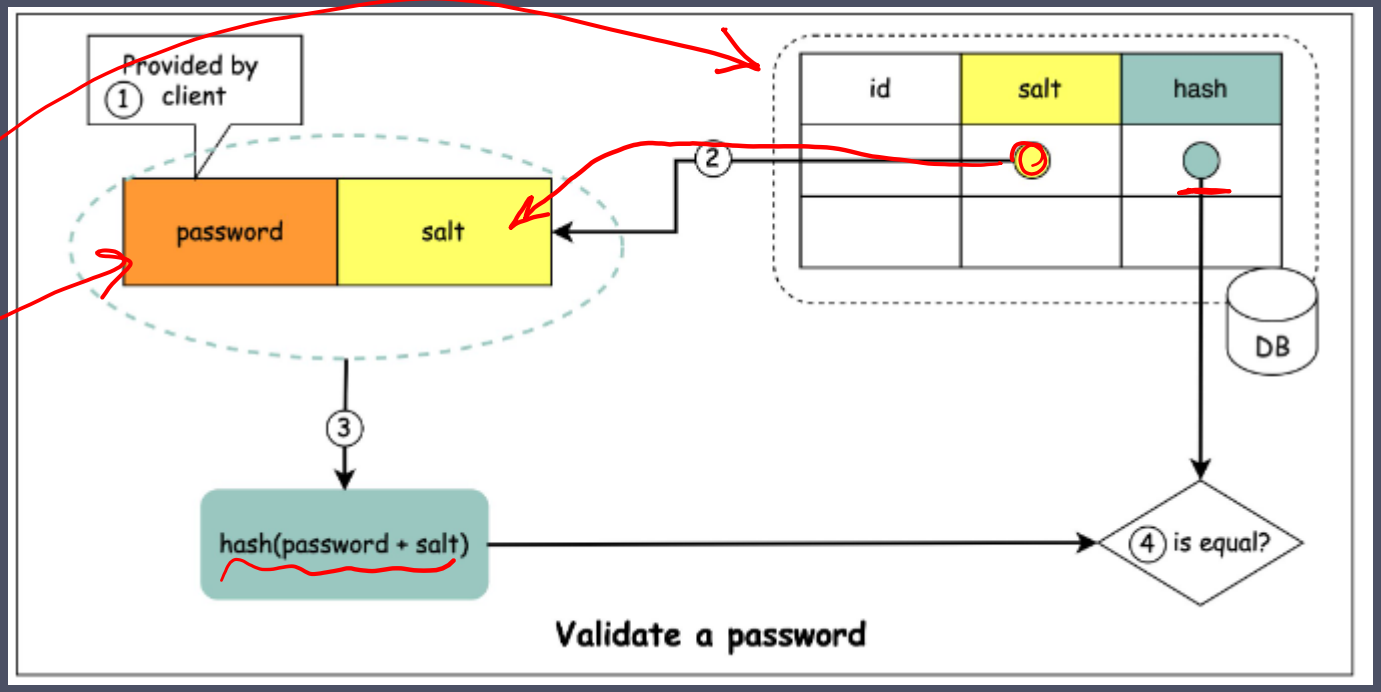
Demo




SIGN UP
Email
Password
SIGN UP


Provided by client
Randomly generated
password
salt
id
salt
hash
email
1
2
DB
hash(password + salt)
Store a password


Sign up
Login
Username *
Password *
Login


Provided by client
1
password
salt
2
id
salt
hash
DB
3
hash(password + salt)
4 is equal?
Validate a password



Password Vulnerabilities

Password Hacking and Cracking

- Password hacking and password cracking are terms that are often used interchangeably, but there is a subtle difference between the two.

- Password Hacking
  - refers to gaining unauthorized access to a system
  - Usually, original password is changed

- Password Cracking
  - to the process of attempting to recover a password
  - Usually, original password is NOT changed

Password Vulnerabilities

Exploiting user mistakes	•Users more likely use default passwords, write or share the passwords through social engineering tactics
Exploiting multiple password use	•Different network devices share the same or a similar password for a given user
Electronic monitoring	•Password communicated across a network in plaintext format
Brute force Attack	•Try all possible passwords
Offline dictionary attack	•Compares the password hashes against hashes of commonly used passwords
Rainbow table attacks	•Pre-compute tables of hash values of ALL passwords*

Offline Dictionary Attack

Dictionary of Commonly Used Passwords

Password	Password Hash
Jhon	Hkdjutye
Secret	Lfjaskebad
Bold	Fasf572dnas
2023	Adnskjf30
World	42n34nasd
…	…
…	…
Cooler	Af45xbc2js
…	…

Target User

UID	Password Hash
Admin	af45xbc2js

Rainbow Table Attack

Hash Values of ALL Passwords (of Length 04 in this example)

Password	Password Hash
Aaaa	Kfj8673hdb
Aaab	Hfge7w95j
Aaac	Jfhty673
Aaad	Hdg486hd
Aaae	Hdri9274
…	…
…	…
Cool	Rh75jd3h5
…	…

Target User

UID	Password Hash
Admin	Rh75jd3h5



Securing Passwords

Modern Approaches

- Complex password policy
  - Forcing users to pick stronger passwords
- However, password-cracking techniques have also improved
  - The processing capacity available for password cracking has increased dramatically
  - The use of sophisticated algorithms to generate potential passwords
  - Studying examples and structures of actual passwords in use

Password File Access Control

One way to block offline guessing attacks by denying access to encrypted passwords (password hashes)

- Make available only to privileged users
- Shadow password file

Vulnerabilities

- Weakness in the OS that allows access to the file
- Accident with permissions making it readable
- Users with same password on other systems
- Access from backup media
- Sniff passwords in network traffic

Password Selection Strategies

User education

Users can be told the importance of using hard to guess passwords and can be provided with guidelines for selecting strong passwords

Computer generated passwords

Users have trouble remembering them

Reactive password checking

System periodically runs its own password cracker to find guessable passwords

Complex password policy

User is allowed to select their own password, however the system checks to see if the password is allowable, and if not, rejects it

Goal is to eliminate guessable passwords while allowing the user to select a password that is memorable





Memory Cards and Smart Cards

Recall

The four means of authenticating user identity are based on:

Something the individual knows

- Password, PIN, answers to prearranged questions

Something the individual possesses (token)

- Smartcard, electronic keycard, physical key

Something the individual is (static biometrics)

- Fingerprint, retina, face

Something the individual does (dynamic biometrics)

- Voice pattern, handwriting, typing rhythm

Memory Cards

- Can store but do not process data
- The most common is the magnetic stripe card e.g. ATM
- Can include an internal electronic memory
- Can be used alone for physical access
  - Hotel room
  - ATM
- Provides significantly greater security when combined with a password or PIN
- Drawbacks of memory cards include:
  - Requires a special reader
  - Loss/theft of token/memory card
  - User dissatisfaction



Smart Tokens



https://upload.wikimedia.org/wikipedia/commons/d/db/SecurityTokens.CryptoCard.agr.jpg

- Physical characteristics:
  - Include an embedded microprocessor
  - A smart token may look like a bank card
  - Can look like calculators, keys, small portable objects
- User interface:
  - Manual interfaces include a keypad and display for human/token interaction
- Electronic interface
  - A smart card or other token requires an electronic interface to communicate with a compatible reader/writer
  - Contact and contactless interfaces
- Authentication protocol:
  - Classified into three categories:
    - Static
    - Dynamic password generator
    - Challenge-response

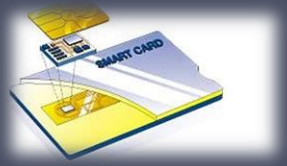
Smart Cards

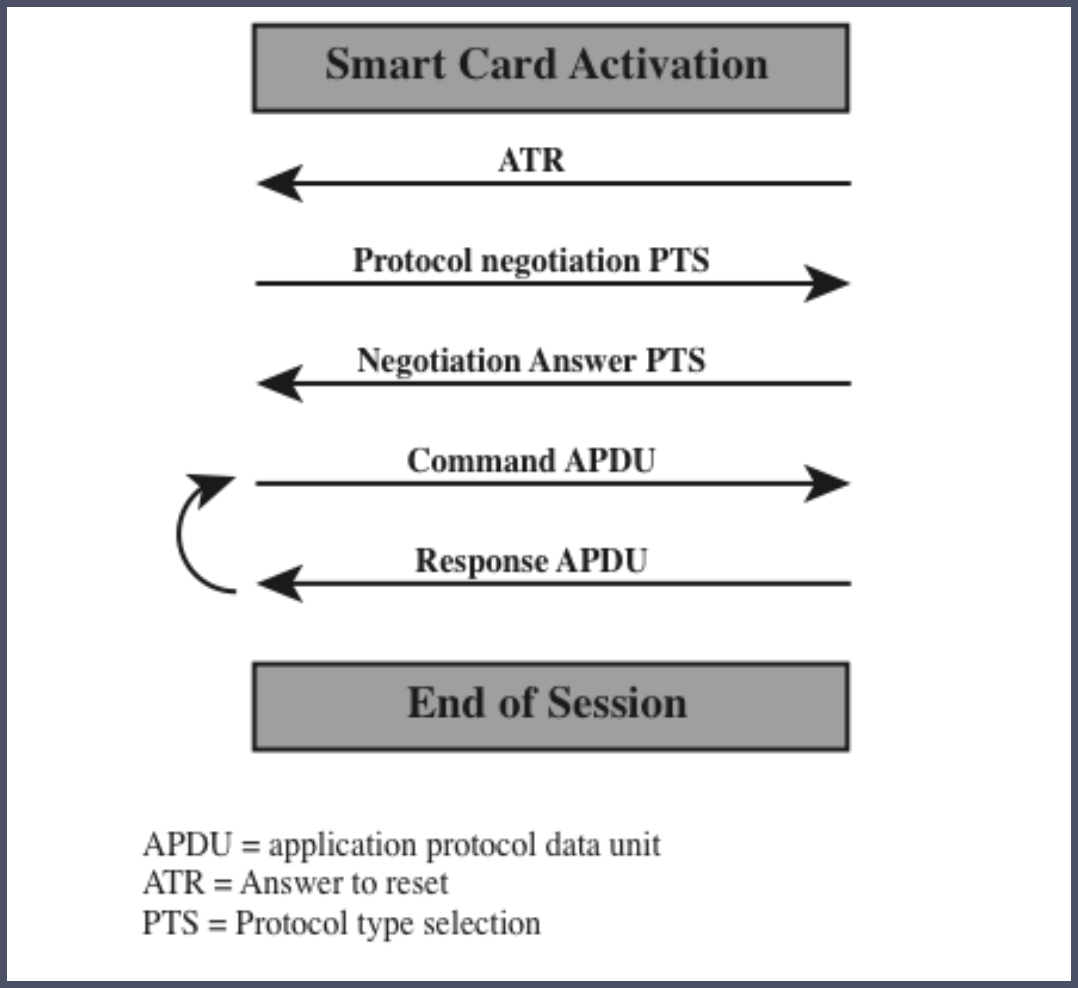
- Most important category of smart token
  - Has the appearance of a credit card
  - Has an electronic interface
  - May use any of the smart token protocols
- Contain:
  - An entire microprocessor
    - Processor
    - Memory
    - I/O ports
- Typically include three types of memory:
  - Read-only memory (ROM)
    - Stores data that does not change during the card's life
  - Electrically erasable programmable ROM (EEPROM)
    - Holds application data and programs
  - Random access memory (RAM)
    - Holds temporary data generated when applications are executed



Interaction Between Reader and Smart Card







APDU = application protocol data unit
ATR = Answer to reset
PTS = Protocol type selection



Biometric Authentication

Recall

The four means of authenticating user identity are based on:

Something the individual knows

- Password, PIN, answers to prearranged questions

Something the individual possesses (token)

- Smartcard, electronic keycard, physical key

Something the individual is (static biometrics)

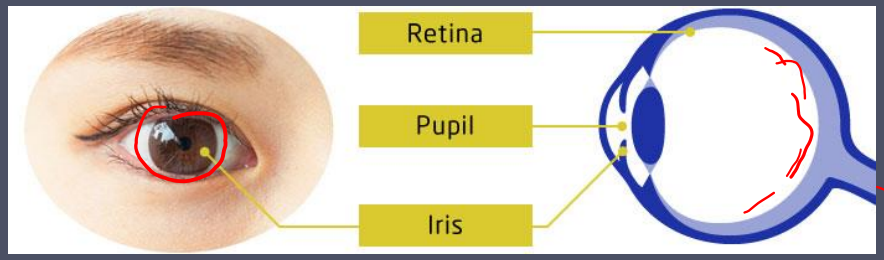
- Fingerprint, retina, face

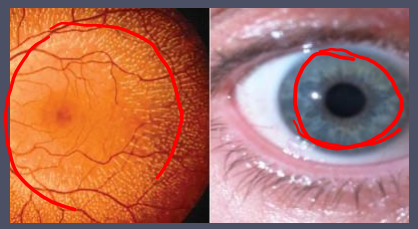
Something the individual does (dynamic biometrics)

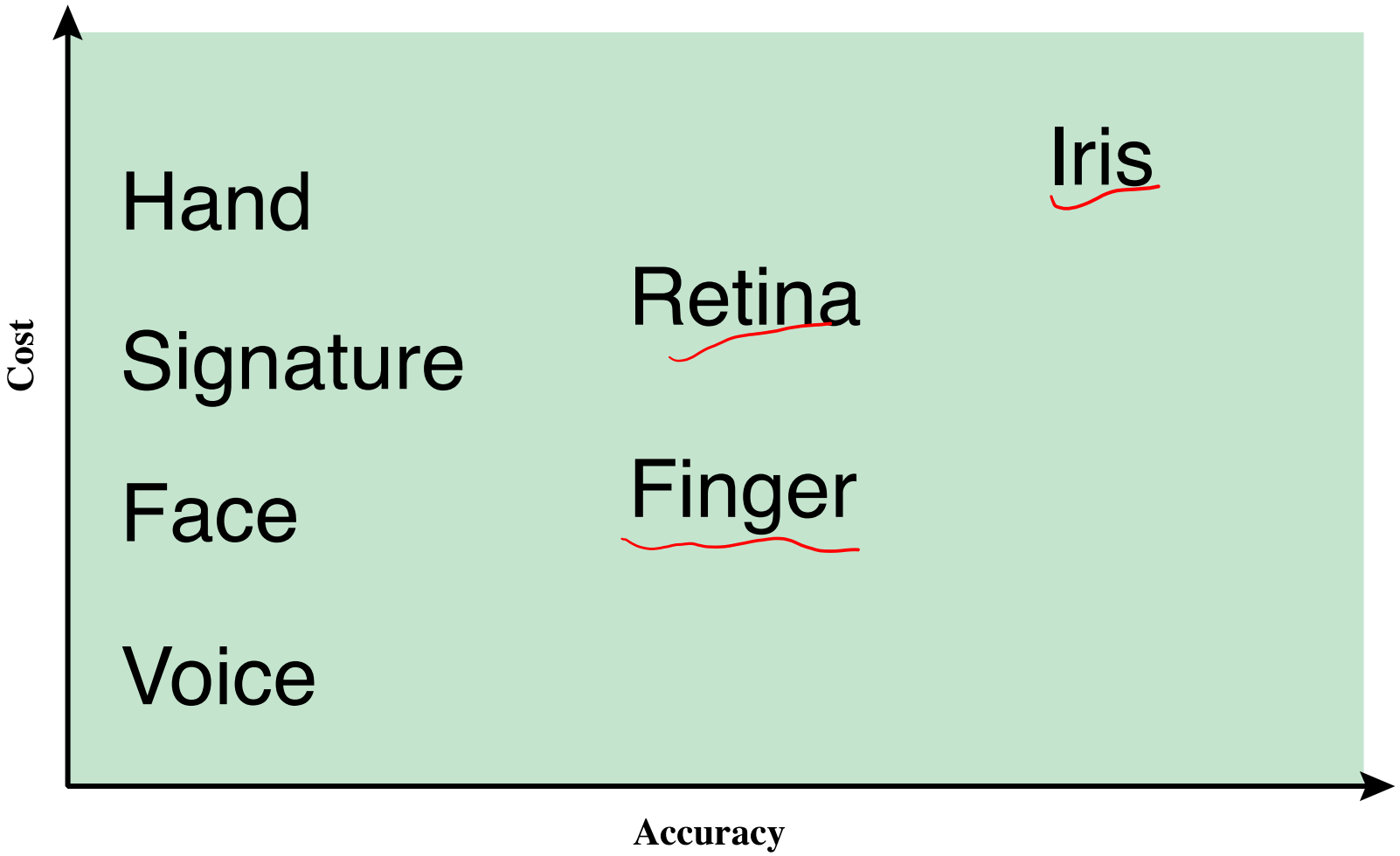
- Voice pattern, handwriting, typing rhythm

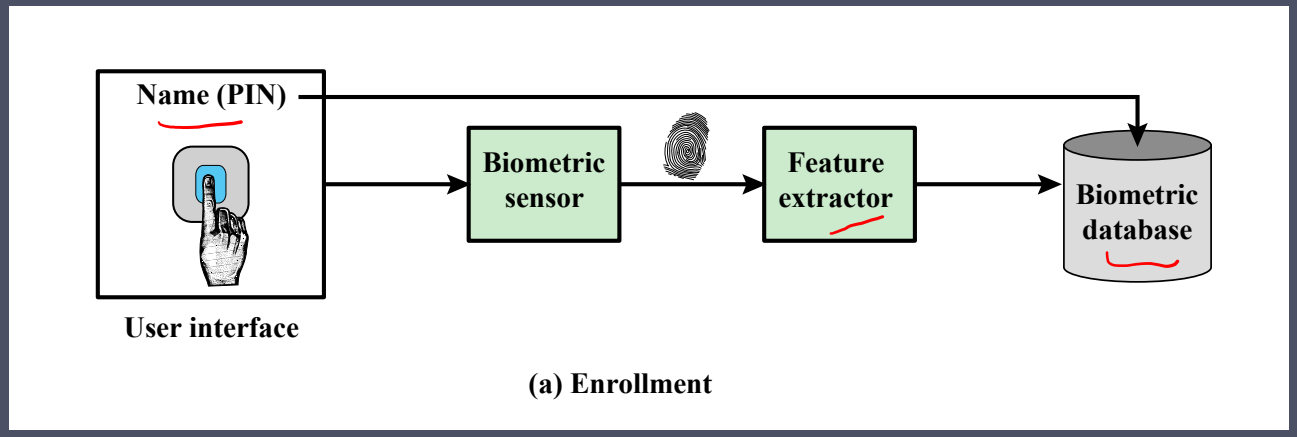
Biometric Authentication

- Attempts to authenticate an individual based on unique physical characteristics
- Based on pattern recognition
- This is technically complex and expensive when compared to passwords and tokens
- Physical characteristics used include:
  - Facial characteristics
  - Fingerprints
  - Hand geometry
  - Retinal pattern
  - Iris
  - Signature
  - Voice

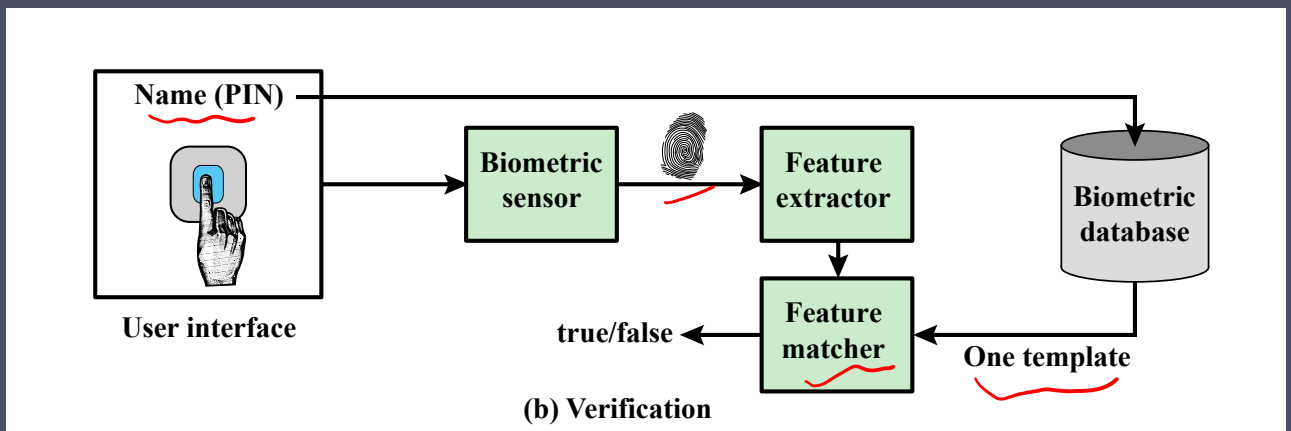




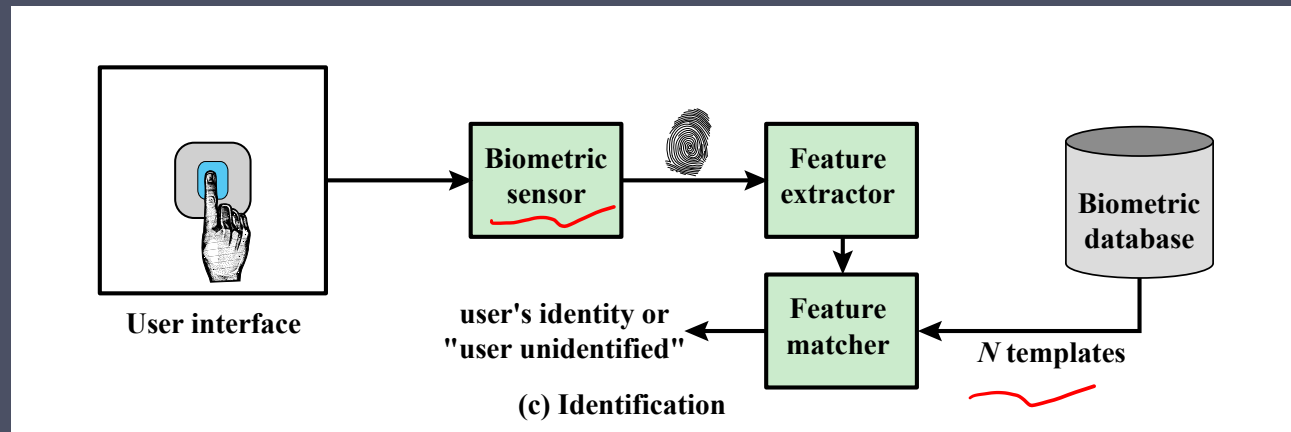

Hand
Signature
Face
Voice
Retina
Finger
Iris
Cost
Accuracy



(a) Enrollment



(b) Verification



(c) Identification

Biometric Authentication

Pros

- Difficult to frog
- Convenience
- More secure and non-transferable*

Cons

- Costly
- Complex
- False Acceptance Rate (FAR) and False Rejection Rate (FRR)
- Rigid
- Attacker can fool the system



Multi-factor Authentication

Recall

The four means of authenticating user identity are based on:

Something the individual knows

- Password, PIN, answers to prearranged questions

Something the individual possesses (token)

- Smartcard, electronic keycard, physical key

Something the individual is (static biometrics)

- Fingerprint, retina, face

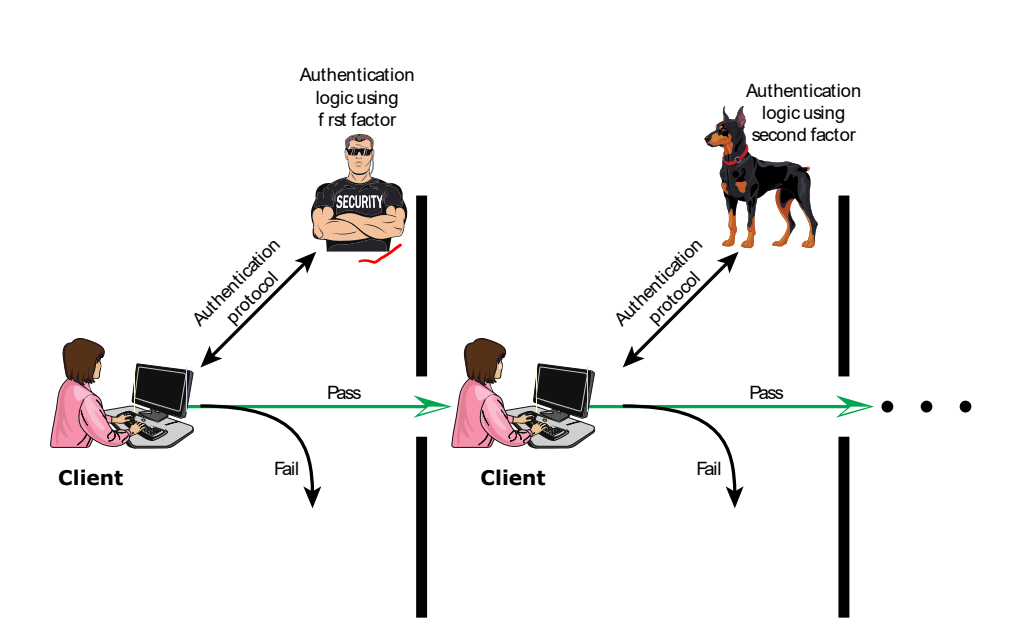
Something the individual does (dynamic biometrics)

- Voice pattern, handwriting, typing rhythm

Multi-factor Authentication

- 80% of hacking data breaches come from weak or compromised passwords, according to Verizon's 2019 Data Breach Investigations Report

- Multi-factor authentication (MFA) is the practice of requiring at least one additional form of user authentication—besides a password—when accessing a remote network.



Multi-factor Authentication

- Most Common Method for MFA
  - When logging in to a system remotely, the user first enters the regular password and is then prompted to enter the one-time password or passcode.
  - This is also commonly known as 2FA



SFA vs. 2FA vs. MFA

SFA

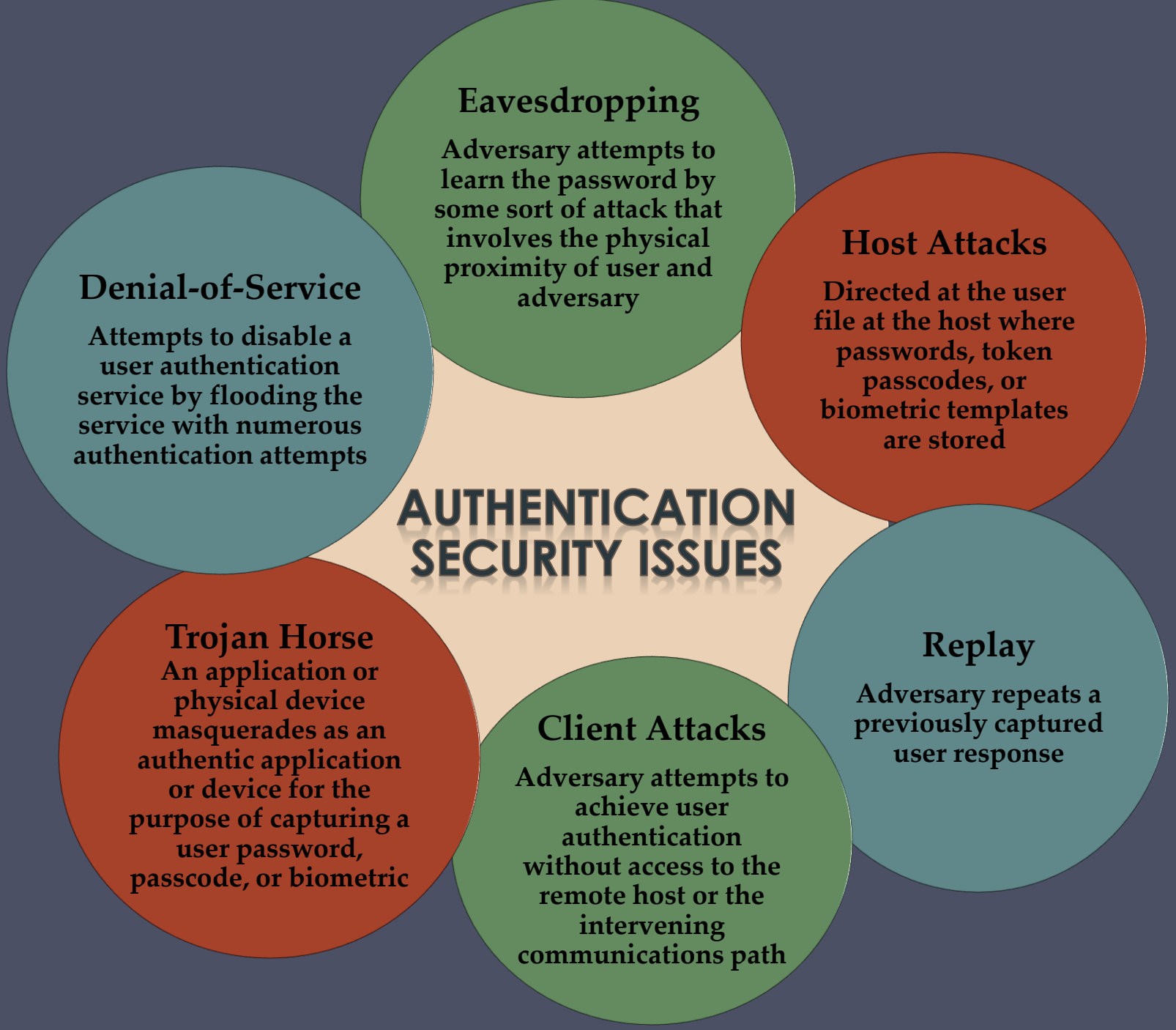
- Simplest form of authentication method.
- Matches one credential to verify a person online.
- The most popular example is password (credential) to a username.

2FA

- 2FA uses the same password/username combination, but with the addition of being asked to verify who a person is by using something only he or she owns, such as a mobile device.
- Putting it simply: it uses two factors to confirm an identity.

MFA

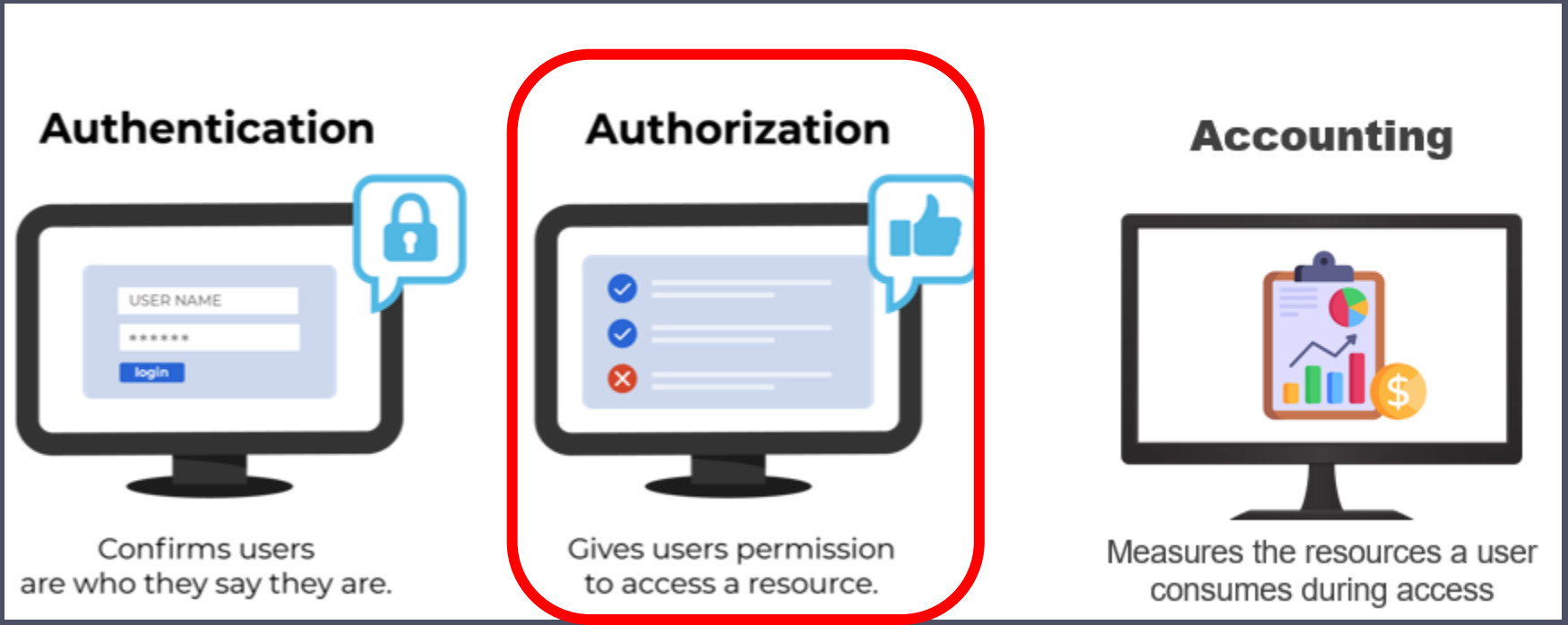
- Multi-factor authentication uses a combination of the following factors: something you know, something you have, and something you are.
- 2FA is a subset of MFA,


AUTHENTICATION SECURITY ISSUES
Eavesdropping
Adversary attempts to learn the password by some sort of attack that involves the physical proximity of user and adversary
Host Attacks
Directed at the user file at the host where passwords, token passcodes, or biometric templates are stored
Denial-of-Service
Attempts to disable a user authentication service by flooding the service with numerous authentication attempts
Replay
Adversary repeats a previously captured user response
Trojan Horse
An application or physical device masquerades as an authentic application or device for the purpose of capturing a user password, passcode, or biometric
Client Attacks
Adversary attempts to achieve user authentication without access to the remote host or the intervening communications path



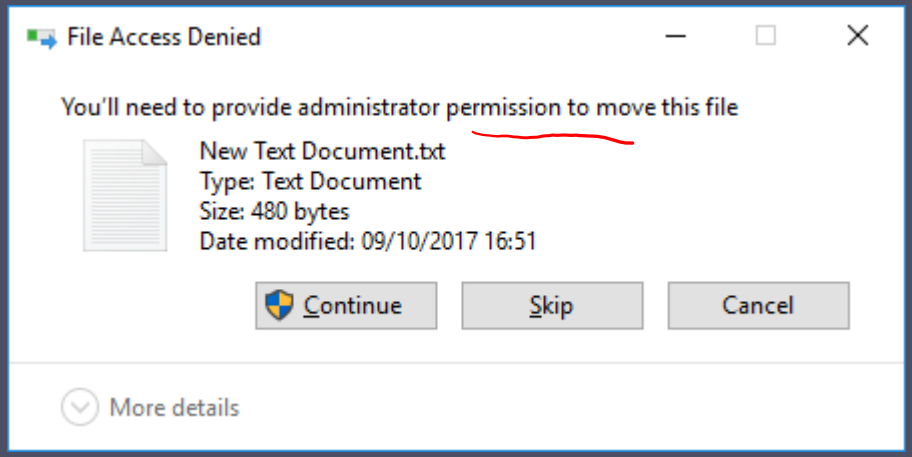
Access Control

Recap

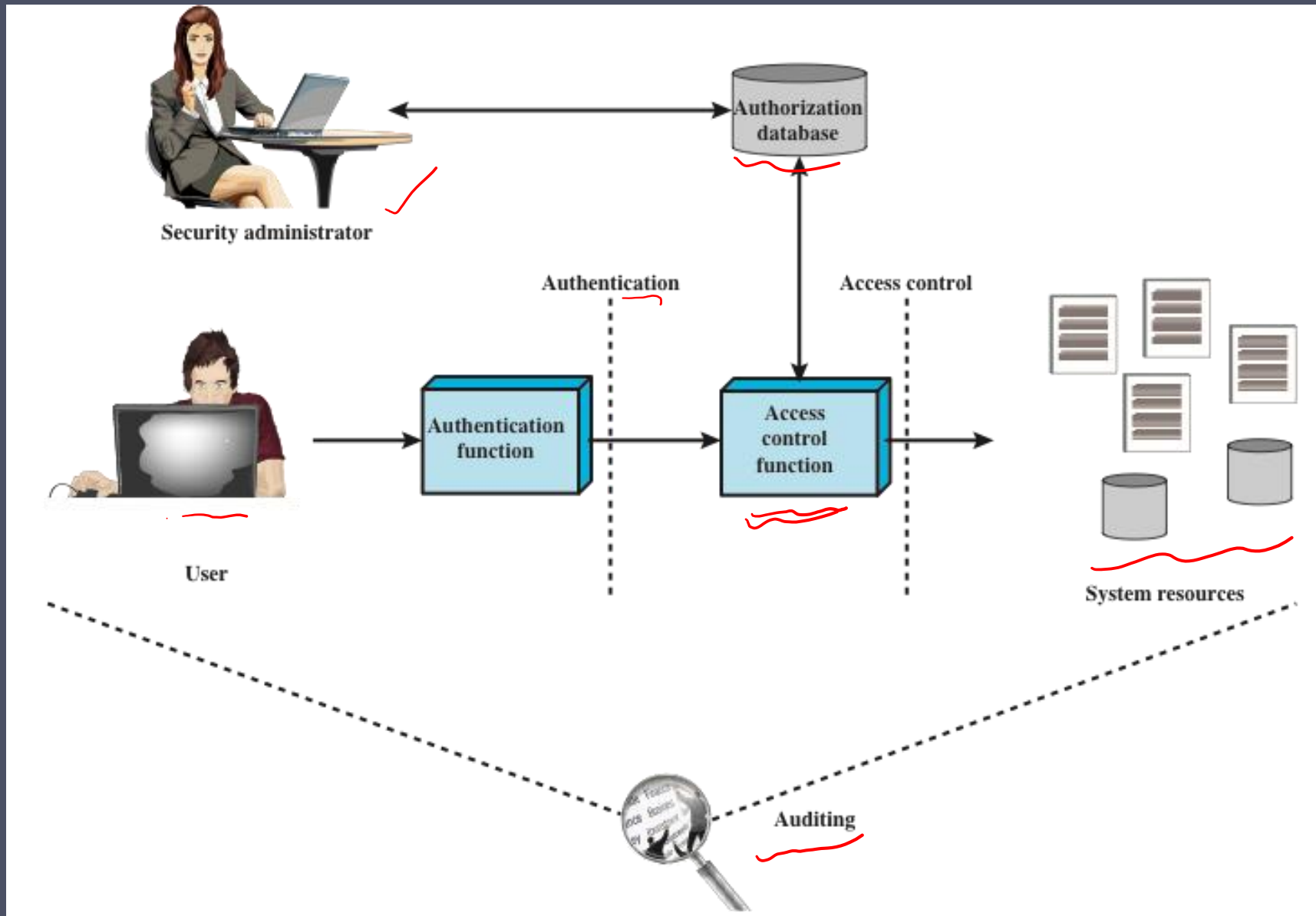

Authentication
USER NAME
******
login
Confirms users
are who they say they are.
Authorization
Gives users permission
to access a resource.
Accounting
Measures the resources a user
consumes during access

Access Control

"the process of granting or denying specific requests to: (1) obtain and use information and related information processing services; and (2) enter specific physical facilities"






Authorization database
Security administrator
Authentication
Access control
Authentication function
Access control function
User
System resources
Auditing

Subjects, Objects, and Access Rights

Subject

An entity capable of accessing objects

Three classes
- Owner
- Group
- World (Everyone)

Object

A resource to which access is controlled

Entity used to contain and/or receive information

Access right

Describes the way in which a subject may access an object

Could include:
- Read
- Write
- Execute
- Delete
- Create
- Search



Access Control Policies

https://www.assurancelab.com.au/resources/post/user-access-controls#gallery

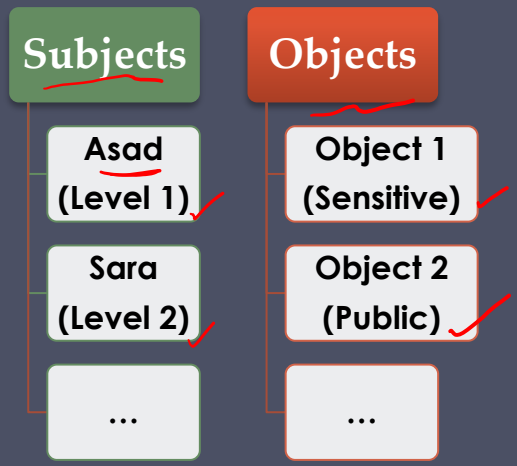
Access Control Policies

- Mandatory access control (MAC)
- Discretionary access control (DAC)
- Role-based access control (RBAC)
- Attribute-based access control (ABAC)

Mandatory Access Control (MAC)

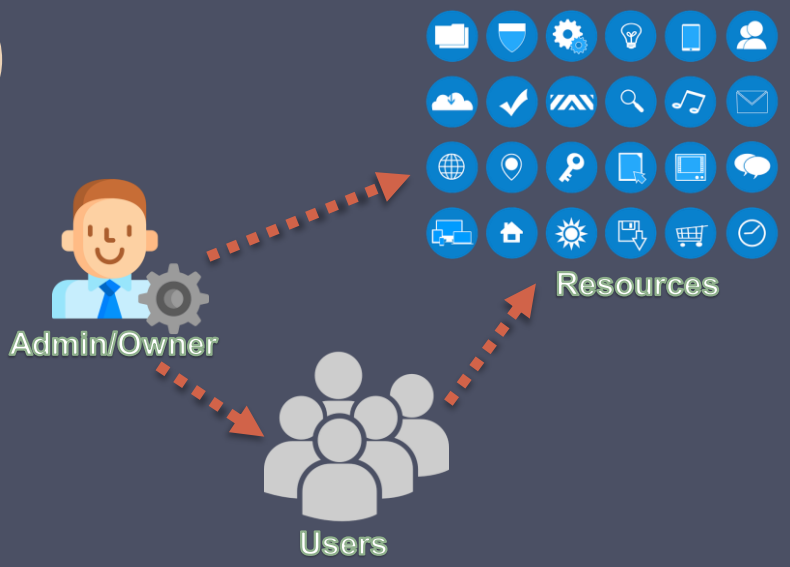
- Controls access based on comparing security labels (which indicate how sensitive or critical system resources are) with security clearances (which indicate system entities are eligible to access certain resources).
- This policy is termed *mandatory because*
  - *passing through security* clearance is *mandatory* for every user…
  - *an entity that has* clearance to access a resource may not, just by its own volition, enable another entity to access that resource.
- Commonly used in organizations where confidentiality is very important e.g. military etc.
- The higher the clearance the more in depth the background checks should be.

Military Classification	Business Classification
TOP SECRET	HIGHLY SENSITIVE
SECRET	SENSITIVE
CONFIDENCIAL	INTERNAL
UNCLASSIFIED	PUBLIC



Discretionary Access Control (DAC)

- Scheme in which an entity may be granted access rights that permit the entity, by its own volition, to enable another entity to access some resource
- Often provided using an **Access Matrix**
  - One dimension consists of identified subjects that may attempt data access to the resources
  - The other dimension lists the objects that may be accessed
- Each entry in the matrix indicates the access rights of a particular subject for a particular object
- Controls access based on the identity
- Useful for small size organizations…

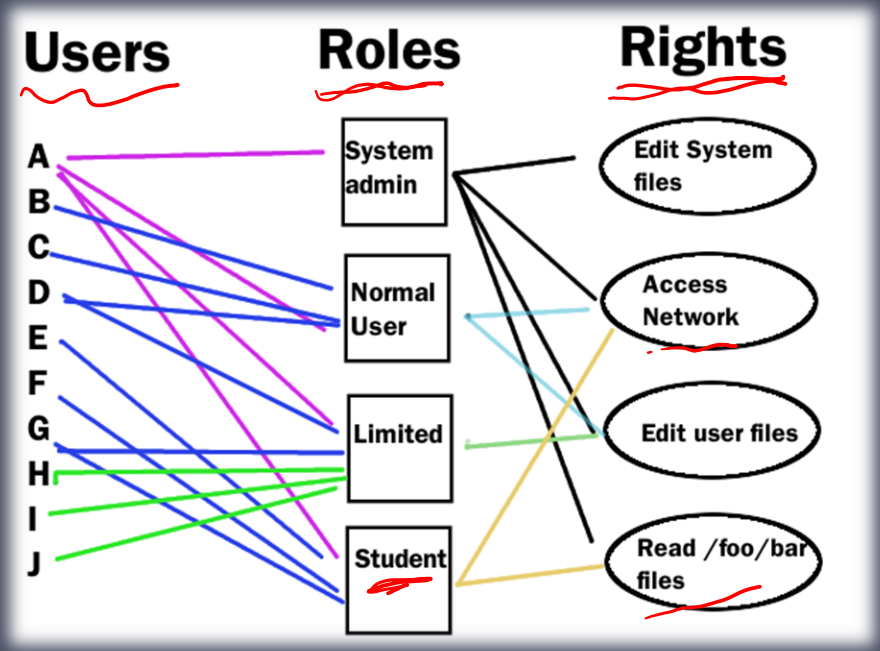


Objects	Users: U1	U2	U3	U4	...	Un
O1		Read/ Write	Write	Read/ Write		
O2	Read					Write
O3	Write			Read/ Write		Read

Access Matrix

Role-based Access Control (RBAC)

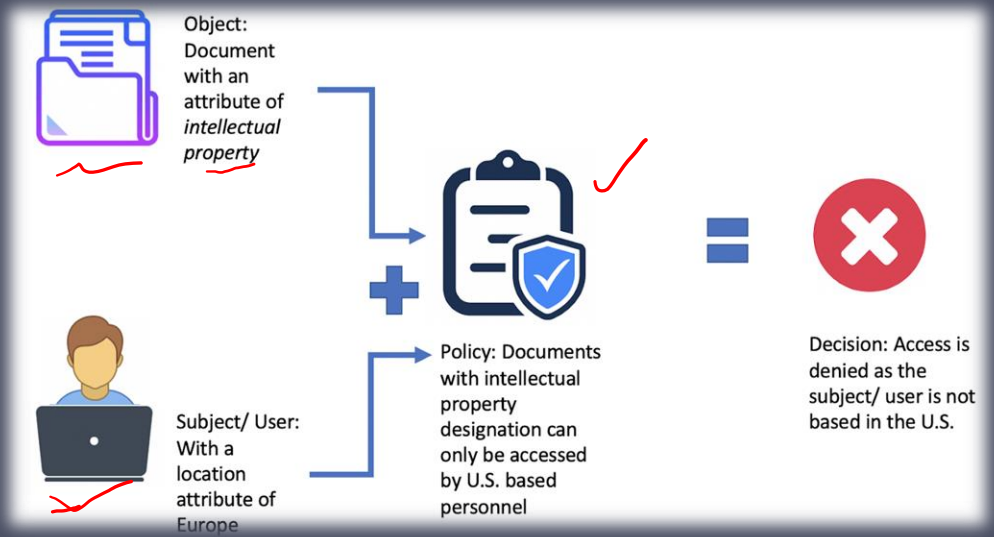
- DAC is not feasible for large size organizations…
  - Something better and easy to manage is needed
- Among such solutions is RBAC
- Controls access based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles.

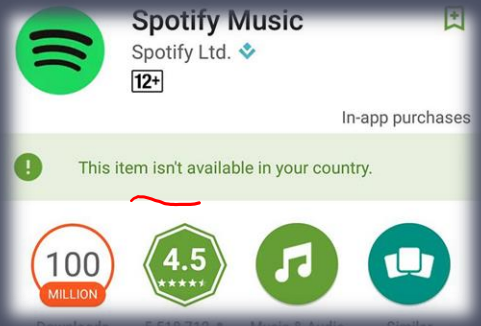


https://sites.google.com/site/cacsolin/role-based-access-control

Attribute-based Access Control (ABAC)

- Controls access based on attributes of the user, the resource to be accessed, and current environmental conditions and policies.





Object Attributes	Subject Attributes	Environment Conditions Attributes
• Type • Author • Owner • Date Created • Last Updated • Classification	• Name • Employee # • Designation • Department/ Affiliation • Clearance	• Location • Time Zone • Current time • Current Day

https://blog.privacera.com/what-is-attribute-based-access-control-and-why-is-it-important-70b91f4cad6

Summary

- Mandatory access control (MAC)
  - Controls access based on comparing security labels with security clearances
- Discretionary access control (DAC)
  - Controls access based on the identity of the requestor and on access rules (authorizations) stating what requestors are (or are not) allowed to do
- Role-based access control (RBAC)
  - Controls access based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles
- Attribute-based access control (ABAC)
  - Controls access based on attributes of the user, the resource to be accessed, and current environmental conditions



Cryptography

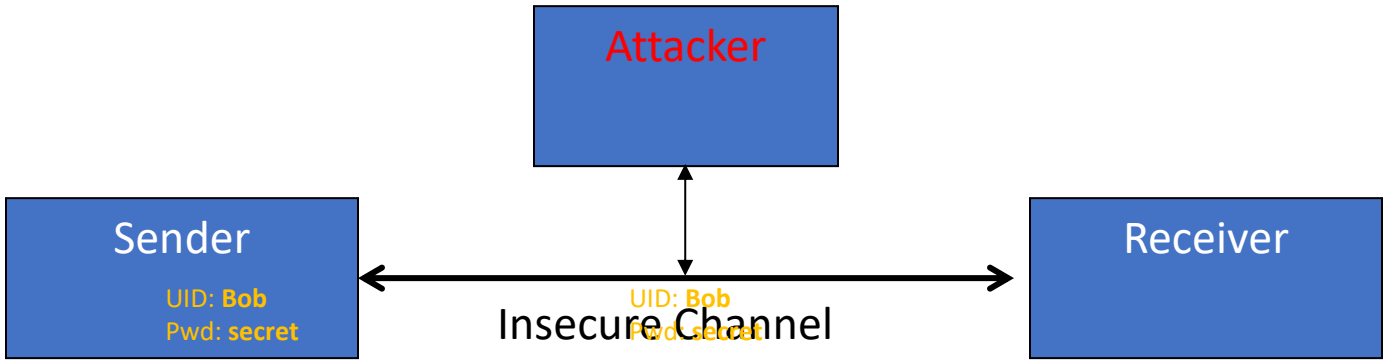
https://www.fortinet.com/resources/cyberglossary/what-is-cryptography

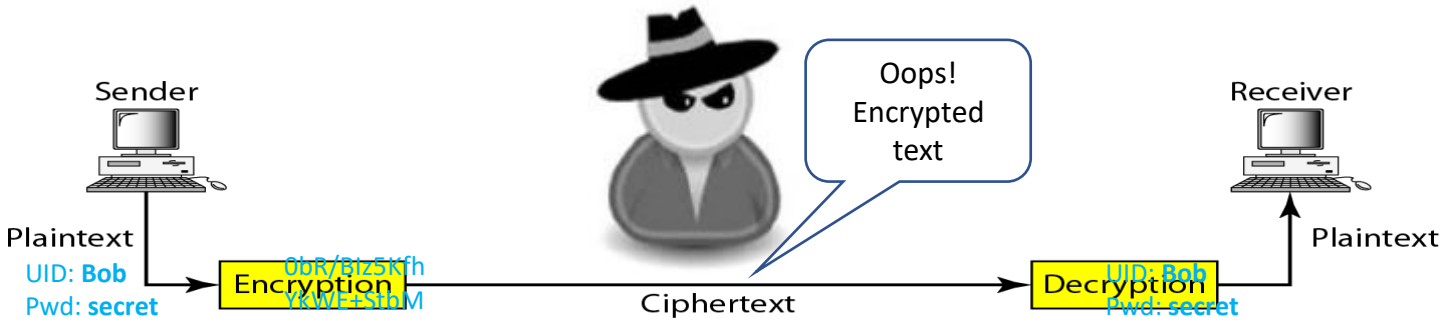
Cryptography

What is cryptography?

- **Cryptography**
  - The art of secret writing
  - Cryptography is the making
- **Cryptanalysis**
  - Cryptanalysis is the breaking

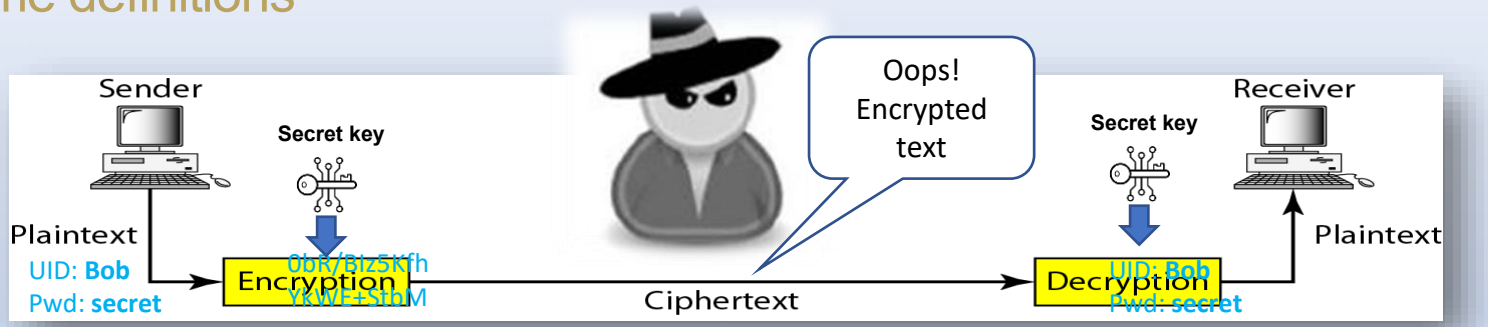
- **Why Cryptography?**
  - Cryptography aims to provide secure communications in the presence of an adversary/attacker.





Cryptography

Some definitions



Plaintext: This is the original message or data that is to be secured.

Encryption algorithm: This is the mechanism of securing the message and data. The encryption algorithm performs various substitutions and transformations on the plaintext.

Secret key: The secret key is also input to the algorithm. The exact substitutions and transformations performed by the algorithm depend on the key.

Ciphertext: This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts.

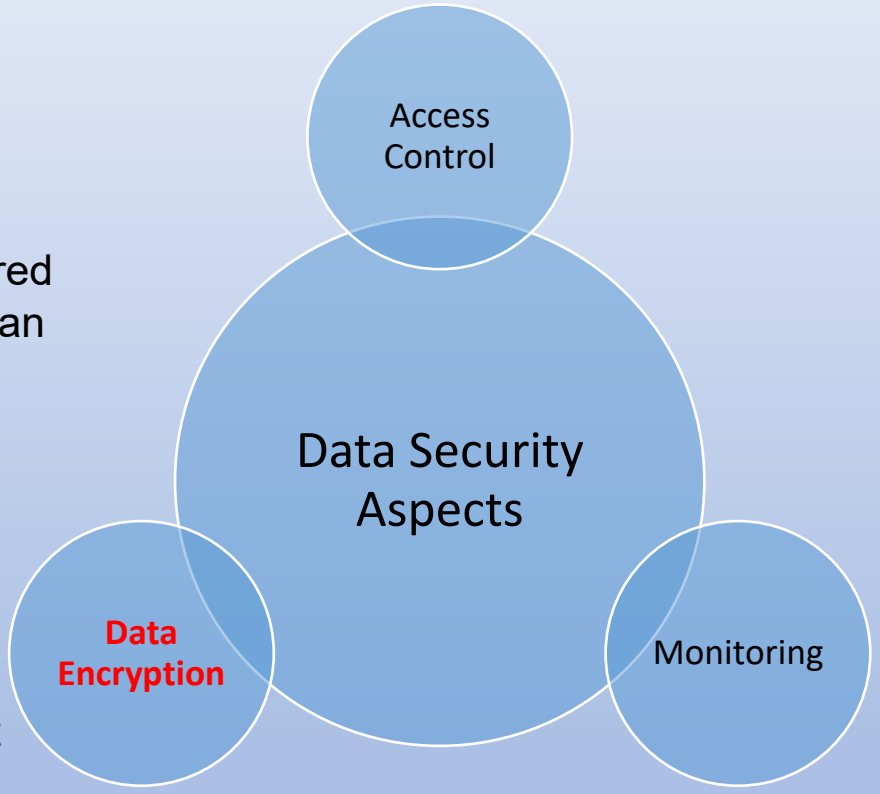
Decryption algorithm: This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the same secret key and produces the original plaintext.

Data Security Aspects

Data Security

Data Security Aspects

- **Access Control** who can access the data
- **Monitoring** who is using the data and how
- **Data Encryption** strong encryption is required to transform the data from plaintext (or human readable format) to cipher text
- **Stages of Data**
  - Data at rest
  - Data in transit
  - Data in use
- **Cryptographic algorithms** helps to protect the data in all stages from un-authorized access and alteration

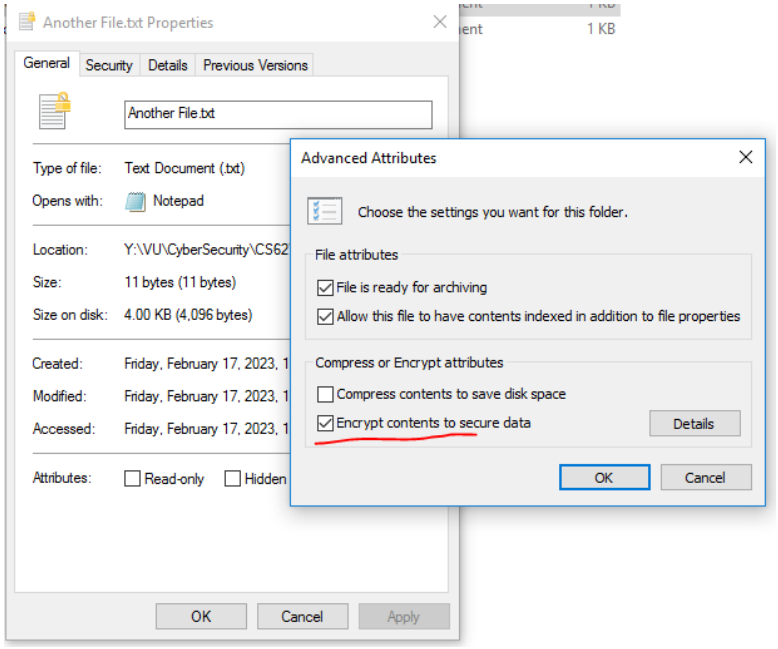


Data Security

Is it good to encrypt your files always?

- Encrypt when its needed…
- Be careful with Keys when encrypted…

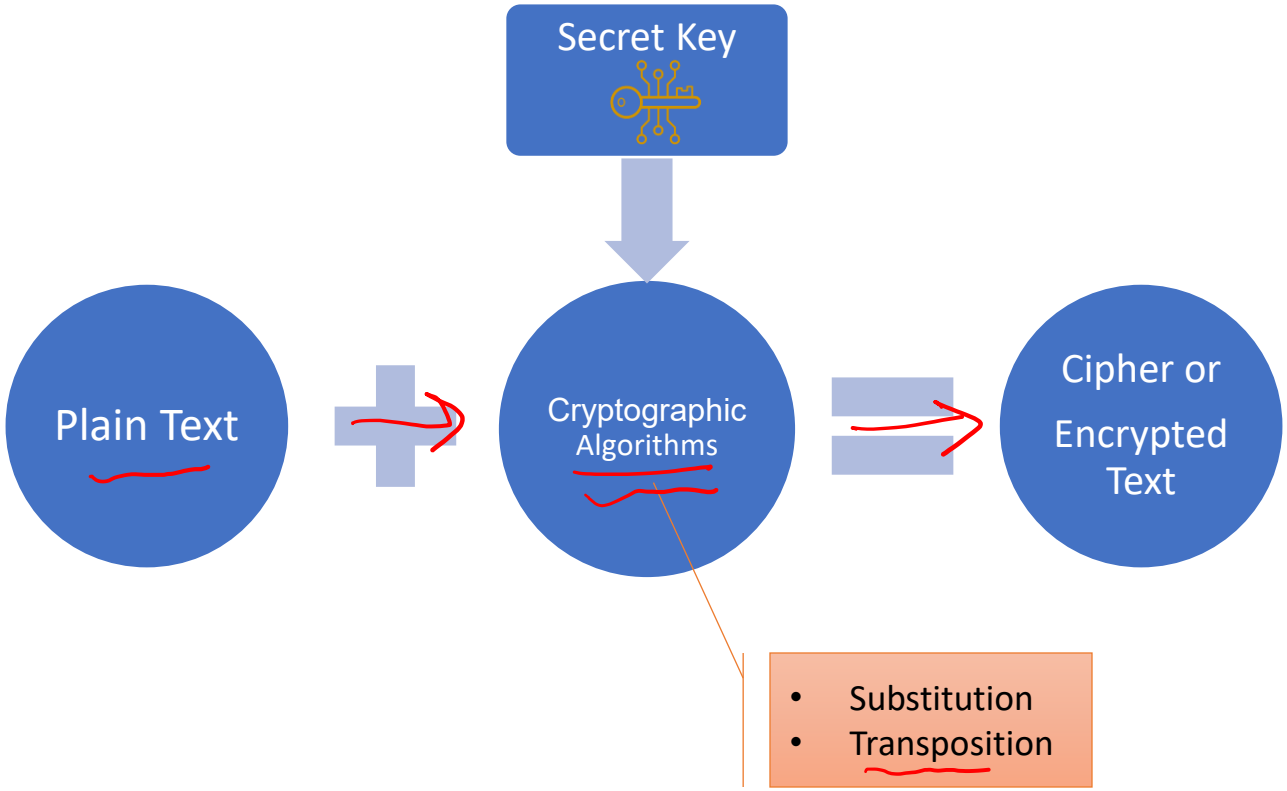
- Windows files security
  - Access rights
  - Encryption



Cryptographic Algorithms and Kerchoff's Principle

Cryptographic Algorithms

also referred as Ciphers or Encryption Algorithms

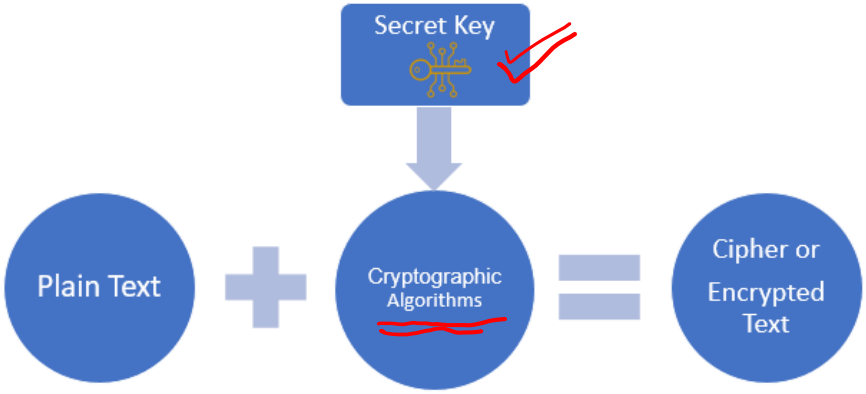


Feistel network consisting multiple rounds of processing of the plaintext, each round consisting of a “substitution” step followed by a permutation step.

Kerchoff's Principle

Kerckhoffs's principle of cryptography was stated by Dutch-born cryptographer Auguste Kerckhoffs in the 19th century.

- Kerckhoff's principle is **the concept that a Cryptographic system should be designed to be secure, even if all its details, except for the key, are publicly known**.



- In other words,
  - Secrecy of the cryptographic system should rely on the secret keys
  - No need to hide the procedure or algorithm for encryption
  - Rather, its better if procedure or algorithm for encryption are made public as this will help in identification and removing the flaws/loopholes

Classical Ciphers

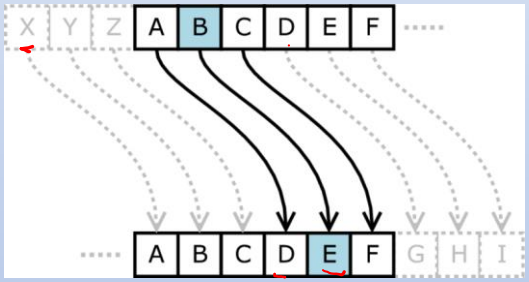
The Caesar Cipher

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Classical Ciphers

The Caesar Cipher

The Caesar cipher is one of the earliest and simplest methods of encryption technique and is based on substitution and involves shifting each letter of the plaintext message by a certain number of letters,



- **Caesars cipher**
  - Replace every 'A' in the message with a 'D'
  - Replace every 'B' in the message with a 'E'
  - Replace every 'C' in the message with a 'F', etc.

- **Considerations**
  - Algorithms are public (Kerchoff's Principle)
  - Encrypt/decrypt depends on a key
  - The only secret is the key
  - For Caesars cipher, key is ***n***, since shift forward ***n*** to encrypt, shift backward n to decrypt
  - Encryption: $C_i = (P_i + n) \bmod 26$
  - Decryption: $P_i = (C_i - n) \bmod 26$

Text : **ATTACKATONCE**
Shift: **4**
Cipher: EXXEGOEXSRGI

Demo https://cryptii.com/

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Caesar Cipher

Cryptanalysis of Caesar Cipher – Brute force

- Ciphertext = "GRR MGAR OY JOBOJKJ OT ZNXKK VGXZY"
- Perform decryption with each possible key:
- Plaintext with n= 1
- FQQ LFZQ NX INANIJI NS YMWJJ UFWYX
- Plaintext with n= 2
- EPP KEYP MW HMZMHIH MR XLVII TEVXW
- Plaintext with n= 3
- DOO JDXO LV GLYLGHG LQ WKUHH SDUWV
- Plaintext with n= 4
- CNN ICWN KU FKXKFGF KP VJTGG RCTVU
- Plaintext with n= 5
- BMM HBVM JT EJWJEFE JO UISFF QBSUT
- Plaintext with n= 6
- ALL GAUL IS DIVIDED IN THREE PARTS

Classical Ciphers

Vigenere Cipher

Classical Ciphers

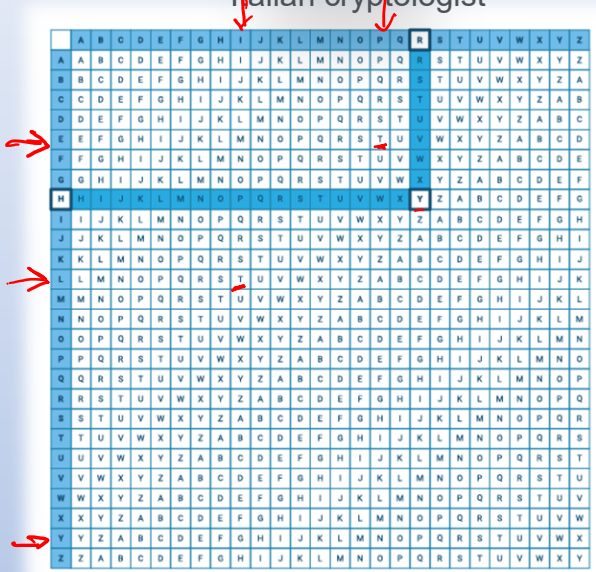
Vigenere Cipher

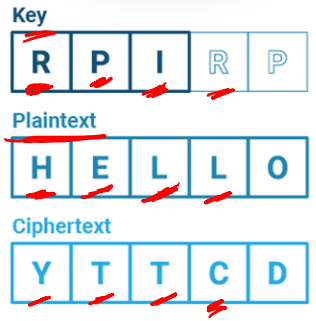


Giovan Battista
Italian cryptologist



Blaise de Vigenère
French cryptographer





- Developed in 1553.
- It is a method of encrypting alphabetic text by using a series of interwoven Caesar ciphers, based on the letters of a keyword.
- Its based on polyalphabetic substitution
- **Key**: A word W of Length M.
- **Plain text** P of length N.
- Repeat the Key until it matches the length of the plain text.
- For each letter P_j of the plain text, apply a Caesar Cipher of length W_j

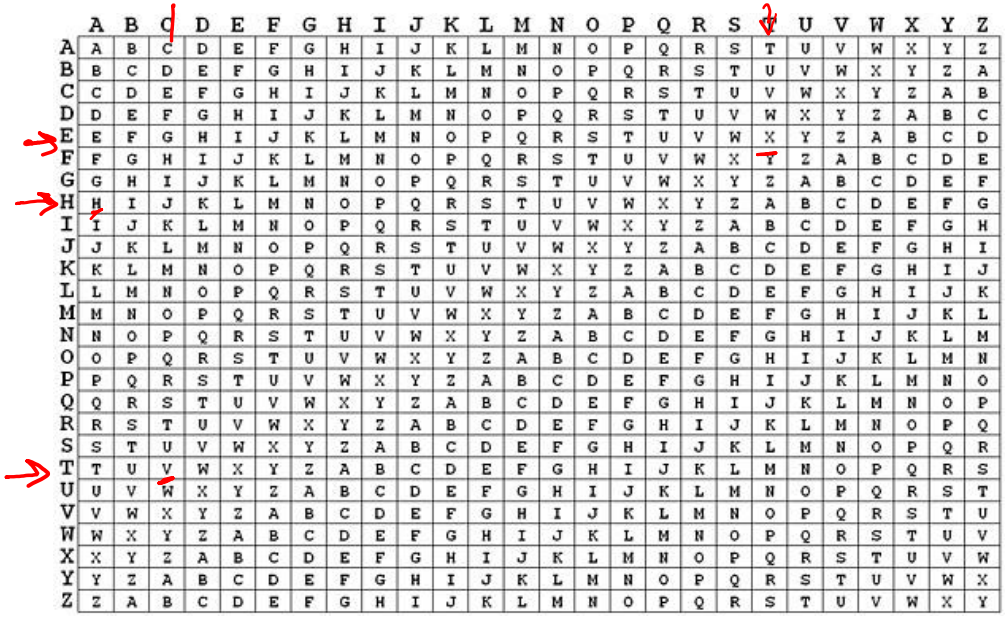
Example

- Key: **RPI**
- Plain Text: HELLO
- Expanded key: RPIRP
- Cipher Text: YTTCD

Demo https://cryptii.com/pipes/vigenere-cipher

Exercise

Vigenere Cipher



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

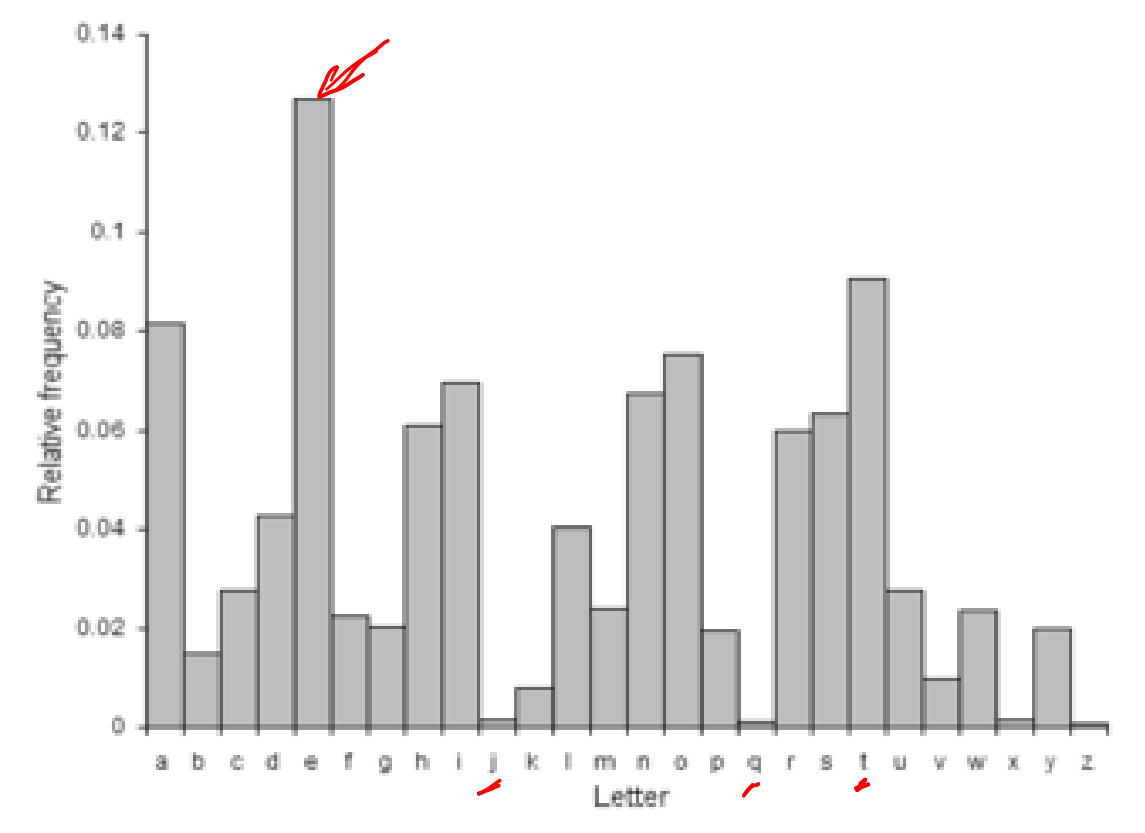
- *The apple is in the corner and the pear is there too (plain)*
- *cat (key)*

- *Find the cipher?*

- *the app lei sin the cor ner and the pea ris the ret oo (plain)*
- *cat cat cat cat cat cat cat cat cat cat cat cat ca (key)*

- *Answer*
- *Vhx cpi neb uig vhx eok pek cnw vhx ret til vhx tem qo (cipher)*

Frequency of the letters of the alphabet in English

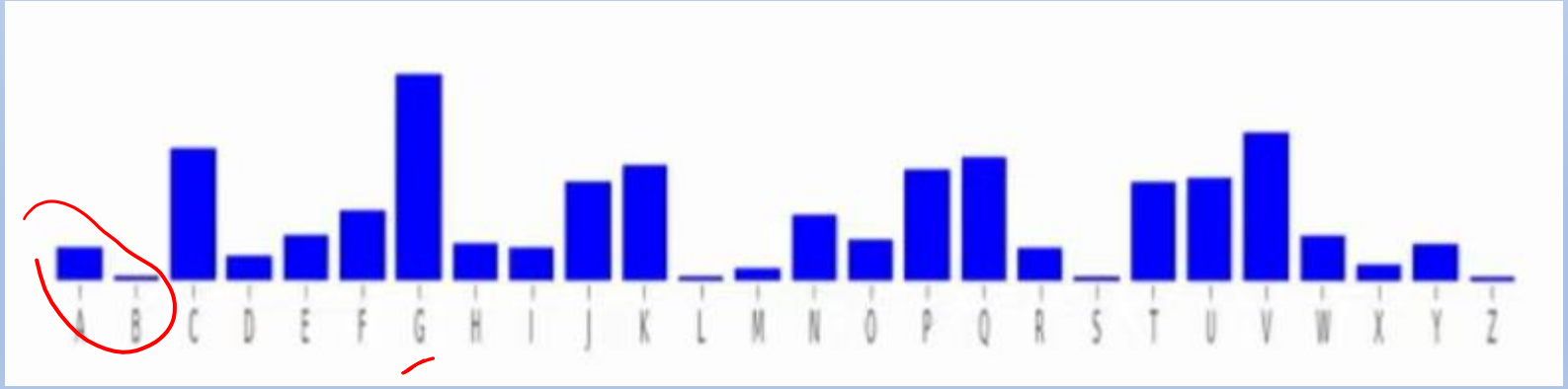


Caesar Cipher

Cryptanalysis of Caesar Cipher



Frequency analysis of Plain Text



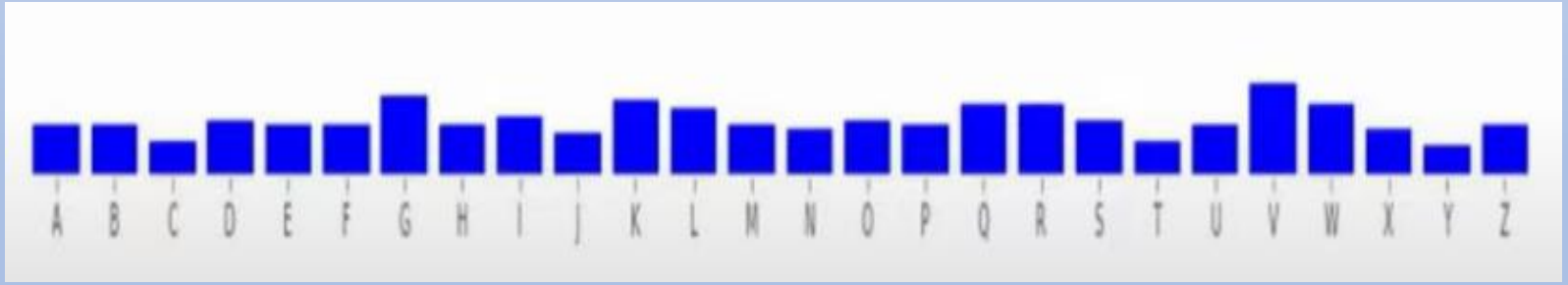
Frequency analysis of Caesar Cipher Text

Vigenere Cipher

Cryptanalysis of Vigenere Cipher



Frequency analysis of Plain Text



Frequency analysis of Vigenere Cipher Text

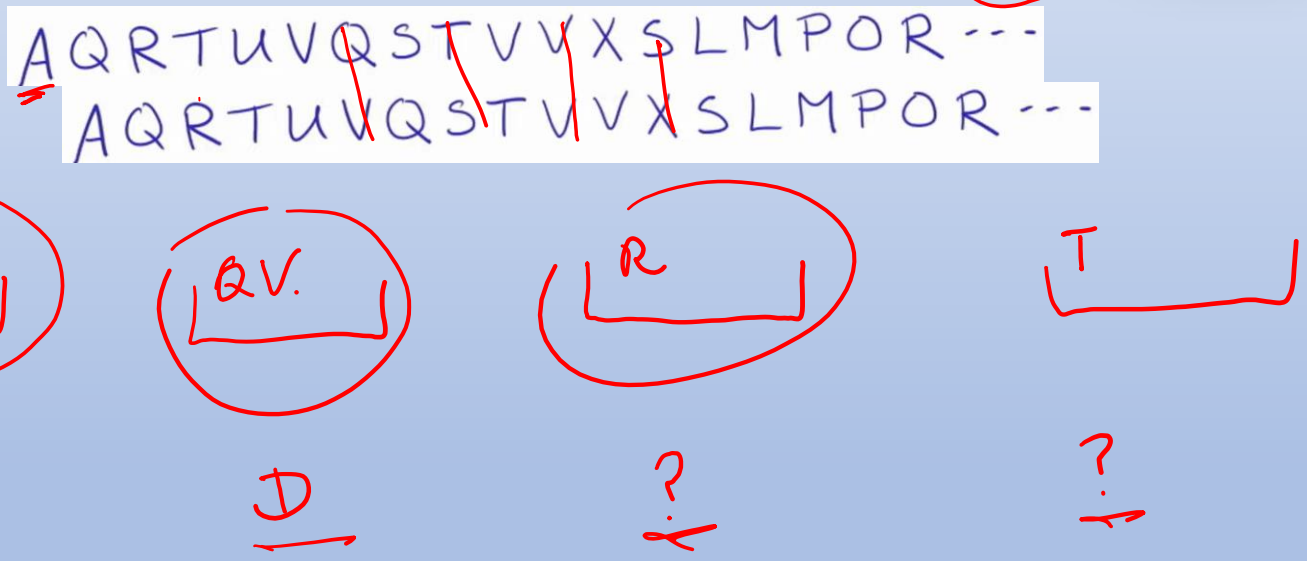
Vigenere Cipher



Cryptanalysis of Vigenere Cipher

- Three steps
  - Find the length of the key (Kasiski test)
  - Divide the message into that many shift cipher encryptions.
  - Use frequency analysis to solve the resulting shift ciphers.

Cipher Text



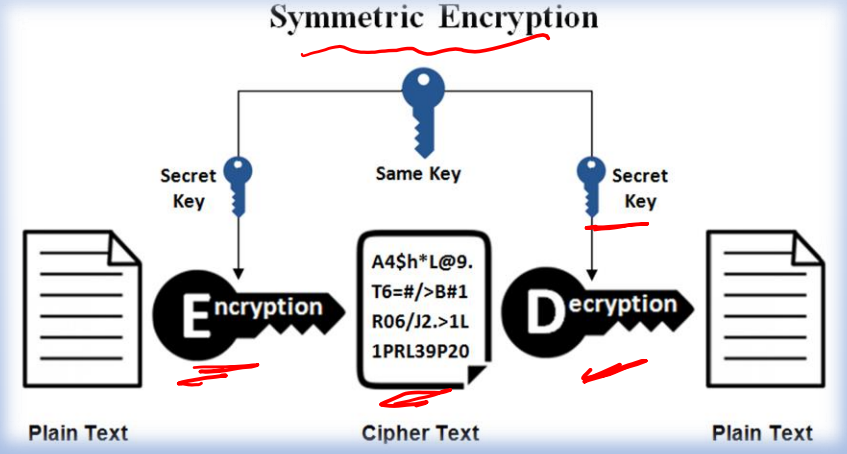
Cryptanalysis of Vigenere cipher: not just how, but why it works
https://www.youtube.com/watch?v=QgHnr8-h0xI

Modern Cryptography Algorithm Types

Symmetric and Asymmetric

Modern Cryptography Algorithm Types

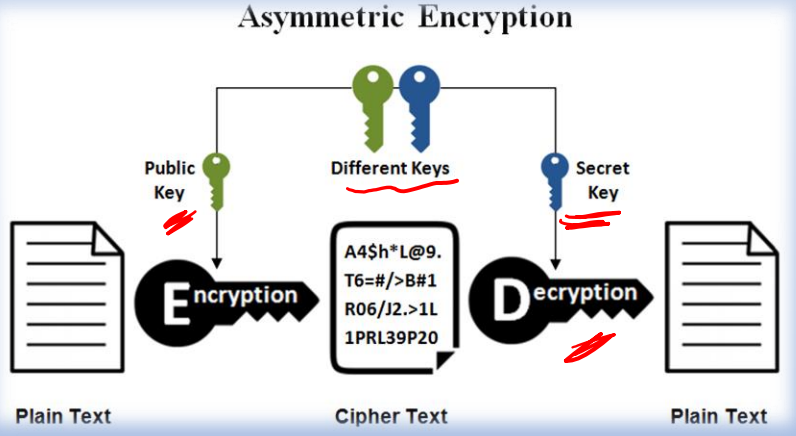
Symmetric Cryptography



- Need a strong encryption algorithm*
- Secure Key Exchange
- Its relatively fast

Asymmetric Cryptography

also knows as Public Key Cryptography



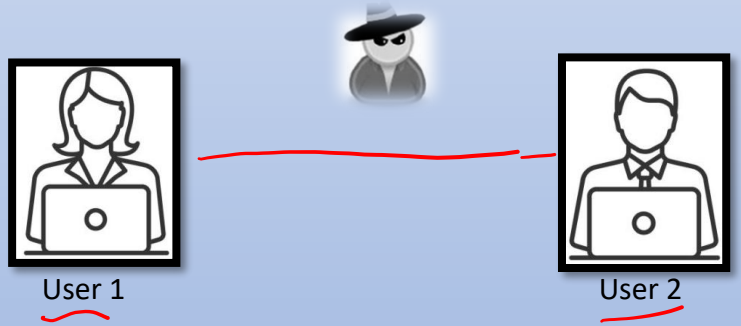
- Public and private keys are mathematically related
- **The private key** is never shared
- Its relatively slow

https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences

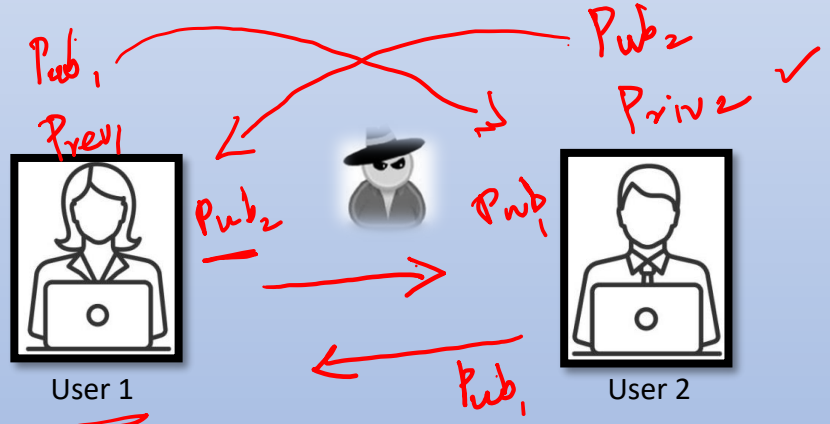
Modern Cryptography Algorithm

Communication Perspective

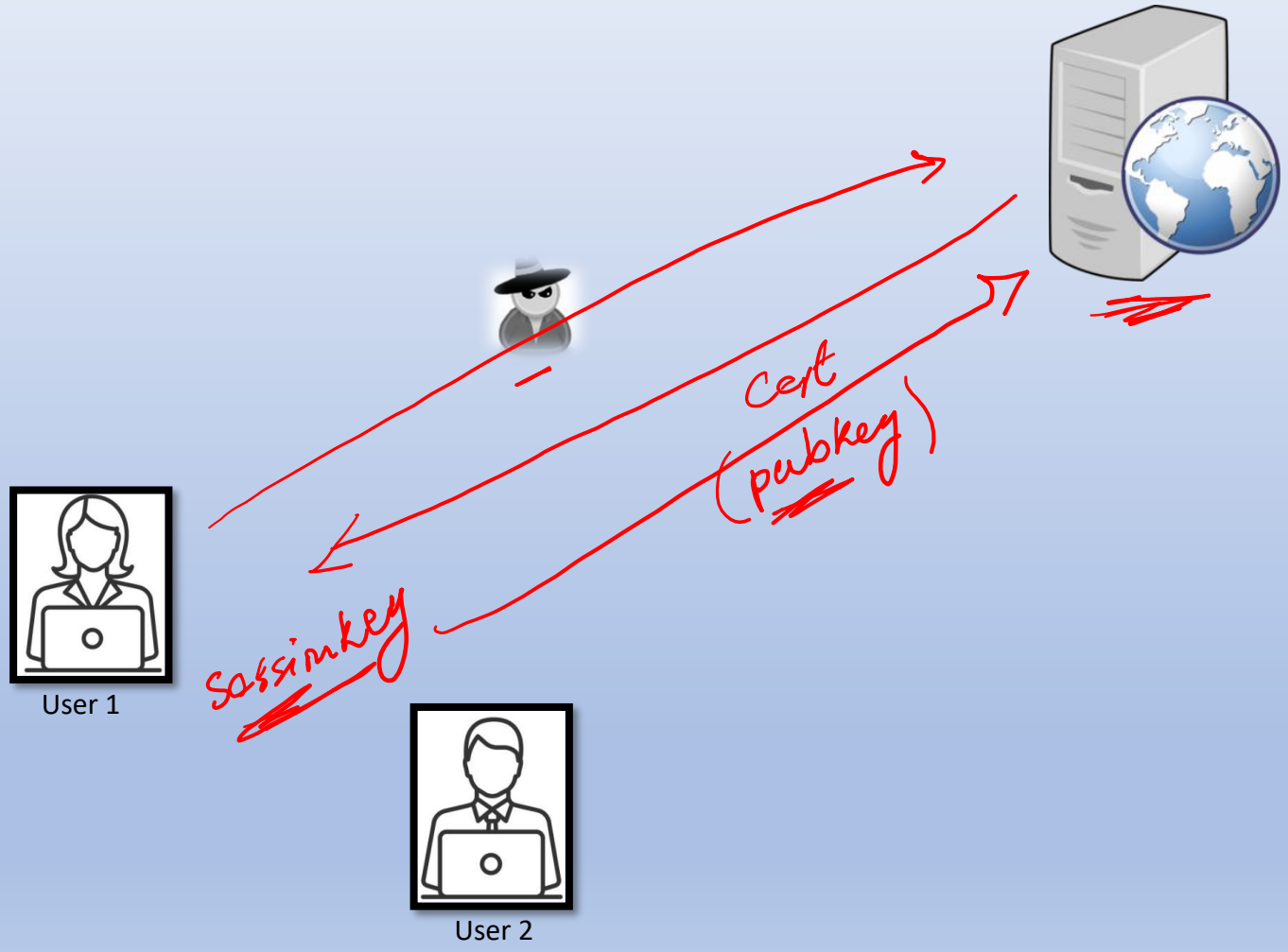
Symmetric Cryptography



Asymmetric Cryptography



How Modern Cryptographic Algorithm Are Used?



Five Aspects of Security

Five Aspects of Security

Confidentiality
- Assurance that information is not disclosed to unauthorized individuals even they get access to it

Encryption

Integrity
- Information is not tampered by any unauthorized entities, if tempered then receiver must be able to detect that

Hashing

Availability
- Authorized users have timely and easy access to information when needed

IDS and IPS

Authenticity
- Prevents impersonation and enables receiver to **verify the sender of the message is who he claimed to be**

Digital signature

Non-Repudiation
- Sender can't deny after sending the message

Digital signature

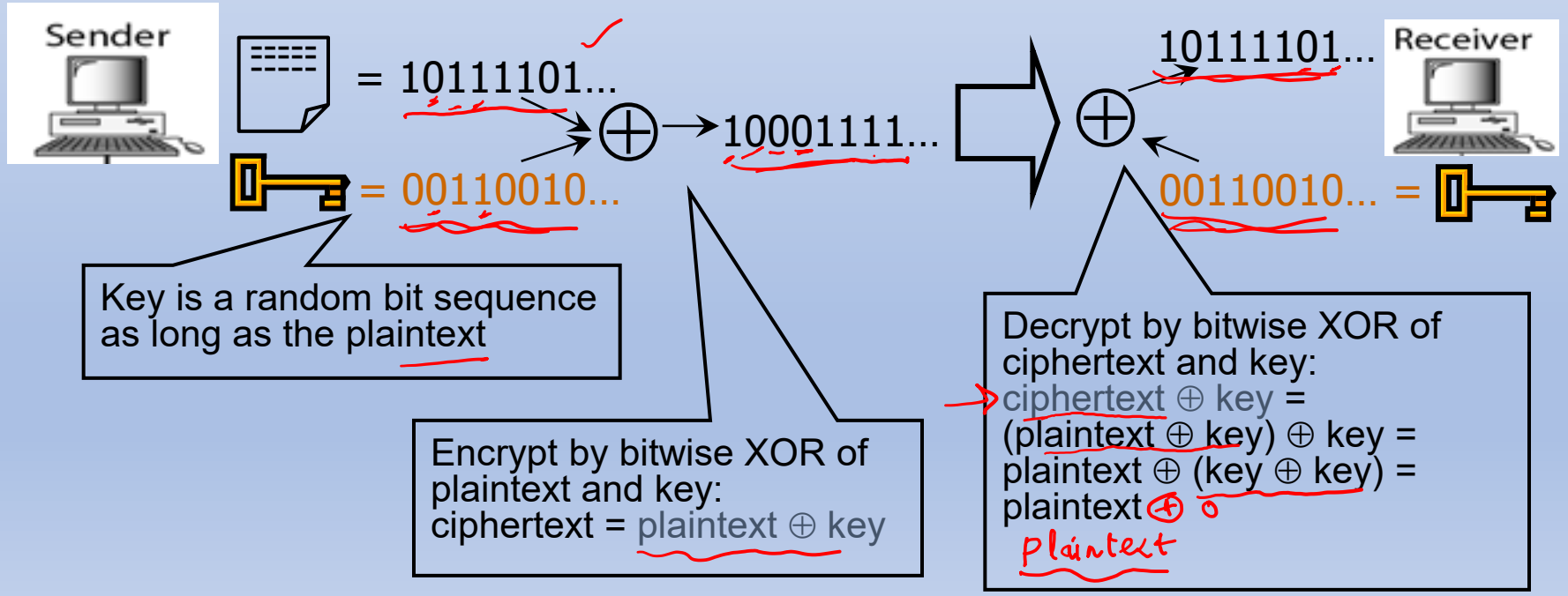
One Time Pad

An Example of Symmetric Encrpytion

One Time Pad

Example of Symmetric Encrpytion

- Invented by Gilbert Vernam in the 1920s
- The message is a bitstring $m \epsilon \{0,1\}^n$
- The key is a bitstring as long as the message, $k \epsilon \{0,1\}^n$
- The ciphertext is obtained by XORing each bit of the plaintext with each bit of the key: c = m ⊕ k.



One Time Pad

Advantages

- **Easy to compute**
  - Encryption and decryption are the same operation
  - Bitwise XOR is very cheap to compute
- **As secure as theoretically possible**
  - Given a ciphertext, all plaintexts are equally likely, regardless of attacker's computational resources
  - if and only if the key sequence is truly random
    - —True randomness is expensive to obtain in large quantities

One Time Pad

Disadvantages

- **Key must be as long as the plaintext**
  - Impractical in most realistic scenarios
  - Still used for diplomatic and intelligence traffic
- **Does not guarantee integrity**
  - One-time pad only guarantees confidentiality
  - Attacker cannot recover plaintext, but can easily change it to something else
- **Insecure if keys are reused**
  - Attacker can obtain XOR of plaintexts

ROT13

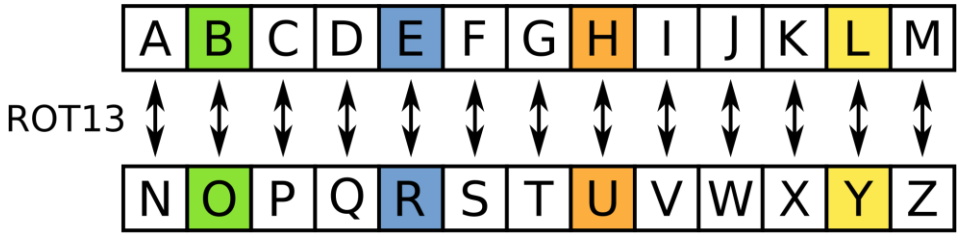
(Rotate by 13 places)

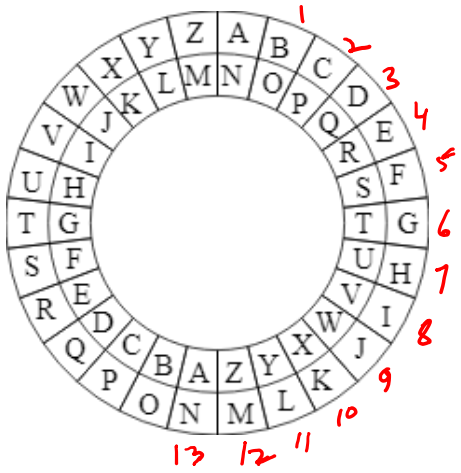
An Example of Symmetric Encrpytion

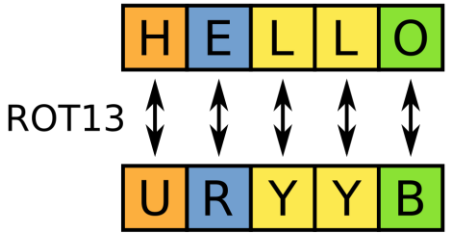
Symmetric Encryption

ROT13

- ROT13 cipher(read as – “rotate by 13 places”) is a special case of the Ceaser cipher in which the shift is always 13.
- This is an example of substitution **cipher**







Poor Encryption: ROT13

- No “key”
- Susceptible to frequency analysis
- Susceptible to brute forcing

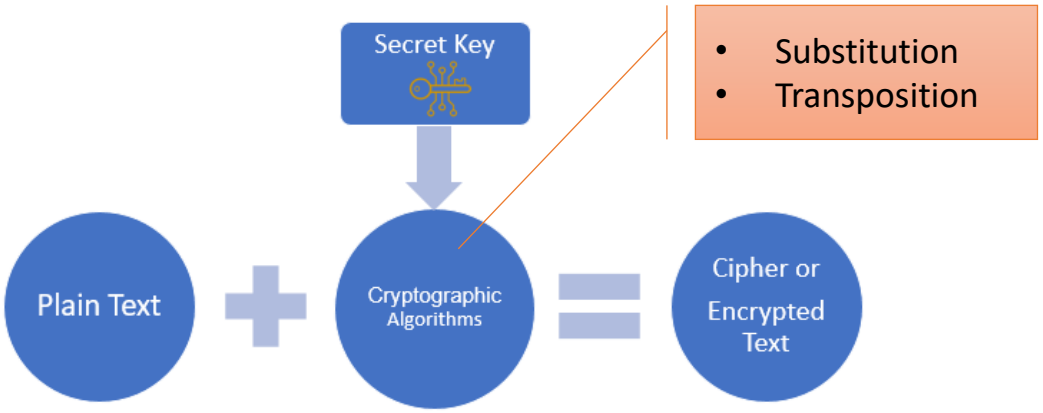
Confusion and Diffusion

Properties of the operation of a secure cipher

Confusion and Diffusion

Properties of the operation of a secure cipher

- Concept was originally presented by Claude Shannon in 1945



- Confusion refers to making the relationship between the Ciphertext and the Key as complex and involved as possible;
  - Make use of Substitution

- Diffusion refers to dissipating the statistical structure of Plaintext over the bulk of Ciphertext
  - Make use of Transposition

Feistel Cipher/Network consisting multiple rounds of processing of the plaintext, each round consisting of a "substitution" step followed by a permutation step.

Operational Modes of Symmetric Encryption

Stream Cipher and Block Cipher

Operational Modes of Symmetric Encryption

Symmetric encryption schemes follows two distinct modes of operation:

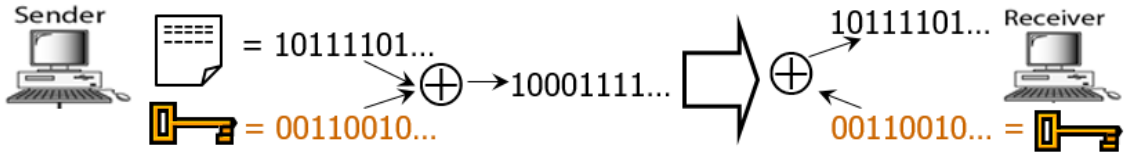
- **Stream Cipher**
  - Plain text is encrypted bit by bit
  - Plain text and key are XORed

- **Block Cipher**
  - Plain text is encrypted block by block
  - The whole block is encrypted with a key

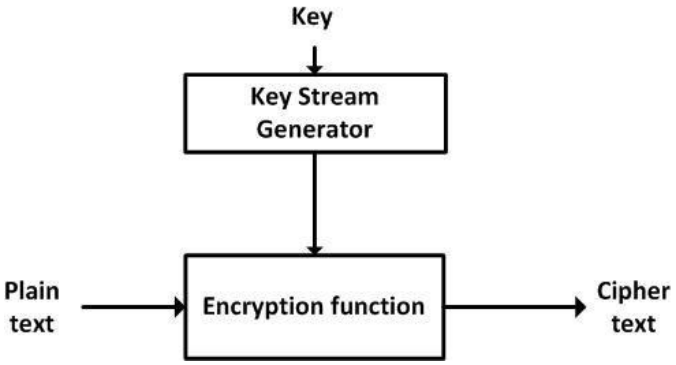
Stream Ciphers

- Each bit of plaintext is encrypted one by one, with the corresponding bit of the keystream, obtaining a bit of ciphertext.

- To describe a stream cipher, it is enough to describe the key stream generator. Once the key stream is obtained, it works like the one- time pad.
- The key stream must be generated from a random seed

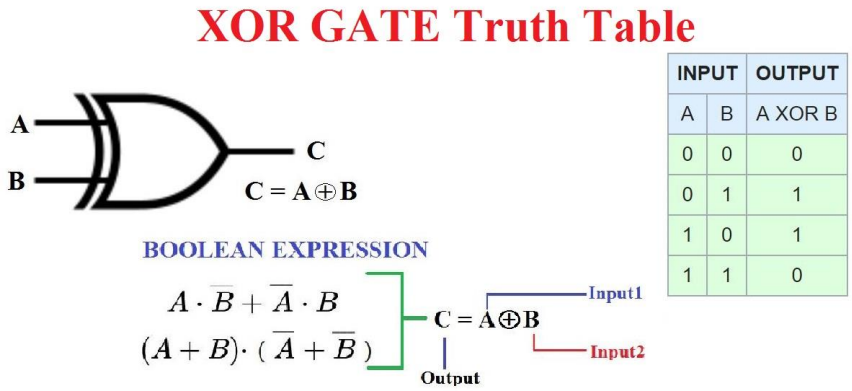


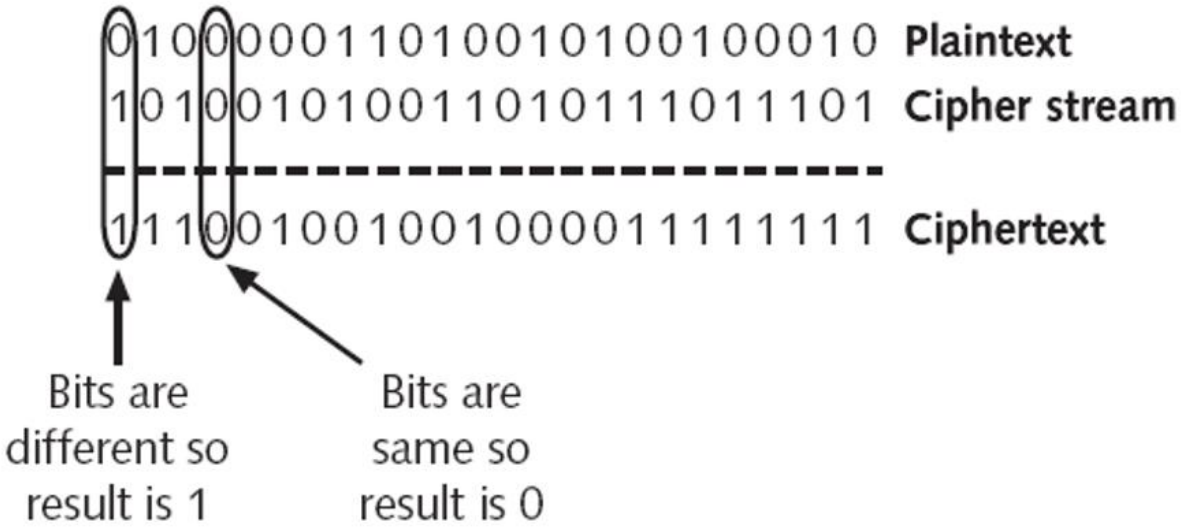
One Time Pad



Stream Ciphers

Stream Encryption

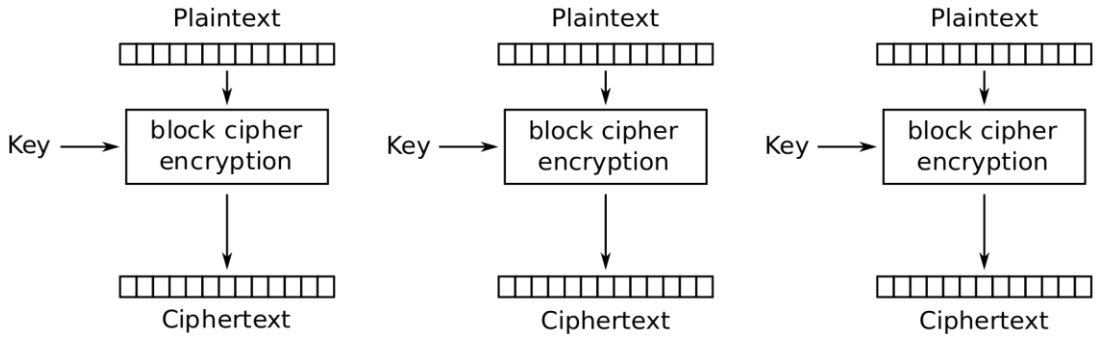




Block Ciphers

- Block ciphers operate on blocks of plaintext one at a time to produce blocks of ciphertext.
- The encryption of a bit in a plaintext will depend on the other bits in the block.
- The block sizes are usually reasonably large e.g. 64 bits, 128 bits, even more.





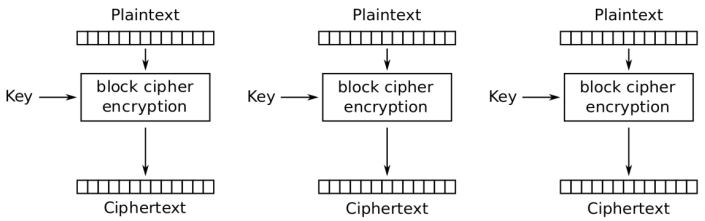
- The most famous block cipher is DES (Data Encryption Standard).
- Since DES is the most studied scheme and the design principles of DES have inspired a lot of ciphers used nowadays, we will have a slight view of DES.

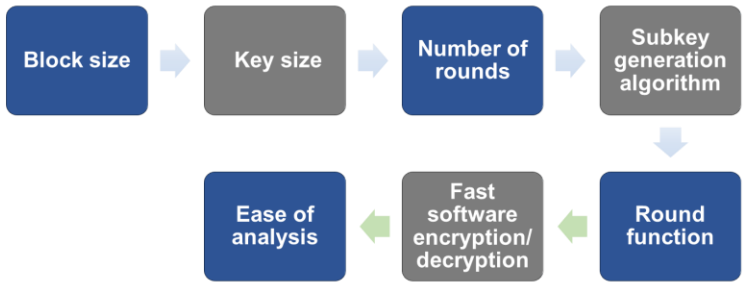
https://sandilands.info/crypto/BlockCipherModesofOperation.html

Block Ciphers Design Considerations

Block Ciphers Design Considerations

- Processes the input one block of elements at a time
- Produces an output block for each input block
- **Block size:** Larger block sizes mean greater security (all other things being equal) but reduced encryption/decryption speed. block size of 128 bits is a reasonable trade-off.
- **Key size**: Larger key size means greater security but may decrease encryption/ decryption speed. The most common key length in modern algorithms is 128 bits.
- **Number of rounds**: The essence of a symmetric block cipher is that a single round offers inadequate security but that multiple rounds offer increasing security. A typical size is 16 rounds.
- **Subkey generation algorithm** : Greater complexity in this algorithm should lead to greater difficulty of cryptanalysis.
- **Round function**: Again, greater complexity generally means greater resistance to cryptanalysis.
- **Fast software encryption/decryption:** In many cases, encryption is embedded in applications or utility functions and the speed of execution of the algorithm becomes a concern.
- **Ease of analysis:** Although we would like to make our algorithm as difficult as possible to cryptanalyze, there is great benefit in making the algorithm easy to analyze vulnerabilities.





	DES	Triple DES	AES
Plaintext block size (bits)	64	64	128
Ciphertext block size (bits)	64	64	128
Key size (bits)	56	112 or 168	128, 192, or 256

DES = Data Encryption Standard
AES = Advanced Encryption Standard

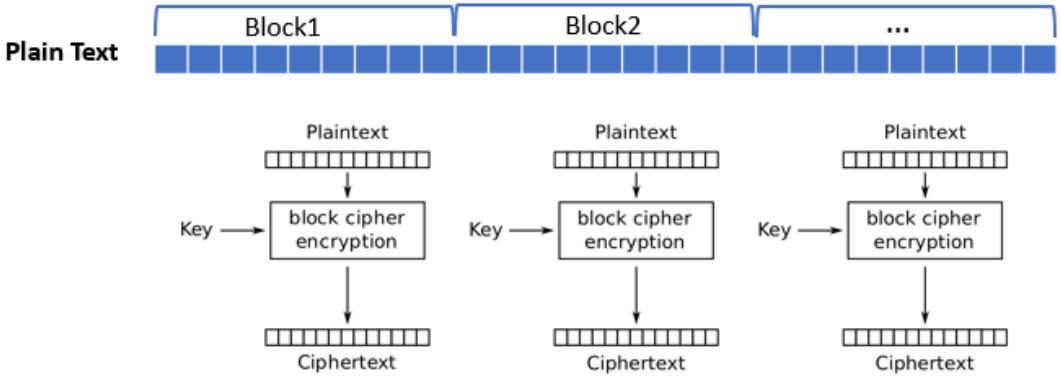
Block Cipher Modes

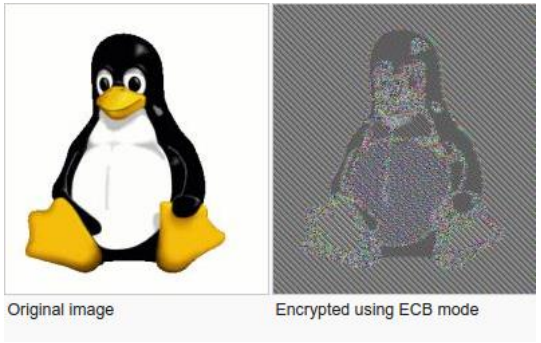
Symmetric Encryption

Block Cipher Modes - Symmetric Encryption

Practical Security Issues

- Typically, symmetric encryption is applied to a unit of data larger than a single 64-bit or 128-bit block.
- The simplest approach to multiple-block encryption:
  - Each block of plaintext is encrypted using the same key
  - Cryptanalysts may be able to exploit regularities in the plaintext
  - This is commonly known as **Electronic Code Book (ECB) mode**



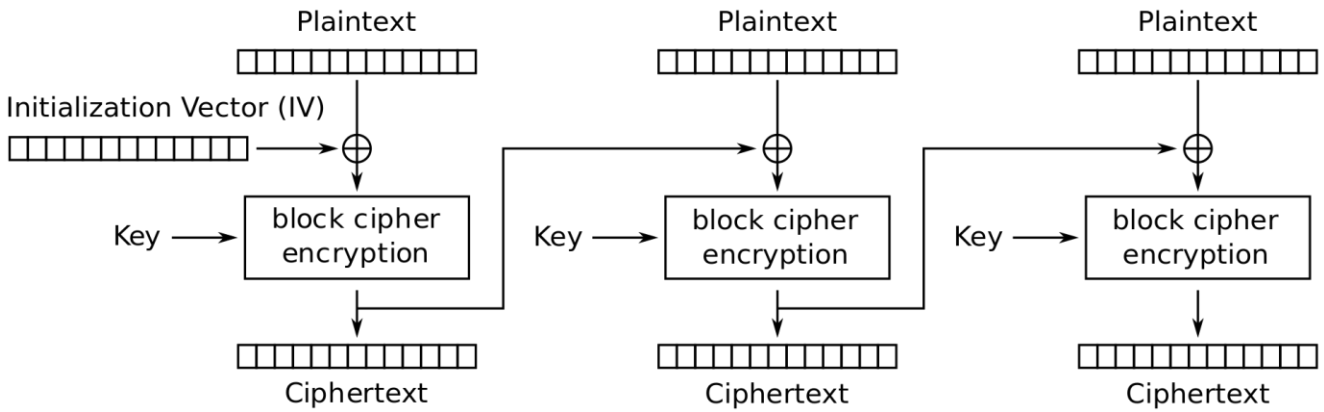


- Alternative techniques developed to increase the security of symmetric block encryption for large sequences
- Overcomes the weaknesses of ECB
- Consequently…different Block cipher modes were designed

- **Electronic Code Book (ECB) Mode**
- Cipher Block Chaining (CBC) Mode
- Cipher Feedback Mode (CFB)
- Output Feedback Mode (OFM)
- Counter mode (CTR)

Cipher Block Chaining Mode

- Input to encryption algorithm is XOR of next 64-bits plaintext and preceding 64-bits ciphertext
- Typical applications: General-purpose block-oriented transmission; authentication
- Initialization Vector (IV) must be known by sender/receiver, but secret from attacker

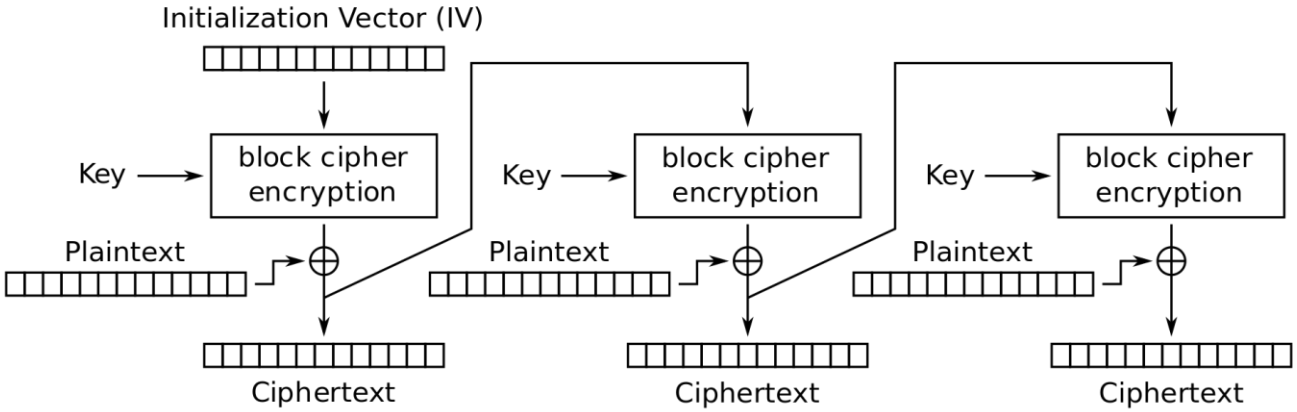


https://sandilands.info/crypto/BlockCipherModesofOperation.html

- Electronic Code Book (ECB) Mode
- Cipher Block Chaining (CBC) Mode
- **Cipher Feedback Mode (CFB)**
- Output Feedback Mode (OFM)
- Counter mode (CTR)

Cipher Feedback Mode

- Converts block cipher into stream cipher
- No need to pad message to integral number of blocks
- Operate in real-time: each character encrypted and transmitted immediately
- Input processed *s* bits at a time
- Preceding ciphertext used as input to cipher to produce pseudo-random output
- XOR output with plaintext to produce ciphertext
- Typical applications: General-purpose stream-oriented transmission; authentication



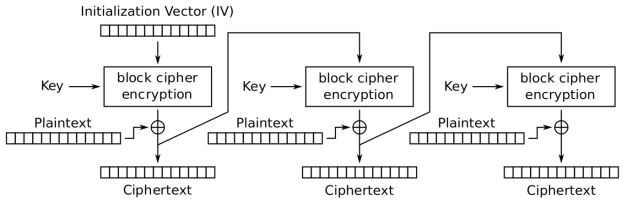
Cipher Feedback (CFB) mode encryption

https://sandilands.info/crypto/BlockCipherModesofOperation.html

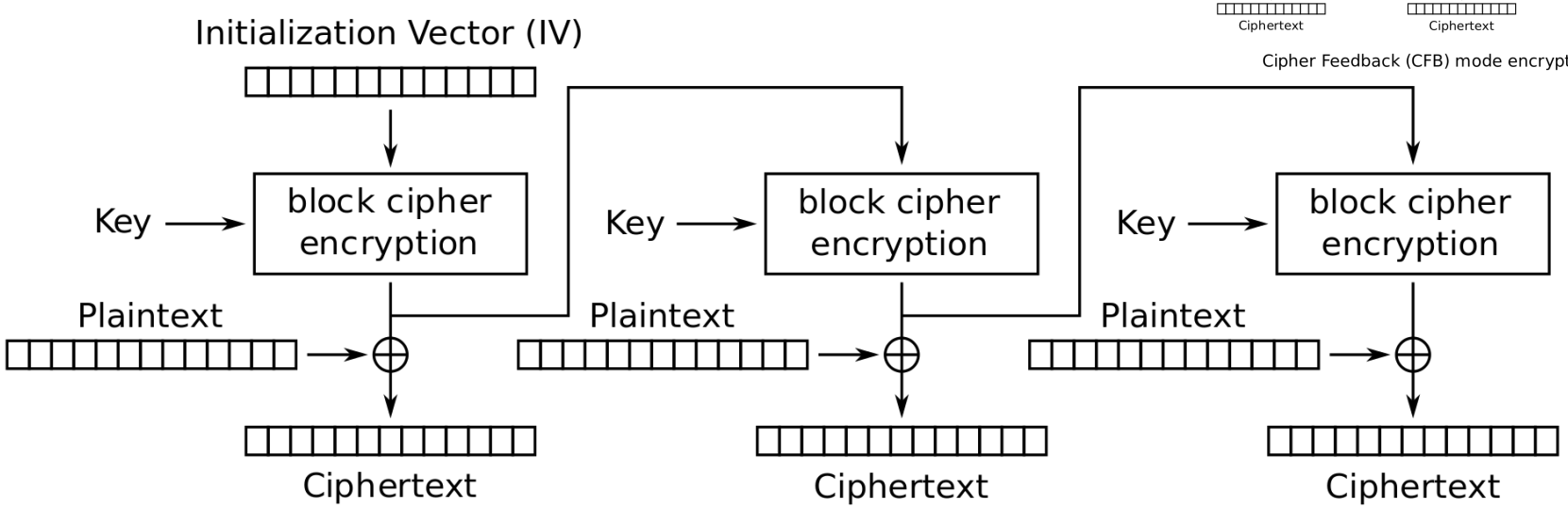
- Electronic Code Book (ECB) Mode
- Cipher Block Chaining (CBC) Mode
- Cipher Feedback Mode (CFB)
- **Output Feedback Mode (OFM)**
- Counter mode (CTR)

Output Feedback Mode

- Converts block cipher into stream cipher
- Similar to CFB, except input to encryption algorithm is preceding encryption output
- Typical applications: stream-oriented transmission over noisy channels (e.g. satellite communications)
- Advantage compared to OFB: bit errors do not propagate
- Disadvantage: more vulnerable to message stream modification attack



Cipher Feedback (CFB) mode encryption

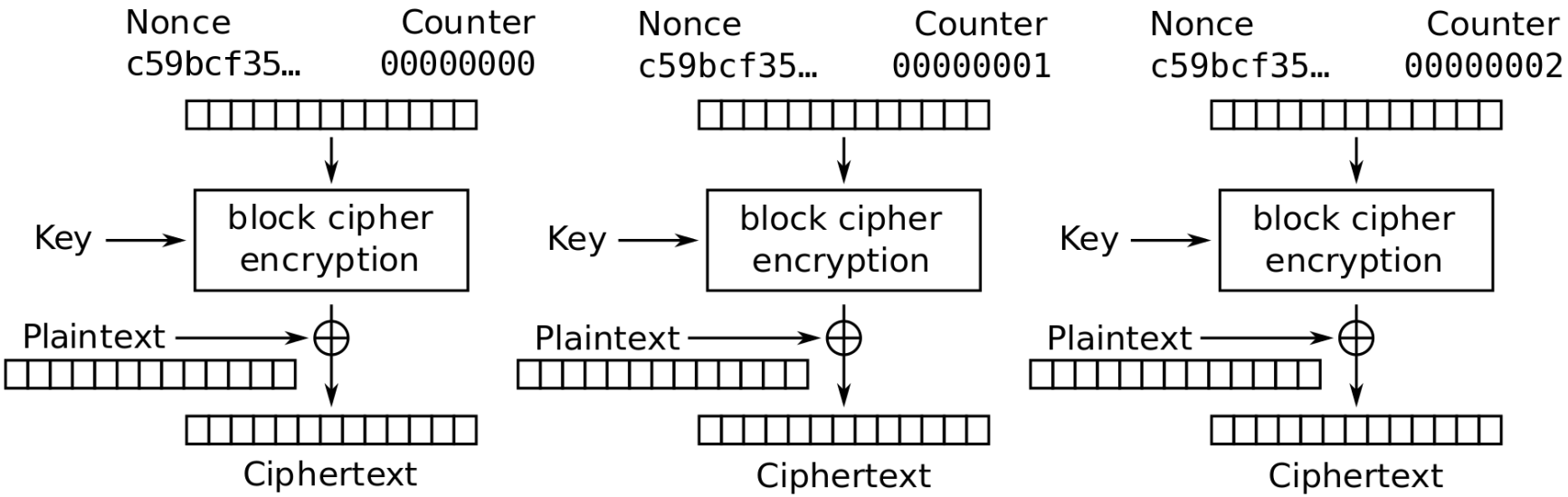


https://sandilands.info/crypto/BlockCipherModesofOperation.html

- Electronic Code Book (ECB) Mode
- Cipher Block Chaining (CBC) Mode
- Cipher Feedback Mode (CFB)
- Output Feedback Mode (OFM)
- **Counter Mode (CTR)**

Counter Mode

- Converts block cipher into stream cipher
- Each block of plaintext XORed with encrypted counter
- Typical applications: General-purpose block-oriented transmission; useful for high speed requirements
- Efficient hardware and software implementations
- Simple and secure



https://sandilands.info/crypto/BlockCipherModesofOperation.html

Block Cipher Modes - Symmetric Encryption

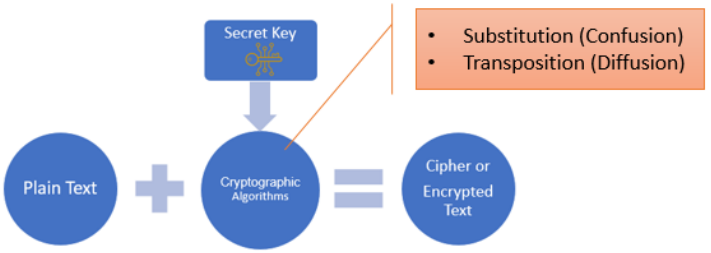
Summary

Mode	Description	Typical Application
Electronic Codebook (ECB)	Each block of 64 plaintext bits is encoded independently using the same key.	•Secure transmission of single values (e.g., an encryption key)
Cipher Block Chaining (CBC)	The input to the encryption algorithm is the XOR of the next 64 bits of plaintext and the preceding 64 bits of ciphertext.	•General-purpose block-oriented transmission •Authentication
Cipher Feedback (CFB)	Input is processed *s* bits at a time. Preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with plaintext to produce next unit of ciphertext.	•General-purpose stream-oriented transmission •Authentication
Output Feedback (OFB)	Similar to CFB, except that the input to the encryption algorithm is the preceding DES output.	•Stream-oriented transmission over noisy channel (e.g., satellite communication)
Counter (CTR)	Each block of plaintext is XORed with an encrypted counter. The counter is incremented for each subsequent block.	•General-purpose block-oriented transmission •Useful for high-speed requirements

Attack Strategies on Symmetric Encryption

Brute-force Attacks

- Try all possible keys on some ciphertext until an intelligible translation into plaintext is obtained
- On average half of all possible keys must be tried to achieve success
- Number of Keys are dictated by the key size.



Cryptanalytic Attacks

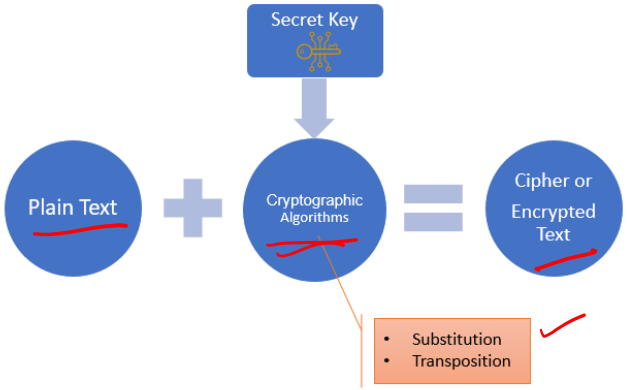
- Rely on:
  - Nature of the algorithm
  - Some knowledge of the general characteristics of the plaintext
  - Some sample plaintext-ciphertext pairs
- Exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or the key being used
  - If successful, all future and past messages encrypted with that key are compromised

Feistel Network

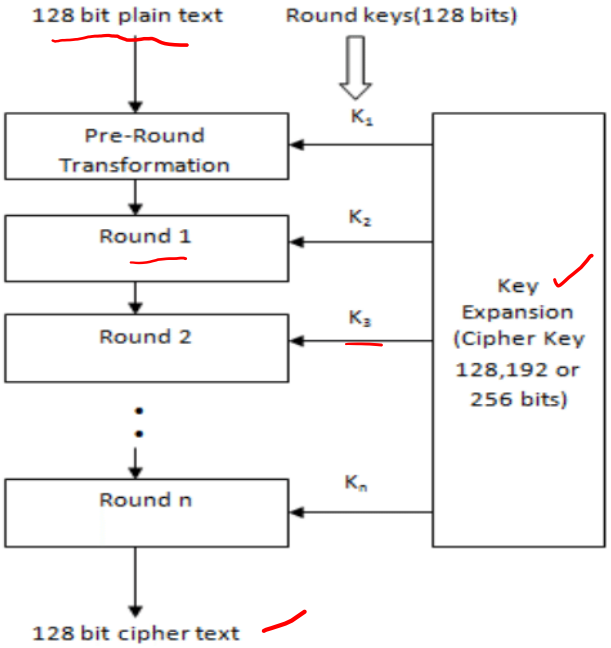
Symmetric Encryption

Encryption/Decryption Process

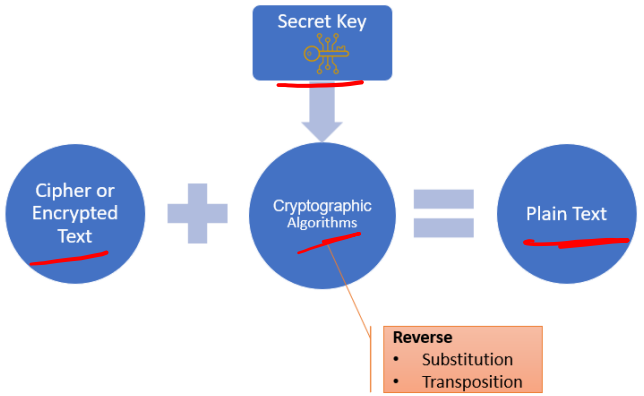
Encryption Process



Feistel network consisting multiple rounds of processing of the plaintext, each round consisting of a "substitution" step followed by a permutation step.



Decryption Process



We want to make encryption process hard for attacker to break our algorithm…How?

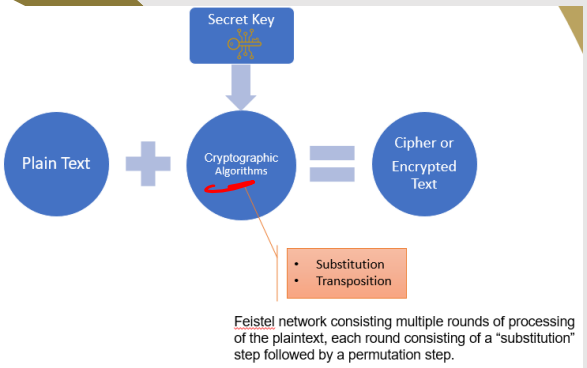
More rounds, complex substitution and transposition…

But, users with the Key should be able decrypt it **easily**…How?

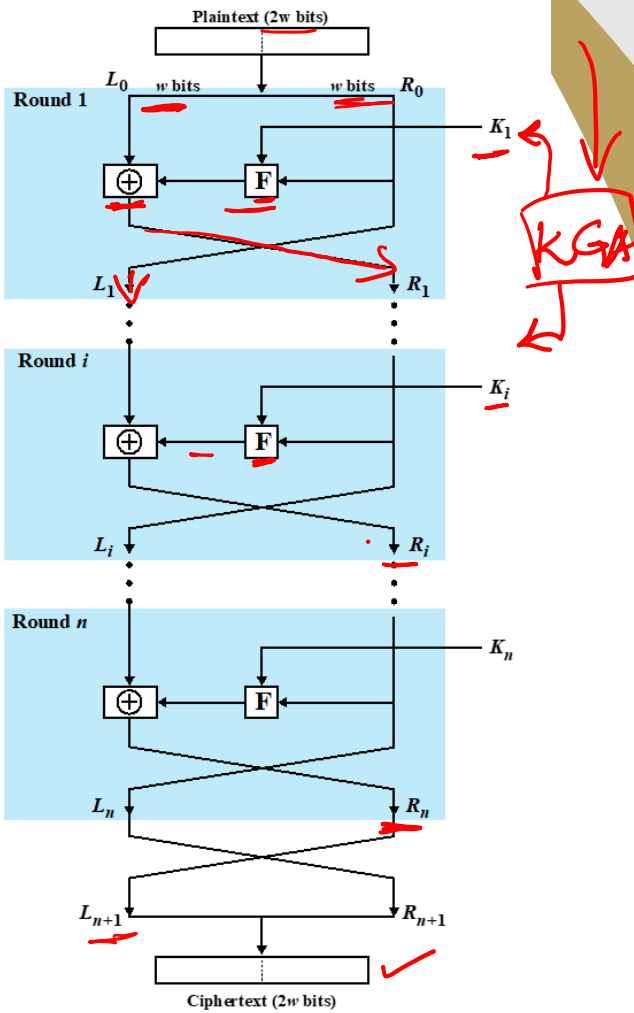
Feistel Network

Feistel Network - Symmetric Encryption

- Many encryption algorithms incorporate a structure first proposed by Horst Feistel of IBM (1973); a **Feistel Network**.
- Feistel structure consisting multiple rounds of processing of the plaintext, each round consisting of a “substitution” step followed by a permutation step.
- Many advance encryption algorithms are designed using this Feistel structure
  - This includes the DES standard.



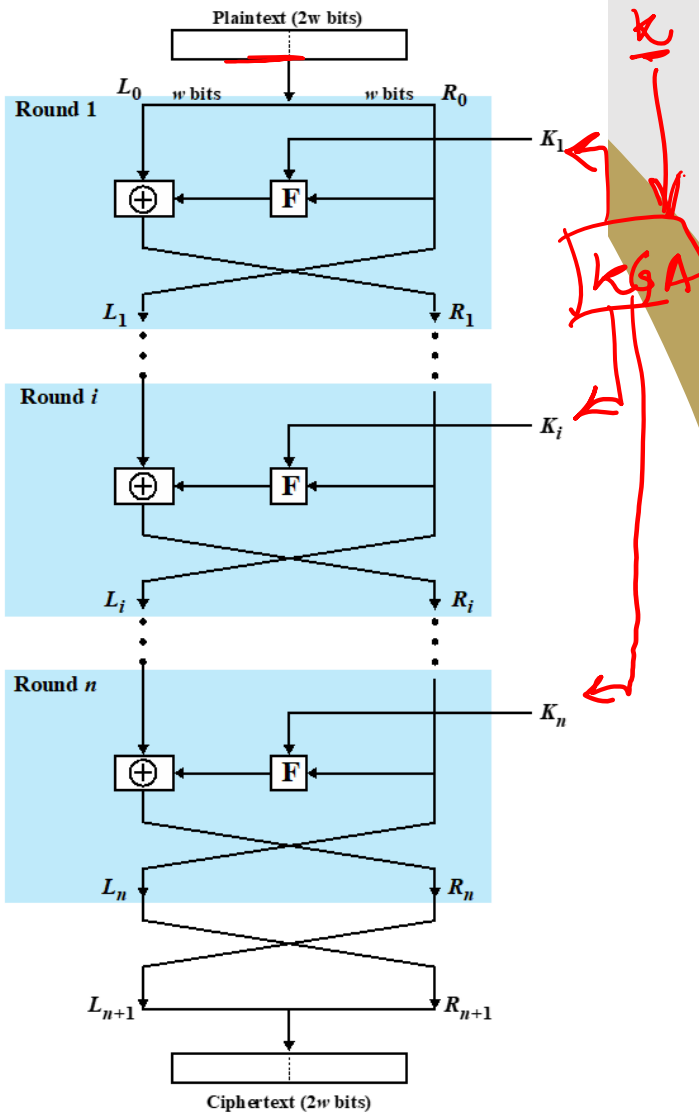
Feistel network consisting multiple rounds of processing of the plaintext, each round consisting of a “substitution” step followed by a permutation step.



Feistel Network –

Brief explanation

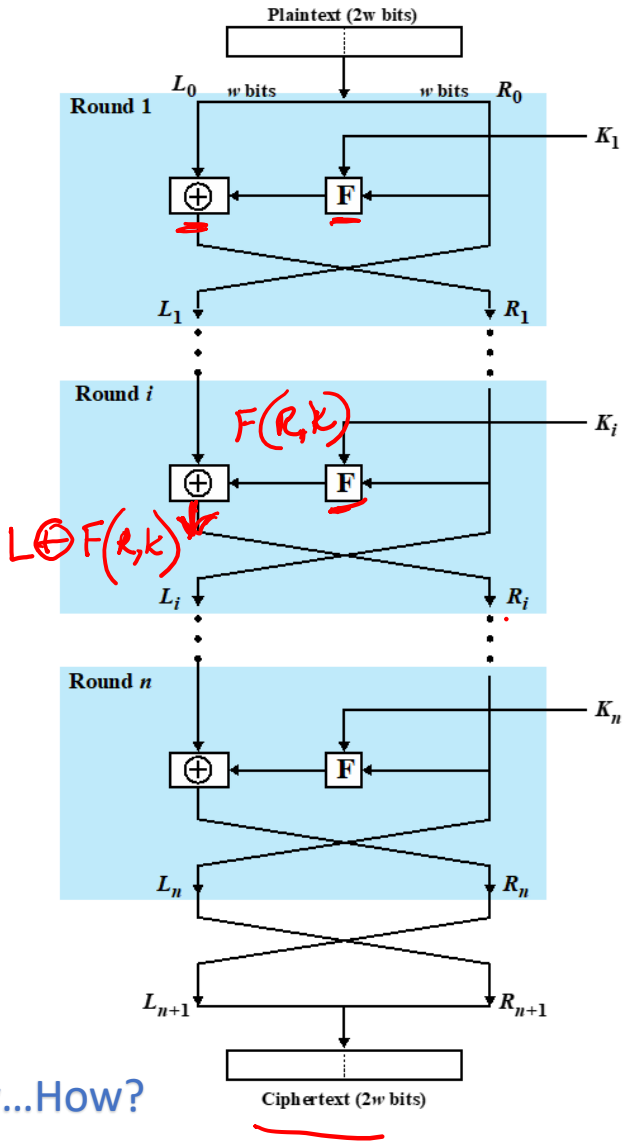
- The inputs to the encryption algorithm are a plaintext block of length 2w bits and a key K .
- The plaintext block is divided into two halves, L^0 and R^0.
- The two halves of the data pass through n rounds of processing and then combine to produce the ciphertext block.
- Each round i has as inputs L^{i-1} and R^{i-1} , derived from the previous round, as well as a subkey K^i, derived from the overall K .
- In general, the subkeys K^i are different from K and from each other and are generated from the key by a subkey generation algorithm.



Feistel Network –

Brief explanation

- All rounds have the same structure. A substitution is performed on the left half of the data.
- This is done by applying a round function F to the right half of the data and then taking the exclusive-OR (XOR) of the output of that function and the left half of the data.
- The round function has the same general structure for each round but is parameterized by the round subkey K^i .
- Following this substitution, a permutation is performed that consists of the interchange of the two halves of the data.



What's happening inside round function "F"?

Users with the Key should be able decrypt it **easily**...How?

Feistel Network

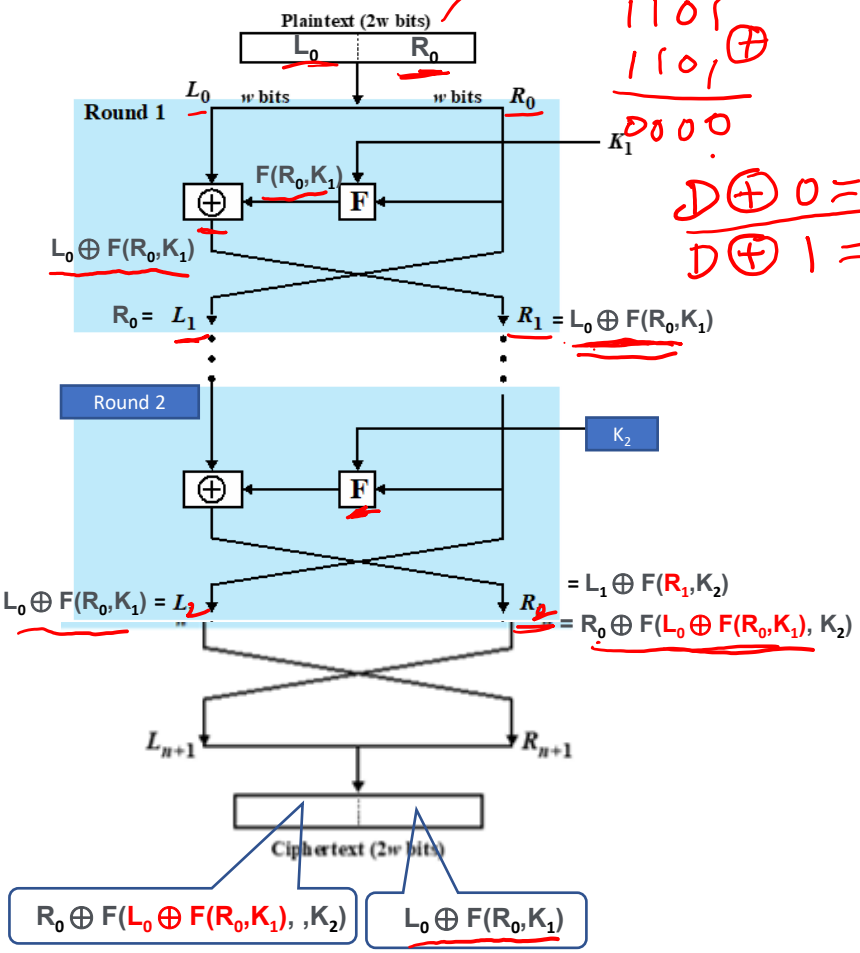
Encryption/Decryption Process

What's happening inside round function "F"?

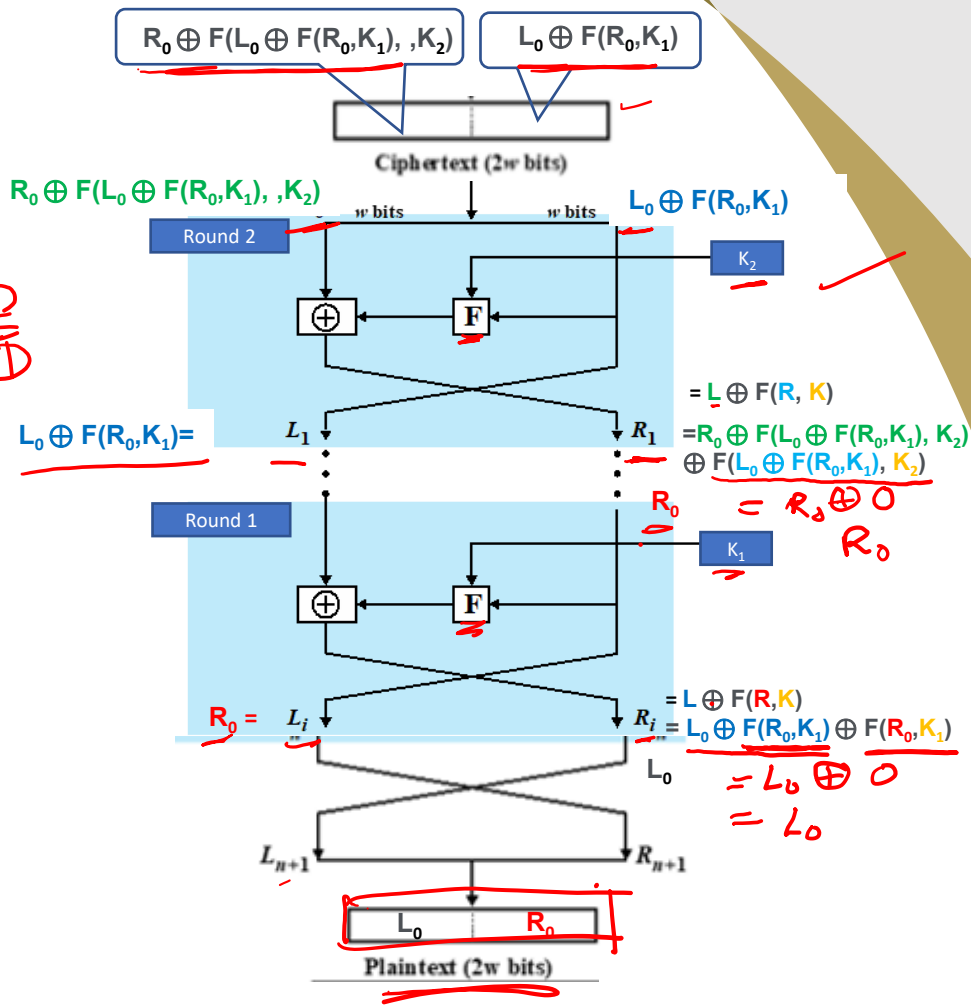
Users with the Key should be able decrypt it **easily**...How?

Feistel Network

Encryption Process



Decryption Process



Data Encryption Standard (DES)

Symmetric Encryption Algorithm

Data Encryption Standard (DES)

Symmetric Encryption Algorithm

Until recently was the most widely used encryption scheme

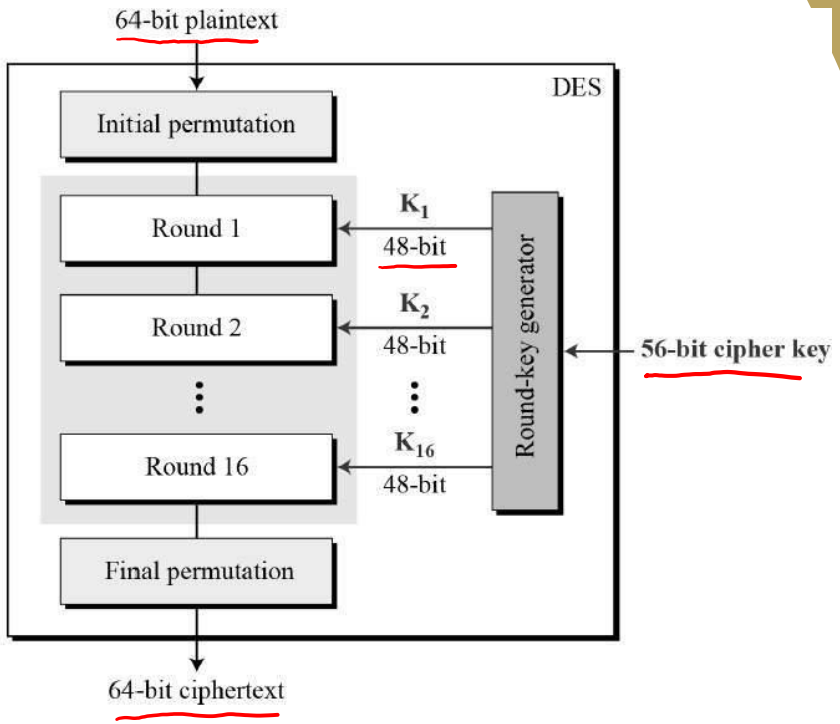
- **Federal Information Processing Standards** FIPS PUB 46
- Referred to as the Data Encryption Algorithm (DEA)

- DES is the most studied encryption algorithm
- DES is a Feistel Cipher.

Working

- **64 bit plaintext block**
- **56 bit key**
- to produce a **64 bit ciphertext block**
- Total**16 rounds**

- Concerns about the use of a 56-bit key
  - Prone to brute-force attack…



https://csrc.nist.gov/csrc/media/publications/fips/46/3/archive/1999-10-25/documents/fips46-3.pdf

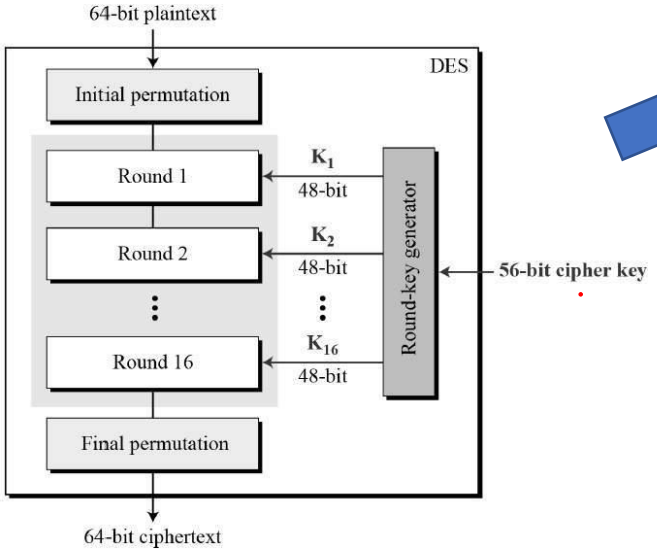
Data Encryption Standard (DES)

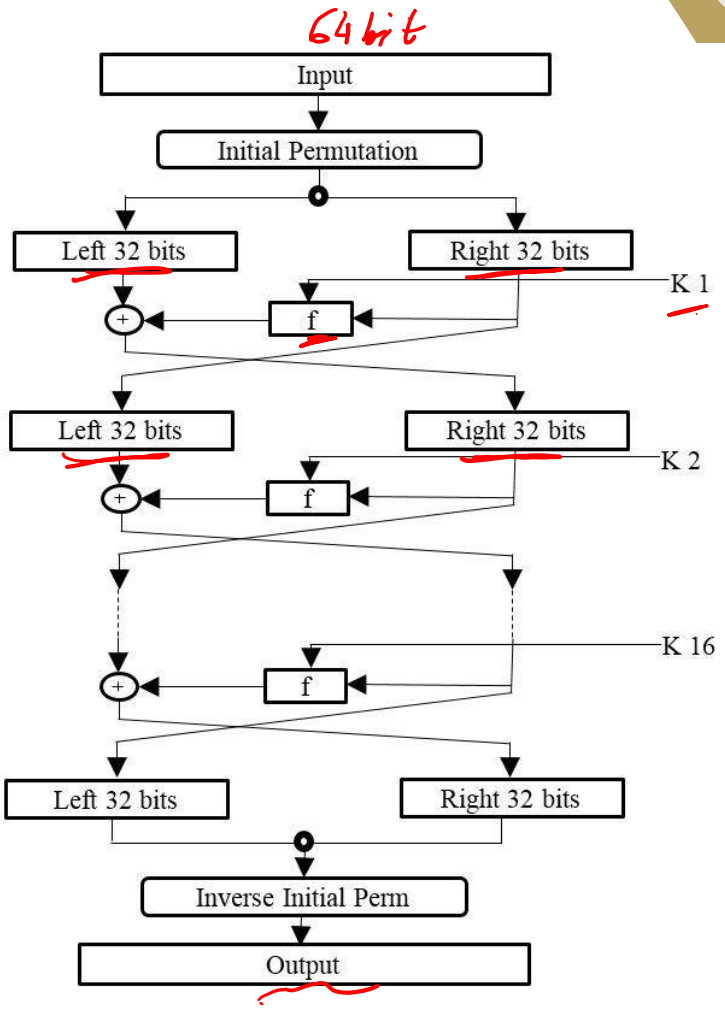
Symmetric Encryption Algorithm

- DES is the most studied encryption algorithm
- DES is a Feistel Cipher.

Working

- **64 bit plaintext block**
- **56 bit key**
- to produce a **64 bit ciphertext block**
- Total**16 rounds**

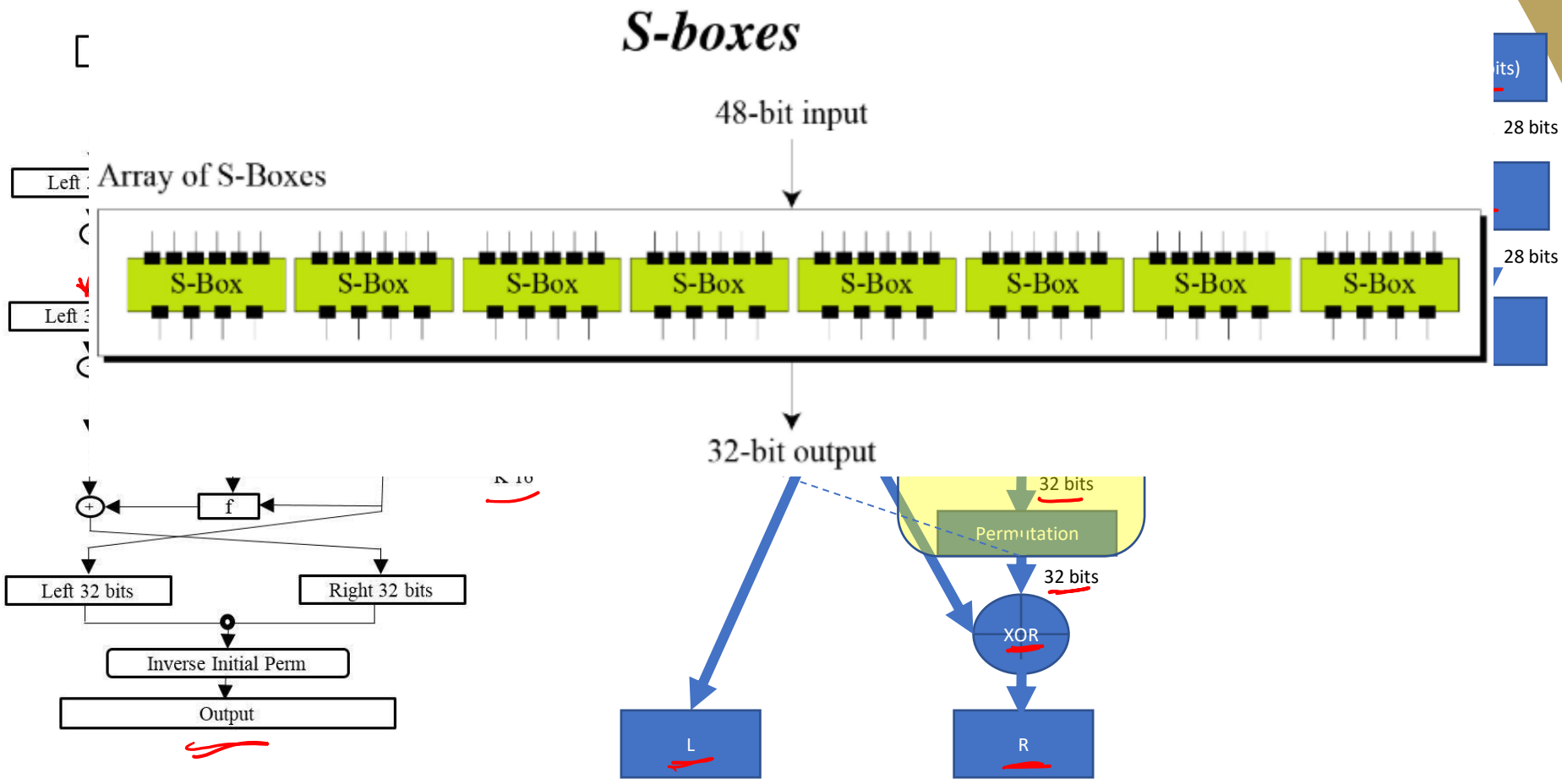




Data Encryption Standard (DES)

What happens in each round?

- 16 Rounds.
- In each round we apply:
  - Expansion Box.
  - Substitution Box.
  - XOR with the round key.



Data Encryption Standard (DES)

How strong?

Concerns about the use of a 56-bit key

Brute-force attacks

- Try all possible keys on some ciphertext until an intelligible translation into plaintext is obtained
- On average ***half of all possible keys must be tried*** to achieve success
- Number of Keys are dictated by the key size.

Key size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 decryptions/s	Time Required at 10^{13} decryptions/s
56	DES	$2^{56} \approx 7.2 \times 10^{16}$	2^{55} ns = 1.125 years	1 hour

$= \frac{3.6 \times 10^{16}}{10^9} = \frac{3.6 \times 10^7 \text{ sec}}{3.2 \times 10^7}$

Think…what can you do to make it strong??

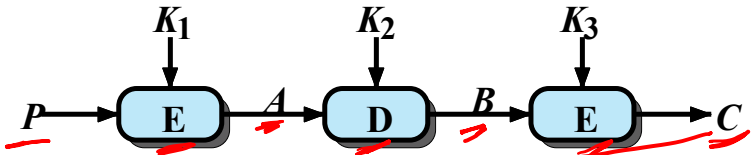
Triple DES (3DES)

Symmetric Encryption Algorithm

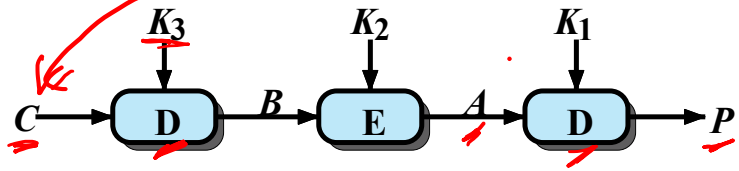
Triple DES (3DES)

Symmetric Encryption Algorithm

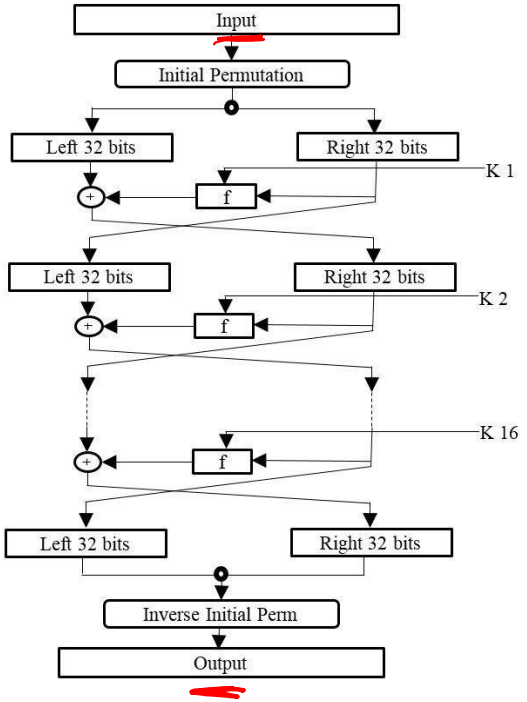
- Designed to address security concerns over DES
  - Original DES soon become prone to brute-force attack
- Need more secure encryption algorithms
- Repeats basic DES algorithm three times using either two or three unique keys
- First standardized for use in financial applications in ANSI standard X9.17 in 1985

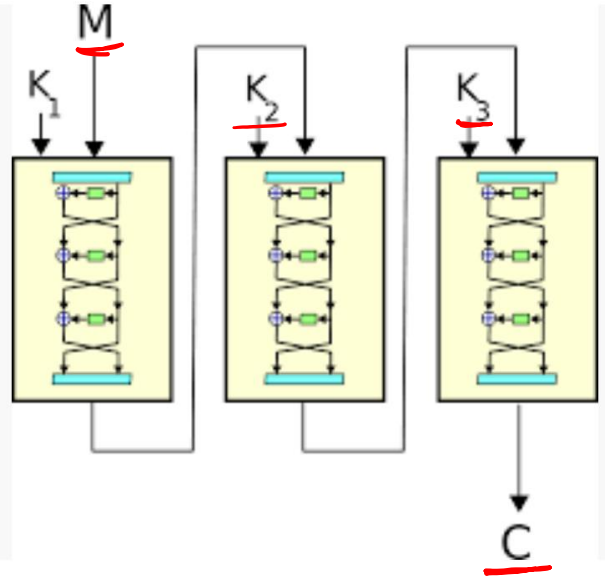


(a) Encryption



(b) Decryption





Triple DES (3DES)

Symmetric Encryption Algorithm

Attractions:

- With three distinct keys, 3DES has an effective key length of 168 bits.
- 168-bit key length overcomes the vulnerability to brute-force attack of DES
- Underlying encryption algorithm is the same as in DES

Key size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 decryptions/s	Time Required at 10^{13} decryptions/s
56	DES	$2^{56} \approx 7.2 \times 10^{16}$	2^{55} ns = 1.125 years	1 hour
168	Triple DES	$2^{168} \approx 3.7 \times 10^{50}$	2^{167} ns = 5.8×10^{33} years	5.8×10^{29} years

Drawbacks:

- Algorithm is sluggish in software
- Uses a 64-bit block size

Advanced Encryption Standard (AES)

Symmetric Encryption Algorithm

Advanced Encryption Standard (AES)

Symmetric Encryption Algorithm

Needed a replacement for 3DES

3DES was not reasonable for long term use

NIST National Institute of Standards and Technology

NIST called for proposals for a new AES in 1997

- **Should have a security strength equal to or better than 3DES**
- Significantly improved efficiency
- Symmetric block cipher
- 128 bit data and 128/192/256 bit keys

Proposal submissions

- In a first round of evaluation, 15 proposed algorithms were accepted.
- Second round narrowed the field to 5 algorithms.

Selected Rijndael in November 2001

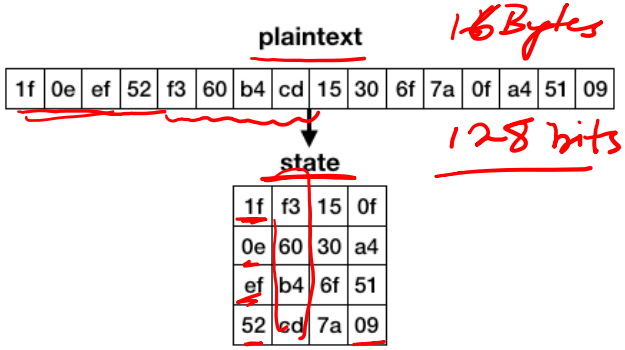
Published as FIPS 197

AES is now widely available in commercial products.

Advanced Encryption Standard (AES)

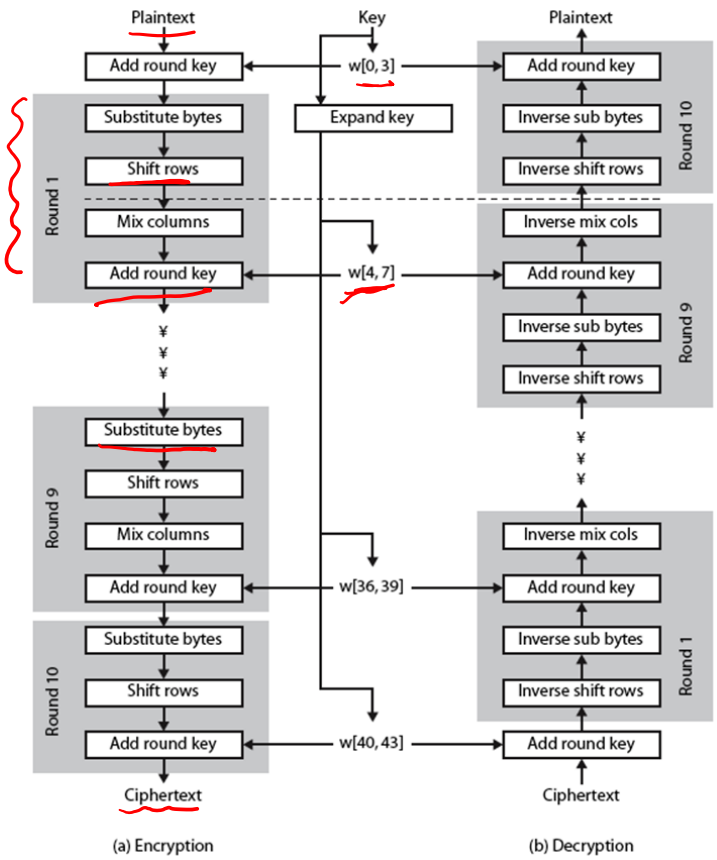
Symmetric Encryption Algorithm

- An **iterative** rather than **Feistel** cipher
  - Processes data as block of 4 columns of 4 bytes
  - Operates on entire data block in every round
- Designed to be:
  - Resistant against known attacks
  - Speed and code compactness on many CPUs
  - Design simplicity
- Data block viewed as 4-by-4 table of bytes
  - Such a table is called the **current state**
- Key is expanded to array of words
- Has 10 rounds in which state the following transformations (called `layers'):
  - BS- byte substitution (1 S-box used on every byte)
  - SR- shift rows (permute bytes between groups/columns)
  - MC- mix columns (uses matrix multiplication in GF(256))
  - ARK- add round key (XOR state with round k
- First and last round are a little different



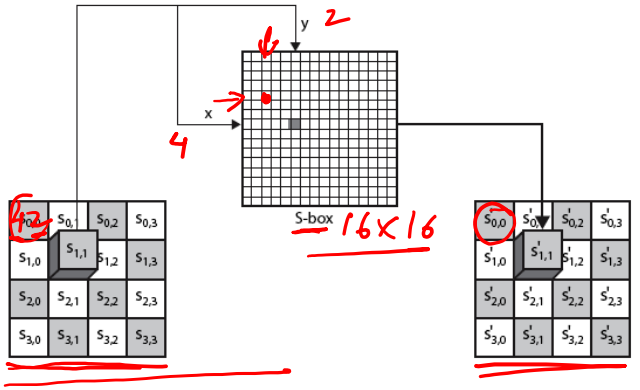
Algorithm	Key length (bits)	Block size (bits)	No of round
AES- 128	128	128	10
AES- 192	192	128	12
AES- 256	256	128	14

AES Working

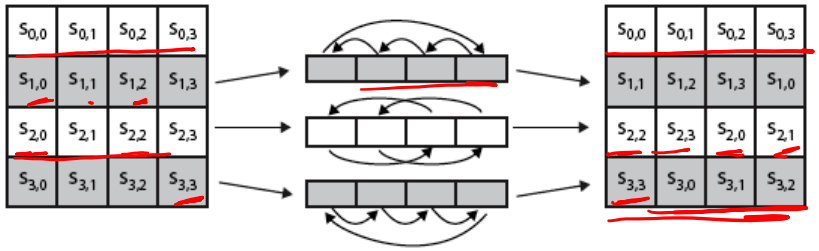


(a) Encryption (b) Decryption

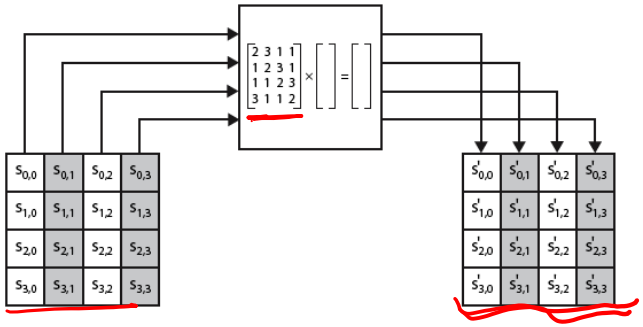
BS



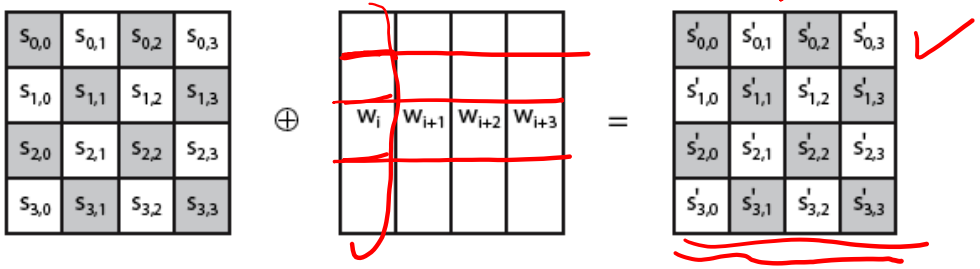
SR



MC

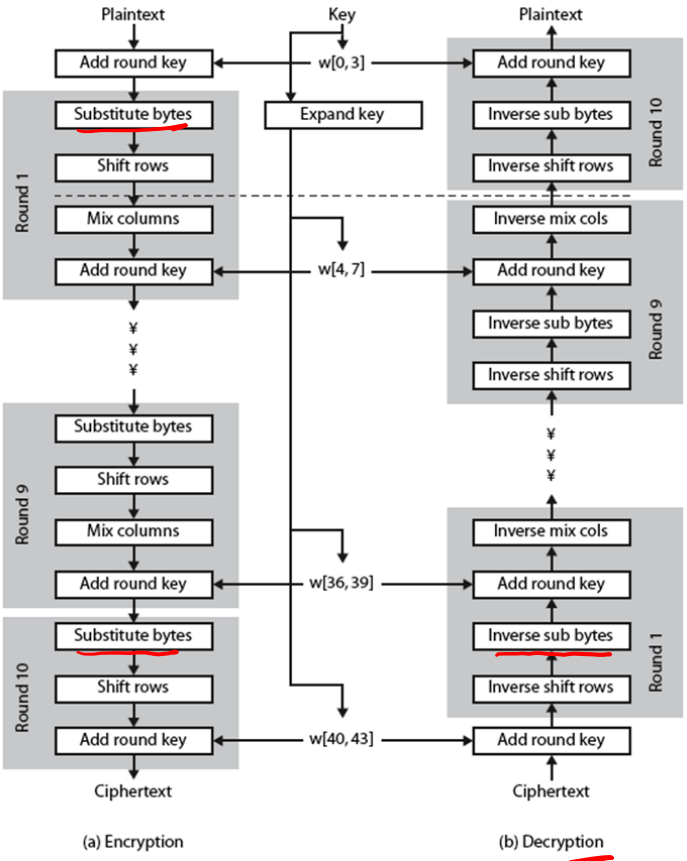


ARK

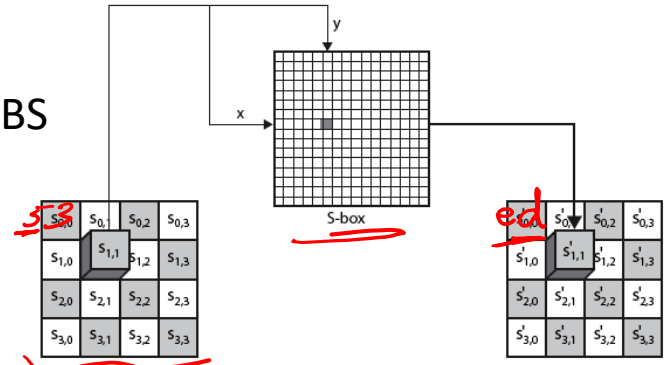


AES Working

Byte Substitution



BS



x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

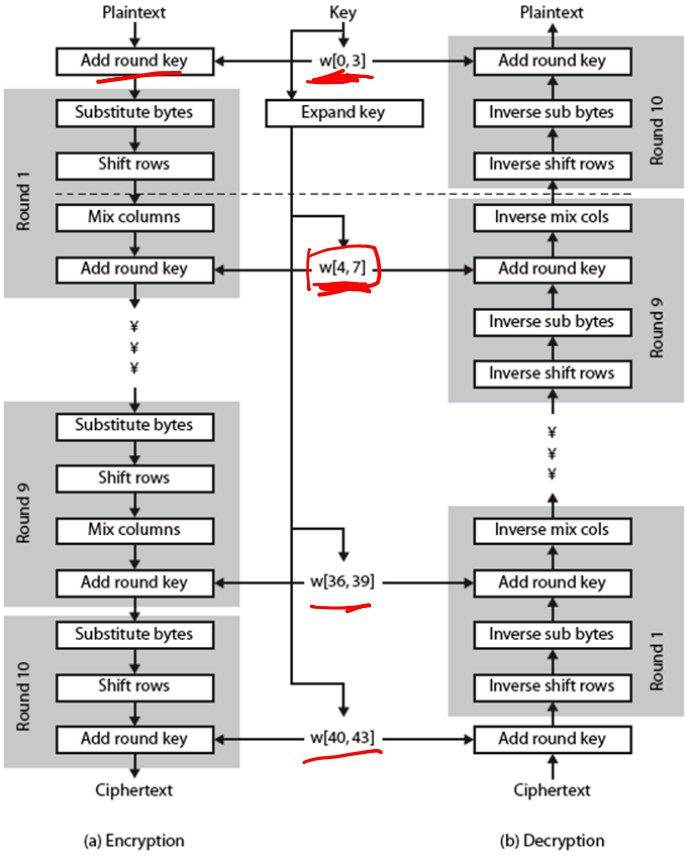
AES S-box

x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

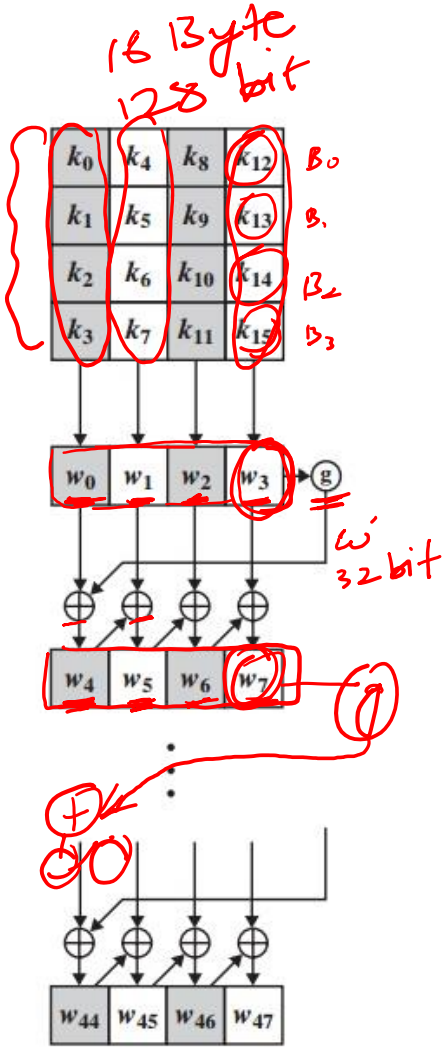
AES – Inverse S-box

AES Sub-Key Generation

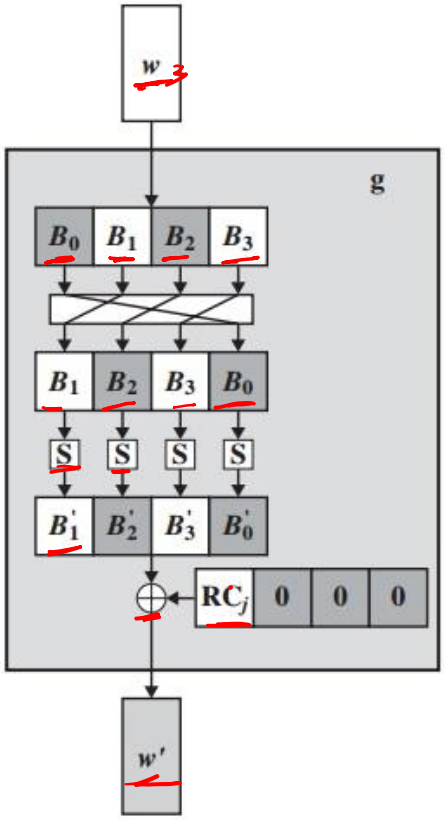
Key Expansion



(a) Encryption (b) Decryption



(a) Overall algorithm



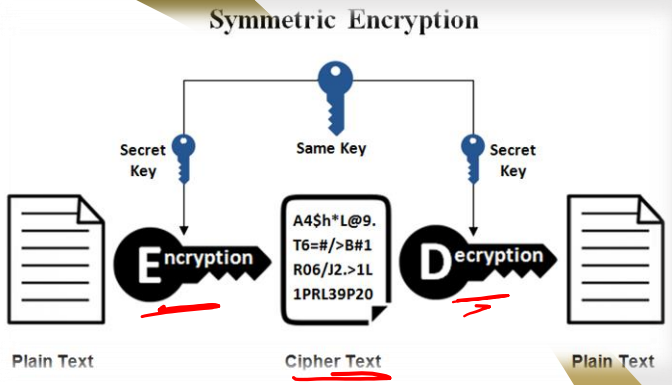
(b) Function g

Public-Key Cryptography

Asymmetric Encryption

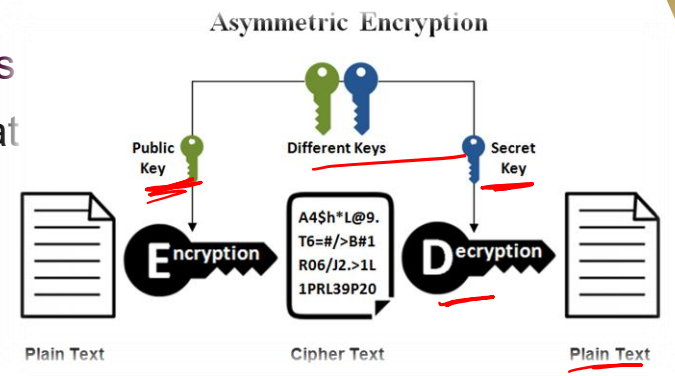
Public-Key Cryptography

Asymmetric Encryption



Why Public-Key?

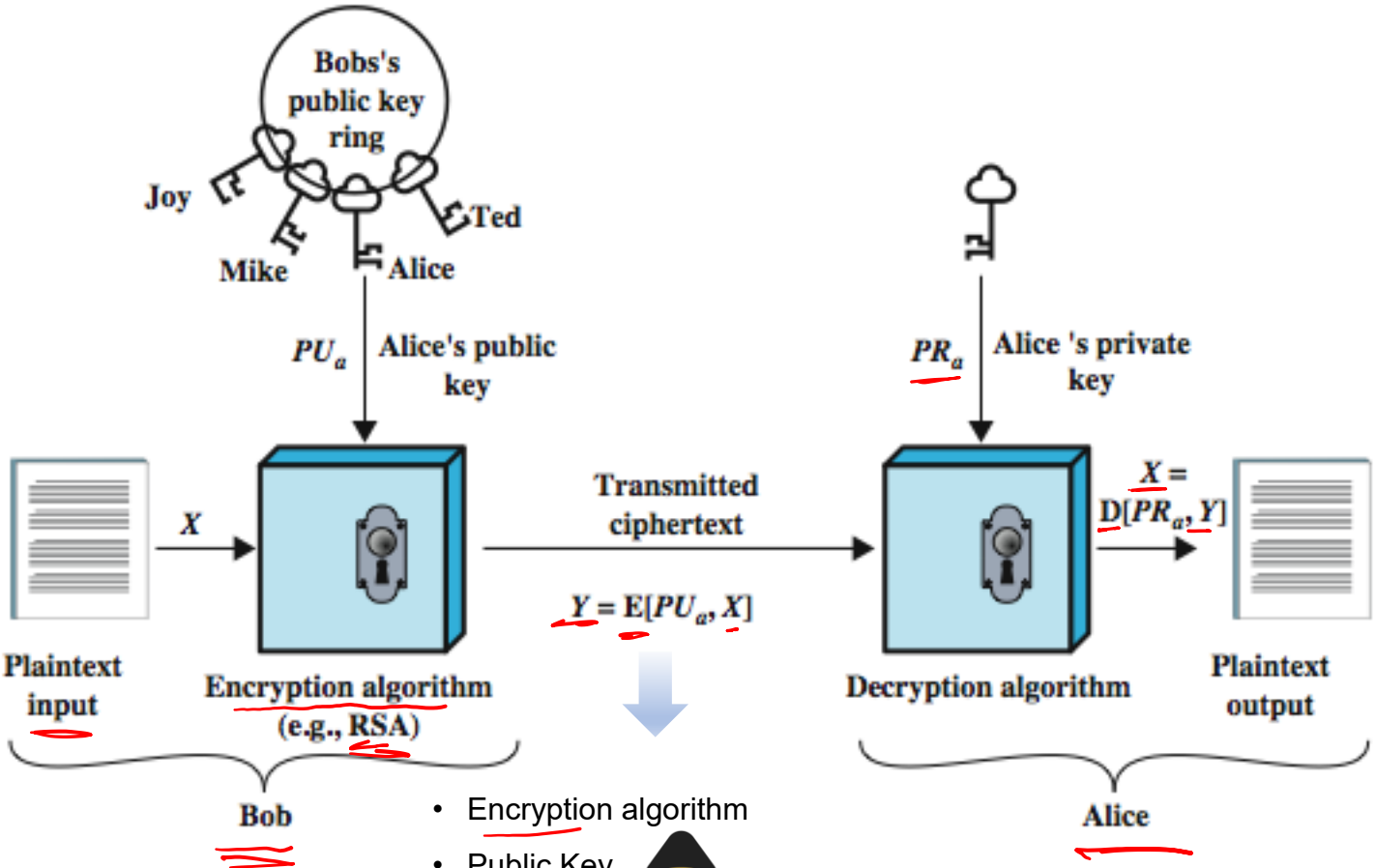
- Developed to address two major issues:
  - **key distribution** – how to have secure key exchange among communicating parties
  - **digital signatures** – how to verify a message comes intact from the claimed sender
- Public-Key Cryptography was designed to address these concerns
- Public invention due to Whitfield Diffie & Martin Hellman at
  - known earlier in classified community



- Probably most significant advancement in the history of cryptography
- Uses two keys – a public & a private key
- Asymmetric since different keys are used for encryption and decryption
- Uses clever application of number theoretic concepts to function
- This is not meant to replace Symmetric Encryption (private key crypto) but rather to complement…

Public-Key Cryptography

How public and private keys are used?



- Encryption algorithm
- Public Key
- Ciphertext



Private Key??
Plaintext??

Public-Key Cryptography

Example of public and private keys

Symmetric



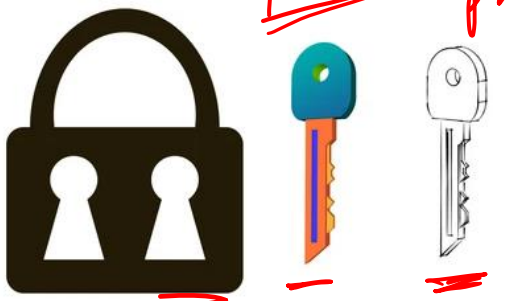


10 x 10 x 10 x 10 = 10,000



private

public



One-way Functions

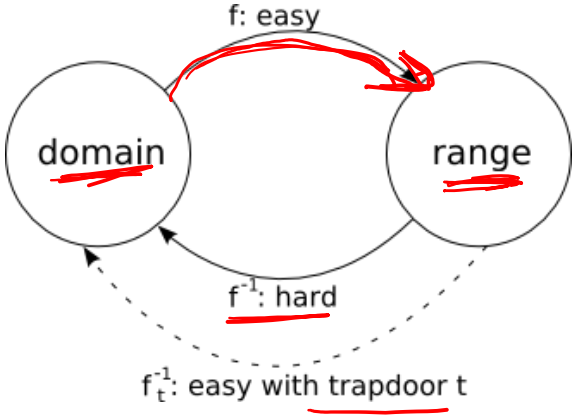
Base for Modern Cryptography

One-way Functions

Base for Modern Cryptography

- A **one-way function** is "easy" to compute and "difficult" to reverse.





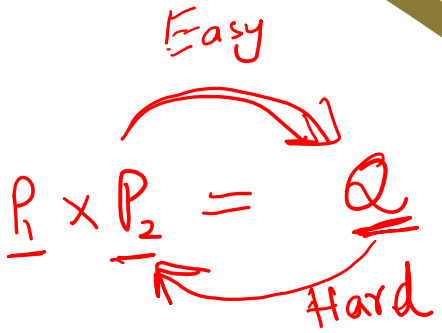
- The process of **exponentiation** means raising numbers to a power.
- Raising **2** to the power **3**, normally denoted 2^3 just means multiplying **2** by itself **3** times. In other words:
  - $2^3 = (2 \times 2 \times 2)$
  - $a^x = a \times a \times a \times a \times \ldots \times a$
- **Modular exponentiation** means computing a^x mod some other number **n**.
  - a^x mod n.
- In other words, given a number **a** and a pr… funct…
  - $f(x) = a^x \bmod n$ is a one-way function

For x=b, we can easily compute $y=f(b)=a^b \bmod n$ But its reverse is :(

For a particular y=c, its difficult to get respective x Such that $c=f(b)=a^x \bmod n$

One-way Functions

Base for Modern Cryptography



Another Example

- It is easy to take two prime numbers and multiply them together.
- If the numbers are small, we can do this in our heads, on a piece of paper.
- What if numbers get bigger and bigger?
- Multiplication of two **big** prime numbers is **believed** to be a one-way function.
- Check Wikipedia for RSA Numbers
- https://en.wikipedia.org/wiki/RSA_numbers#:~:text=In%20mathematics%2C%20the%20RSA%20numbers,prime%20factors%20of%20each%20number.
- One of the modern asymmetric algorithm RSA is based on this idea

RSA Algorithm

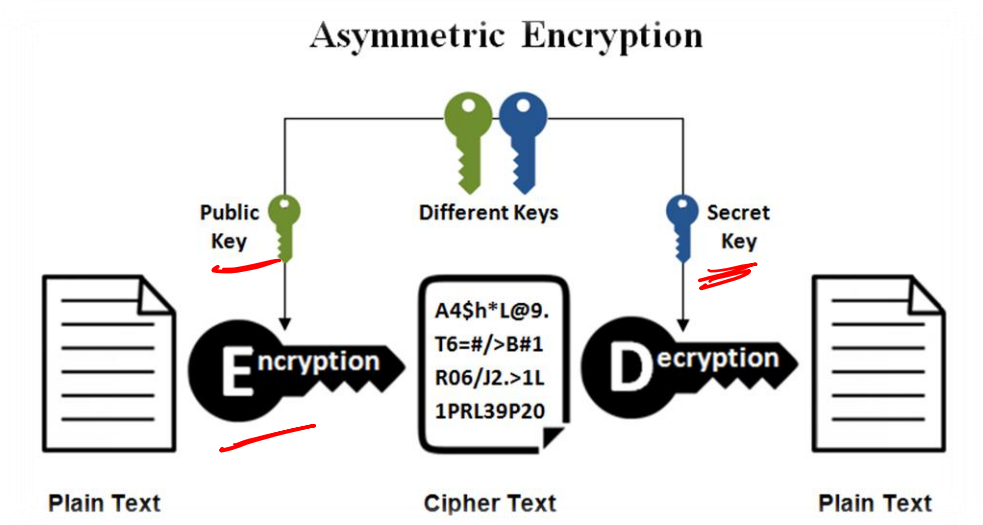
Asymmetric Encryption Algorithm

RSA Algorithm

Asymmetric Encryption Algorithm



- The **RSA** algorithm was the first practical implementation of public key encryption.
- It is named after the three researchers Ron Rivest, Adi Shamir and Len Adleman



RSA Algorithm

How the public and private keys are selected?

- Let **n** be the product of two large primes **p** and **q** **(i.e. n=pxq)**
  - at least 512 bits.
- Select a special number **e** $\in \{1, (p-1)(q-1)\}$
  - greater than 1 and less than (**p**-1)(**q**-1). The precise mathematical property that **e** must have is that there must be no numbers that divide neatly into **e** and into (**p**-1)(**q**-1), except for 1.
- Publish the pair of numbers (**n**,**e**)
- Compute the private key **d** from **p**, **q** and **e**
- The private key **d** is computed to be the unique inverse of **e** modulo (**p**-1)(**q**-1).
- In other words, **d** is the unique number less than (**p**-1)(**q**-1) that when multiplied by **e** gives you 1 modulo (**p**-1)(**q**-1).
  - ed = 1 mod (p-1)(q-1)

Public key: (e, n)
Private key: (d, n)

RSA Algorithm

How the message is encrypted and decrypted?

Encryption

Given a message M, $0 < M < n$ $\quad M \in Z_n - \{0\}$

use public key (e, n)

compute $C = M^e \bmod n$ $\quad C \in Z_n - \{0\}$

$ed = 1 \bmod (p-1)(q-1)$

Decryption

Given a ciphertext C, use private key (d)

Compute $C^d \bmod n = (M^e \bmod n)^d \bmod n = M^{ed} \bmod n = M$

Sender Side

Plaintext: M

Encryption

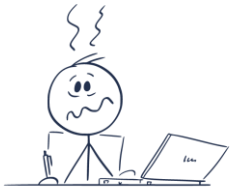
$C = M^e \bmod (n=pq)$

Ciphertext: C

Receiver Side

Ciphertext: C

Plaintext: $M = C^d \bmod n$



From n, difficult to figure out p,q

From (n,e), difficult to figure d.

From (n,e) and C, difficult to figure out M s.t. $C = M^e$

RSA Algorithm

Can we see the public and private keys?

- Let **n** be the product of two large primes **p** and **q** **(i.e. n=pxq)**
  - at least 512 bits.
- Select a special number **e**
  - greater than 1 and less than (**p**-1)(**q**-1). The precise mathematical property that **e** must have is that there must be no numbers that divide neatly into **e** and into (**p**-1)(**q**-1), except for 1.
- Publish the pair of numbers (**n**,**e**)
- Compute the private key **d** from **p**, **q** and **e**
- The private key **d** is computed to be the unique inverse of **e** modulo (**p**-1)(**q**-1).
- In other words, **d** is the unique number less than (**p**-1)(**q**-1) that when multiplied by **e** gives you 1 modulo (**p**-1)(**q**-1).
  - ed = 1 mod (p-1)(q-1)

Public key: (e, n)
Private key: (d, n)

A Digital Certificate is **an electronic file that is tied to a cryptographic key pair and authenticates the identity of a website, individual, organization, user, device or server**. It is also known as a public key certificate or identity certificate.

https://www.boxentriq.com/code-breaking/hex-to-decimal-converter

RSA Algorithm - Working Example

Asymmetric Encryption Algorithm

RSA Algorithm Example

How are the public and private keys generated?

- Assume we have generated the RSA public-private key pair:

- Choose two "big" primes p=11 and q=13
- Compute the number **n** =p*q = 143
- Number **e=?** ∈ **[1,** (p-1)(q-1)**] = [1, 120]**
  - Relative prime with (p-1)(q-1)
- **e=7**

- private exponent ***d*** = ?
  - ed = 1 mod (p-1)(q-1)
- ***d*** =103

Public key: (e, n)
Private key: (d, n)

- Let **n** be the product of two large primes **p** and **q** **(i.e. n=pxq)**
  - at least 512 bits.
- Select a special number **e**
  - greater than 1 and less than (**p**-1)(**q**-1). The precise mathematical property that **e** must have is that there must be no numbers that divide neatly into **e** and into (**p**-1)(**q**-1), except for 1.
- Publish the pair of numbers (**n**,**e**)
- Compute the private key **d** from **p**, **q** and **e**
- The private key **d** is computed to be the unique inverse of **e** modulo (**p**-1)(**q**-1).
- In other words, **d** is the unique number less than (**p**-1)(**q**-1) that when multiplied by **e** gives you 1 modulo (**p**-1)(**q**-1).
  - ed = 1 mod (p-1)(q-1)

Public key: (e, n)
Private key: (d, n)

https://cryptobook.nakov.com/asymmetric-key-ciphers/the-rsa-cryptosystem-concepts

RSA Algorithm Example

How the message is encrypted and decrypted?

- number **n** say 143
- **e=7**
- ***d*** =103

Public key: (e, n) (7, 143)
Private key: (d, n) (103, 143)

- Let's **encrypt** a secret message ***msg*** = **83**

$C = 83^{7} \bmod 143 = 8$

Encryption
$C = M^{e} \bmod (n=pq)$

- Let's now try **decryption** of the secret message **C=*8***

$M = 8^{103} \bmod 143 = 83$

Plaintext: $M = C^{d} \bmod n$

https://cryptobook.nakov.com/asymmetric-key-ciphers/the-rsa-cryptosystem-concepts

Diffie–Hellman Key Exchange Protocol

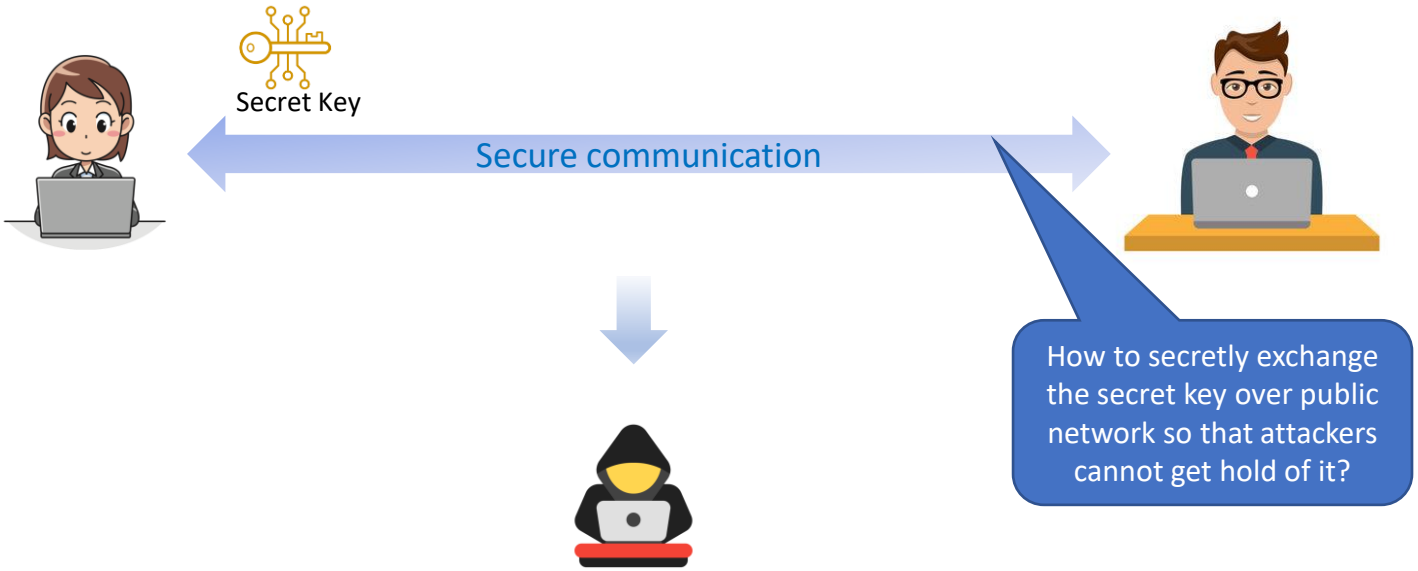
For Secure Key Exchange

Diffie–Hellman Key Exchange Protocol

For Secure Key Exchange

Two major issues with symmetric encryptions algorithms:

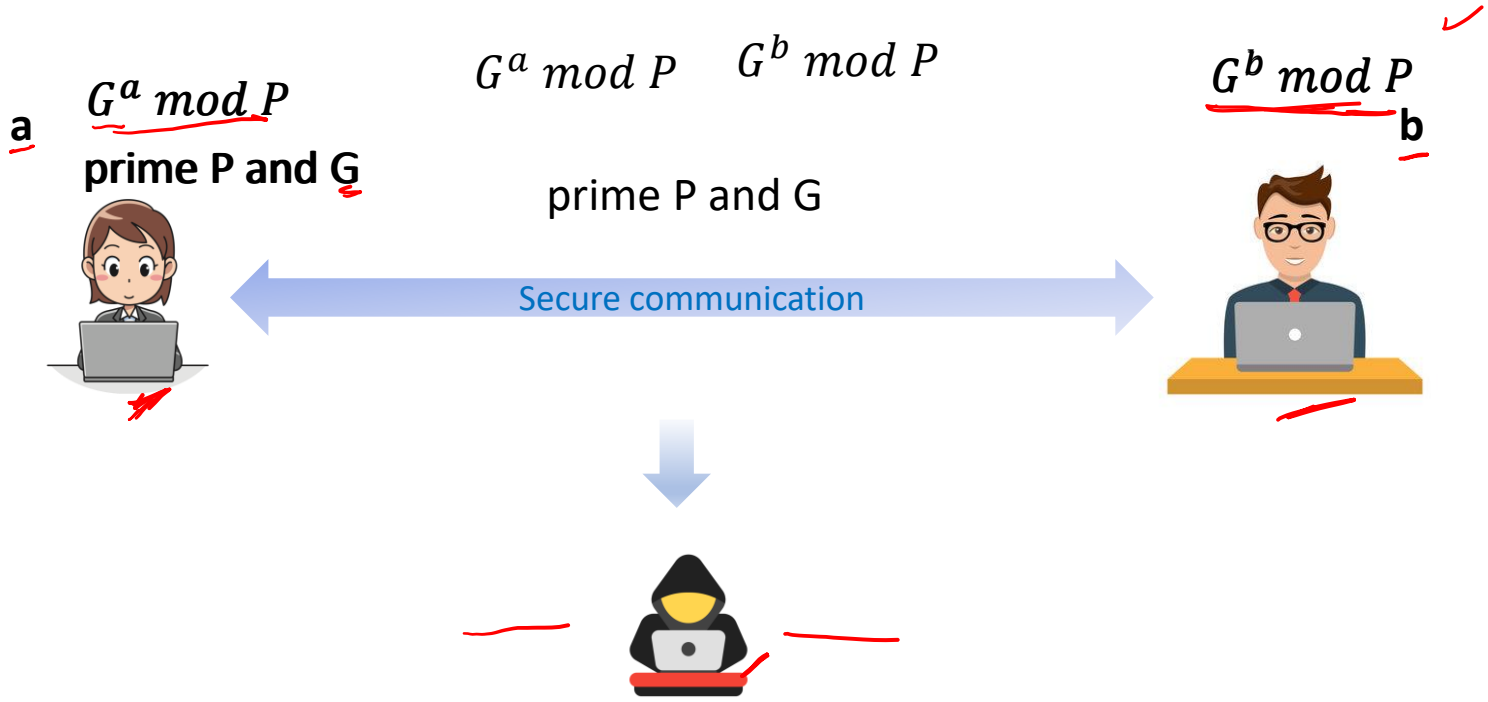
- **key distribution** – how to have secure key exchange among communicating parties
- **digital signatures** – how to verify a message comes intact from the claimed sender



Diffie–Hellman Key Exchange Protocol

How Keys are secretly exchanged?

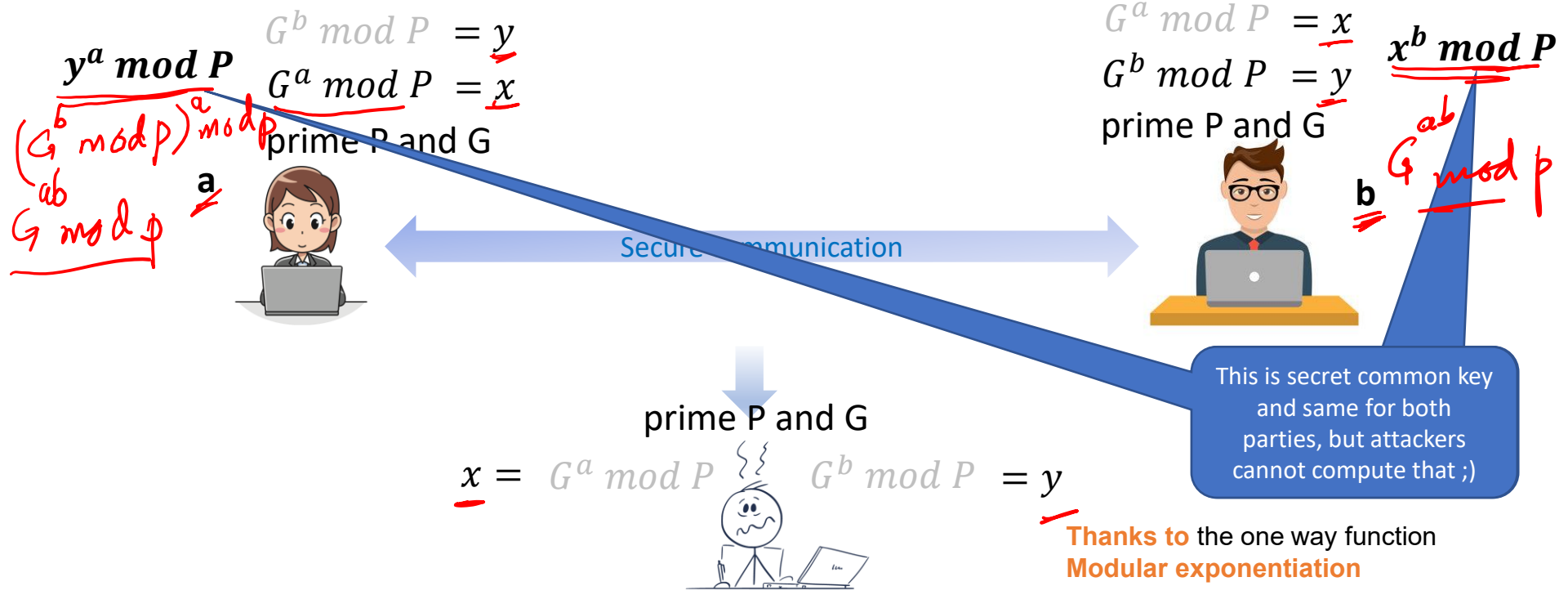
- Lets see, how two users can secretly exchange the key in presence of attacker
- Either party can choose one prime P and G (a primitive root of P) and exchange with the other…attacker can also see that
- Next, each party choose their private values
  - lets say, user-1 choose "**a**" and user-2 choose **"b"**.
- Afterwards, both parties compute a number $G^x \ mod \ P$ and send it to the other
- Finally, both parties can generate the common secret key



Diffie–Hellman Key Exchange Protocol

How Keys are secretly exchanged?

- Lets see, how two users can secretly exchange the key in presence of attacker
- Either party can choose one prime P and G (a primitive root of P) and exchange with the other…attacker can also see that
- Next, each party choose their private values
  - lets say, user-1 choose "**a**" and user-2 choose **"b"**.
- Afterwards, both parties compute a number $G^x \ mod \ P$ and send it to the other
- Finally, both parties can generate the common secret key



Thanks to the one way function
Modular exponentiation

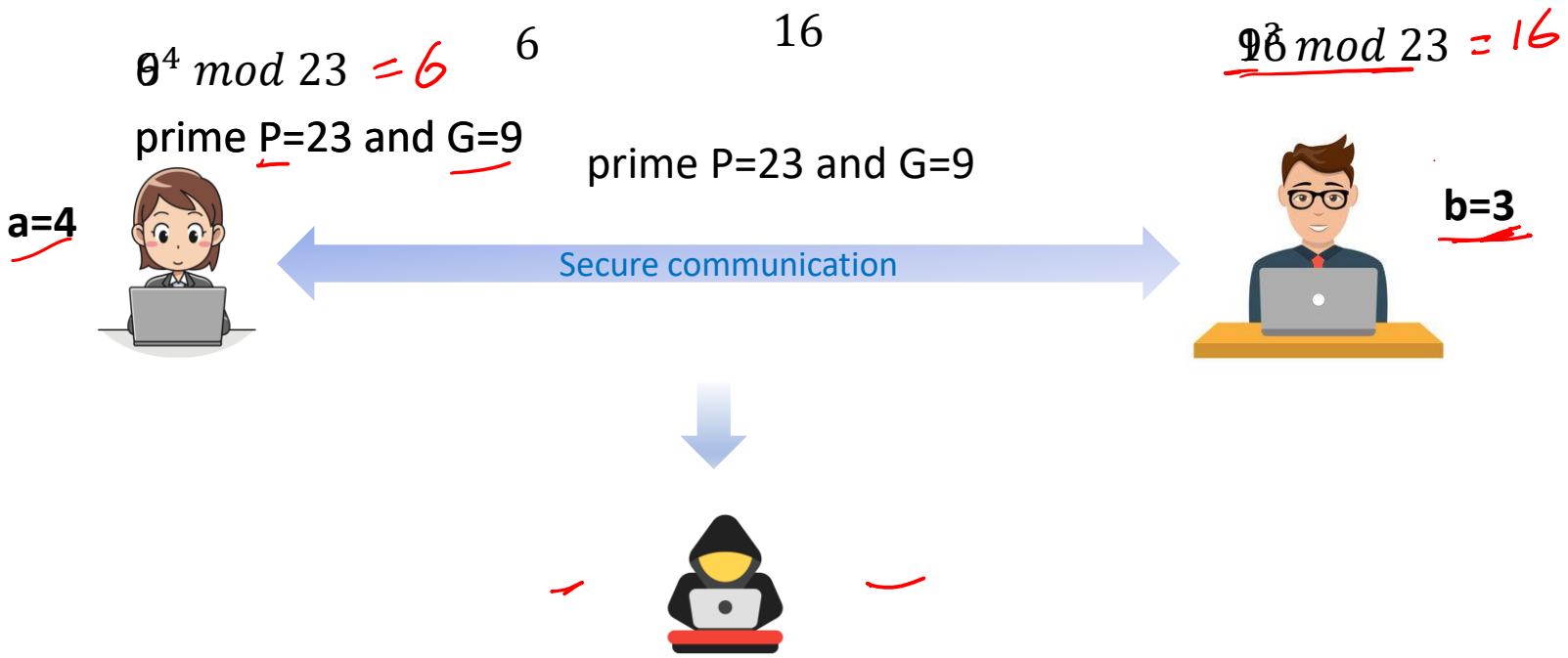
Diffie–Hellman Key Exchange Working Example

Secure Key Exchange

Diffie–Hellman Key Exchange - Example

How Keys are secretly exchanged?

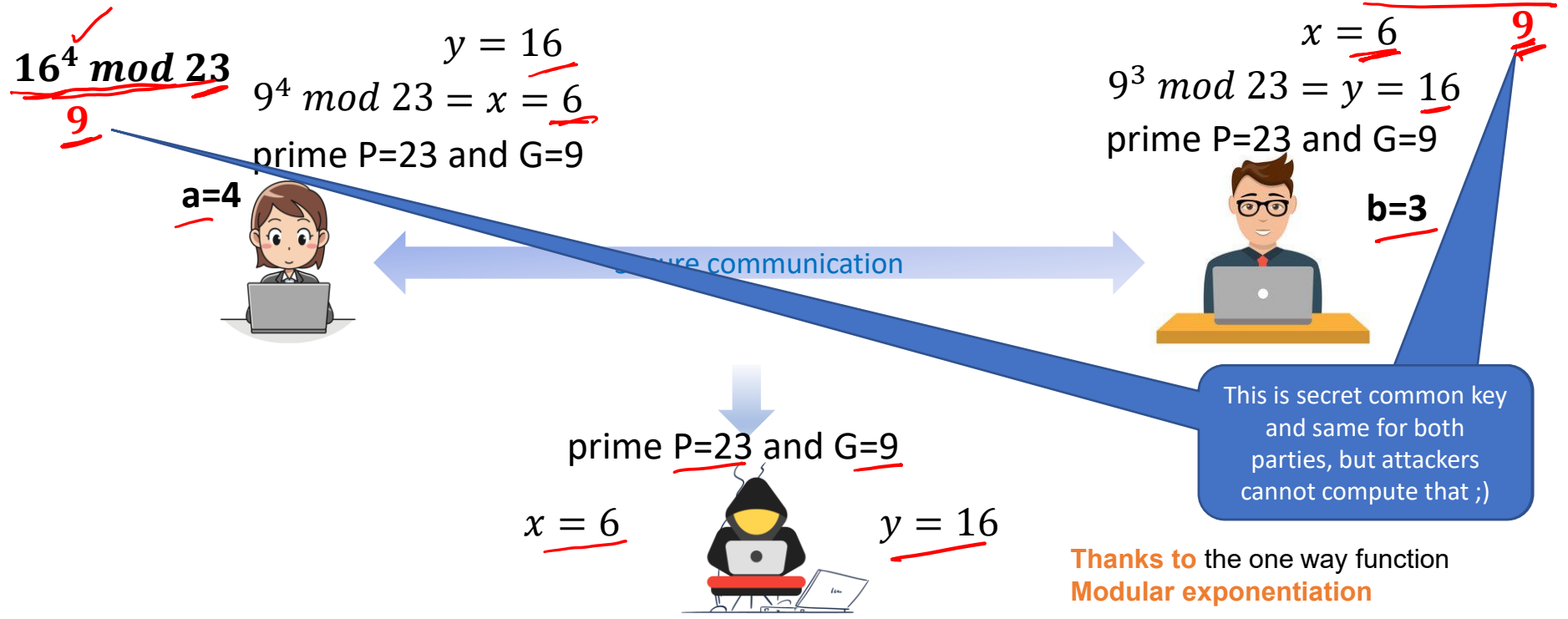
- Lets see, how two users can secretly exchange the key in presence of attacker
- Either party can choose one prime P=23 and G=9 (a primitive root of P) and exchange with the other…attacker can also see that
- Next, each party choose their private values
  - lets say, user-1 choose "**a=4**" and user-2 choose **"b=3"**.
- Afterwards, both parties compute a number $G^x \ mod \ P$ and send it to the other
- Finally, both parties can generate the common secret key



Diffie–Hellman Key Exchange - Example

How Keys are secretly exchanged?

- Lets see, how two users can secretly exchange the key in presence of attacker
- Either party can choose one prime P and G (a primitive root of P) and exchange with the other…attacker can also see that
- Next, each party choose their private values
  - lets say, user-1 choose "**a**" and user-2 choose **"b"**.
- Afterwards, both parties compute a number $G^x \ mod \ P$ and send it to the other
- Finally, both parties can generate the common secret key



Thanks to the one way function
Modular exponentiation

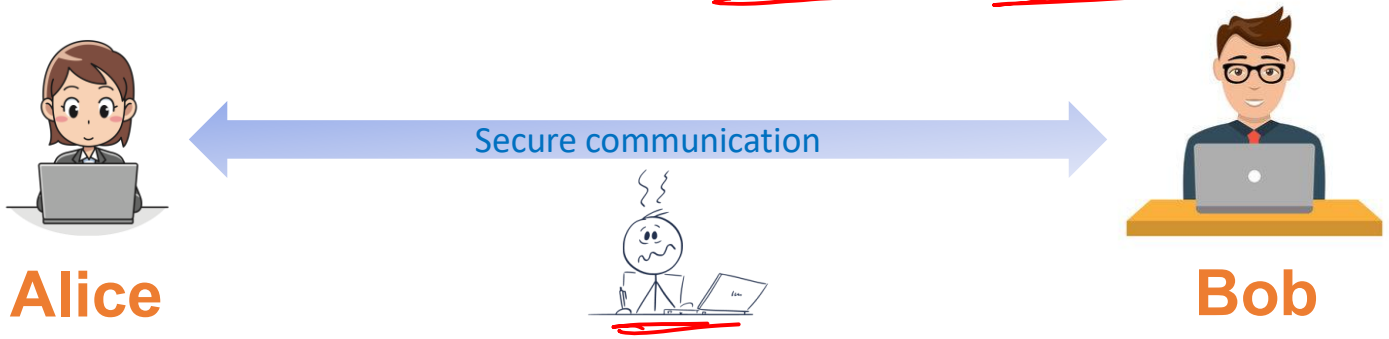
Security Issue in the Diffie-Hellman

Can we trust the Diffie-Hellman Algorithm?

Security Issue in the Diffie-Hellman

Can we trust the Diffie-Hellman Algorithm for secure Key exchange?

- Diffie-Hellman Algorithm is safe against sniffing attack…interception



- But what if attacker sits in the middle?



Man in the Middle Attack

Network Devices

Introduction

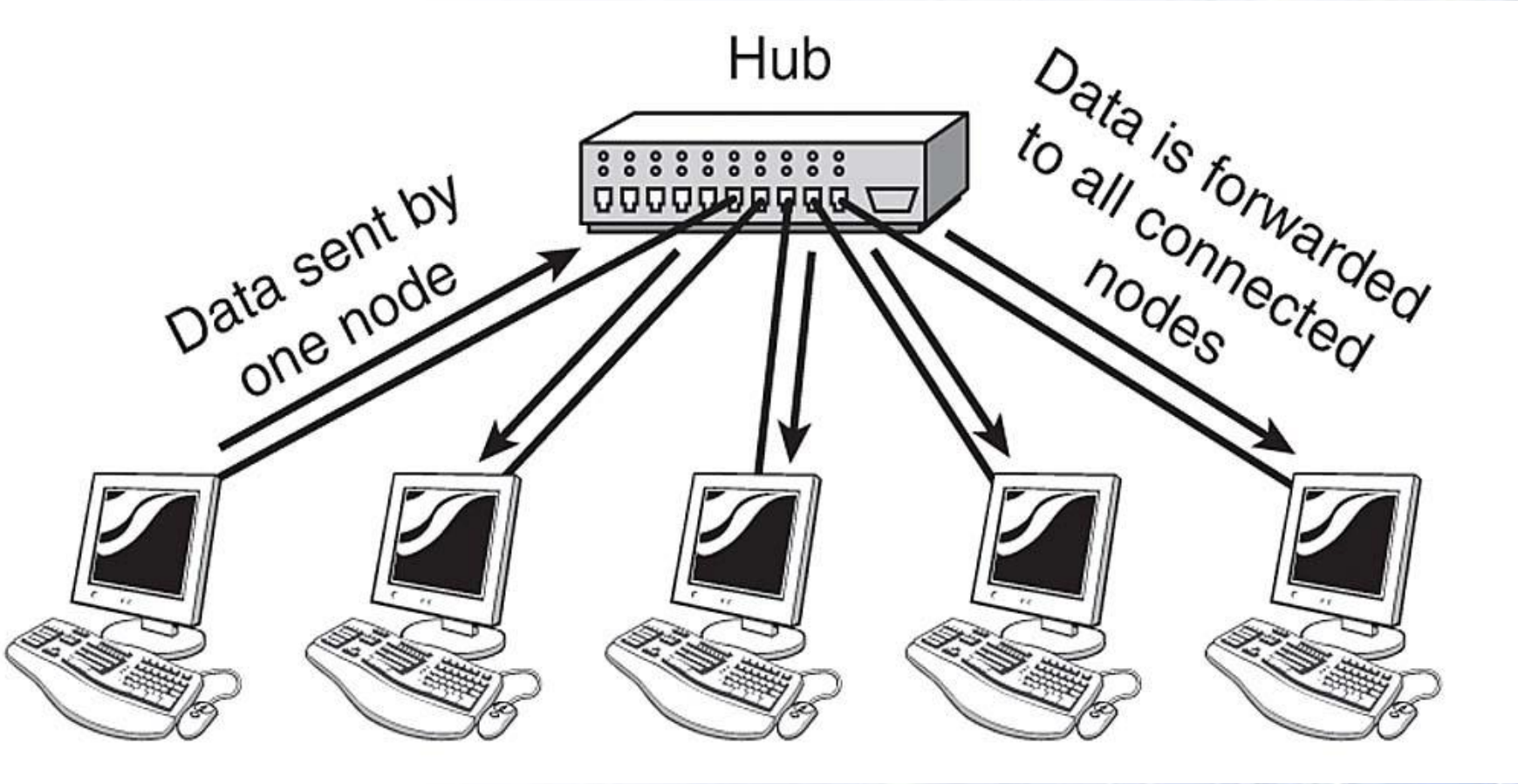
- In this topic we will cover the basics of network devices and their functions.
- We will discuss different types of network devices, including routers, switches, firewalls, and more.

Hub

- A network hub is a device that broadcasts data to every computer or Ethernet-based device connected to it.
- Network hubs are best suited for small, simple local area network (LAN) environments.



Working of Hub

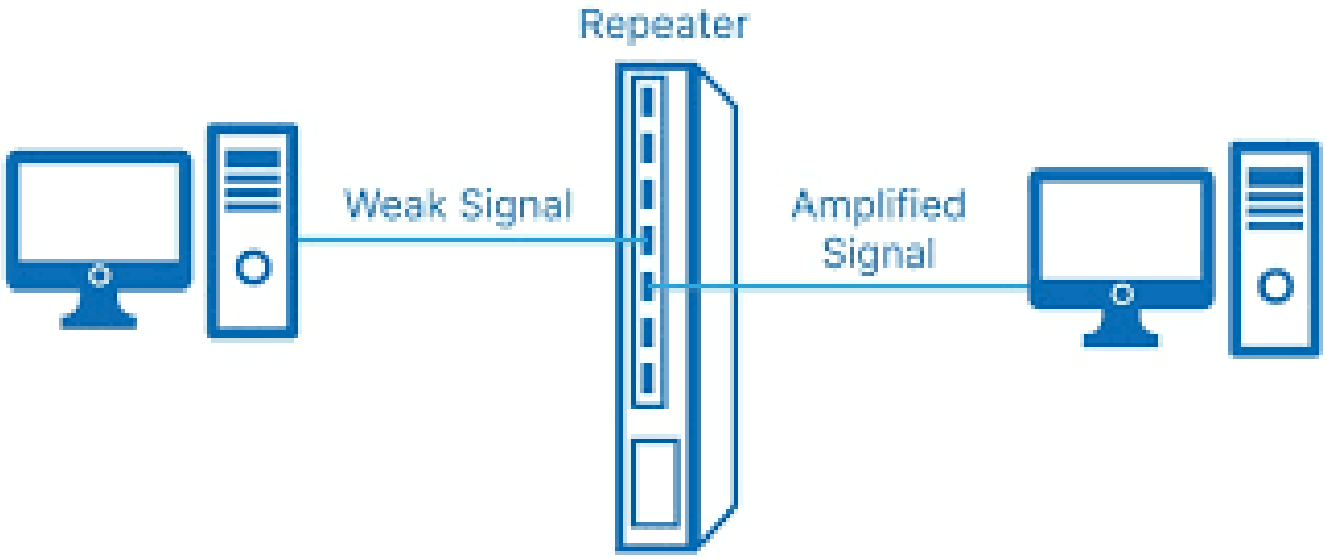


Repeater

- Repeaters are network devices operating at physical layer of the OSI model that amplify or regenerate an incoming signal before retransmitting it.
- They are incorporated in networks to expand its coverage area. They are also known as signal boosters.



Working of Repeater



Switch

- A switch is a network device that connects devices on a local area network (LAN).
- It operates at the data link layer of the OSI model and uses MAC addresses to direct traffic to the appropriate device.



Switch’s working

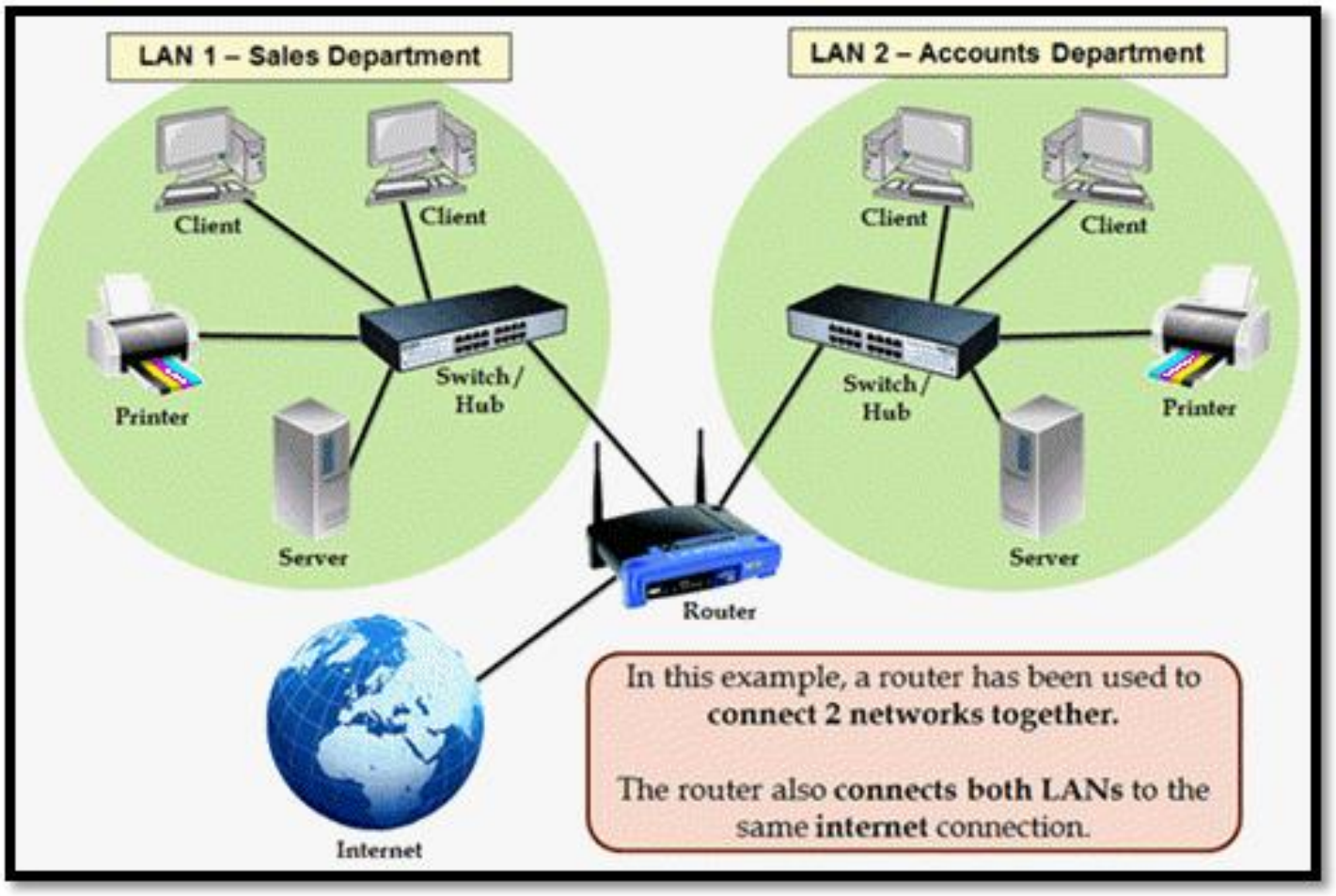


Routers

- A router is a network device that connects multiple networks and routes traffic between them.
- It operates at the network layer of the OSI model and uses routing tables to determine the best path for data to travel.

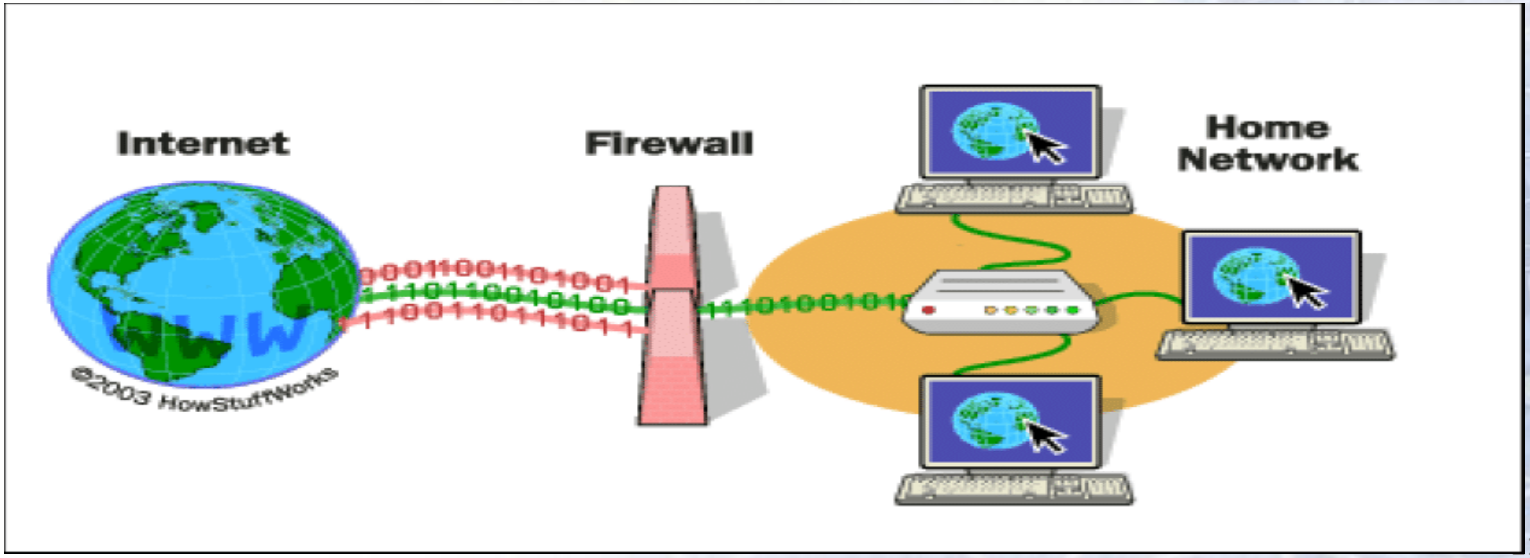


Router's working



Firewalls

- A firewall is a network security device that monitors and controls incoming and outgoing network traffic.
- It can block unauthorized access to a network and prevent malicious traffic from entering or leaving the network.

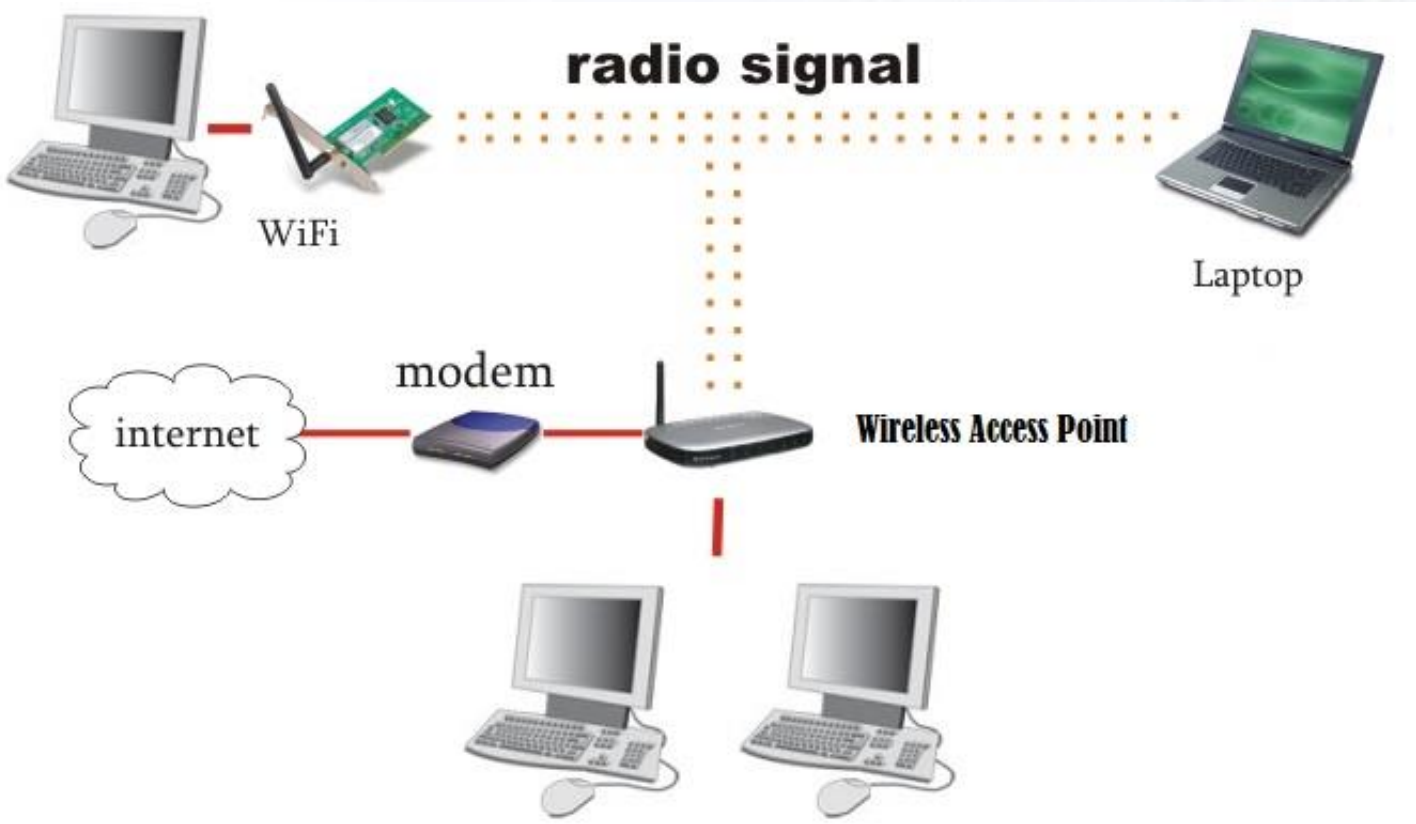


Wireless Access Points

- A wireless access point (WAP) is a network device that allows wireless devices to connect to a wired network.
- It provides a wireless signal for devices to connect to and can support multiple wireless devices simultaneously.



Wireless Access Point's working

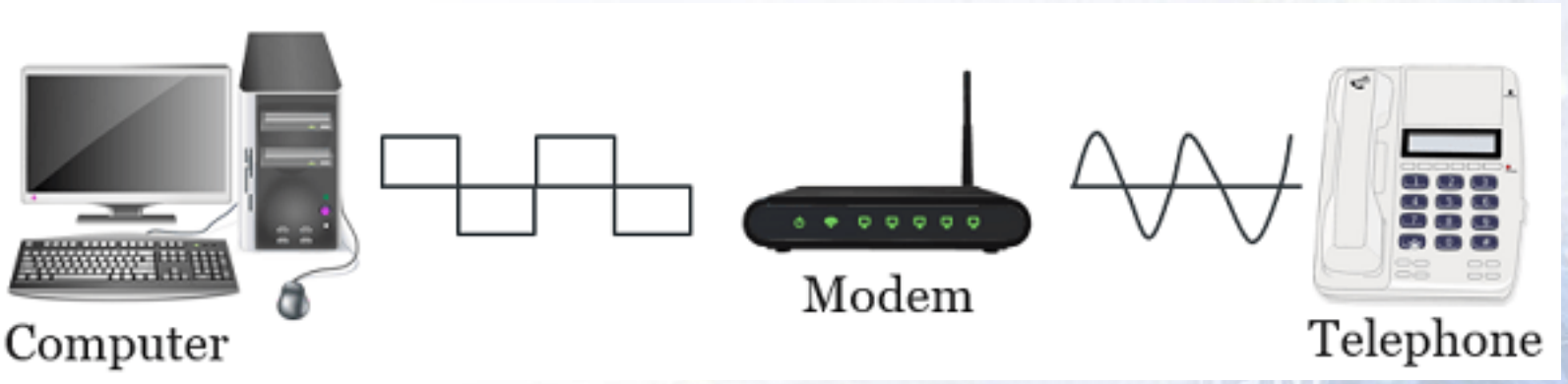


Modems

- A modem is a network device that modulates and demodulates signals between a computer and the internet service provider (ISP).
- It converts digital signals from a computer into analog signals that can travel over phone lines or cable lines, and vice versa.



Working of Modem

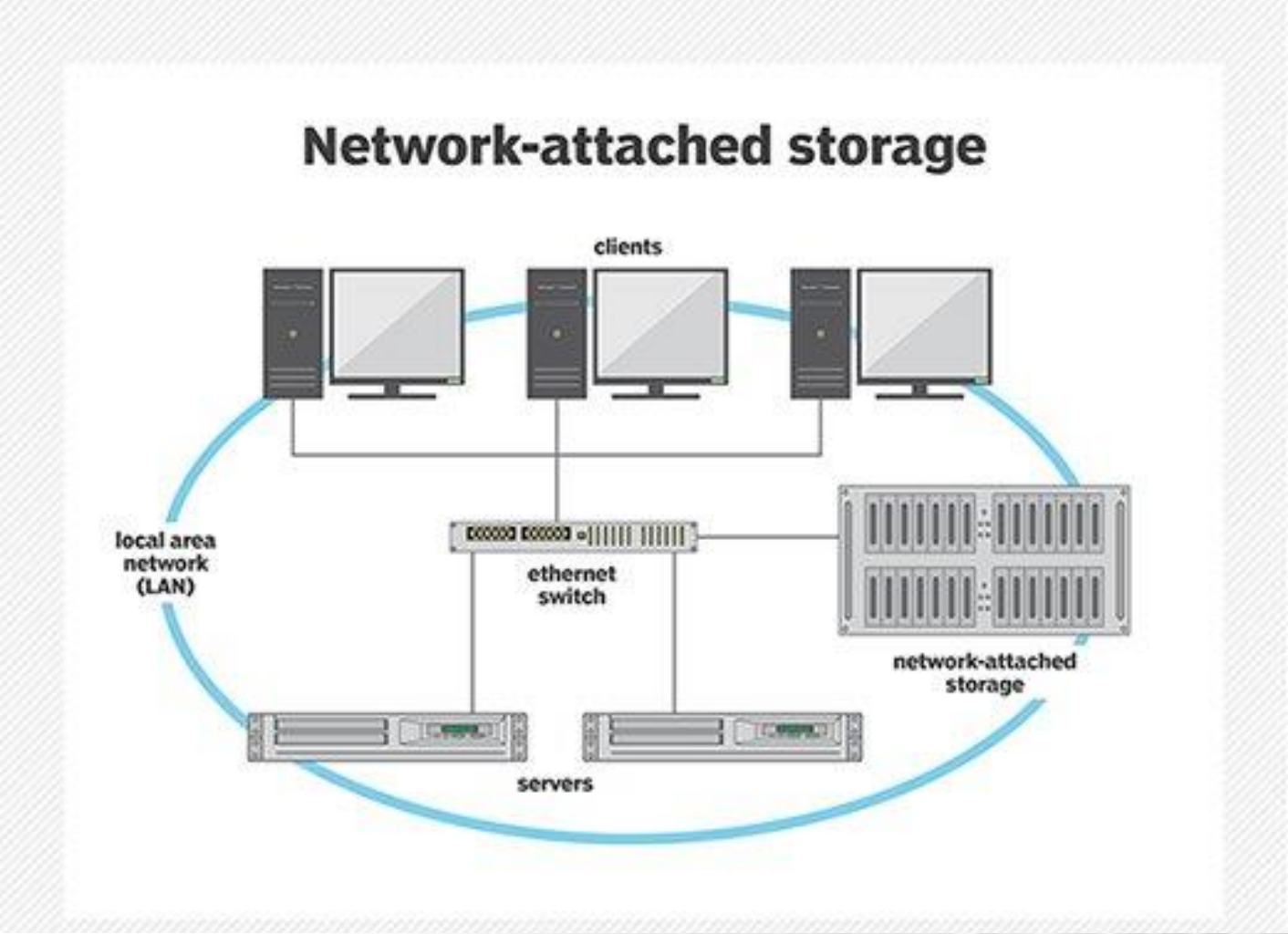


Network Attached Storage (NAS)

- Network Attached Storage (NAS) is a network device that allows multiple devices to share and access files from a central location.
- It can provide data redundancy, backup, and storage capabilities for a network.



Network Attached Storage working



Conclusion

- In conclusion, network devices are essential components of a computer network.
- Understanding the functions and capabilities of each device can help network administrators design, configure, and maintain a secure and efficient network infrastructure.

Perimeter Security

Introduction

- In this topic we will cover the basics of perimeter security and its importance in protecting a network.
- We will discuss different types of perimeter security, including physical and logical measures.

Physical Perimeter Security

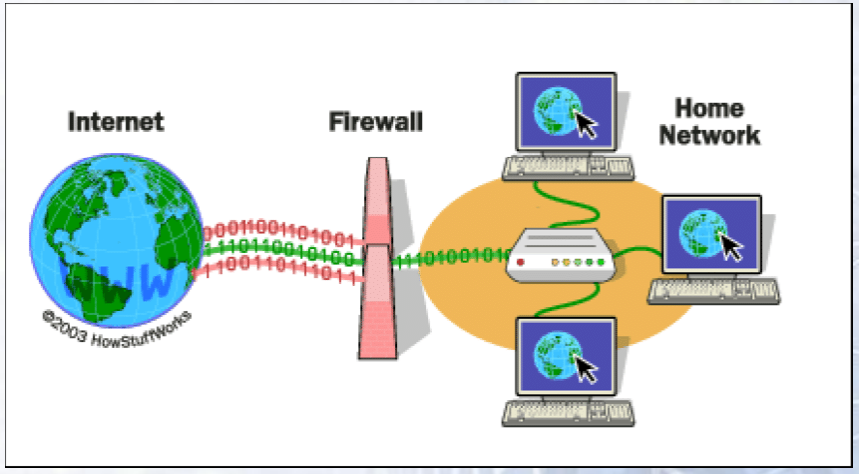
- Physical perimeter security includes measures such as fences, gates, walls, and security cameras.
- These measures restrict access to a physical location and can prevent unauthorized entry.

Logical Perimeter Security

- Logical perimeter security includes measures such as firewalls, intrusion detection systems, and virtual private networks (VPNs).
- These measures control access to a network and can prevent unauthorized access.

Firewalls

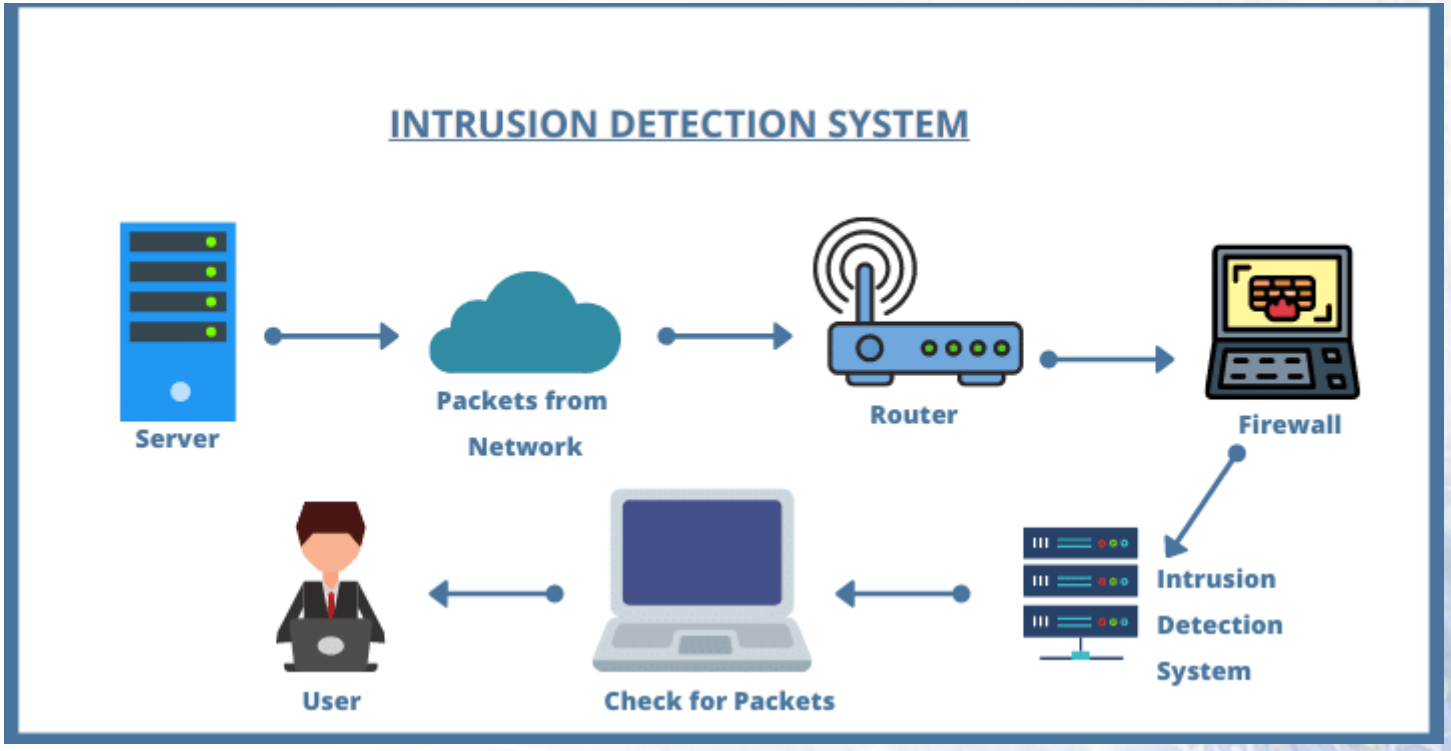
- A firewall is a logical perimeter security device that monitors and controls incoming and outgoing network traffic.
- It can block unauthorized access to a network and prevent malicious traffic from entering or leaving the network.



Intrusion Detection Systems (IDS)

- An intrusion detection system (IDS) is a logical perimeter security device that monitors a network for suspicious activity.
- It can detect and alert network administrators of potential security breaches.

Working of Intrusion Detection Systems (IDS)

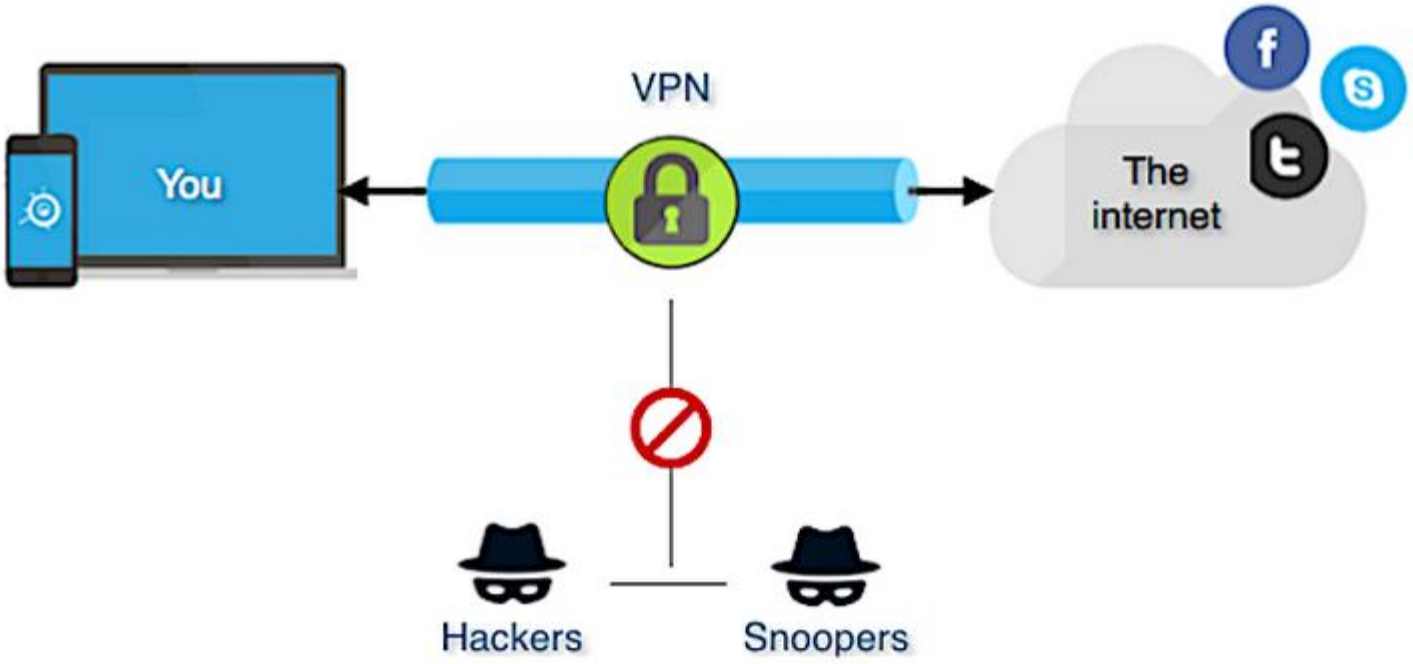


Virtual Private Networks (VPNs)

- A virtual private network (VPN) is a logical perimeter security measure that allows remote users to securely connect to a network.
- It encrypts traffic between the remote user and the network, providing secure access to network resources.



Working of VPN



Access Control

- Access control is a logical perimeter security measure that restricts access to network resources based on user credentials and permissions.
- It ensures that only authorized users have access to sensitive information.



Conclusion

- In conclusion, perimeter security is a critical component of network security.
- Physical and logical measures can be used to protect a network from unauthorized access and malicious attacks.
- Understanding the various types of perimeter security measures and their functions can help network administrators design, configure, and maintain a secure network infrastructure.

What is an intrusion?

Introduction

- In this topic we will cover the basics of intrusion and its impact on a network.
- We will discuss what an intrusion is, types of intrusions, and how to prevent them.

What is an intrusion?

- An intrusion is an unauthorized attempt to access, use, or modify a network, system, or device.
- It can occur through various means, including malware, phishing attacks, and brute-force attacks.

Types of Intrusions

There are different types of intrusions, including:

- **External Intrusion**: when an attacker attempts to gain access to a network from outside.
- **Internal Intrusion**: when an attacker gains access to a network from within, such as an employee with malicious intent.
- **Insider Threat**: when an employee or contractor intentionally or unintentionally causes harm to a network.
- **Distributed Denial of Service (DDoS)**: when an attacker floods a network with traffic to disrupt normal operations.

Impact of Intrusions

Intrusions can have severe impacts on a network, including:

- Data theft or loss
- Financial loss
- Reputation damage
- Disruption of operations

Prevention Measures

To prevent intrusions, organizations can implement various measures, including:

- Firewalls and intrusion detection/prevention systems
- Regular software updates and patching
- Strong password policies
- Employee training on phishing and social engineering attacks
- Access control policies

Incident Response

- Despite preventative measures, intrusions can still occur.
- Organizations should have an incident response plan in place to quickly and effectively respond to a security breach.

Conclusion

- In conclusion, intrusions are unauthorized attempts to access, use, or modify a network, system, or device.
- They can have severe impacts on an organization, but prevention measures and incident response plans can help mitigate the risks.

Examples of Intrusion

Introduction

- In this topic we will cover some common examples of intrusions.
- We will discuss the types of attacks used in each example and the impact on the affected network.

Malware Infection

- Malware is a type of software designed to harm a computer system or network.
- Examples of malware include viruses, worms, and Trojan horses.
- A malware infection can result in stolen data, financial loss, and network downtime.



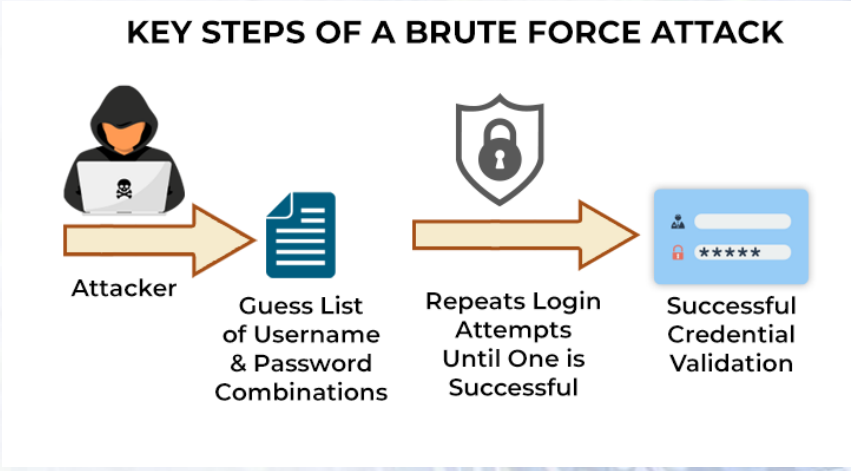
Phishing Attacks

- Phishing attacks are attempts to trick individuals into revealing sensitive information.
- Attackers often use email or social media to deceive victims into clicking a malicious link or providing personal information.
- A successful phishing attack can result in stolen login credentials or sensitive data.



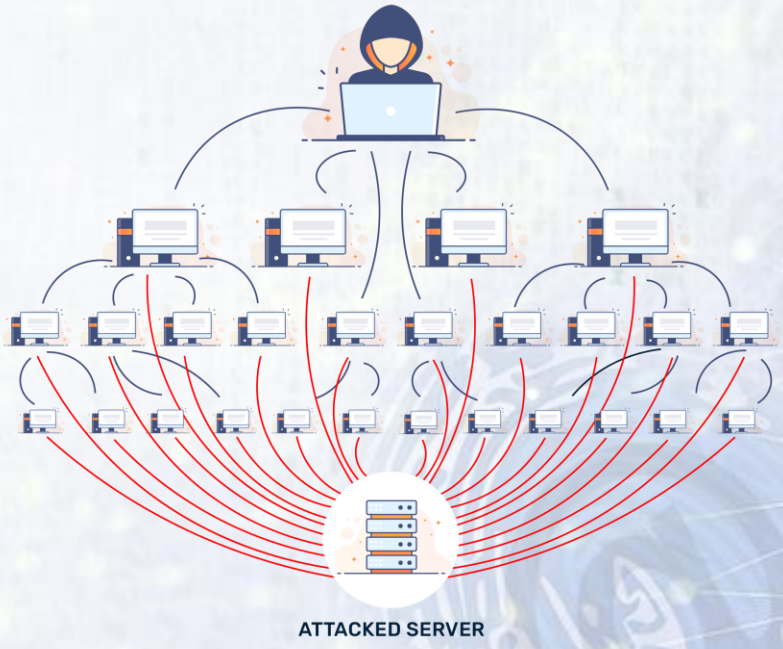
Brute-Force Attacks

- A brute-force attack is an attempt to gain unauthorized access to a system or network by guessing passwords.
- Attackers use automated tools to try multiple password combinations until they find the correct one.
- A successful brute-force attack can result in unauthorized access to sensitive data.



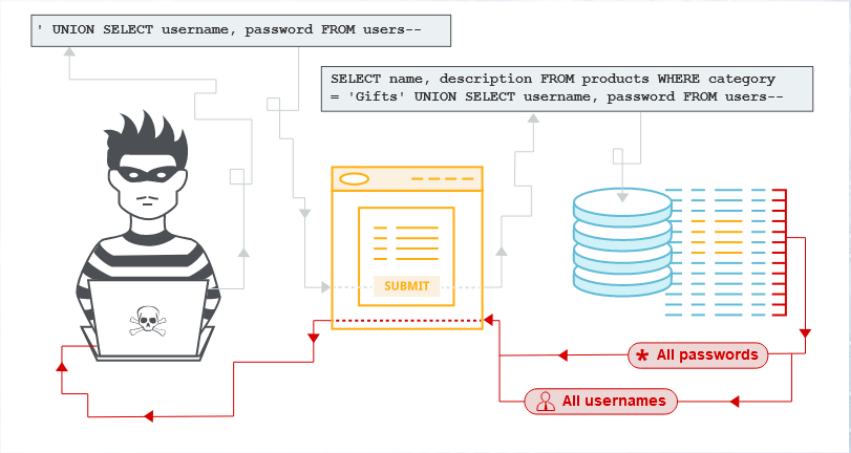
Distributed Denial of Service (DDoS)

- A DDoS attack is an attempt to disrupt normal network operations by overwhelming the network with traffic.
- Attackers use a botnet, a group of compromised devices, to flood the network with traffic.
- A successful DDoS attack can result in network downtime and financial loss.



SQL Injection

- An SQL injection is an attack that targets the database of a web application.
- Attackers input malicious SQL code into a web form to access or modify sensitive information stored in the database.
- A successful SQL injection can result in unauthorized access to sensitive data.



Conclusion

- In conclusion, there are various examples of intrusions that can impact a network.
- Attackers use different types of attacks, including malware infections, phishing attacks, brute-force attacks, DDoS attacks, and SQL injections.
- Organizations must implement strong security measures, such as firewalls, intrusion detection systems, and access control policies, to prevent and mitigate the impact of intrusions.

Intruder Behavior

Introduction

- In this topic we will cover intruder behavior and how it can impact a network.
- We will discuss the different types of intruders and their motivations for attacking a network.

Types of Intruders

There are different types of intruders, including:

Script Kiddies: inexperienced attackers who use pre-written scripts to launch attacks.

- **Hacktivists**: attackers who target a network to promote a political or social cause.
- **Insiders**: employees or contractors who intentionally or unintentionally cause harm to a network.
- **Cybercriminals**: attackers who target a network for financial gain.
- **Nation-state Actors**: attackers who are sponsored by a government to gain access to sensitive information.

Motivations for Intruder Behavior

Intruders may have various motivations for attacking a network, including:

- Financial gain
- Political or social reasons
- Espionage
- Personal challenge
- Revenge

Intruder Methods

Intruders use various methods to gain access to a network, including:

- Exploiting vulnerabilities in software or hardware
- Social engineering, such as phishing attacks
- Brute-force attacks
- Distributed denial of service (DDoS) attacks
- Insider threats

Impact of Intruder Behavior

Intruder behavior can have severe impacts on a network, including:

- Data loss or theft
- Financial loss
- Reputation damage
- Disruption of operations
- Legal consequences

Prevention and Mitigation

To prevent and mitigate the impact of intruder behavior, organizations can implement various measures, including:

- Strong passwords and access control policies
- Regular software updates and patching
- Employee training on social engineering attacks
- Firewalls and intrusion detection/prevention systems
- Incident response plans

Conclusion

- In conclusion, intruder behavior can have severe impacts on a network, and there are different types of intruders with varying motivations for attacking a network.
- Organizations must implement strong security measures to prevent and mitigate the impact of intruder behavior, including strong passwords, access control policies, regular software updates, employee training, and incident response plans.

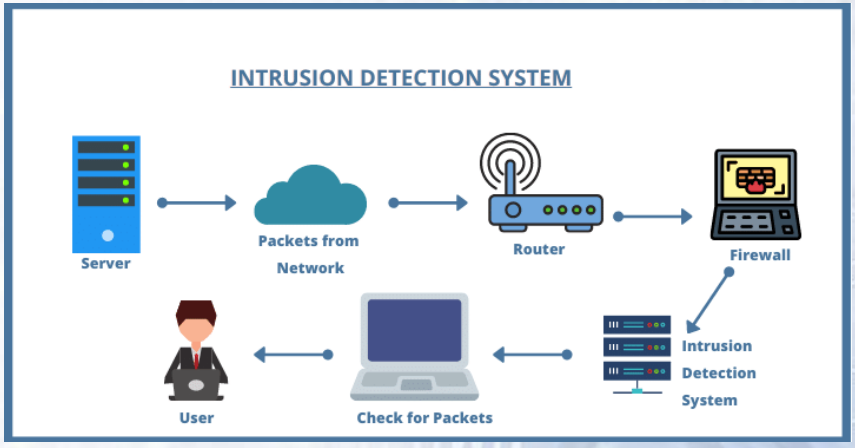
Intrusion Detection System (IDS)

Introduction

- In this topic we will cover Intrusion Detection System (IDS) and its importance in network security.
- We will discuss the types of IDS and how they work to detect intrusions.

What is an IDS?

- An IDS is a security tool designed to detect and alert on malicious activity on a network.
- IDS can detect unauthorized access, malware infections, phishing attacks, and other types of intrusions.



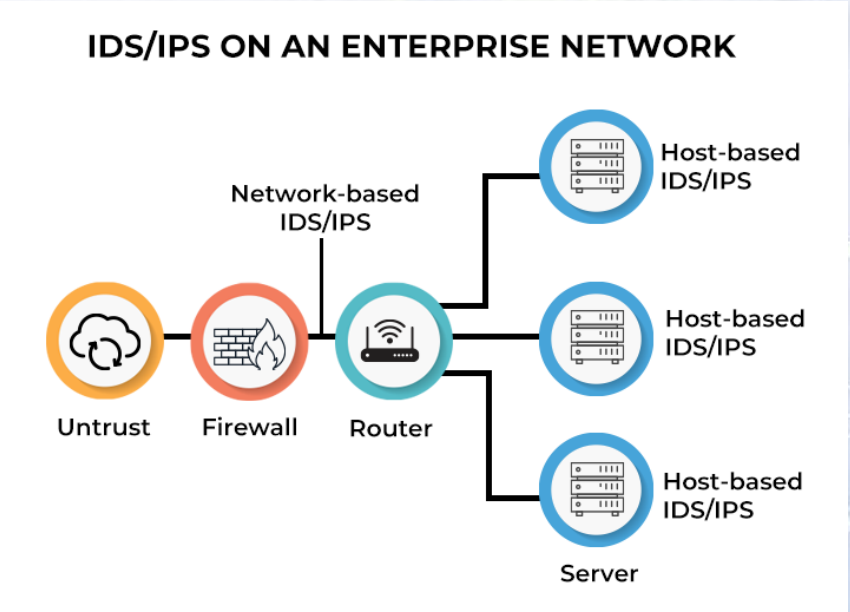
Types of IDS

There are two types of IDS:

- **Network-based IDS (NIDS)**: These monitor network traffic for suspicious activity, such as unusual traffic patterns or known attack signatures.
- **Host-based IDS (HIDS)**: These monitor activity on individual devices, such as servers or workstations, to detect unauthorized access or system-level attacks.

How IDS Works?

- IDS works by comparing network traffic or system activity against known attack signatures, behavior patterns, or other indicators of compromise (IoCs).
- IDS can detect intrusions by analyzing packet headers and payloads, system logs, and other data sources.
- IDS alerts security teams or generates automated responses, such as blocking traffic or quarantining affected devices.



Benefits of IDS

IDS provides several benefits, including:

- Early detection and alerting of intrusions, reducing the impact of an attack.
- Faster incident response by identifying the affected devices and the scope of the attack.
- Improved visibility into network traffic and activity, allowing security teams to identify vulnerabilities and potential attack vectors.

Limitations of IDS

IDS has some limitations, including:

- IDS may generate false positives or false negatives, leading to unnecessary alerts or missed intrusions.
- IDS requires maintenance and updates to stay current with the latest attack signatures and IoCs.
- IDS may not detect new or unknown attack vectors.

Conclusion

- In conclusion, IDS is an important tool in network security that can detect and alert on intrusions, reducing the impact of an attack.
- Organizations must choose the right type of IDS, NIDS or HIDS, based on their network architecture and security needs.
- IDS has limitations, and organizations must implement complementary security measures, such as firewalls, access control, and endpoint security, to achieve a comprehensive security posture.

IDS Analysis Approaches

Introduction

- In this topic we will cover IDS analysis approaches and how they can be used to detect and respond to network intrusions.
- We will discuss the different types of IDS analysis approaches and how they work.

Types of IDS Analysis Approaches

There are three main types of IDS analysis approaches:

- Signature-based analysis
- Anomaly-based analysis
- Hybrid analysis

Signature-based Analysis

- Signature-based analysis compares network traffic against known attack signatures or patterns.
- IDS with signature-based analysis can identify known attacks with high accuracy but may miss new or unknown attacks.
- Signature-based analysis requires regular updates to stay current with new attack signatures.

Anomaly-based Analysis

- Anomaly-based analysis detects deviations from normal network traffic or user behavior.
- IDS with anomaly-based analysis can identify new or unknown attacks but may generate more false positives than signature-based analysis.
- Anomaly-based analysis requires a baseline of normal network traffic or user behavior to be established and updated regularly.

Hybrid Analysis

- Hybrid analysis combines signature-based and anomaly-based analysis to achieve a more comprehensive detection capability.
- IDS with hybrid analysis can identify known and unknown attacks with fewer false positives but require more resources to operate effectively.

IDS Analysis Approaches in Action

IDS analysis approaches can be applied to detect various types of network intrusions, including:

- Malware infections
- Unauthorized access attempts
- Data exfiltration
- Denial of service attacks

Conclusion

- In conclusion, IDS analysis approaches are essential for detecting and responding to network intrusions effectively.
- Organizations must choose the right type of IDS analysis approach based on their network architecture and security needs.
- IDS analysis approaches require regular maintenance, updates, and baseline establishment to operate effectively.

Host-Based IDS

Introduction

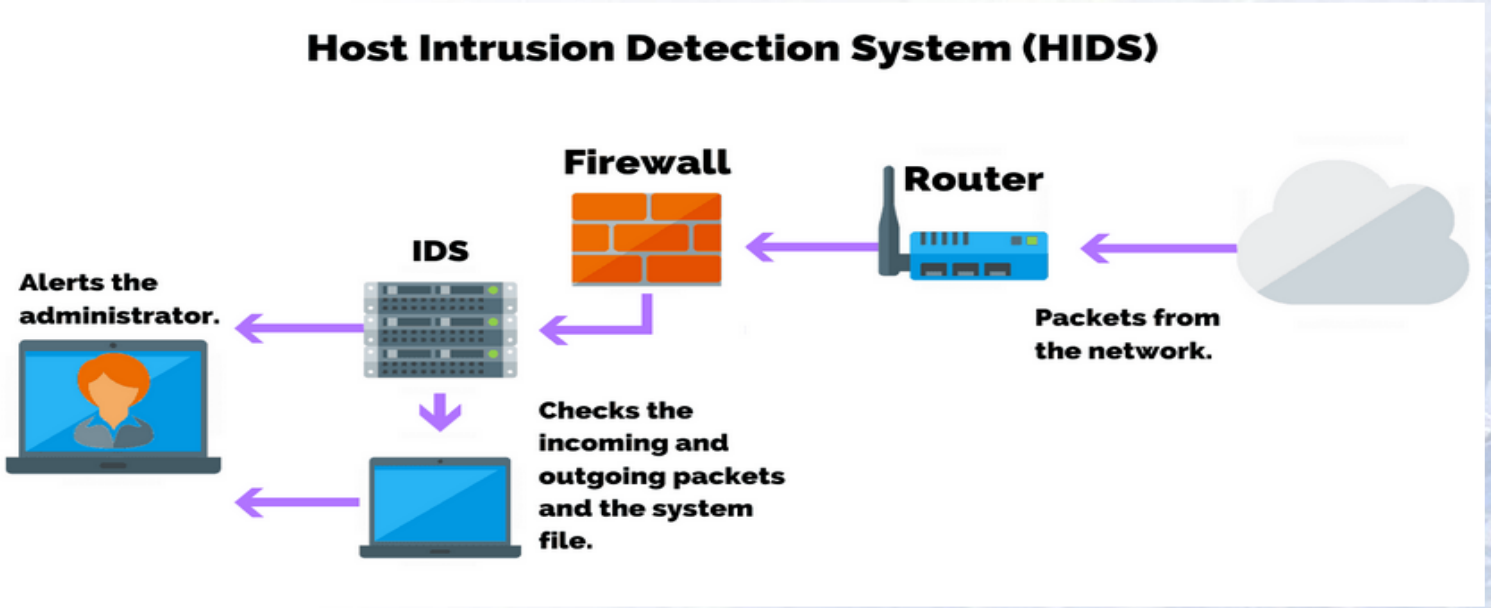
- In this topic we will cover Host-Based Intrusion Detection System (HIDS) and its importance in host-level security.
- We will discuss how HIDS works and its benefits and limitations.

What is HIDS?

- HIDS is an intrusion detection system that monitors activity on individual devices, such as servers or workstations, to detect unauthorized access or system-level attacks.
- HIDS can detect malicious activity that network-based IDS (NIDS) may not capture, such as file modifications or process-level attacks.

How HIDS Works?

- HIDS works by collecting and analyzing system activity logs, file integrity, and system performance metrics to identify suspicious activity.
- HIDS can detect unauthorized access attempts, malware infections, and other types of host-level attacks.
- HIDS alerts security teams or generates automated responses, such as terminating malicious processes or isolating affected devices.



Benefits of HIDS

HIDS provides several benefits, including:

- Granular visibility into host-level activity, allowing for faster incident response and reducing the impact of an attack.
- Detecting threats that may evade NIDS, such as fileless malware or process-level attacks.
- Enhancing compliance by monitoring and reporting on system-level activity.

Limitations of HIDS

HIDS has some limitations, including:

- HIDS can generate a high number of alerts, leading to alert fatigue and missed intrusions.
- HIDS requires maintenance and updates to stay current with the latest attack patterns and IoCs.
- HIDS may not detect sophisticated or zero-day attacks.

HIDS Deployment

HIDS can be deployed in several ways, including:

- **Agent-based:** HIDS agent installed on each monitored device.
- **Agentless:** HIDS uses system logs and network packets for analysis.
- **Hybrid:** HIDS uses a combination of agent-based and agentless approaches.

Conclusion

- In conclusion, HIDS is an essential tool in host-level security that can detect and alert on intrusions, reducing the impact of an attack.
- Organizations must choose the right type of HIDS deployment based on their network architecture and security needs.
- HIDS has limitations, and organizations must implement complementary security measures, such as firewalls, access control, and endpoint security, to achieve a comprehensive security posture.

Network-Based IDS

Introduction

- Network-based Intrusion Detection Systems (NIDS) are security tools that monitor and analyze network traffic to detect suspicious activity or malicious attacks.
- NIDS is one of the most important security measures in modern-day networks.
- NIDS provides a higher level of security by detecting and alerting the network administrator of potential threats.

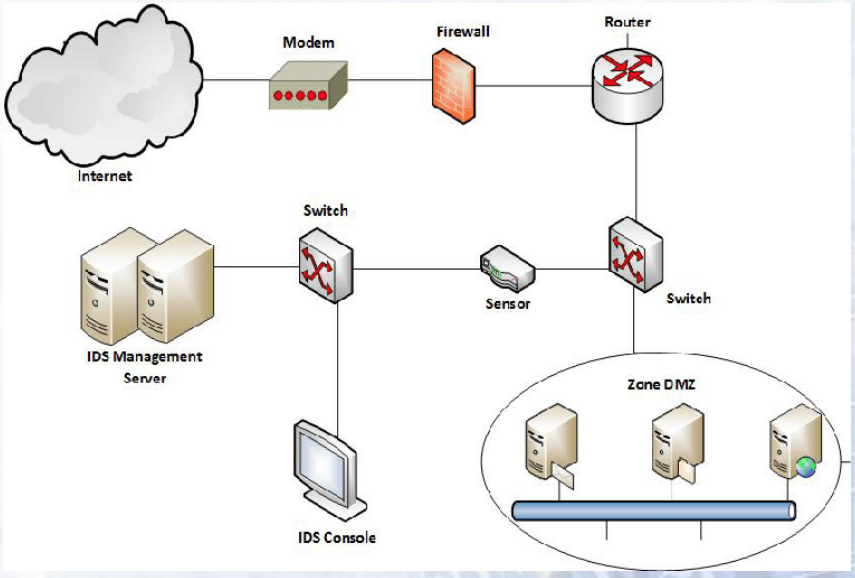
Types of NIDS

- **Signature-based NIDS**: Uses a pre-defined database of known attack patterns, and alerts when a network packet matches a signature in the database.
- **Anomaly-based NIDS**: Analyzes the network traffic for abnormal behavior or traffic patterns, and alerts the administrator when such activity is detected.
- **Hybrid NIDS**: Combines both signature-based and anomaly-based detection methods to provide a more comprehensive approach to intrusion detection.

NIDS Architecture

NIDS architecture includes the following components:

- **Network Taps:** Collect and route network traffic to the NIDS for analysis.
- **Sensors:** Monitor network traffic and analyze packets for malicious activity.
- **Console:** Provides the interface for administrators to configure and manage the NIDS, and review alerts and logs.



NIDS Deployment

NIDS can be deployed in two ways: passive or active.

- **Passive deployment**: Does not alter the network traffic or packets, and only analyzes network traffic.
- **Active deployment**: Alters network traffic or packets, such as dropping or modifying packets, to prevent malicious activity.

Advantages of NIDS

- Provides real-time monitoring of network traffic.
- Detects and alerts the administrator of potential threats, allowing for timely action to be taken.
- Can be deployed on a variety of network architectures and sizes.
- Can be configured to monitor specific types of traffic, such as web traffic or email traffic.

Disadvantages of NIDS

- **False positives**: Alerts generated by NIDS may not always indicate a genuine threat, which can lead to unnecessary investigations.
- **Limited visibility**: NIDS can only monitor network traffic, and may not be able to detect attacks on endpoints or applications.
- **Performance impact**: NIDS can impact network performance, especially if the network traffic is high.

Conclusion

- NIDS is an important tool for network security, providing real-time monitoring and alerting of potential threats.
- NIDS architecture includes sensors, network taps, and a console for management and configuration.
- NIDS can be deployed passively or actively, with advantages and disadvantages for each deployment method.

WIPS - Wireless IPS

Introduction

- Wireless Intrusion Prevention Systems (WIPS) are security tools that detect and prevent unauthorized access to wireless networks.
- WIPS is a crucial security measure for modern-day wireless networks.
- WIPS provides a higher level of security by detecting and preventing potential threats to wireless networks.

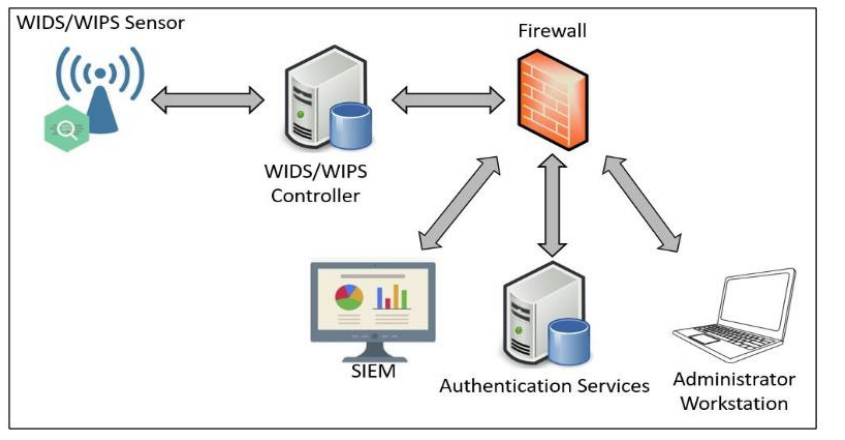
Types of WIPS

- **Overlay WIPS:** A separate wireless sensor network is deployed to monitor and secure the wireless network.
- **Integrated WIPS:** The WIPS functionality is integrated into the wireless access points (APs) themselves.

WIPS Architecture

WIPS architecture includes the following components:

- **Access Points:** Provide wireless connectivity to devices and also monitor for suspicious activity.
- **Sensors:** Detect wireless attacks or suspicious behavior and notify the access points to take appropriate action.
- **Management Console:** Provides the interface for administrators to configure and manage the WIPS, and review alerts and logs.



WIPS Deployment

- WIPS can be deployed in two ways: standalone or integrated.
- Standalone deployment: A separate sensor network is deployed to monitor wireless traffic and detect attacks.
- Integrated deployment: WIPS functionality is integrated into wireless APs themselves, reducing the need for additional hardware.

Advantages of WIPS

- Provides real-time monitoring of wireless traffic.
- Detects and prevents potential threats to the wireless network, including rogue APs and unauthorized access attempts.
- Can be configured to monitor and protect specific types of wireless traffic, such as voice or data.
- Supports compliance with regulatory requirements, such as PCI-DSS.

Disadvantages of WIPS

- **False positives**: Alerts generated by WIPS may not always indicate a genuine threat, which can lead to unnecessary investigations.
- **Limited visibility**: WIPS can only monitor wireless traffic, and may not be able to detect attacks on wired networks or applications.
- **Performance impact**: WIPS can impact wireless performance, especially if the wireless network traffic is high.

Conclusion

- WIPS is a crucial tool for wireless network security, providing real-time monitoring and prevention of potential threats.
- WIPS architecture includes access points, sensors, and a management console for configuration and management.
- WIPS can be deployed standalone or integrated, with advantages and disadvantages for each deployment method.

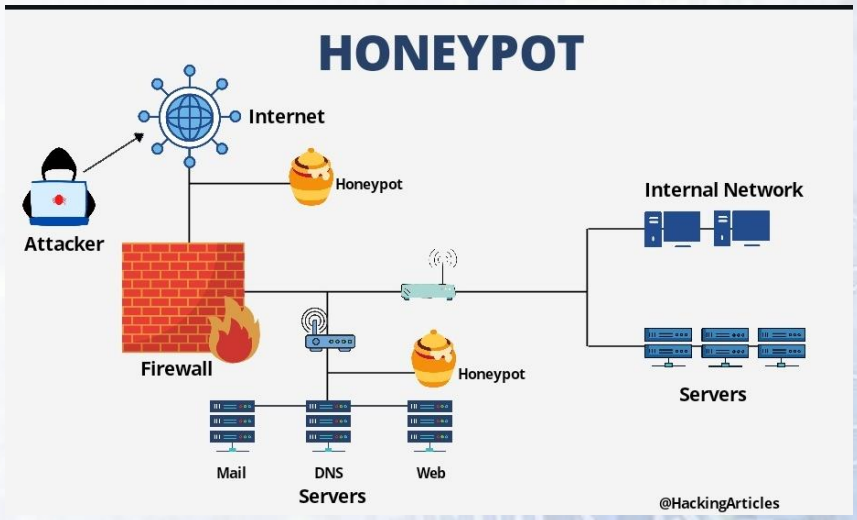
Honeypots

Introduction

- Honeypots are a type of security tool that simulate vulnerable systems or applications to attract attackers and gather information about their techniques and motives.
- Honeypots are a crucial tool for modern-day cybersecurity.
- Honeypots can provide valuable insights into attacker behavior and help improve overall security posture.

Types of Honeypots

- **Production honeypots:** Real systems or applications that are deployed to gather information about attackers.
- **Research honeypots:** Simulated systems or applications that are deployed in a controlled environment to gather research data about attacker behavior.



Advantages of Honeypots

- Provides early warning of potential attacks, allowing for quick detection and response.
- Can gather valuable intelligence about attacker techniques, tactics, and motives.
- Helps identify vulnerabilities in systems or applications that can be remediated to improve overall security posture.
- Can divert attackers away from real systems and applications, reducing the risk of successful attacks.

Disadvantages of Honeypots

- **False positives**: Honeypots can generate false alarms, which can lead to unnecessary investigations and waste of resources.
- **Security risks**: Honeypots can be compromised by attackers, potentially exposing sensitive information or systems.
- **Maintenance overhead**: Honeypots require regular maintenance and updates, which can be resource-intensive.

Honeypot Deployment Strategies

- **Low interaction honeypots**: Simulate only the most basic functionality of a system or application, providing limited interaction with attackers.
- **Medium interaction honeypots**: Simulate more functionality of a system or application, allowing attackers to interact with them more fully.
- **High interaction honeypots**: Provide a full simulation of a real system or application, allowing attackers to interact with it as if it were real.

Honeypot Tools

Examples of honeypot tools include:

- **KFSensor:** A Windows-based honeypot that simulates vulnerable services and applications.
- **Honeyd:** A customizable honeypot that can simulate multiple operating systems and services.
- **Cowrie:** A high-interaction honeypot that simulates a full SSH environment.

Conclusion

- Honeypots are a crucial tool for modern-day cybersecurity, providing valuable insights into attacker behavior and improving overall security posture.
- Honeypots can be deployed in different ways, with advantages and disadvantages for each deployment strategy.
- Honeypot tools, such as KFSensor, Honeyd, and Cowrie, are available as open-source solutions or as part of commercial cybersecurity solutions.

Vulnerability Mangement & Assessment

Vulnerability Mangement & Assessment

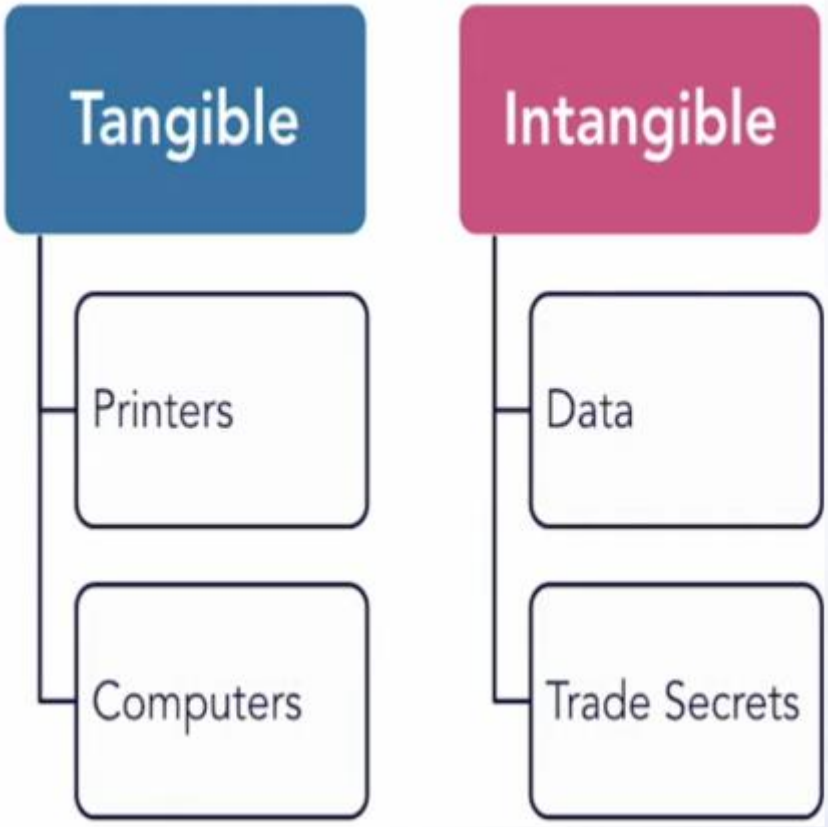
- **Vulnerability assessment:**
- is the process of identifying and evaluating security vulnerabilities in a system or network.
- involves running scans and tests to discover vulnerabilities
- analyzing the results to determine the severity and potential impact of each vulnerability.

- **Vulnerability management:**
- process of addressing and mitigating vulnerabilities that have been identified through the vulnerability assessment.
- includes prioritizing vulnerabilities based on severity and potential impact, developing a plan to address them, and implementing the necessary fixes or patches.
- remediated through patching and configuration of security settings.

Terms



Assets


Tangible
Printers
Computers
Intangible
Data
Trade Secrets

RISK

- Risk refers to the potential harm or damage that can be caused by a cyber attack or security breach.
- Includes bussiness disruption, financial loss.

Threat

- Anything that can exploit a vulnerability
- obtain , damge or destroy an asset

What is a vulnerability ?

- **vulnerability**

refers to a weakness or flaw in a system, application, or network

exploited by attackers to gain unauthorized access, steal data, disrupt operations

Vulnerabilities can be caused by software bugs, configuration errors, design flaws, or unpatched systems that leave systems exposed to potential attacks.

Examples of common vulnerabilities:

- Weak or easily guessable passwords
- Unpatched software vulnerabilities
- Misconfigured settings
- Malware infections

- A vulnerability assessment uses automated network security scanning tools.

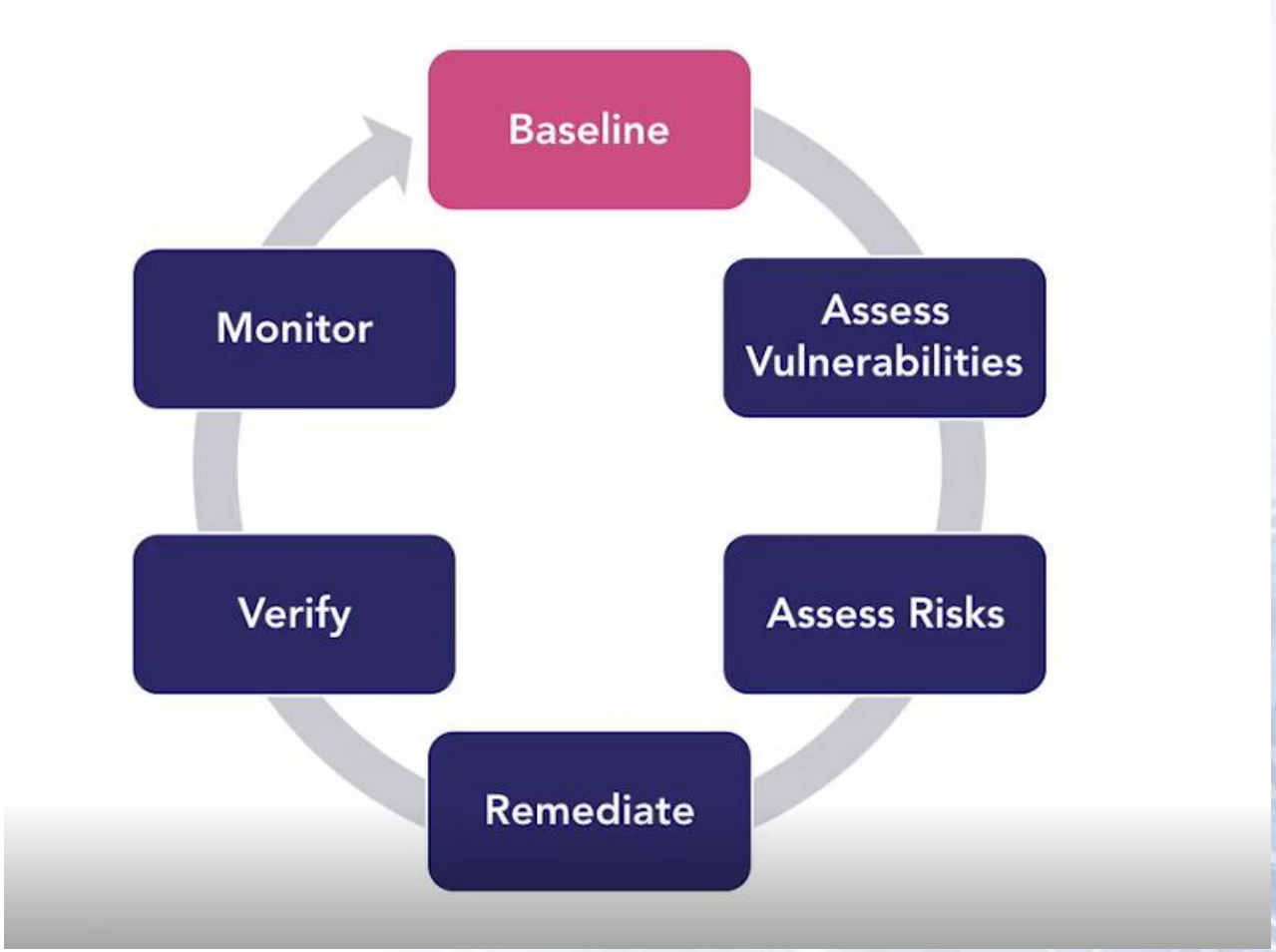
- Common vulnerability scanners ?
  - OpenVAS
  - Nessus
  - Qualys
  - Rapid7
  - Nmap

END

Vulnerability management life cycle

- **Threats exist, as well as vulnerabilities.**
- **You can’t control the threats.**
- **You can reduce the vulnerabilities**

Vulnerability management life cycle

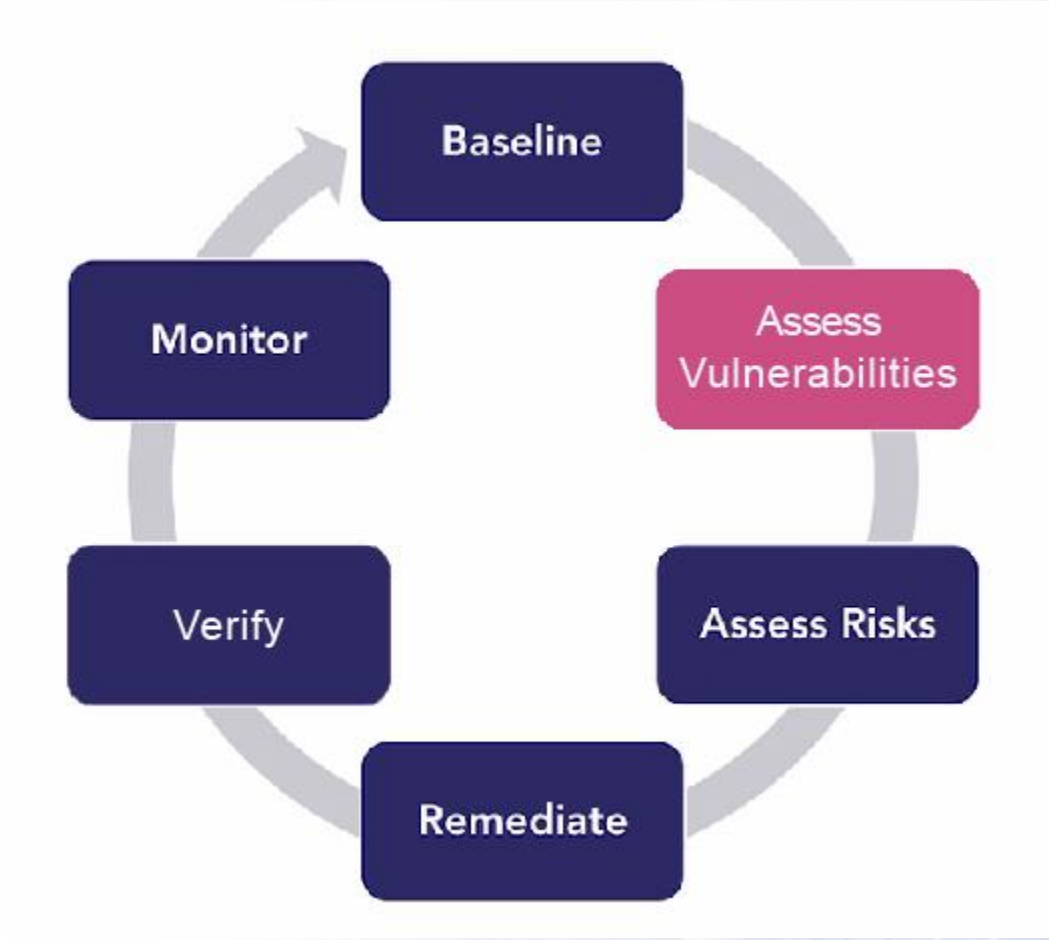


Vulnerability management life cycle

Initial Assessment:

- **Identify assets, define risk and possible business impact**
- **Helps answer the question: "Why are we doing this?"**
- **Understanding the overall impact of a cyber attack will inspire everyone to be more vested in mitigating vulnerabilities**

Vulnerability management life cycle

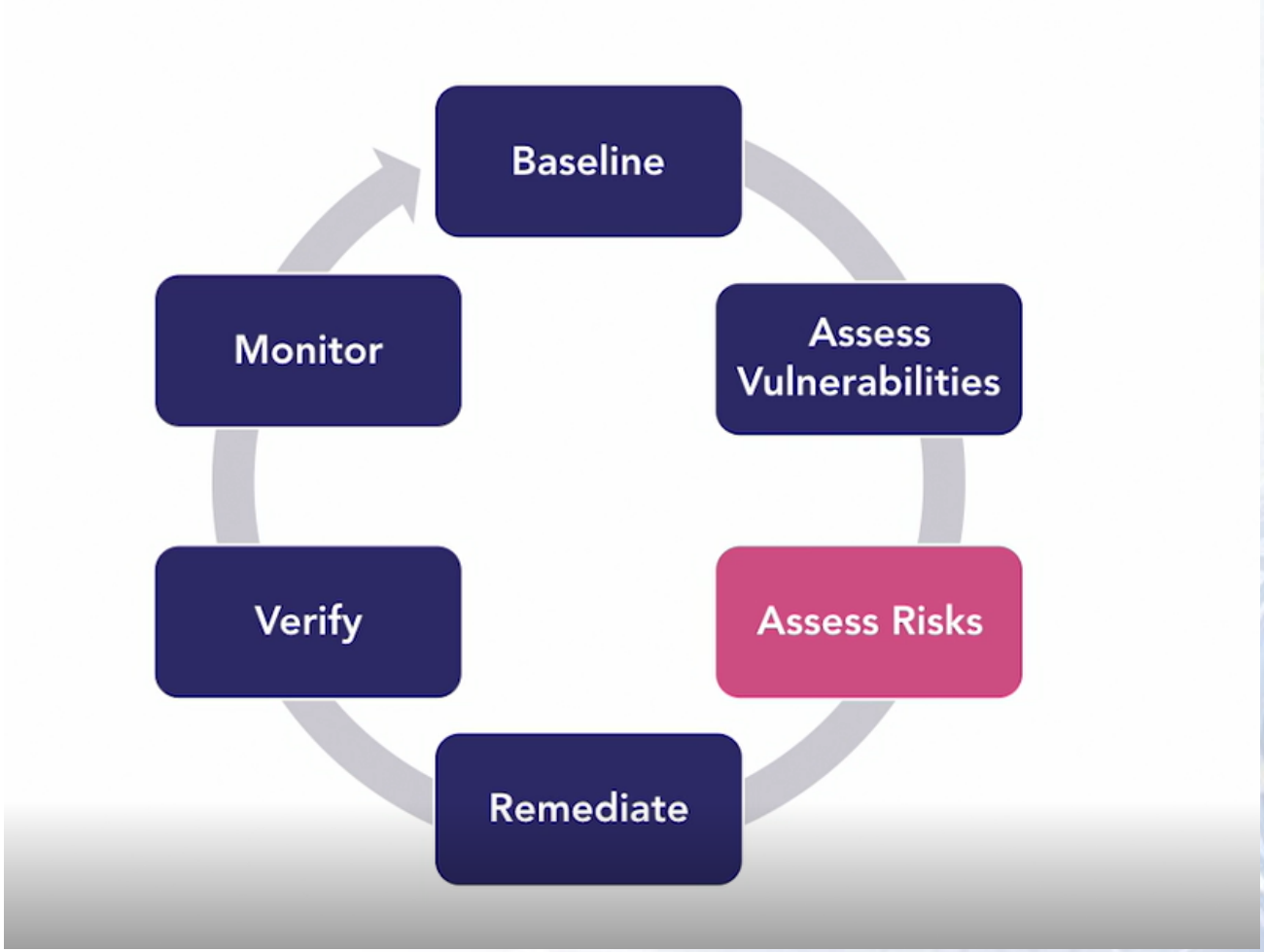


Vulnerability management life cycle

- **Plan:**

- **Check for compliance requirements**
- **Determine the best time to perform the scan**
- **Decide on what tools to use**
  -Port Scan, network scans, or web application scans
- **Run the automated scan**
- **Generate report**

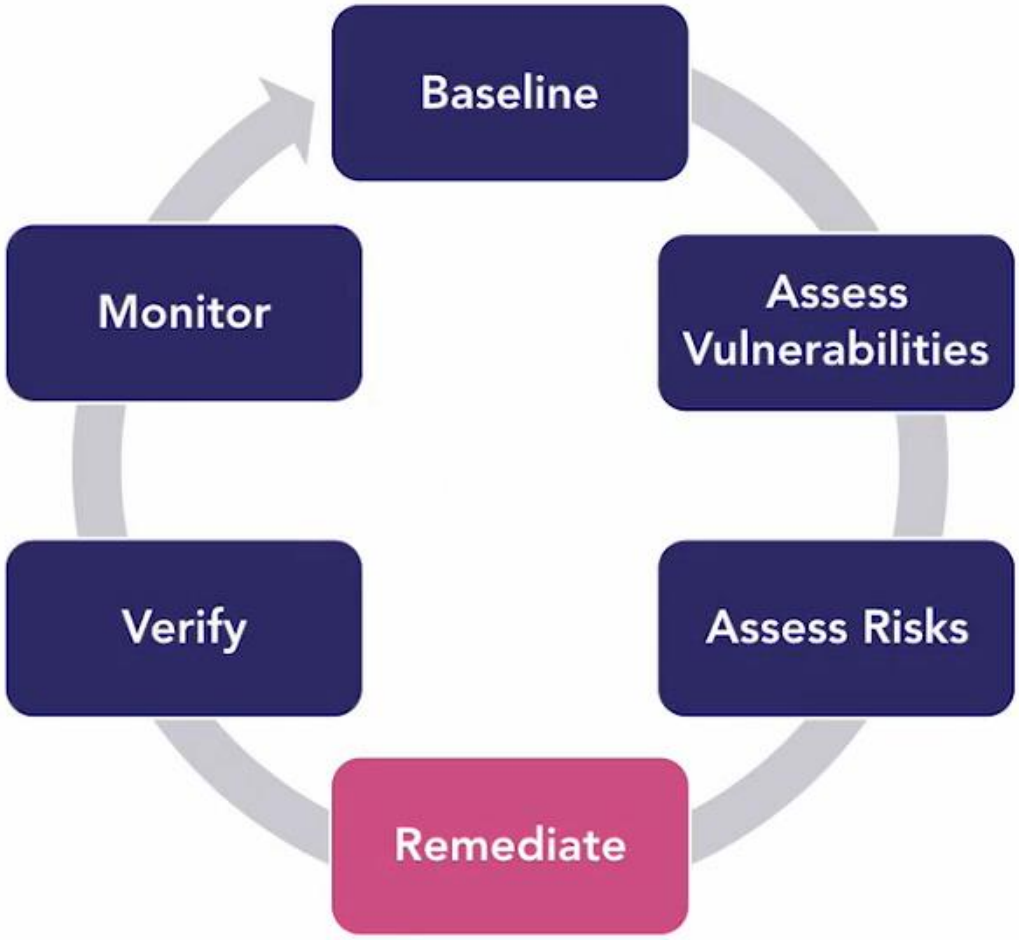
Vulnerability management life cycle



Vulnerability management life cycle

- **Detailed description, discovery date ,what was affected**
  - OS, application, network, or mobile device
- **Common Vulnerabilities and exposures(CVE) score**
- **Prioritize according to the risk level**
- **Determine a time to reassess the vulnerability**

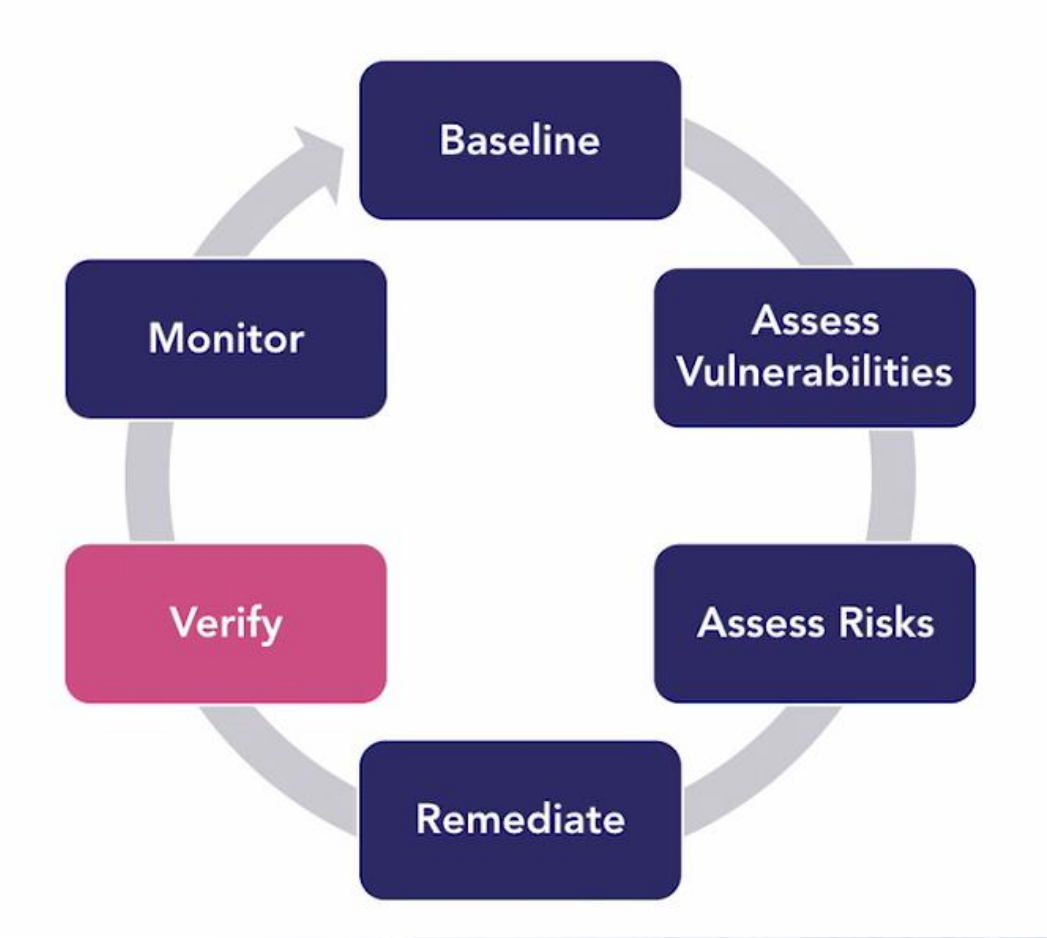
Vulnerability management life cycle



Vulnerability management life cycle

- Remediate
- Take steps to correct system integrity
- Research the best way to mitigate the vulnerability
  - Research vulnerabilities
  - Evaluate fixes and remediation method
  - Test the patches and fixes
  - Apply patches/fixes
  - Monitor results

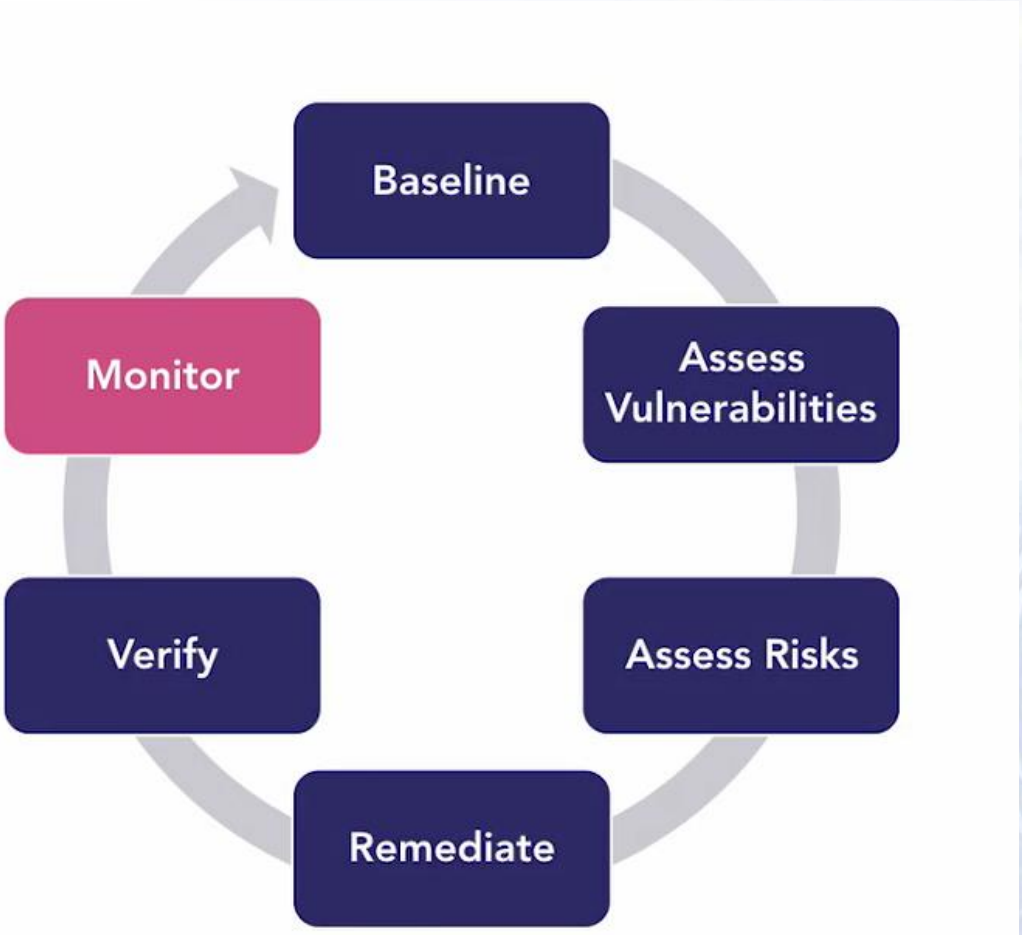
Vulnerability management life cycle



Vulnerability management life cycle

- **Retest and verify:**
- Retest and verify that you successfully corrected the problem
- This involves rescanning the system and comparing the results

Vulnerability management life cycle



Vulnerability management life cycle

- Vulnerability management life cycle
  A continuous best practice process to protect your organization and data

Why Is A VM Program Required ?

- What is a patch ?

  "A **patch** is a piece of software designed to update a computer program or its supporting data, to fix or improve it. This includes fixing **security** vulnerabilities and other bugs"

https://en.wikipedia.org/wiki/Patch_(computing)

Why Is A VM Program Required ?

- What is patch management ?

  Patch management is an area of systems management that involves acquiring, testing, and installing multiple patches (code changes) to an administered computer system.

http://searchenterprisedesktop.techtarget.com/definition/patch-management

Why Is A VM Program Required ?

- Patch management tasks :

  Maintaining current knowledge of available patches, deciding what patches are appropriate for particular systems, ensuring that patches are installed.

http://searchenterprisedesktop.techtarget.com/definition/patch-management

Why Is A VM Program Required ?

- Patch management tasks:

  properly, testing systems after installation, and documenting all associated procedures, such as specific configs required.

http://searchenterprisedesktop.techtarget.com/definition/patch-management

Why Is A VM Program Required ?

Risk of not patching:

- By not applying a patch you might be leaving the door open for a malware attack

Why Is A VM Program Required ?

- Risk of not patching:
- Defects in clients like web browsers, email programs, image viewers, instant messaging software, and media players may allow malicious websites, etc. to infect or compromise your computer.

Why Is A VM Program Required ?

A VM program addresses timely management of patching to ensure that vulnerabilities are not present for hackers to exploit.

END

What Is An Exploit ?

- What is an exploit ?
  - Program or some code that takes advantage of a security hole (i.e. a vulnerability) in an application or system, so that an attacker can use it for their benefit.

https://www.welivesecurity.com/2015/02/27/exploits-work/

What Is An Exploit ?

- Remote exploit:

  A *remote exploit* works over a network and exploits the security vulnerability without any prior access to the vulnerable system.

  For example, an attacker compromises a web server on a corporate network, the attacker can then use the compromised web server to attack other systems on the network

https://en.wikipedia.org/wiki/Exploit_(computer_security)

What Is An Exploit ?

- Local exploit:

  A *local exploit* requires prior access to the vulnerable system and usually increases the privileges of the person running the exploit past those granted by the system administrator.

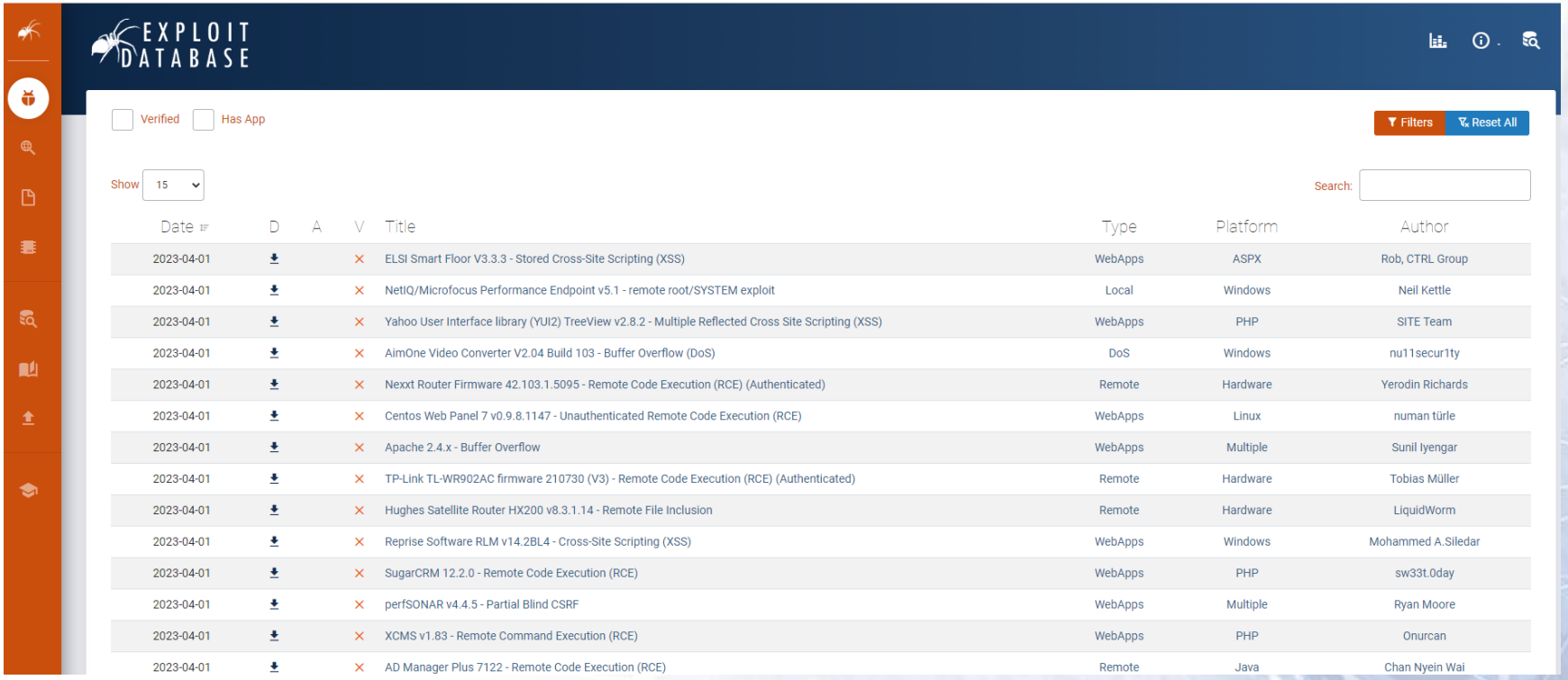
https://en.wikipedia.org/wiki/Exploit_(computer_security)

What Is An Exploit ?

- Exploit database:
  - The Exploit Database is a CVE compliant archive of public exploits and corresponding vulnerable software, developed for use by penetration testers and vulnerability researchers.

https://www.exploit-db.com/about/

What Is An Exploit ?



Date	D	A	V	Title	Type	Platform	Author
2023-04-01				ELSI Smart Floor V3.3.3 - Stored Cross-Site Scripting (XSS)	WebApps	ASPX	Rob, CTRL Group
2023-04-01				NetIQ/Microfocus Performance Endpoint v5.1 - remote root/SYSTEM exploit	Local	Windows	Neil Kettle
2023-04-01				Yahoo User Interface library (YUI2) TreeView v2.8.2 - Multiple Reflected Cross Site Scripting (XSS)	WebApps	PHP	SITE Team
2023-04-01				AimOne Video Converter V2.04 Build 103 - Buffer Overflow (DoS)	DoS	Windows	nu11secur1ty
2023-04-01				Nexxt Router Firmware 42.103.1.5095 - Remote Code Execution (RCE) (Authenticated)	Remote	Hardware	Yerodin Richards
2023-04-01				Centos Web Panel 7 v0.9.8.1147 - Unauthenticated Remote Code Execution (RCE)	WebApps	Linux	numan türle
2023-04-01				Apache 2.4.x - Buffer Overflow	WebApps	Multiple	Sunil Iyengar
2023-04-01				TP-Link TL-WR902AC firmware 210730 (V3) - Remote Code Execution (RCE) (Authenticated)	Remote	Hardware	Tobias Müller
2023-04-01				Hughes Satellite Router HX200 v8.3.1.14 - Remote File Inclusion	Remote	Hardware	LiquidWorm
2023-04-01				Reprise Software RLM v14.2BL4 - Cross-Site Scripting (XSS)	WebApps	Windows	Mohammed A.Siledar
2023-04-01				SugarCRM 12.2.0 - Remote Code Execution (RCE)	WebApps	PHP	sw33t.0day
2023-04-01				perfSONAR v4.4.5 - Partial Blind CSRF	WebApps	Multiple	Ryan Moore
2023-04-01				XCMS v1.83 - Remote Command Execution (RCE)	WebApps	PHP	Onurcan
2023-04-01				AD Manager Plus 7122 - Remote Code Execution (RCE)	Remote	Java	Chan Nyein Wai

https://www.exploit-db.com/

What Is An Exploit ?

- Zero-day exploit:

A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix

Security Breach Case Study 1: Home Dept 2014

- 56 million payment cards compromised
- Early September 2014

Security Breach Case Study 1: Home Dept 2014

- Sequence of events:
  - The attackers were able to gain access to one of Home Depot's vendor environments by using a third-party vendor's login credentials

Security Breach Case Study 1: Home Dept 2014

- Sequence of events:
  - Then they exploited a zero-day vulnerability in Windows, which allowed them to rotate from the vendor-specific environment to the Home Depot corporate environment.

Security Breach Case Study 1: Home Dept 2014

- Sequence of events:
  - Once they were in the Home Depot network, they were able install memory scraping malware on over 7,500 self-checkout POS terminals (Smith, 2014).

Security Breach Case Study 1: Home Dept 2014

- Sequence of events:
  - This malware was able to grab 56 million credit and debit cards. The malware was also able to capture 53 million email addresses (Winter, 2014).

Security Breach Case Study 1: Home Dept 2014

- Sequence of events:
  - The stolen payment cards were used to put up for sale and bought by carders. The stolen email addresses were helpful in putting together large phishing campaigns.

https://www.sans.org/reading-room/whitepapers/breaches/case-study-home-depot-data-breach-36367

Security Breach Case Study 1: Home Dept 2014

- Home Depot didn't have secure configuration of the software or hardware on the POS terminals.
- There was no proof of regularly scheduled vulnerability scanning of the POS environment.

https://www.sans.org/reading-room/whitepapers/breaches/case-study-home-depot-data-breach-36367

Security Breach Case Study 1: Home Dept 2014

- They didn't have proper network separation between the Home Depot corporate network and the POS network.

https://www.sans.org/reading-room/whitepapers/breaches/case-study-home-depot-data-breach-36367

Security Breach Case Study 1: Home Dept 2014

- Overall:

Several controls missing, vendor management of IDs and access management missing, and monitoring of the network was missing

END

Security Breach Case Study 2: Anthem

- Health Insurer Anthem
- Affected 78.8 million individuals

http://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627

Security Breach Case Study 2: Anthem

- Sequence of events:
  - Data breach began on Feb. 18, 2014, when a user within one of Anthem's subsidiaries opened a phishing email containing malicious content

http://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627

Security Breach Case Study 2: Anthem

- Sequence of events:

– Opening the email launched the download of malicious files to the user's computer and allowed hackers to gain remote access to that computer and dozens of other systems within the Anthem enterprise, including Anthem's data warehouse

http://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627

Security Breach Case Study 2: Anthem

- Sequence of events:
  - Starting with the initial remote access, the attacker was able to move laterally across Anthem systems and escalate privileges, gaining increasingly greater ability to access information and make changes in the environment

Security Breach Case Study 2: Anthem

- Sequence of events:
  - The attacker utilized at least 50 accounts and compromised at least 90 systems within the Anthem enterprise environment including, eventually, the company's enterprise data warehouse -

Security Breach Case Study 2: Anthem

- Sequence of events:
  - a system that stores a large amount of consumer personally identifiable information
  - Queries to that data warehouse resulted in access to an exfiltration of approximately 78.8 m unique user records

Security Breach Case Study 2: Anthem

- Vulnerabilities:
  - Exploitable vulnerabilities were found in anthem network
  - User security awareness training conducted to prevent phishing and social engineering

http://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627

Security Breach Case Study 2: Anthem

- Remediation measures:
  - Implemented two-factor authentication on all remote access tools, deployed a privileged account management solution and added enhanced logging resources to its security event and incident management solutions

Security Breach Case Study 2: Anthem

- Remediation measures:
  - Further, the company conducted a complete reset of passwords for all privileged users, suspended all remote access pending implementation of two-factor authentication and created new Network Admin IDs

END

VM Challenges & Pitfalls

- Challenges:
  - Internal expertise on VM tool
  - Not enough support from IT teams
  - Vulnerability patching causing application failure
  - Management support

VM Challenges & Pitfalls

- Internal expertise on VM tool
  - Not too much expertise required
  - Monitor traffic pattern
  - Train staff if possible
  - Patch small portions of the network first

VM Challenges & Pitfalls

- Not enough support from IT teams:
  - Create reports and share among IT management
  - Highlight and educate risks to IT management and board

VM Challenges & Pitfalls

- Patching causing application failure:
  - In test environment create work around or compensating controls
  - Test the compensating controls
  - Document the compensating controls

VM Challenges & Pitfalls

- Not enough management support:
  - Share reports with management highlighting recent incidents
  - Share industry-specific or geographically relevant breach reports
  - Create awareness

Vulnerability scanners

- Vulnerability scanners are automated tools used to identify, assess, and report security vulnerabilities

Test for vulnerabilties

- Vulnerabilties or weakness exist in many different places:

software, operating systems,networks and even people

- There are many choices today for assessment tools
- Some are free, some online and some are subscription-based

Types of vulnerability scanners

- There are two types of vulnerability scanners
- Network-based scanners: These scanners scan an organization's network to identify vulnerabilities in network devices such as routers, switches, and firewalls.

- Host-based scanners: These scanners are installed on individual systems or servers to identify vulnerabilities in the underlying operating system, applications, and services.

vulnerability scanners

Provide comprehensive view of their potential attack surface

- identify vulnerabilities
- Prioritize remediation efforts
- Improve security posture
- Save time and resources

Vulnerbailtuy scanners examples

OpenVAS

HACKER TARGET

SCANNERS TOOLS RESEARCH SERVICES ABOUT PRICING LOG IN

The OpenVAS scanner is a comprehensive vulnerability assessment system that can detect security issues in all manner of servers and network devices. Use this hosted version of the OpenVAS software to effortlessly test your Internet infrastructure.

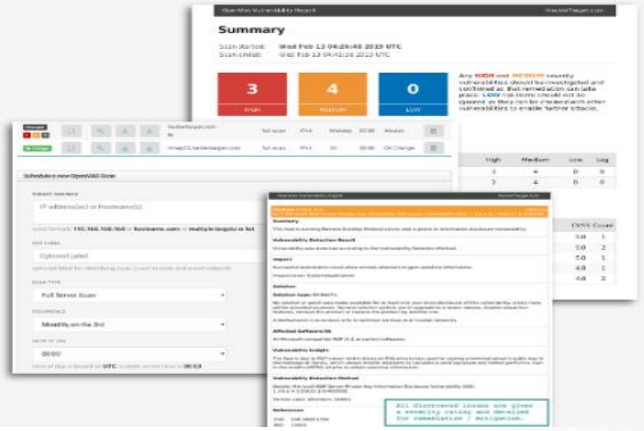
Results are delivered to your email address for analysis, allowing you to start re-mediating any risks your systems face from external threats.

Sample Reports

Launch OpenVAS Vulnerability Scan

Login for access to OpenVAS Vulnerability Scanning

Detect vulnerabilities in servers, networks and web sites



MEMBERSHIP BENEFITS

- Find **security vulnerabilities** in any Internet facing system
- **Detailed reporting** for risk assessment and re-mediation
- **Vulnerability Alerts** on detected change in scheduled report
- **Custom scan options;** Network/Server, Web, WordPress and Joomla Scans
- Access to **27 Vulnerability Scanners** and **OSINT** Tools
- **Trusted** Open Source Tools

VIEW PLANS USE CASES

https://www.greenbone.net/en/testnow/

Vega helps you find and fix cross-site scripting (XSS), SQL injection, and more.

Vega is a free and open source web security scanner and web security testing platform to test the security of web applications. Vega can help you find and validate SQL Injection, Cross-Site Scripting (XSS), inadvertently disclosed sensitive information, and other vulnerabilities. It is written in Java, GUI based, and runs on Linux, OS X, and Windows.

Vega can help you find vulnerabilities such as: reflected cross-site scripting, stored cross-site scripting, blind SQL injection, remote file include, shell injection, and others. Vega also probes for TLS / SSL security settings and identifies opportunities for improving the security of your TLS servers.

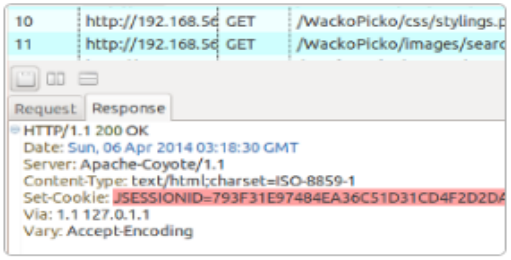
Vega includes an automated scanner for quick tests and an intercepting proxy for tactical inspection. The Vega scanner finds XSS (cross-site scripting), SQL injection, and other vulnerabilities. Vega can be extended using a powerful API in the language of the web: Javascript.

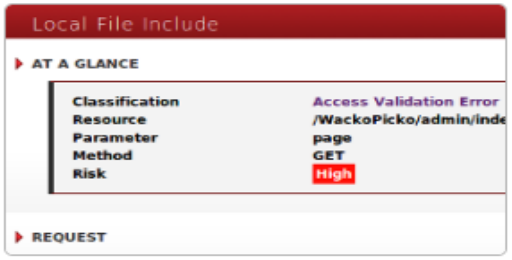
Vega was developed by Subgraph in Montreal.

DOWNLOAD

Automated, Manual, and Hybrid Security Testing







Automated Scanner

Vega includes a website crawler powering its automated scanner. Vega can automatically log into websites when supplied with user credentials.

Intercepting Proxy

Vega can be used to observe and interact with communication between clients and servers, and will perform SSL interception for HTTP websites.

Proxy Scanner

The Vega proxy can also be configured to run attack modules while the user is browsing the target site through it. This allows for semi-automated, user-driven security testing to ensure maximum

Summary

This document reports on the results of an automatic security scan. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

It only lists hosts that produced issues.

All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC".

Scan started: **Mon Dec 7 12:51:47 2015 UTC**
Scan ended:
Task: testasp.vulnweb.com

Vulnerability Summary

HIGH	MEDIUM	LOW
2	8	0

Any **HIGH** and **MEDIUM** risk vulnerabilities should be investigated and confirmed so that remediation can take place. **LOW** risk items should not be ignored as they can be stepping stones to High risk attacks.

Host Summary

Host	Start	End	High	Medium	Low	Log	False Positive
87.230.29.167	Dec 7, 12:51:52	(not finished)	2	8	0	23	0
Total: 1			2	8	0	23	0

Results per Host

Host 87.230.29.167

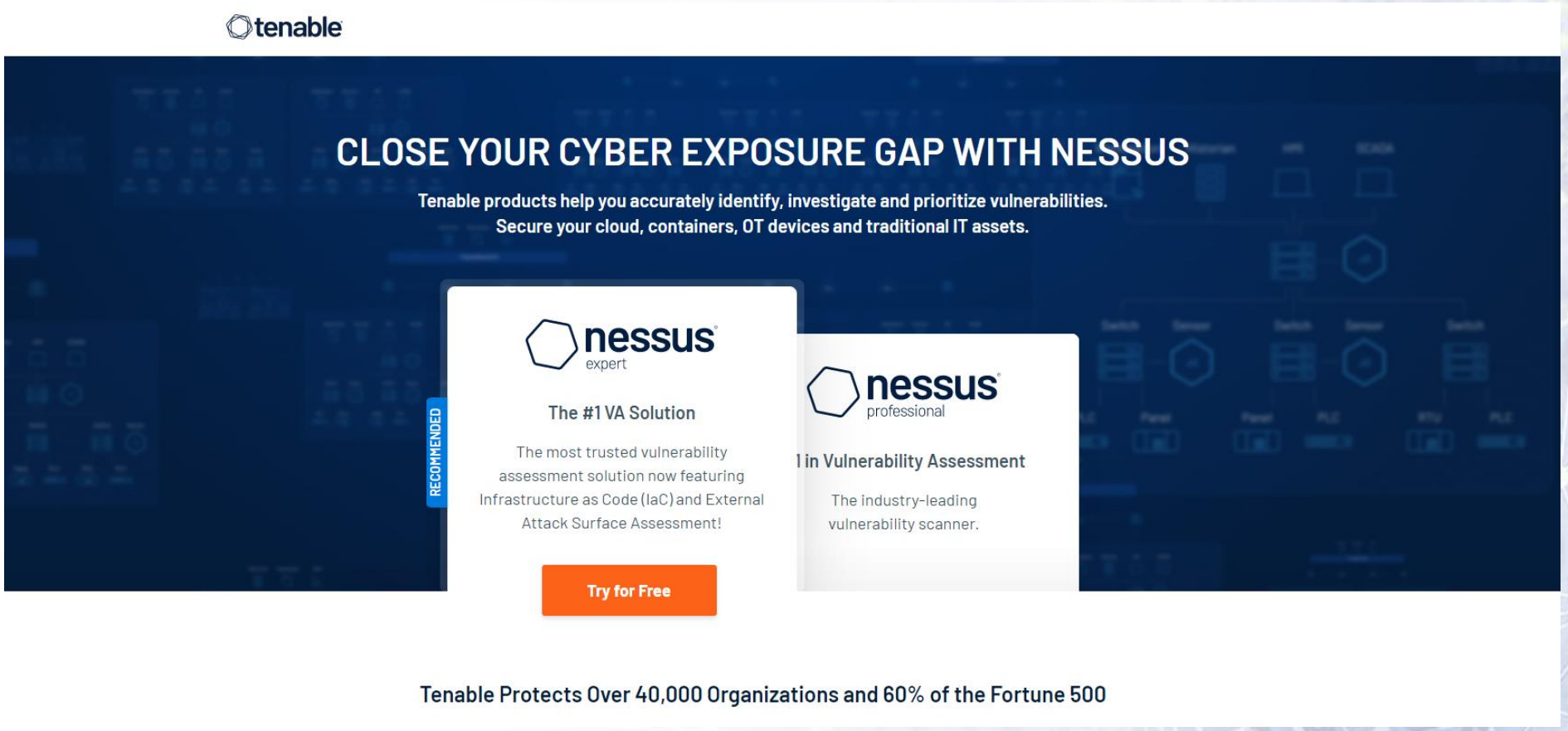
Scanning of this host started at: Mon Dec 7 12:51:52 2015 UTC
Number of results: 33

Port Summary for Host 87.230.29.167

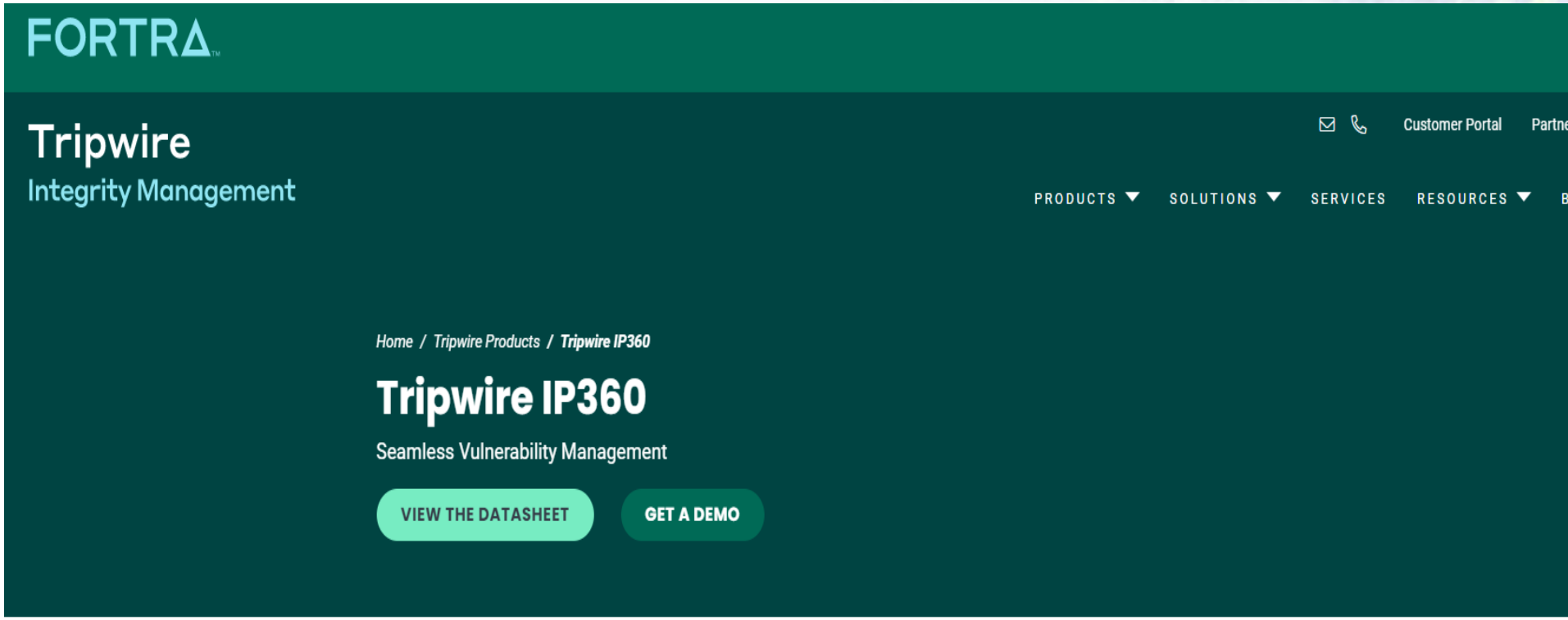
Service (Port)	Threat Level
80/tcp	High
139/tcp	Log
3389/tcp	Medium

https://hackertarget.com/sample-vulnerability-report/sample-openvas-report.pdf

https://hackertarget.com/sample-vulnerability-report/metasploitable-2.0-openvas.pdf


tenable
CLOSE YOUR CYBER EXPOSURE GAP WITH NESSUS
Tenable products help you accurately identify, investigate and prioritize vulnerabilities.
Secure your cloud, containers, OT devices and traditional IT assets.
RECOMMENDED
nessus expert
The #1 VA Solution
The most trusted vulnerability assessment solution now featuring Infrastructure as Code (IaC) and External Attack Surface Assessment!
Try for Free
nessus professional
l in Vulnerability Assessment
The industry-leading vulnerability scanner.
Tenable Protects Over 40,000 Organizations and 60% of the Fortune 500

Tripwire



Nobody needs more unnecessary alerts. Ready for prioritized risk scoring that focuses on what really matters?

Major Banking Institution Case Study

This multinational banking institution has been around for over 100 years, dedicated to helping a customer base of over 20 million people in countries all over the world.

In order to serve such a large customer base and keep financial services at competitive rates, they've taken advantage of the latest in cloud technology to reduce the operating costs of their IT infrastructure and outward-facing services—from online banking apps to mortgage calculators. In doing so, they've migrated many of these customer-facing services to operate in all of the major cloud platforms, including Microsoft Azure, Google Cloud and soon Amazon Web Services. It's a challenge for organizations adopting cloud infrastructure to properly secure those environments due to the elasticity and short lifespan of servers, as well as the ever-growing presence of containers.

INDUSTRY: Banking and Financial Services

HEADCOUNT: 90,000

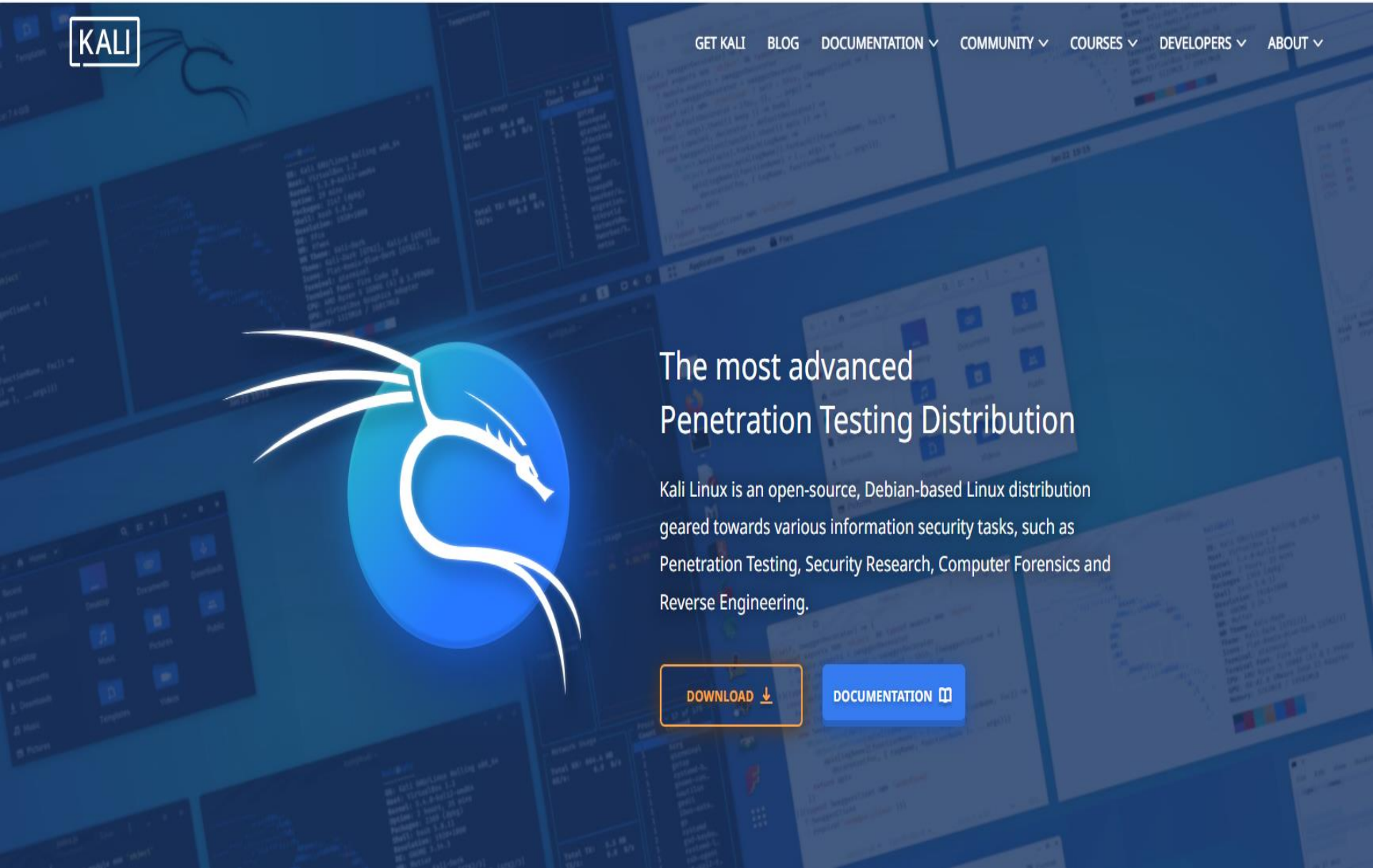
CUSTOMER SINCE: 2000

SOLUTIONS:

- Tripwire Enterprise
- Tripwire IP360

> Over the past 18 years, this multinational bank has kept their trust in Tripwire. They've relied on our promises to deliver the solutions that protect both their enterprise and the millions of customers that drive their success.

KALI Linux


KALI
GET KALI
BLOG
DOCUMENTATION
COMMUNITY
COURSES
DEVELOPERS
ABOUT
The most advanced
Penetration Testing Distribution
Kali Linux is an open-source, Debian-based Linux distribution geared towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering.
DOWNLOAD
DOCUMENTATION

Try Nessus Expert Free for 7 Days

Nessus® is the most comprehensive vulnerability assessment tool on the market today. Nessus Expert will help automate the vulnerability assessment process for the modern attack surface, save time on your compliance cycles and allow you to engage your IT team.

	Nessus Expert 7-Day Trial	Nessus Expert Purchase
Designed For	Consultants, Pen Testers, Developers and SMB's wanting to evaluate Nessus Expert	Consultants, Pen Testers, Developers and SMB's to use for their security practice
Real-Time Vulnerability Updates	✓	✓
Vulnerability Scanning	✓	✓
External Attack Surface Scanning	✓	✓
Scan Cloud Infrastructure	✓	✓
Unlimited Scans	✓	✓
Number of IPs Per Scanner	32	Unlimited
Web Application Scanning	✓	✓

Register

Please register to evaluate Nessus. An activation code will be emailed to the address you provide.

First Name

Last Name

Business Email

Details regarding your trial will be sent to this email.

Phone

Title

Company Name

Company Size (Employees)

Qualys Cloud Platform.

The revolutionary architecture that powers Qualys' IT, security, and compliance cloud apps.

Watch video



QUALYS CLOUD PLATFORM

Cloud Platform - Free Trial

FREE SERVICES

60-Day Remote Endpoint Protection

Global AssetView

Community Edition

SSL Labs

CertView

CloudView

BrowserCheck

Everything visible, everything secure.

Qualys Cloud Platform gives you a continuous, always-on assessment of

SONICWALL

PRODUCTS SOLUTIONS PARTNERS SUPPORT CONTACT SALES

SONICWALL PHISHING QUIZ

Over 90% of today's data breaches start with a phishing attack. Can you spot when you're being phished?

Test your ability to identify fraudulent emails and see how susceptible you really are to social engineering and phishing scams.
The SonicWall Phishing Quiz uses real examples from some of the most common phishing email attacks. Take the test and reveal your Phishing IQ today.

TAKE THE QUIZ



https://www.sonicwall.com/phishing-iq-test/#

SONICWALL

PRODUCTS SOLUTIONS PARTNERS SUPPORT CONTACT SALES

Back

Question: 1/10

01 02 03 04 05 06 07 08 09 10

You've received a pricing inquiry!

PHISHING LEGITIMATE

Re: Inquiry.

From: June Zhang support@bpricessearcher.shop

To: rizqwan cs205@vu.edu.pk

From: June Zhang support@bpricessearcher.shop

To: rizqwan cs205@vu.edu.pk

Subject: Re: Inquiry.

Hello, Nice to meet you, Pls kindly study our quotation form below and input the required prices.

Waiting for your reply so as to proceed to send our officiail order.

June Zhang,

Sales Manager

Quotation.xlsx (174.60K)

DOWNLOAD

SONICWALL

PRODUCTS SOLUTIONS PARTNERS SUPPORT CONTACT SALES

GOOD JOB, RIZQWAN!

You answered 6/10 questions correctly

Email Me My Results

Email Address →

By submitting this form, you agree to receive the SonicWall Newsletter and accept our Terms of Use and acknowledge our Privacy Statement. You can unsubscribe at any time from the Preference Center.



Question Summary:

Answered Incorrectly

1. You've Received A Pricing Inquiry!

You Said: Legitimate

LEARN WHY

Answered Correctly

2. Failed DHL Delivery

You Said: Phishing

LEARN WHY

Answered Correctly

3. It's Time To Update Your Office 365 Password

You Said: Phishing

LEARN WHY

Answered Incorrectly

4. Confirm Your Account With Doodle

You Said: Phishing

LEARN WHY

Answered Correctly

5. You're Invited To Join A Webcast!

You Said: Legitimate

LEARN WHY

Answered Correctly

6. Current Procurement Information For Sonicwall INC.

You Said: Phishing

LEARN WHY

Answered Incorrectly

7. 2: Qa-Partnership | 7:4

You Said: Legitimate

LEARN WHY

Answered Correctly

8. Microsoft Subscription Expiry

You Said: Phishing

LEARN WHY

Answered Correctly

9. Bill 22427 From Steven Murphy Electrical Contractors Pty Ltd Is Due

You Said: Legitimate

LEARN WHY

Answered Incorrectly

10. Your Credit Card Payment Is Due On Aug 7

You Said: Phishing

LEARN WHY

Incorrect

This is actually a phishing email. Be cautious about hyperlinks and attachments you open from emails – they may direct you to malicious websites designed to get you to share sensitive information.

Re: Inquiry.

From: June Zhang support@bpricessearcher.shop

To: rizqwan cs205@vu.edu.pk

From: June Zhang support@bpricessearcher.shop

To: rizqwan cs205@vu.edu.pk

Subject: Re: Inquiry.

Hello, Nice to meet you Pls kindly study our quotation form below and input the required prices.

Waiting for your reply so as to proceed to send our officiail order.

June Zhang,

Sales Manager

- -

Quotation.xlsx (174.60K)

DOWNLOAD

PREVIEW

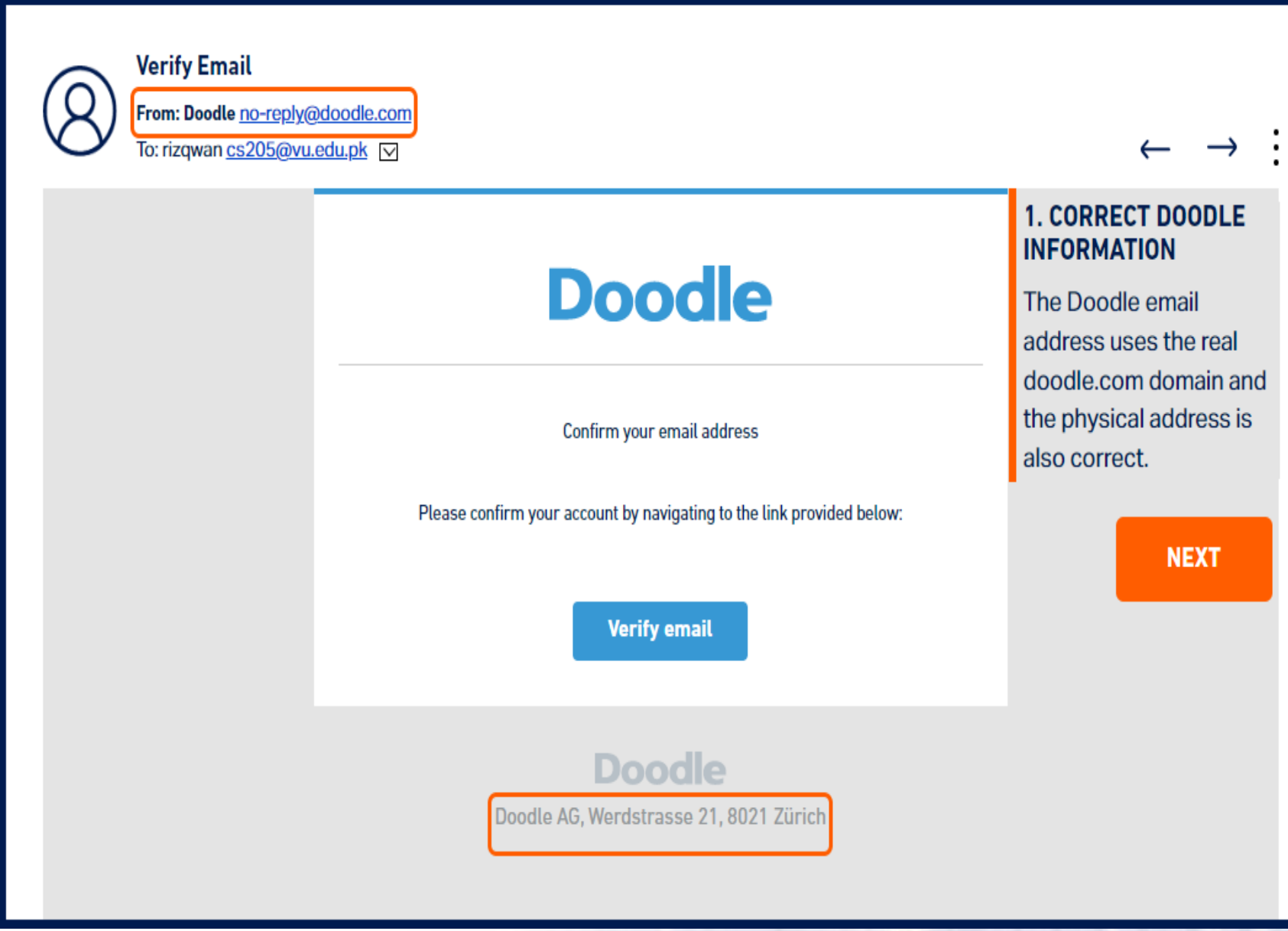
1. MISSPELLED WORDS

While it is not unusual for a real email to have some spelling errors, this particular email has too many misspelled words and grammatical errors for a professional email.

NEXT

Incorrect

This is a legitimate Doodle email communication.



- Vulnerability scanners typically work by scanning systems, applications, and network devices for known vulnerabilities and misconfigurations, using a database of known vulnerabilities and attack vectors.

SECURITY HARDENING – MANUAL & AUTOMATED WORK

- Manual & Automated mechanisms for security hardening & validation

SECURITY HARDENING – MANUAL & AUTOMATED WORK

- Step 1: Scan an IT asset using Qualys compliance scan, NESSUS compliance scan, or CIS CAT PRO Tool
- Acquire report of failed controls

SECURITY HARDENING – MANUAL & AUTOMATED WORK

- **Step 2: Apply the failed controls using AD (for Windows) or manually for other systems & devices**

SECURITY HARDENING – MANUAL & AUTOMATED WORK

- Step 3: Use the automated feature of Qualys compliance scan, Nessus compliance scan or CIS CAT Pro Tool to verify that the applied controls are in place
- Compare the ‘before’ and ‘after’ report

SECURITY HARDENING – MANUAL & AUTOMATED WORK

- Step 4: manually verify if any discrepancy is found (control should be in place but not being validated by the tool)

SECURITY HARDENING – MANUAL & AUTOMATED WORK

- Step 5: For any system or device for which the Qualys compliance scan, Nessus compliance scan, or CIS CAT Pro Tool scan cannot be performed, conduct the validation of control implementation manually

SECURITY HARDENING – MANUAL & AUTOMATED WORK

- Use sampling where necessary during manual validation work to reduce workload
- For example, 15-20 % of assets may be checked at random
- Or 15-20% of controls may be checked on an asset

END

SCAP

(Security Content Automation Protocol)

SCAP

- SCAP was developed by the **National Institute of Standards and Technology (NIST)** in collaboration with various government agencies and industry partners
- To create a consistent language and format for discussing secuirty issues

SCAP Components

- Common Weakness Enumeration (CWE)
- Common vulnerabilities and exposures (CVE)
- Common Configuration Enumeration (CCE)
- Common Platform Enumeration (CPE)
- Common vulnerability scoring system (CVSS)

Common Weakness Enumeration (CWE)

- CVE is a community-developed list of software and hardware weakness types.
- It serves as a measuring stick for security tools, and as a baseline for weakness identification, mitigation, and prevention efforts.
- https://cwe.mitre.org/index.html

CWE™ is a community-developed list of software and hardware weakness types. It serves as a common language, a measuring stick for security tools, and as a baseline for weakness identification, mitigation, and prevention efforts.

CWE List Quick Access

Search CWE

ENHANCED BY Google

View CWE

- by Software Development
- by Hardware Design
- by Research Concepts
- by Other Criteria

Total Weaknesses: 933

Viewing Customized CWE information

The CWE Team, in collaboration with the CWE/CAPEC User Experience Working Group (UEWG), has updated how users can view Weaknesses to display only those weakness details that are most relevant to them, as noted below. This update replaces the often-overlooked dropdown menu with four new filter options that better reflect the needs of our audience.

These content viewing options are available at the top of each CWE Weakness. Please review the hover text below for a description of each content filter.

Conceptual Operational Mapping Friendly Complete

Community Engagement

Hardware CWE Special Interest Group	Join HW CWE SIG
ICS/OT Special Interest Group	Join ICS/OT SIG
REST API Working Group	Join REST API WG
User Experience Working Group	Join UE WG
CWE/CAPEC Board	Read meeting minutes

Please see our Guidelines for New Content Suggestions
For other ways to get involved, contact us

CWE News

News Hardware Weaknesses Added to CWE List 3 Years Ago Today

News "CWE-CAPEC ICS/OT SIG" Booth at *S4x23*

News CWE Version 4.10 Now Available

Blog Community Actively Working to Enhance CWE's ICS/OT Coverage

Podcast "Using CWE/CAPEC in Education"

More >>

Page Last Updated: February 24, 2023

Activate Windows
Go to Settings to activate Windows.

MITRE

Use of the Common Weakness Enumeration (CWE) and the associated references from this website are subject to the Terms of Use. CWE is sponsored by the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and managed by the Homeland Security Systems Engineering and Development Institute (HSSEDI) which is operated by The MITRE Corporation (MITRE). Copyright © 2006–2023, The MITRE Corporation. CWE, CWSS, CWRAF, and the CWE logo are trademarks of The MITRE Corporation.

HSSEDI

Common vulnerabilities and exposures (CVE)

- CVE Provides detailed information on known vulnerabilities
- is used to identify and classify vulnerabilities that may impact a software and hardware products.

Common Configuration Enumeration (CCE)

- Common Configuration Enumeration (CCE) is a standardized method of identifying and describing security-relevant system configuration settings.
- CCE is maintained by the National Institute of Standards and Technology (NIST) .
- Security teams evaluate the security posture of their systems, identify misconfigured settings that may increase their risk.
- https://cce.mitre.org/lists/cce_list.html

Common Configuration Enumeration
Unique Identifiers for Common System Configuration Issues

CCE Website is in "Archive" status – read the announcement

About CCE
Documents
FAQs
CCE List
References
Editorial Policies
CCE in Use
CCE Community
CCE Working Group
Discussion Archive
News & Events
Calendar
Search the Site

CCE List
About CCE Entries
CCE Entry Creation Process
Use Cases
References
Editorial Policies

CCE List – Archive

IMPORTANT: The CCE List is now hosted at http://nvd.nist.gov/cce/index.cfm.

Version – CCE 5 (Archive)

The Common Configuration Enumeration (CCE) List is posted below. In Version 5 CCE-IDs are assigned according to "platform groups." The CCE List is available for download in two formats: the canonical Microsoft Excel spreadsheet format, and an alternative XML format. Spreadsheets are available in a single combined file and by individual platform group. XML is only available for the single combined file, containing CCE entries for all platform groups.

Please note that the spreadsheets are the canonical format. In the case of any discrepancy between the XML and the spreadsheets, the spreadsheets should be preferred. Also, the format of the XML itself is version 0.2 of that encoding, and is subject to change.

IMPORTANT: Activity on the CCE effort has been suspended, and the CCE Web site has been moved to "Archive" status. Read the complete message on the homepage.

Release Details

The current release of CCE is 5.20130214 (CCE Version 5, updated on February 14, 2013). A ChangeLog is available that details the changes since the last release, 5.20120521.

Total CCEs: 12,163

DOWNLOADS (XML format)	DATE UPDATED
CCE v5 - All Platform Groups-COMBINED FILE (11.5 MB)	February 14, 2013

DOWNLOADS (MS Excel format)	DATE UPDATED
CCE v5 - All Platform Groups-COMBINED FILE (5398 KB)	February 14, 2013
CCE v5 - AIX 5.3 (226 KB)	May 6, 2009
CCE v5 - Apache HTTP 1.3 (47 KB)	February 14, 2013
CCE v5 - Apache HTTP 2.0 (97 KB)	February 14, 2013
CCE v5 - Apache HTTP 2.2 (123 KB)	February 14, 2013
CCE v5 - Apache Tomcat 4 (71 KB)	February 14, 2013
CCE v5 - Apache Tomcat 5 (48 KB)	February 14, 2013
CCE v5 - Apache Tomcat 6 (47 KB)	February 14, 2013
CCE v5 - HP-UX 11.23 (202 KB)	May 6, 2009
CCE v5 - Internet Explorer 7 (260 KB)	March 14, 2012
CCE v5 - Internet Explorer 8 (906 KB)	September 26, 2010

Activate Windows
Go to Settings to activate Windows.

Common Platform Enumeration (CPE)

- **CPE** is a standardized method of describing and identifying software systems, applications, and operating systems using a unique identifier format.
- provides a structured and uniform way of describing the attributes of a software product, such as the vendor name, product name, version number, and edition.

- https://nvd.nist.gov/products/cpe

Common Platform Enumeration (CPE)

- consists of three components separated by colons:
- The first component identifies the vendor name,
- The second component identifies the product name, and
- The third component identifies the version number.
- For example, the CPE string for Windows 10 would be:
- cpe:/o:microsoft:windows_10
- This format is used by various security tools, such as vulnerability scanners, to identify and match software products with known vulnerabilities or other security issues.

- https://nvd.nist.gov/products/cpe

NOTICE

In September 2023, the NVD plans to retire all legacy data feeds while guiding any remaining data feed users to updated application-programming interfaces (APIs). APIs have many benefits over data feeds and have been the proven and preferred approach to web-based automation for over a decade. For additional information on the NVD API, please visit the developers pages. Click here for more information on the NVD timeline.

Official Common Platform Enumeration (CPE) Dictionary

CPE is a structured naming scheme for information technology systems, software, and packages. Based upon the generic syntax for Uniform Resource Identifiers (URI), CPE includes a formal name format, a method for checking names against a system, and a description format for binding text and tests to a name.

Below is the current official version of the CPE Product Dictionary. The dictionary provides an agreed upon list of official CPE names. The dictionary is provided in XML format and is available to the general public. Please check back frequently as the CPE Product Dictionary will continue to grow to include all past, present and future product releases. The CPE Dictionary is updated nightly when modifications or new names are added.

As of December 2009, The National Vulnerability Database is now accepting contributions to the Official CPE Dictionary. Organizations interested in submitting CPE Names should contact the NVD CPE team at cpe_dictionary@nist.gov for help with the processing of their submission.

The CPE Dictionary hosted and maintained at NIST may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

Common vulnerability scoring system (CVSS)

- CVSS is a standardized method of assessing and scoring the severity of cyber security vulnerabilities.
- prioritize and manage vulnerabilities based on their potential impact.

Common Vulnerabilities and Scoring System

Exploitability Matrix:

- Access Vector
- Attack Complexity
- Privileges Required
- User Interaction

National Vulnerability Database (NVD)

- NVD is the largest publicly available source of vulnerability intelligence by National Institute of Standards and Technology (NIST)
- Vulnerabilities in the NVD are called Common Vulnerabilities and Exposures (CVE).
- https://nvd.nist.gov/

Common Vulnerabilities and Exposures

- Common Vulnerabilities and Exposures (CVE) is a standardized list of publicly known cyber security vulnerabilities and exposures.

- Each CVE entry includes a unique identifier, a description of the vulnerability, the affected software or hardware, and a score based on the Common Vulnerability Scoring System (CVSS).

- The score is derived from a set of metrics using the (CVSS)
- The CVE feeds into the National Vulnerabilities Database(NVD)

https://cve.mitre.org/

https://www.cvedetails.com/vulnerabilities-by-types.php

https://www.cvedetails.com/vulnerability-list/opsqli-1/sql-injection.html

TOTAL CVE Records: 198864

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG and CVE Record Format JSON are underway.

NOTICE: Changes are coming to CVE List Content Downloads in 2023.

The mission of the CVE® Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.

CVE News

News has moved to the new CVE website.

Go to new News page >>

CVE Podcast

Podcasts have moved to the new CVE website.

Go to new Podcast page >>

CVE Blog

Blogs are moving to the new CVE website.

Go to new Blogs page >>

Become a CNA

CVE Numbering Authorities, or "CNAs," are essential to the CVE Program's success and every CVE Record is added to the CVE List by a CNA.

Join today!

- Business benefits
- No fee or contract
- Few requirements
- Easy to join

Go to new CVE website



Learn How to Become a CNA >>>

Watch CNA Onboarding Videos >>

Newest CVE Records

Tweets from @CVEnew

CVE
@CVEnew · 2h

CVE-2023-0665 HashiCorp Vault's PKI mount issuer endpoints did not correctly authorize access to remove an issuer or modify issuer metadata, potentially resulting in denial of service of the PKI mount. This bug did not affect public or private key... cve.mitre.org/cgi-bin/cvenam...

Follow @CVEnew >>

Page Last Updated or Reviewed: July 22, 2022

Use of the CVE® List and the associated references from this website are subject to the terms of use. CVE is sponsored by the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Copyright © 1999-2023, The MITRE Corporation. CVE and the CVE logo are registered trademarks of The MITRE Corporation.

Switch to https://

Home

Browse :

Vendors

Products

Vulnerabilities By Date

Vulnerabilities By Type

Reports :

CVSS Score Report

CVSS Score Distribution

Search :

Vendor Search

Product Search

Version Search

Vulnerability Search

By Microsoft References

Top 50 :

Vendors

Vendor Cvss Scores

Products

Product Cvss Scores

Versions

Other :

Microsoft Bulletins

Bugtraq Entries

CWE Definitions

About & Contact

Feedback

CVE Help

FAQ

Articles

External Links :

NVD Website

CWE Web Site

View CVE :

Go

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

View BID :

Go

(e.g.: 12345)

Search By Microsoft Reference ID:

Go

Browse Vulnerabilities By Date

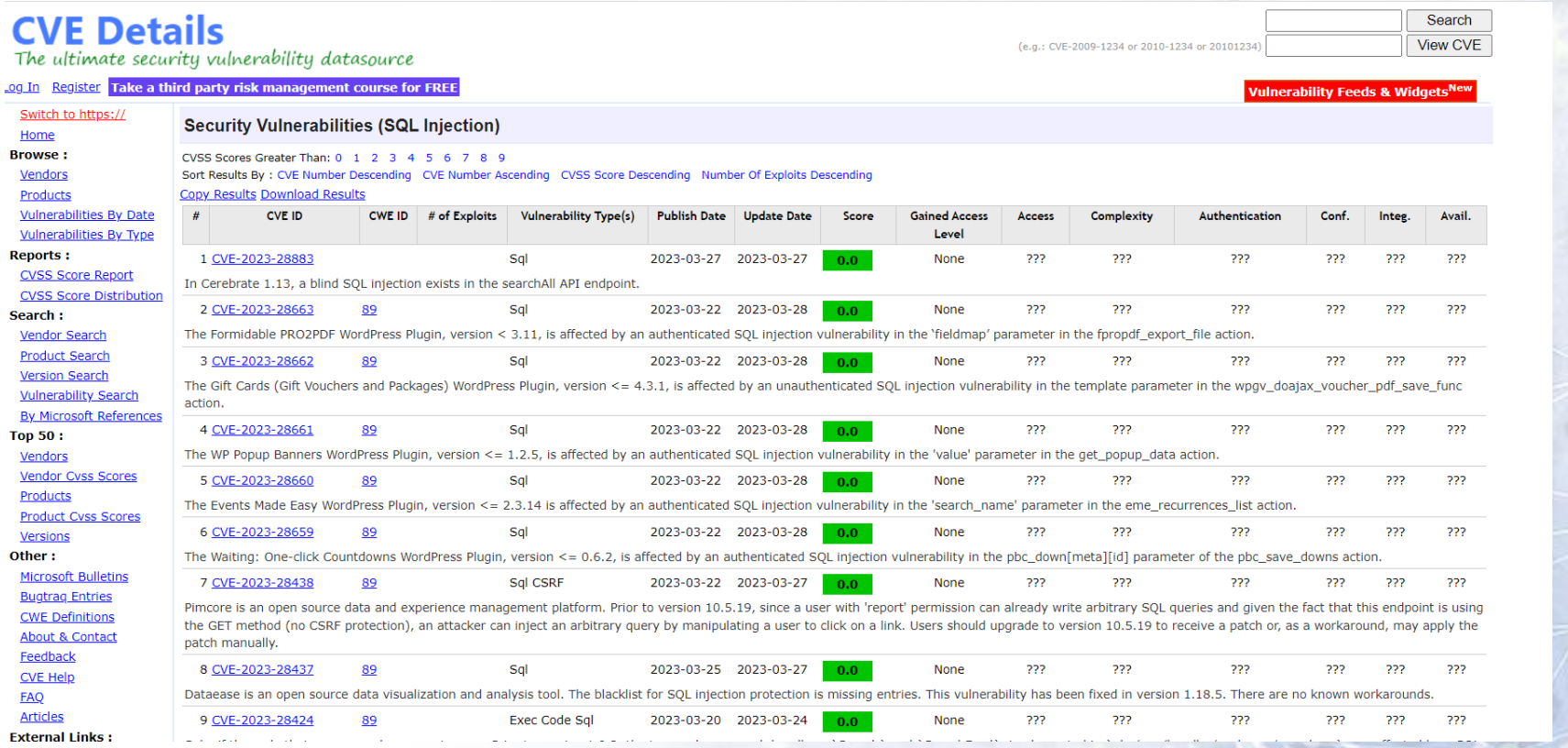
Year	# of Vulnerabilities												
1999	894	January	February	March	April	May	June	July	August	September	October	November	December
2000	1020	January	February	March	April	May	June	July	August	September	October	November	December
2001	1677	January	February	March	April	May	June	July	August	September	October	November	December
2002	2156	January	February	March	April	May	June	July	August	September	October	November	December
2003	1527	January	February	March	April	May	June	July	August	September	October	November	December
2004	2451	January	February	March	April	May	June	July	August	September	October	November	December
2005	4935	January	February	March	April	May	June	July	August	September	October	November	December
2006	6610	January	February	March	April	May	June	July	August	September	October	November	December
2007	6520	January	February	March	April	May	June	July	August	September	October	November	December
2008	5632	January	February	March	April	May	June	July	August	September	October	November	December
2009	5736	January	February	March	April	May	June	July	August	September	October	November	December
2010	4653	January	February	March	April	May	June	July	August	September	October	November	December
2011	4155	January	February	March	April	May	June	July	August	September	October	November	December
2012	5297	January	February	March	April	May	June	July	August	September	October	November	December
2013	5191	January	February	March	April	May	June	July	August	September	October	November	December
2014	7939	January	February	March	April	May	June	July	August	September	October	November	December
2015	6504	January	February	March	April	May	June	July	August	September	October	November	December
2016	6454	January	February	March	April	May	June	July	August	September	October	November	December
2017	14714	January	February	March	April	May	June	July	August	September	October	November	December
2018	16557	January	February	March	April	May	June	July	August	September	October	November	December
2019	17344	January	February	March	April	May	June	July	August	September	October	November	December
2020	18325	January	February	March	April	May	June	July	August	September	October	November	December
2021	20171	January	February	March	April	May	June	July	August	September	October	November	December
2022	25227	January	February	March	April	May	June	July	August	September	October	November	December
2023	7057	January	February	March									

Warning : Vulnerabilities with publish dates before 1999 are not included in this table and chart. (Because there are not many of them and they make the page look bad; and they may not be actually published in those years.)

Vulnerabilities By Year



Common Vulnerabilities and Exposures



CVE Details

The ultimate security vulnerability datasource

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234) Search View CVE

og In Register Take a third party risk management course for FREE

Vulnerability Feeds & Widgets New

Switch to https://
Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions
Other :
Microsoft Bulletins
Bugtraq Entries
CWE Definitions
About & Contact
Feedback
CVE Help
FAQ
Articles
External Links :

Security Vulnerabilities (SQL Injection)

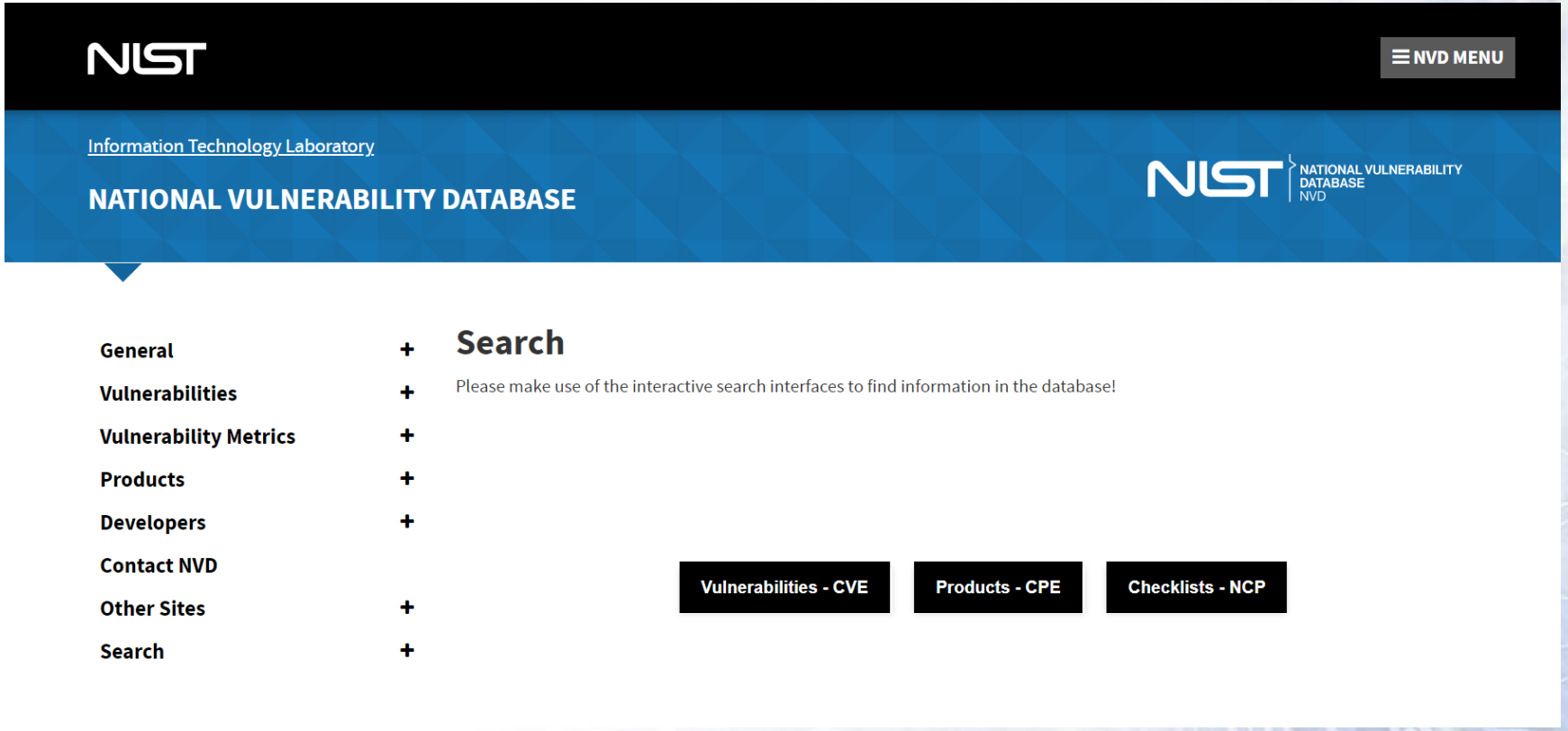
CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2023-28883			Sql	2023-03-27	2023-03-27	0.0	None	???	???	???	???	???	???
In Cerebrate 1.13, a blind SQL injection exists in the searchAll API endpoint.														
2	CVE-2023-28663	89		Sql	2023-03-22	2023-03-28	0.0	None	???	???	???	???	???	???
The Formidable PRO2PDF WordPress Plugin, version < 3.11, is affected by an authenticated SQL injection vulnerability in the 'fieldmap' parameter in the fpropdf_export_file action.														
3	CVE-2023-28662	89		Sql	2023-03-22	2023-03-28	0.0	None	???	???	???	???	???	???
The Gift Cards (Gift Vouchers and Packages) WordPress Plugin, version <= 4.3.1, is affected by an unauthenticated SQL injection vulnerability in the template parameter in the wpgv_doajax_voucher_pdf_save_func action.														
4	CVE-2023-28661	89		Sql	2023-03-22	2023-03-28	0.0	None	???	???	???	???	???	???
The WP Popup Banners WordPress Plugin, version <= 1.2.5, is affected by an authenticated SQL injection vulnerability in the 'value' parameter in the get_popup_data action.														
5	CVE-2023-28660	89		Sql	2023-03-22	2023-03-28	0.0	None	???	???	???	???	???	???
The Events Made Easy WordPress Plugin, version <= 2.3.14 is affected by an authenticated SQL injection vulnerability in the 'search_name' parameter in the eme_recurrences_list action.														
6	CVE-2023-28659	89		Sql	2023-03-22	2023-03-28	0.0	None	???	???	???	???	???	???
The Waiting: One-click Countdowns WordPress Plugin, version <= 0.6.2, is affected by an authenticated SQL injection vulnerability in the pbc_down[meta][id] parameter of the pbc_save_downs action.														
7	CVE-2023-28438	89		Sql CSRF	2023-03-22	2023-03-27	0.0	None	???	???	???	???	???	???
Pimcore is an open source data and experience management platform. Prior to version 10.5.19, since a user with 'report' permission can already write arbitrary SQL queries and given the fact that this endpoint is using the GET method (no CSRF protection), an attacker can inject an arbitrary query by manipulating a user to click on a link. Users should upgrade to version 10.5.19 to receive a patch or, as a workaround, may apply the patch manually.														
8	CVE-2023-28437	89		Sql	2023-03-25	2023-03-27	0.0	None	???	???	???	???	???	???
Dataease is an open source data visualization and analysis tool. The blacklist for SQL injection protection is missing entries. This vulnerability has been fixed in version 1.18.5. There are no known workarounds.														
9	CVE-2023-28424	89		Exec Code Sql	2023-03-20	2023-03-24	0.0	None	???	???	???	???	???	???

Common Vulnerabilities and Expore



https://nvd.nist.gov/search

Common Vulnerabilities and Exposures

NIST

NVD MENU

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NIST NATIONAL VULNERABILITY DATABASE NVD

- **General** +
- **Vulnerabilities** +
- **Vulnerability Metrics** +
- **Products** +
- **Developers** +
- **Contact NVD**
- **Other Sites** +
- **Search** +



Understanding Vulnerability Detail Pages



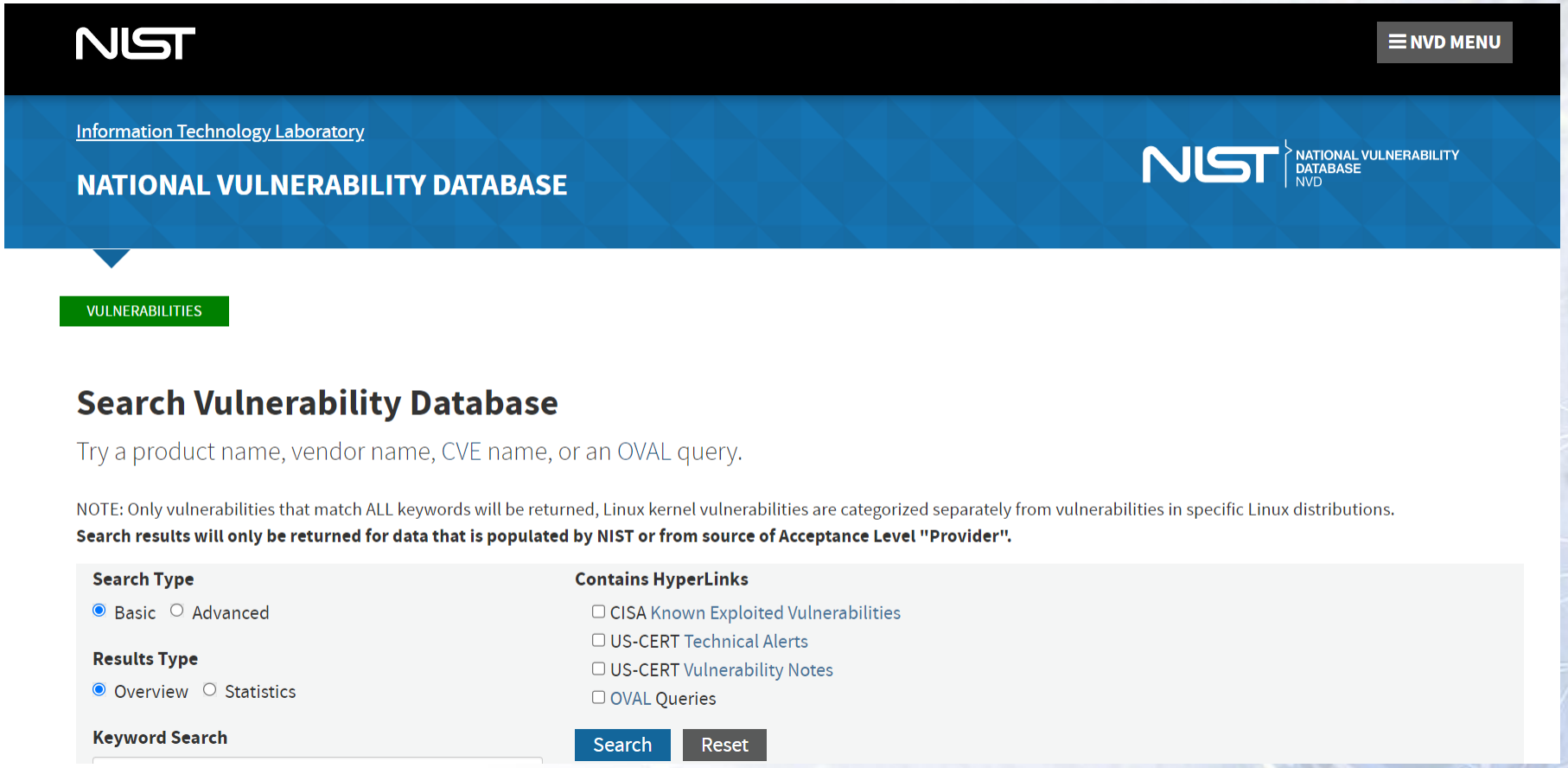
Vulnerability Statuses

Vulnerabilities

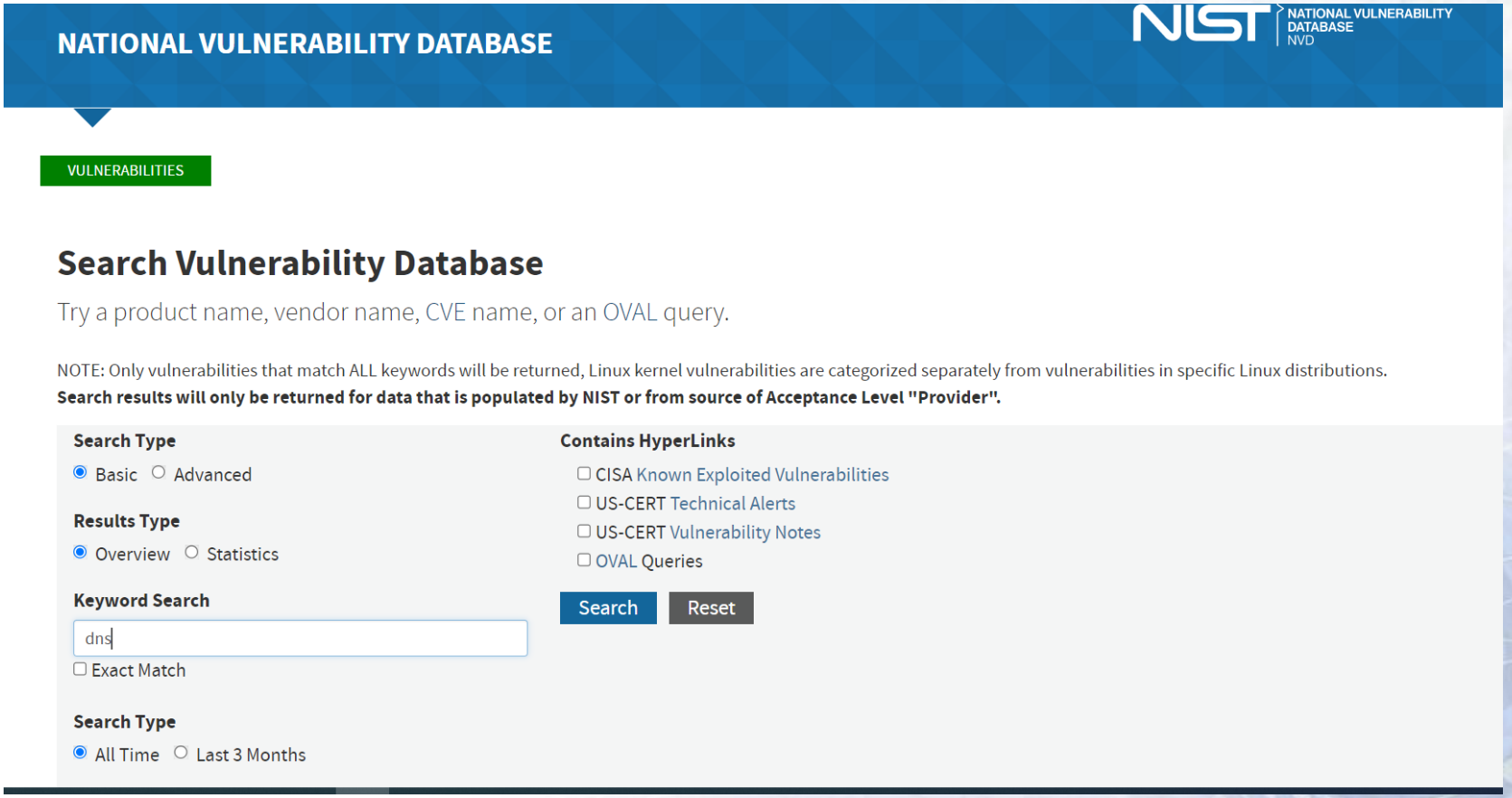
All vulnerabilities in the NVD have been assigned a CVE identifier and thus, abide by the definition below.

CVE defines a vulnerability as:

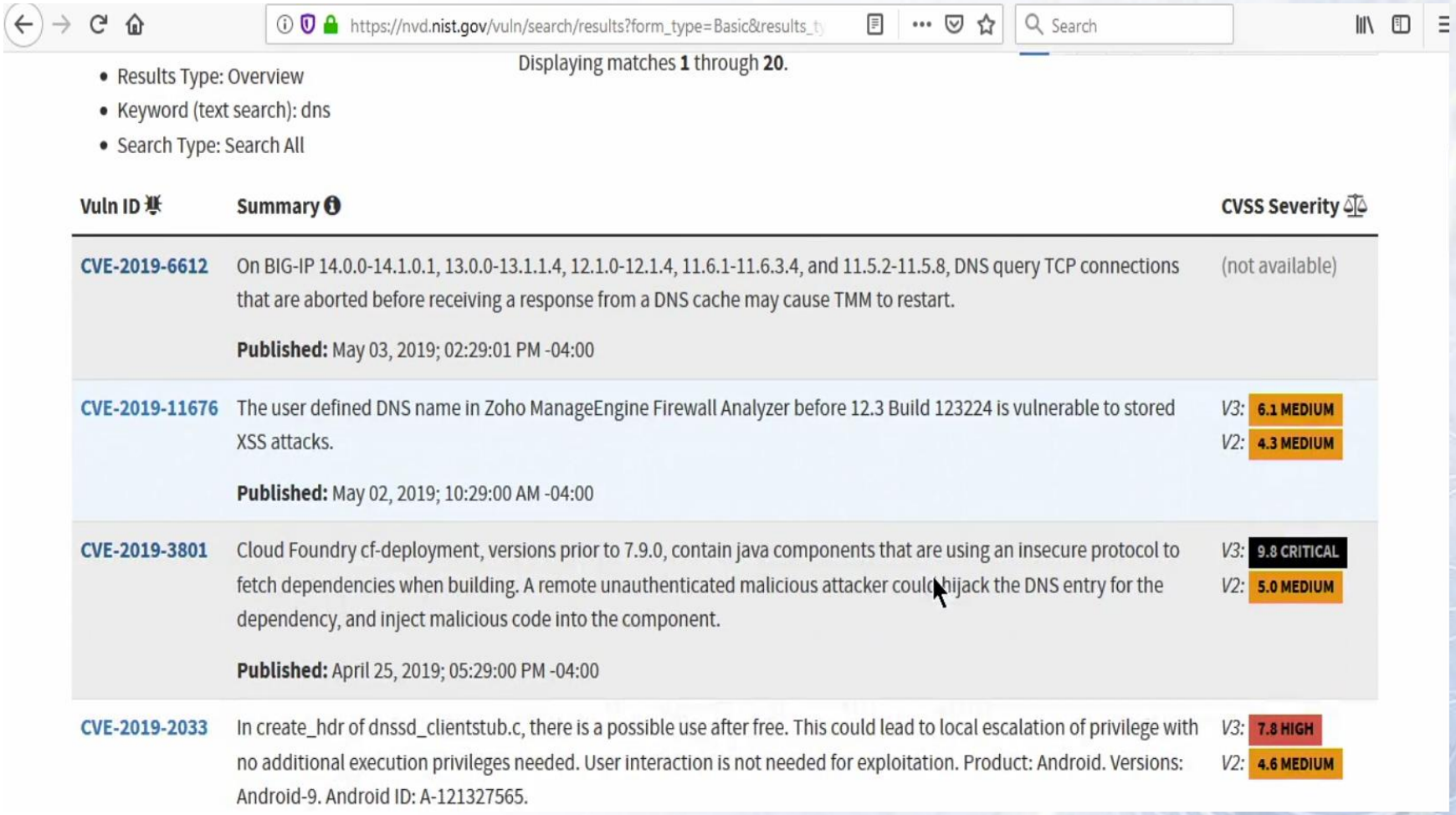
Common Vulnerabilities and Exposures



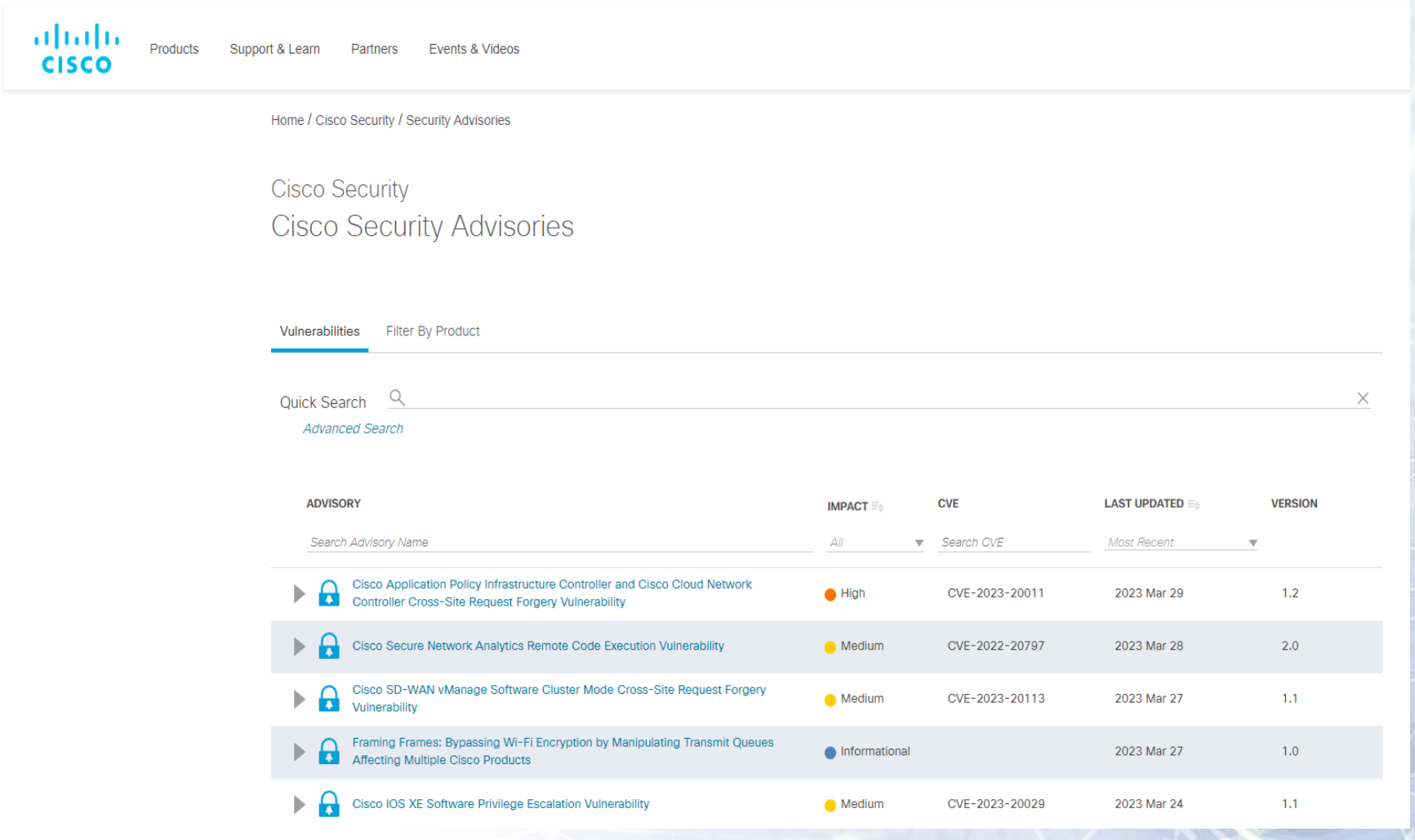
Common Vulnerabilities and Exposures



Common Vulnerabilities and Expore

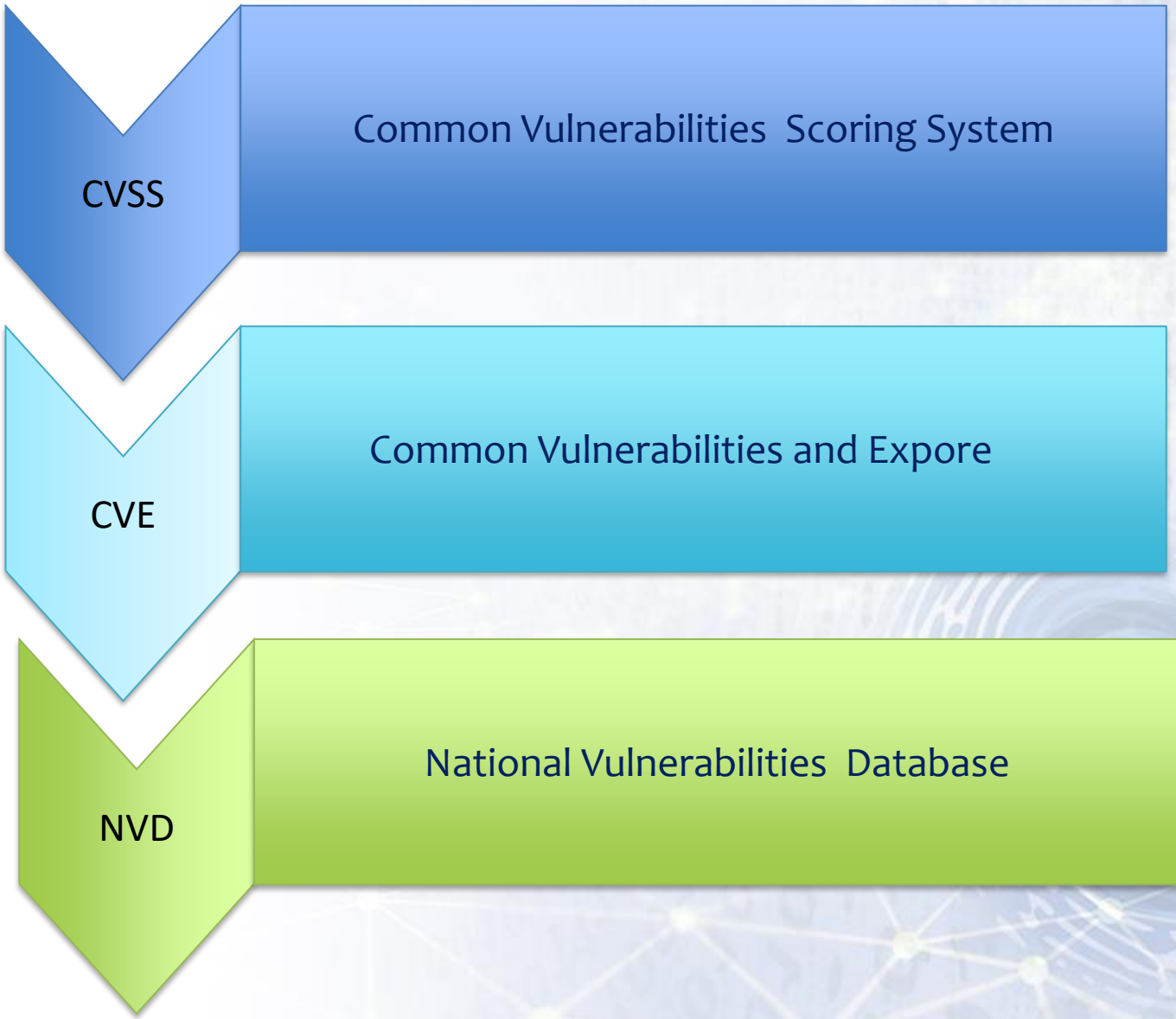


Common Vulnerabilities and Exposures



https://sec.cloudapps.cisco.com/security/center/publicationListing.x

Common Vulnerabilities and Exposures



Common Vulnerabilities and Scoring System

- Industry standard that rates the severity of vulnerabilities
- Used in Common Vulnerabilities and Exposures (CVE) listings to aid in prioritizing vulnerabilities
- Based on a set of metrics that determines the overall score

Common Vulnerabilities and Scoring System

TABLE F-2: ASSESSMENT SCALE – VULNERABILITY SEVERITY

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The vulnerability is exposed and exploitable, and its exploitation could result in severe impacts. Relevant security control or other remediation is not implemented and not planned; or no security measure can be identified to remediate the vulnerability.
High	80-95	8	The vulnerability is of high concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant security control or other remediation is planned but not implemented; compensating controls are in place and at least minimally effective.
Moderate	21-79	5	The vulnerability is of moderate concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant security control or other remediation is partially implemented and somewhat effective.
Low	5-20	2	The vulnerability is of minor concern, but effectiveness of remediation could be improved. Relevant security control or other remediation is fully implemented and somewhat effective.
Very Low	0-4	0	The vulnerability is not of concern. Relevant security control or other remediation is fully implemented, assessed, and effective.

CVSS severity factors

- **Attack vector:** the attacker needs to be authenticated or whether the attack can be launched remotely.
- **Attack complexity:** the attack requires special knowledge or tools
- **Privileges required:** an attacker would need administrative access or user-level access.
- **Impact on confidentiality, integrity, and availability:** potential impact of the vulnerability on the confidentiality, integrity, and availability of systems and data.
- CVSS uses a scoring system ranging from 0 to 10, with higher scores indicating more severe vulnerabilities.

CVSS Score Qualitative Rating:

Score	Rating
0.0	None
0.1 – 3.9	Low
4.0 – 6.9	Medium
7.0 – 8.9	High
9.0 – 10.0	Critical

https://www.first.org/cvss/v3.1/examples

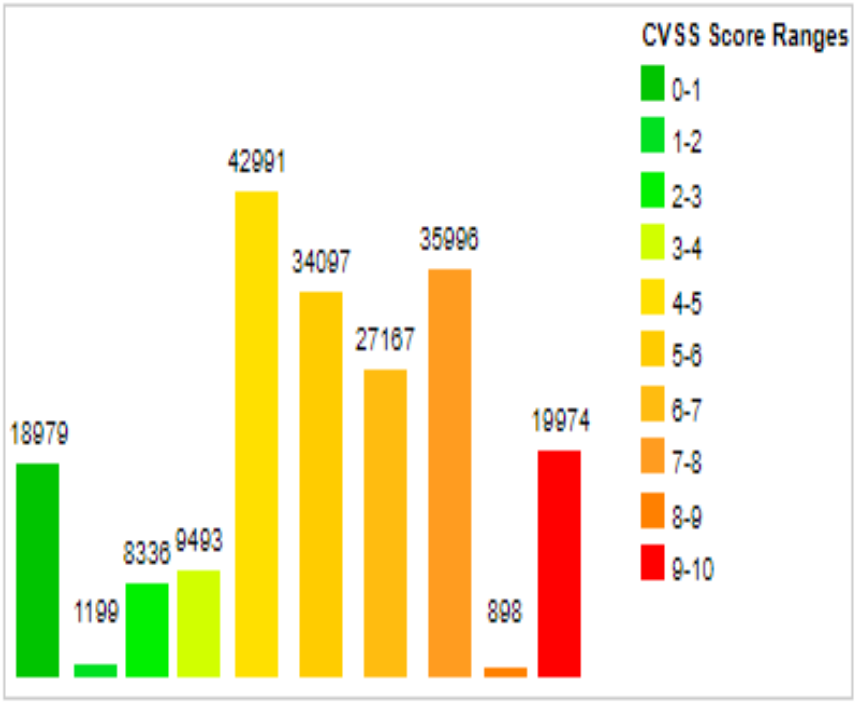
https://nvd.nist.gov/vuln-metrics/cvss

Current CVSS Score Distribution For All Vulnerabilities

Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	18979	9.50
1-2	1199	0.60
2-3	8336	4.20
3-4	9493	4.80
4-5	42991	21.60
5-6	34097	17.10
6-7	27167	13.60
7-8	35996	18.10
8-9	898	0.50
9-10	19974	10.00
Total	199130	

Vulnerability Distribution By CVSS Scores



Common Vulnerabilities and Scoring System

Impact Metrics:

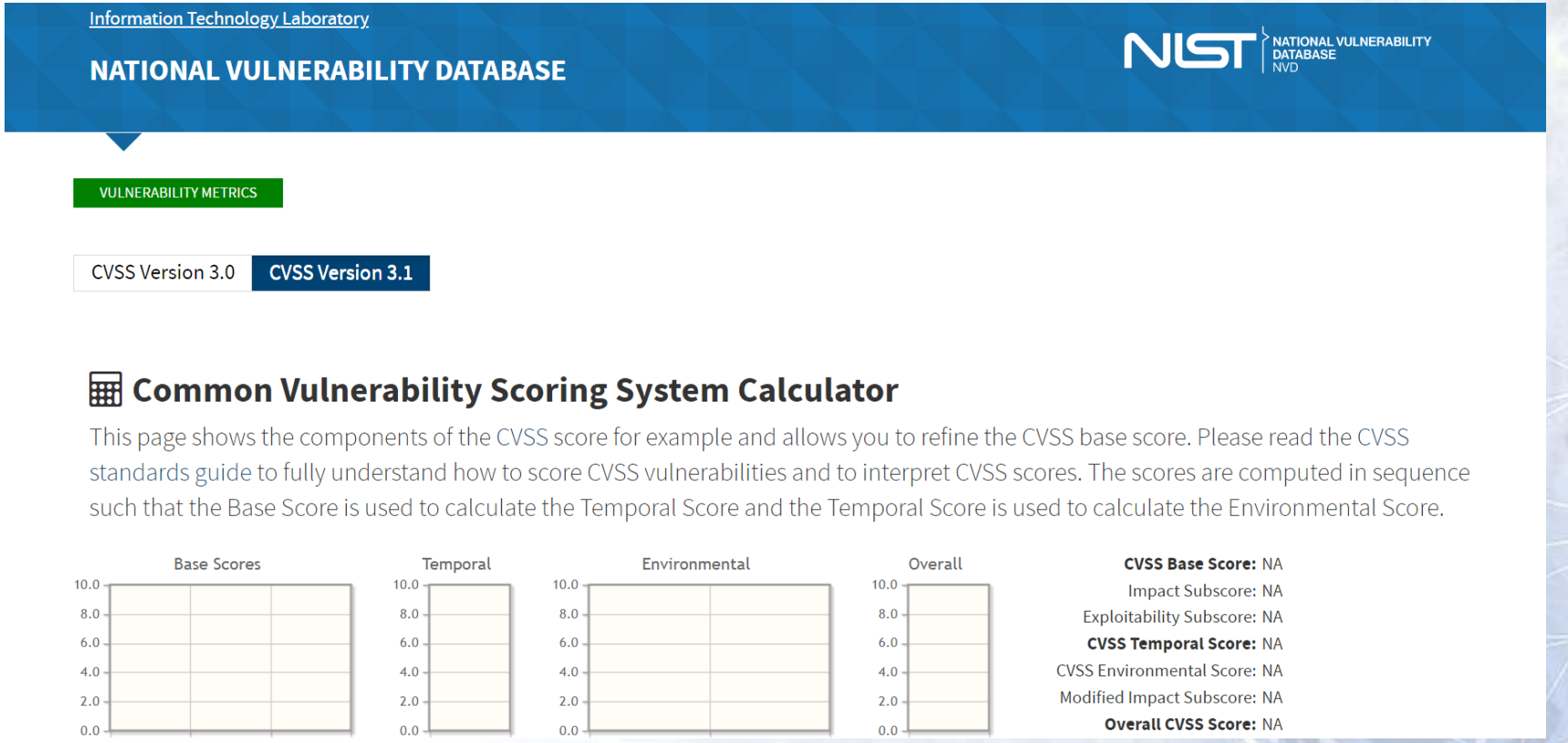
- What impact will this have if the threat is able to exploit the vulnerability?
- Will it be a violation of confidentiality, integrity, or availability

Common Vulnerabilities and Scoring System

Temporal Metrics:

- The Current state of the exploit

Common Vulnerabilities and Scoring System



https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

Common Vulnerabilities and Scoring System

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*

Network (AV:N)	Adjacent Network (AV:A)	Local (AV:L)	Physical (AV:P)

Attack Complexity (AC)*

Low (AC:L)	High (AC:H)

Privileges Required (PR)*

None (PR:N)	**Low (PR:L)**	High (PR:H)

User Interaction (UI)*

None (UI:N)	**Required (UI:R)**

Scope (S)*

Unchanged (S:U)	**Changed (S:C)**

Impact Metrics

Confidentiality Impact (C)*

None (C:N)	Low (C:L)	**High (C:H)**

Integrity Impact (I)*

None (I:N)	Low (I:L)	**High (I:H)**

Availability Impact (A)*

None (A:N)	Low (A:L)	High (A:H)

Common Vulnerabilities and Scoring System

* - All base metrics are required to generate a base score.

Temporal Score Metrics

Exploit Code Maturity (E)

Not Defined (E:X)	Unproven that exploit exists (E:U)	**Proof of concept code (E:P)**	Functional exploit exists (E:F)	High (E:H)

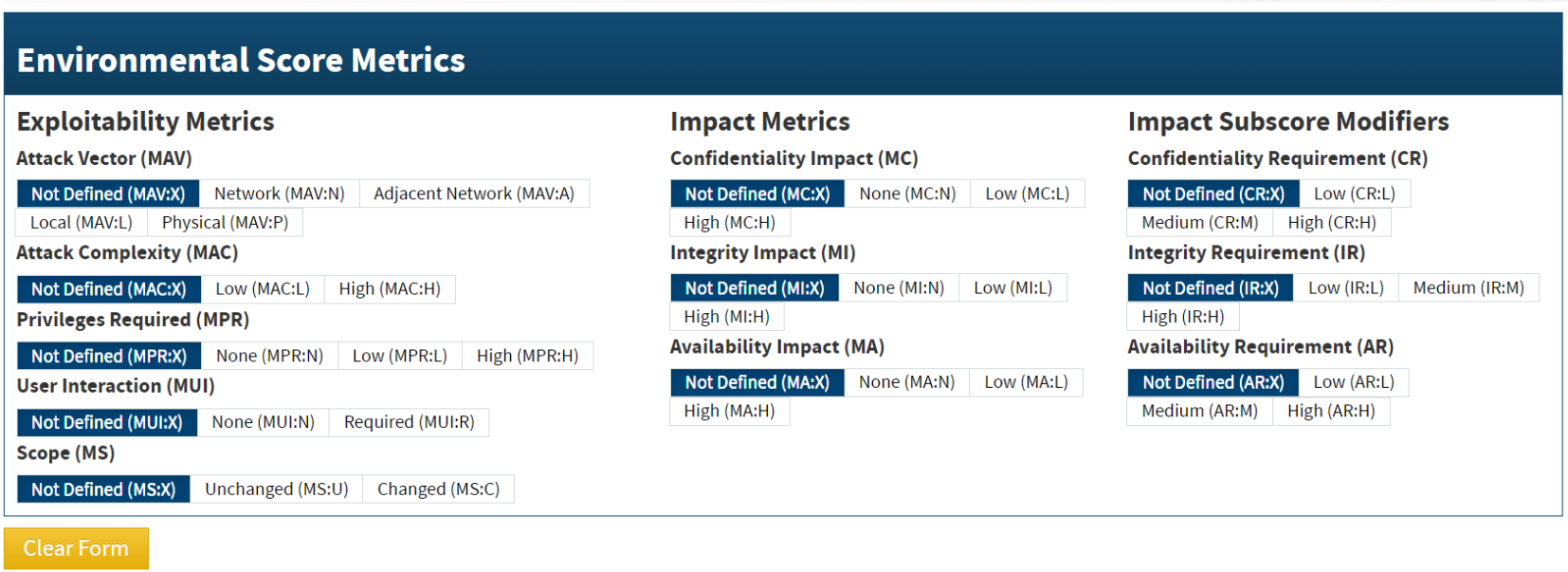
Remediation Level (RL)

Not Defined (RL:X)	Official fix (RL:O)	Temporary fix (RL:T)	**Workaround (RL:W)**	Unavailable (RL:U)

Report Confidence (RC)

Not Defined (RC:X)	Unknown (RC:U)	Reasonable (RC:R)	**Confirmed (RC:C)**

Common Vulnerabilities and Scoring System

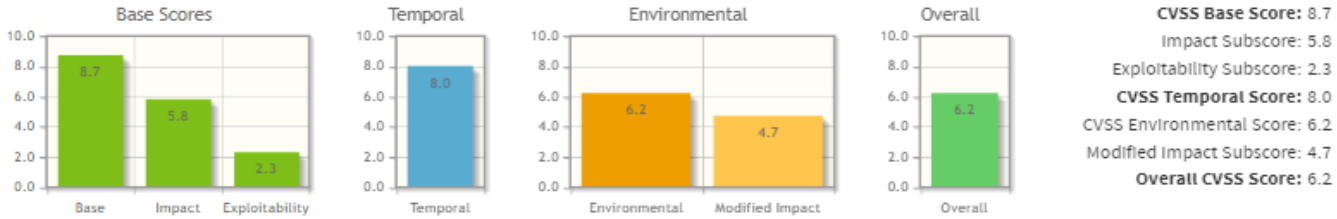


VULNERABILITY METRICS

CVSS Version 3.0 **CVSS Version 3.1**

Common Vulnerability Scoring System Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



CVSS Base Score: 8.7
Impact Subscore: 5.8
Exploitability Subscore: 2.3
CVSS Temporal Score: 8.0
CVSS Environmental Score: 6.2
Modified Impact Subscore: 4.7
Overall CVSS Score: 6.2

Show Equations

CVSS v3.1 Vector

AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:N/E:P/RL:W/RC:X/CR:M/IR:X/AR:M/MAV:L/MAC:X/MPR:L/MUI:R/MS:X/MC:X/MI:L/MA:X

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*

Network (AV:N) | Adjacent Network (AV:A) | Local (AV:L) | Physical (AV:P)

Attack Complexity (AC)*

Low (AC:L) | High (AC:H)

Privileges Required (PR)*

None (PR:N) | **Low (PR:L)** | High (PR:H)

User Interaction (UI)*

None (UI:N) | **Required (UI:R)**

Scope (S)*

Unchanged (S:U) | **Changed (S:C)**

Impact Metrics

Confidentiality Impact (C)*

None (C:N) | Low (C:L) | **High (C:H)**

Integrity Impact (I)*

None (I:N) | Low (I:L) | **High (I:H)**

Availability Impact (A)*

None (A:N) | Low (A:L) | High (A:H)

What Is CVE & Vulnerability Database ?

Impact

CVSS Severity (version 3.0):

CVSS v3 Base Score: 9.8 Critical
Vector: CVSS:3.0/AV:N/AC:L/I
(legend)
Impact Score: 5.9
Exploitability Score: 3.9

CVSS Version 3 Metrics:

Attack Vector (AV): Network
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Unchanged
Confidentiality (C): High
Integrity (I): High
Availability (A): High

What Is CVE & Vulnerability Database ?

CVSS Severity (version 2.0):

CVSS v2 Base Score: 7.5 HIGH
Vector: (AV:N/AC:L/Au:N/C:P/I:P/A:P) (legend)
Impact Subscore: 6.4
Exploitability Subscore: 10.0

CVSS Version 2 Metrics:

Access Vector: Network exploitable
Access Complexity: Low
Authentication: Not required to exploit
Impact Type: Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service

NESUSS

- Nessus dates back to 1998
- Nessus moved to closed source commercial product in 2005
- The most trusted and gold standard vulnerability assessment solution
- Most widely deployed security standard


1
Nessus Essentials
Available for free use by the security community
2
Nessus Professional
Available for commercial use on a subscription basis

- Nessus Essential is limited to scanning only 16 IP addresses


Nessus | Tenable®
tenable
Downloads Blog Contact Login Global
Cyber Exposure Products Solutions Research Services Company Partners
Free Trial
Buy Now
THE NESSUS FAMILY
Nessus is trusted by more than 27,000 organizations worldwide as one of the most widely deployed security technologies on the planet - and the gold standard for vulnerability assessment.
nessus Essentials
FREE DOWNLOAD
Scan 16 IPs
✓ Use anywhere
✓ Free training and guidance
✓ Support via Tenable Community
Ideal for: Educators, students and individuals starting their careers in Cyber Security
nessus Professional
7-DAY FREE TRIAL
Scan 32 IPs
✓ Use anywhere, try for 7 days
✓ Configuration Assessment
✓ Live Results
✓ Custom Reporting
✓ Support via Tenable Community
Ideal for: Consultants, Pen Testers and
nessus Professional
SUBSCRIPTION
Scan Unlimited IPs
✓ Unlimited assessments
✓ Use anywhere, annual subscription
✓ Configuration assessment
✓ Live Results
✓ Custom Reporting
✓ Email and Community Support

1

Outdated Protocols

SSL is no longer a secure protocol!

2

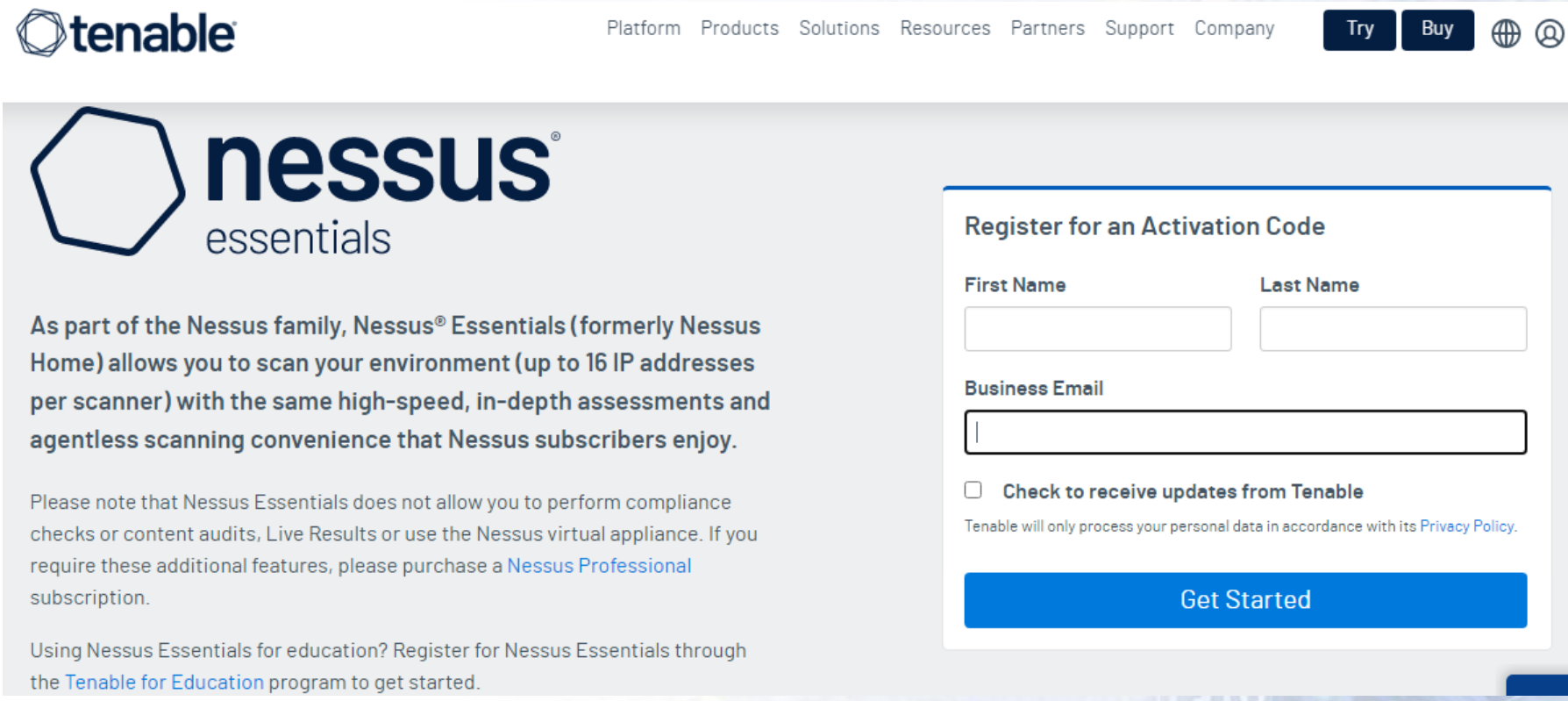
Insecure Cipher Suites

Only support strong encryption!

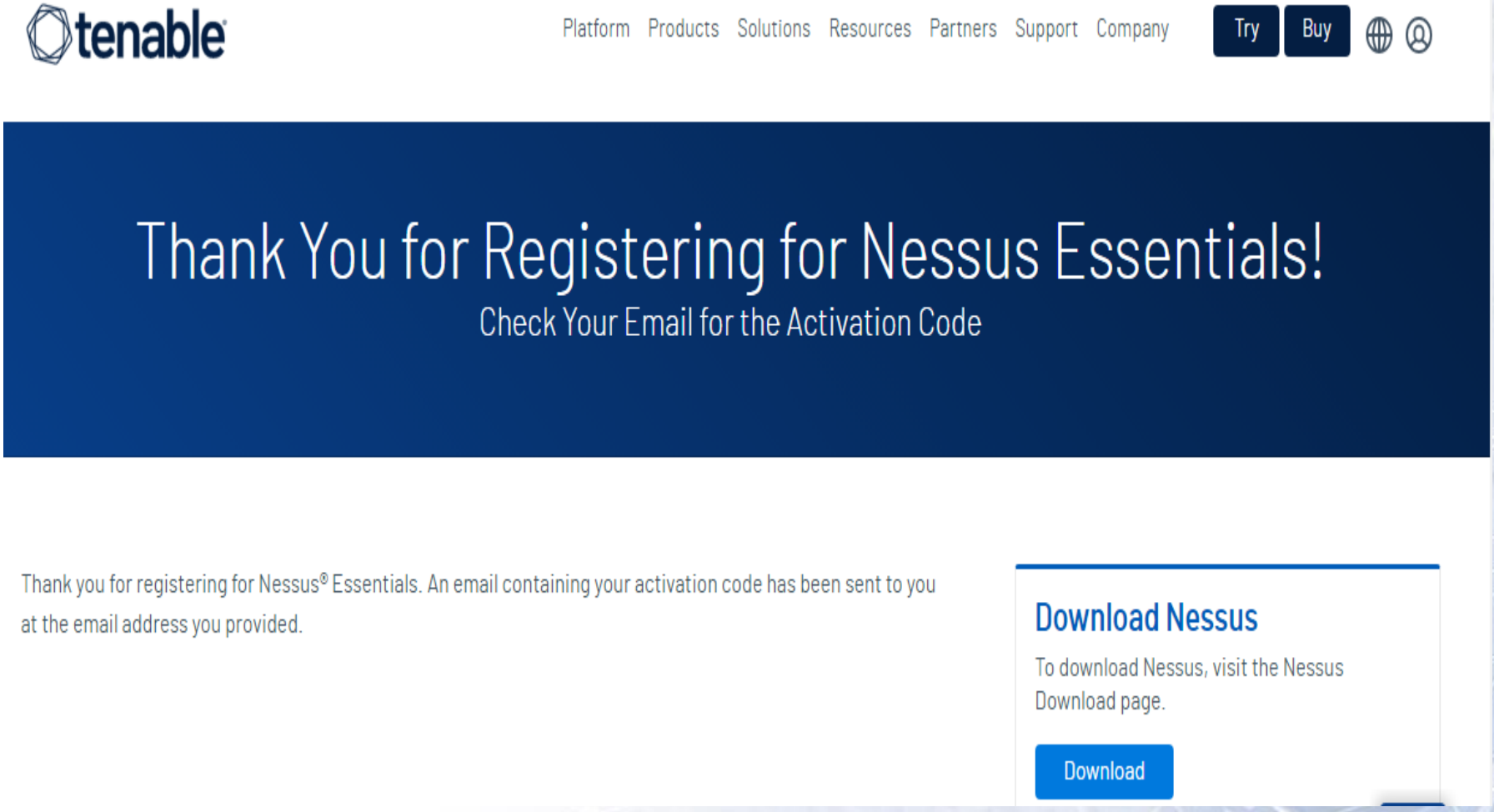
3

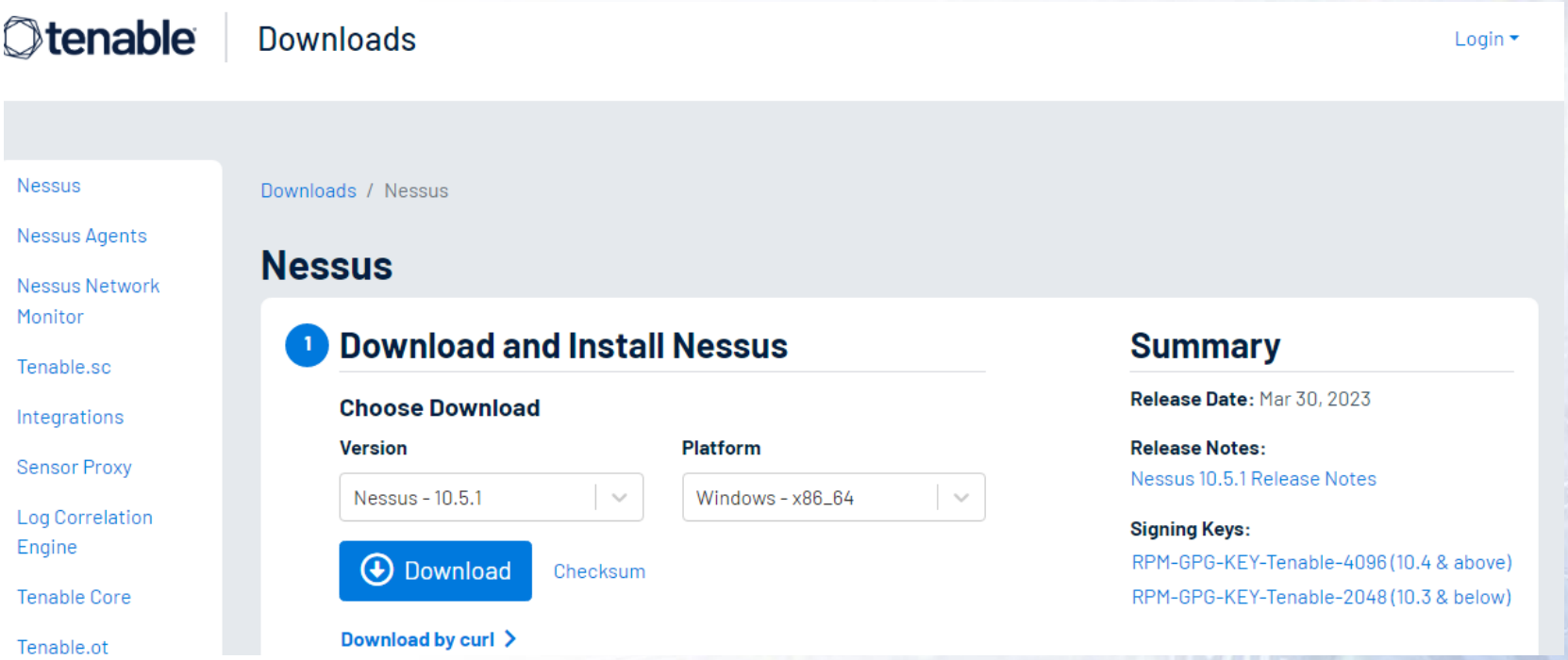
Certificate Issues

Watch for expired, self-signed, or invalid certificates.

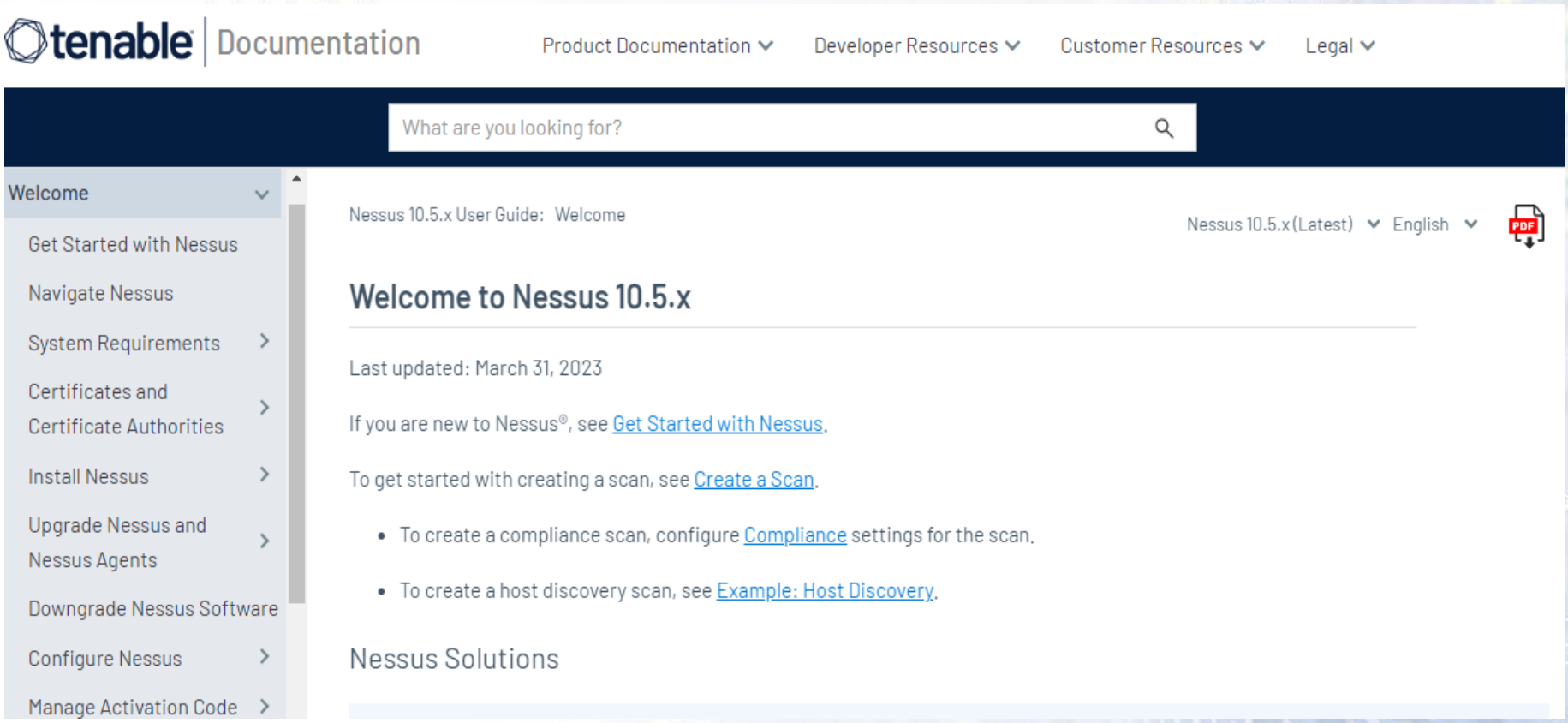


https://www.tenable.com/products/nessus/nessus-essentials?action=register


tenable
Platform Products Solutions Resources Partners Support Company
Try Buy
Thank You for Registering for Nessus Essentials!
Check Your Email for the Activation Code
Thank you for registering for Nessus® Essentials. An email containing your activation code has been sent to you at the email address you provided.
Download Nessus
To download Nessus, visit the Nessus Download page.
Download

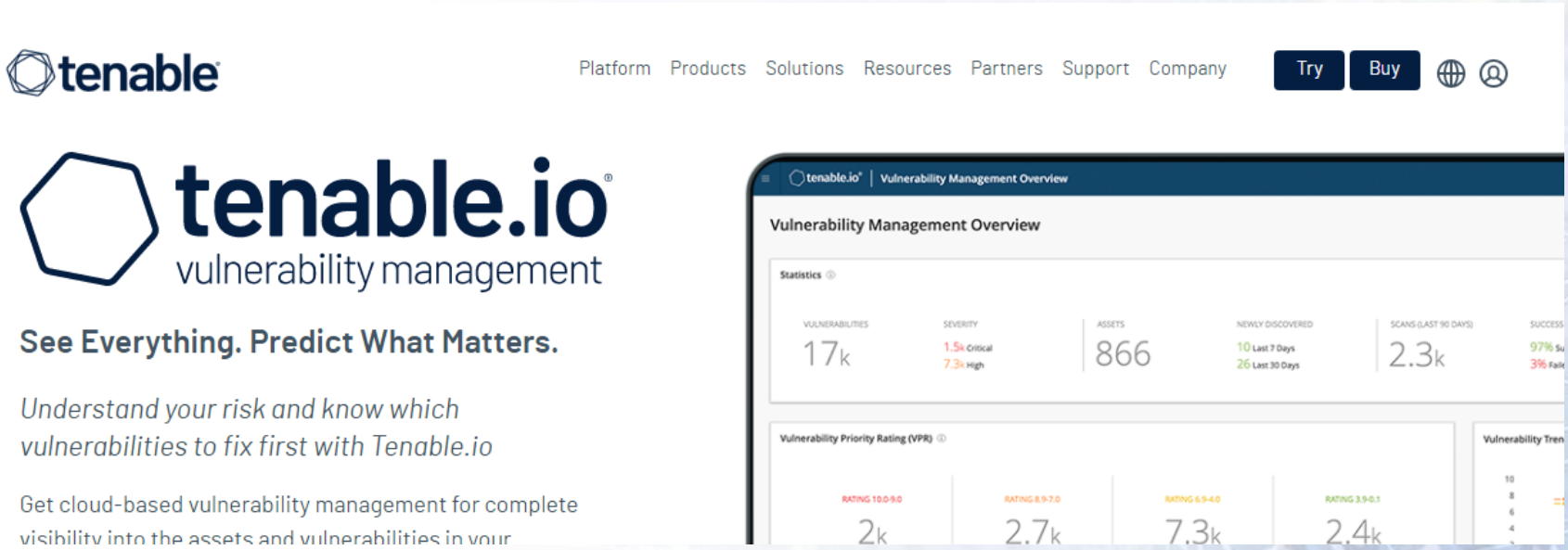


https://www.tenable.com/downloads/nessus?loginAttempted=true

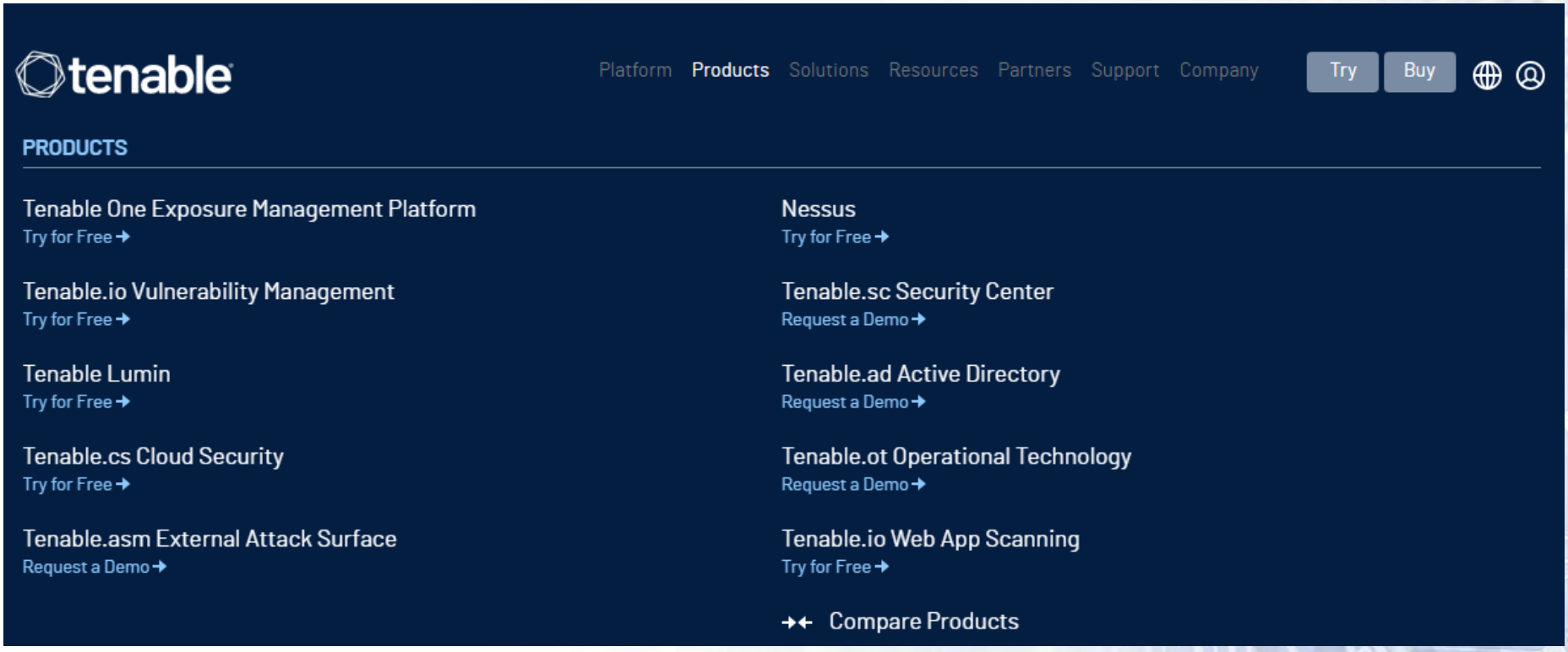


https://docs.tenable.com/nessus/Content/GettingStarted.htm

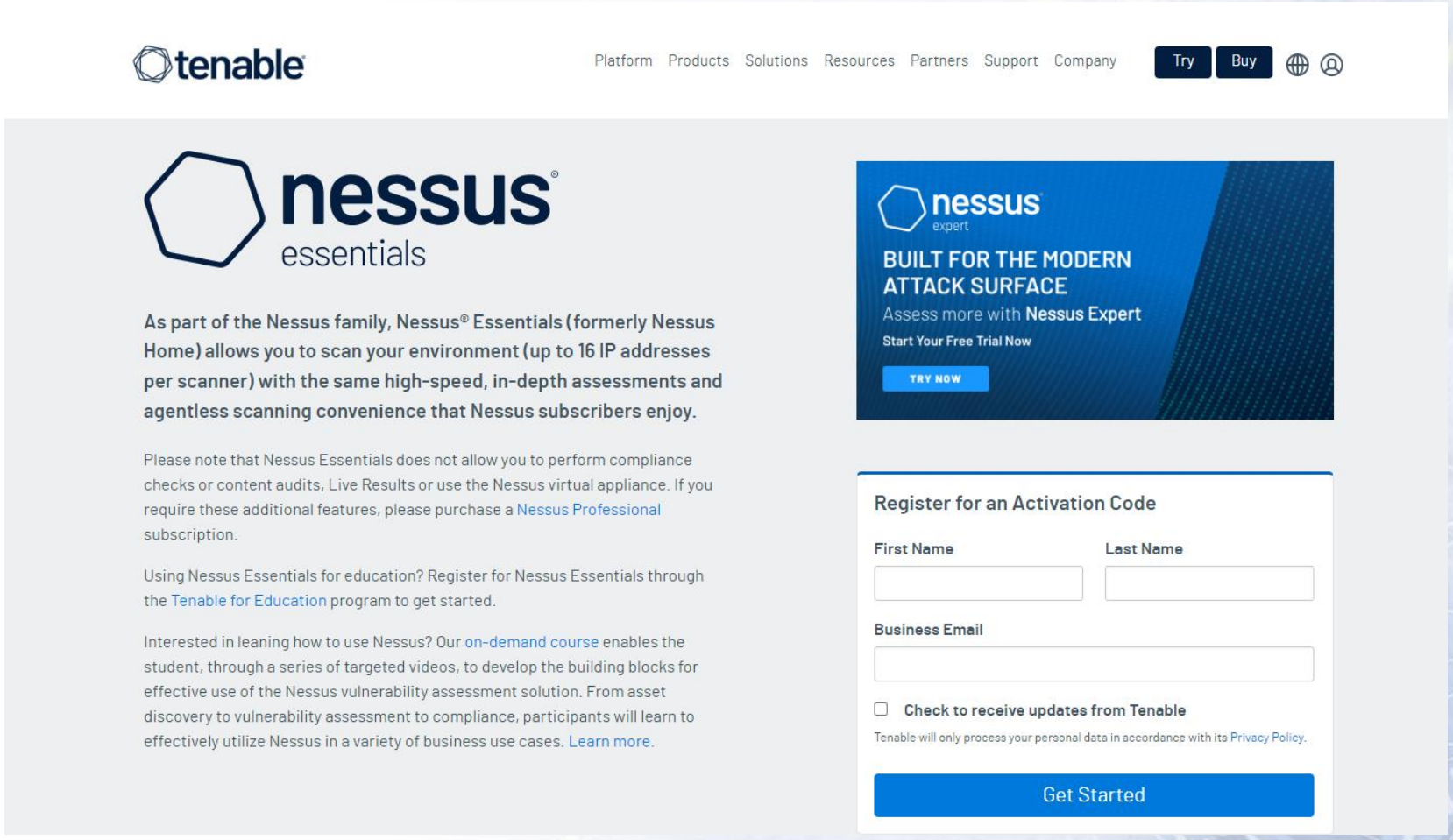
Cloud based service



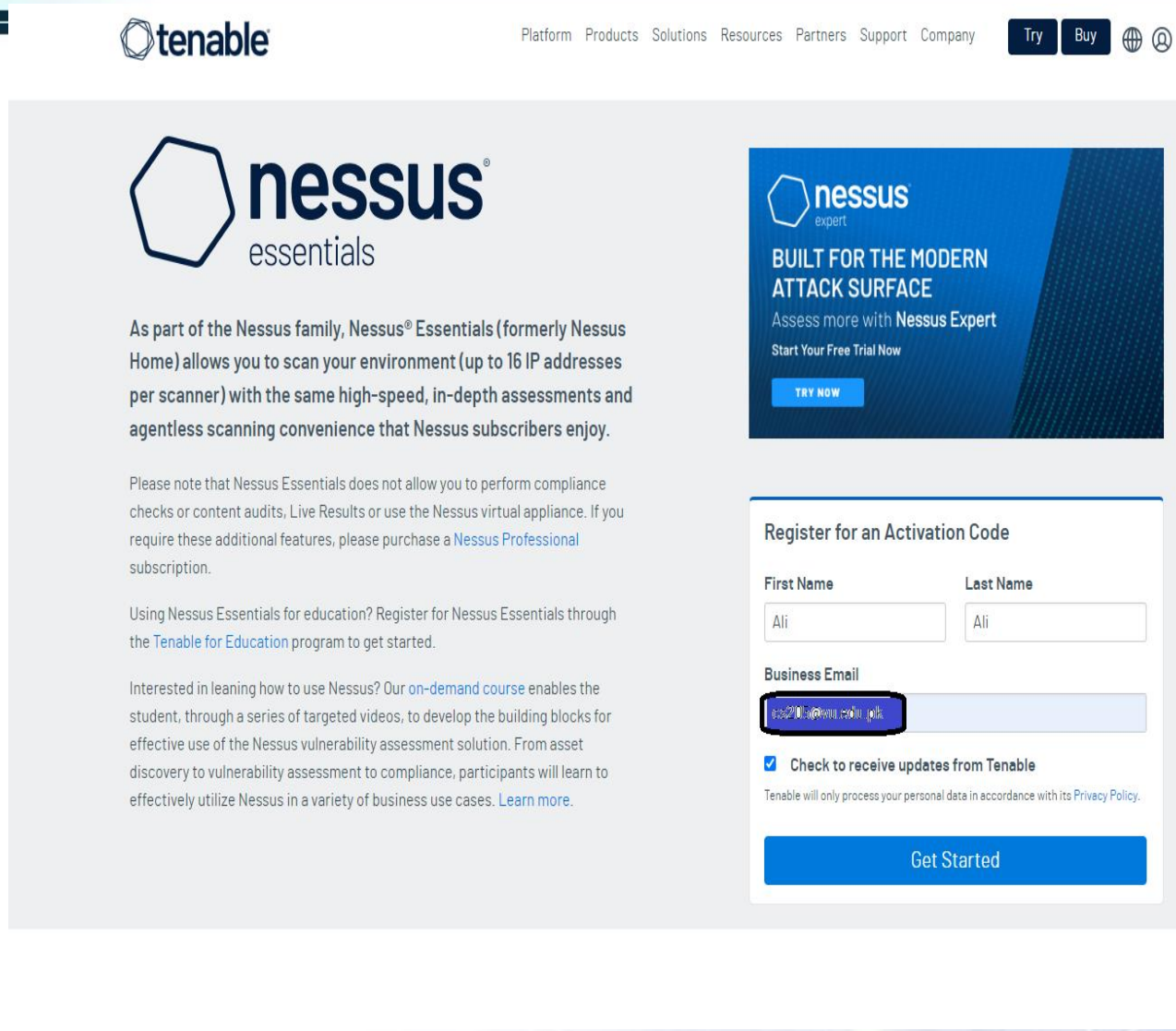

CLOSE YOUR CYBER EXPOSURE GAP WITH NESSUS
Tenable products help you accurately identify, investigate and prioritize vulnerabilities.
Secure your cloud, containers, OT devices and traditional IT assets.
RECOMMENDED
nessus expert
The #1 VA Solution
The most trusted vulnerability assessment solution now featuring Infrastructure as Code (IaC) and External Attack Surface Assessment!
Try for Free
nessus professional
l in Vulnerability Assessment
The industry-leading vulnerability scanner.

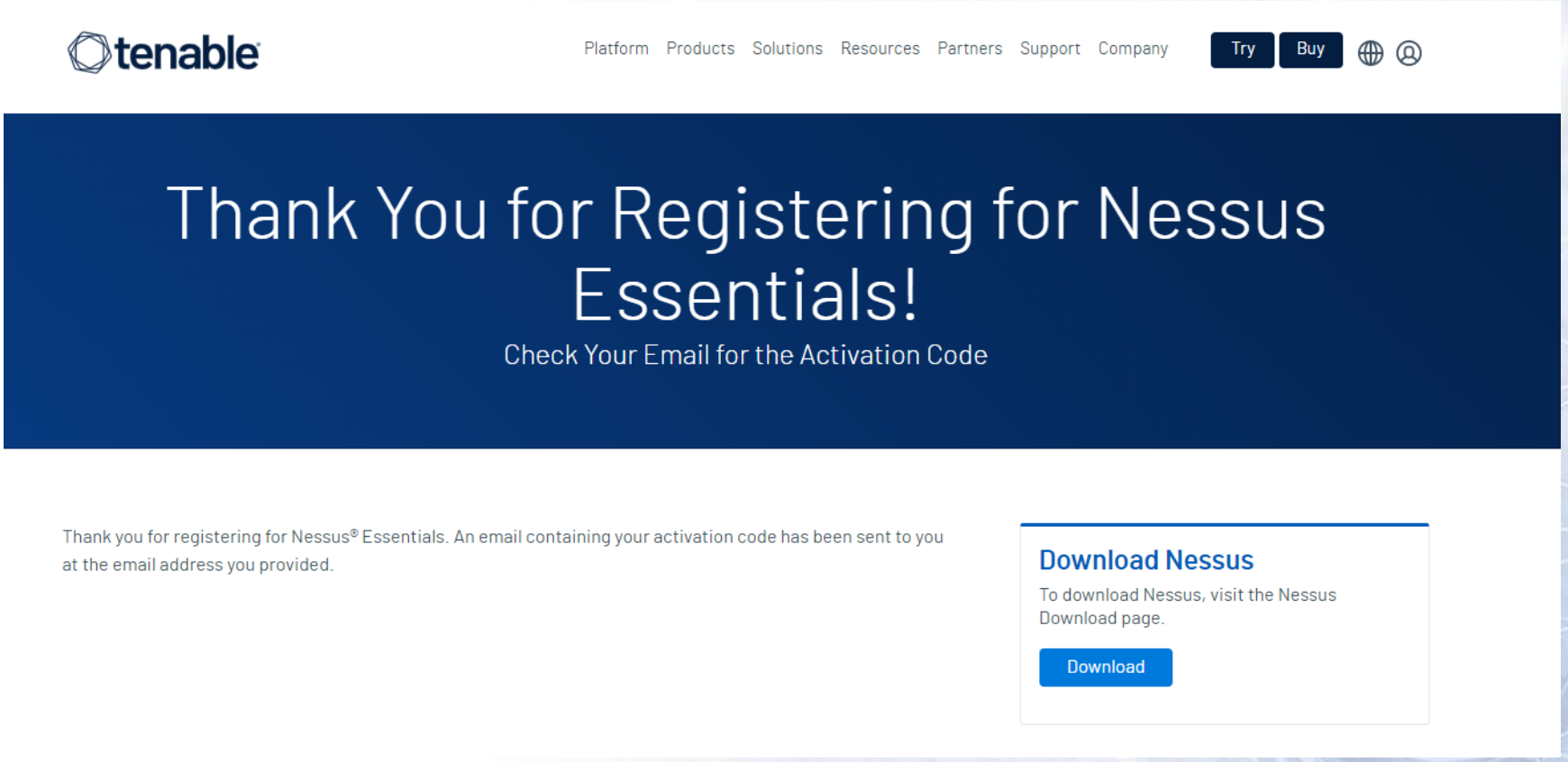

tenable
Platform
Products
Solutions
Resources
Partners
Support
Company
Try
Buy
PRODUCTS
Tenable One Exposure Management Platform
Try for Free
Tenable.io Vulnerability Management
Try for Free
Tenable Lumin
Try for Free
Tenable.cs Cloud Security
Try for Free
Tenable.asm External Attack Surface
Request a Demo
Nessus
Try for Free
Tenable.sc Security Center
Request a Demo
Tenable.ad Active Directory
Request a Demo
Tenable.ot Operational Technology
Request a Demo
Tenable.io Web App Scanning
Try for Free
Compare Products

NESUSS



https://www.tenable.com/products/nessus/nessus-essentials


tenable
Platform Products Solutions Resources Partners Support Company
Try Buy
nessus essentials
As part of the Nessus family, Nessus® Essentials (formerly Nessus Home) allows you to scan your environment (up to 16 IP addresses per scanner) with the same high-speed, in-depth assessments and agentless scanning convenience that Nessus subscribers enjoy.
Please note that Nessus Essentials does not allow you to perform compliance checks or content audits, Live Results or use the Nessus virtual appliance. If you require these additional features, please purchase a Nessus Professional subscription.
Using Nessus Essentials for education? Register for Nessus Essentials through the Tenable for Education program to get started.
Interested in leaning how to use Nessus? Our on-demand course enables the student, through a series of targeted videos, to develop the building blocks for effective use of the Nessus vulnerability assessment solution. From asset discovery to vulnerability assessment to compliance, participants will learn to effectively utilize Nessus in a variety of business use cases. Learn more.
nessus expert
BUILT FOR THE MODERN ATTACK SURFACE
Assess more with Nessus Expert
Start Your Free Trial Now
TRY NOW
Register for an Activation Code
First Name
Ali
Last Name
Ali
Business Email
Check to receive updates from Tenable
Tenable will only process your personal data in accordance with its Privacy Policy.
Get Started


tenable
Platform Products Solutions Resources Partners Support Company
Try Buy
Thank You for Registering for Nessus Essentials!
Check Your Email for the Activation Code
Thank you for registering for Nessus® Essentials. An email containing your activation code has been sent to you at the email address you provided.
Download Nessus
To download Nessus, visit the Nessus Download page.
Download

Welcome To Nessus Essentials

Welcome to Nessus Essentials and congratulations on taking action to secure your network! We offer the latest plugins for vulnerability scanning today, helping you identify more vulnerabilities and keep your network protected.

If you're looking for more advanced capabilities, such as live results and configuration checks – as well as the ability to scan unlimited IPs, check out Nessus Professional. To learn more view the Nessus Professional datasheet.

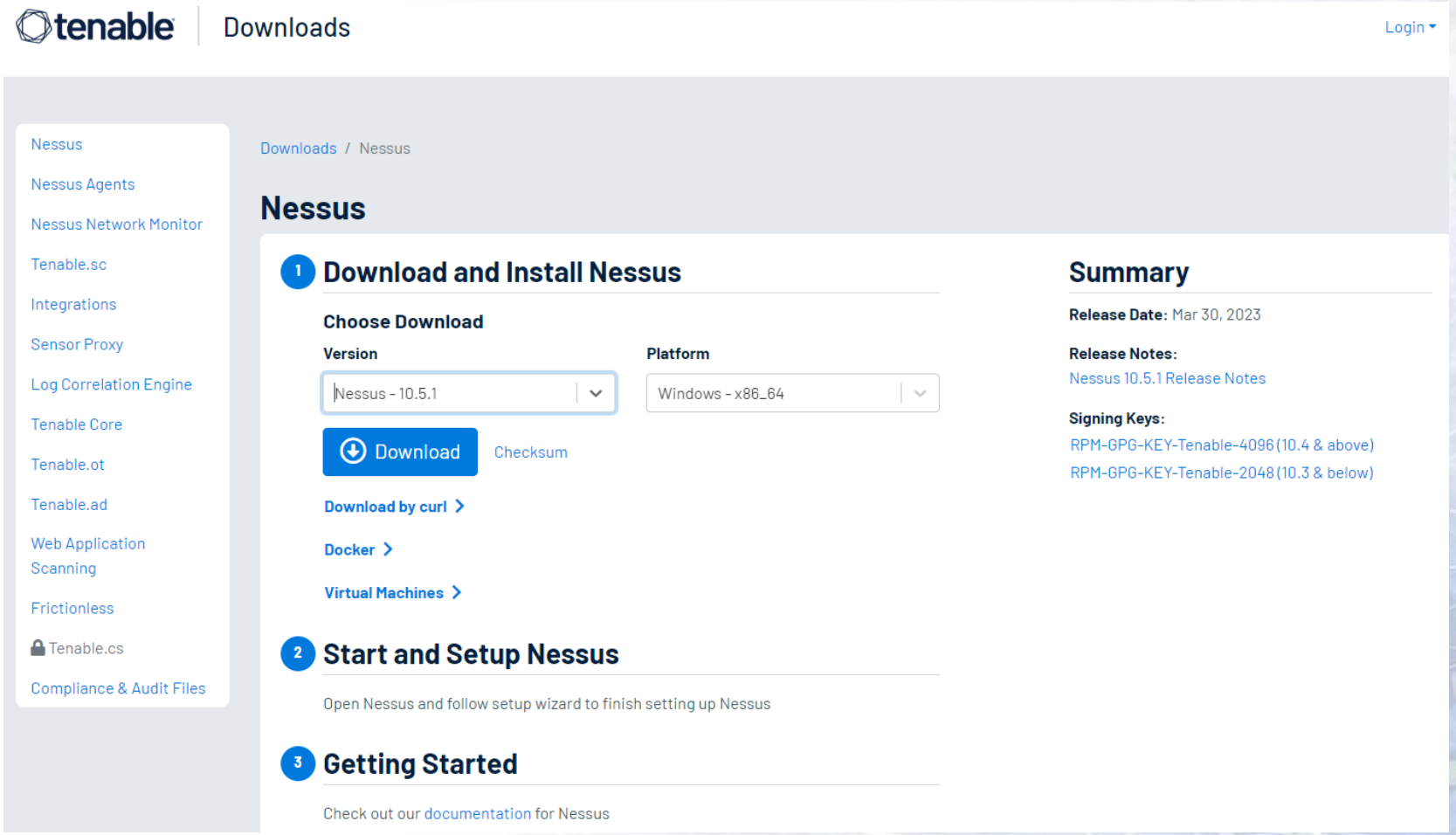
Activating Your Nessus Essentials License
Your activation code for Nessus Essentials is:
QC□U-2'I□-MZ□M-PKR□-48TF

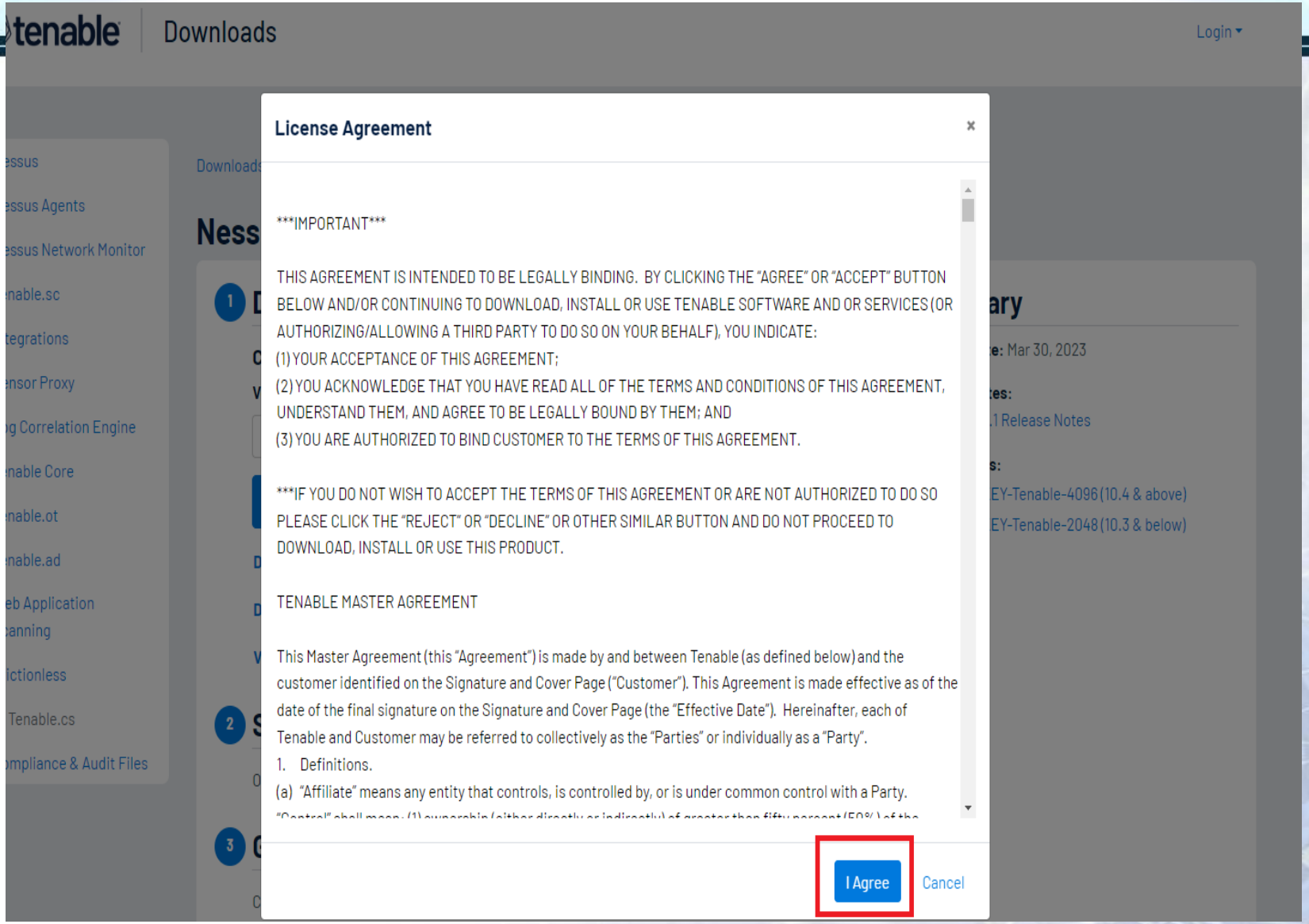
Download Nessus

This is a one-time code. If you uninstall and then reinstall you will need to register the scanner again and receive another activation code.

After initial installation of Nessus you will be prompted to set up and activate your scanner. For further details on activating your subscription review the installation guide.

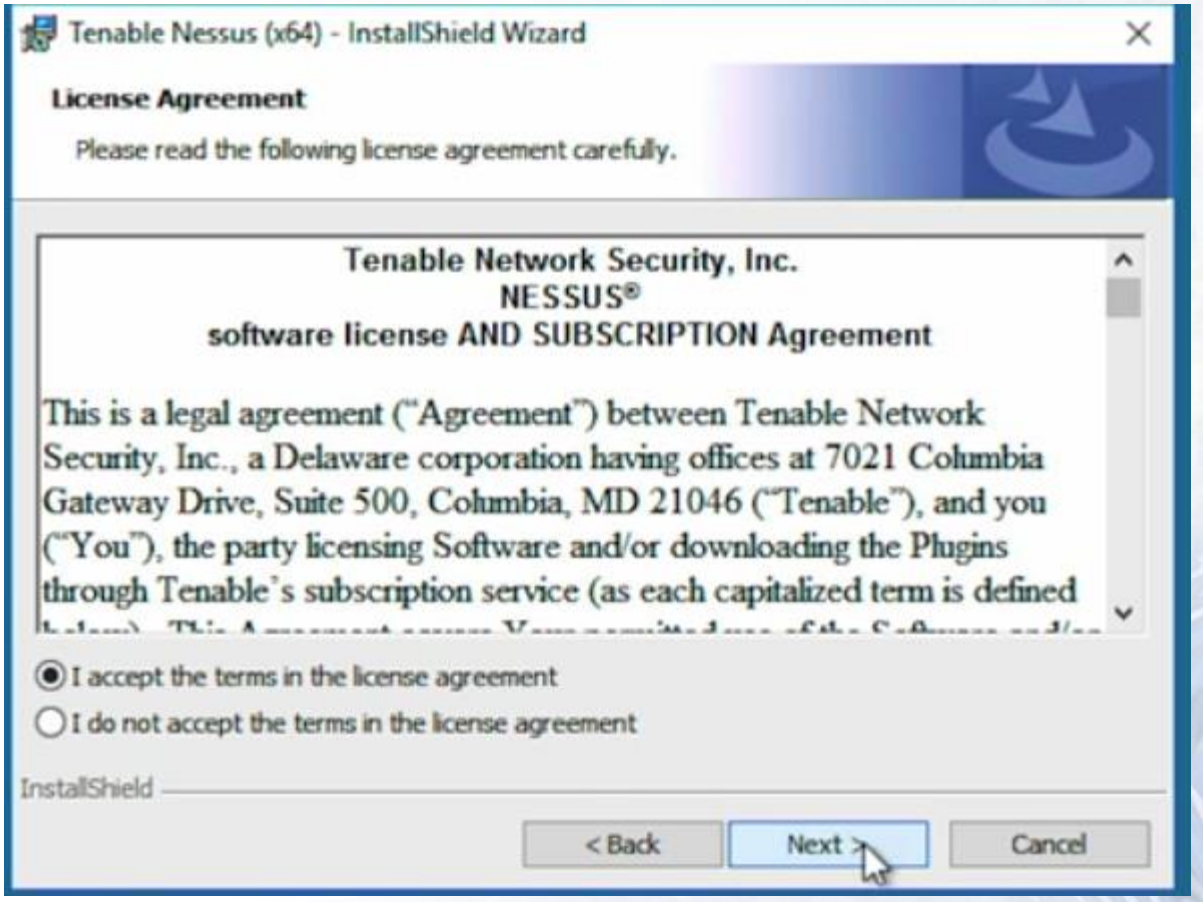
No internet access on your Nessus system?
If your Nessus installation cannot reach the internet directly, please follow the offline registration instructions.

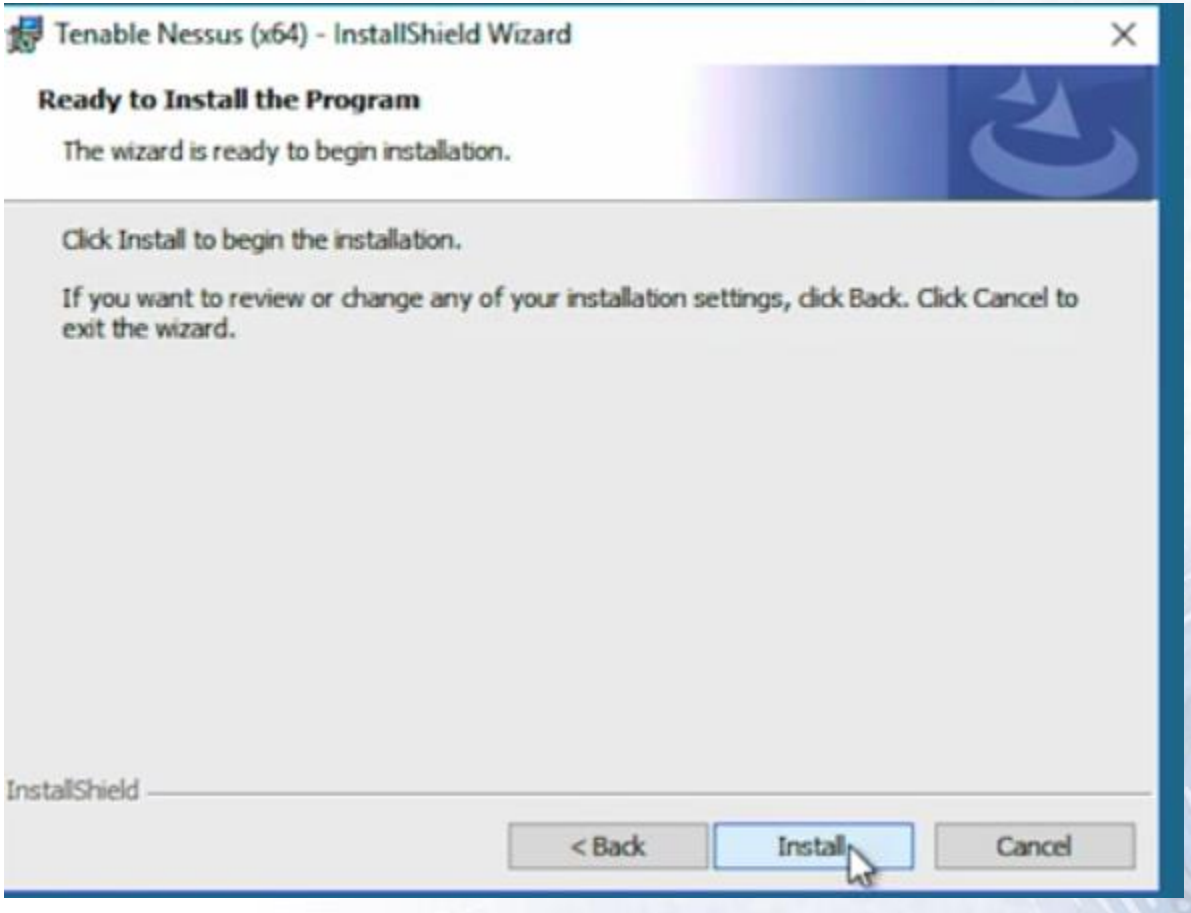

tenable
Downloads
Login
Nessus
Nessus Agents
Nessus Network Monitor
Tenable.sc
Integrations
Sensor Proxy
Log Correlation Engine
Tenable Core
Tenable.ot
Tenable.ad
Web Application Scanning
Frictionless
Tenable.cs
Compliance & Audit Files
Downloads / Nessus
Nessus
1 Download and Install Nessus
Choose Download
Version
Nessus - 10.5.1
Platform
Windows - x86_64
Download
Checksum
Download by curl
Docker
Virtual Machines
2 Start and Setup Nessus
Open Nessus and follow setup wizard to finish setting up Nessus
3 Getting Started
Check out our documentation for Nessus
Summary
Release Date: Mar 30, 2023
Release Notes:
Nessus 10.5.1 Release Notes
Signing Keys:
RPM-GPG-KEY-Tenable-4096 (10.4 & above)
RPM-GPG-KEY-Tenable-2048 (10.3 & below)

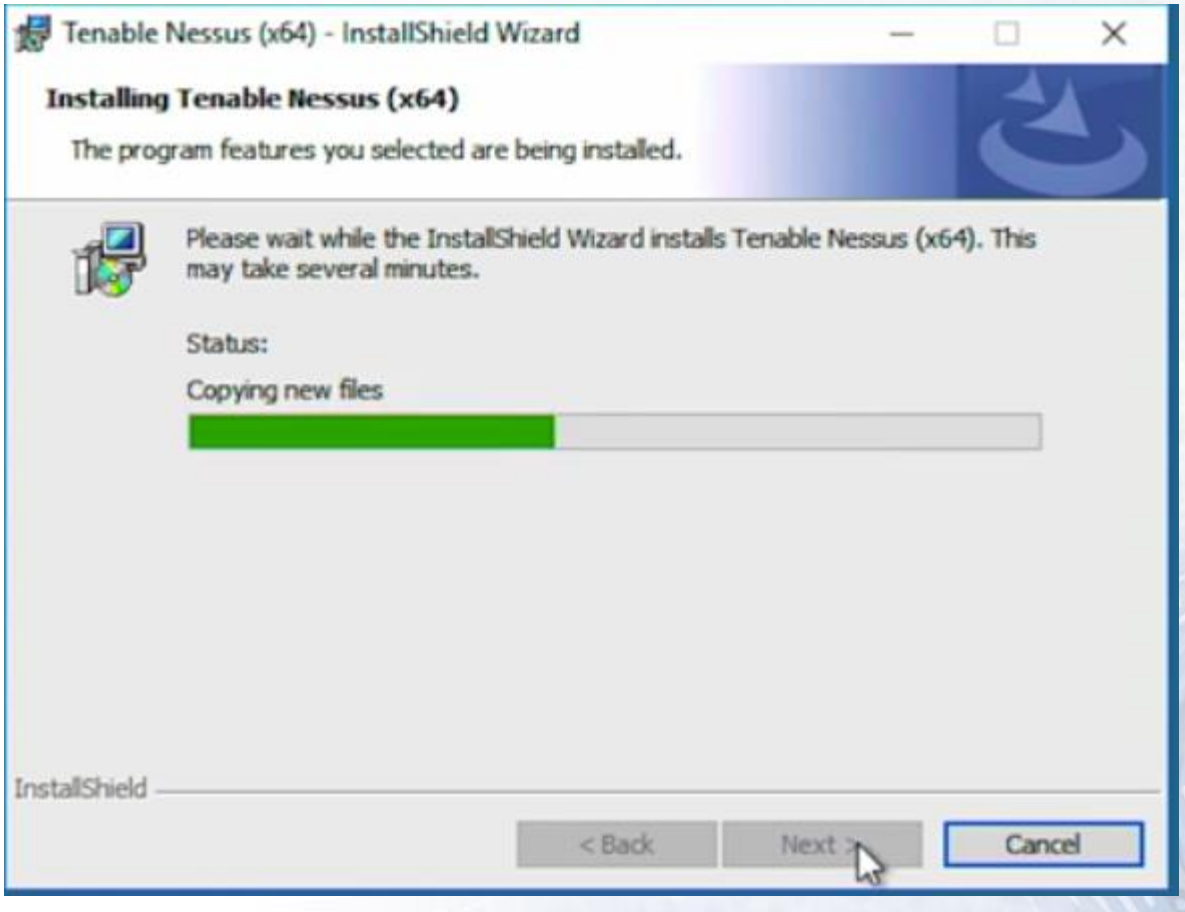

tenable
Downloads
Login
License Agreement
IMPORTANT
THIS AGREEMENT IS INTENDED TO BE LEGALLY BINDING. BY CLICKING THE "AGREE" OR "ACCEPT" BUTTON BELOW AND/OR CONTINUING TO DOWNLOAD, INSTALL OR USE TENABLE SOFTWARE AND OR SERVICES (OR AUTHORIZING/ALLOWING A THIRD PARTY TO DO SO ON YOUR BEHALF), YOU INDICATE:
(1) YOUR ACCEPTANCE OF THIS AGREEMENT;
(2) YOU ACKNOWLEDGE THAT YOU HAVE READ ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT, UNDERSTAND THEM, AND AGREE TO BE LEGALLY BOUND BY THEM; AND
(3) YOU ARE AUTHORIZED TO BIND CUSTOMER TO THE TERMS OF THIS AGREEMENT.
***IF YOU DO NOT WISH TO ACCEPT THE TERMS OF THIS AGREEMENT OR ARE NOT AUTHORIZED TO DO SO PLEASE CLICK THE "REJECT" OR "DECLINE" OR OTHER SIMILAR BUTTON AND DO NOT PROCEED TO DOWNLOAD, INSTALL OR USE THIS PRODUCT.
TENABLE MASTER AGREEMENT
This Master Agreement (this "Agreement") is made by and between Tenable (as defined below) and the customer identified on the Signature and Cover Page ("Customer"). This Agreement is made effective as of the date of the final signature on the Signature and Cover Page (the "Effective Date"). Hereinafter, each of Tenable and Customer may be referred to collectively as the "Parties" or individually as a "Party".
1. Definitions.
(a) "Affiliate" means any entity that controls, is controlled by, or is under common control with a Party.
I Agree
Cancel

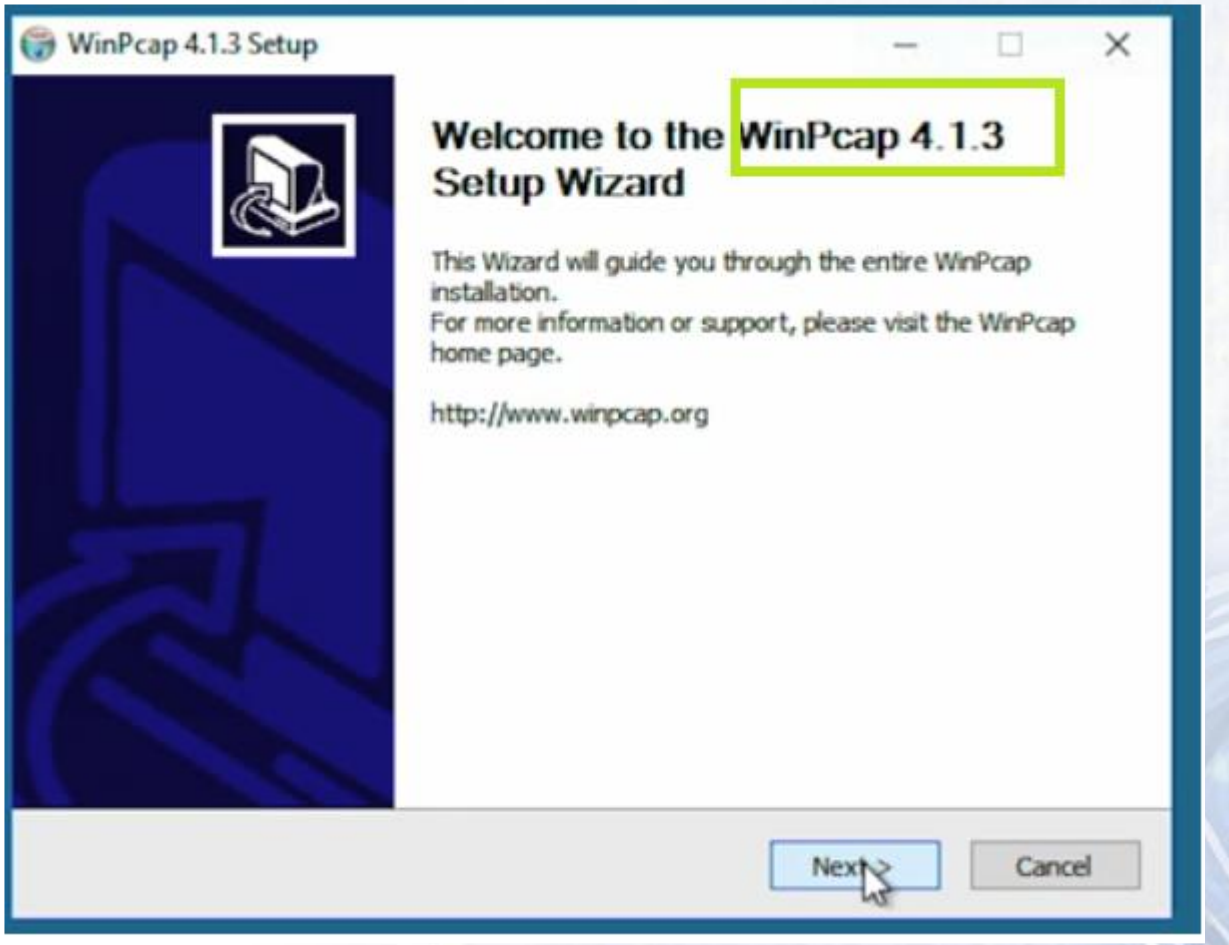

Open File - Security Warning
Do you want to run this file?
Name: ...\Users\Administrator\Downloads\Nessus-8.1.2-x64.msi
Publisher: Tenable Network Security Inc.
Type: Windows Installer Package
From: C:\Users\Administrator\Downloads\Nessus-8.1.2-x64....
Run
Cancel
Always ask before opening this file
While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust.
What's the risk?


Tenable Nessus (x64) - InstallShield Wizard
Welcome to the InstallShield Wizard for Tenable Nessus (x64)
The InstallShield(R) Wizard will install Tenable Nessus (x64) on your computer. To continue, click Next.
WARNING: This program is protected by copyright law and international treaties.
< Back
Next >
Cancel

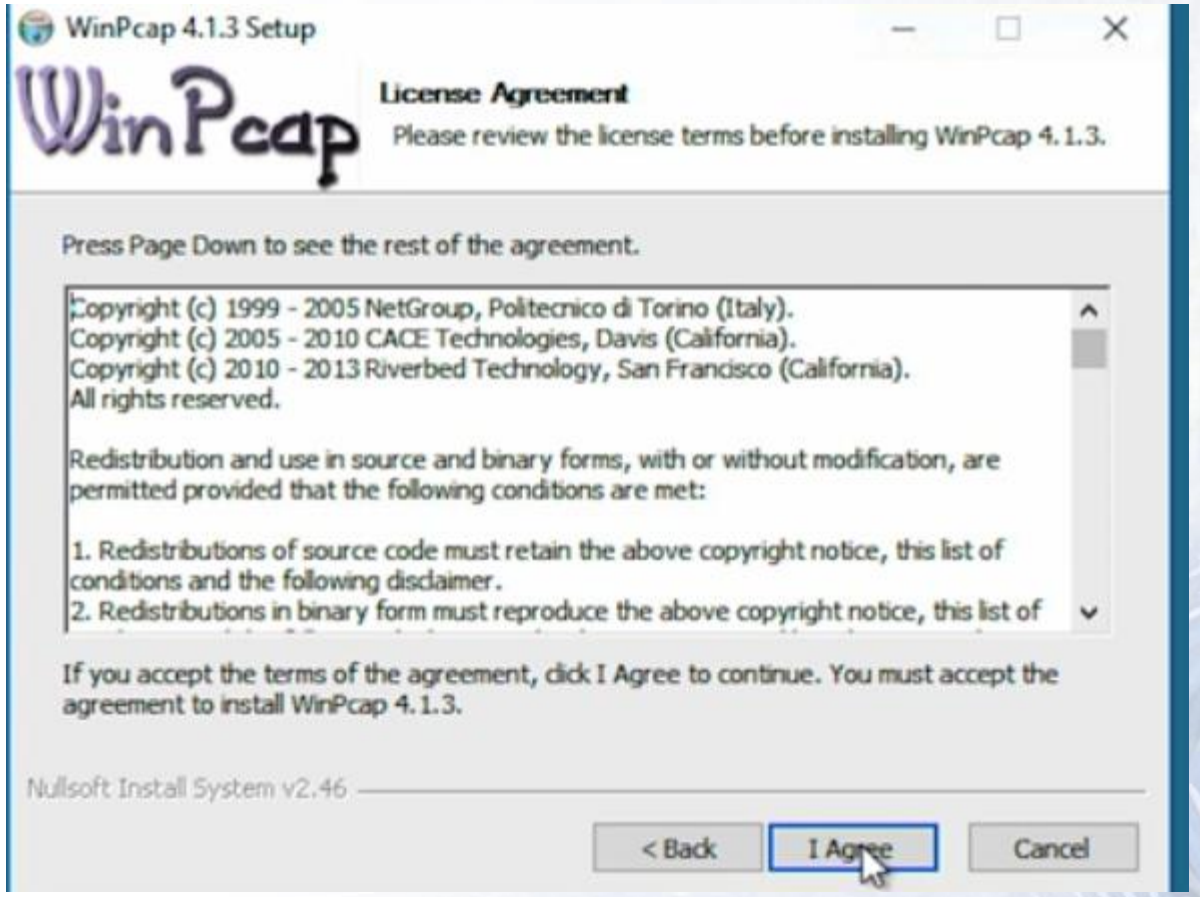

Tenable Nessus (x64) - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
Tenable Network Security, Inc.
NESSUS®
software license AND SUBSCRIPTION Agreement
This is a legal agreement ("Agreement") between Tenable Network Security, Inc., a Delaware corporation having offices at 7021 Columbia Gateway Drive, Suite 500, Columbia, MD 21046 ("Tenable"), and you ("You"), the party licensing Software and/or downloading the Plugins through Tenable's subscription service (as each capitalized term is defined
I accept the terms in the license agreement
I do not accept the terms in the license agreement
InstallShield
< Back
Next >
Cancel

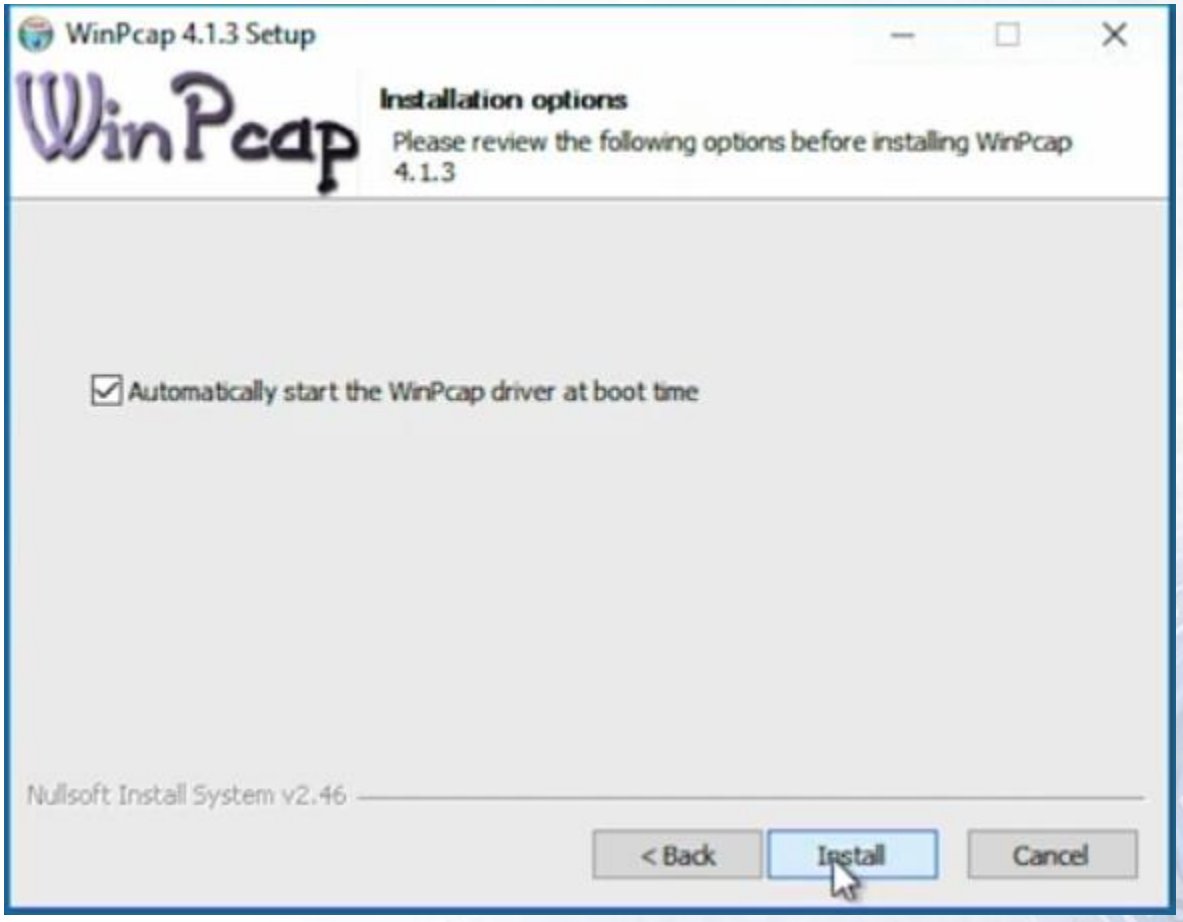

Tenable Nessus (x64) - InstallShield Wizard
Ready to Install the Program
The wizard is ready to begin installation.
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield
< Back
Install
Cancel


Tenable Nessus (x64) - InstallShield Wizard
Installing Tenable Nessus (x64)
The program features you selected are being installed.
Please wait while the InstallShield Wizard installs Tenable Nessus (x64). This may take several minutes.
Status:
Copying new files
InstallShield
< Back
Next >
Cancel

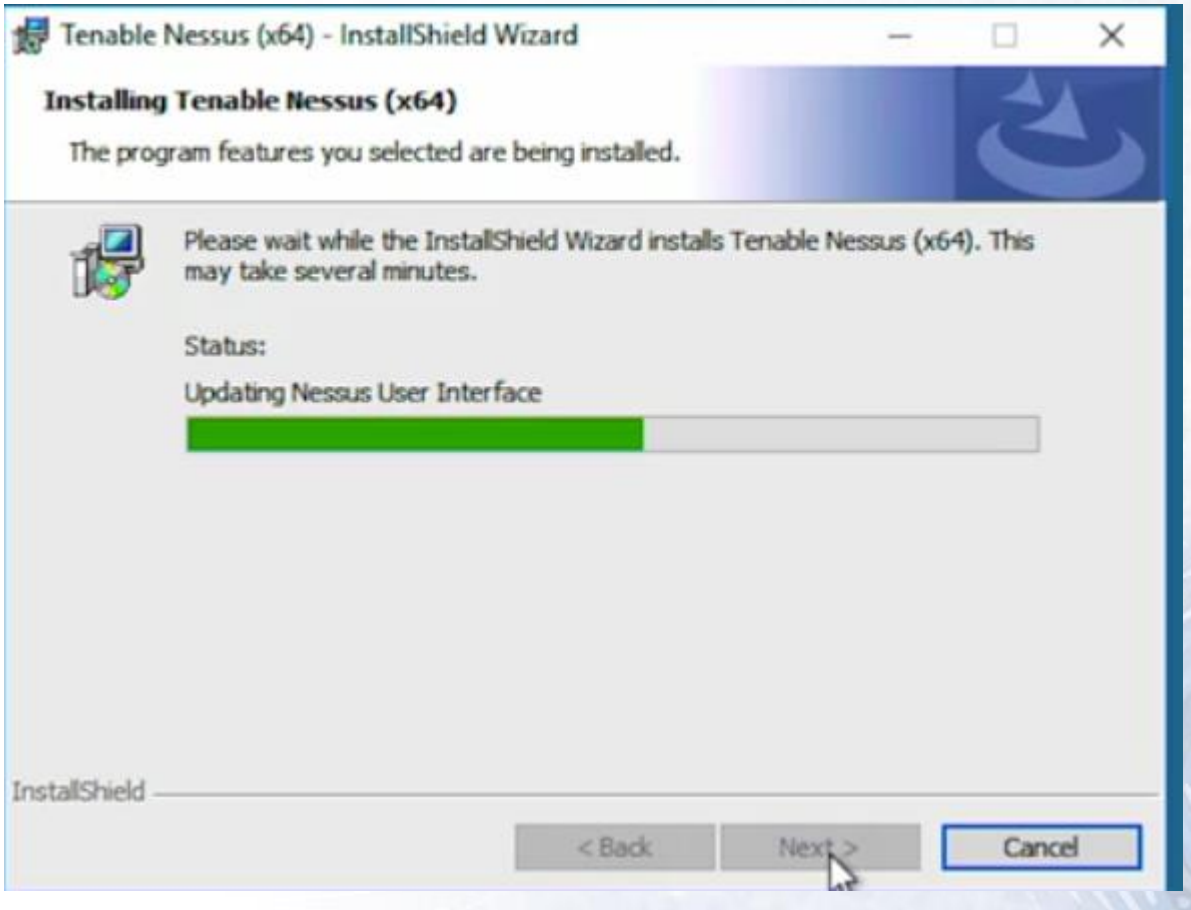

WinPcap 4.1.3 Setup
Welcome to the WinPcap 4.1.3 Setup Wizard
This Wizard will guide you through the entire WinPcap installation.
For more information or support, please visit the WinPcap home page.
http://www.winpcap.org
Next >
Cancel

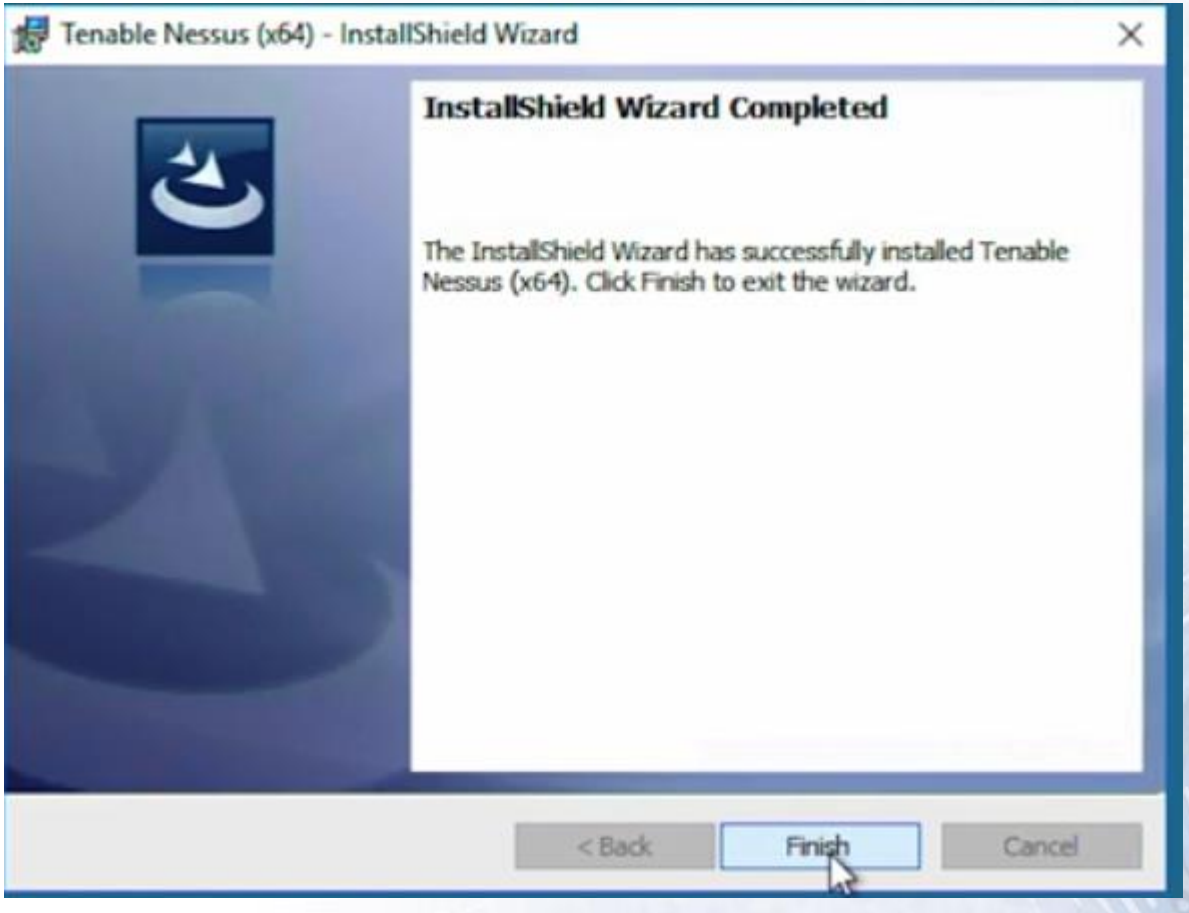
- Nessus installer realize that i don’t have windows packet capture library
- Nessus can’t work on winods without **WinPcap**


WinPcap 4.1.3 Setup
WinPcap
License Agreement
Please review the license terms before installing WinPcap 4.1.3.
Press Page Down to see the rest of the agreement.
Copyright (c) 1999 - 2005 NetGroup, Politecnico di Torino (Italy).
Copyright (c) 2005 - 2010 CACE Technologies, Davis (California).
Copyright (c) 2010 - 2013 Riverbed Technology, San Francisco (California).
All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install WinPcap 4.1.3.
Nullsoft Install System v2.46
< Back
I Agree
Cancel

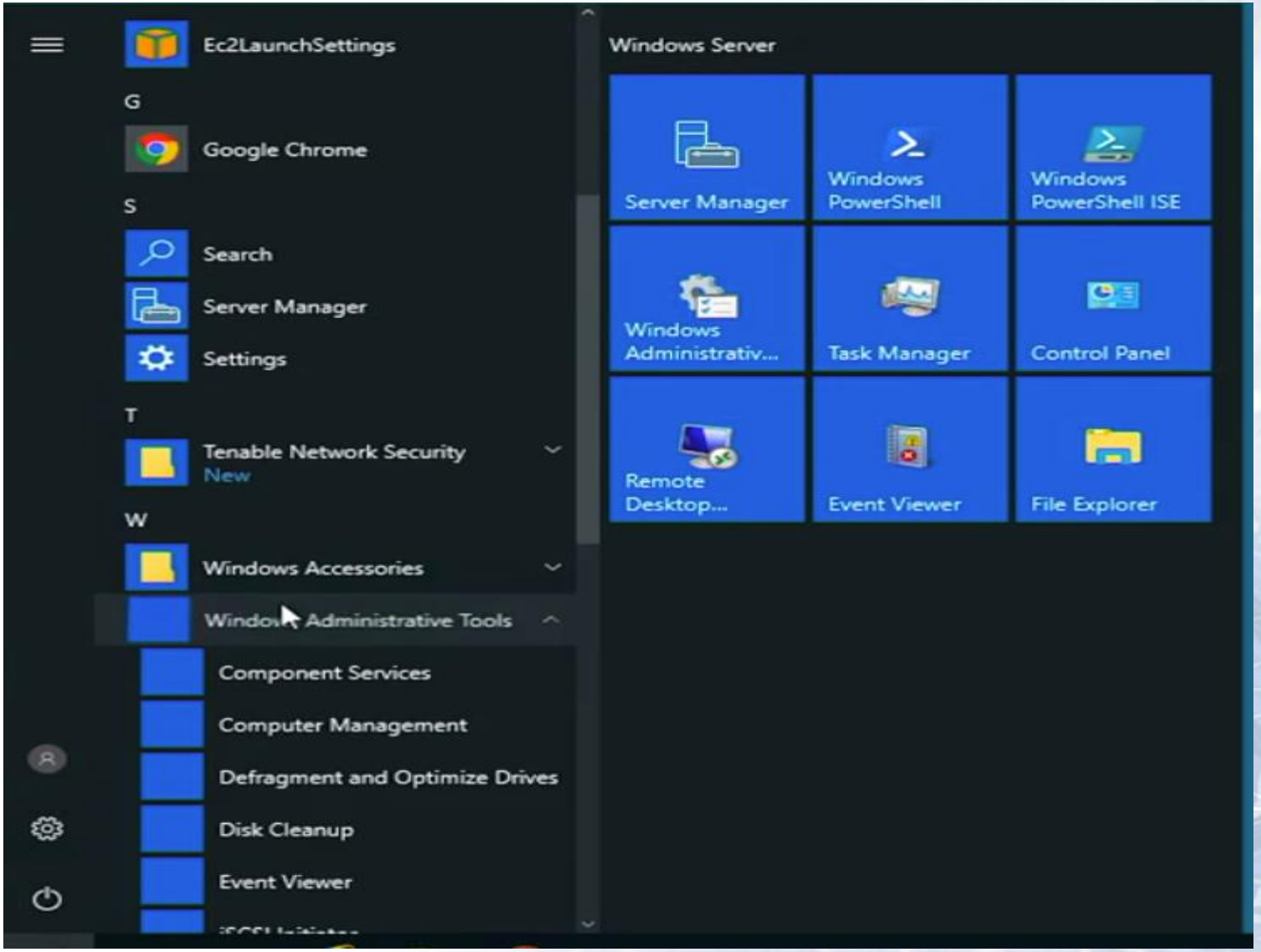

WinPcap 4.1.3 Setup
WinPcap
Installation options
Please review the following options before installing WinPcap 4.1.3
Automatically start the WinPcap driver at boot time
Nullsoft Install System v2.46
< Back
Install
Cancel


WinPcap 4.1.3 Setup
Completing the WinPcap 4.1.3 Setup Wizard
WinPcap 4.1.3 has been installed on your computer.
Click Finish to close this wizard.
< Back
Finish
Cancel

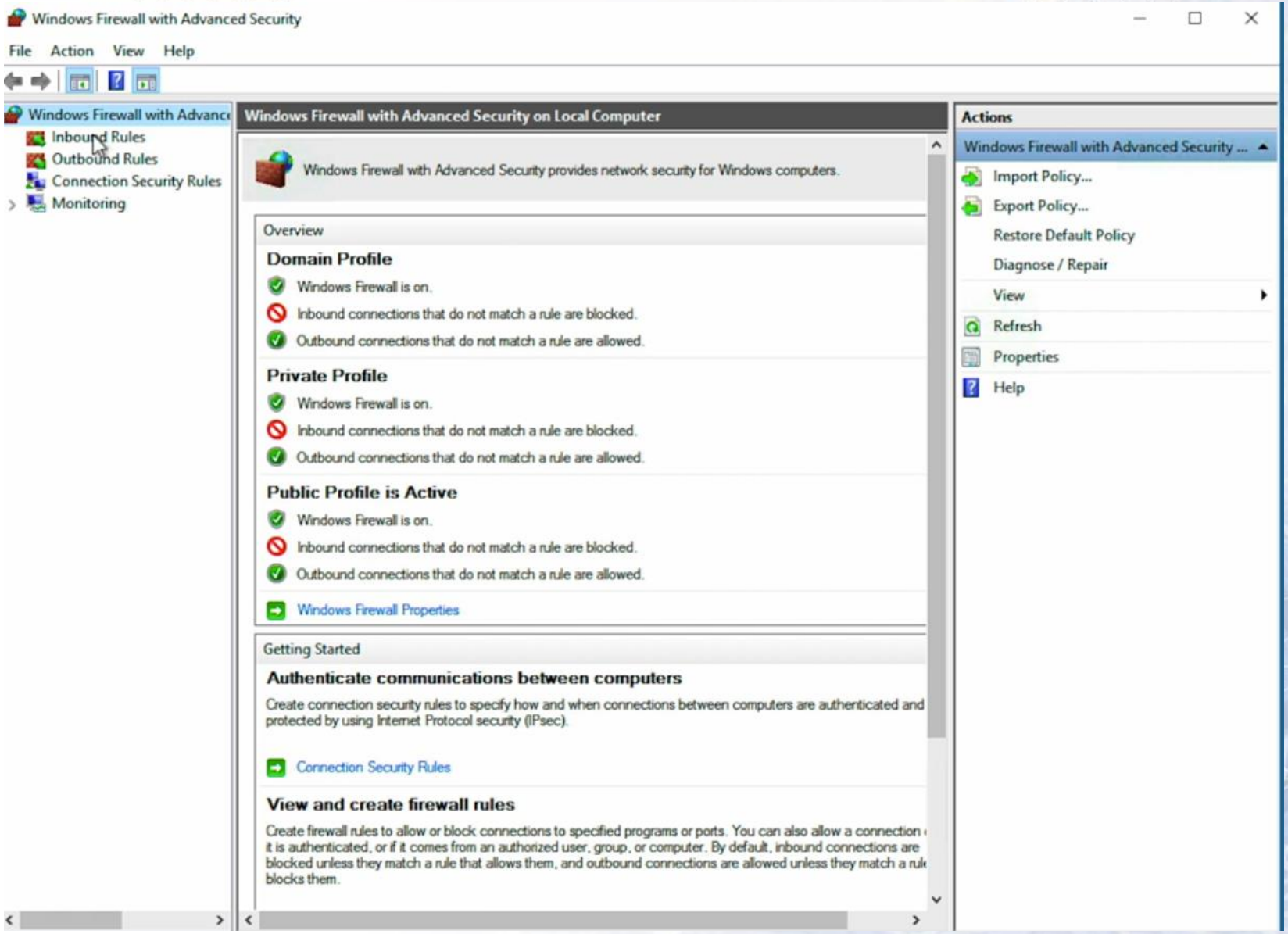

Tenable Nessus (x64) - InstallShield Wizard
Installing Tenable Nessus (x64)
The program features you selected are being installed.
Please wait while the InstallShield Wizard installs Tenable Nessus (x64). This may take several minutes.
Status:
Updating Nessus User Interface
InstallShield
< Back
Next >
Cancel

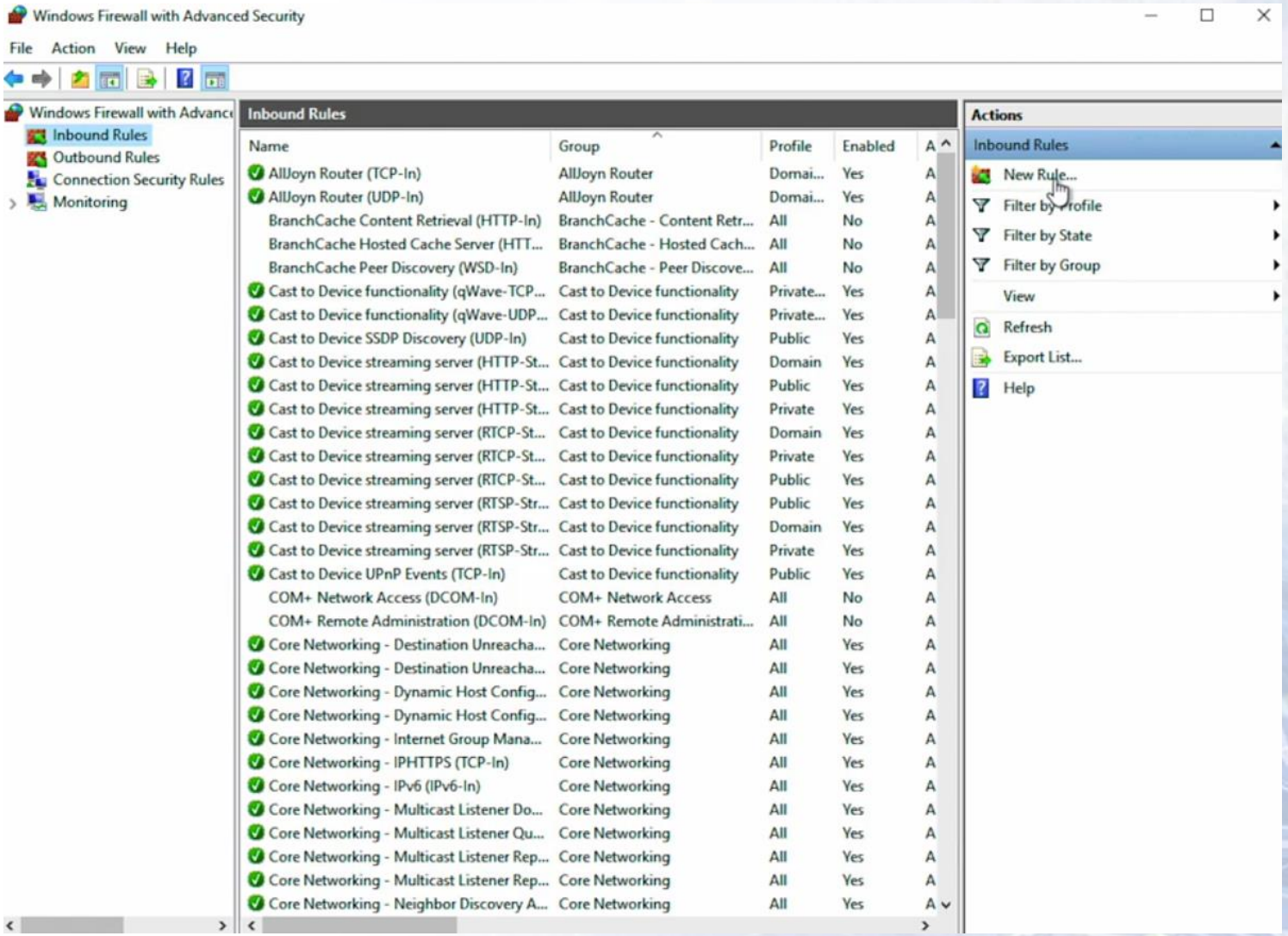

Tenable Nessus (x64) - InstallShield Wizard
InstallShield Wizard Completed
The InstallShield Wizard has successfully installed Tenable Nessus (x64). Click Finish to exit the wizard.
< Back
Finish
Cancel

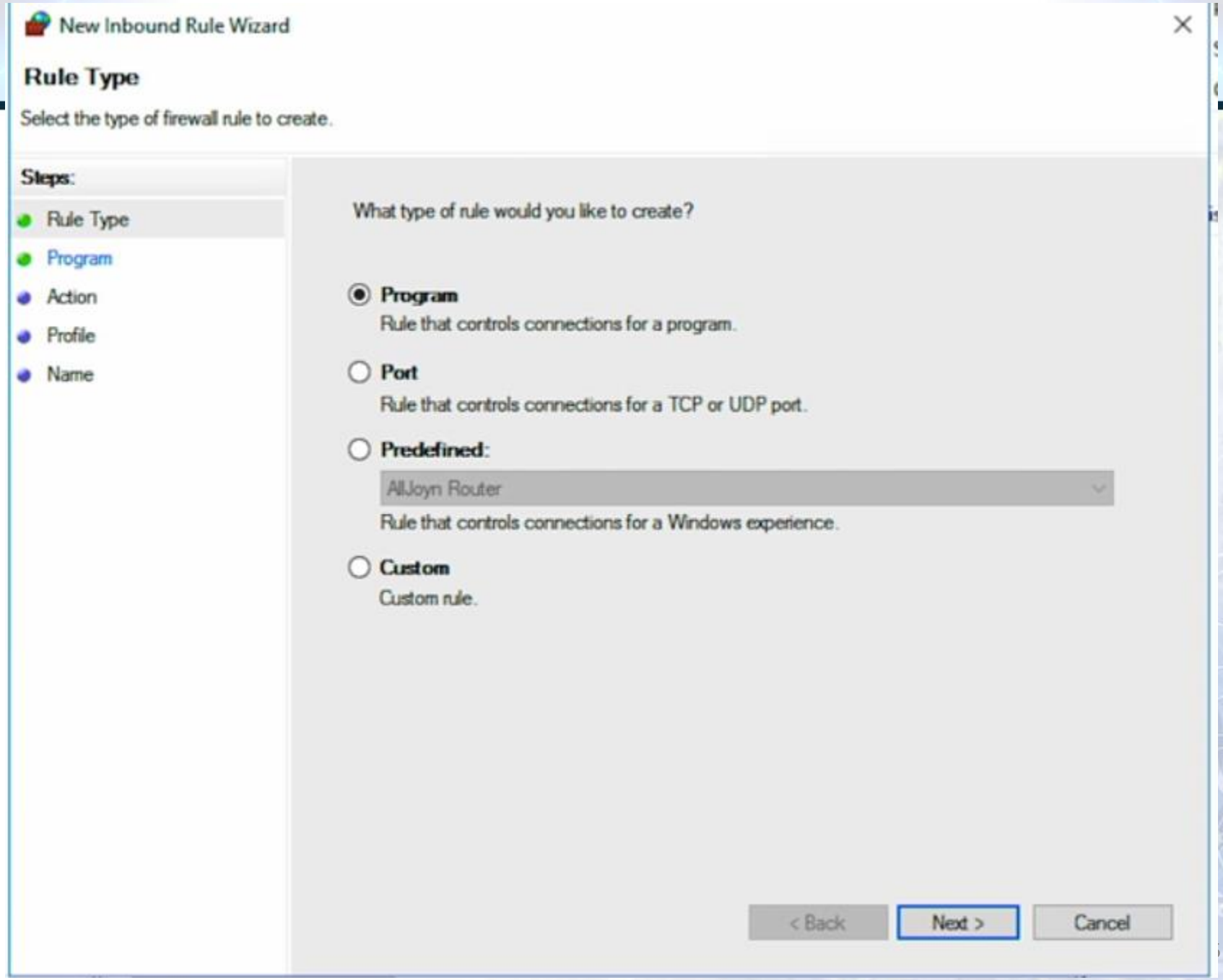
Nessus Manger use TCP port 8834

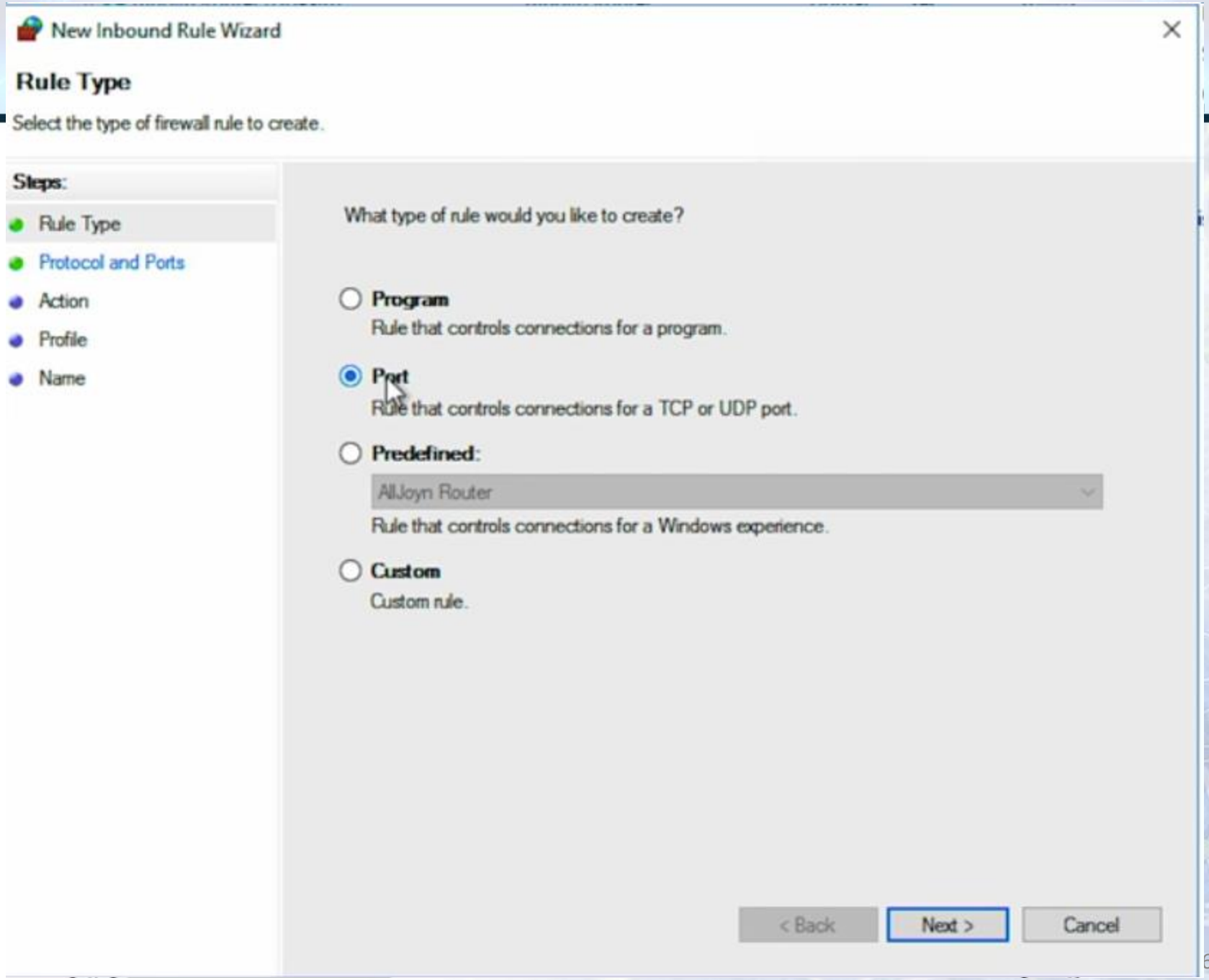

Ec2LaunchSettings
G
Google Chrome
S
Search
Server Manager
Settings
T
Tenable Network Security
New
W
Windows Accessories
Windows Administrative Tools
Component Services
Computer Management
Defragment and Optimize Drives
Disk Cleanup
Event Viewer
Windows Server
Server Manager
Windows PowerShell
Windows PowerShell ISE
Windows Administrativ...
Task Manager
Control Panel
Remote Desktop...
Event Viewer
File Explorer

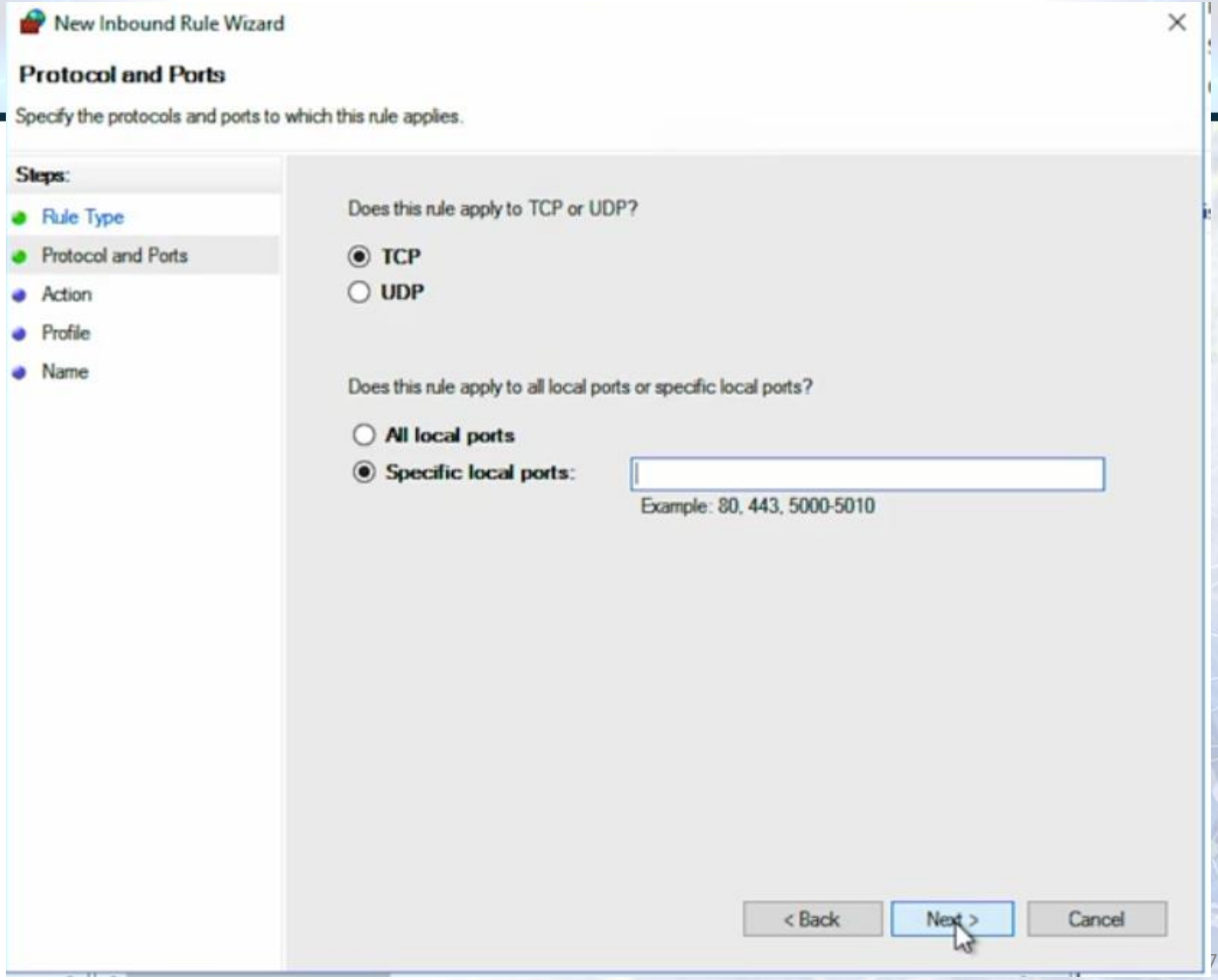

Computer Management
Defragment and Optimize Drives
Disk Cleanup
Event Viewer
iSCSI Initiator
Local Security Policy
Microsoft Azure Services
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Print Management
Resource Monitor
Services
System Configuration
System Information
Task Scheduler
Windows Firewall with Advanced...
Windows Memory Diagnostic
Windows Server
Server Manager
Windows PowerShell
Windows PowerShell ISE
Windows Administrativ...
Task Manager
Control Panel
Remote Desktop...
Event Viewer
File Explorer

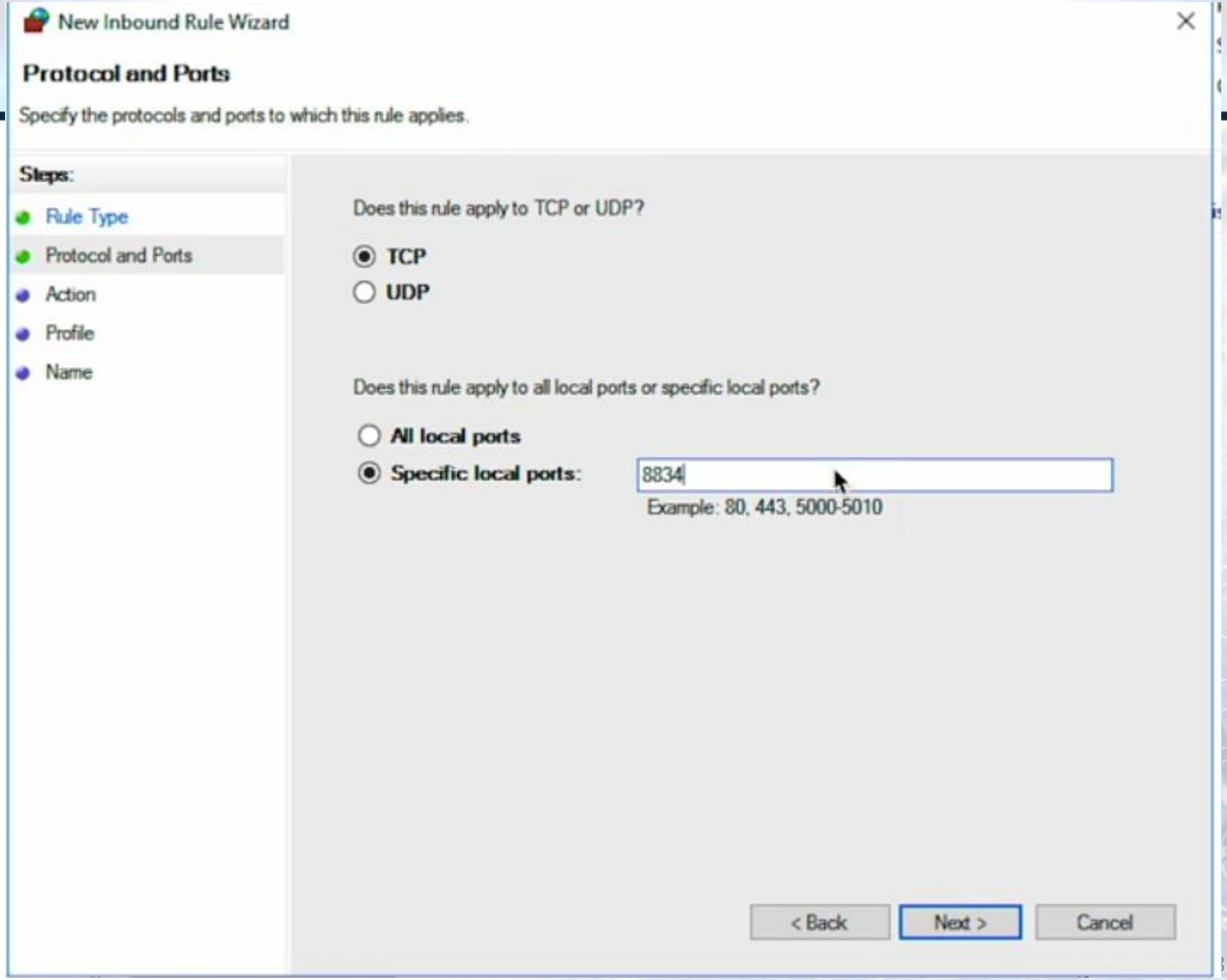

Windows Firewall with Advanced Security
File Action View Help
Windows Firewall with Advanc
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Windows Firewall with Advanced Security on Local Computer
Windows Firewall with Advanced Security provides network security for Windows computers.
Overview
Domain Profile
Windows Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Private Profile
Windows Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Public Profile is Active
Windows Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Windows Firewall Properties
Getting Started
Authenticate communications between computers
Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).
Connection Security Rules
View and create firewall rules
Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connection
it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections are
blocked unless they match a rule that allows them, and outbound connections are allowed unless they match a rul
blocks them.
Actions
Windows Firewall with Advanced Security ...
Import Policy...
Export Policy...
Restore Default Policy
Diagnose / Repair
View
Refresh
Properties
Help

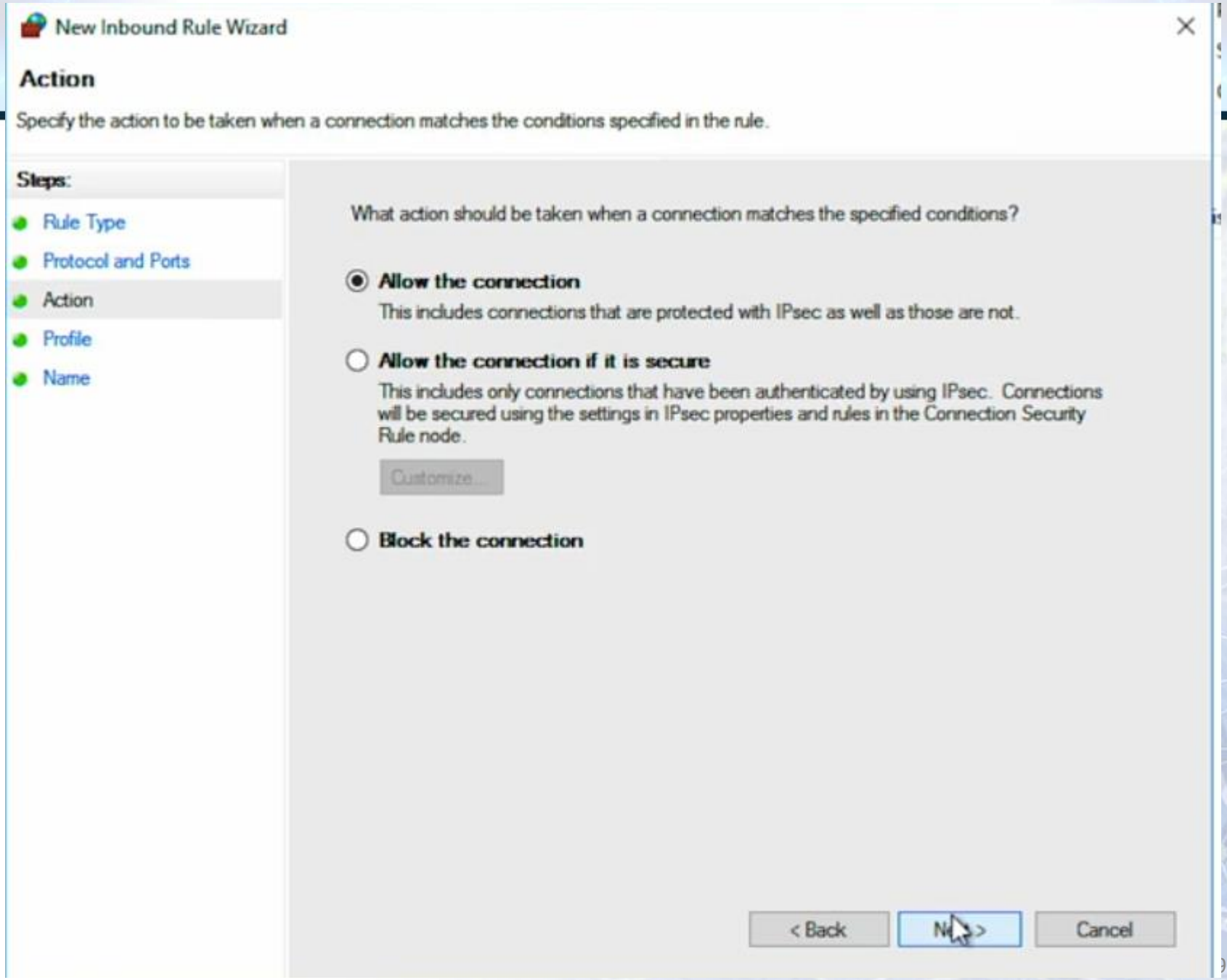

Windows Firewall with Advanced Security
File Action View Help
Windows Firewall with Advanc
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name | Group | Profile | Enabled
AllJoyn Router (TCP-In) | AllJoyn Router | Domai... | Yes
AllJoyn Router (UDP-In) | AllJoyn Router | Domai... | Yes
BranchCache Content Retrieval (HTTP-In) | BranchCache - Content Retr... | All | No
BranchCache Hosted Cache Server (HTT... | BranchCache - Hosted Cach... | All | No
BranchCache Peer Discovery (WSD-In) | BranchCache - Peer Discove... | All | No
Cast to Device functionality (qWave-TCP... | Cast to Device functionality | Private... | Yes
Cast to Device functionality (qWave-UDP... | Cast to Device functionality | Private... | Yes
Cast to Device SSDP Discovery (UDP-In) | Cast to Device functionality | Public | Yes
Cast to Device streaming server (HTTP-St... | Cast to Device functionality | Domain | Yes
Cast to Device streaming server (HTTP-St... | Cast to Device functionality | Public | Yes
Cast to Device streaming server (HTTP-St... | Cast to Device functionality | Private | Yes
Cast to Device streaming server (RTCP-St... | Cast to Device functionality | Domain | Yes
Cast to Device streaming server (RTCP-St... | Cast to Device functionality | Private | Yes
Cast to Device streaming server (RTCP-St... | Cast to Device functionality | Public | Yes
Cast to Device streaming server (RTSP-Str... | Cast to Device functionality | Public | Yes
Cast to Device streaming server (RTSP-Str... | Cast to Device functionality | Domain | Yes
Cast to Device streaming server (RTSP-Str... | Cast to Device functionality | Private | Yes
Cast to Device UPnP Events (TCP-In) | Cast to Device functionality | Public | Yes
COM+ Network Access (DCOM-In) | COM+ Network Access | All | No
COM+ Remote Administration (DCOM-In) | COM+ Remote Administrati... | All | No
Core Networking - Destination Unreacha... | Core Networking | All | Yes
Core Networking - Destination Unreacha... | Core Networking | All | Yes
Core Networking - Dynamic Host Config... | Core Networking | All | Yes
Core Networking - Dynamic Host Config... | Core Networking | All | Yes
Core Networking - Internet Group Mana... | Core Networking | All | Yes
Core Networking - IPHTTPS (TCP-In) | Core Networking | All | Yes
Core Networking - IPv6 (IPv6-In) | Core Networking | All | Yes
Core Networking - Multicast Listener Do... | Core Networking | All | Yes
Core Networking - Multicast Listener Qu... | Core Networking | All | Yes
Core Networking - Multicast Listener Rep... | Core Networking | All | Yes
Core Networking - Multicast Listener Rep... | Core Networking | All | Yes
Core Networking - Neighbor Discovery A... | Core Networking | All | Yes
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help

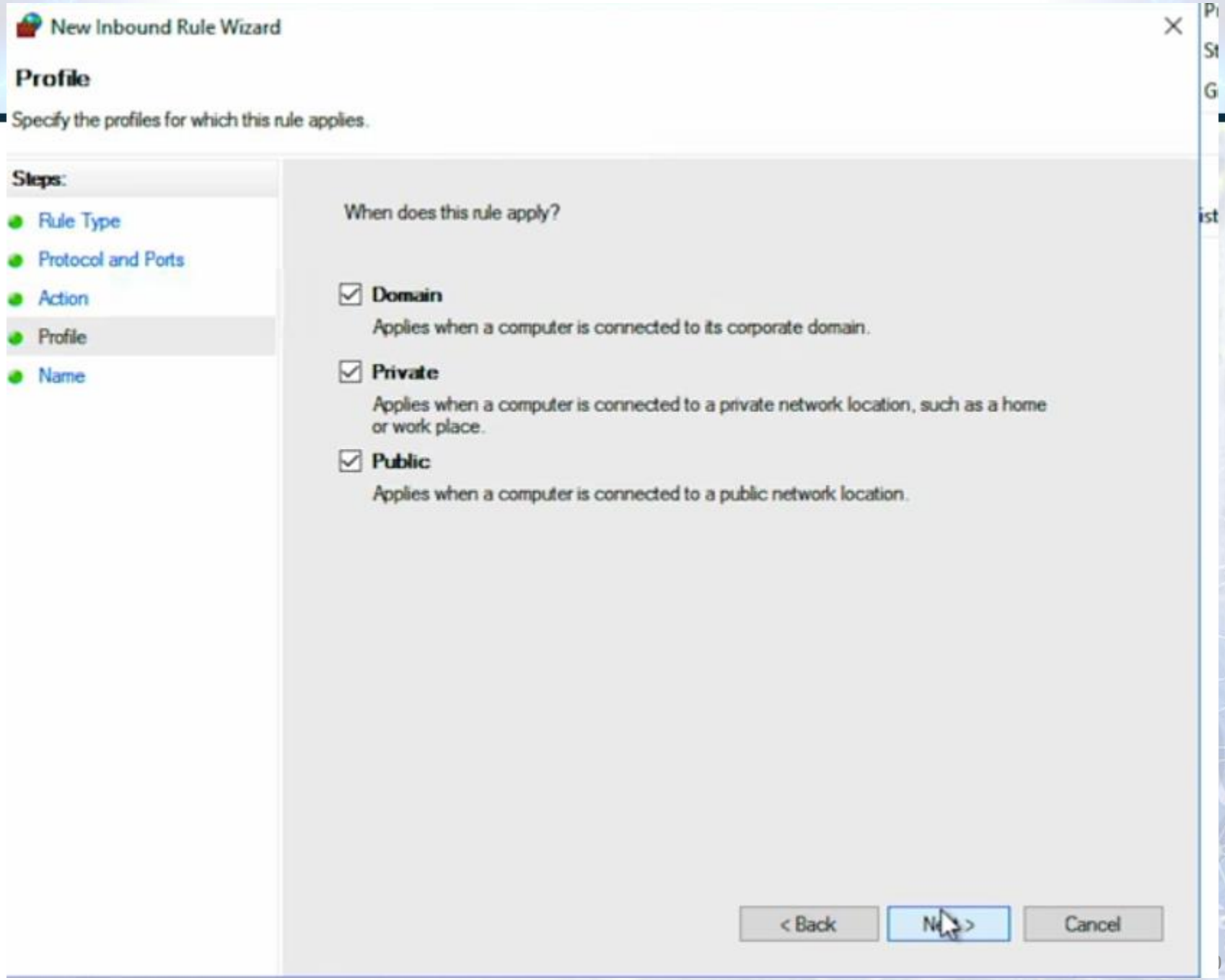

New Inbound Rule Wizard
Rule Type
Select the type of firewall rule to create.
Steps:
Rule Type
Program
Action
Profile
Name
What type of rule would you like to create?
Program
Rule that controls connections for a program.
Port
Rule that controls connections for a TCP or UDP port.
Predefined:
AllJoyn Router
Rule that controls connections for a Windows experience.
Custom
Custom rule.
< Back
Next >
Cancel

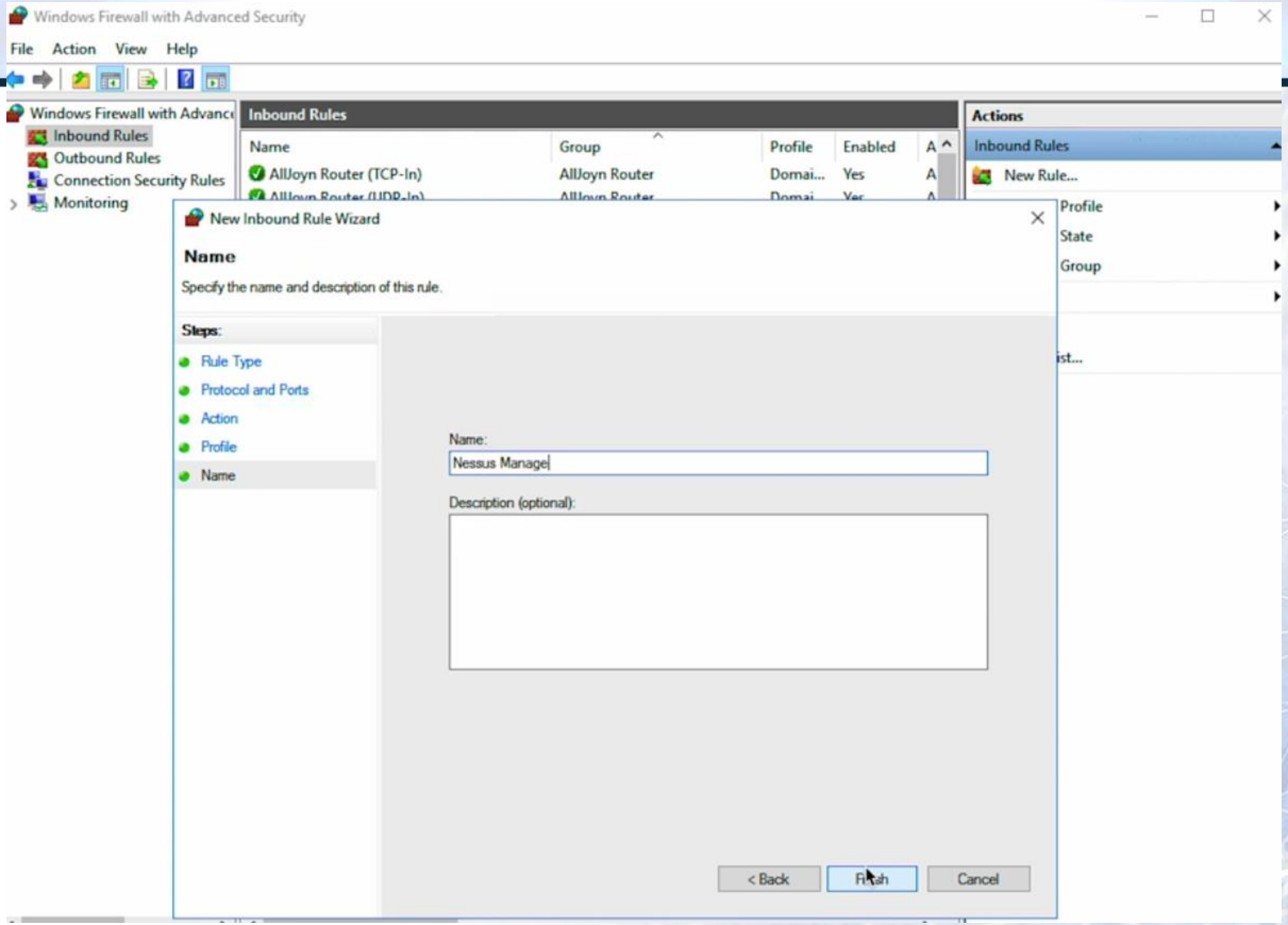

New Inbound Rule Wizard
Rule Type
Select the type of firewall rule to create.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
What type of rule would you like to create?
Program
Rule that controls connections for a program.
Port
Rule that controls connections for a TCP or UDP port.
Predefined:
AllJoyn Router
Rule that controls connections for a Windows experience.
Custom
Custom rule.
< Back
Next >
Cancel

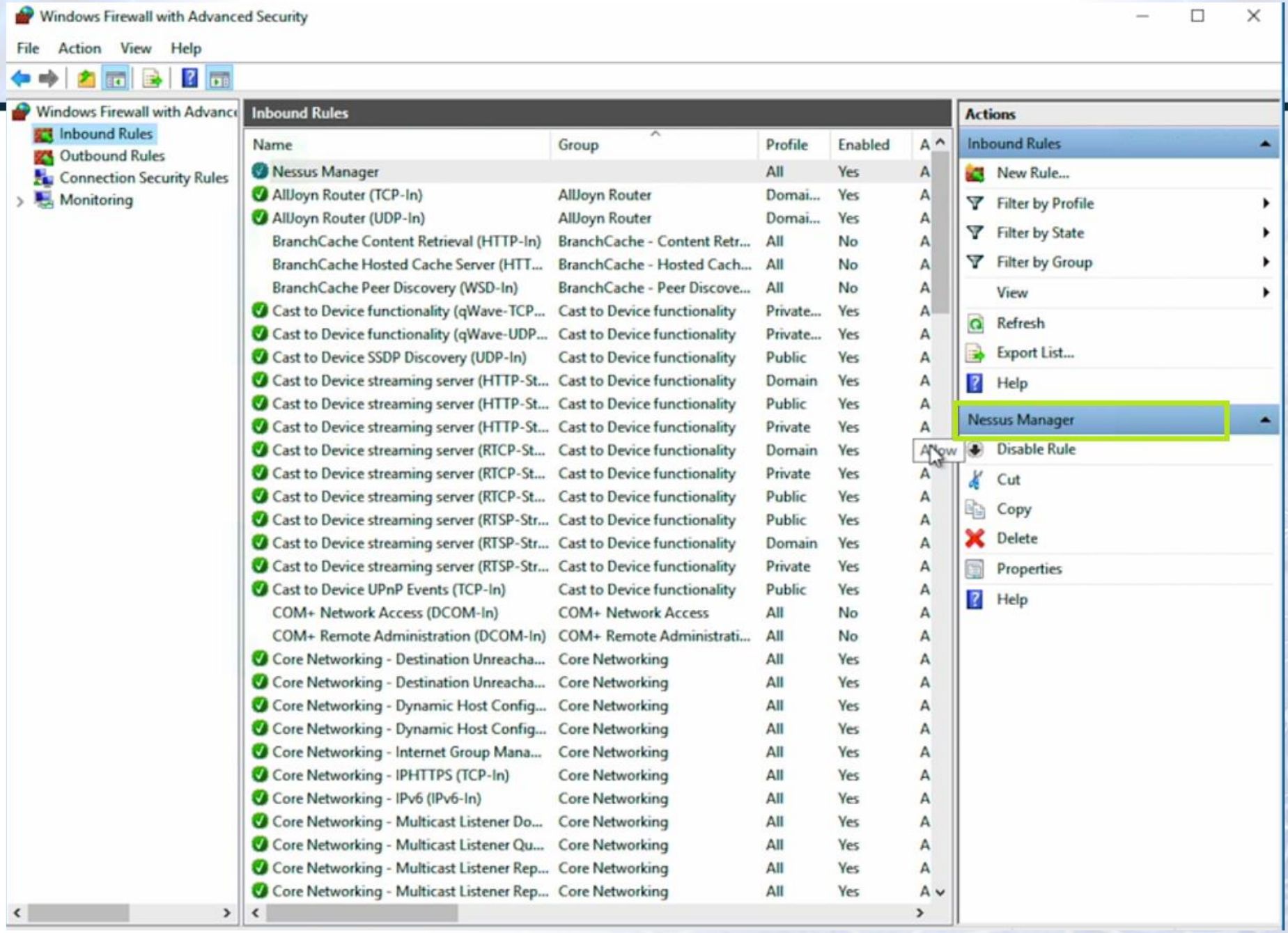

New Inbound Rule Wizard
Protocol and Ports
Specify the protocols and ports to which this rule applies.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
Does this rule apply to TCP or UDP?
TCP
UDP
Does this rule apply to all local ports or specific local ports?
All local ports
Specific local ports:
Example: 80, 443, 5000-5010
< Back
Next >
Cancel


New Inbound Rule Wizard
Protocol and Ports
Specify the protocols and ports to which this rule applies.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
Does this rule apply to TCP or UDP?
TCP
UDP
Does this rule apply to all local ports or specific local ports?
All local ports
Specific local ports:
8834
Example: 80, 443, 5000-5010
< Back
Next >
Cancel


New Inbound Rule Wizard
Action
Specify the action to be taken when a connection matches the conditions specified in the rule.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
What action should be taken when a connection matches the specified conditions?
Allow the connection
This includes connections that are protected with IPsec as well as those are not.
Allow the connection if it is secure
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
Customize...
Block the connection
< Back
Cancel


New Inbound Rule Wizard
Profile
Specify the profiles for which this rule applies.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
When does this rule apply?
Domain
Applies when a computer is connected to its corporate domain.
Private
Applies when a computer is connected to a private network location, such as a home or work place.
Public
Applies when a computer is connected to a public network location.
< Back
Cancel


Windows Firewall with Advanced Security
File Action View Help
Windows Firewall with Advanc
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name
Group
Profile
Enabled
AllJoyn Router (TCP-In)
AllJoyn Router
Domai...
Yes
Actions
Inbound Rules
New Rule...
Profile
State
Group
New Inbound Rule Wizard
Name
Specify the name and description of this rule.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
Name:
Nessus Manage
Description (optional):
< Back
Finish
Cancel


Windows Firewall with Advanced Security
File Action View Help
Windows Firewall with Advanc
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name Group Profile Enabled A
Nessus Manager All Yes A
AllJoyn Router (TCP-In) AllJoyn Router Domai... Yes A
AllJoyn Router (UDP-In) AllJoyn Router Domai... Yes A
BranchCache Content Retrieval (HTTP-In) BranchCache - Content Retr... All No A
BranchCache Hosted Cache Server (HTT... BranchCache - Hosted Cach... All No A
BranchCache Peer Discovery (WSD-In) BranchCache - Peer Discove... All No A
Cast to Device functionality (qWave-TCP... Cast to Device functionality Private... Yes A
Cast to Device functionality (qWave-UDP... Cast to Device functionality Private... Yes A
Cast to Device SSDP Discovery (UDP-In) Cast to Device functionality Public Yes A
Cast to Device streaming server (HTTP-St... Cast to Device functionality Domain Yes A
Cast to Device streaming server (HTTP-St... Cast to Device functionality Public Yes A
Cast to Device streaming server (HTTP-St... Cast to Device functionality Private Yes A
Cast to Device streaming server (RTCP-St... Cast to Device functionality Domain Yes A
Cast to Device streaming server (RTCP-St... Cast to Device functionality Private Yes A
Cast to Device streaming server (RTCP-St... Cast to Device functionality Public Yes A
Cast to Device streaming server (RTSP-Str... Cast to Device functionality Public Yes A
Cast to Device streaming server (RTSP-Str... Cast to Device functionality Domain Yes A
Cast to Device streaming server (RTSP-Str... Cast to Device functionality Private Yes A
Cast to Device UPnP Events (TCP-In) Cast to Device functionality Public Yes A
COM+ Network Access (DCOM-In) COM+ Network Access All No A
COM+ Remote Administration (DCOM-In) COM+ Remote Administrati... All No A
Core Networking - Destination Unreacha... Core Networking All Yes A
Core Networking - Destination Unreacha... Core Networking All Yes A
Core Networking - Dynamic Host Config... Core Networking All Yes A
Core Networking - Dynamic Host Config... Core Networking All Yes A
Core Networking - Internet Group Mana... Core Networking All Yes A
Core Networking - IPHTTPS (TCP-In) Core Networking All Yes A
Core Networking - IPv6 (IPv6-In) Core Networking All Yes A
Core Networking - Multicast Listener Do... Core Networking All Yes A
Core Networking - Multicast Listener Qu... Core Networking All Yes A
Core Networking - Multicast Listener Rep... Core Networking All Yes A
Core Networking - Multicast Listener Rep... Core Networking All Yes A
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
Nessus Manager
Disable Rule
Cut
Copy
Delete
Properties
Help

Accessing Nessus

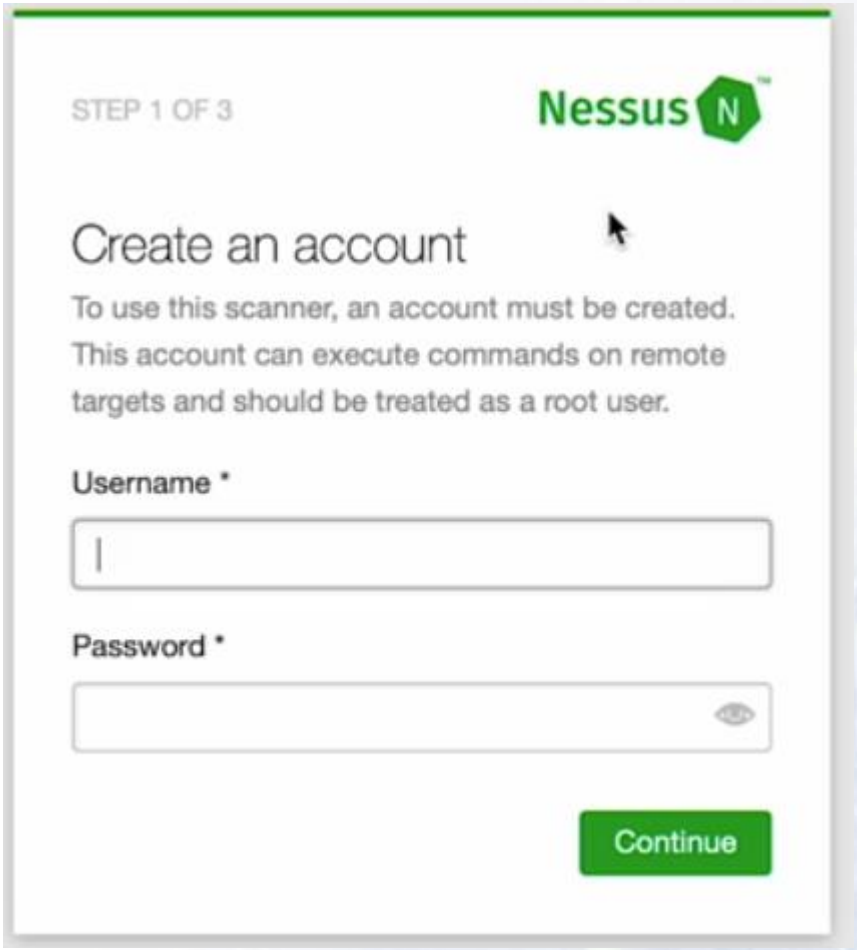
1. First, ensure that the Nessus vulnerability scanner is installed on your system.

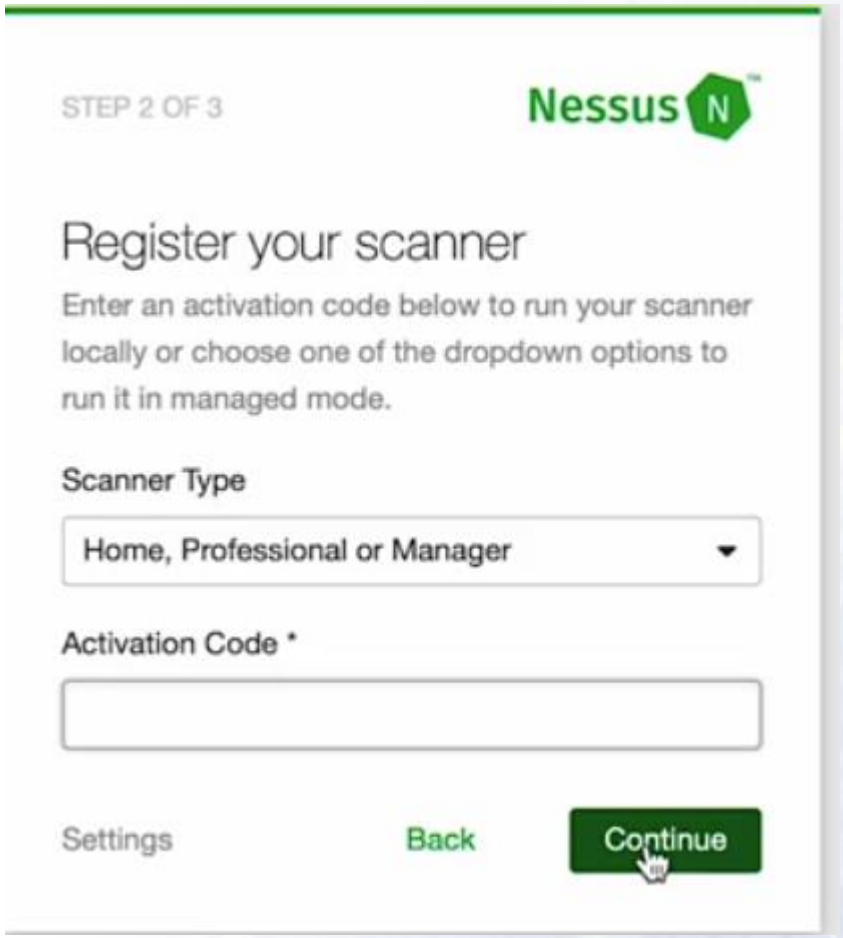
2. Once Nessus is installed, open a web browser (Chrome, Firefox, etc.) on the system you installed Nessus on.

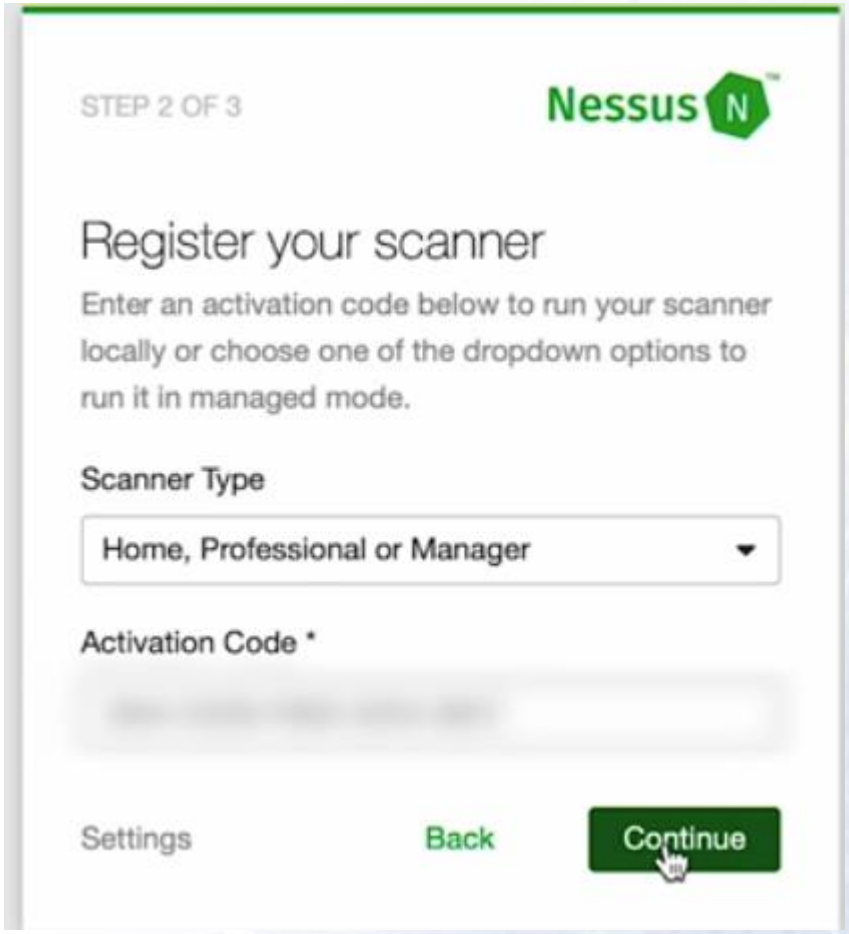
3. In the web browser, navigate to the following URL: https://localhost:8834/ OR https://127.0.0.1:8834/

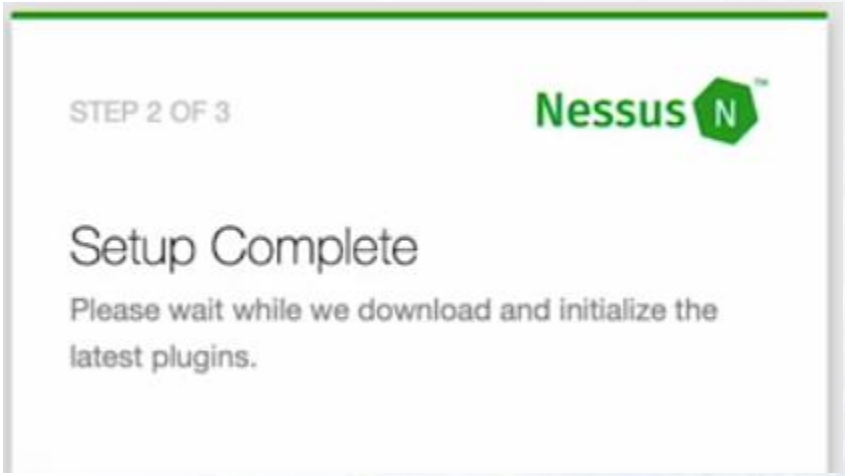
4. If Nessus is running on the same system that you are accessing the web interface from, the Nessus login page should appear in your web browser.

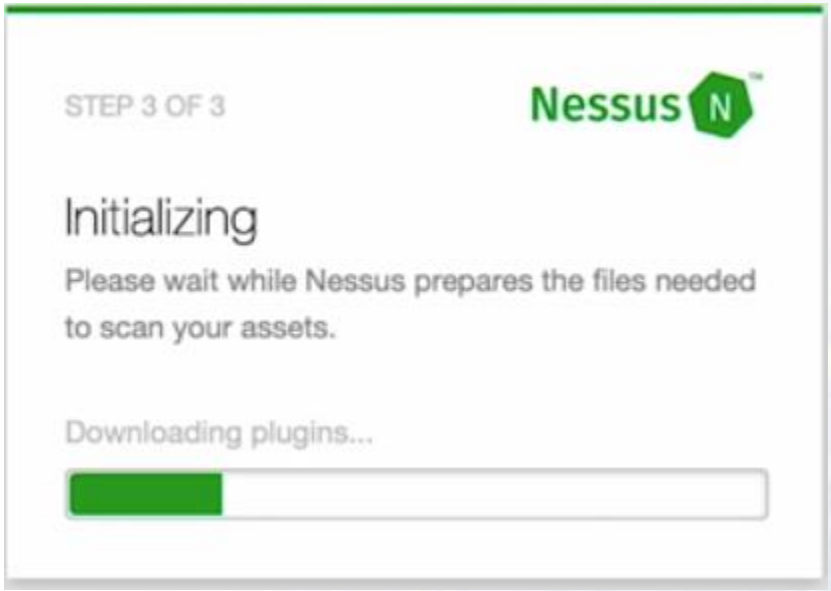
5. Enter your Nessus username and password and click "Login" to access the Nessus web interface.


STEP 1 OF 3
Nessus
Create an account
To use this scanner, an account must be created. This account can execute commands on remote targets and should be treated as a root user.
Username *
Password *
Continue


STEP 2 OF 3
Nessus
Register your scanner
Enter an activation code below to run your scanner locally or choose one of the dropdown options to run it in managed mode.
Scanner Type
Home, Professional or Manager
Activation Code *
Settings
Back
Continue


STEP 2 OF 3
Nessus
Register your scanner
Enter an activation code below to run your scanner locally or choose one of the dropdown options to run it in managed mode.
Scanner Type
Home, Professional or Manager
Activation Code *
Settings
Back
Continue


STEP 2 OF 3
Nessus
Setup Complete
Please wait while we download and initialize the latest plugins.


STEP 3 OF 3
Nessus
Initializing
Please wait while Nessus prepares the files needed to scan your assets.
Downloading plugins...

Nessus Features

- Lets take a look at Nessus features

Nessus Features

- Nessus (Reports):
  - Customize reports to sort by vulnerability or host
  - Create an executive summary or compare scan results
  - Targeted email notifications of scan results

Nessus Features

- Nessus (Scan Types):
  - Asset discovery
  - Un-credentialed vulnerability discovery
  - Credentialed scanning for system hardening & missing patches

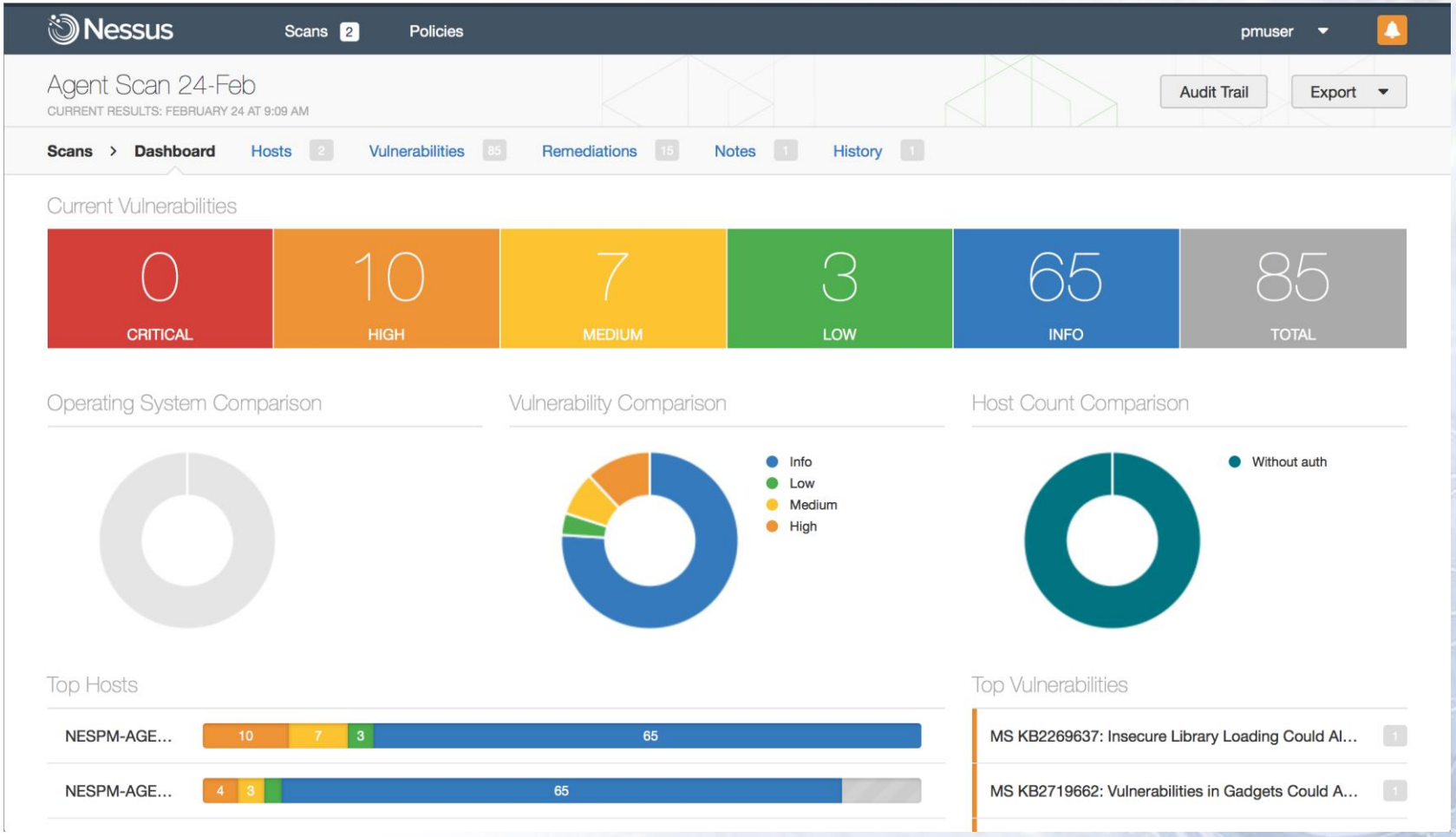
Nessus Features

- Nessus (Compliance & Config Scans):
  - Compliance auditing: FFIEC, FISMA, CyberScope, GLBA, HIPAA/ HITECH, NERC, PCI, SCAP, SOX
  - Configuration auditing: CERT, CIS, COBIT/ITIL, DISA STIGs, FDCC, ISO, NIST, NSA

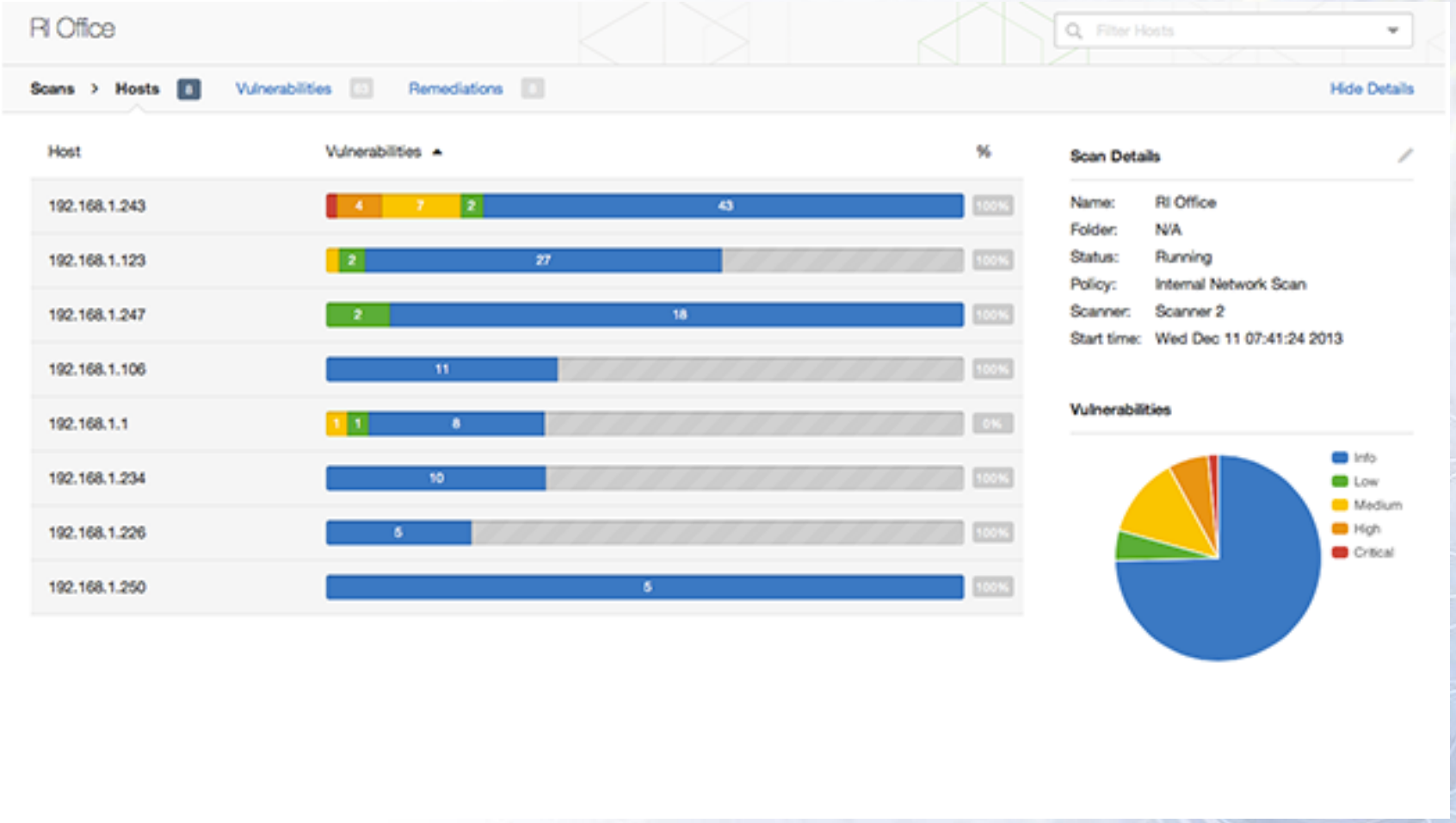
Nessus Features

- Nessus (Risk scores):
  - Vulnerability ranking based on CVE, five severity levels (Critical, High, Medium, Low, Info), customizable severity levels for recasting of risk

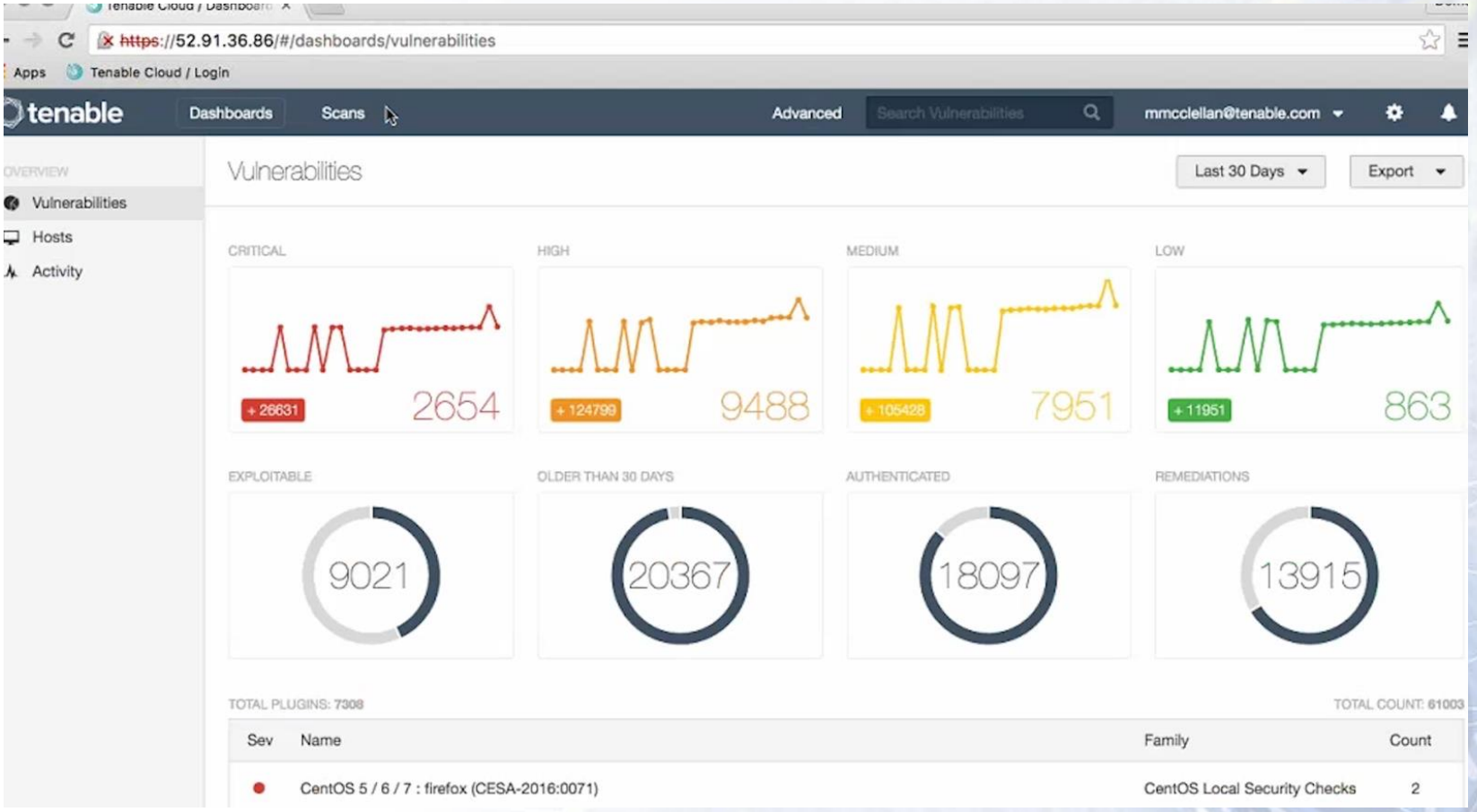
Nessus Features



Nessus Features



Nessus Features



Nessus Features

- Nessus is a cost-effective scanner that gets most of the job done for vulnerability scanning
- It has CIS and DISA compliance templates

Qualys Features

- Lets take a look at Qualys features

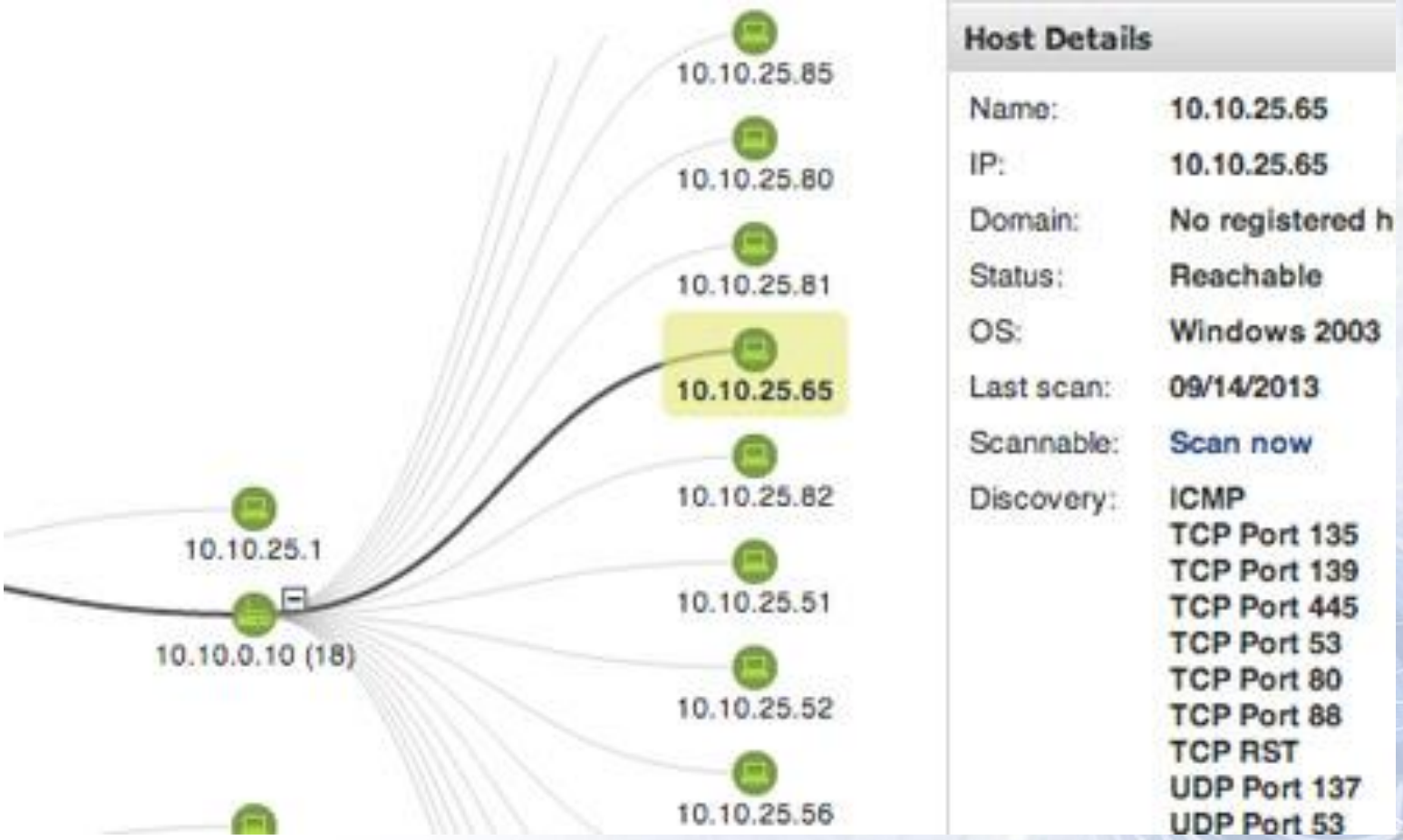
Qualys Features

- Qualys:
  - Cloud-based service
  - On-premise device
  - Complete suite
  - Scalable and immediate deployment

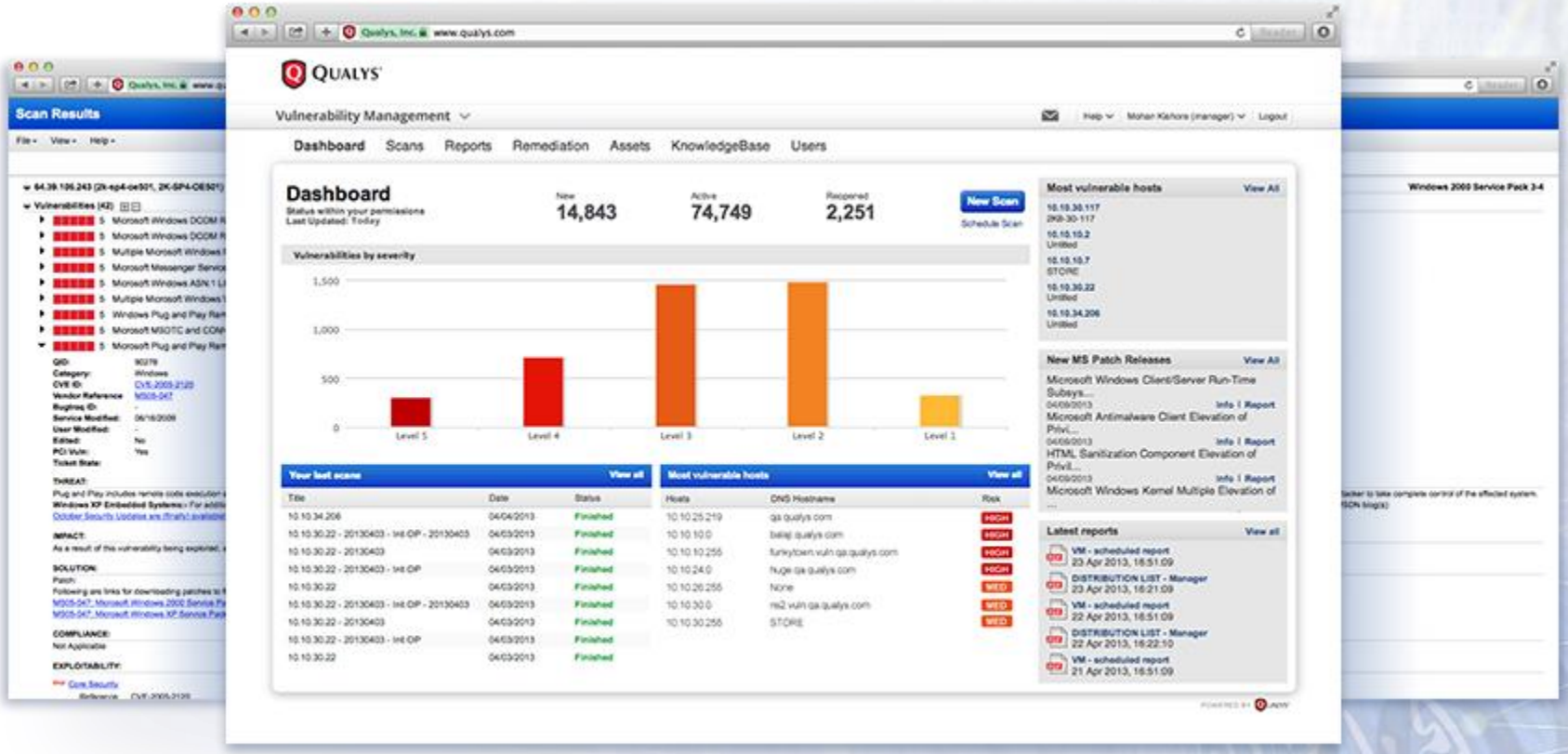
Qualys Features

- Qualys:
  - Asset discovery; find and organize hosts
  - Prioritize & manage remediation tickets
  - Continuous monitoring service
  - Policy compliance scanning
  - Qualys Secure Seal for websites

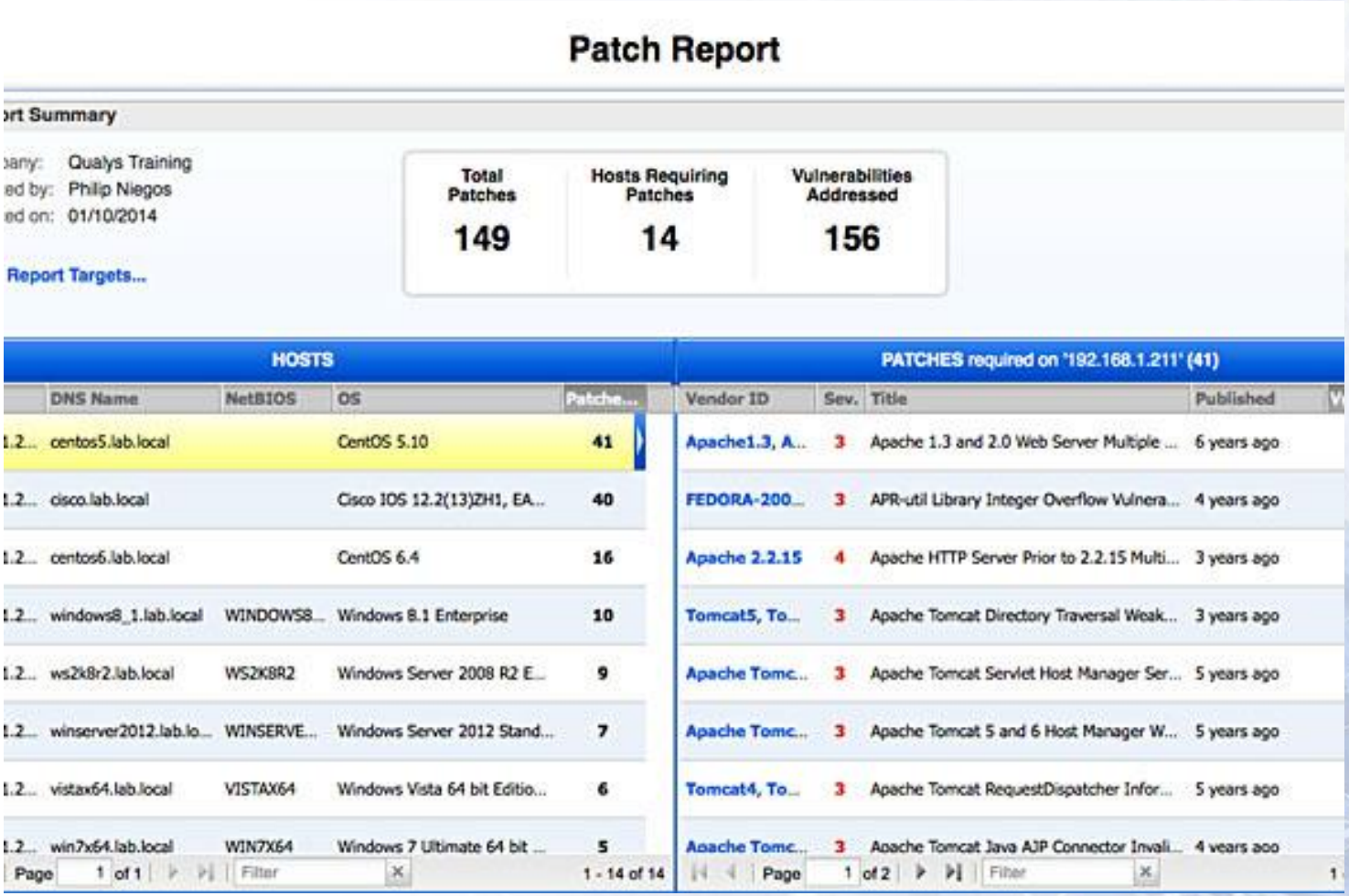
Qualys Features



Qualys Features



Qualys Features



Patch Report

ort Summary

bany: Qualys Training
ed by: Philip Niegos
ed on: 01/10/2014

Report Targets...

Total Patches	Hosts Requiring Patches	Vulnerabilities Addressed
149	14	156

HOSTS

	DNS Name	NetBIOS	OS	Patche...
1.2...	centos5.lab.local		CentOS 5.10	41
1.2...	cisco.lab.local		Cisco IOS 12.2(13)ZH1, EA...	40
1.2...	centos6.lab.local		CentOS 6.4	16
1.2...	windows8_1.lab.local	WINDOWS8...	Windows 8.1 Enterprise	10
1.2...	ws2k8r2.lab.local	WS2K8R2	Windows Server 2008 R2 E...	9
1.2...	winserver2012.lab.lo...	WINSERVE...	Windows Server 2012 Stand...	7
1.2...	vistax64.lab.local	VISTAX64	Windows Vista 64 bit Editio...	6
1.2...	win7x64.lab.local	WIN7X64	Windows 7 Ultimate 64 bit ...	5

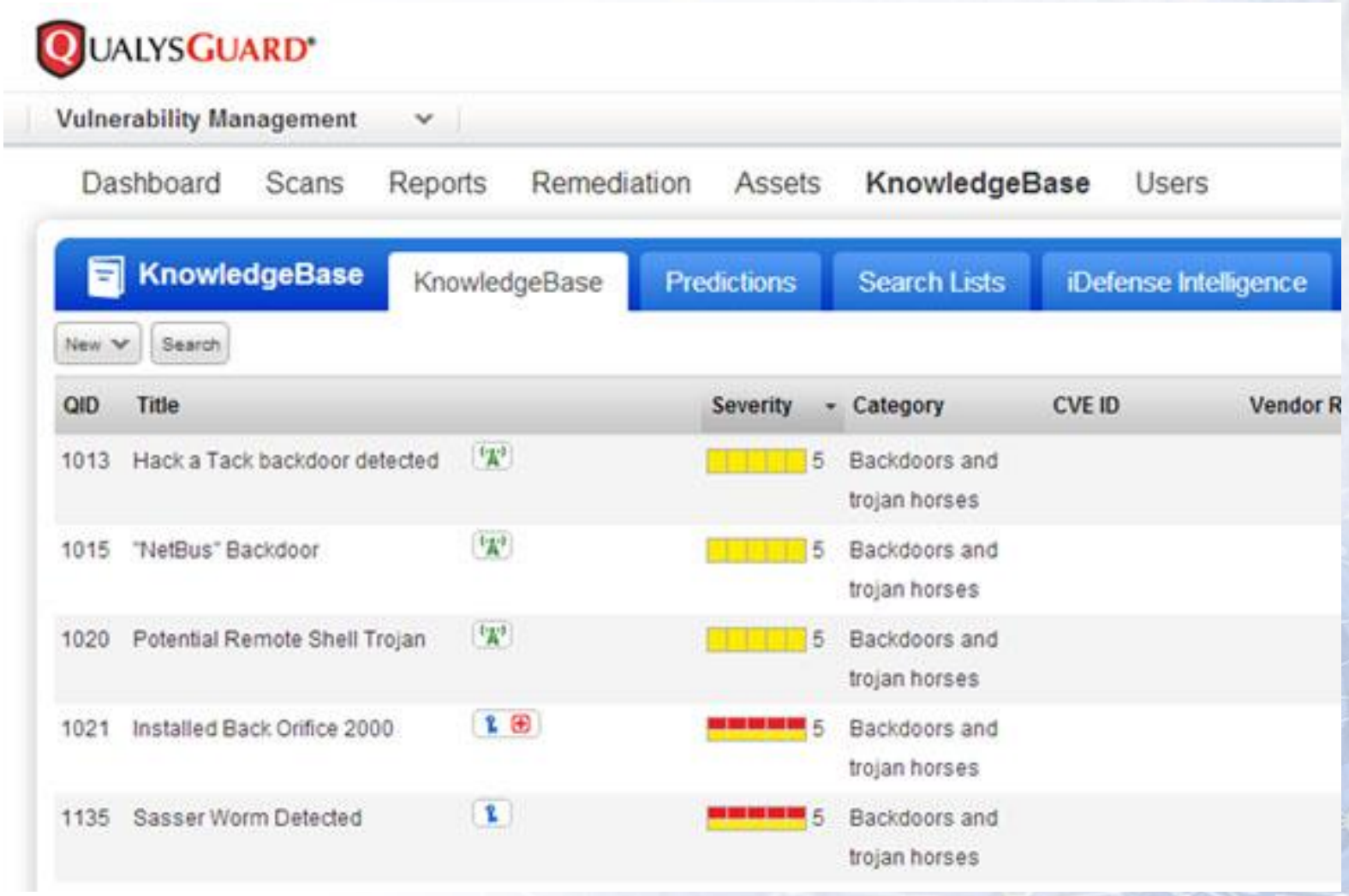
Page 1 of 1 | Filter | 1 - 14 of 14

PATCHES required on '192.168.1.211' (41)

Vendor ID	Sev.	Title	Published
Apache1.3, A...	3	Apache 1.3 and 2.0 Web Server Multiple ...	6 years ago
FEDORA-200...	3	APR-util Library Integer Overflow Vulnera...	4 years ago
Apache 2.2.15	4	Apache HTTP Server Prior to 2.2.15 Multi...	3 years ago
Tomcat5, To...	3	Apache Tomcat Directory Traversal Weak...	3 years ago
Apache Tomc...	3	Apache Tomcat Servlet Host Manager Ser...	5 years ago
Apache Tomc...	3	Apache Tomcat 5 and 6 Host Manager W...	5 years ago
Tomcat4, To...	3	Apache Tomcat RequestDispatcher Infor...	5 years ago
Apache Tomc...	3	Apache Tomcat Java AJP Connector Invali...	4 years ago

Page 1 of 2 | Filter

Qualys Features



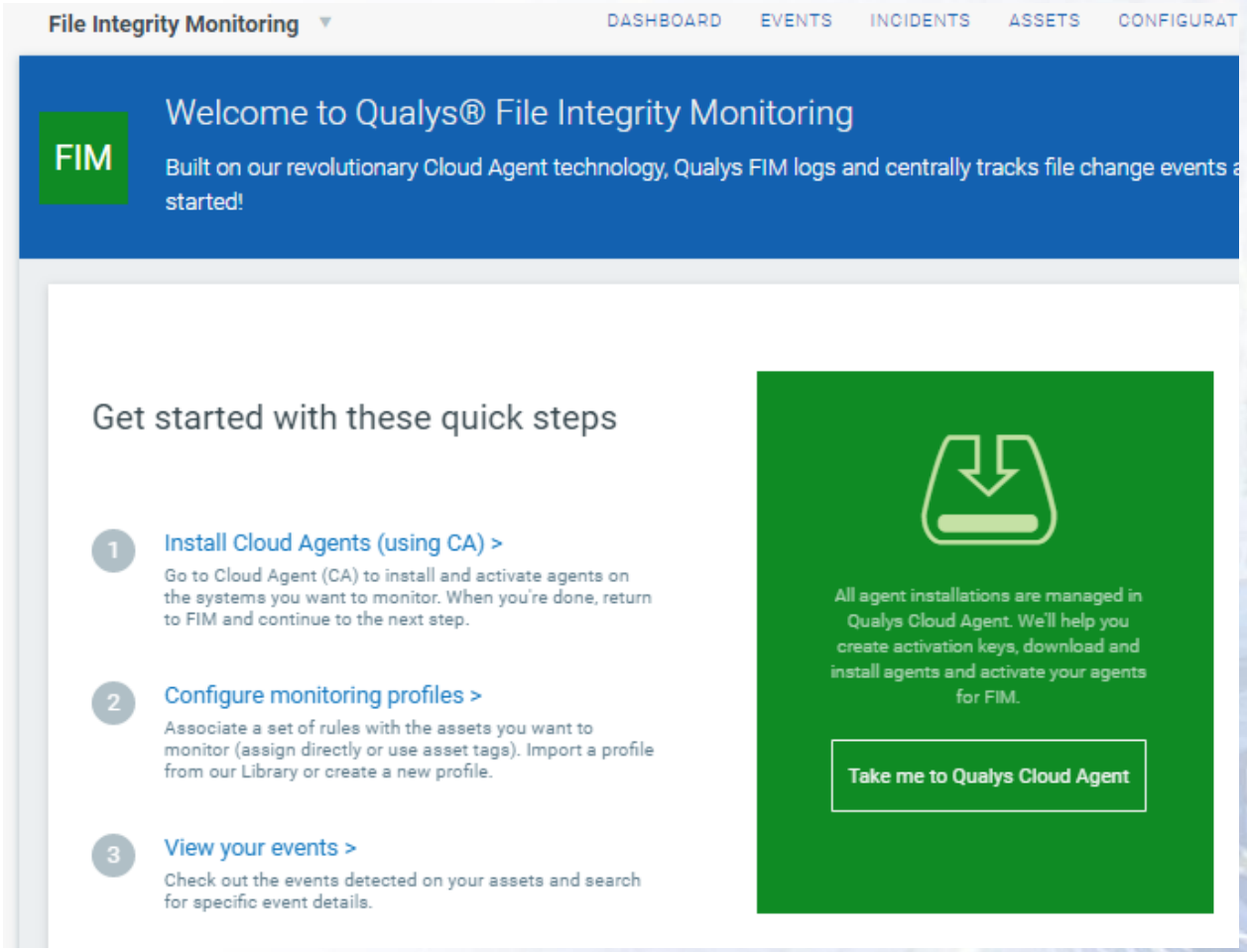
Qualys Features



Secure Seal

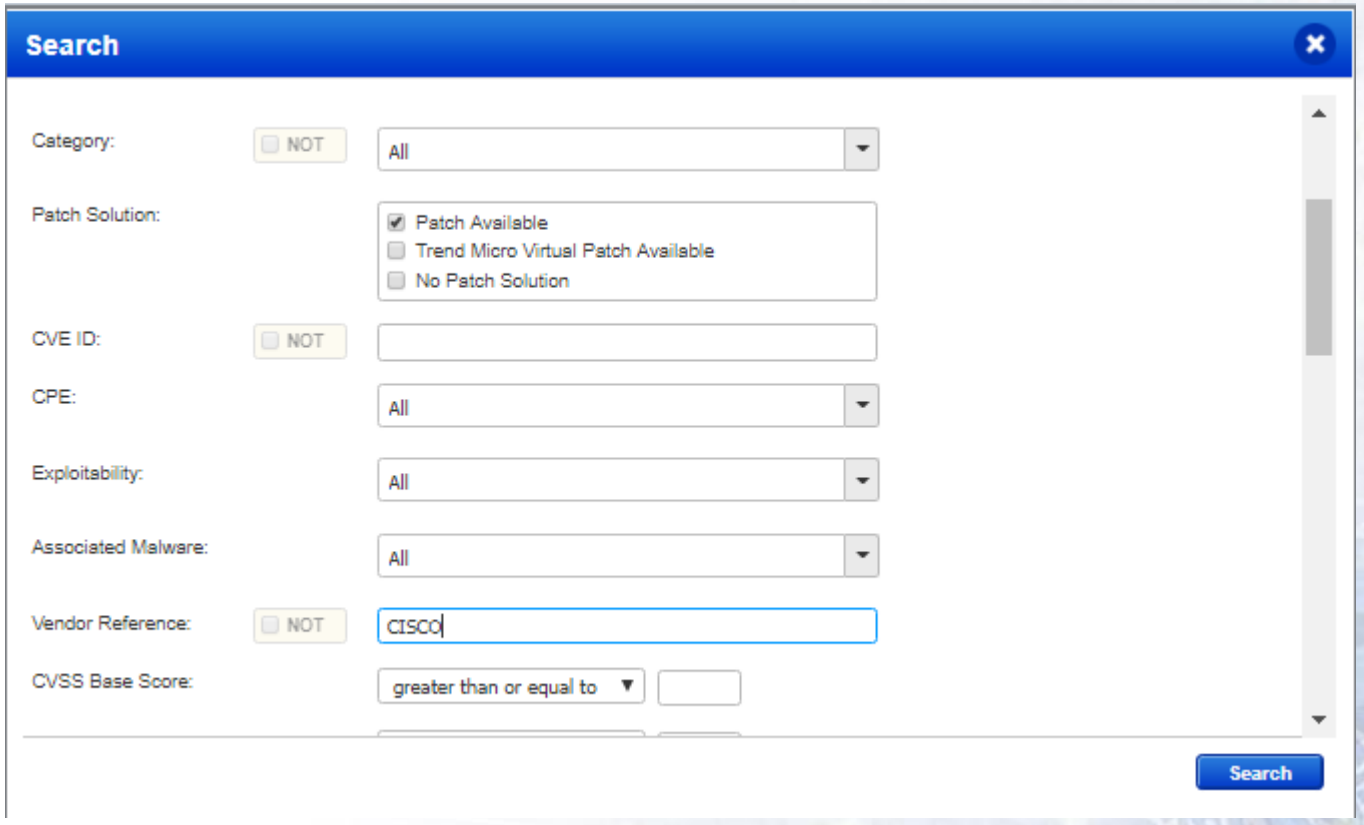
- A Secure Seal for websites refers to a visual indicator, such as a badge or logo, displayed on a website to indicate that the site has been verified and is secure.
- The purpose of the secure seal is to assure visitors that the website is legitimate, trustworthy, and has taken measures to protect the privacy and security of their personal and financial information.

QUALYS FEATURES



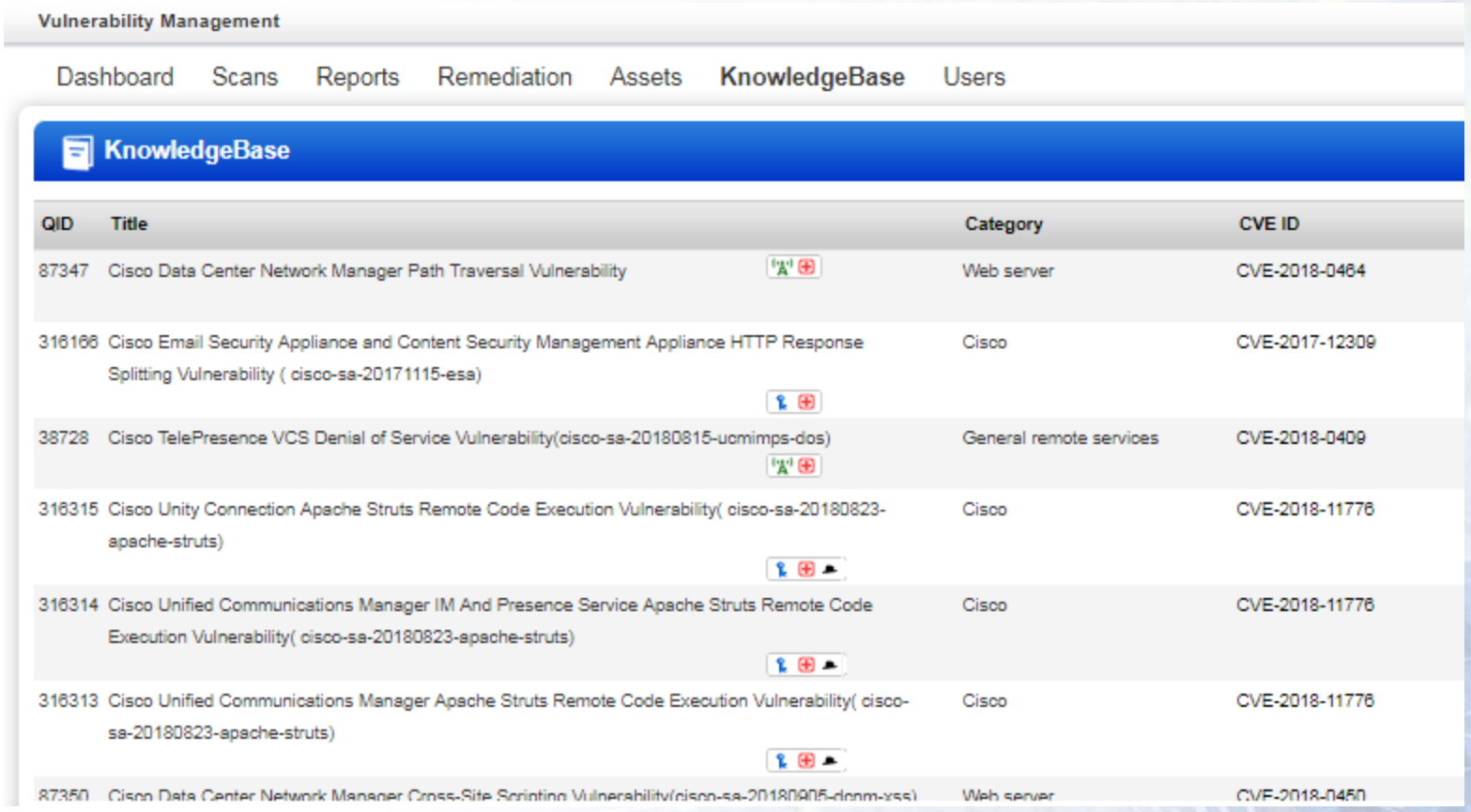
FILE INTEGRITY MONITORING

QUALYS FEATURES



SEARCH KNOWLEDGEBASE

QUALYS FEATURES



CISCO VULNERABILITIES – PATCH AVAILABLE

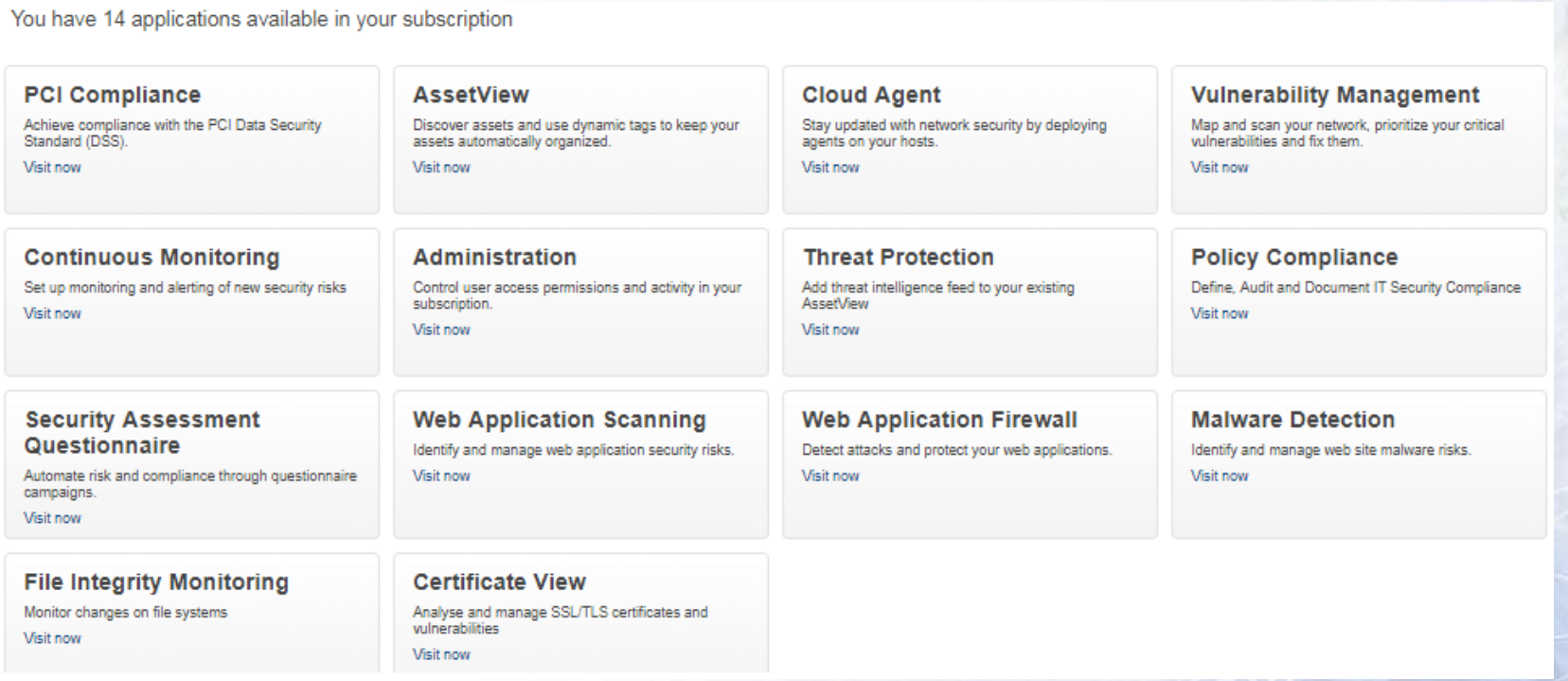
Qualys Features

- Qualys:
  - Website scanning
  - Annual subscription service model
  - Qualys is a convenient and scalable VM tool that comes with several modules
  - Several advantages due to cloud-based service

QUALYS DEMO - PART 2

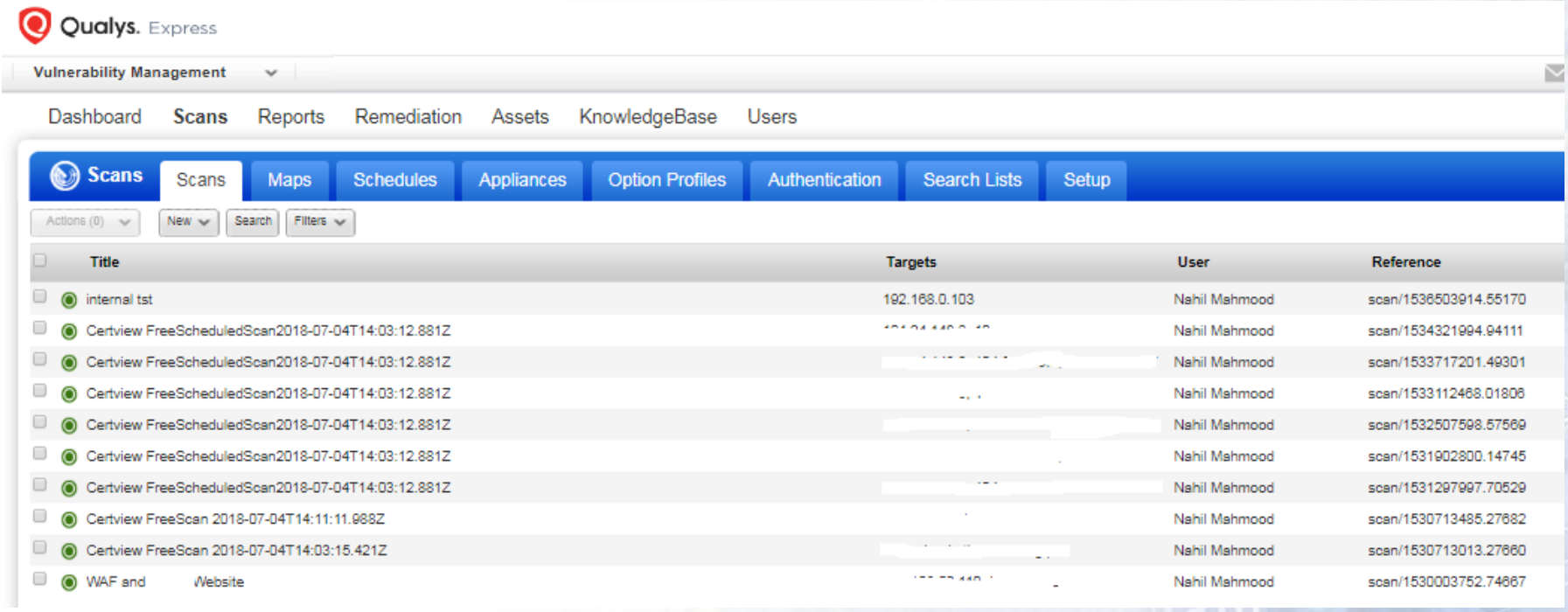
- Lets have a look at the Qualys features

QUALYS DEMO - PART 2



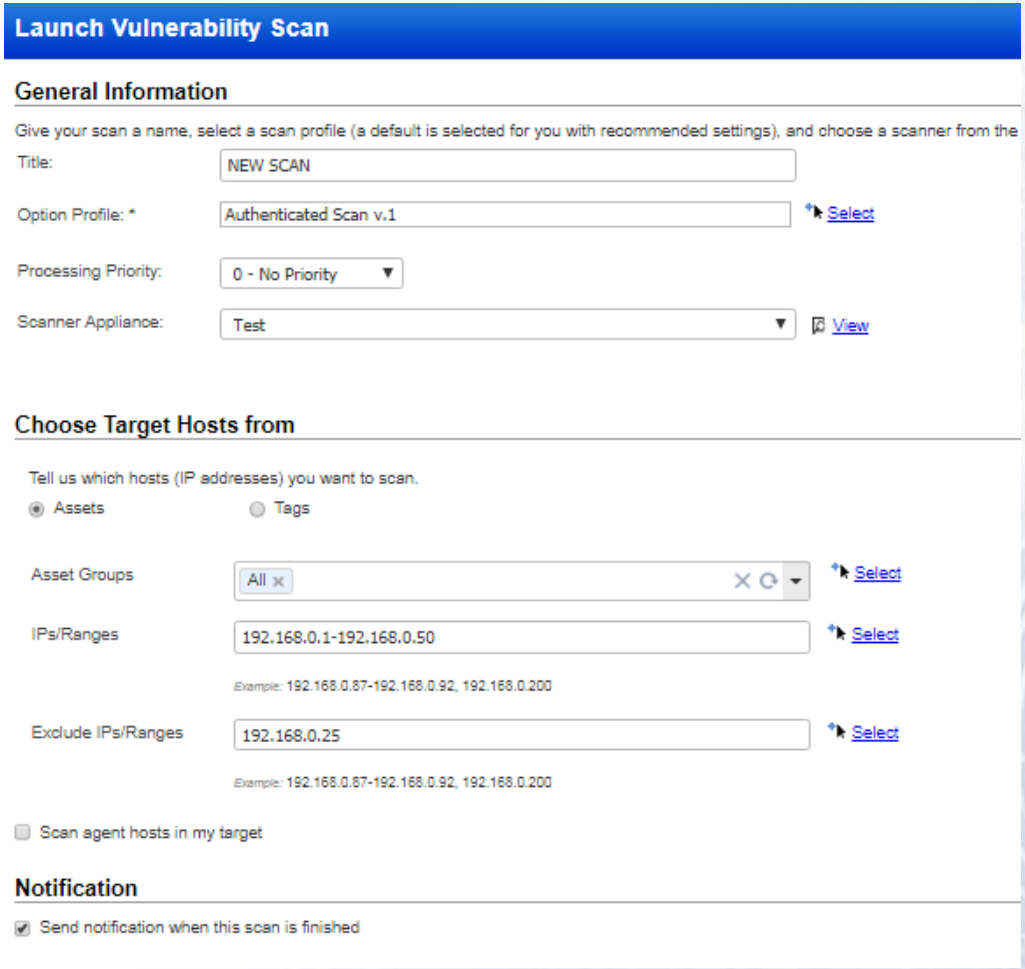
QUALYS
14 APPLICATIONS

QUALYS DEMO - PART 2



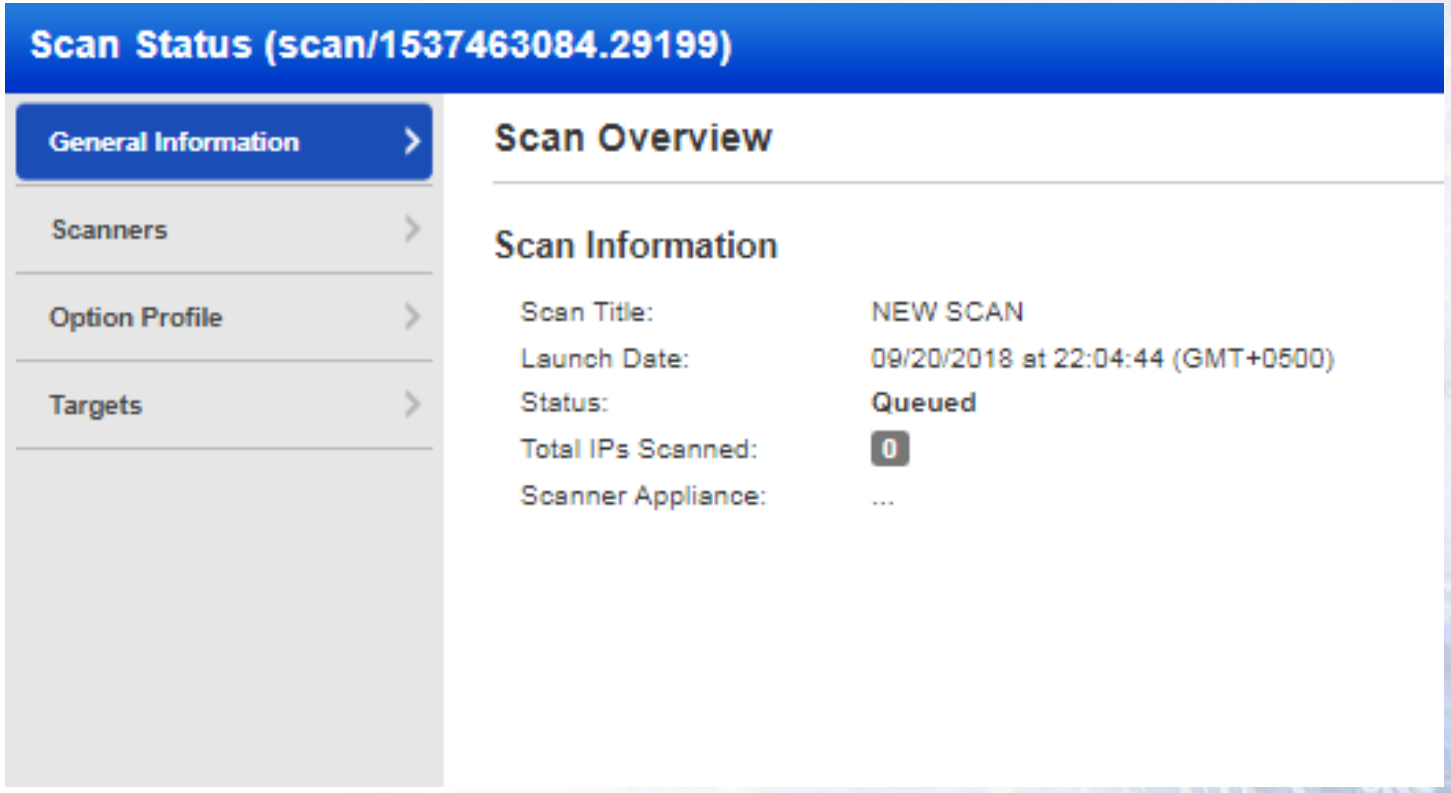
VULNERABILITY MANAGEMENT DASHBOARD

QUALYS DEMO - PART 2



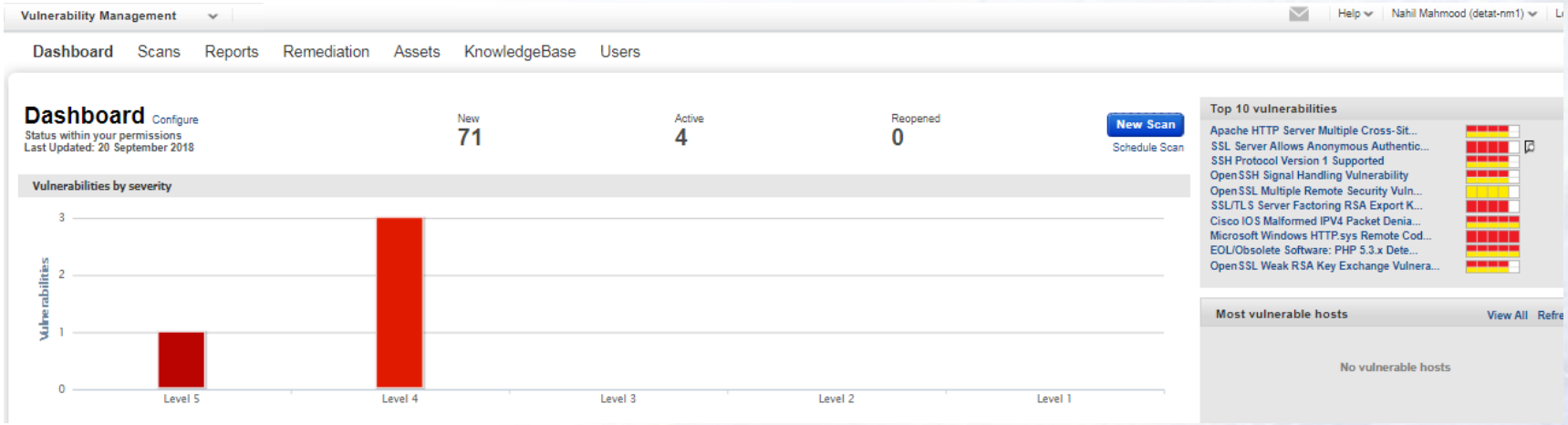
LAUNCH VULNERABILITY SCAN

QUALYS DEMO - PART 2



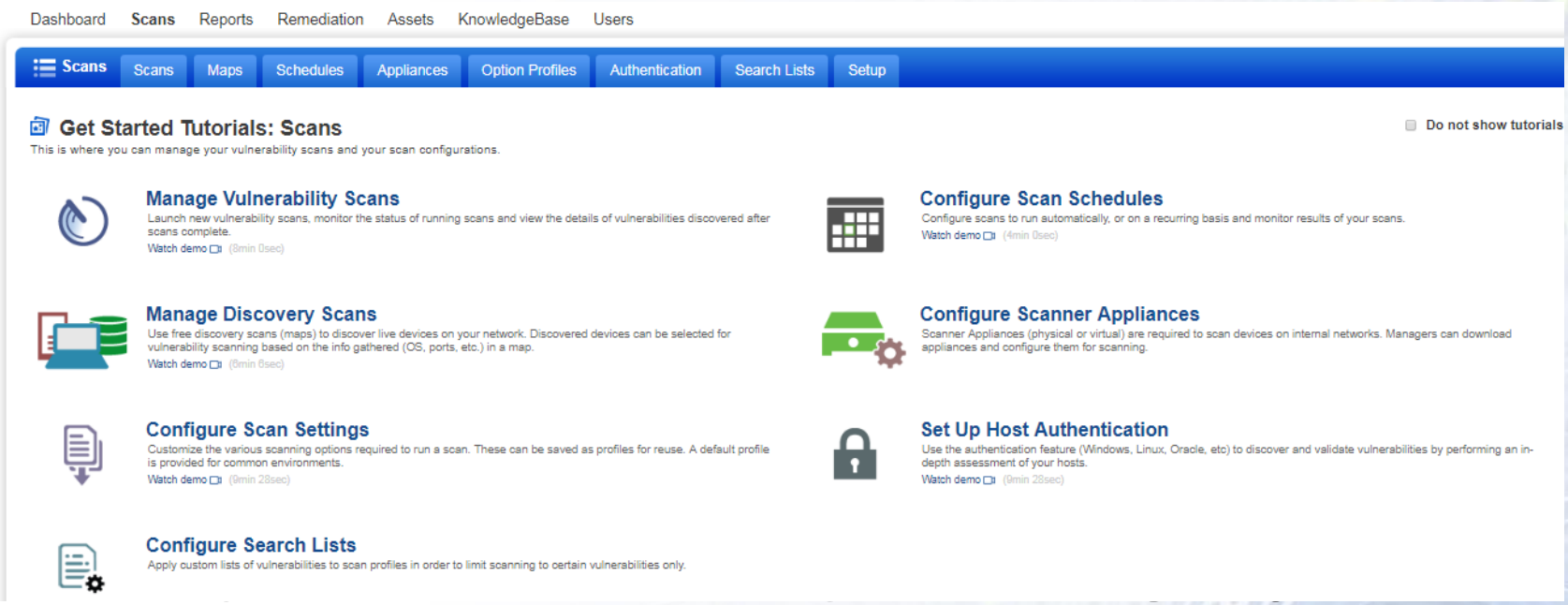
SCAN INITIATED

QUALYS DEMO - PART 2



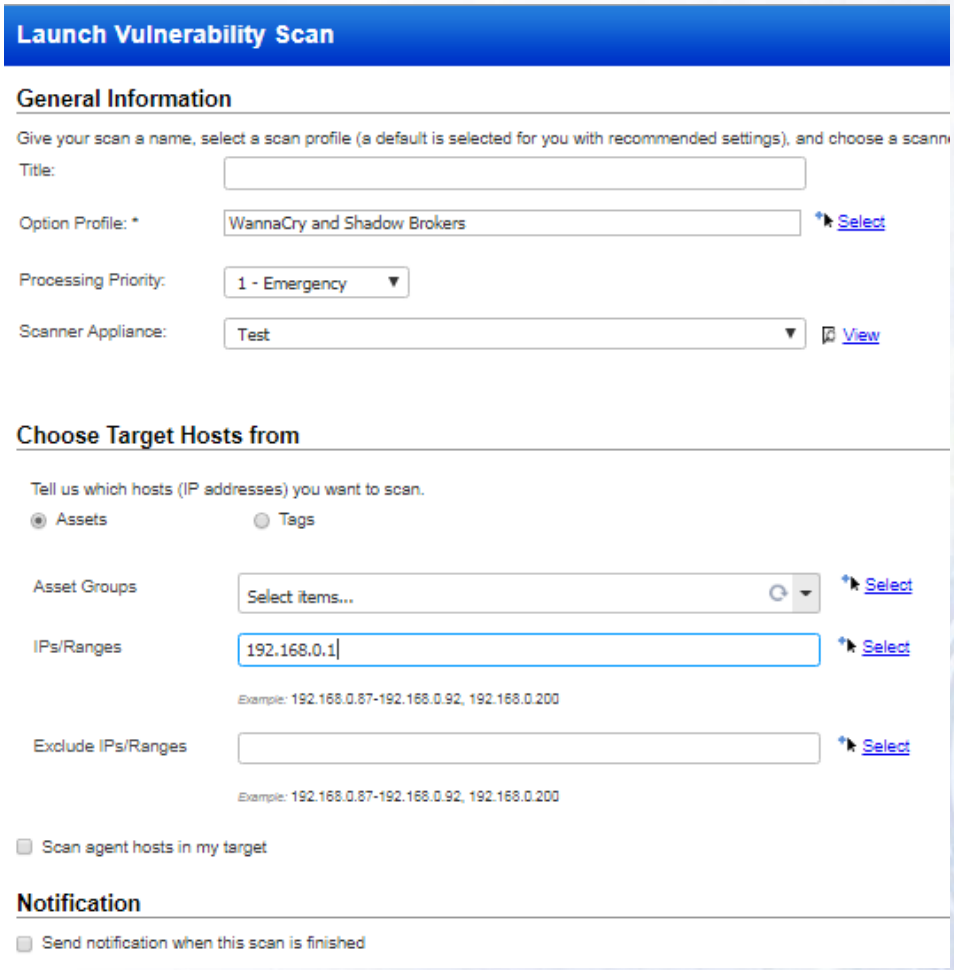
VULNERABILITY MANAGEMENT DASHBOARD

QUALYS DEMO - PART 2



SCAN TUTORIALS

QUALYS DEMO - PART 2

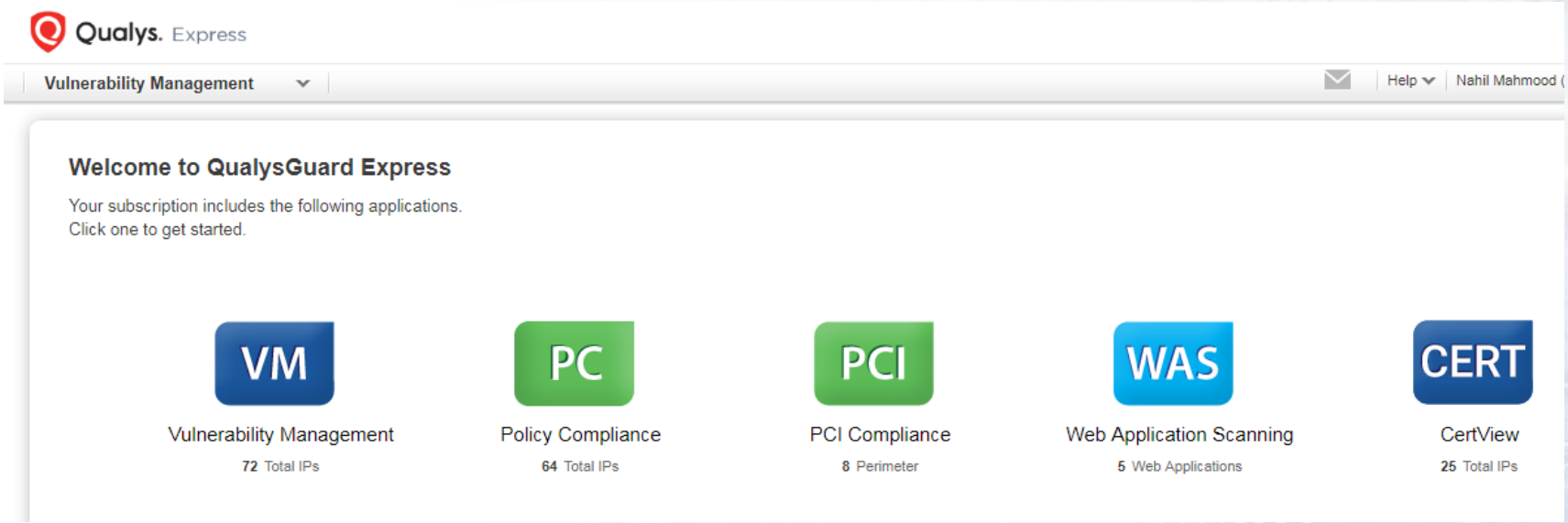


WANNACRY & SHADOW BROKERS SCAN

QUALYS DEMO – SECURITY HARDENING

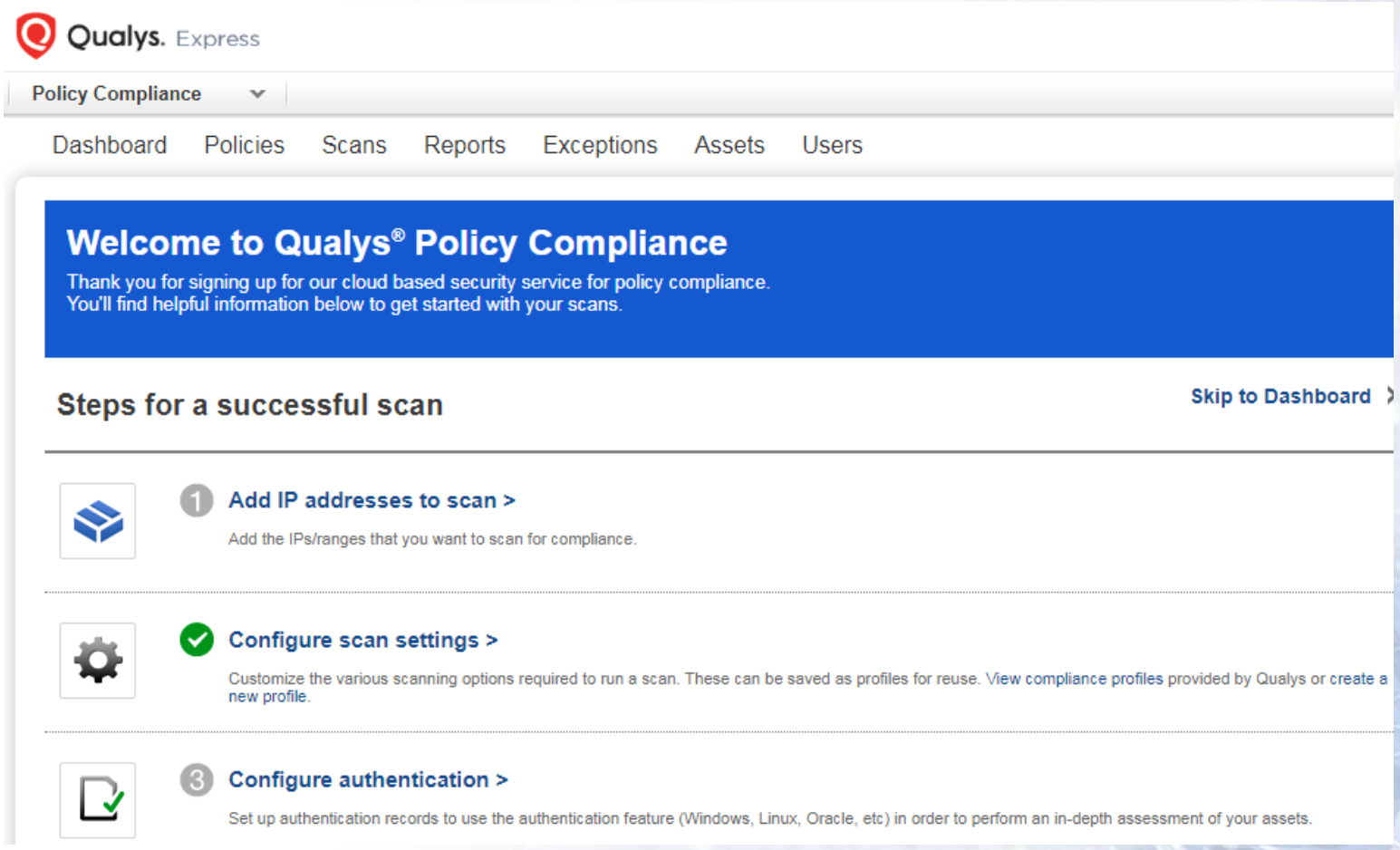
- Lets have a look at how Qualys can aid in the security hardening process

QUALYS DEMO – SECURITY HARDENING



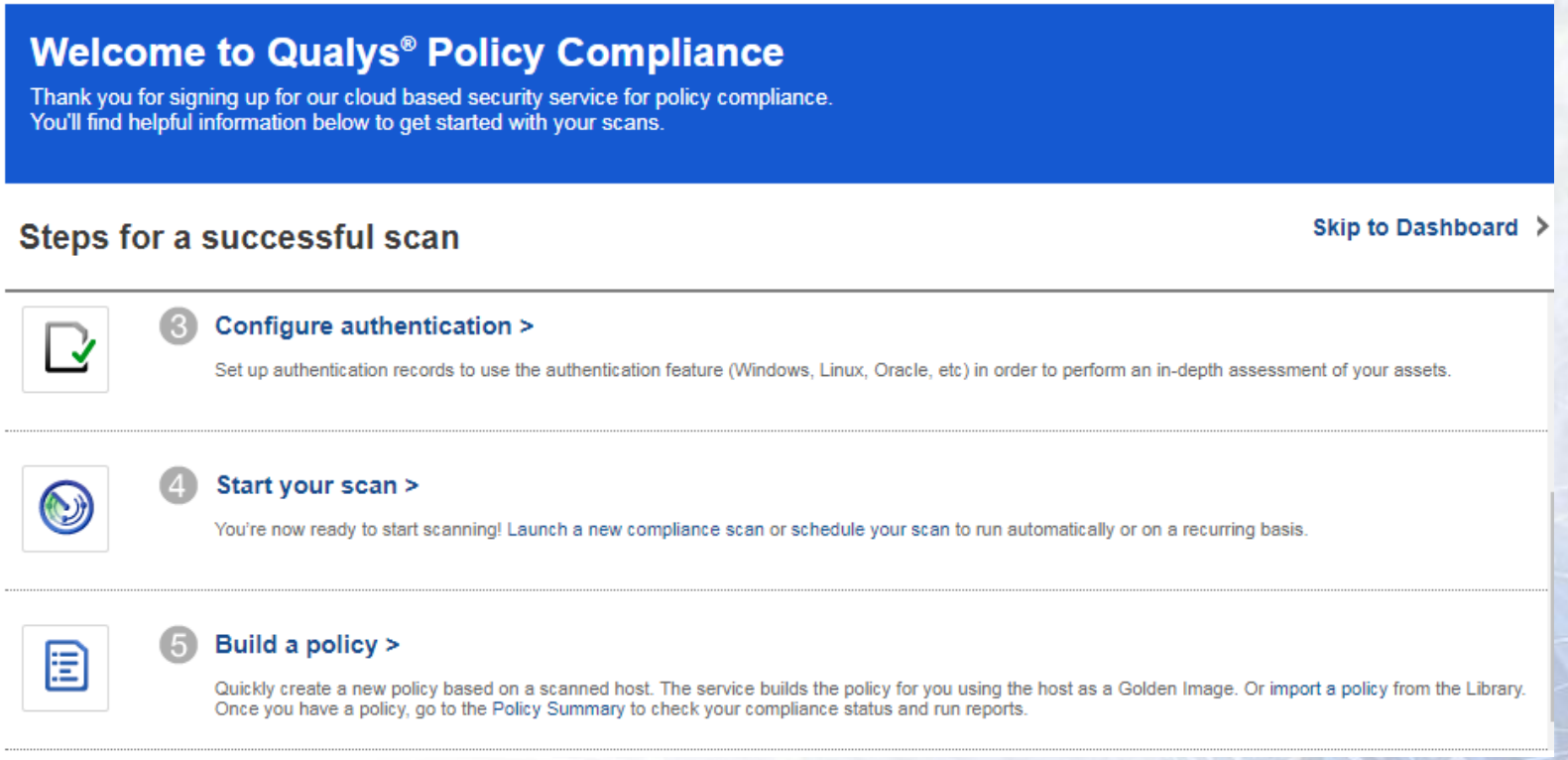
QUALYS GUARD – HOME SCREEN

QUALYS DEMO – SECURITY HARDENING



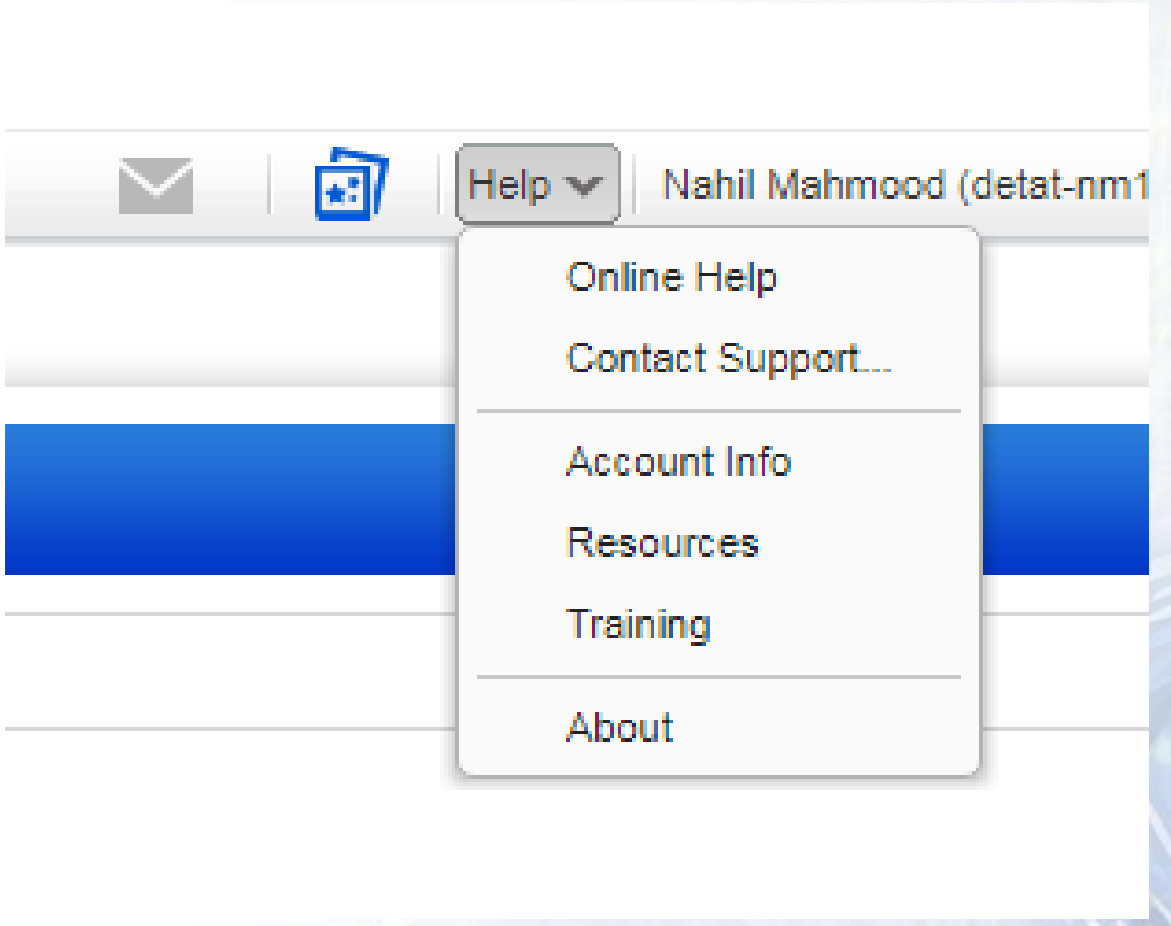
POLICY COMPLIANCE – HOME SCREEN

QUALYS DEMO – SECURITY HARDENING



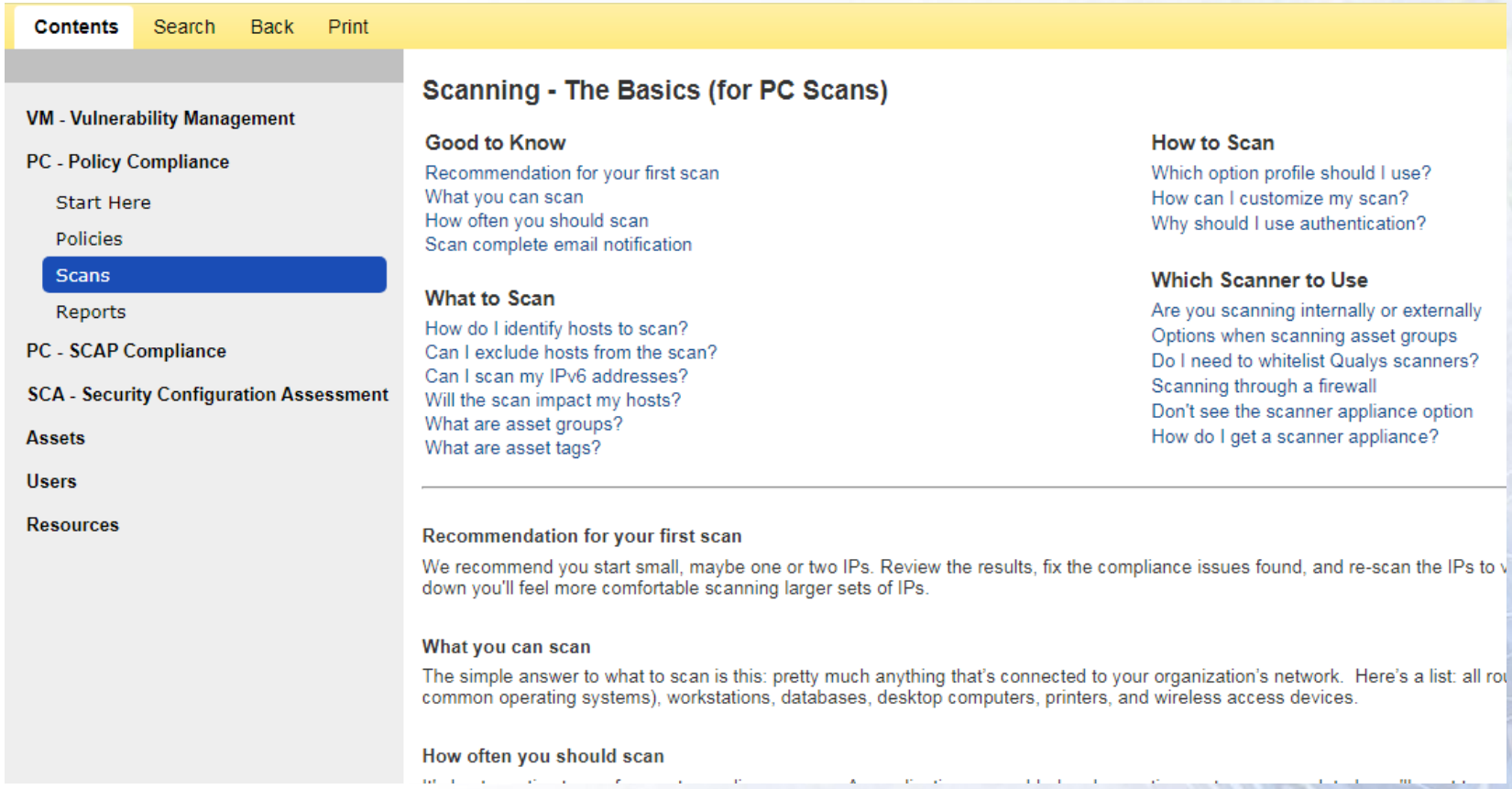
POLICY COMPLIANCE – 5 STEPS

QUALYS DEMO – SECURITY HARDENING



HELP OPTIONS

QUALYS DEMO – SECURITY HARDENING



ONLINE HELP – POLICY COMPLIANCE

QUALYS DEMO – SECURITY HARDENING

Resources

Look to these resources to help you with our cloud security and compliance solutions.

Get Started

Quick Tour
Evaluator's Guide
Community Edition
Securing Amazon Web Services with Qualys

Watch Videos

VM | PC | WAS | WAF | AWS EC2 | Express Lite | More Videos

Get started with your applications

CloudView
Container Security
Indication of Compromise
Web Application Scanning
- Crawling REST services using WAS
- Jenkins Plugin for WAS: user guide | download
- Qualys Browser Recorder: user guide | download
Web Application Firewall
Policy Compliance
SCAP Compliance
Security Configuration Assessment
PCI Compliance
File Integrity Monitoring

Scan Authentication

Get system and account requirements for supported technologies below.

Cloud Agents

Cloud Agent Getting Started Guide
Windows Installation Guide
Linux Installation Guide
Unix Installation Guide
Mac Installation Guide

Using a scanner appliance?

Scanner Appliance User Guide
Scanner Appliance Quick Start (prior version)
Virtual Scanner Appliance User Guide
Offline Scanner Appliance User Guide
Consultant Scanner Personal Edition User Guide
Cloud Platforms: AWS | Azure | GCE | OpenStack
Qualys Scanner - Static Route Configuration
Qualys Scanner - VLAN Scanning Guide
Scanner Appliance FAQs

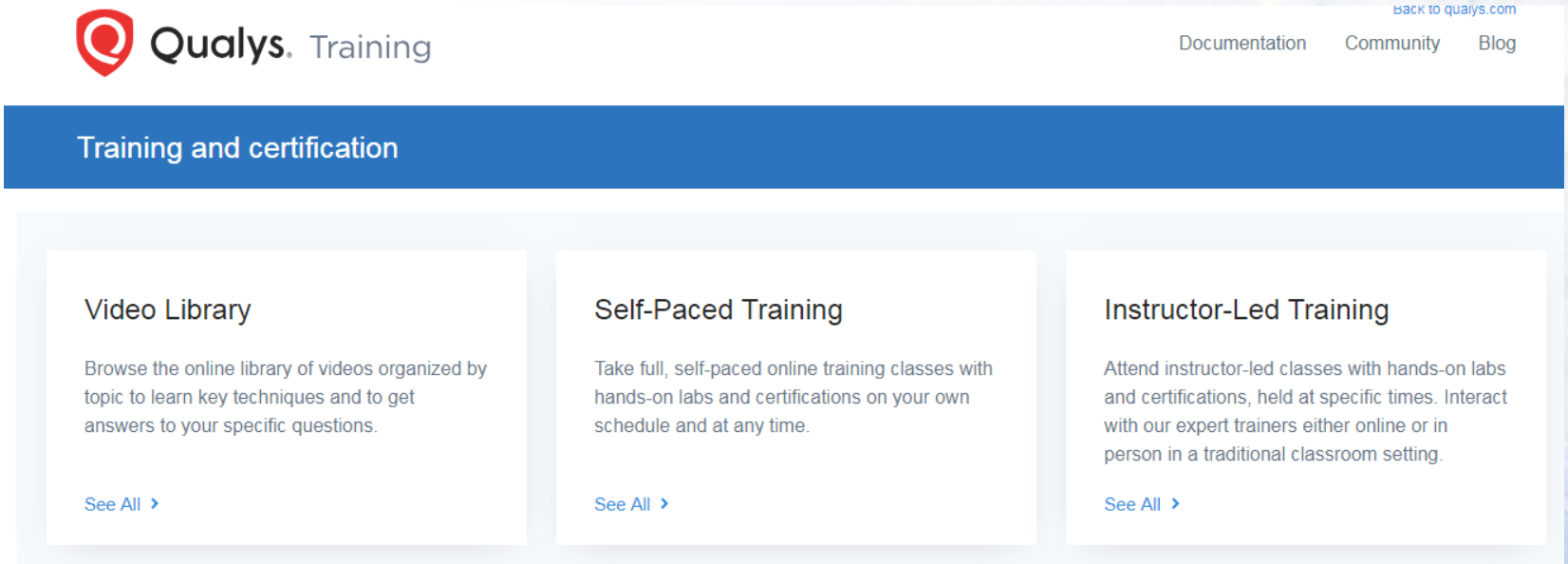
API Documentation

Qualys API Quick Reference for all APIs
Qualys API (VM, SCA, PC)

Cloud Agent (CA) API
Web Application Scanning (WAS) API
Web Application Firewall (WAF) API
Malware Detection (MD) API

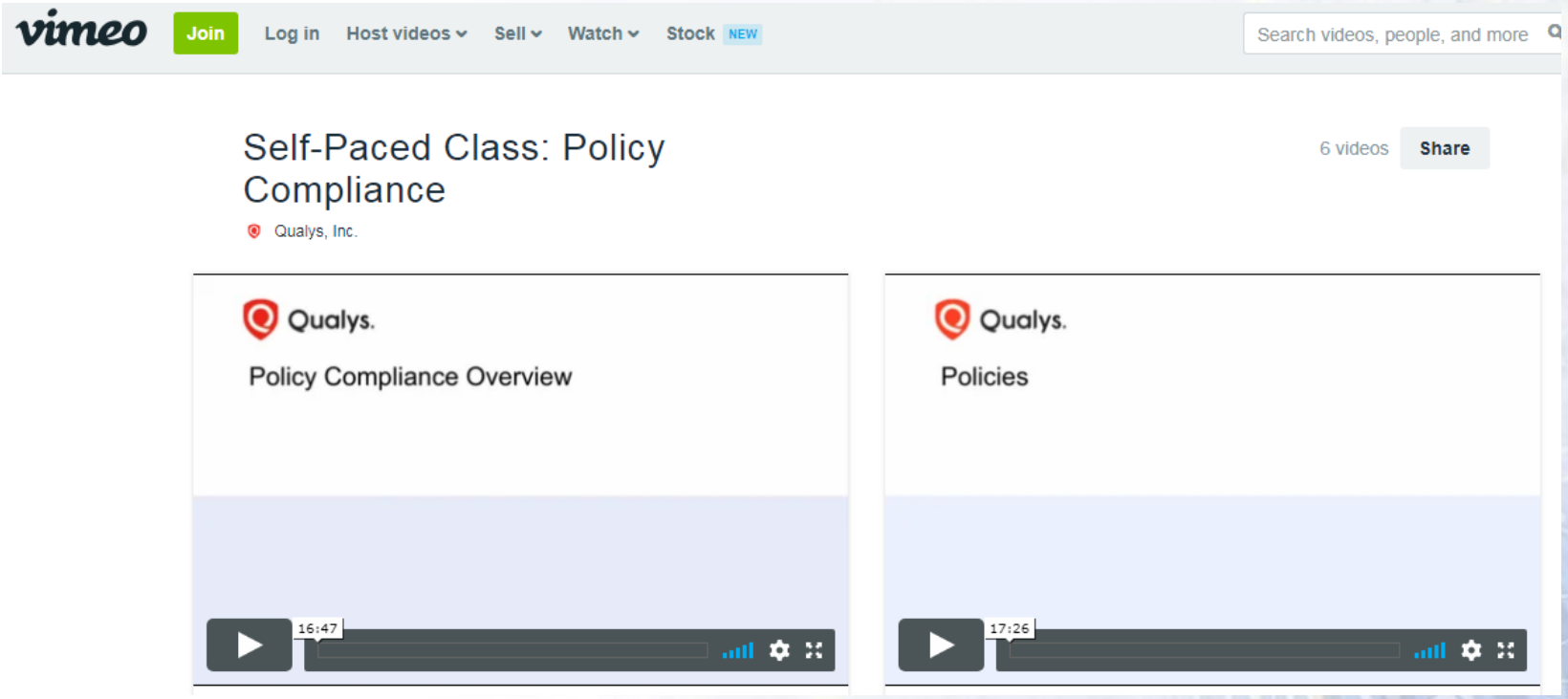
RESOURCES

QUALYS DEMO – SECURITY HARDENING



QUALYS WEBSITE - TRAINING

QUALYS DEMO – SECURITY HARDENING



TRAINING VIDEOS - VIMEO

QUALYS DEMO – SECURITY HARDENING

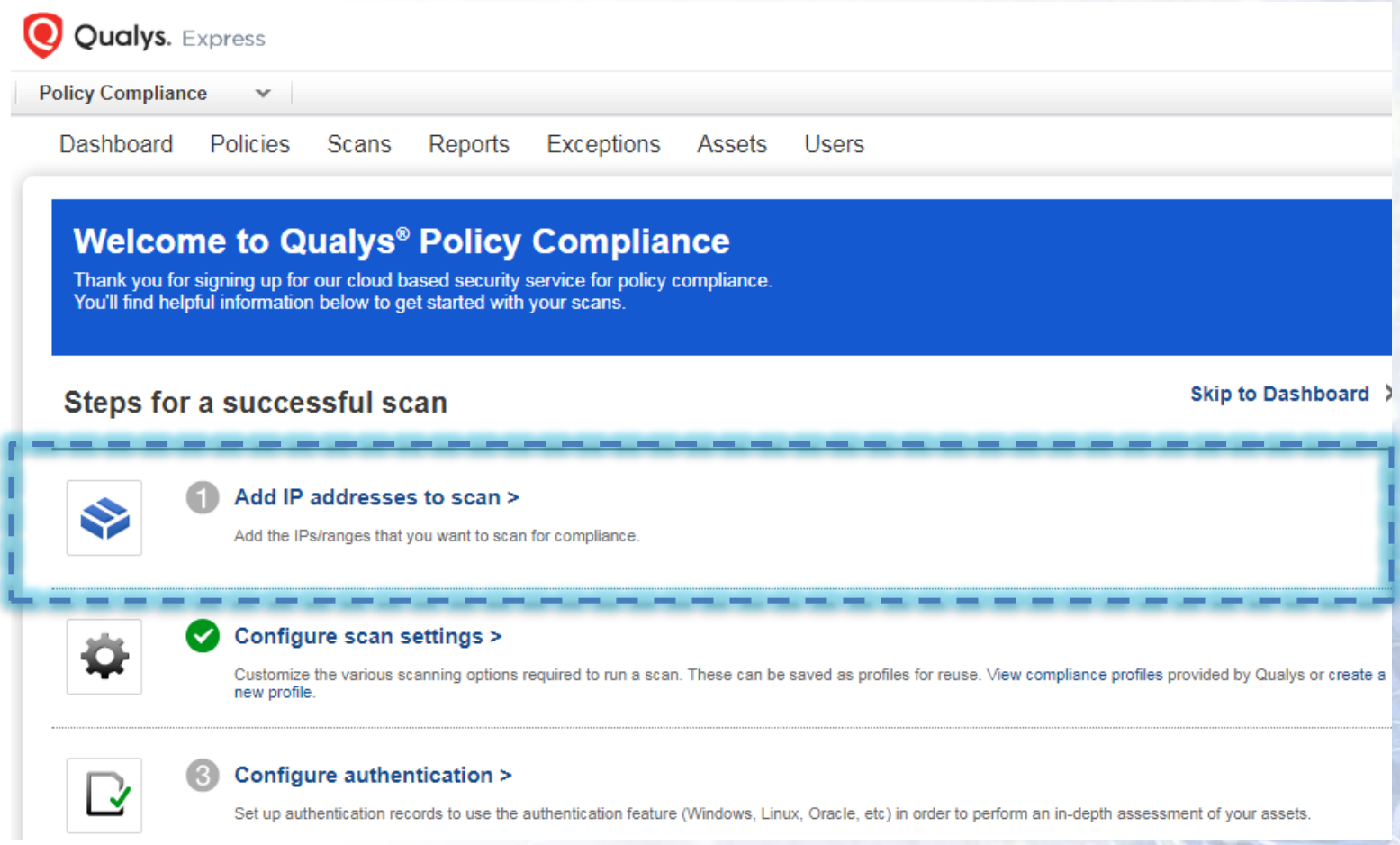
- Qualys is an excellent tool with detailed online help, training, and resources to aid the new user

END

QUALYS DEMO – SECURITY HARDENING II

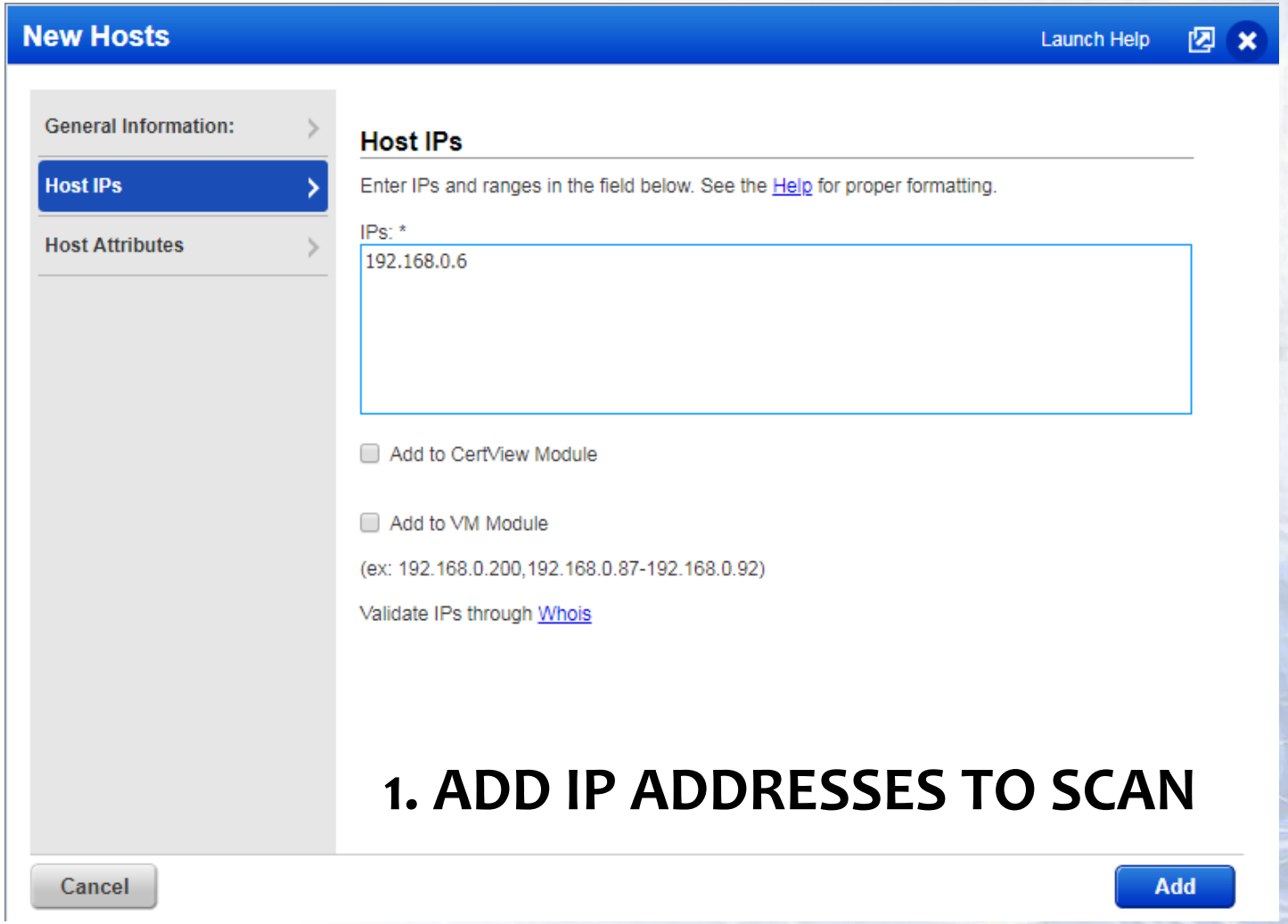
- Lets have a detailed look at Qualys interface for Policy Compliance

QUALYS DEMO – SECURITY HARDENING II

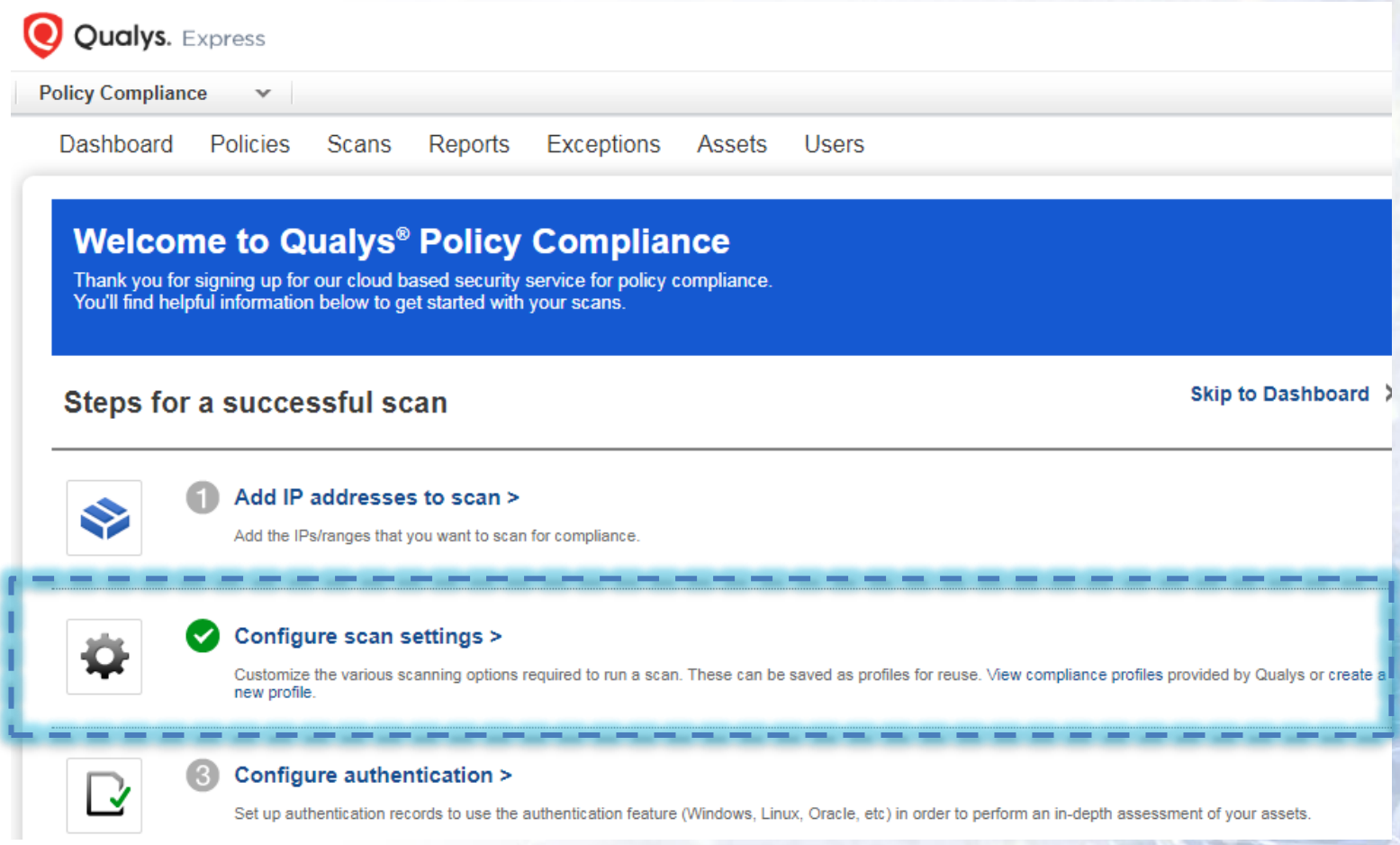


1. ADD IP ADDRESSES TO SCAN

QUALYS DEMO – SECURITY HARDENING

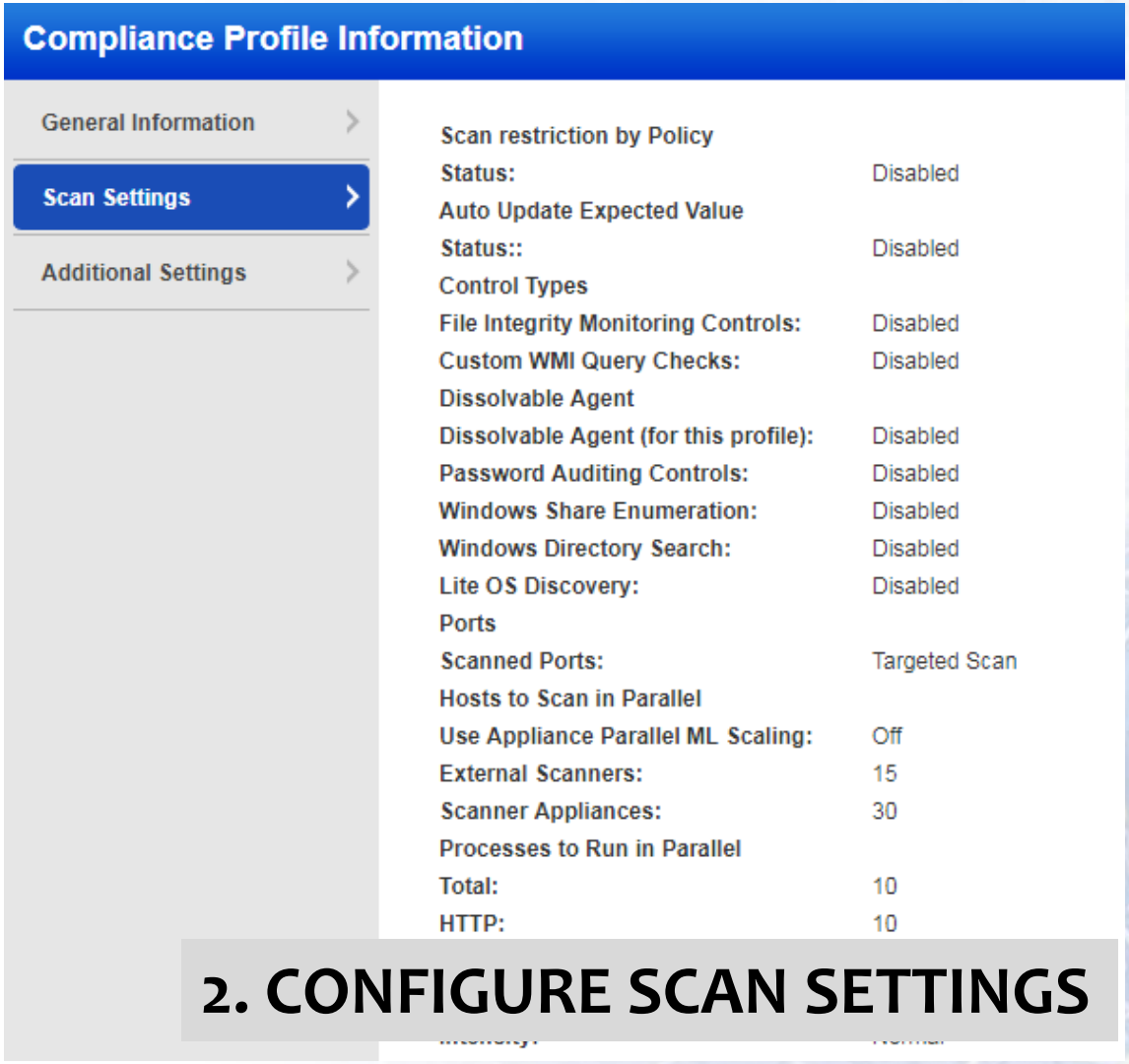


QUALYS DEMO – SECURITY HARDENING



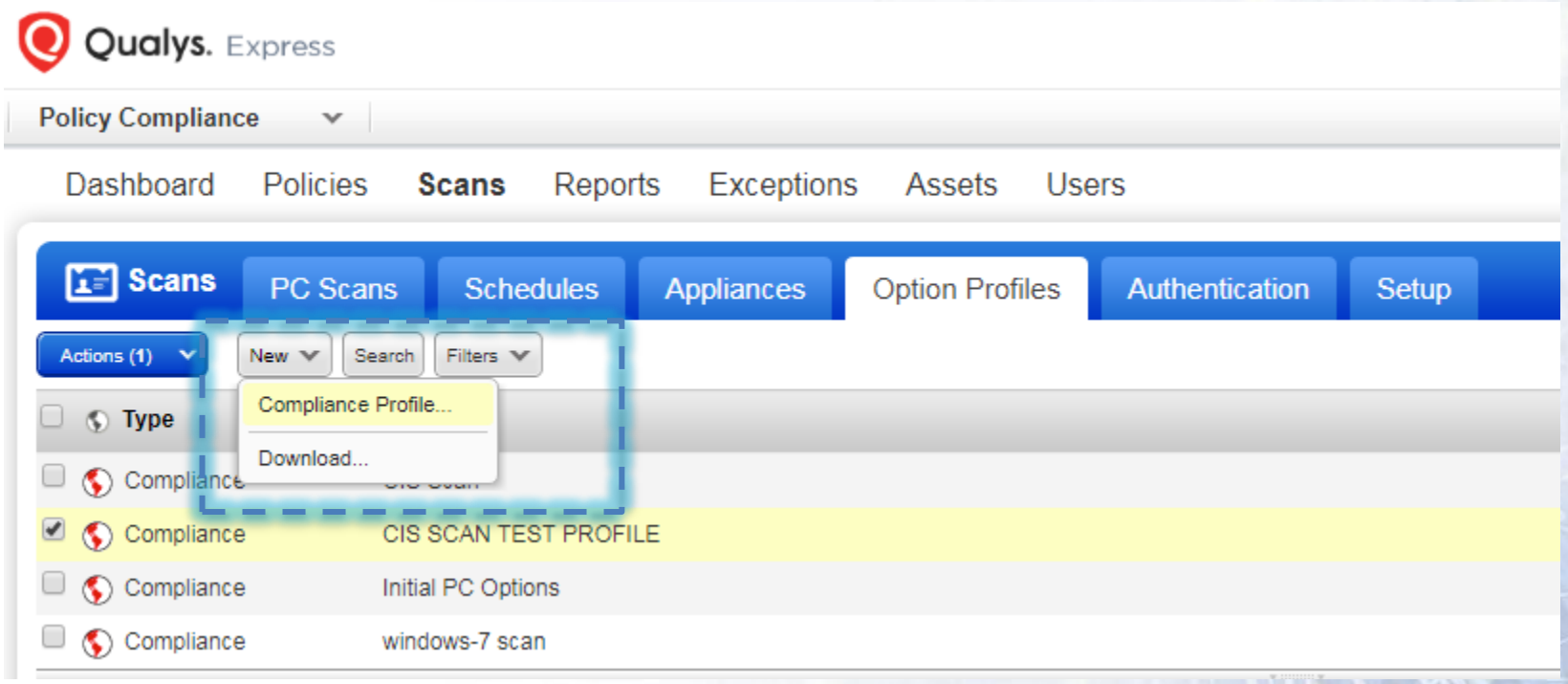
2. CONFIGURE SCAN SETTINGS

QUALYS DEMO – SECURITY HARDENING



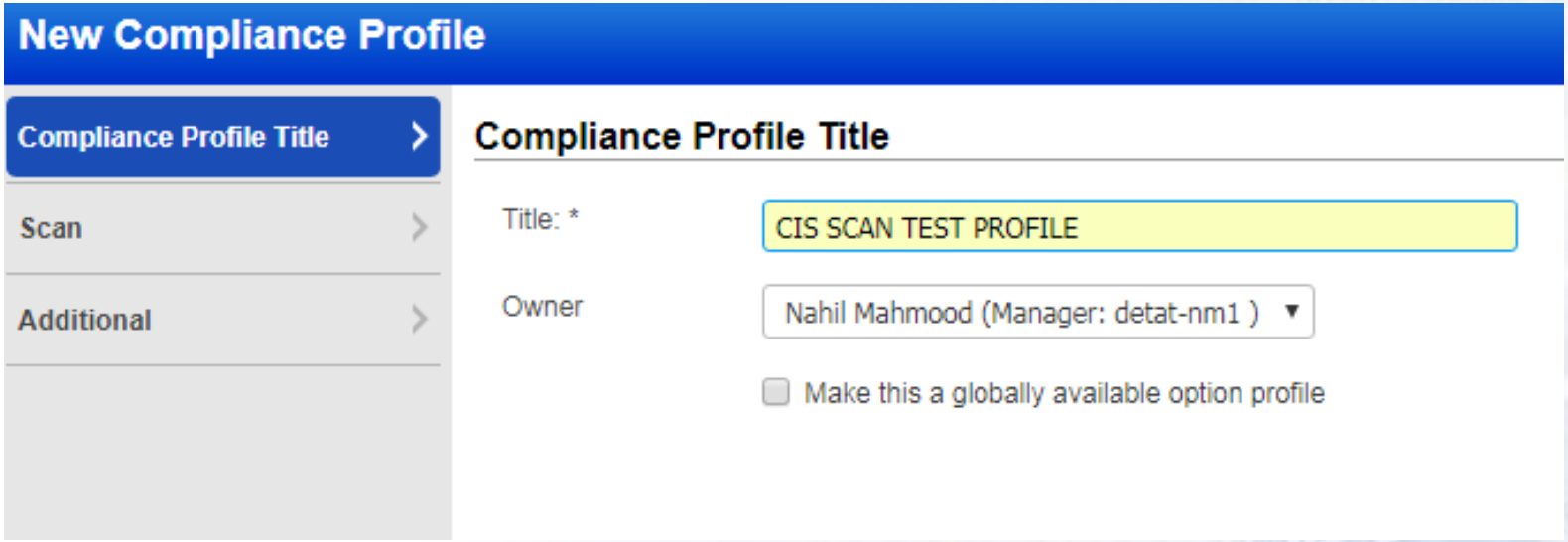
2. CONFIGURE SCAN SETTINGS

QUALYS DEMO – SECURITY HARDENING



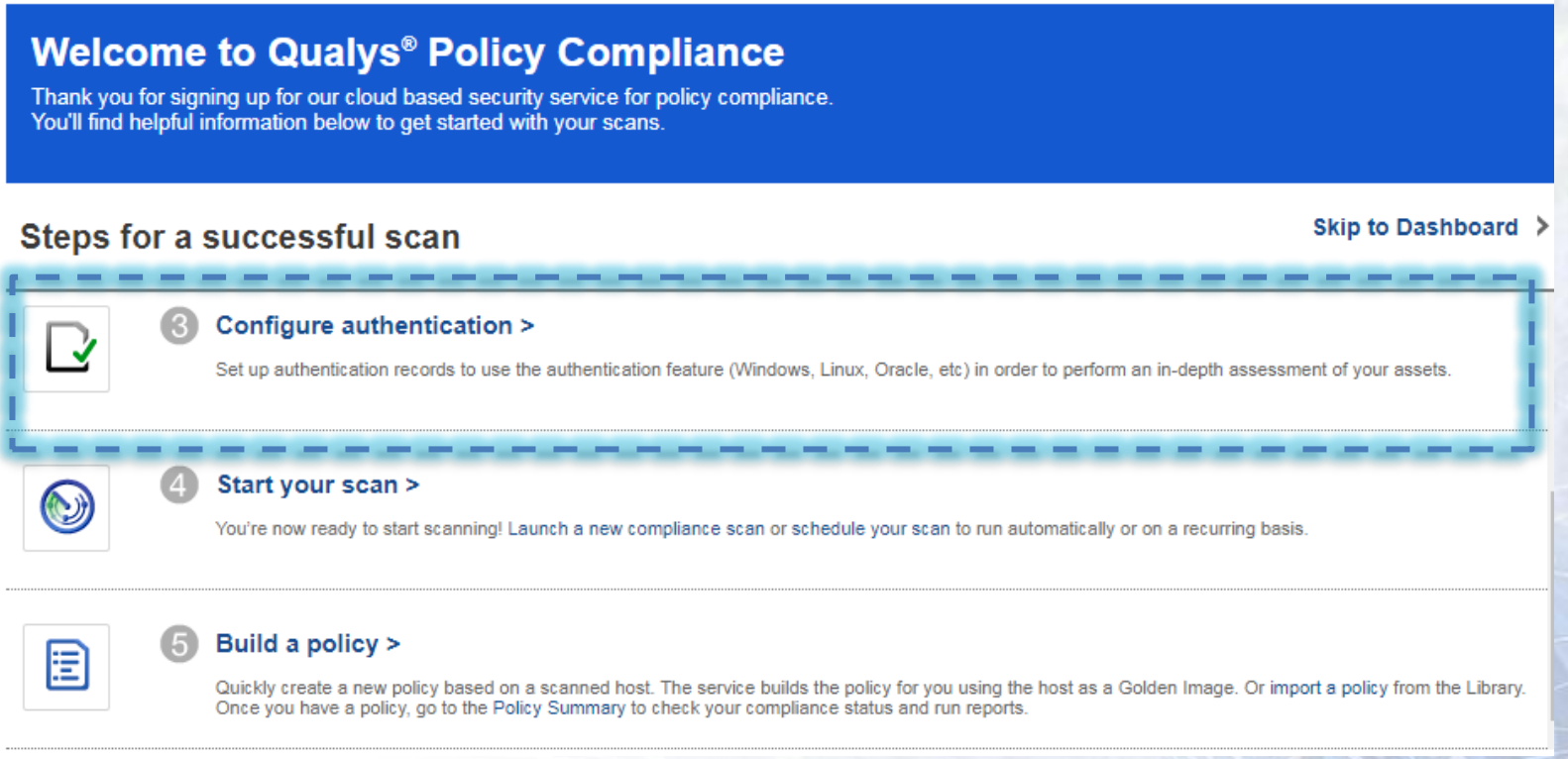
NEW COMPLIANCE PROFILE

QUALYS DEMO – SECURITY HARDENING



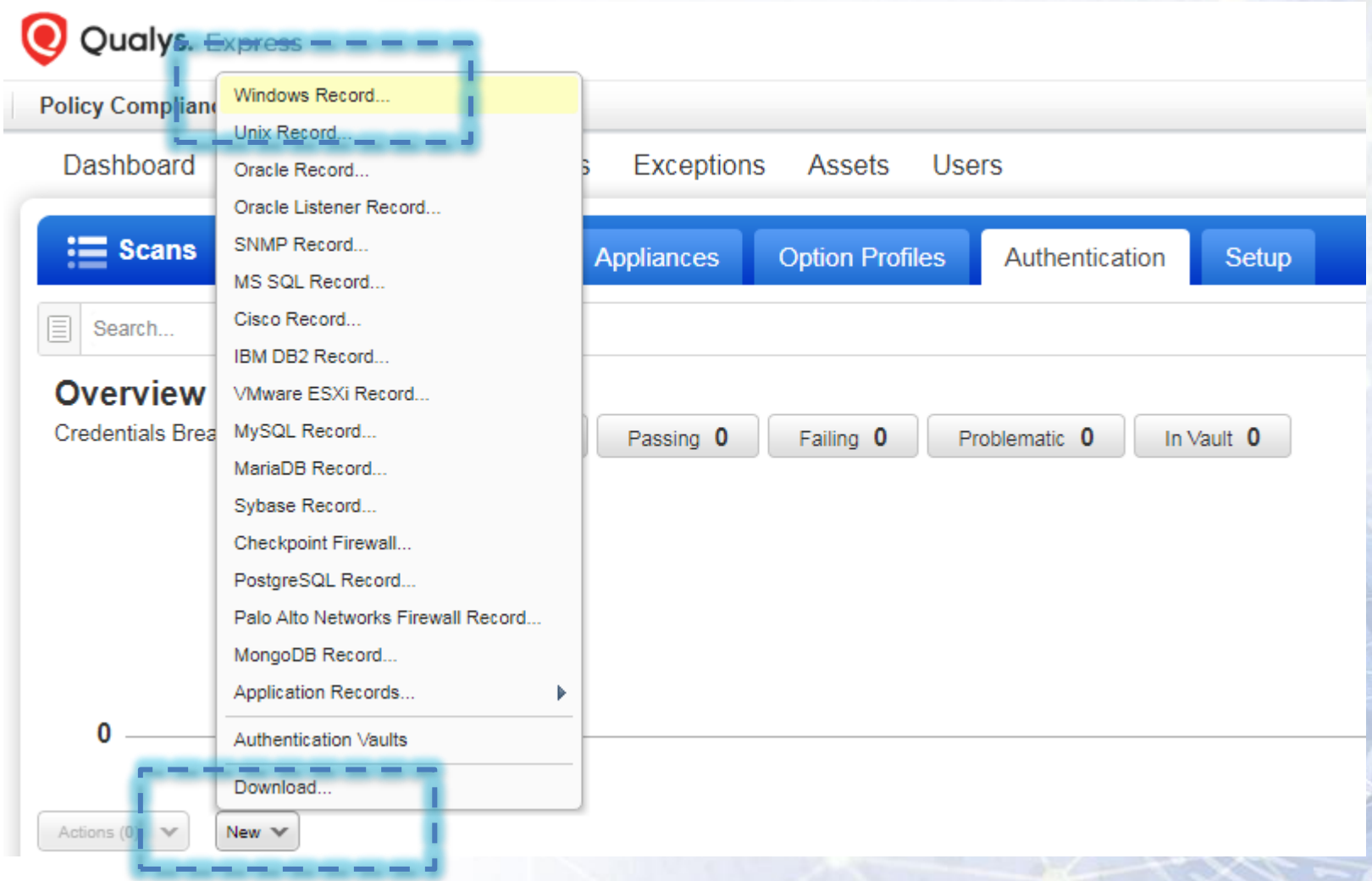
'CIS SCAN TEST PROFILE' CREATED

QUALYS DEMO – SECURITY HARDENING

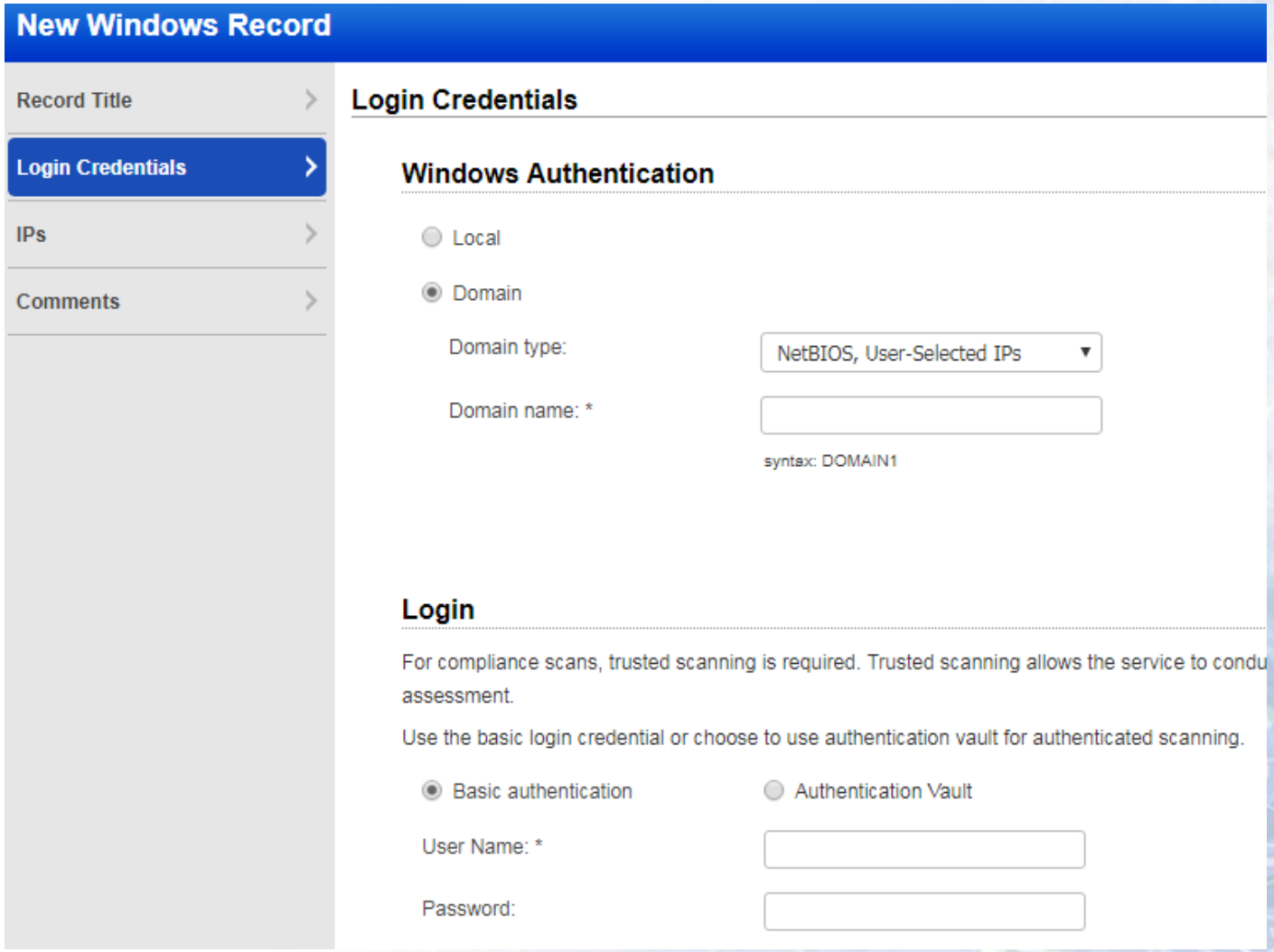


3. CONFIGURE AUTHENTICATION

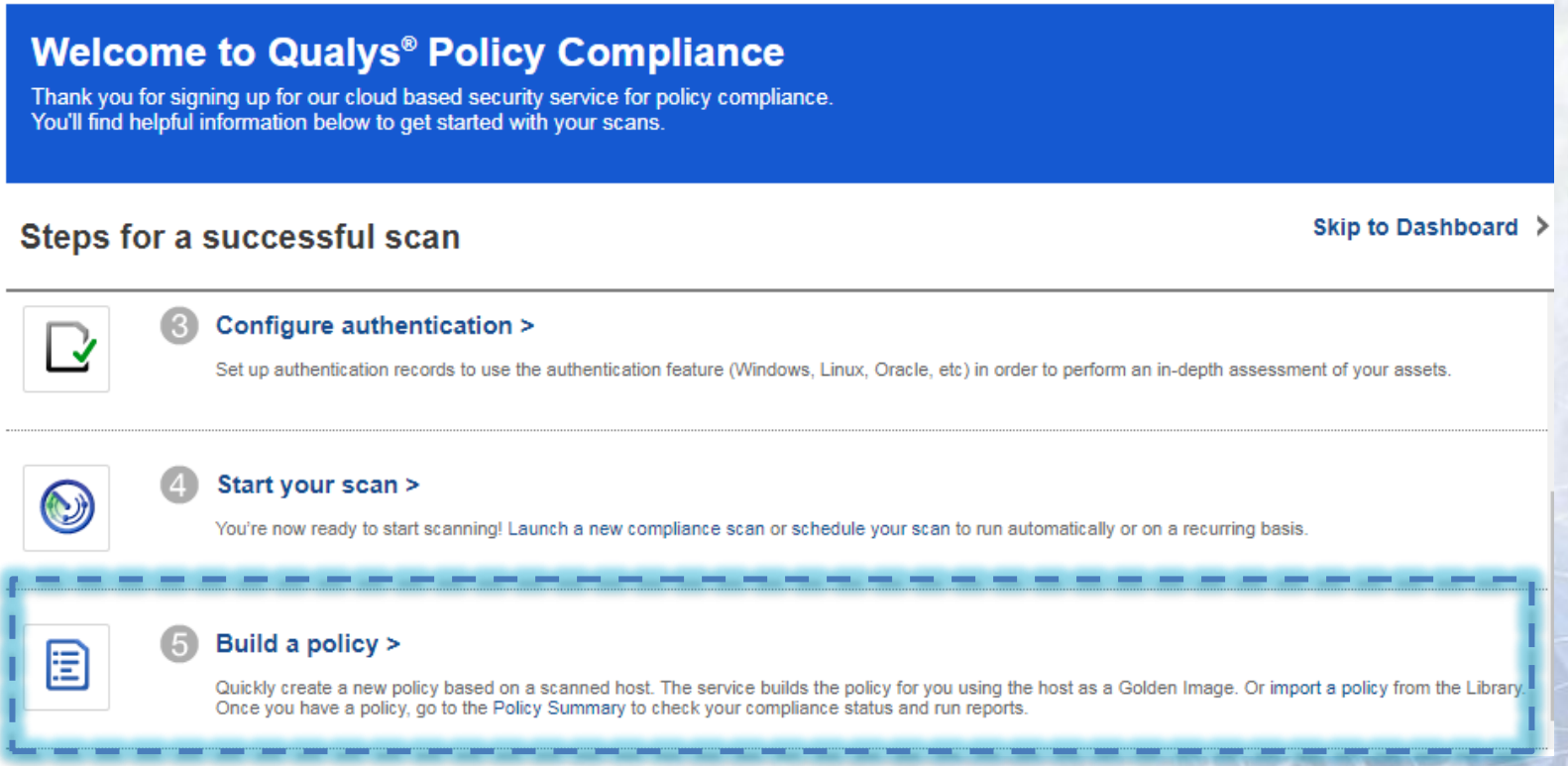
QUALYS DEMO – SECURITY HARDENING



QUALYS DEMO – SECURITY HARDENING

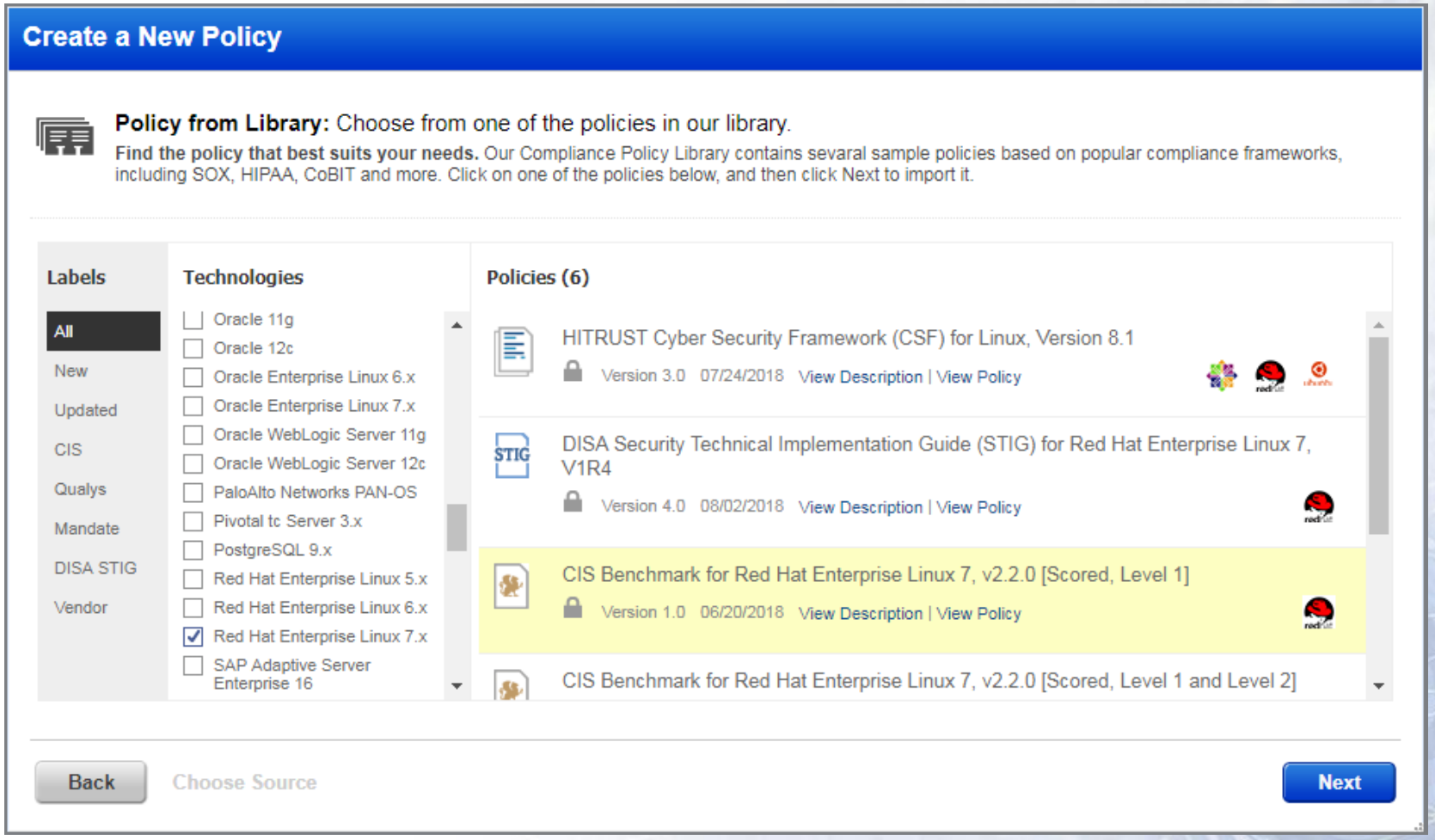


QUALYS DEMO – SECURITY HARDENING



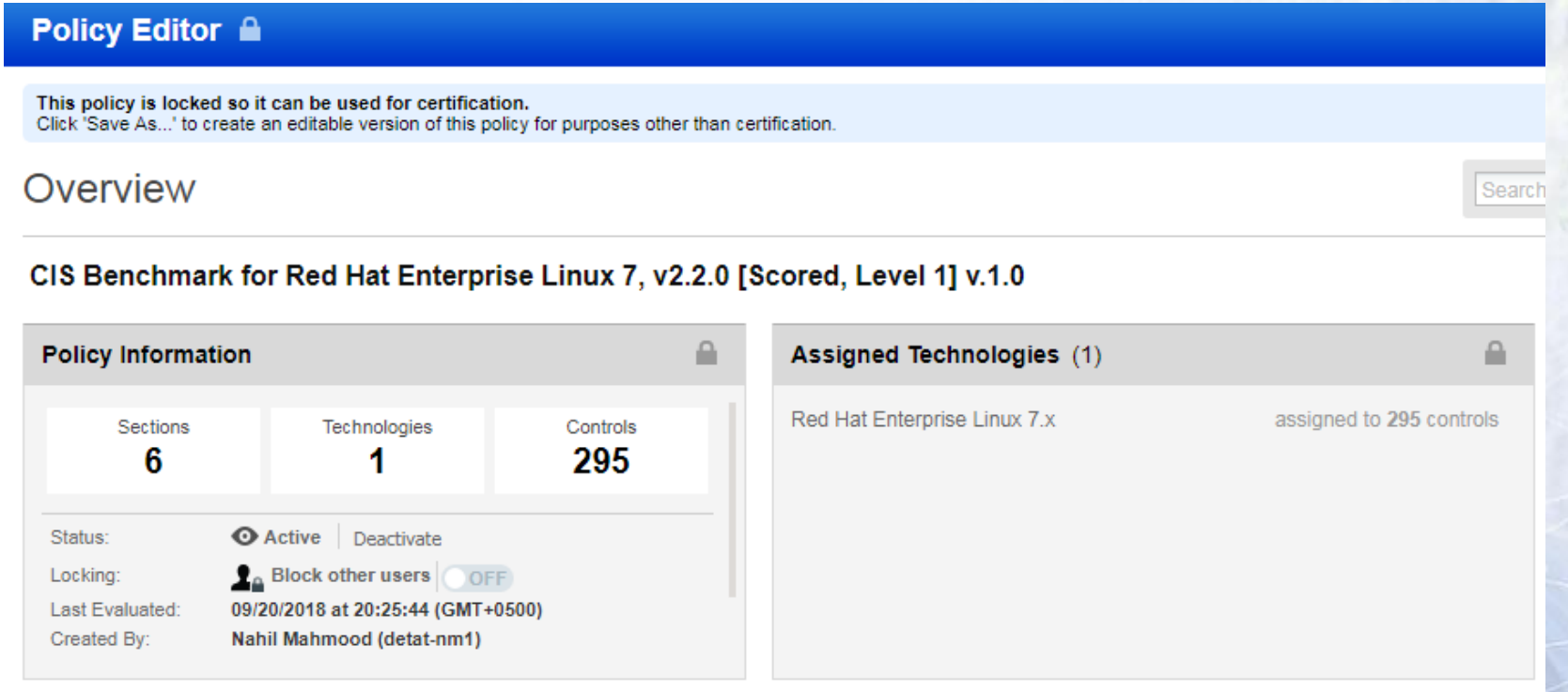
3. CONFIGURE AUTHENTICATION

QUALYS DEMO – SECURITY HARDENING



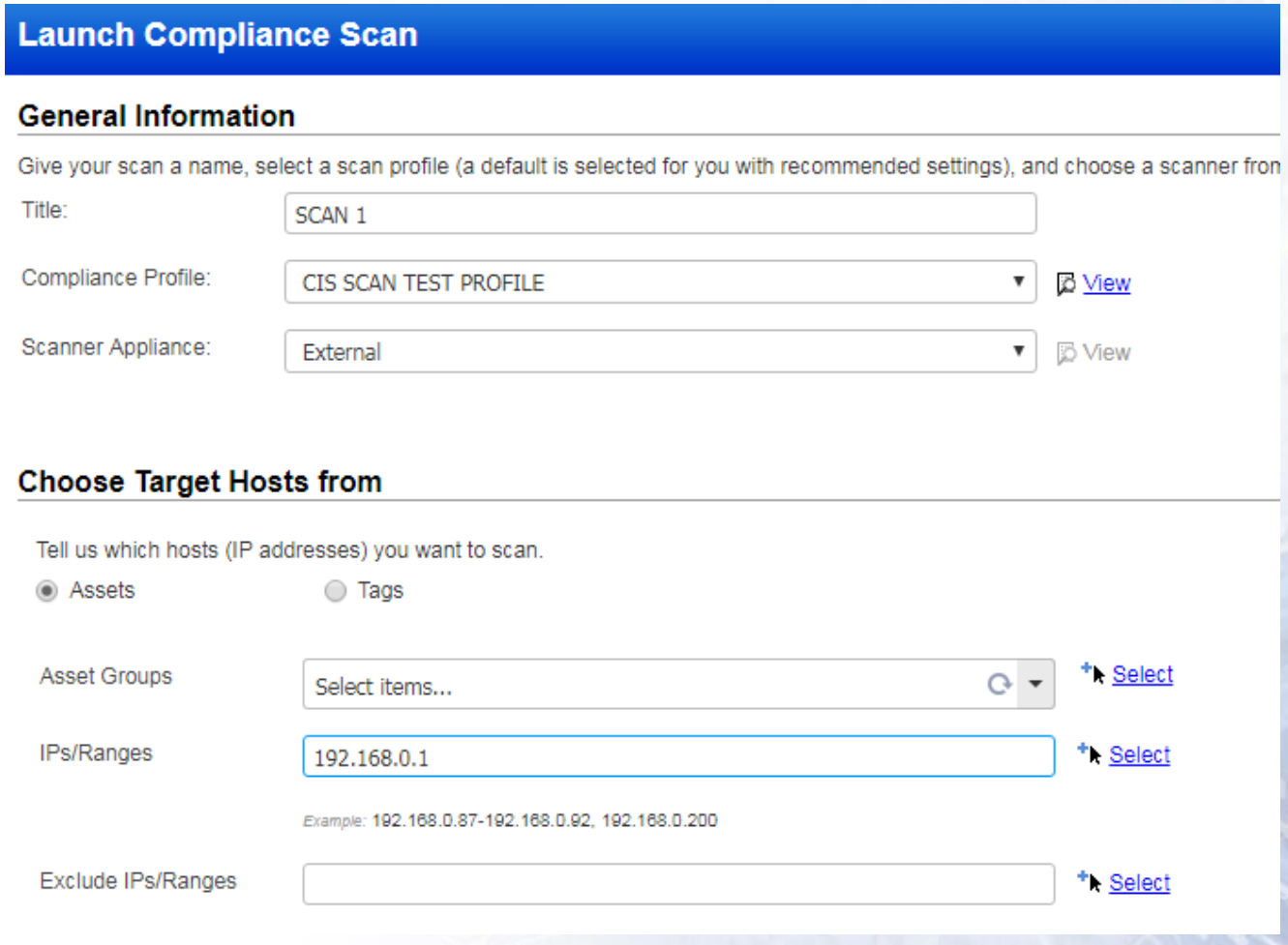
COMPLIANCE LIBRARY: CIS RED HAT ENT. LINUX 7

QUALYS DEMO – SECURITY HARDENING



POLICY EDITOR

QUALYS DEMO – SECURITY HARDENING



LAUNCH COMPLIANCE SCAN

QUALYS DEMO – SECURITY HARDENING II

- The scan features may also be adjusted from the main Qualys dashboard

END

- **Kali Linux**
- **Virtual Box**

- **Virtual Box**
- https://www.virtualbox.org/wiki/Downloads
- **Kali Linux**
- https://www.kali.org/
- https://www.osboxes.org/kali-linux/#kali-linux-2022-3-vbox

KALI

GET KALI BLOG DOCUMENTATION COMMUNITY COURSES DEVELOPERS ABOUT



The most advanced Penetration Testing Distribution

Kali Linux is an open-source, Debian-based Linux distribution geared towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering.

DOWNLOAD

DOCUMENTATION



VirtualBox

search...
Login Preferen

Download VirtualBox

Here you will find links to VirtualBox binaries and its source code.

About
Screenshots
Downloads
Documentation
End-user docs
Technical docs
Contribute
Community

VirtualBox binaries

By downloading, you agree to the terms and conditions of the respective license.

If you're looking for the latest VirtualBox 6.1 packages, see VirtualBox 6.1 builds. Version 6.1 will remain supported until December 2023.

VirtualBox 7.0.6 platform packages

- Windows hosts
- macOS / Intel hosts
- Developer preview for macOS / Arm64 (M1/M2) hosts
- Linux distributions
- Solaris hosts
- Solaris 11 IPS hosts

The binaries are released under the terms of the GPL version 3.

See the changelog for what has changed.

You might want to compare the checksums to verify the integrity of downloaded packages. *The SHA256 checksums should be favored as the MD5 algorithm must be treated as insecure!*

- SHA256 checksums, MD5 checksums

Note: After upgrading VirtualBox it is recommended to upgrade the guest additions as well.

VirtualBox 7.0.6 Oracle VM VirtualBox Extension Pack

- All supported platforms

Support VirtualBox RDP, disk encryption, NVMe and PXE boot for Intel cards. See this chapter from the User Manual for an introduction to this Extension Pack. The Extension Pack binaries are released under the VirtualBox Personal Use and Evaluation License (PUEL). *Please install the same version extension pack as your installed version of VirtualBox.*

VirtualBox 7.0.6 Software Developer Kit (SDK)

- All platforms

User Manual


CentOS
archlinux
fedora
openSUSE
& Many More
debian
x86
ORACLE
VirtualBox
copyright: osboxes.org

Oracle VM VirtualBox Manager

File Machine Help

New Settings Discard Start

Machine Tools Global Tools

CyberOps Workstation 64
Powered Off

Windows 7
Powered Off

Server 2016
Powered Off

WinDev1903Eval
Powered Off

Welcome to VirtualBox!

The left part of this window lists all virtual machines and virtual machine groups on your computer.

The right part of this window represents a set of tools which are currently opened (or can be opened) for the currently chosen machine. For a list of currently available tools check the corresponding menu at the right side of the main tool bar located at the top of the window. This list will be extended with new tools in future releases.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for more information and latest news.

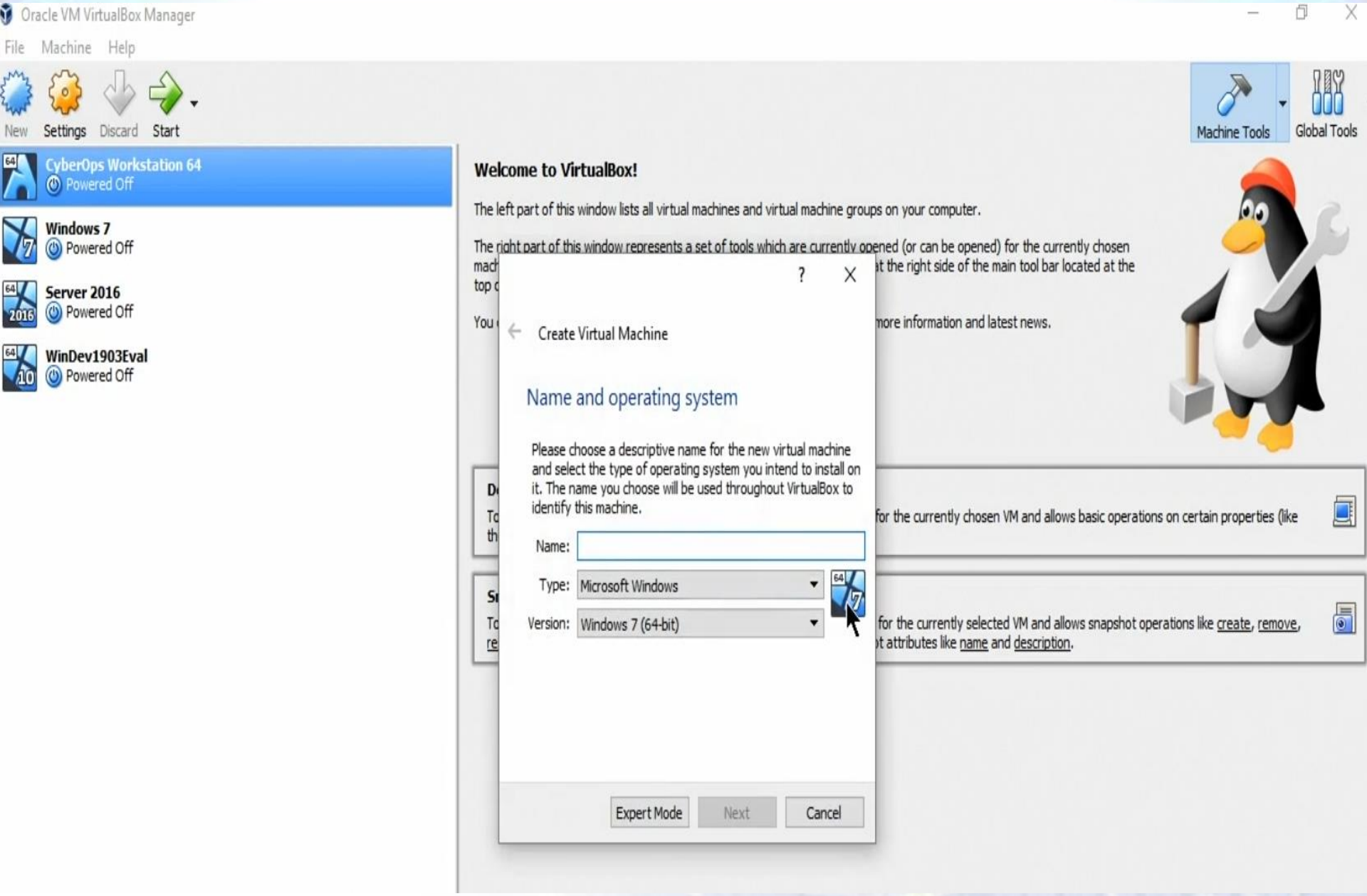


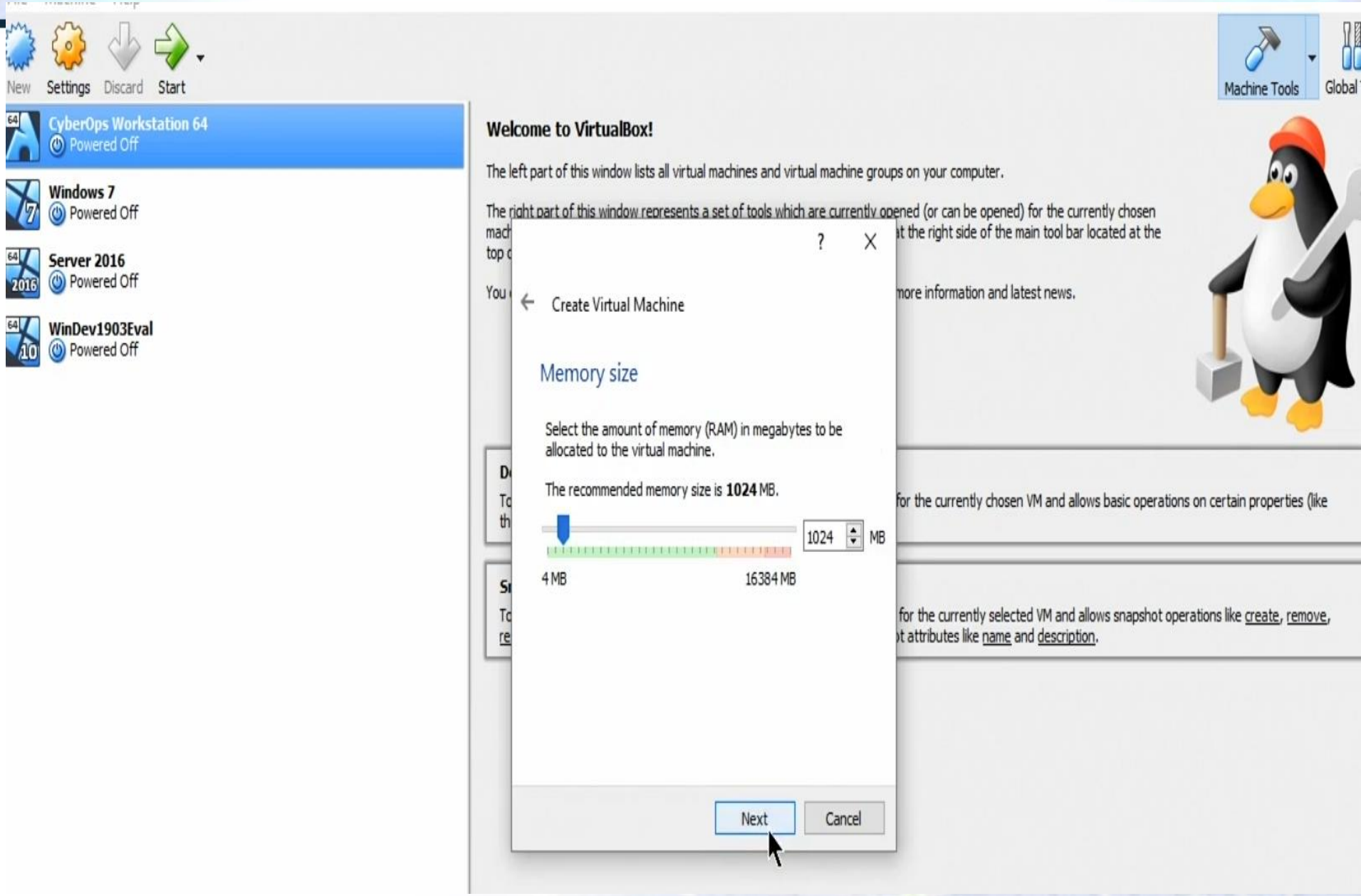
Details

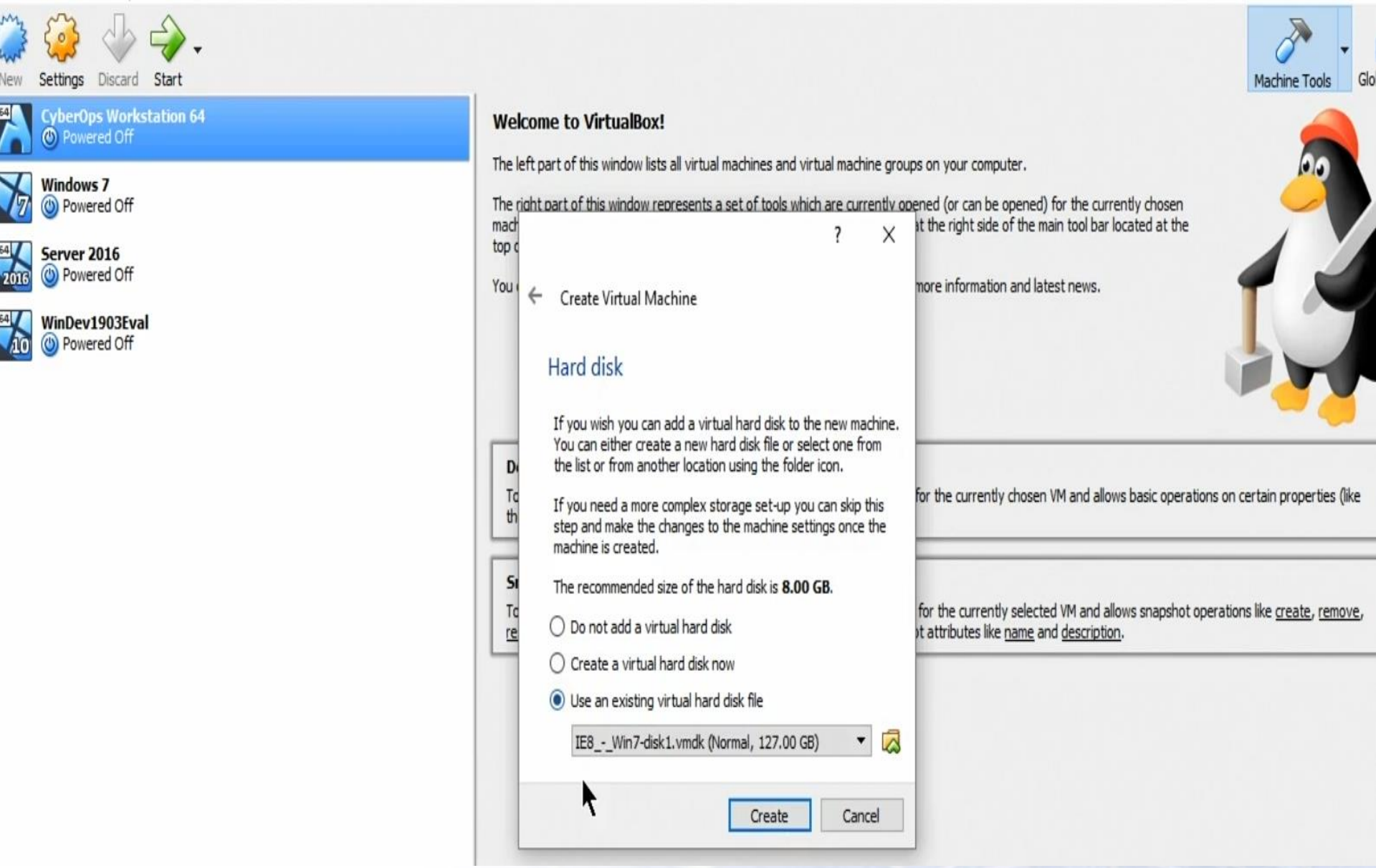
Tool to observe virtual machine (VM) details. Reflects groups of properties for the currently chosen VM and allows basic operations on certain properties (like the machine storage devices).

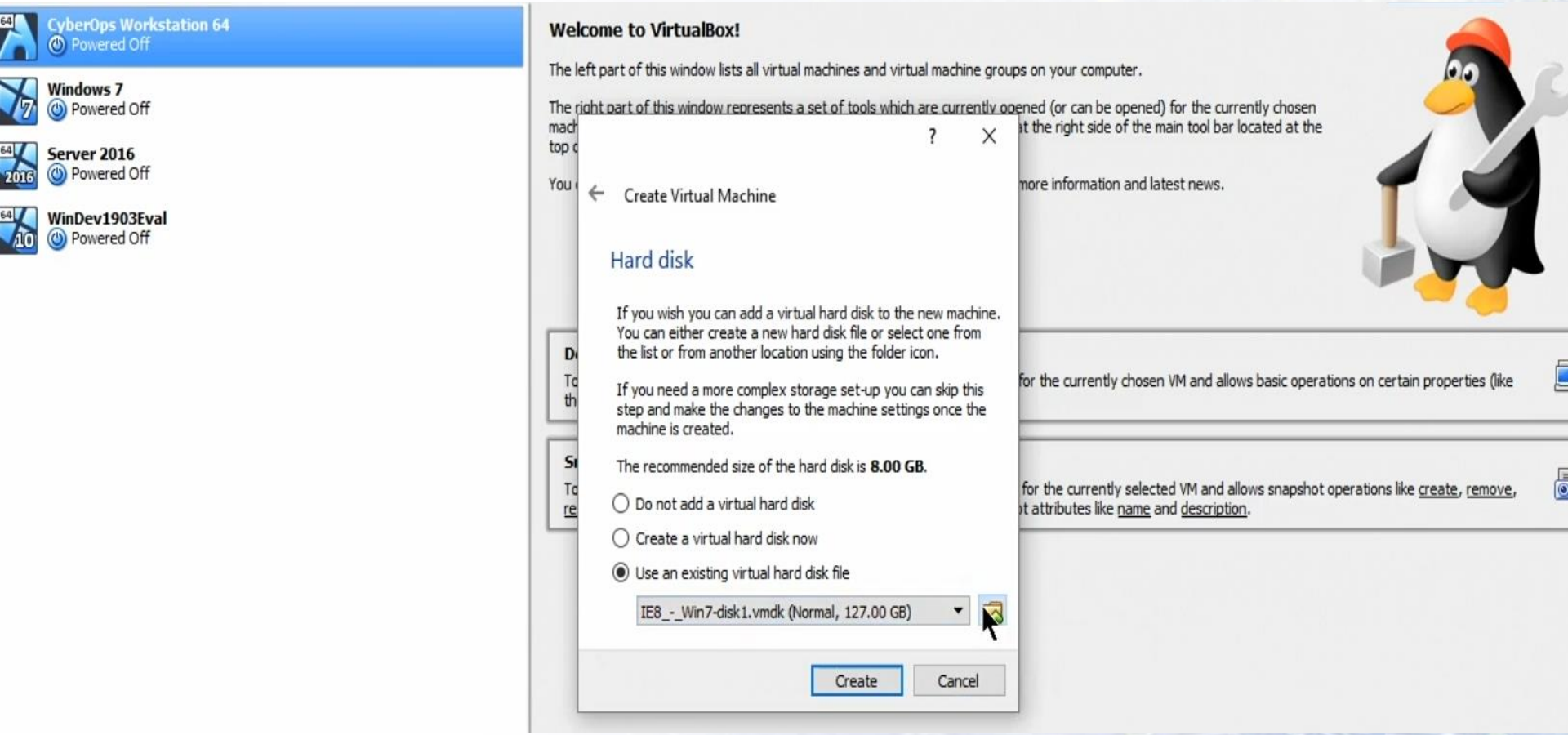
Snapshots

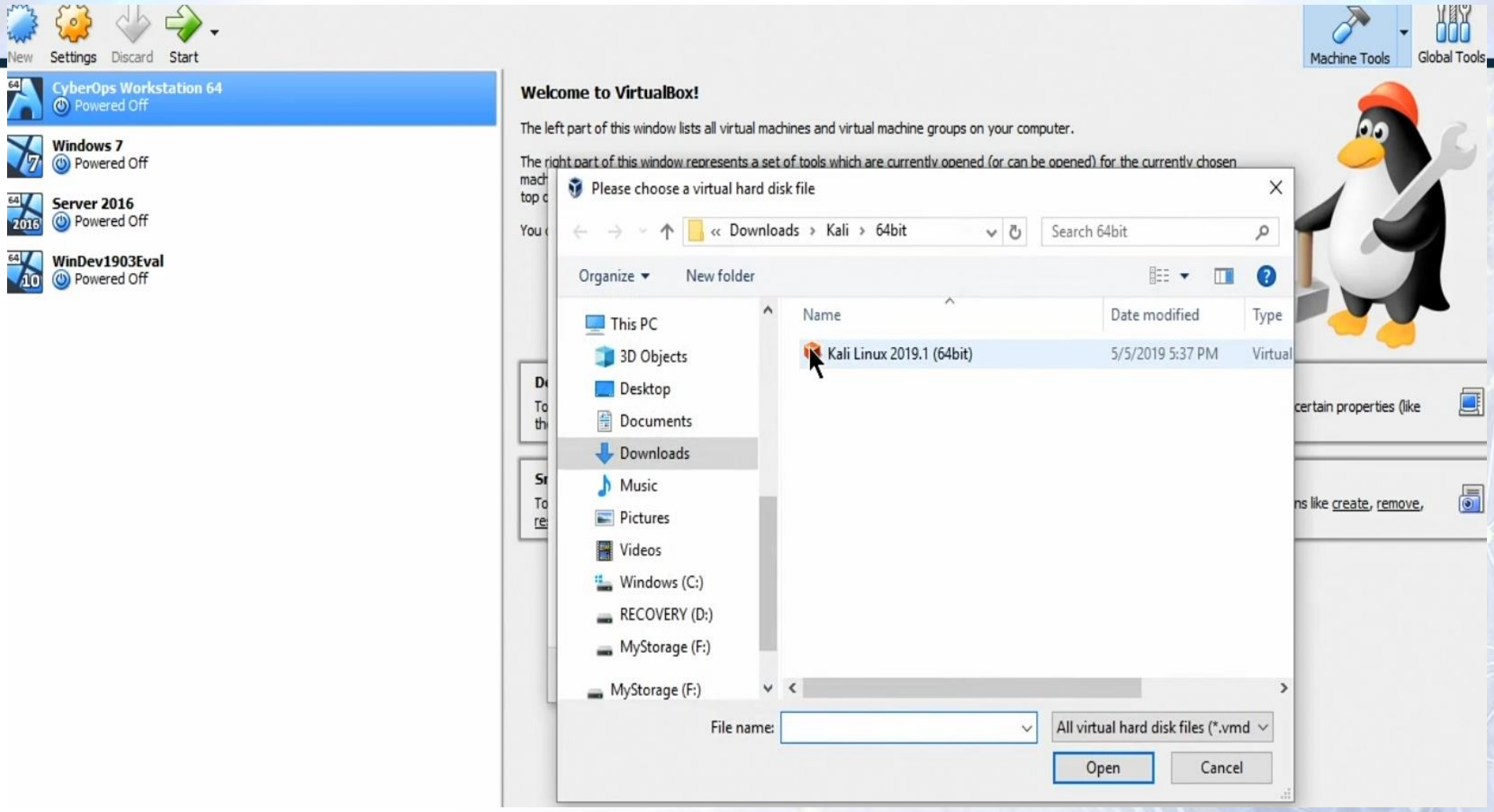
Tool to control virtual machine (VM) snapshots. Reflects snapshots created for the currently selected VM and allows snapshot operations like create, remove, restore (make current) and observe their properties. Allows to edit snapshot attributes like name and description.

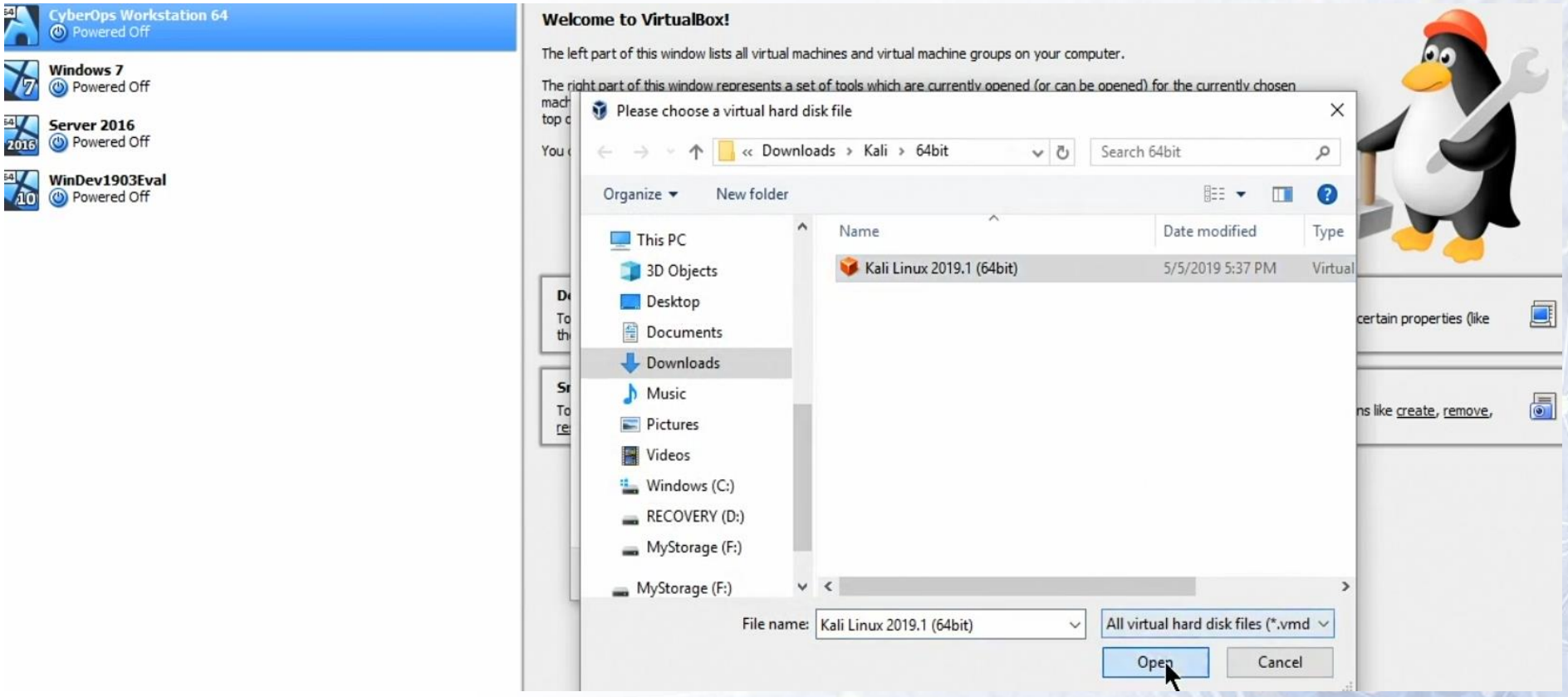

Oracle VM VirtualBox Manager
File Machine Help
New Settings Discard Start
Machine Tools
Global Tools
CyberOps Workstation 64
Powered Off
Windows 7
Powered Off
Server 2016
Powered Off
WinDev1903Eval
Powered Off
Welcome to VirtualBox!
The left part of this window lists all virtual machines and virtual machine groups on your computer.
The right part of this window represents a set of tools which are currently opened (or can be opened) for the currently chosen
Create Virtual Machine
Name and operating system
Please choose a descriptive name for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.
Name:
Type: Microsoft Windows
Version: Windows 7 (64-bit)
Expert Mode
Next
Cancel

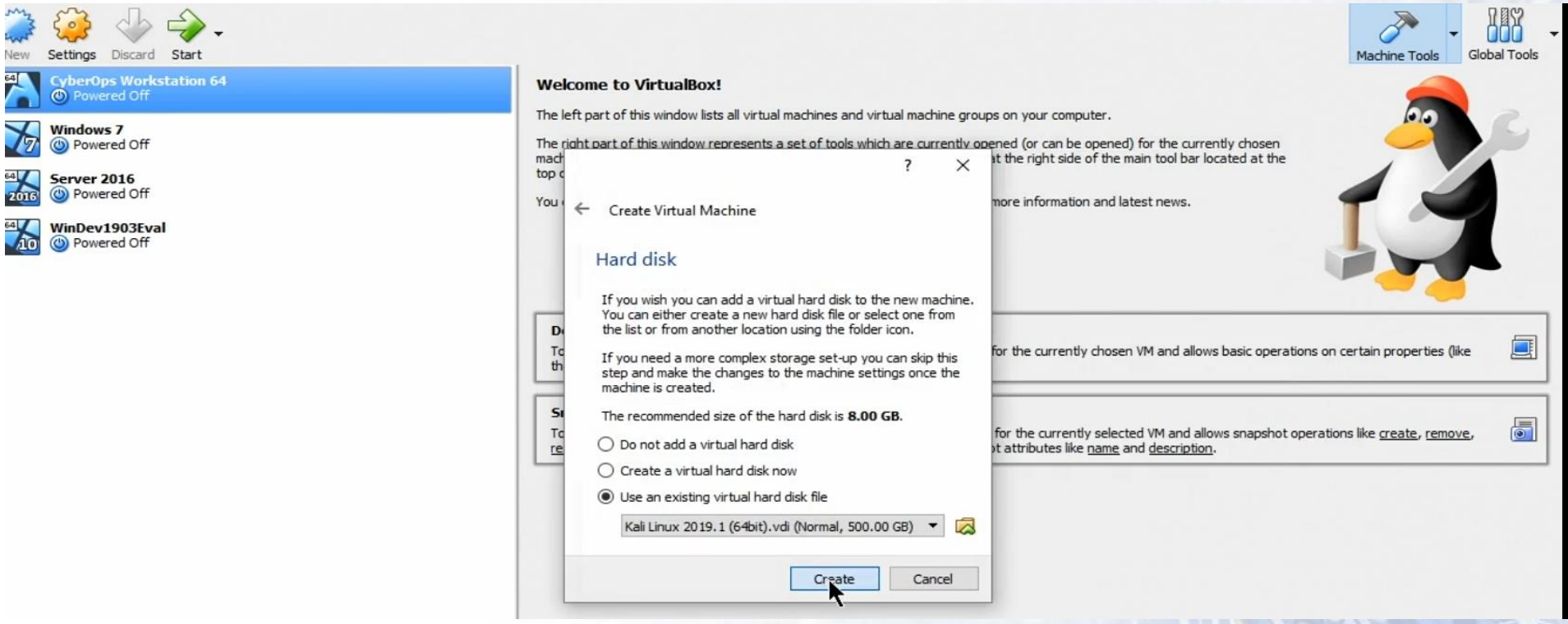

New
Settings
Discard
Start
Machine Tools
CyberOps Workstation 64
Powered Off
Windows 7
Powered Off
Server 2016
Powered Off
WinDev1903Eval
Powered Off
Welcome to VirtualBox!
The left part of this window lists all virtual machines and virtual machine groups on your computer.
The right part of this window represents a set of tools which are currently opened (or can be opened) for the currently chosen
at the right side of the main tool bar located at the
more information and latest news.
Create Virtual Machine
Memory size
Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.
The recommended memory size is 1024 MB.
1024
MB
4 MB
16384 MB
for the currently chosen VM and allows basic operations on certain properties (like
for the currently selected VM and allows snapshot operations like create, remove,
attributes like name and description.
Next
Cancel

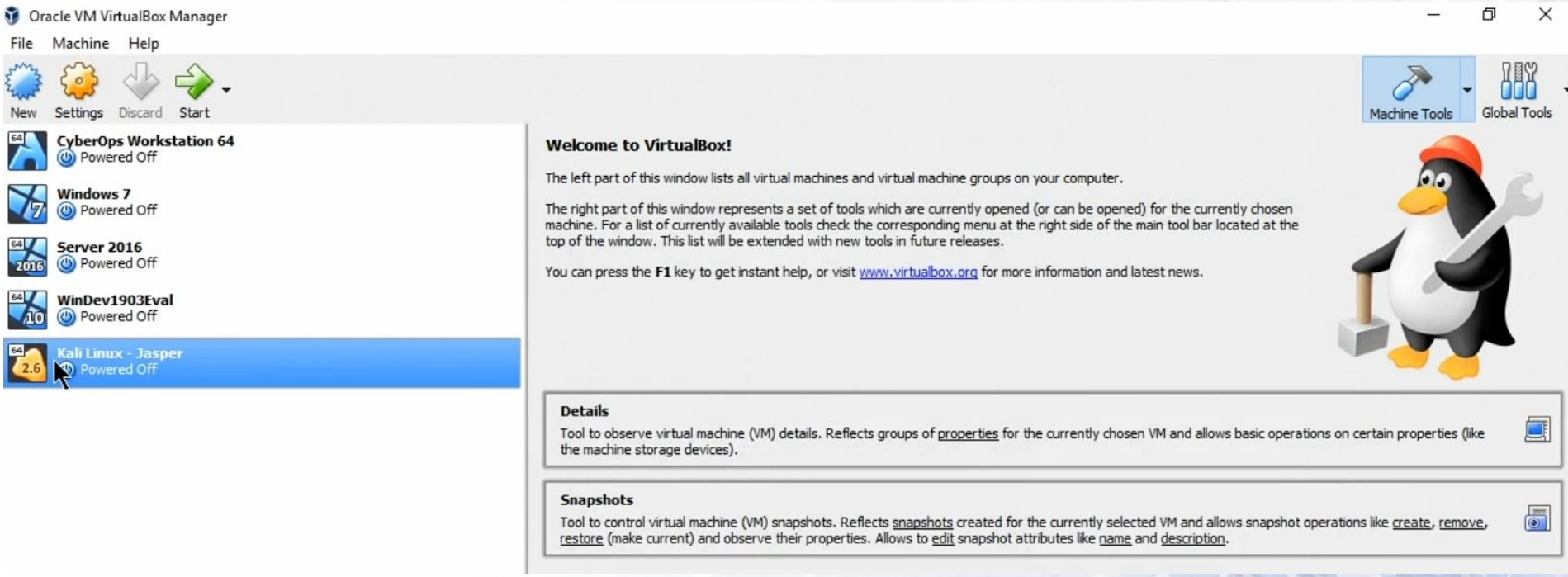

New
Settings
Discard
Start
Machine Tools
CyberOps Workstation 64
Powered Off
Windows 7
Powered Off
Server 2016
Powered Off
WinDev1903Eval
Powered Off
Welcome to VirtualBox!
The left part of this window lists all virtual machines and virtual machine groups on your computer.
Create Virtual Machine
Hard disk
If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.
If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.
The recommended size of the hard disk is 8.00 GB.
Do not add a virtual hard disk
Create a virtual hard disk now
Use an existing virtual hard disk file
IE8_-_Win7-disk1.vmdk (Normal, 127.00 GB)
Create
Cancel

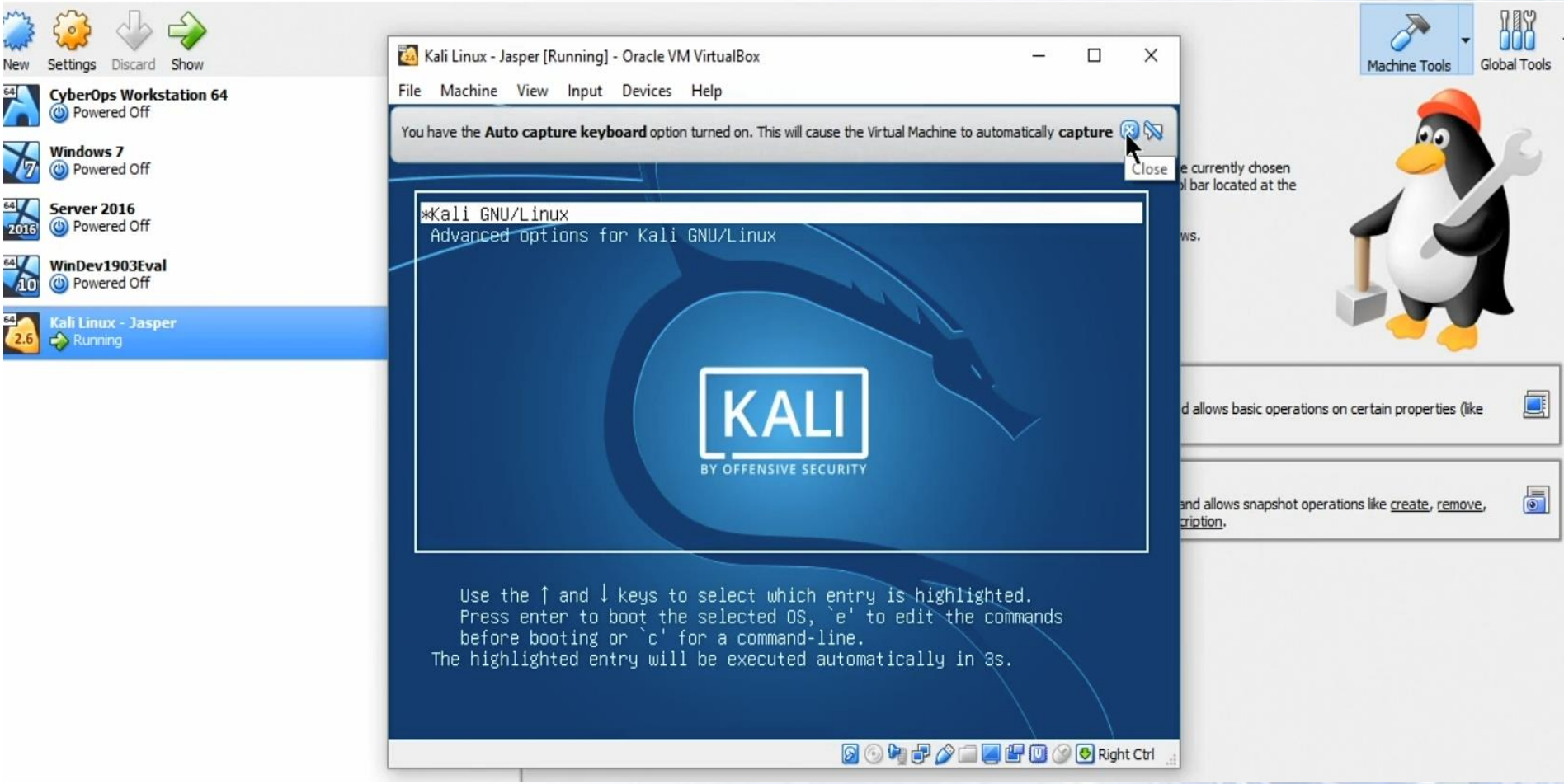

CyberOps Workstation 64
Powered Off
Windows 7
Powered Off
Server 2016
Powered Off
WinDev1903Eval
Powered Off
Welcome to VirtualBox!
The left part of this window lists all virtual machines and virtual machine groups on your computer.
Create Virtual Machine
Hard disk
If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.
If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.
The recommended size of the hard disk is 8.00 GB.
Do not add a virtual hard disk
Create a virtual hard disk now
Use an existing virtual hard disk file
IE8_-_Win7-disk1.vmdk (Normal, 127.00 GB)
Create
Cancel

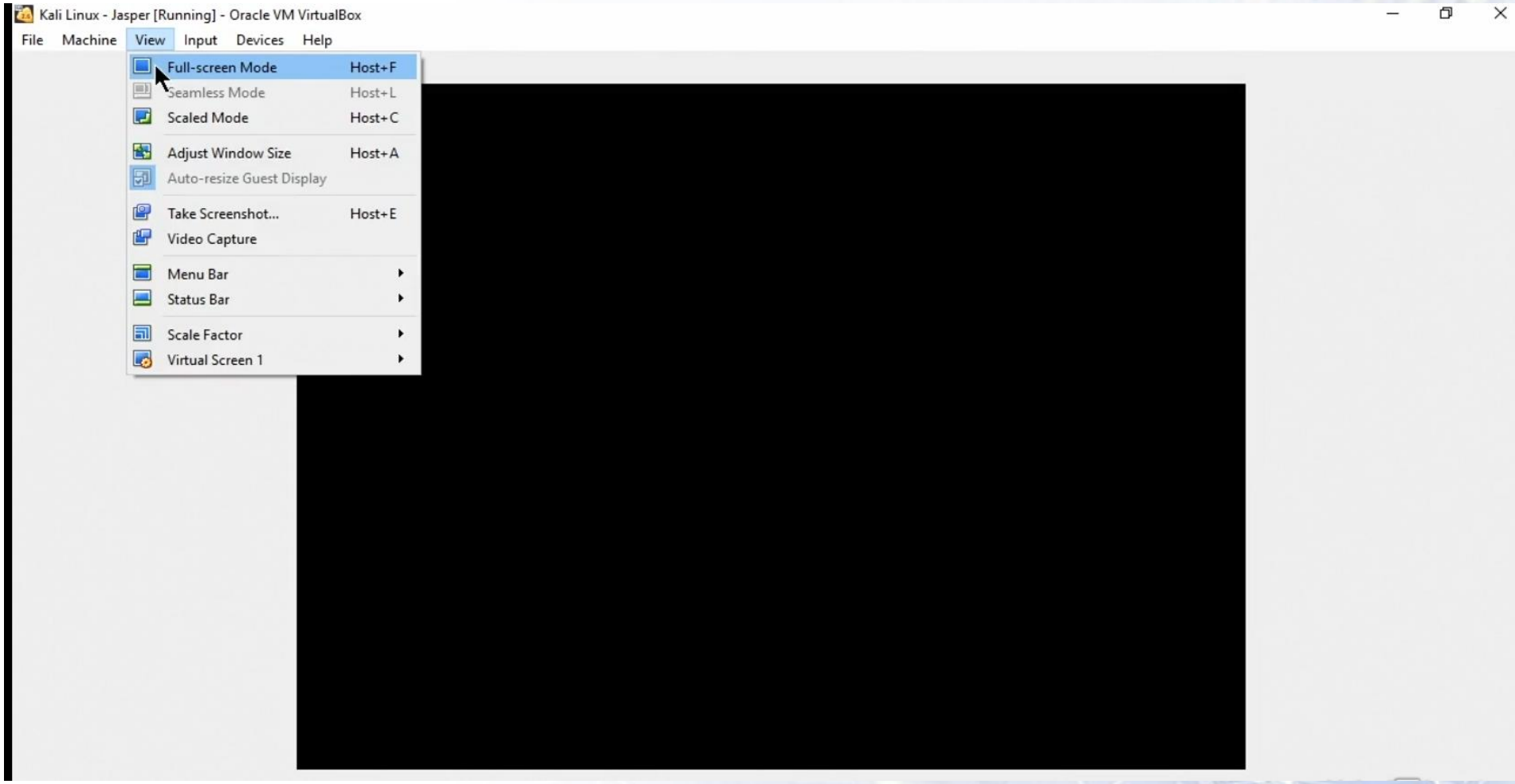

New
Settings
Discard
Start
Machine Tools
Global Tools
CyberOps Workstation 64
Powered Off
Windows 7
Powered Off
Server 2016
Powered Off
WinDev1903Eval
Powered Off
Welcome to VirtualBox!
The left part of this window lists all virtual machines and virtual machine groups on your computer.
Please choose a virtual hard disk file
« Downloads › Kali › 64bit
Search 64bit
Organize
New folder
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Windows (C:)
RECOVERY (D:)
MyStorage (F:)
MyStorage (F:)
Name
Date modified
Type
Kali Linux 2019.1 (64bit)
5/5/2019 5:37 PM
Virtual
File name:
All virtual hard disk files (*.vmd
Open
Cancel
certain properties (like
create, remove,

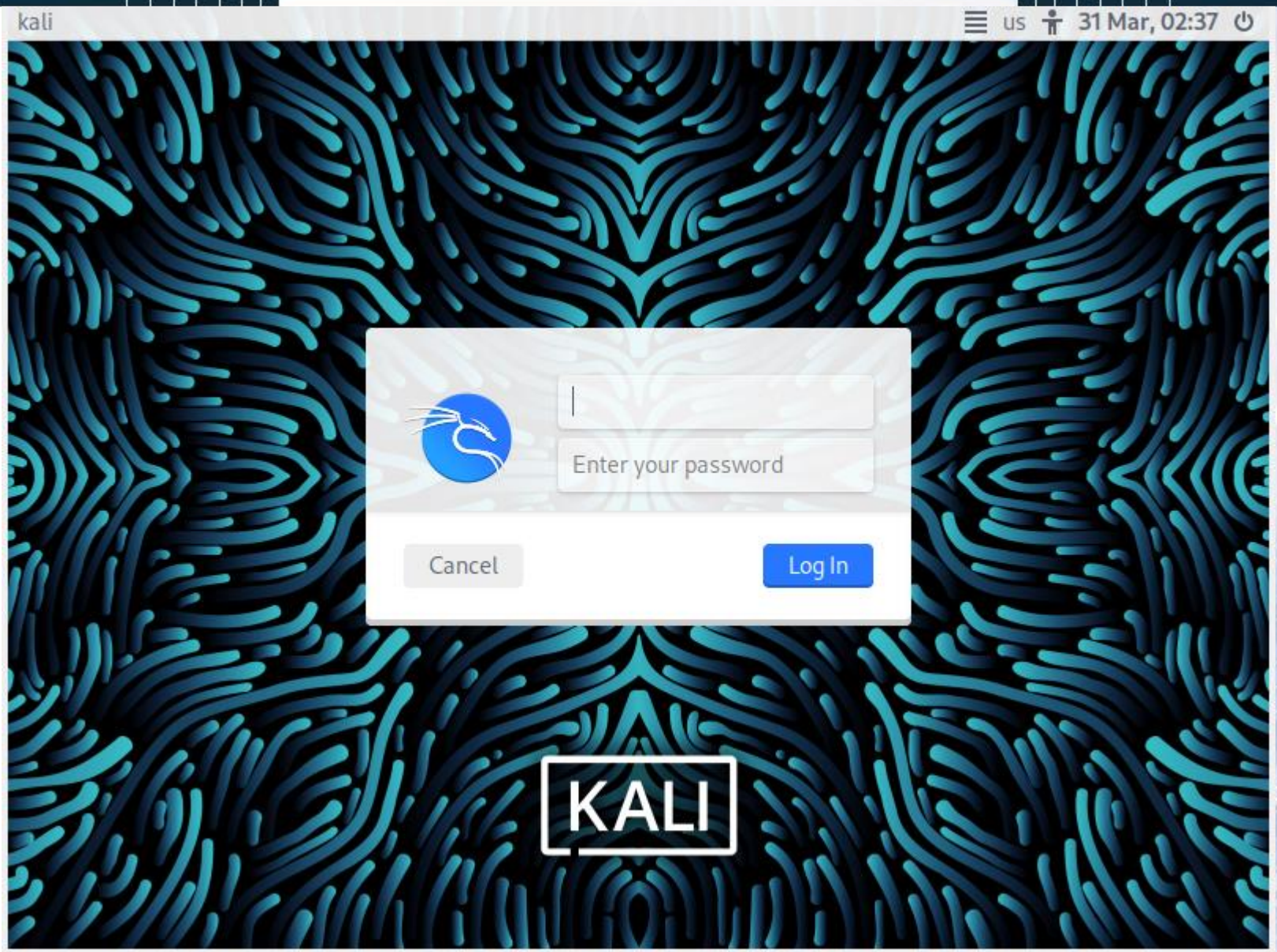

CyberOps Workstation 64
Powered Off
Windows 7
Powered Off
Server 2016
Powered Off
WinDev1903Eval
Powered Off
Welcome to VirtualBox!
The left part of this window lists all virtual machines and virtual machine groups on your computer.
The right part of this window represents a set of tools which are currently opened (or can be opened) for the currently chosen
Please choose a virtual hard disk file
« Downloads › Kali › 64bit
Search 64bit
Organize
New folder
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Windows (C:)
RECOVERY (D:)
MyStorage (F:)
MyStorage (F:)
Name
Date modified
Type
Kali Linux 2019.1 (64bit)
5/5/2019 5:37 PM
Virtual
certain properties (like
ns like create, remove,
File name:
Kali Linux 2019.1 (64bit)
All virtual hard disk files (*.vmd
Open
Cancel

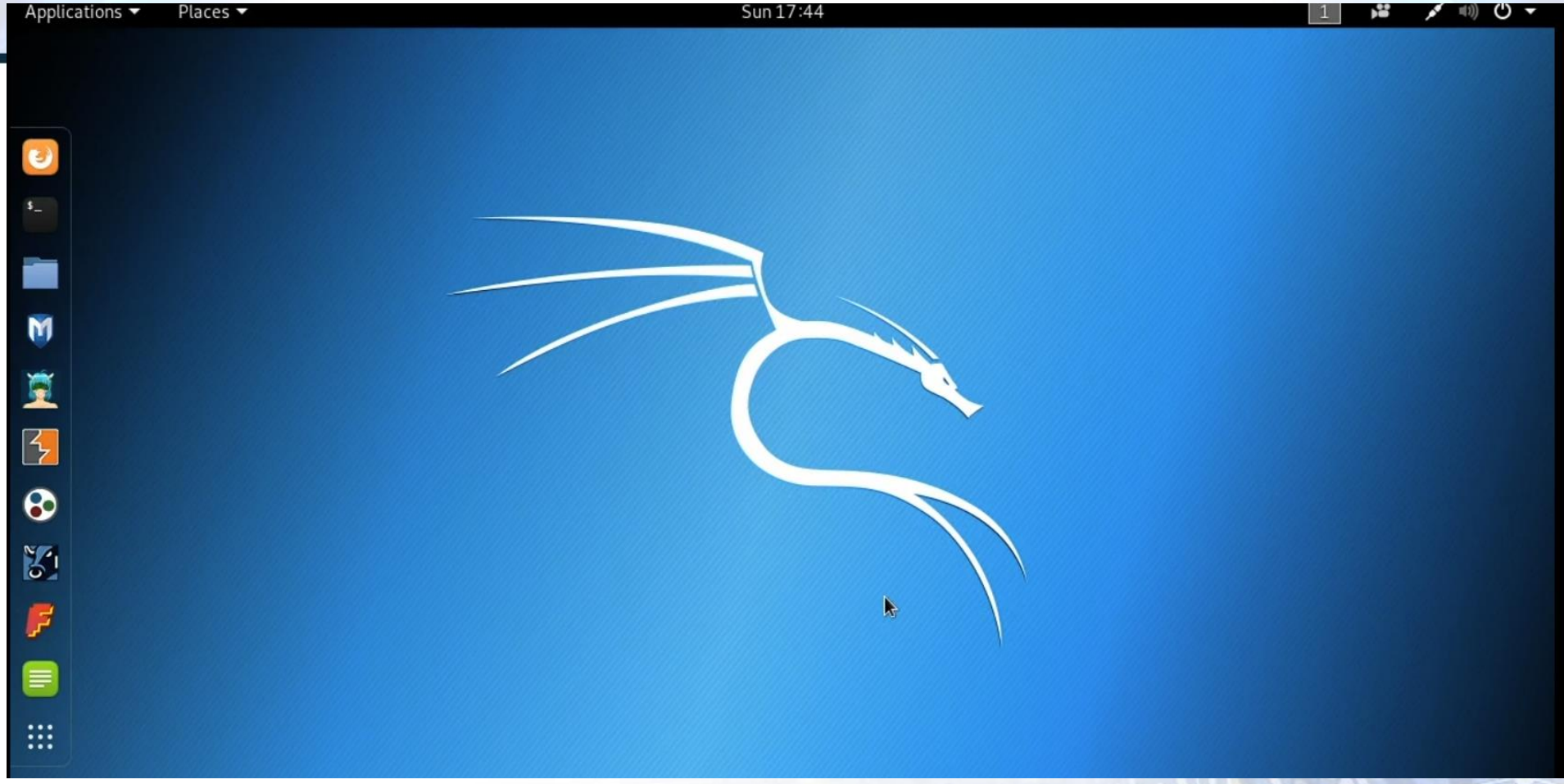

New
Settings
Discard
Start
Machine Tools
Global Tools
CyberOps Workstation 64
Powered Off
Windows 7
Powered Off
Server 2016
Powered Off
WinDev1903Eval
Powered Off
Welcome to VirtualBox!
The left part of this window lists all virtual machines and virtual machine groups on your computer.
more information and latest news.
for the currently chosen VM and allows basic operations on certain properties (like
for the currently selected VM and allows snapshot operations like create, remove,
attributes like name and description.
Create Virtual Machine
Hard disk
If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.
If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.
The recommended size of the hard disk is 8.00 GB.
Do not add a virtual hard disk
Create a virtual hard disk now
Use an existing virtual hard disk file
Kali Linux 2019.1 (64bit).vdi (Normal, 500.00 GB)
Create
Cancel

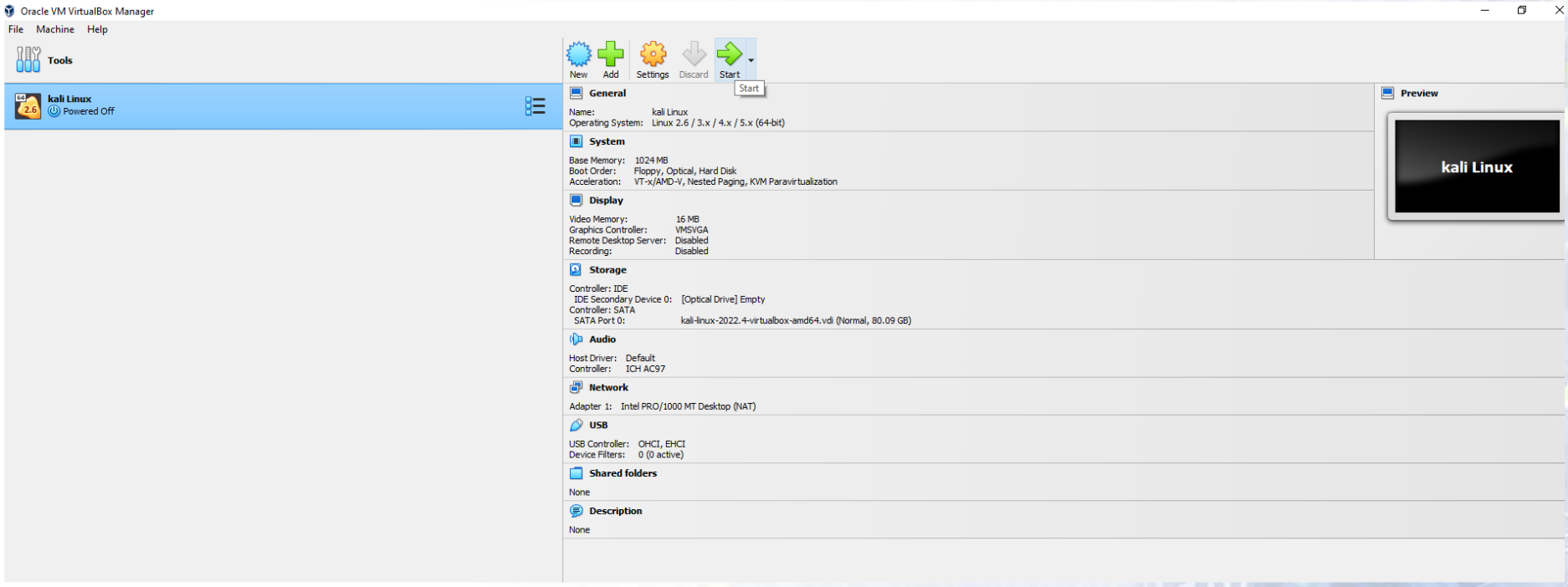

Oracle VM VirtualBox Manager
File
Machine
Help
New
Settings
Discard
Start
Machine Tools
Global Tools
CyberOps Workstation 64
Powered Off
Windows 7
Powered Off
Server 2016
Powered Off
WinDev1903Eval
Powered Off
Kali Linux - Jasper
Powered Off
Welcome to VirtualBox!
The left part of this window lists all virtual machines and virtual machine groups on your computer.
The right part of this window represents a set of tools which are currently opened (or can be opened) for the currently chosen machine. For a list of currently available tools check the corresponding menu at the right side of the main tool bar located at the top of the window. This list will be extended with new tools in future releases.
You can press the F1 key to get instant help, or visit www.virtualbox.org for more information and latest news.
Details
Tool to observe virtual machine (VM) details. Reflects groups of properties for the currently chosen VM and allows basic operations on certain properties (like the machine storage devices).
Snapshots
Tool to control virtual machine (VM) snapshots. Reflects snapshots created for the currently selected VM and allows snapshot operations like create, remove, restore (make current) and observe their properties. Allows to edit snapshot attributes like name and description.


New
Settings
Discard
Show
CyberOps Workstation 64
Powered Off
Windows 7
Powered Off
Server 2016
Powered Off
WinDev1903Eval
Powered Off
Kali Linux - Jasper
Running
Kali Linux - Jasper [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
You have the Auto capture keyboard option turned on. This will cause the Virtual Machine to automatically capture
Close
*Kali GNU/Linux
Advanced options for Kali GNU/Linux
KALI
BY OFFENSIVE SECURITY
Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, `e' to edit the commands
before booting or `c' for a command-line.
The highlighted entry will be executed automatically in 3s.
Right Ctrl
Machine Tools
Global Tools
currently chosen
bar located at the
ws.
allows basic operations on certain properties (like
and allows snapshot operations like create, remove,
cription.


Kali Linux - Jasper [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Full-screen Mode Host+F
Seamless Mode Host+L
Scaled Mode Host+C
Adjust Window Size Host+A
Auto-resize Guest Display
Take Screenshot... Host+E
Video Capture
Menu Bar
Status Bar
Scale Factor
Virtual Screen 1


kali
us
31 Mar, 02:37
Enter your password
Cancel
Log In
KALI


Applications
Places
Sun 17:44
1


Oracle VM VirtualBox Manager
File
Machine
Help
Tools
kali Linux
Powered Off
New
Add
Settings
Discard
Start
Start
General
Name: kali Linux
Operating System: Linux 2.6 / 3.x / 4.x / 5.x (64-bit)
System
Base Memory: 1024 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, KVM Paravirtualization
Display
Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: kali-linux-2022.4-virtualbox-amd64.vdi (Normal, 80.09 GB)
Audio
Host Driver: Default
Controller: ICH AC97
Network
Adapter 1: Intel PRO/1000 MT Desktop (NAT)
USB
USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)
Shared folders
None
Description
None
Preview
kali Linux

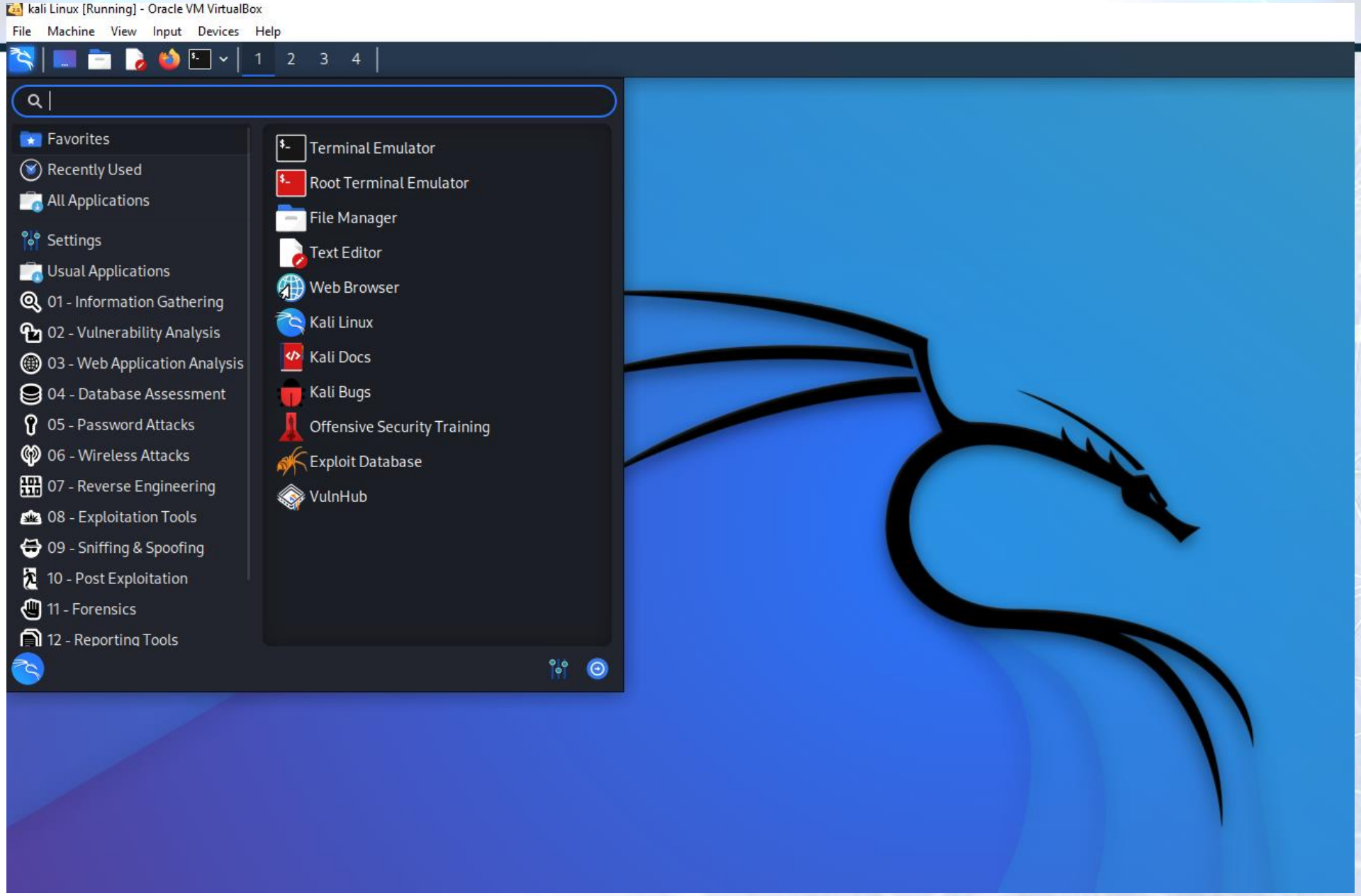
- **Nikto**

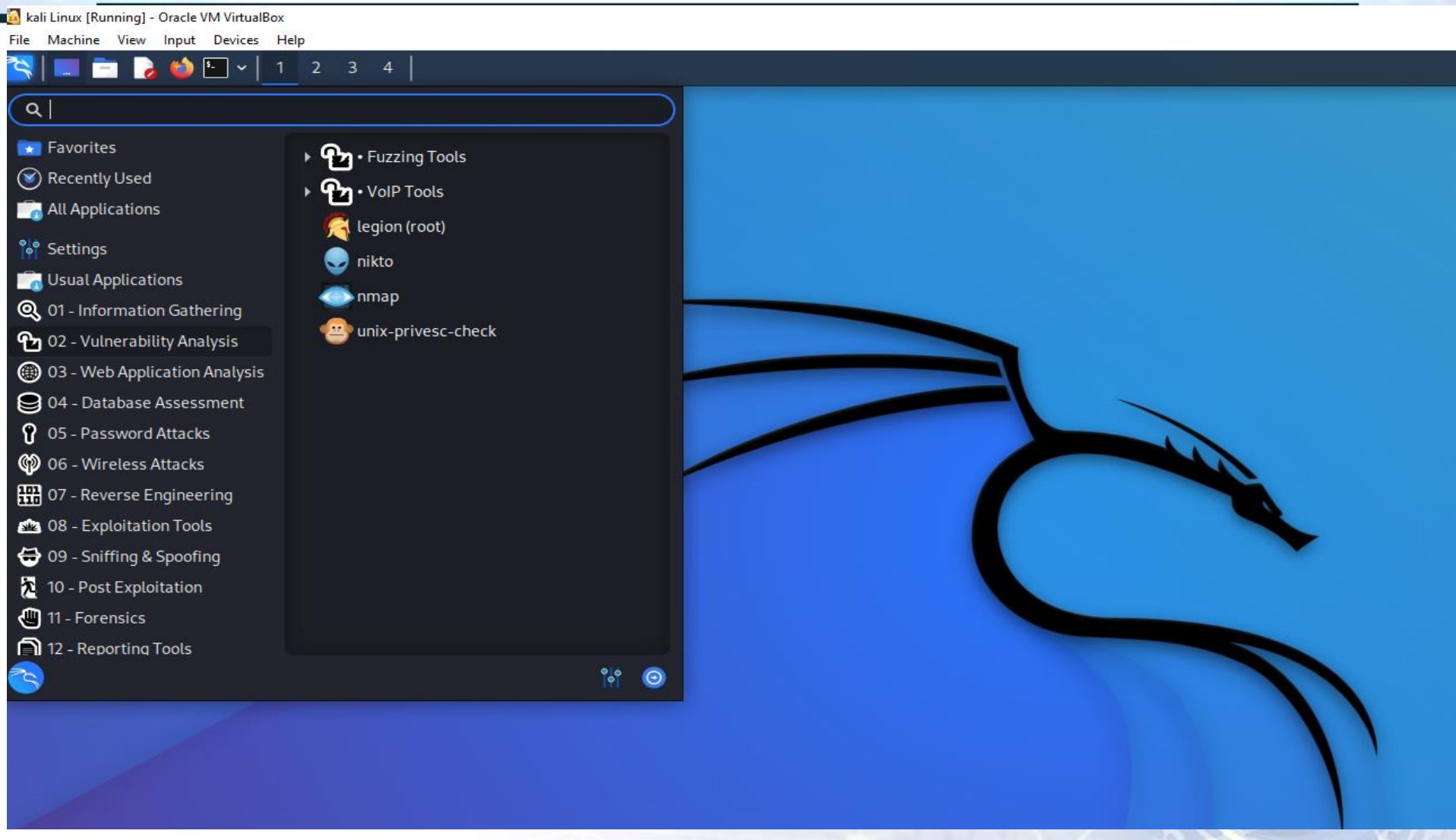
- Web server scaning is a black box test that identifies security vulnerabilties.

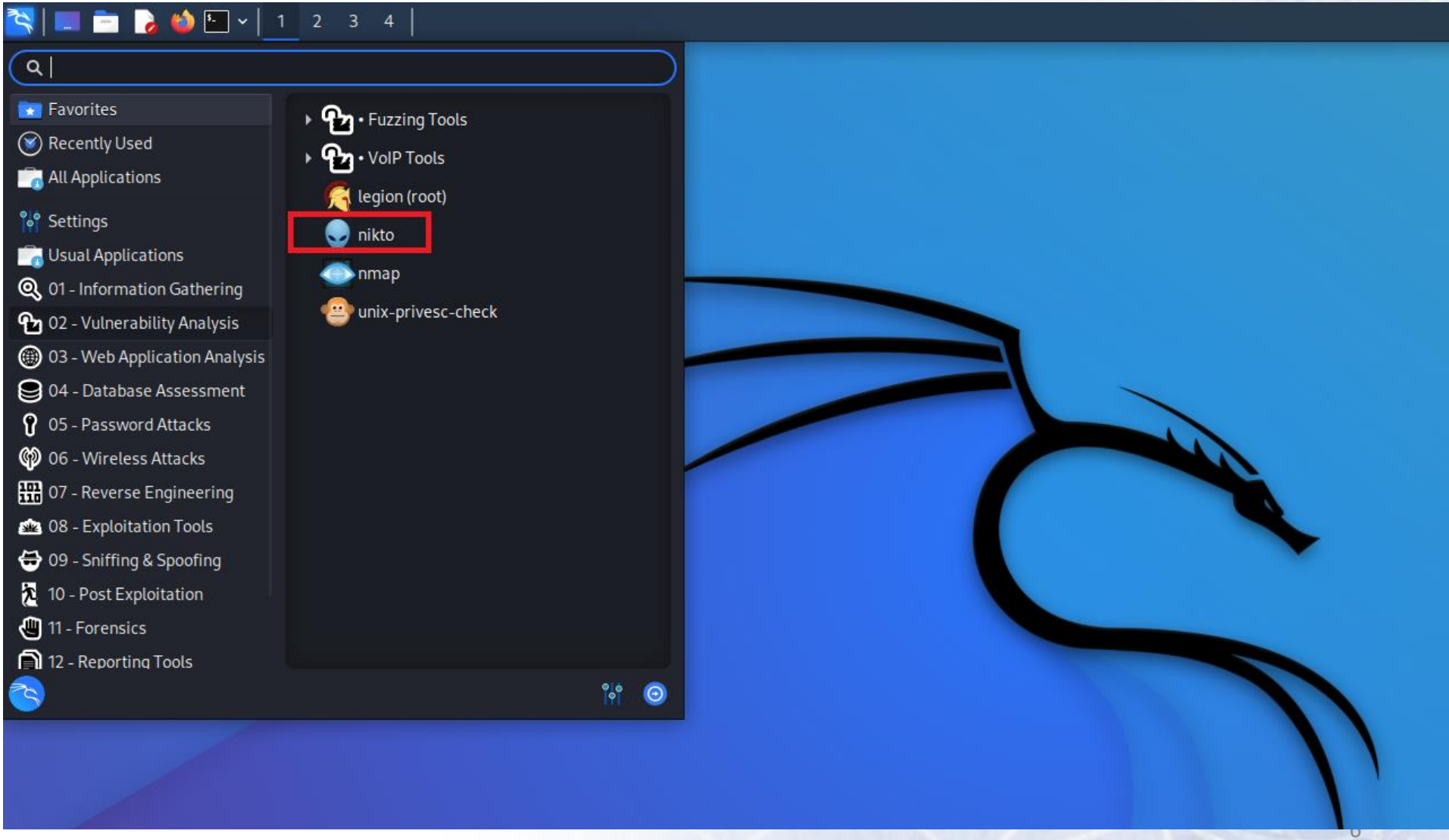
Built into Kali Linux and is an open-source web server scanner

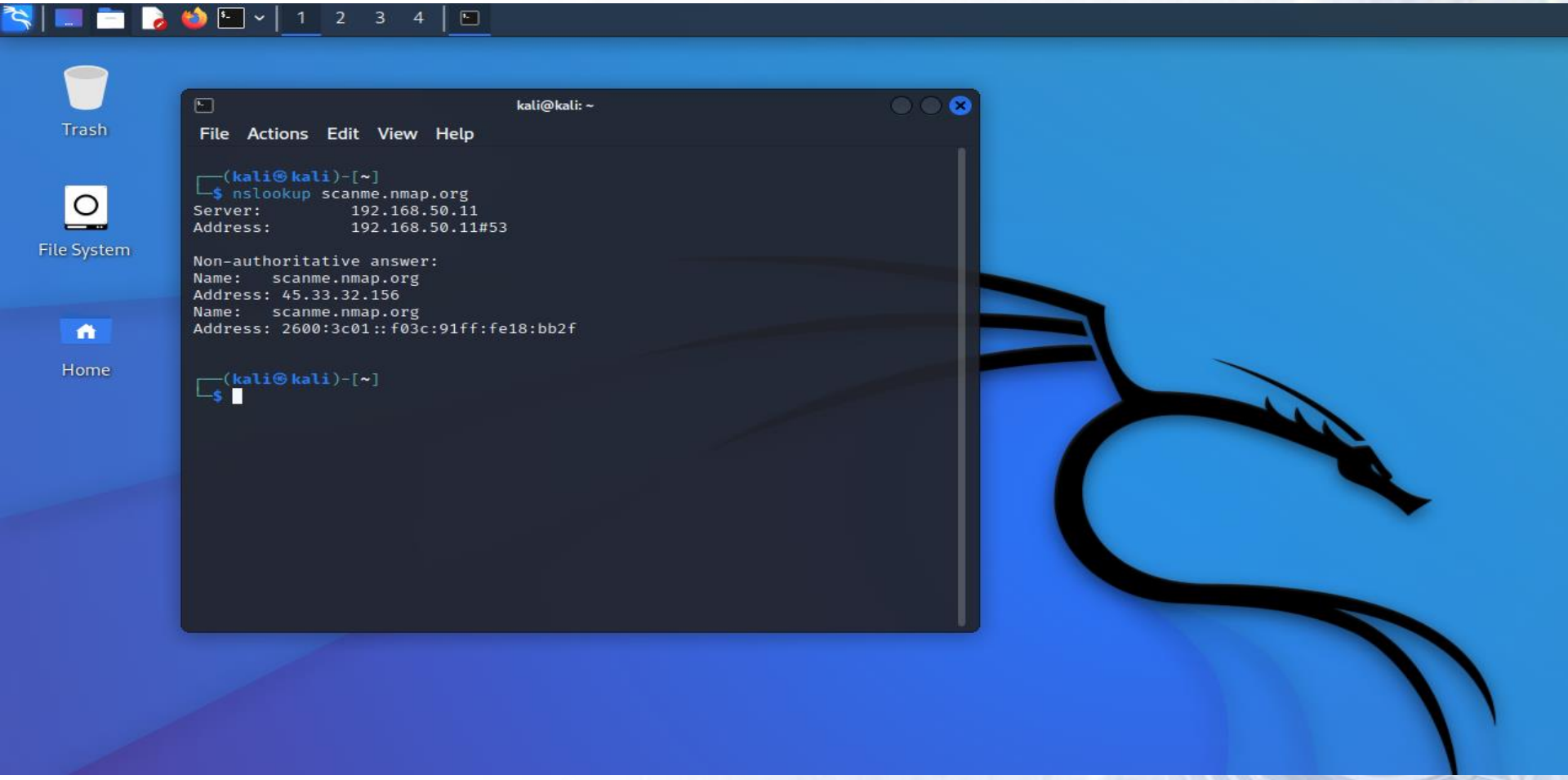
Performs complete testing on web servers for vulnerabilities

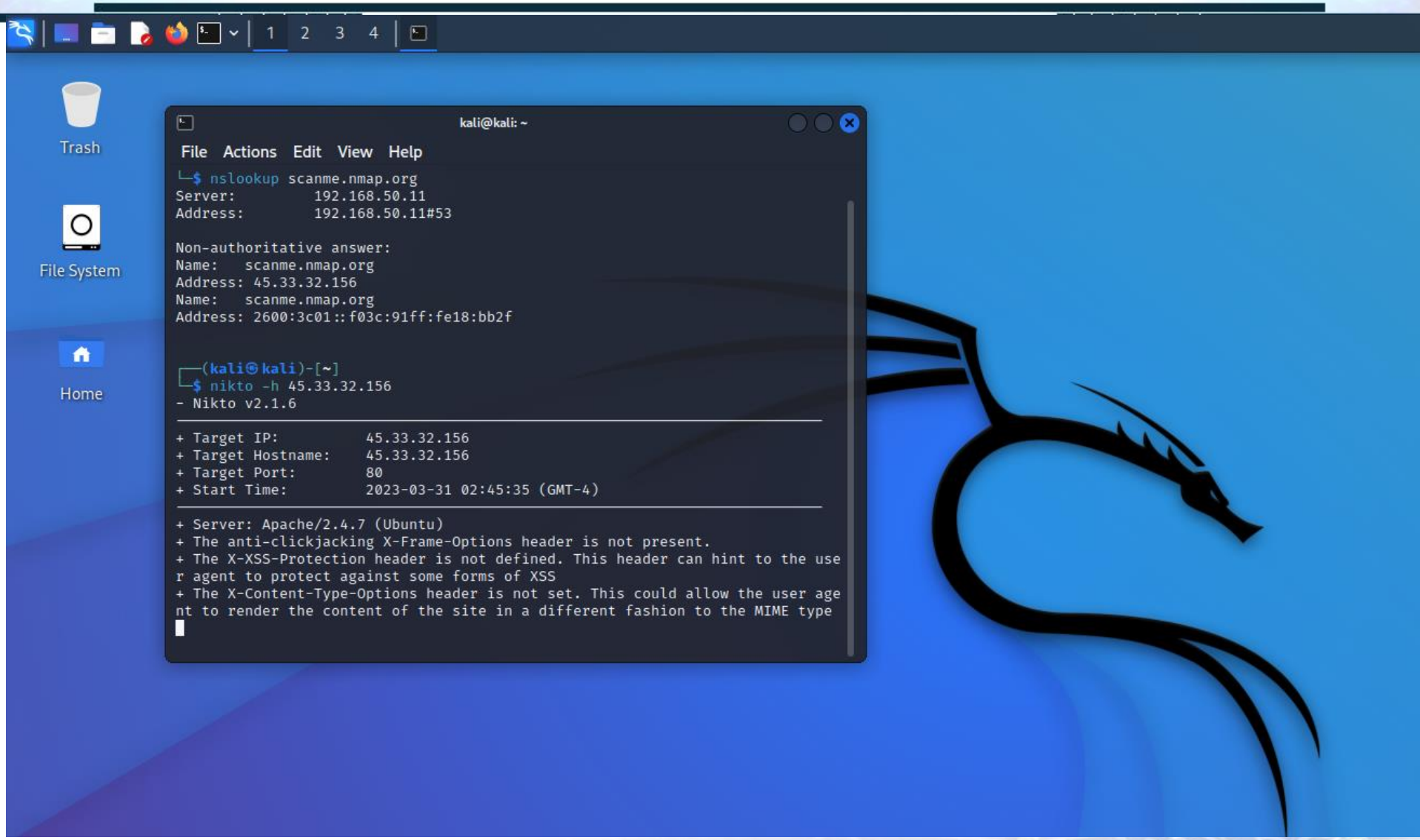
Scans for outdated versions of servers, server-specific problems, missing headers and dangerous files and CGIs


kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
Favorites
Recently Used
All Applications
Settings
Usual Applications
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
Terminal Emulator
Root Terminal Emulator
File Manager
Text Editor
Web Browser
Kali Linux
Kali Docs
Kali Bugs
Offensive Security Training
Exploit Database
VulnHub


kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
Favorites
Recently Used
All Applications
Settings
Usual Applications
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
• Fuzzing Tools
• VoIP Tools
legion (root)
nikto
nmap
unix-privesc-check


1
2
3
4
Favorites
Recently Used
All Applications
Settings
Usual Applications
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
• Fuzzing Tools
• VoIP Tools
legion (root)
nikto
nmap
unix-privesc-check


1 2 3 4
Trash
File System
Home
kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ nslookup scanme.nmap.org
Server: 192.168.50.11
Address: 192.168.50.11#53
Non-authoritative answer:
Name: scanme.nmap.org
Address: 45.33.32.156
Name: scanme.nmap.org
Address: 2600:3c01::f03c:91ff:fe18:bb2f
┌──(kali㉿kali)-[~]
└─$


1 2 3 4
Trash
File System
Home
kali@kali: ~
File Actions Edit View Help
└─$ nslookup scanme.nmap.org
Server: 192.168.50.11
Address: 192.168.50.11#53
Non-authoritative answer:
Name: scanme.nmap.org
Address: 45.33.32.156
Name: scanme.nmap.org
Address: 2600:3c01::f03c:91ff:fe18:bb2f
┌──(kali㉿kali)-[~]
└─$ nikto -h 45.33.32.156
- Nikto v2.1.6
+ Target IP: 45.33.32.156
+ Target Hostname: 45.33.32.156
+ Target Port: 80
+ Start Time: 2023-03-31 02:45:35 (GMT-4)
+ Server: Apache/2.4.7 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the use
r agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user age
nt to render the content of the site in a different fashion to the MIME type



Nmap(Network Mapper)

Nmap

Nmap, short for Network Mapper, is a free and open source utility network discovery and security auditing tool.

It is the world's leading port scanner,known for its simple and easy to remember flags that provide powerful scanning options.

- Guess the operating system running on a target machine
- Get accurate packet routes till the target machine
- Discovering connected hosts on a network
- Analyzing free ports on a target host
- Detecting running services on a system along with version number
- Uncovering network vulnerabilities and system loopholes

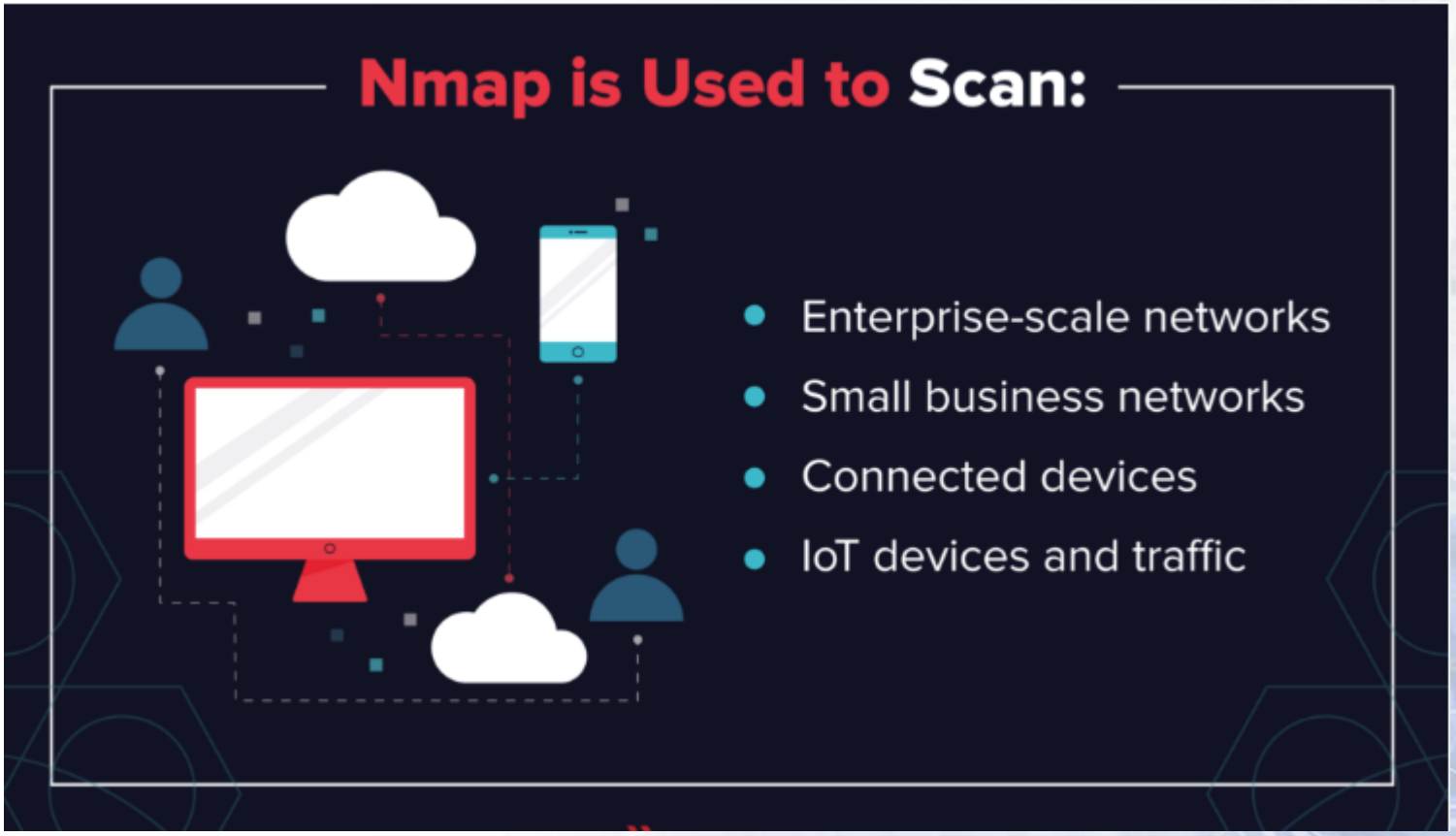
Nmap

Network administrators often use

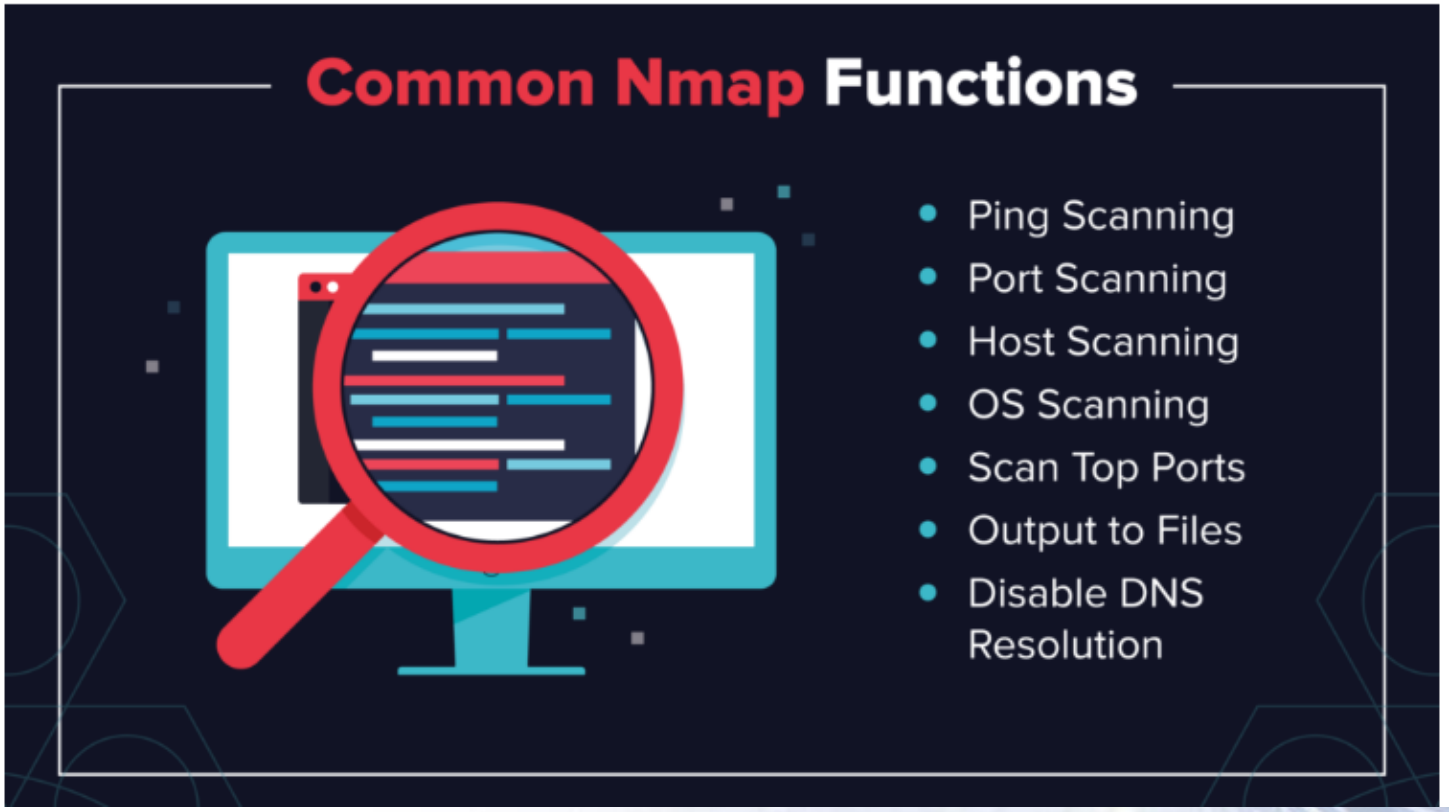
- to detect the devices that are presently working on the system
- the port number to which the devices are attached
- the free ports that may be used.
- what services (application name and version) those hosts are offering
- what operating systems (and OS versions) they are running

Nmap

- helpful while performing network penetration testing.
- not only gives network information but also assists in discovering security issues in the system.
- Nmap is platform-agnostic and may be run on various standard operating systems, including Linux, Windows, macOS.
- It is straightforward to use and includes both a command-line interface(CLI) and a graphical user interface(GUI).


Nmap is Used to Scan:
Enterprise-scale networks
Small business networks
Connected devices
IoT devices and traffic

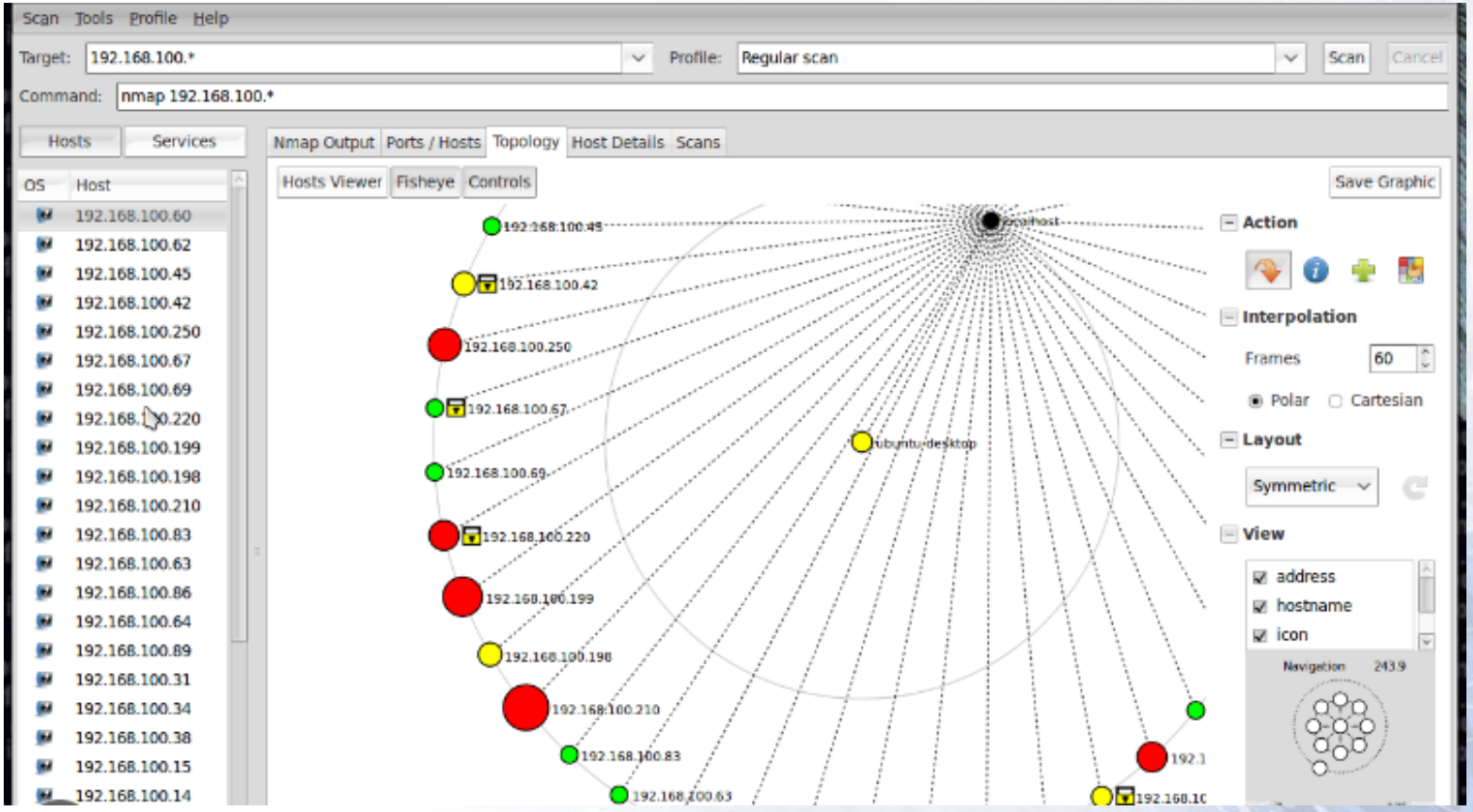
Nmap Commands



Zenmap

- Nmap has a graphical user interface called Zenmap. It helps you develop visual mappings of a network for better usability and reporting.

Zenmap GUI


Scan Tools Profile Help
Target: 192.168.100.*
Profile: Regular scan
Scan
Cancel
Command: nmap 192.168.100.*
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
192.168.100.60
192.168.100.62
192.168.100.45
192.168.100.42
192.168.100.250
192.168.100.67
192.168.100.69
192.168.100.220
192.168.100.199
192.168.100.198
192.168.100.210
192.168.100.83
192.168.100.63
192.168.100.86
192.168.100.64
192.168.100.89
192.168.100.31
192.168.100.34
192.168.100.38
192.168.100.15
192.168.100.14
Hosts Viewer
Fisheye
Controls
Save Graphic
192.168.100.45
192.168.100.42
192.168.100.250
192.168.100.67
192.168.100.69
192.168.100.220
192.168.100.199
192.168.100.198
192.168.100.210
192.168.100.83
192.168.100.63
ubuntu-desktop
Action
Interpolation
Frames
60
Polar
Cartesian
Layout
Symmetric
View
address
hostname
icon
Navigation

Nmap Commands

- various commands you can use in Nmap along with their flag and usage description with an example on how to use it.

Basic Nmap Scan against IP or host

nmap 1.1.1.1

- Now, if you want to scan a hostname, simply replace the IP for the host, as you see below:

nmap scanme.com

Nmap Commands with flags

Flag	Use	Example
-Pn	only port scan	nmap -Pn192.168.1.1
-sn	only host discover	nmap -sn192.168.1.1
-PR	arp discovery on a local network	nmap -PR192.168.1.1
-n	disable DNS resolution	nmap -n 192.168.1.1

Flag	Use	Example
-p	specify a port or port range	nmap -p 1-30 192.168.1.1
-p-	scan all ports	nmap -p- 192.168.1.1
-F	fast port scan	nmap -F 192.168.1.1

Flag	Use	Example
-sV	detect the version of services running	nmap -sV 192.168.1.1
-A	aggressive scan	nmap -A 192.168.1.1
-O	detect operating system of the target	nmap -O 192.168.1.1

Nmap **Benefits** and **Installation**

- Time tested security and networking tool
- Open source package with large community
- Available for most operating systems
- Free!

- **Download Link**

https://nmap.org/download



Npcap.com Seclists.org Sectools.org Insecure.org

Site Search

Download | Reference Guide | Book | Docs | Zenmap GUI | In the Movies

Downloading Nmap

Get the latest Nmap for your system:

- Windows
- macOS
- Linux (RPM)
- Any other OS (source code)

Older versions (and sometimes newer test releases) are available from the Nmap release archive (and really old ones are in dist-old). For the more security-paranoid (smart) users, GPG detached signatures and SHA-1 hashes for each release are available in the sigs directory (verification instructions). Before downloading, be sure to read the relevant sections for your platform from the Nmap Install Guide. The most important changes (features, bugfixes, etc) in each Nmap version are described in the Changelog. Using Nmap is covered in the Reference Guide, and don't forget to read the other available documentation, particularly the official book Nmap Network Scanning!

Nmap users are encouraged to subscribe to the *Nmap-hackers* mailing list. It is a low volume (7 posts in 2015), moderated list for the most important announcements about Nmap, Insecure.org, and related projects. You can join the 128,953 current subscribers (as of September 2017) by submitting your email address here:

Subscribe to Nmap-hackers

(or subscribe with custom options from the Nmap-hackers list info page)

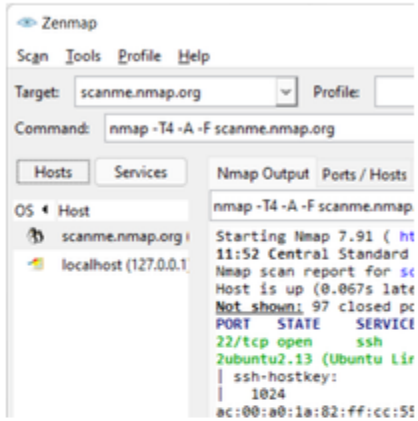
...so get updates by liking Nmap on Facebook or following us @nmap on Twitter.

html#windows

ap.org/download.html#windows

am Jang Newspaper Jo... Join Pak Army - Pak... Peer Zulfiqar Ahma... Jab Ek Sail Ne MUH... Networks Imported From IE Virtual Info

Microsoft Windows binaries



Please read the Windows section of the Install Guide for limitations and installation instructions for the Windows version of Nmap. It's provided as an executable self-installer which includes Nmap's dependencies and the Zenmap GUI. We support Nmap on Windows 7 and newer, as well as Windows Server 2008 R2 and newer. We also maintain a guide for users who must run Nmap on earlier Windows releases..

Note: The version of Npcap included in our installers may not always be the latest version. If you experience problems or just want the latest and greatest version, download and install the latest Npcap release.

Latest stable release self-installer: nmap-7.93-setup.exe
Latest Npcap release self-installer: npcap-1.73.exe

We have written post-install usage instructions. Please notify us if you encounter any problems or have suggestions for the installer.

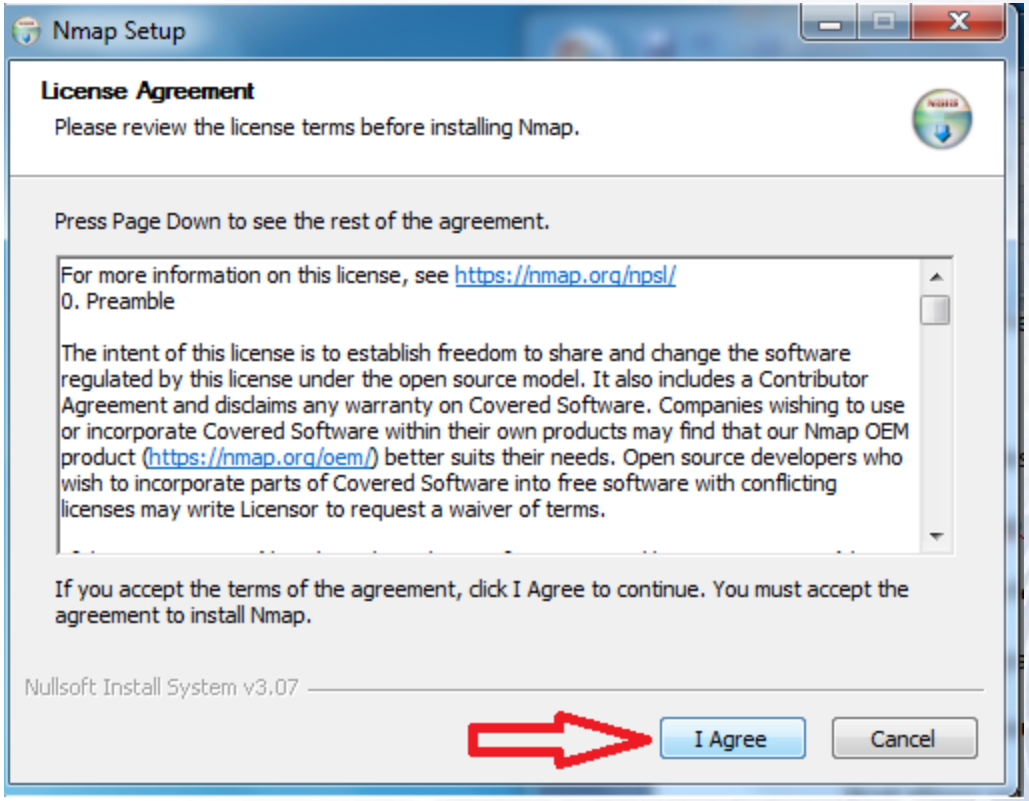
Linux RPM Source and Binaries

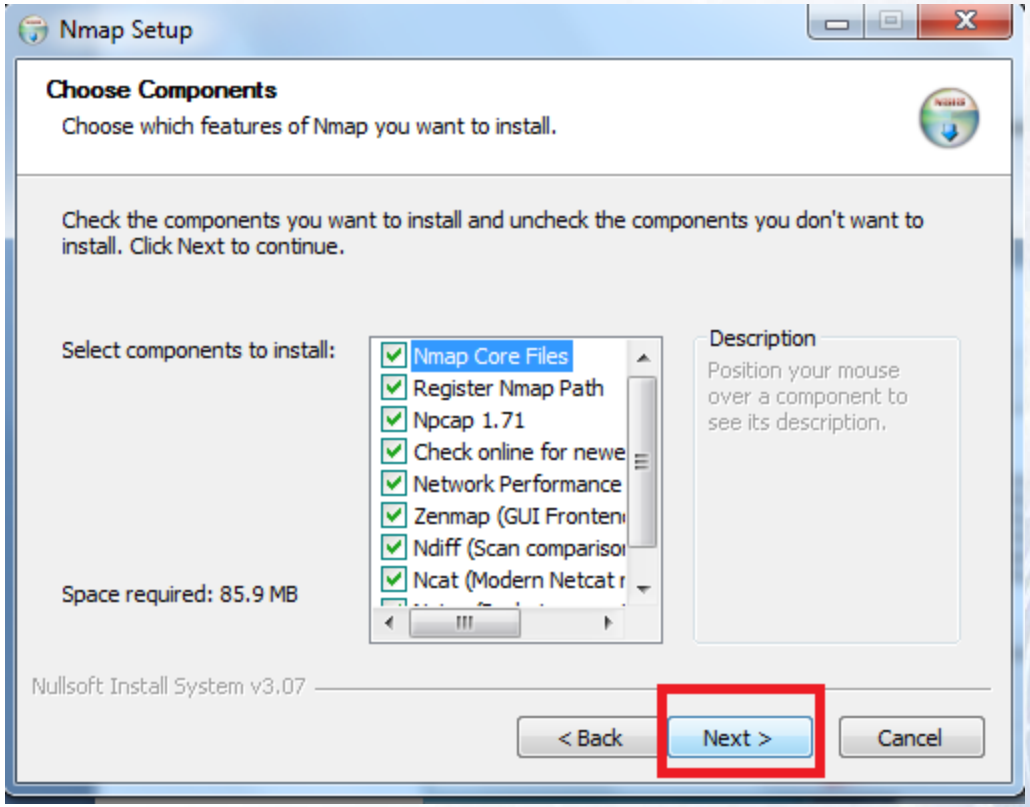
Many popular Linux distributions (Redhat, Mandrake, Suse, etc) use the RPM package management system for quick and easy binary package installation. We have written a detailed guide to installing our RPM packages, though these simple commands usually do the trick:

```
rpm -vhU https://nmap.org/dist/nmap-7.93-1.x86_64.rpm
rpm -vhU https://nmap.org/dist/zenmap-7.93-1.noarch.rpm
rpm -vhU https://nmap.org/dist/ncat-7.93-1.x86_64.rpm
rpm -vhU https://nmap.org/dist/nping-0.7.93-1.x86_64.rpm
```

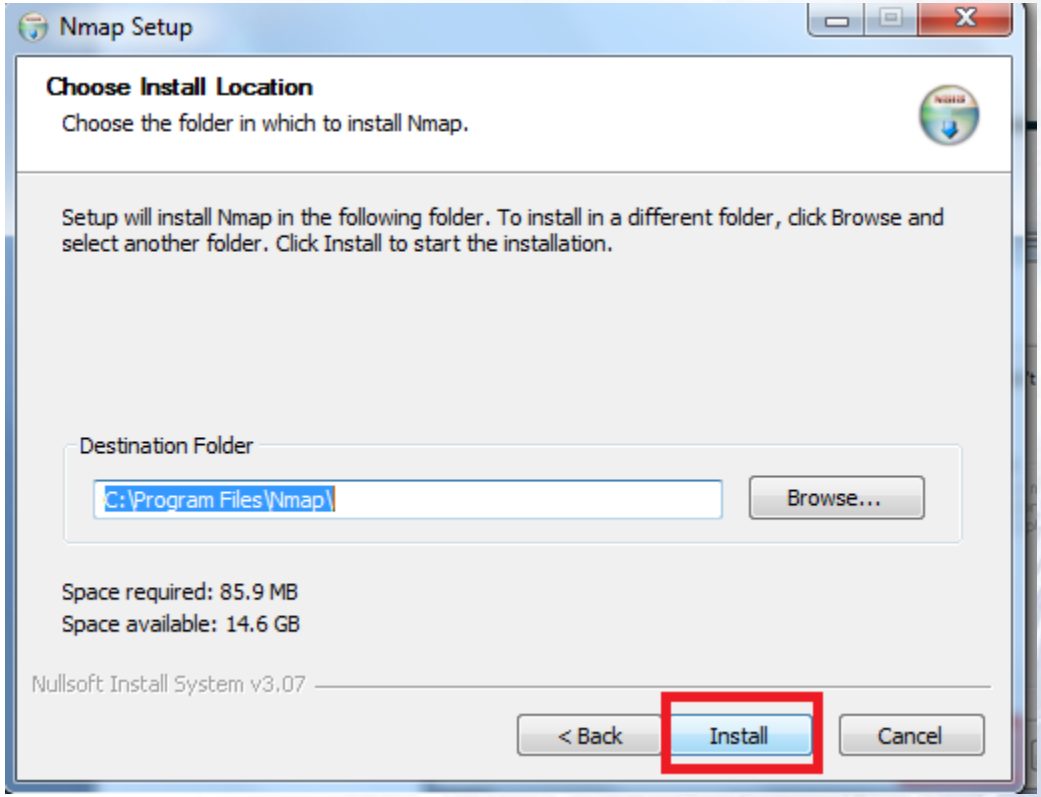
You can also download and install the RPMs yourself:

Latest stable release:
x86-64 (64-bit Linux) Nmap RPM: nmap-7.93-1.x86_64.rpm
x86-64 (64-bit Linux) Ncat RPM: ncat-7.93-1.x86_64.rpm
x86-64 (64-bit Linux) Nping RPM: nping-0.7.93-1.x86_64.rpm
Optional Zenmap GUI (all platforms): zenmap-7.93-1.noarch.rpm
Source RPM (includes Nmap, Zenmap, Ncat, and Nping): nmap-7.93-1.src.rpm

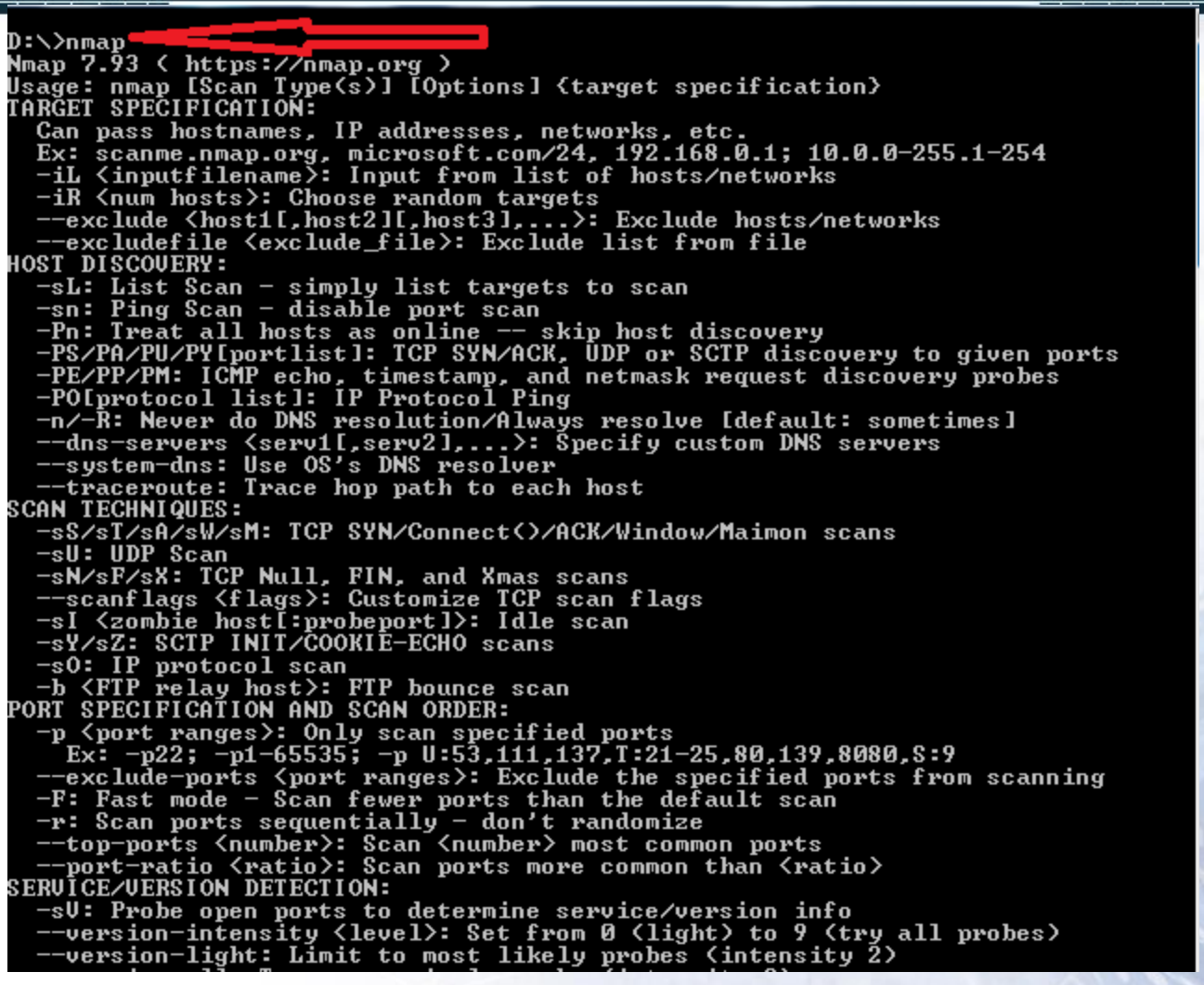

Nmap Setup
License Agreement
Please review the license terms before installing Nmap.
Press Page Down to see the rest of the agreement.
For more information on this license, see https://nmap.org/npsl/
0. Preamble
The intent of this license is to establish freedom to share and change the software regulated by this license under the open source model. It also includes a Contributor Agreement and disclaims any warranty on Covered Software. Companies wishing to use or incorporate Covered Software within their own products may find that our Nmap OEM product (https://nmap.org/oem/) better suits their needs. Open source developers who wish to incorporate parts of Covered Software into free software with conflicting licenses may write Licensor to request a waiver of terms.
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Nmap.
Nullsoft Install System v3.07
I Agree
Cancel


Nmap Setup
Choose Components
Choose which features of Nmap you want to install.
Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.
Select components to install:
Nmap Core Files
Register Nmap Path
Npcap 1.71
Check online for newe
Network Performance
Zenmap (GUI Fronten
Ndiff (Scan comparisor
Ncat (Modern Netcat r
Description
Position your mouse over a component to see its description.
Space required: 85.9 MB
Nullsoft Install System v3.07
< Back
Next >
Cancel

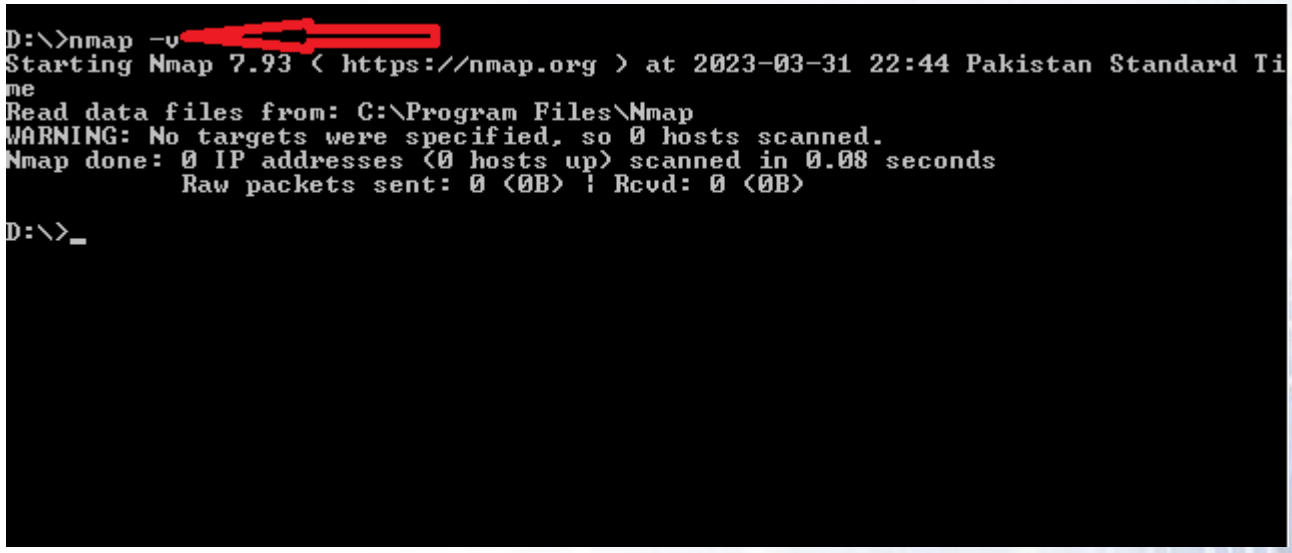
- **Nmap core files includes the Nmap scanning engine**
- **Register Nmap path allows you to execute Nmap from the command line in any directory**
- **Network performance improvements optimization your system for running scans.**
- **Zenmap is a graphical front end for Nmap**
- **Ndiff allows you to compare the results of two Nmap scans.**
- **Ncat allows you to read and write data to network connections from the command line**
- **Nping is a packet generation utility that provides enhancements over the basic ping command.**

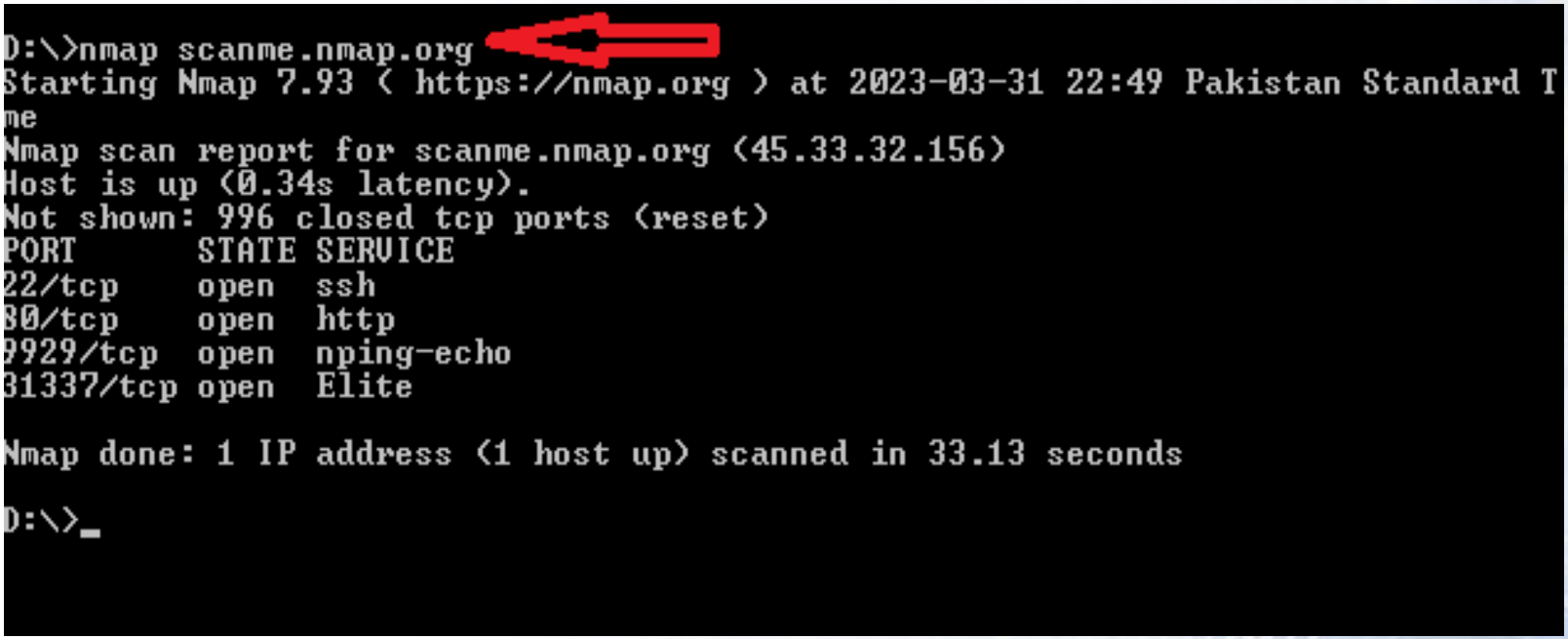

Nmap Setup
Choose Install Location
Choose the folder in which to install Nmap.
Setup will install Nmap in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.
Destination Folder
C:\Program Files\Nmap\
Browse...
Space required: 85.9 MB
Space available: 14.6 GB
Nullsoft Install System v3.07
< Back
Install
Cancel


Nmap -
Zenmap GUI


D:\>nmap
Nmap 7.93 (https://nmap.org)
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
Can pass hostnames, IP addresses, networks, etc.
Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
-iL <inputfilename>: Input from list of hosts/networks
-iR <num hosts>: Choose random targets
--exclude <host1[,host2][,host3],...>: Exclude hosts/networks
--excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
-sL: List Scan - simply list targets to scan
-sn: Ping Scan - disable port scan
-Pn: Treat all hosts as online -- skip host discovery
-PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
-PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
-PO[protocol list]: IP Protocol Ping
-n/-R: Never do DNS resolution/Always resolve [default: sometimes]
--dns-servers <serv1[,serv2],...>: Specify custom DNS servers
--system-dns: Use OS's DNS resolver
--traceroute: Trace hop path to each host
SCAN TECHNIQUES:
-sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
-sU: UDP Scan
-sN/sF/sX: TCP Null, FIN, and Xmas scans
--scanflags <flags>: Customize TCP scan flags
-sI <zombie host[:probeport]>: Idle scan
-sY/sZ: SCTP INIT/COOKIE-ECHO scans
-sO: IP protocol scan
-b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
-p <port ranges>: Only scan specified ports
Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
--exclude-ports <port ranges>: Exclude the specified ports from scanning
-F: Fast mode - Scan fewer ports than the default scan
-r: Scan ports sequentially - don't randomize
--top-ports <number>: Scan <number> most common ports
--port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
-sV: Probe open ports to determine service/version info
--version-intensity <level>: Set from 0 (light) to 9 (try all probes)
--version-light: Limit to most likely probes (intensity 2)

Nmap syntax is the same regardless of the operating system.




D:\>nmap scanme.nmap.org
Starting Nmap 7.93 (https://nmap.org) at 2023-03-31 22:49 Pakistan Standard T
me
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.34s latency).
Not shown: 996 closed tcp ports (reset)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
9929/tcp open nping-echo
31337/tcp open Elite
Nmap done: 1 IP address (1 host up) scanned in 33.13 seconds
D:\>

Use the Snap container manager to install Nmap on Ubuntu and Debian systems.

```
ubuntu@ip-172-31-93-59:~$ sudo snap install nmap
nmap 7.91 from Maximiliano Bertacchini (maxiberta) installed
ubuntu@ip-172-31-93-59:~$
```

```
ubuntu@ip-172-31-93-59:~$ sudo snap install nmap
nmap 7.91 from Maximiliano Bertacchini (maxiberta) installed
ubuntu@ip-172-31-93-59:~$ nmap -V
Nmap version 7.91 ( https://nmap.org )
Platform: x86_64-unknown-linux-gnu
Compiled with: liblua-5.3.3 openssl-1.1.1 libssh2-1.8.0 libz-1.2.11 libpcre-8.39 libpcap-1.8.1 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
ubuntu@ip-172-31-93-59:~$
```

Port Stats &
Running Simple Namp command

Port Stats in Nmap

State	Description
`open`	Accepting connection requests
`closed`	No service responding to requests
`filtered`	Blocked by a firewall
`unfiltered`	Accessible, but scanner was unable to determine whether open or closed

Special cases of port states

- Nmap might be unable to make a definitive statement about the state of the port
- If the Namp is unsure of the state, it may reports two options.

- Open | filtered means that the port is either open or filtered
- Closed | filtered means that the port is either closed or filtered

Scan with DNS

```
[ec2-user@ip-172-31-83-84 ~]$ nmap scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-14 20:30 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.072s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

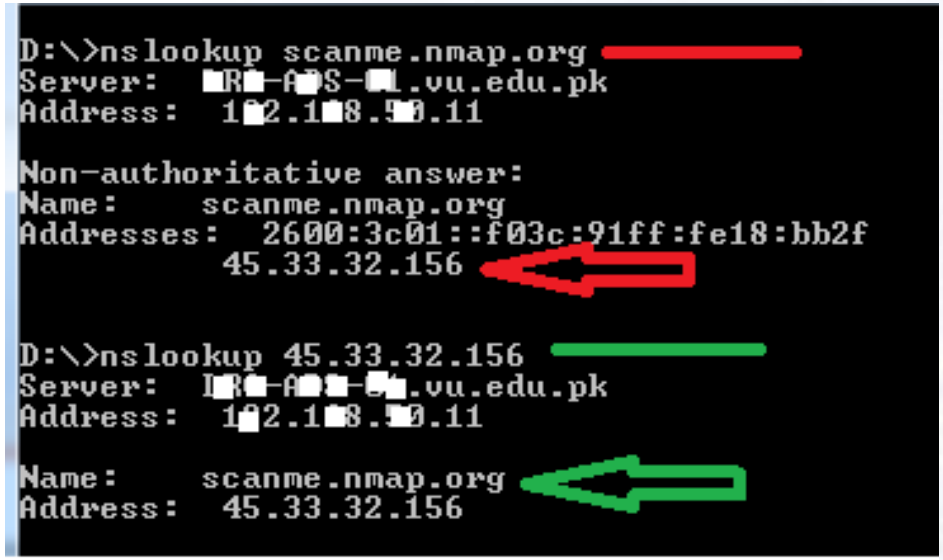
Nmap done: 1 IP address (1 host up) scanned in 1.18 seconds
[ec2-user@ip-172-31-83-84 ~]$
```

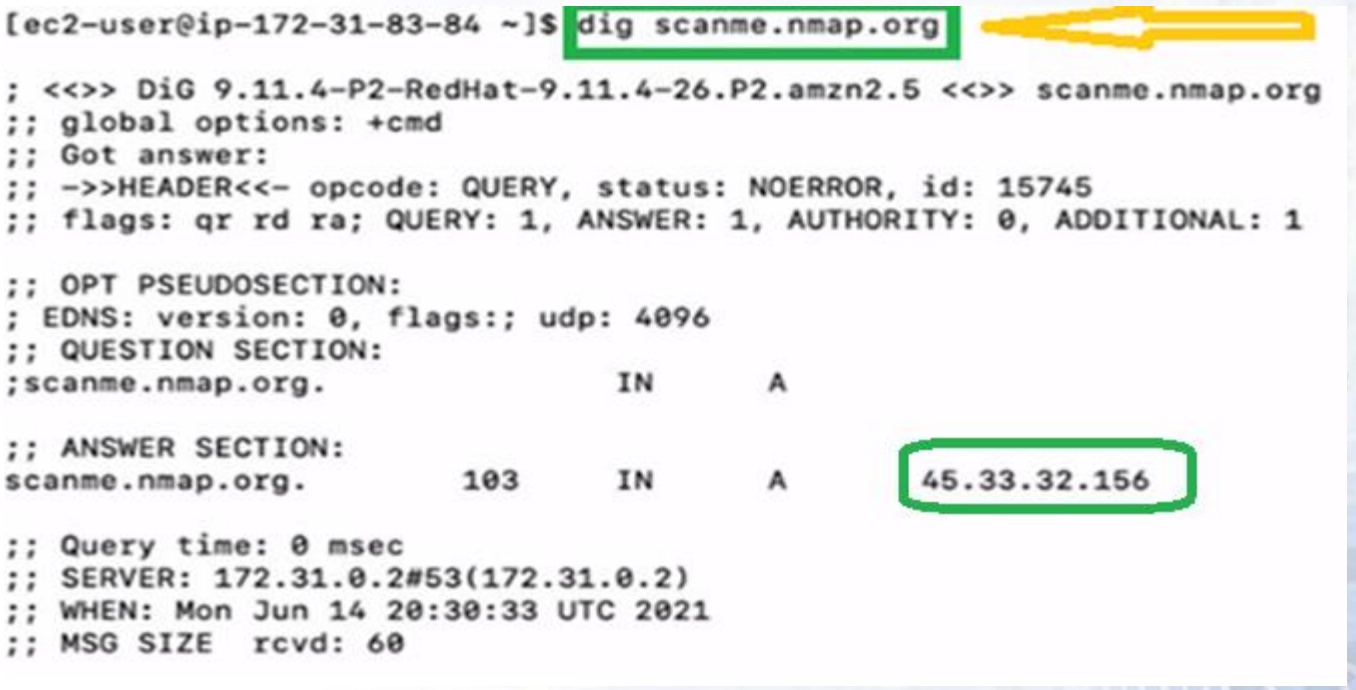
```
[ec2-user@ip-172-31-83-84 ~]$ nmap scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-14 20:30 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.072s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 1.18 seconds
```

- (Microsoft Windows uses nslookup, while Mac OS X and Linux use dig.)

- Both perform DNS queries, and to test out your DNS configuration.
- determine the IP address associated with a domain name

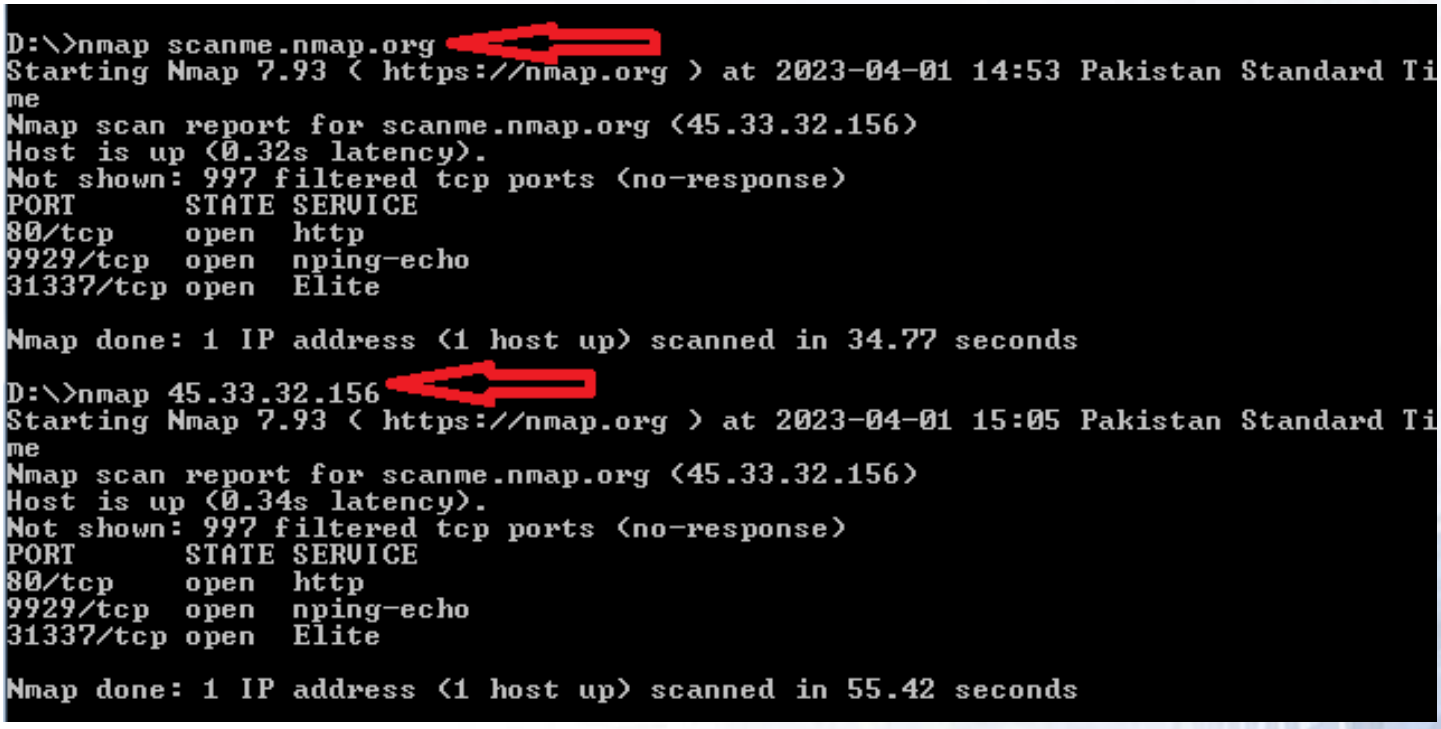

D:\>nslookup scanme.nmap.org
Server:
Address:
Non-authoritative answer:
Name: scanme.nmap.org
Addresses: 2600:3c01::f03c:91ff:fe18:bb2f
45.33.32.156
D:\>nslookup 45.33.32.156
Server:
Address:
Name: scanme.nmap.org
Address: 45.33.32.156


[ec2-user@ip-172-31-83-84 ~]$ dig scanme.nmap.org
; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.amzn2.5 <<>> scanme.nmap.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15745
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;scanme.nmap.org. IN A
;; ANSWER SECTION:
scanme.nmap.org. 103 IN A 45.33.32.156
;; Query time: 0 msec
;; SERVER: 172.31.0.2#53(172.31.0.2)
;; WHEN: Mon Jun 14 20:30:33 UTC 2021
;; MSG SIZE rcvd: 60

Scan with server IP

```
[ec2-user@ip-172-31-83-84 ~]$ nmap 45.33.32.156
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-14 20:31 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.071s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 1.19 seconds
[ec2-user@ip-172-31-83-84 ~]$
```


D:\>nmap scanme.nmap.org
Starting Nmap 7.93 (https://nmap.org) at 2023-04-01 14:53 Pakistan Standard Ti
me
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.32s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT STATE SERVICE
80/tcp open http
9929/tcp open nping-echo
31337/tcp open Elite
Nmap done: 1 IP address (1 host up) scanned in 34.77 seconds
D:\>nmap 45.33.32.156
Starting Nmap 7.93 (https://nmap.org) at 2023-04-01 15:05 Pakistan Standard Ti
me
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.34s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT STATE SERVICE
80/tcp open http
9929/tcp open nping-echo
31337/tcp open Elite
Nmap done: 1 IP address (1 host up) scanned in 55.42 seconds

OS and service Version Detection

- Nmap is able to probe deeper than simply open reports
- Guesses the target OS

Activate operating system detection with the **-O** flag.

```
Mikes-Mac-mini:~ root# nmap -O scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 15:23 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.080s latency).
Not shown: 992 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open     nping-echo
31337/tcp open     Elite
Aggressive OS guesses: Linux 2.6.32 (93%), Linux 2.6.32 or 3.10 (93%), Linux 4.4 (92%), Linux 2.6.32 - 2.6.35 (91%), Linux 2.6.32 - 2.6.39 (91%), Linux 4.0 (90
%), Linux 5.4 (90%), Linux 3.11 - 4.1 (89%), Linux 3.2 - 3.8 (89%), Linux 2.6.18 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 16 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.54 seconds
```

```
Mikes-Mac-mini:~ root# nmap -O 192.168.1.54
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 15:27 EDT
Nmap scan report for 192.168.1.54
Host is up (0.012s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
28201/tcp open  unknown
MAC Address: F0:18:98:5A:B1:A0 (Apple)
Device type: general purpose|media device
Running: Apple OS X 10.11.X, Apple iOS 12.X
OS CPE: cpe:/o:apple:mac_os_x:10.11 cpe:/o:apple:iphone_os:12
OS details: Apple Mac OS X 10.11 (El Capitan) or iOS 12.4 - 13.0 (Darwin 15.6.0 - 19.0.0)
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.98 seconds
```

- **Service version detection**

- Guesses the service versions running on an open port of target system

Activate service version detection with the **-sV** flag.

```
Mikes-Mac-mini:~ root# nmap -sV scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 15:30 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.089s latency).
Not shown: 992 closed ports
PORT      STATE    SERVICE      VERSION
22/tcp    open     ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
25/tcp    filtered smtp
80/tcp    open     http         Apache httpd 2.4.7 ((Ubuntu))
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open     nping-echo   Nping echo
31337/tcp open     tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.80 seconds
```

```
Mikes-Mac-mini:~ root# nmap -sV scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 15:30 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.089s latency).
Not shown: 992 closed ports
PORT      STATE    SERVICE      VERSION
22/tcp    open     ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
25/tcp    filtered smtp
80/tcp    open     http         Apache httpd 2.4.7 ((Ubuntu))
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open     nping-echo   Nping echo
31337/tcp open     tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.80 seconds
```

Port selection
Controls scan behavior

- By default, Nmap scans the 1000 most commonly used TCP ports
- Many of those probably are not used on our network
- Scanning each unused port takes some time
- There are 65535 TCP ports on a system

- If a service is running on any of those ports other than the 1000 most commonly used ports then default Nmap scan will miss it
- There are some options that allow us to customize Nmap scan

The -F flag requests a fast scan of the top 100 TCP ports.

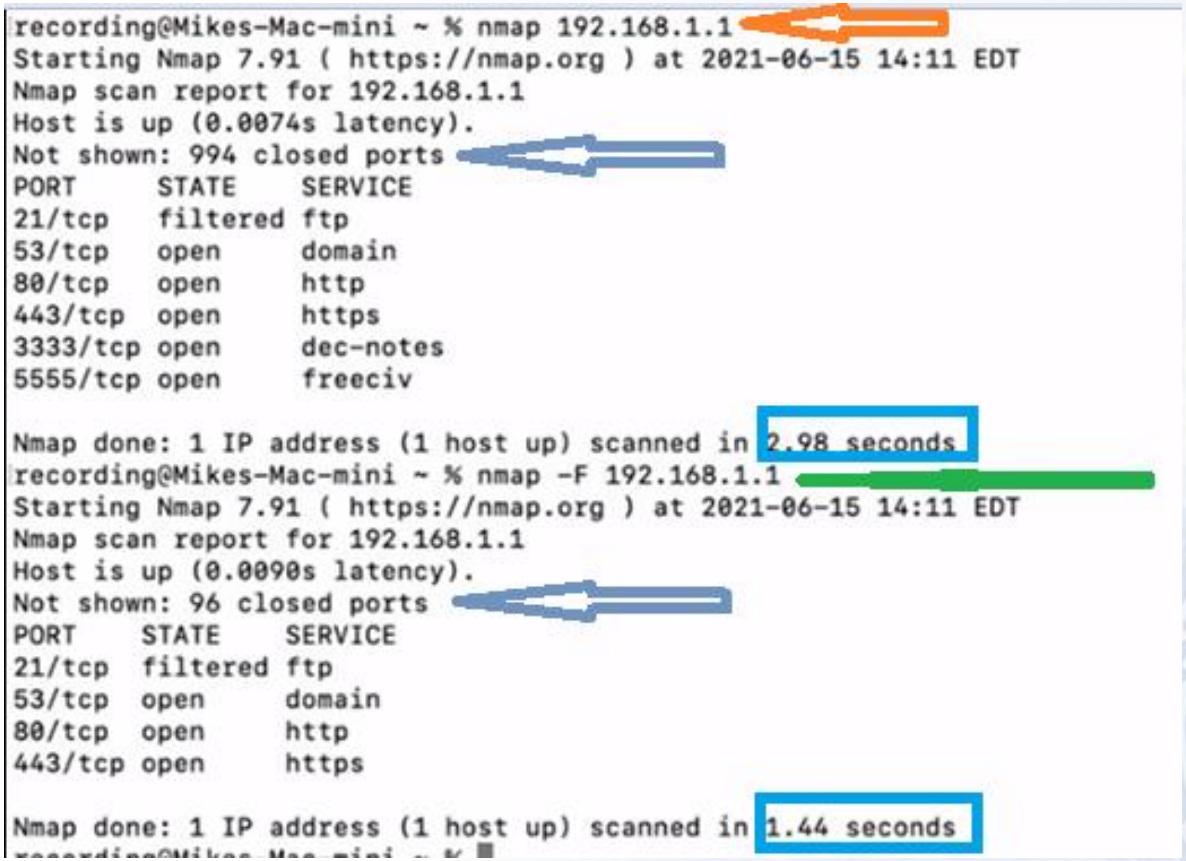
```
recording@Mikes-Mac-mini ~ % nmap 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 14:11 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0074s latency).
Not shown: 994 closed ports
PORT     STATE    SERVICE
21/tcp   filtered ftp
53/tcp   open     domain
80/tcp   open     http
443/tcp  open     https
3333/tcp open     dec-notes
5555/tcp open     freeciv

Nmap done: 1 IP address (1 host up) scanned in 2.98 seconds
```

```
recording@Mikes-Mac-mini ~ % nmap 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 14:11 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0074s latency).
Not shown: 994 closed ports
PORT     STATE    SERVICE
21/tcp   filtered ftp
53/tcp   open     domain
80/tcp   open     http
443/tcp  open     https
3333/tcp open     dec-notes
5555/tcp open     freeciv

Nmap done: 1 IP address (1 host up) scanned in 2.98 seconds
recording@Mikes-Mac-mini ~ % nmap -F 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 14:11 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0090s latency).
Not shown: 96 closed ports
PORT    STATE    SERVICE
21/tcp  filtered ftp
53/tcp  open     domain
80/tcp  open     http
443/tcp open     https

Nmap done: 1 IP address (1 host up) scanned in 1.44 seconds
```

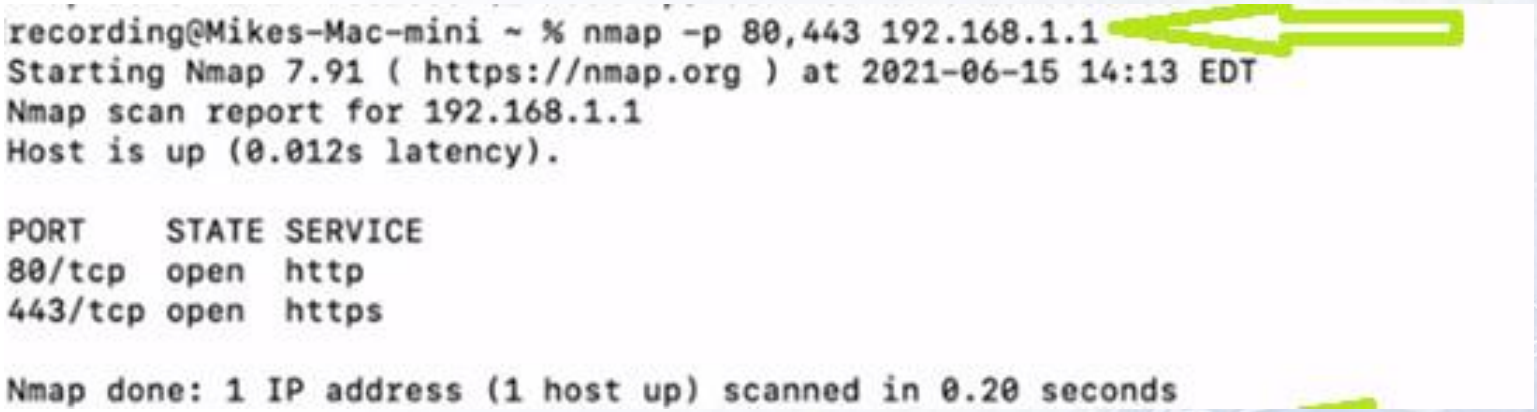

recording@Mikes-Mac-mini ~ % nmap 192.168.1.1
Starting Nmap 7.91 (https://nmap.org) at 2021-06-15 14:11 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0074s latency).
Not shown: 994 closed ports
PORT STATE SERVICE
21/tcp filtered ftp
53/tcp open domain
80/tcp open http
443/tcp open https
3333/tcp open dec-notes
5555/tcp open freeciv
Nmap done: 1 IP address (1 host up) scanned in 2.98 seconds
recording@Mikes-Mac-mini ~ % nmap -F 192.168.1.1
Starting Nmap 7.91 (https://nmap.org) at 2021-06-15 14:11 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0090s latency).
Not shown: 96 closed ports
PORT STATE SERVICE
21/tcp filtered ftp
53/tcp open domain
80/tcp open http
443/tcp open https
Nmap done: 1 IP address (1 host up) scanned in 1.44 seconds

The **-p** flag allows us to specify the ports we'd like to scan.

```
recording@Mikes-Mac-mini ~ % nmap -p 80 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 14:12 EDT
Nmap scan report for 192.168.1.1
Host is up (0.015s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
```


recording@Mikes-Mac-mini ~ % nmap -p 80,443 192.168.1.1
Starting Nmap 7.91 (https://nmap.org) at 2021-06-15 14:13 EDT
Nmap scan report for 192.168.1.1
Host is up (0.012s latency).
PORT STATE SERVICE
80/tcp open http
443/tcp open https
Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds

Scan Service

```
recording@Mikes-Mac-mini ~ % nmap -p http,https 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 14:14 EDT
Nmap scan report for 192.168.1.1
Host is up (0.013s latency).

PORT     STATE  SERVICE
80/tcp   open   http
443/tcp  open   https
8008/tcp closed http

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

```
recording@Mikes-Mac-mini ~ % nmap -p 80 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 14:12 EDT
Nmap scan report for 192.168.1.1
Host is up (0.015s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
recording@Mikes-Mac-mini ~ % nmap -p 80,443 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 14:13 EDT
Nmap scan report for 192.168.1.1
Host is up (0.012s latency).

PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
recording@Mikes-Mac-mini ~ % nmap -p http,https 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 14:14 EDT
Nmap scan report for 192.168.1.1
Host is up (0.013s latency).

PORT     STATE  SERVICE
80/tcp   open   http
443/tcp  open   https
8008/tcp closed http

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

The `-p-` flag requests a full TCP scan of the target system(s).


recording@Mikes-Mac-mini ~ % nmap -p- 192.168.1.1
Starting Nmap 7.91 (https://nmap.org) at 2021-06-15 14:15 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0078s latency).
Not shown: 65528 closed ports
PORT STATE SERVICE
21/tcp filtered ftp
53/tcp open domain
80/tcp open http
443/tcp open https
3333/tcp open dec-notes
5555/tcp open freeciv
7272/tcp open watchme-7272
Nmap done: 1 IP address (1 host up) scanned in 121.38 seconds

Specifying Scan Targets

- Single IP address or DNS name
- List of addresses and names, separated by spaces
- Range of IP addresses
- Subnet mask
- File containing addresses and names
- Scan IPv6

```
recording@Mikes-Mac-mini ~ % nmap 192.168.1.1 192.168.1.3 192.168.1.6
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 13:38 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0081s latency).
Not shown: 994 closed ports
PORT     STATE    SERVICE
21/tcp   filtered ftp
53/tcp   open     domain
80/tcp   open     http
443/tcp  open     https
3333/tcp open     dec-notes
5555/tcp open     freeciv

Nmap scan report for 192.168.1.3
Host is up (0.012s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
23/tcp   open  telnet
80/tcp   open  http
111/tcp  open  rpcbind
8080/tcp open  http-proxy

Nmap scan report for 192.168.1.6
Host is up (0.0090s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 3 IP addresses (3 hosts up) scanned in 7.16 seconds
recording@Mikes-Mac-mini ~ %
```

```
recording@Mikes-Mac-mini ~ % nmap 192.168.1.1,3,6
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 13:39 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0087s latency).
Not shown: 994 closed ports
PORT     STATE    SERVICE
21/tcp   filtered ftp
53/tcp   open     domain
80/tcp   open     http
443/tcp  open     https
3333/tcp open     dec-notes
5555/tcp open     freeciv

Nmap scan report for 192.168.1.3
Host is up (0.0087s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
23/tcp   open  telnet
80/tcp   open  http
111/tcp  open  rpcbind
8080/tcp open  http-proxy

Nmap scan report for 192.168.1.6
Host is up (0.014s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 3 IP addresses (3 hosts up) scanned in 7.75 seconds
```

```
recording@Mikes-Mac-mini ~ % nmap 192.168.1.1-6
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 13:40 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0083s latency).
Not shown: 994 closed ports
PORT     STATE    SERVICE
21/tcp   filtered ftp
53/tcp   open     domain
80/tcp   open     http
443/tcp  open     https
3333/tcp open     dec-notes
5555/tcp open     freeciv

Nmap scan report for 192.168.1.3
Host is up (0.011s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
23/tcp   open  telnet
80/tcp   open  http
111/tcp  open  rpcbind
8080/tcp open  http-proxy

Nmap scan report for 192.168.1.4
Host is up (0.011s latency).
All 1000 scanned ports on 192.168.1.4 are closed

Nmap scan report for 192.168.1.5
Host is up (0.013s latency).
All 1000 scanned ports on 192.168.1.5 are closed

Nmap scan report for 192.168.1.6
Host is up (0.019s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 6 IP addresses (5 hosts up) scanned in 16.02 seconds
```

Scan subnet

```
recording@Mikes-Mac-mini ~ % nmap 192.168.1.0/29
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 13:41 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0080s latency).
Not shown: 994 closed ports
PORT     STATE    SERVICE
21/tcp   filtered ftp
53/tcp   open     domain
80/tcp   open     http
443/tcp  open     https
3333/tcp open     dec-notes
5555/tcp open     freeciv

Nmap scan report for 192.168.1.3
Host is up (0.010s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
23/tcp   open  telnet
80/tcp   open  http
111/tcp  open  rpcbind
8080/tcp open  http-proxy

Nmap scan report for 192.168.1.4
Host is up (0.014s latency).
All 1000 scanned ports on 192.168.1.4 are closed

Nmap scan report for 192.168.1.5
Host is up (0.014s latency).
All 1000 scanned ports on 192.168.1.5 are closed

Nmap scan report for 192.168.1.6
Host is up (0.015s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for 192.168.1.7
Host is up (0.014s latency).
All 1000 scanned ports on 192.168.1.7 are closed

Nmap done: 8 IP addresses (6 hosts up) scanned in 14.75 seconds
```

Scan from file

```
recording@Mikes-Mac-mini ~ % cat scan_targets.txt
192.168.1.1
192.168.1.3
192.168.1.6
192.168.1.8
192.168.1.38
192.168.1.40
192.168.1.42
recording@Mikes-Mac-mini ~ % nmap -iL scan_targets.txt
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 13:42 EDT
```

```
Host is up (0.012s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for 192.168.1.8
Host is up (0.0098s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
5555/tcp open  freeciv
8009/tcp open  ajp13

Nmap scan report for 192.168.1.38
Host is up (0.011s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
23/tcp   open  telnet
80/tcp   open  http
443/tcp  open  https
515/tcp  open  printer
631/tcp  open  ipp
9100/tcp open  jetdirect

Nmap scan report for 192.168.1.40
Host is up (0.013s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
62078/tcp open  iphone-sync

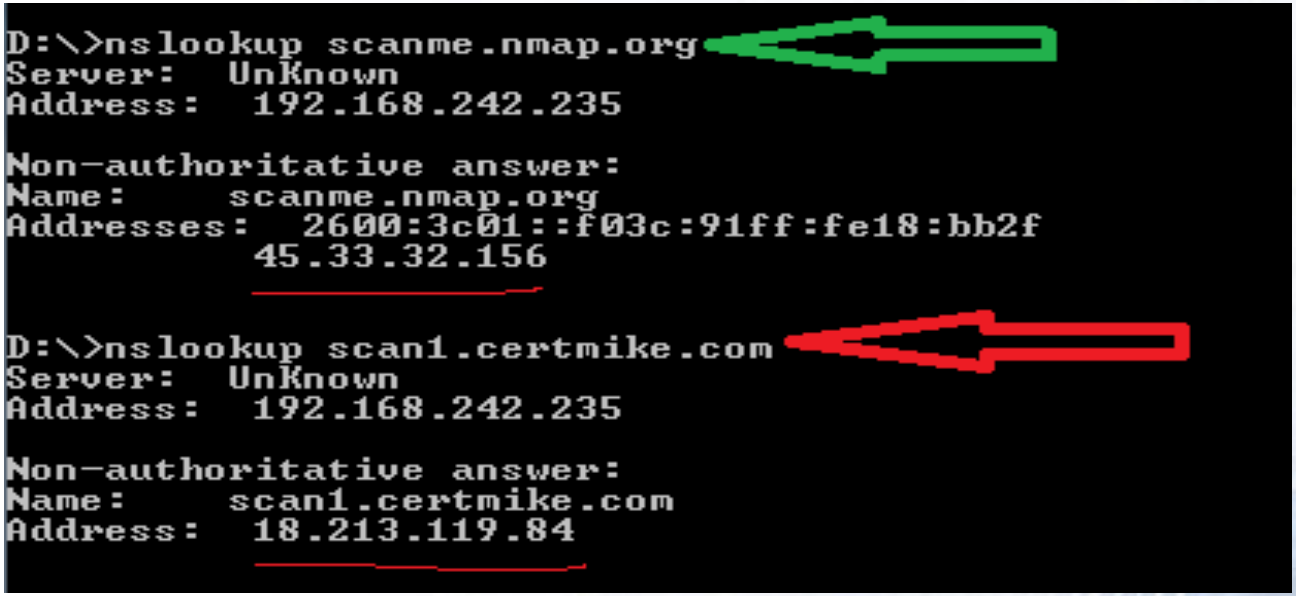
Nmap scan report for 192.168.1.42
Host is up (0.010s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
5000/tcp  open  upnp
7000/tcp  open  afs3-fileserver
7100/tcp  open  font-service
49152/tcp open  unknown
49153/tcp open  unknown
62078/tcp open  iphone-sync

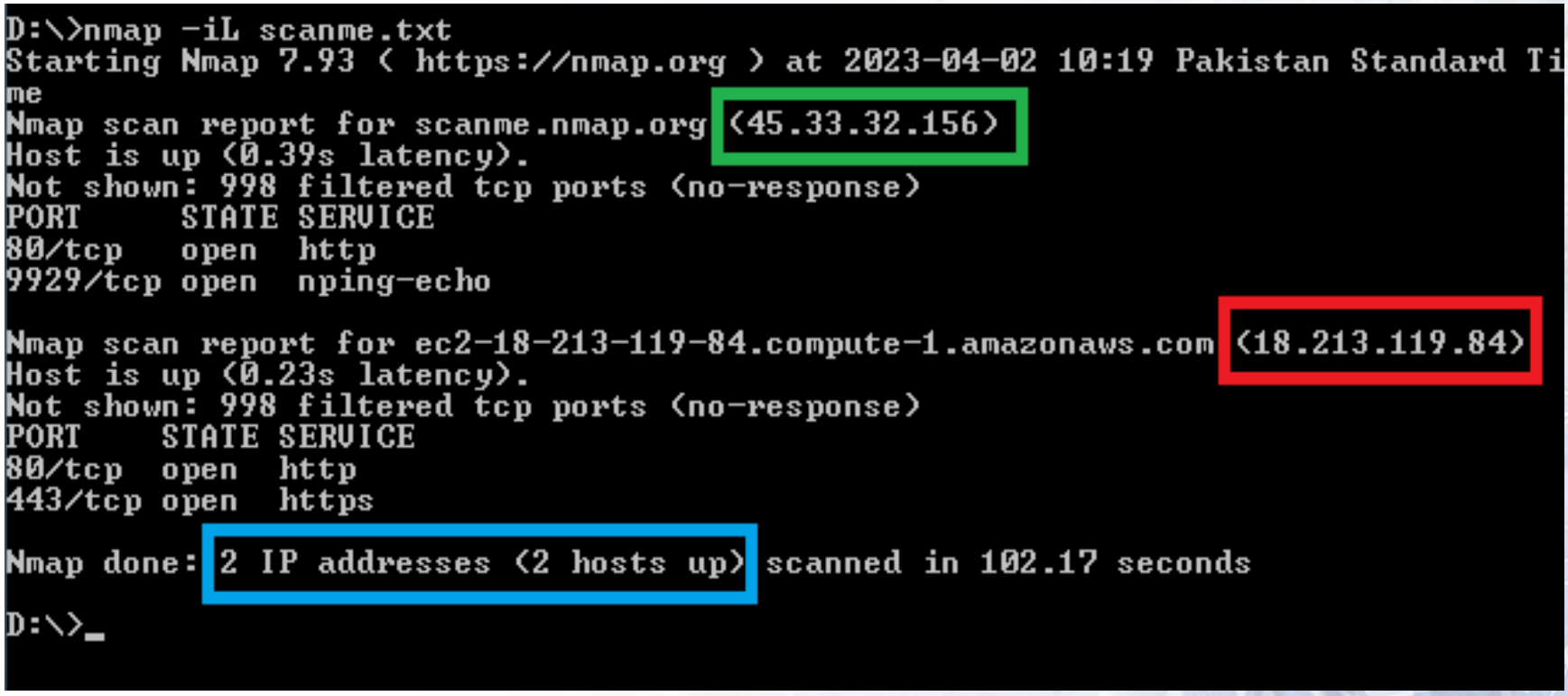
Nmap done: 7 IP addresses (7 hosts up) scanned in 27.92 seconds
```

Scan from file on windows



Nslookup


D:\>nslookup scanme.nmap.org
Server: UnKnown
Address: 192.168.242.235
Non-authoritative answer:
Name: scanme.nmap.org
Addresses: 2600:3c01::f03c:91ff:fe18:bb2f
45.33.32.156
D:\>nslookup scan1.certmike.com
Server: UnKnown
Address: 192.168.242.235
Non-authoritative answer:
Name: scan1.certmike.com
Address: 18.213.119.84


D:\>nmap -iL scanme.txt
Starting Nmap 7.93 (https://nmap.org) at 2023-04-02 10:19 Pakistan Standard Ti
me
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.39s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT STATE SERVICE
80/tcp open http
9929/tcp open nping-echo
Nmap scan report for ec2-18-213-119-84.compute-1.amazonaws.com (18.213.119.84)
Host is up (0.23s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT STATE SERVICE
80/tcp open http
443/tcp open https
Nmap done: 2 IP addresses (2 hosts up) scanned in 102.17 seconds
D:\>

Scanning IPv6

Nmap is able to scan IPv6 addresses with the **-6** flag.

```
recording@Mikes-Mac-mini ~ % nmap 2600:1f18:2763:3000:6b7a:868d:b048:78af
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 13:44 EDT
2600:1f18:2763:3000:6b7a:868d:b048:78af looks like an IPv6 target specification -- you have to use the -6 option.
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.08 seconds
recording@Mikes-Mac-mini ~ %
```

```
recording@Mikes-Mac-mini ~ % nmap 2600:1f18:2763:3000:6b7a:868d:b048:78af
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 13:44 EDT
2600:1f18:2763:3000:6b7a:868d:b048:78af looks like an IPv6 target specification -- you have to use the -6 option.
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.08 seconds
recording@Mikes-Mac-mini ~ % nmap -6 2600:1f18:2763:3000:6b7a:868d:b048:78af
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 13:45 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.16 seconds
recording@Mikes-Mac-mini ~ %
```

Scan Shortcut and Disable DNS option

scanning shortcut

- The **–A** flag offers a scanning shortcut that activate several popular options

-A Options

- Remote operating system detection
- Service and version detection
- Traceroute
- Nmap Scripting engine (NSE)

```
Mikes-Mac-mini:~ root# nmap -A -T4 scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 15:33 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.079s latency).
Not shown: 992 closed ports
PORT      STATE    SERVICE      VERSION
22/tcp    open     ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
25/tcp    filtered smtp
80/tcp    open     http         Apache httpd 2.4.7 ((Ubuntu))
|_http-favicon: Nmap Project
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open     nping-echo   Nping echo
31337/tcp open     tcpwrapped
Aggressive OS guesses: Linux 2.6.32 (93%), Linux 2.6.32 or 3.10 (93%), Linux 4.4 (93%), Linux 2.6.32 - 2.6.35 (91
%), Linux 2.6.32 - 3.0 (90%), Linux 3.11 - 4.1 (89%), Linux 3.2 - 3.8 (89%), Linux 5.0 - 5.4 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 16 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 5900/tcp)
HOP RTT      ADDRESS
1   8.82 ms  192.168.1.1
2   12.34 ms 10.0.0.1
3   30.27 ms 96.120.26.197
4   30.27 ms 96.110.154.133
5   21.36 ms 68.87.231.137
6   30.29 ms be-167-ar01.area4.il.chicago.comcast.net (162.151.144.101)
7   31.34 ms 24.153.89.45
8   31.33 ms be-32241-cs04.350ecermak.il.ibone.comcast.net (96.110.40.61)
```

```
Mikes-Mac-mini:~ root# nmap -A -T4 scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 15:33 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.079s latency).
Not shown: 992 closed ports
PORT      STATE    SERVICE      VERSION
22/tcp    open     ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
25/tcp    filtered smtp
80/tcp    open     http         Apache httpd 2.4.7 ((Ubuntu))
|_http-favicon: Nmap Project
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open     nping-echo   Nping echo
31337/tcp open     tcpwrapped
Aggressive OS guesses: Linux 2.6.32 (93%), Linux 2.6.32 or 3.10 (93%), Linux 4.4 (93%), Linux 2.6.32 - 2.6.35 (91%), Linux 4.0
%), Linux 2.6.32 - 3.0 (90%), Linux 3.11 - 4.1 (89%), Linux 3.2 - 3.8 (89%), Linux 5.0 - 5.4 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 16 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 5900/tcp)
HOP RTT      ADDRESS
1   8.82 ms  192.168.1.1
2   12.34 ms 10.0.0.1
3   30.27 ms 96.120.26.197
```

```
Mikes-Mac-mini:~ root# nmap -A -T4 scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 15:33 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.079s latency).
Not shown: 992 closed ports
PORT      STATE    SERVICE      VERSION
22/tcp    open     ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
25/tcp    filtered smtp
80/tcp    open     http         Apache httpd 2.4.7 ((Ubuntu))
|_http-favicon: Nmap Project
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open     nping-echo   Nping echo
31337/tcp open     tcpwrapped
Aggressive OS guesses: Linux 2.6.32 (93%), Linux 2.6.32 or 3.10 (93%), Linux 4.4 (93%), Linux 2.6.32 - 2.6.35 (91%), Lin
%), Linux 2.6.32 - 3.0 (90%), Linux 3.11 - 4.1 (89%), Linux 3.2 - 3.8 (89%), Linux 5.0 - 5.4 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 16 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 5900/tcp)
HOP RTT      ADDRESS
1   8.82 ms  192.168.1.1
2   12.34 ms 10.0.0.1
```

Namp Scrpting engine that retrieves the SSH key as presented by the host

```
Mikes-Mac-mini:~ root# nmap -A -T4 scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 15:33 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.079s latency).
Not shown: 992 closed ports
PORT      STATE    SERVICE      VERSION
22/tcp    open     ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
25/tcp    filtered smtp
80/tcp    open     http         Apache httpd 2.4.7 ((Ubuntu))
|_http-favicon: Nmap Project
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open     nping-echo   Nping echo
31337/tcp open     tcpwrapped
Aggressive OS guesses: Linux 2.6.32 (93%), Linux 2.6.32 or 3.10 (93%), Linux 4.4 (93%), Linux 2.6.3
%), Linux 2.6.32 - 3.0 (90%), Linux 3.11 - 4.1 (89%), Linux 3.2 - 3.8 (89%), Linux 5.0 - 5.4 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 16 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 5900/tcp)
HOP RTT      ADDRESS
1   8.82 ms  192.168.1.1
2   12.34 ms 10.0.0.1
3   30.27 ms 96.120.26.197
```

```
25/tcp    filtered smtp
80/tcp    open     http         Apache httpd 2.4.7 ((Ubuntu))
|_http-favicon: Nmap Project
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open     nping-echo   Nping echo
31337/tcp open     tcpwrapped
Aggressive OS guesses: Linux 2.6.32 (93%), Linux 2.6.32 or 3.10 (93%), Linux 4.4 (93%), Linux 2.6.32 - 3
%), Linux 2.6.32 - 3.0 (90%), Linux 3.11 - 4.1 (89%), Linux 3.2 - 3.8 (89%), Linux 5.0 - 5.4 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 16 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 5900/tcp)
HOP RTT      ADDRESS
1   8.82 ms  192.168.1.1
2   12.34 ms 10.0.0.1
3   30.27 ms 96.120.26.197
4   30.27 ms 96.110.154.133
5   21.36 ms 68.87.231.137
6   30.29 ms be-167-ar01.area4.il.chicago.comcast.net (162.151.144.101)
7   31.34 ms 24.153.89.45
8   31.33 ms be-32241-cs04.350ecermak.il.ibone.comcast.net (96.110.40.61)
9   33.63 ms be-2211-pe11.350ecermak.il.ibone.comcast.net (96.110.33.198)
10  27.18 ms ae-3.r08.chcgil09.us.bb.gin.ntt.net (129.250.8.65)
11  31.36 ms ae-4.r23.chcgil09.us.bb.gin.ntt.net (129.250.2.205)
12  96.78 ms ae-1.r24.snjsca04.us.bb.gin.ntt.net (129.250.5.17)
13  96.79 ms ae-40.r02.snjsca04.us.bb.gin.ntt.net (129.250.3.121)
14  96.79 ms ce-0-18-0-1.r02.snjsca04.us.ce.gin.ntt.net (192.80.17.170)
15  96.79 ms if-1-4.csw6-fnc1.linode.com (173.230.159.83)
16  96.81 ms scanme.nmap.org (45.33.32.156)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.98 seconds
Mikes-Mac-mini:~ root#
```

- **DNS Resolution**

DNS resolution

- Adds information, but consumes time
- By default, Nmap perform DNS resolution to identify the names of any systems that are scanned by the IP addresses

The **-n** flag disables reverse DNS resolution.

```
recording@Mikes-Mac-mini ~ % nmap 45.33.32.156
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 13:56 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.077s latency).
Not shown: 992 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 17.09 seconds
```

```
recording@Mikes-Mac-mini ~ % nmap 45.33.32.156
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 13:56 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.077s latency).
Not shown: 992 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open     nping-echo
31337/tcp open     Elite

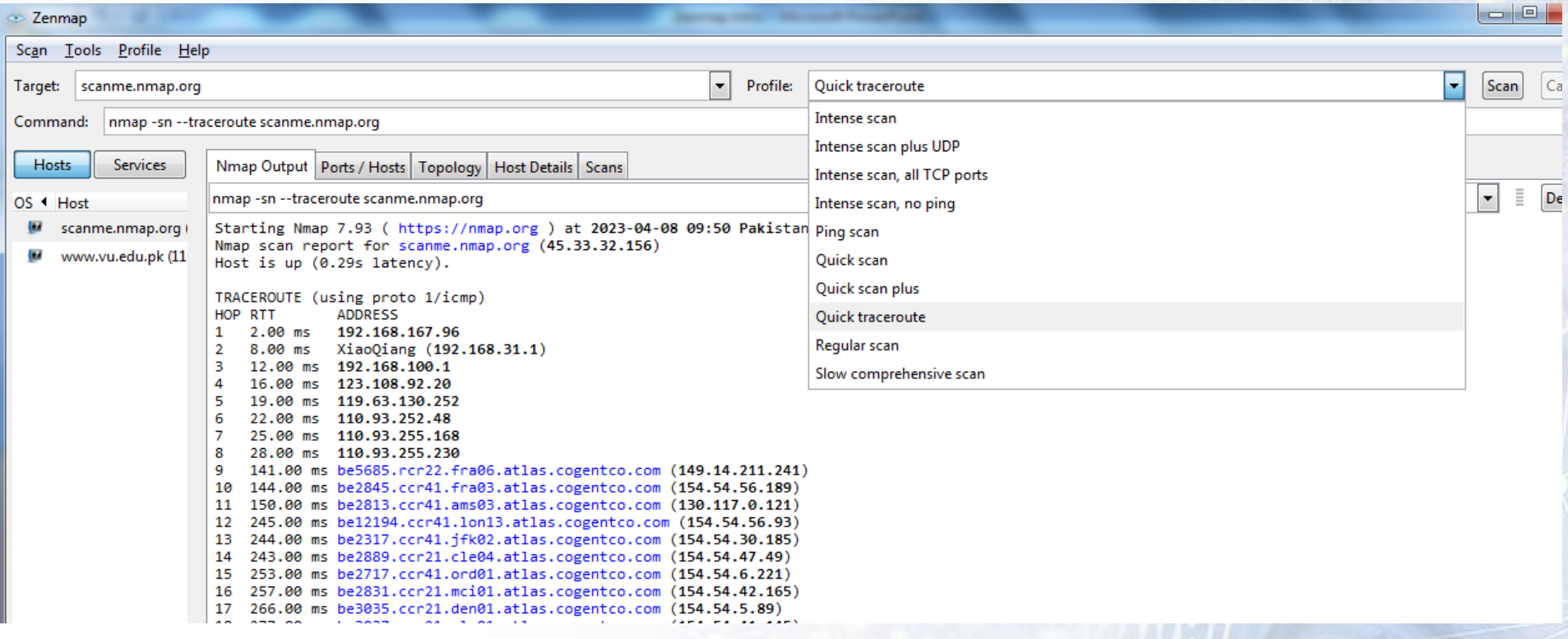
Nmap done: 1 IP address (1 host up) scanned in 17.09 seconds
recording@Mikes-Mac-mini ~ % nmap -n 45.33.32.156
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 13:57 EDT
Nmap scan report for 45.33.32.156
Host is up (0.079s latency).
Not shown: 992 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open     nping-echo
31337/tcp open     Elite

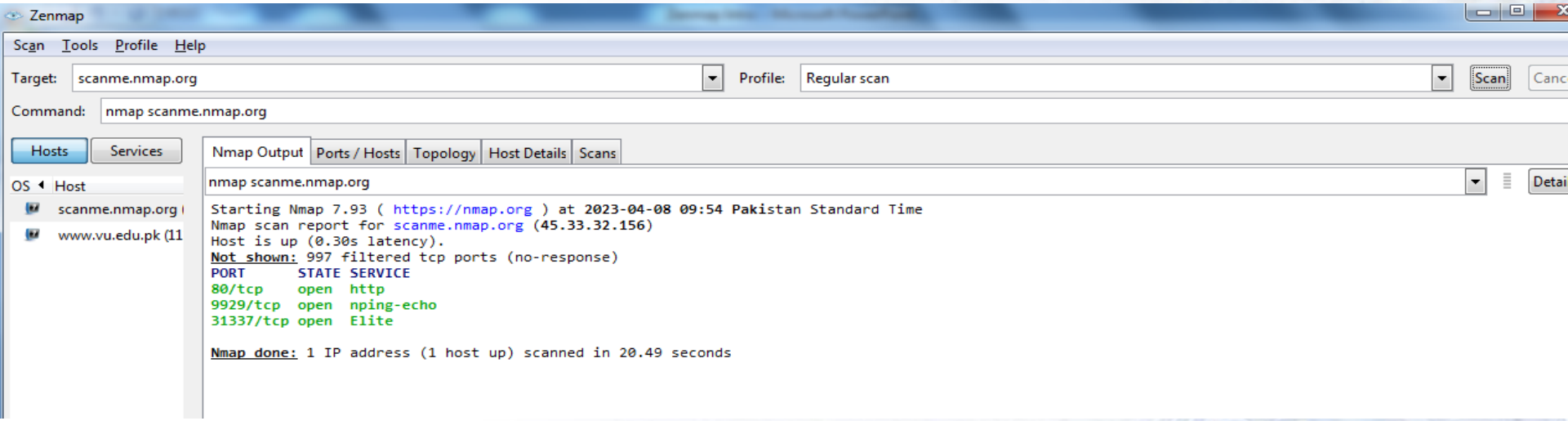
Nmap done: 1 IP address (1 host up) scanned in 16.89 seconds
```

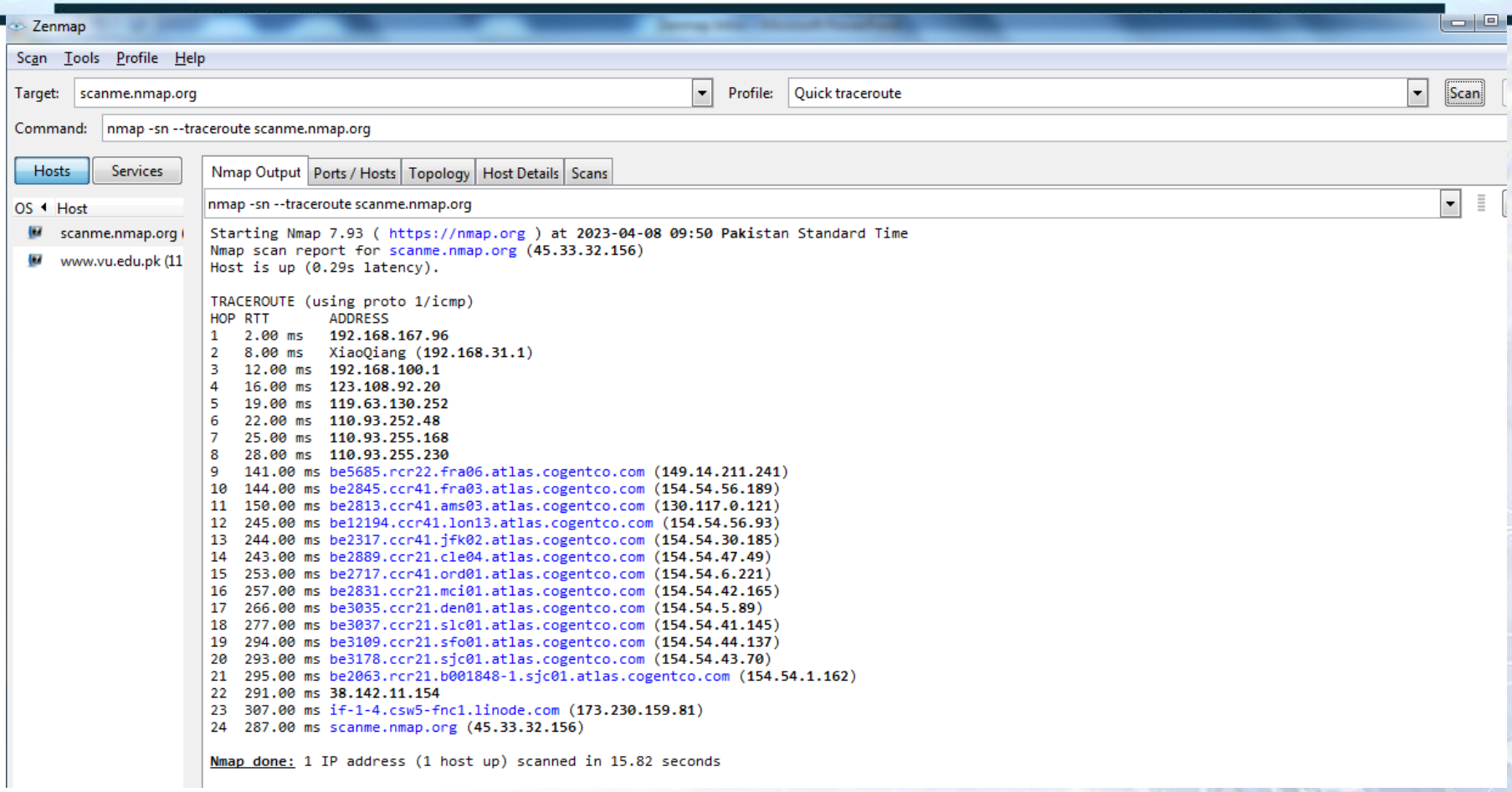
Zenmap

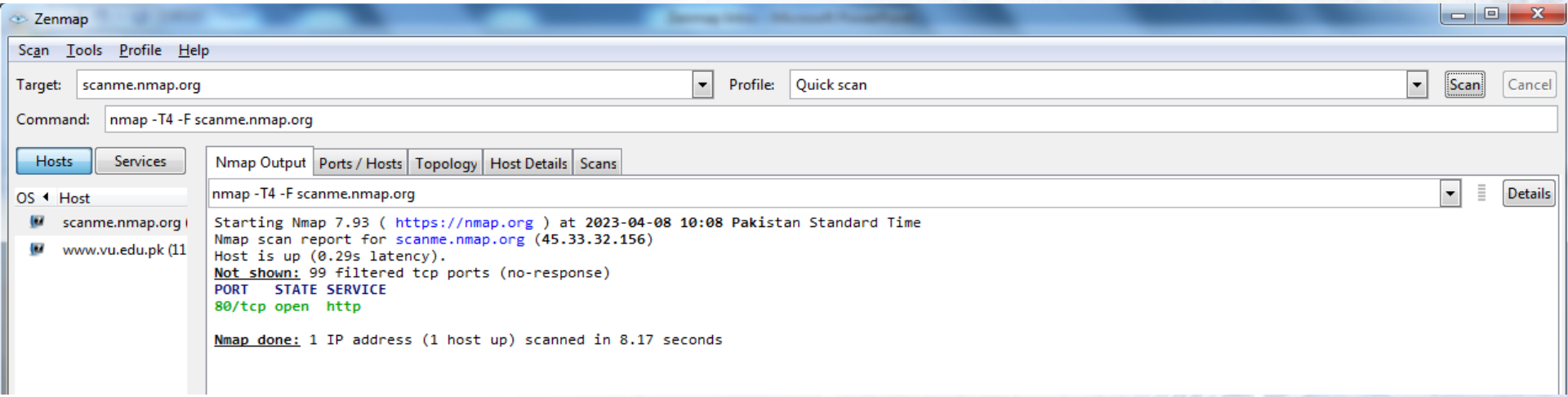
https://nmap.org/book/zenmap-results.html

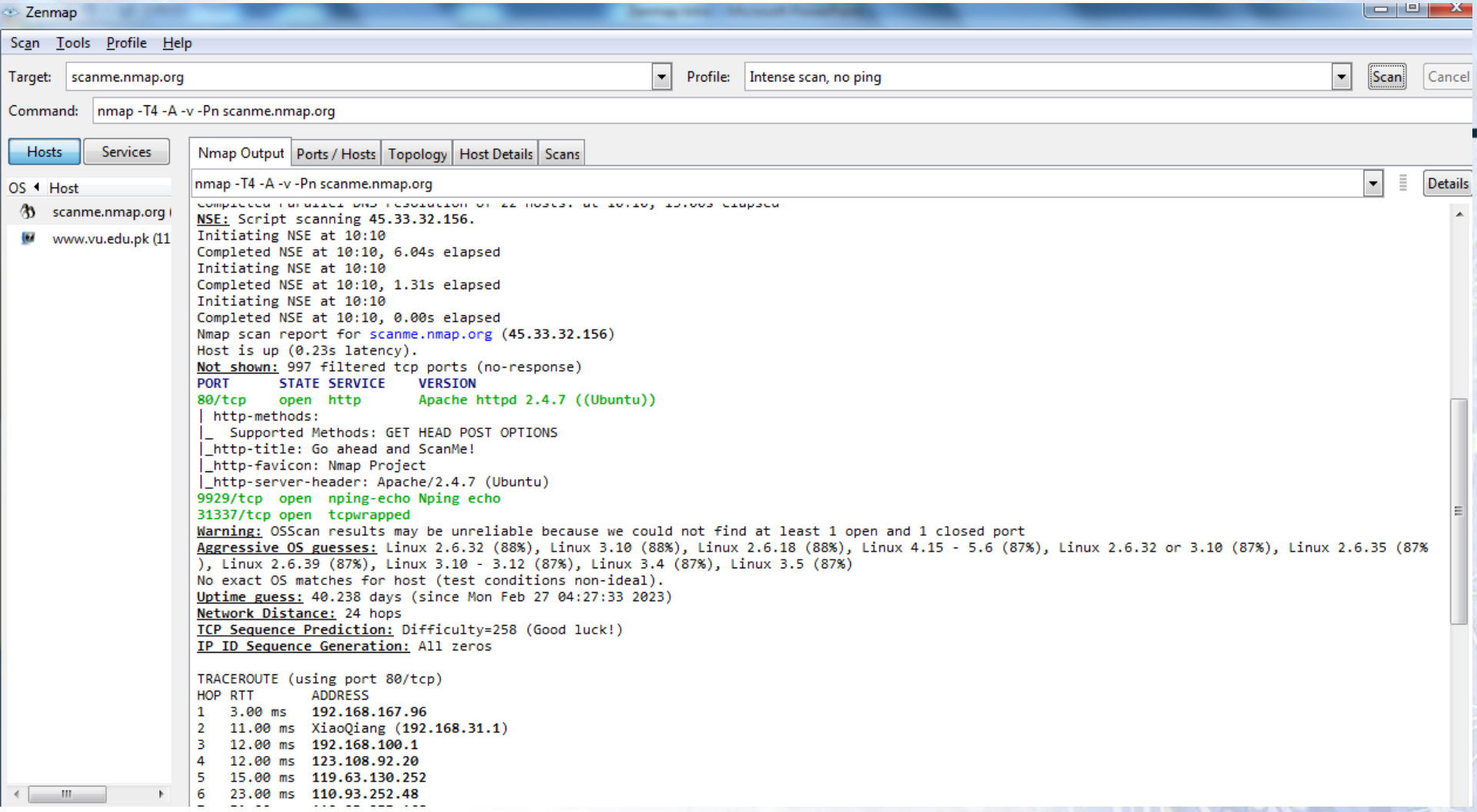
- Zenmap is the official graphical user interface (GUI) for the Nmap Security Scanner.
- Easy for beginners to use while providing advanced features for experienced Nmap users.

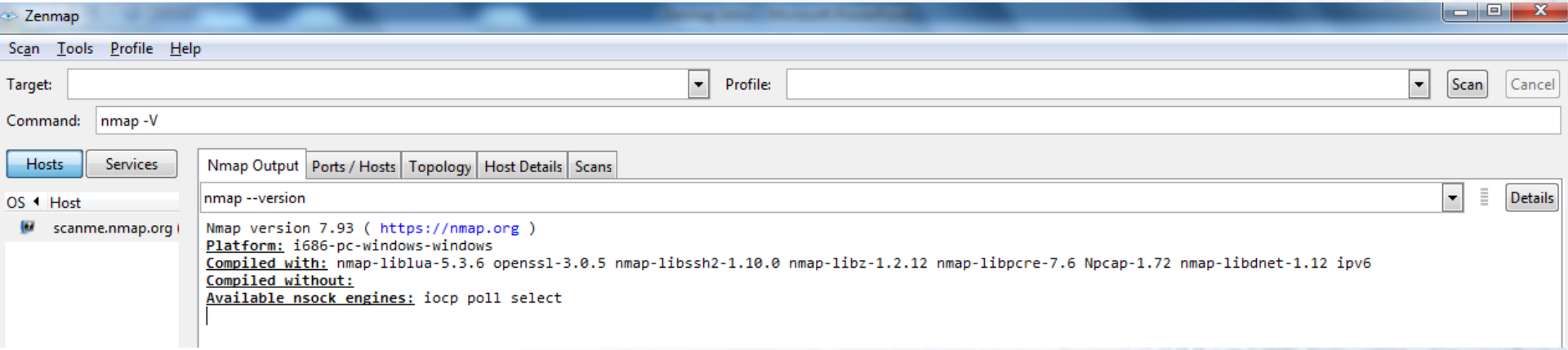

Zenmap
Scan Tools Profile Help
Target: scanme.nmap.org
Profile: Quick traceroute
Scan
Command: nmap -sn --traceroute scanme.nmap.org
Hosts Services
OS Host
scanme.nmap.org
www.vu.edu.pk (11
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -sn --traceroute scanme.nmap.org
Starting Nmap 7.93 (https://nmap.org) at 2023-04-08 09:50 Pakistan
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.29s latency).
TRACEROUTE (using proto 1/icmp)
HOP RTT ADDRESS
1 2.00 ms 192.168.167.96
2 8.00 ms XiaoQiang (192.168.31.1)
3 12.00 ms 192.168.100.1
4 16.00 ms 123.108.92.20
5 19.00 ms 119.63.130.252
6 22.00 ms 110.93.252.48
7 25.00 ms 110.93.255.168
8 28.00 ms 110.93.255.230
9 141.00 ms be5685.rcr22.fra06.atlas.cogentco.com (149.14.211.241)
10 144.00 ms be2845.ccr41.fra03.atlas.cogentco.com (154.54.56.189)
11 150.00 ms be2813.ccr41.ams03.atlas.cogentco.com (130.117.0.121)
12 245.00 ms be12194.ccr41.lon13.atlas.cogentco.com (154.54.56.93)
13 244.00 ms be2317.ccr41.jfk02.atlas.cogentco.com (154.54.30.185)
14 243.00 ms be2889.ccr21.cle04.atlas.cogentco.com (154.54.47.49)
15 253.00 ms be2717.ccr41.ord01.atlas.cogentco.com (154.54.6.221)
16 257.00 ms be2831.ccr21.mci01.atlas.cogentco.com (154.54.42.165)
17 266.00 ms be3035.ccr21.den01.atlas.cogentco.com (154.54.5.89)
Intense scan
Intense scan plus UDP
Intense scan, all TCP ports
Intense scan, no ping
Ping scan
Quick scan
Quick scan plus
Quick traceroute
Regular scan
Slow comprehensive scan

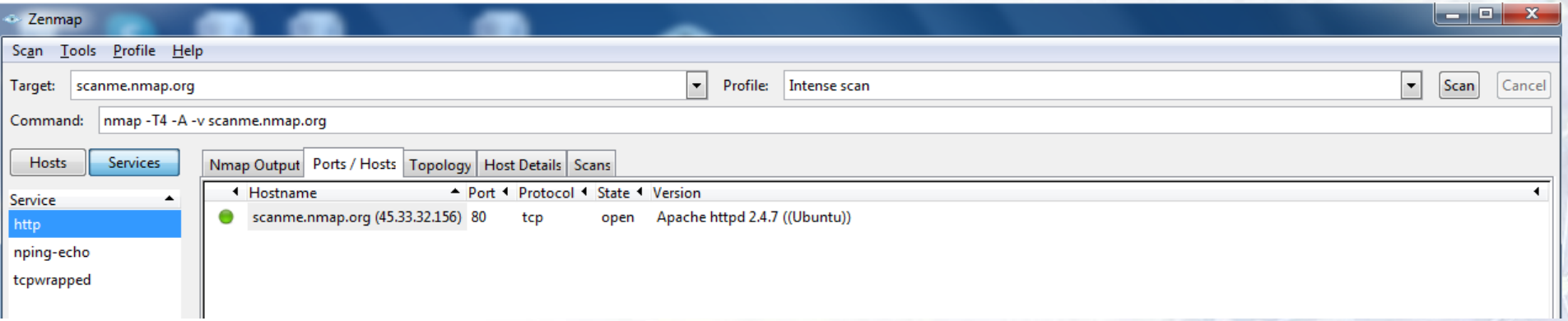

Zenmap
Scan Tools Profile Help
Target: scanme.nmap.org
Profile: Regular scan
Scan
Command: nmap scanme.nmap.org
Hosts
Services
OS Host
scanme.nmap.org
www.vu.edu.pk (11
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap scanme.nmap.org
Starting Nmap 7.93 (https://nmap.org) at 2023-04-08 09:54 Pakistan Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.30s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT STATE SERVICE
80/tcp open http
9929/tcp open nping-echo
31337/tcp open Elite
Nmap done: 1 IP address (1 host up) scanned in 20.49 seconds

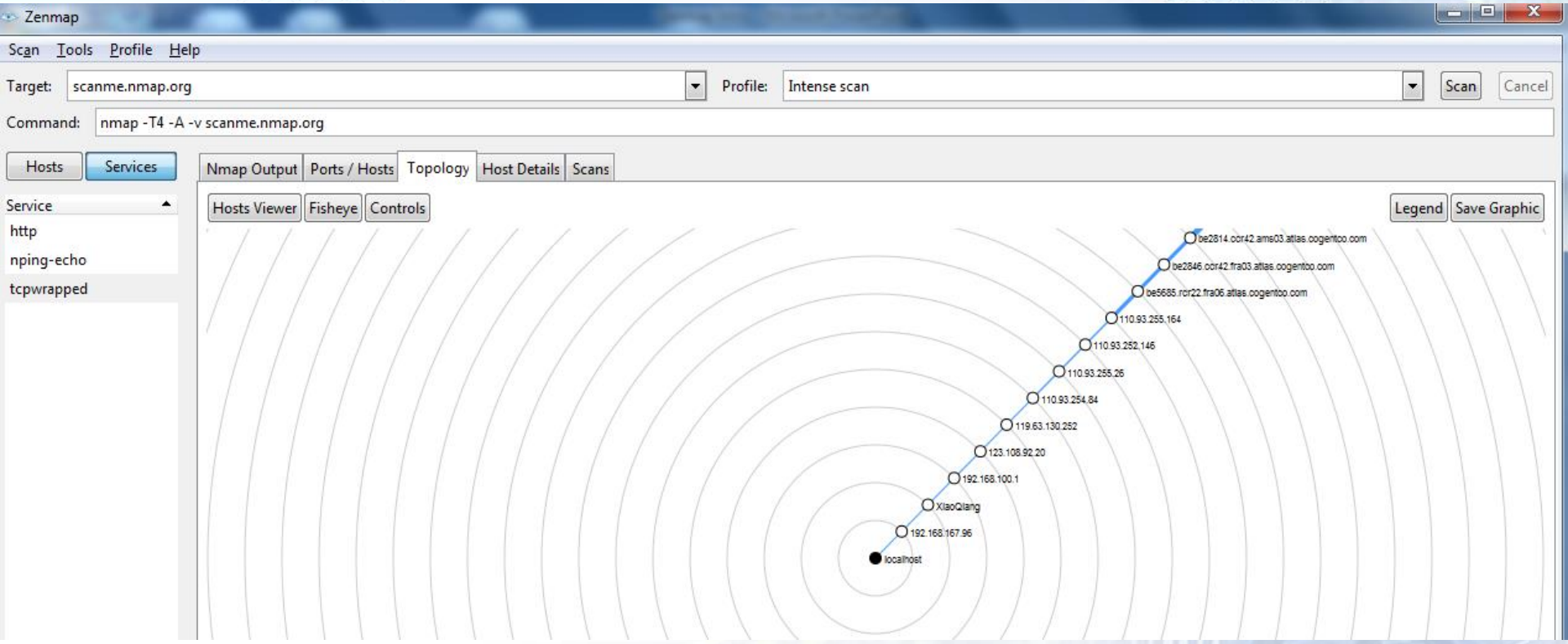

Zenmap
Scan Tools Profile Help
Target: scanme.nmap.org
Profile: Quick traceroute
Scan
Command: nmap -sn --traceroute scanme.nmap.org
Hosts
Services
OS Host
scanme.nmap.org
www.vu.edu.pk (11
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -sn --traceroute scanme.nmap.org
Starting Nmap 7.93 (https://nmap.org) at 2023-04-08 09:50 Pakistan Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.29s latency).
TRACEROUTE (using proto 1/icmp)
HOP RTT ADDRESS
1 2.00 ms 192.168.167.96
2 8.00 ms XiaoQiang (192.168.31.1)
3 12.00 ms 192.168.100.1
4 16.00 ms 123.108.92.20
5 19.00 ms 119.63.130.252
6 22.00 ms 110.93.252.48
7 25.00 ms 110.93.255.168
8 28.00 ms 110.93.255.230
9 141.00 ms be5685.rcr22.fra06.atlas.cogentco.com (149.14.211.241)
10 144.00 ms be2845.ccr41.fra03.atlas.cogentco.com (154.54.56.189)
11 150.00 ms be2813.ccr41.ams03.atlas.cogentco.com (130.117.0.121)
12 245.00 ms be12194.ccr41.lon13.atlas.cogentco.com (154.54.56.93)
13 244.00 ms be2317.ccr41.jfk02.atlas.cogentco.com (154.54.30.185)
14 243.00 ms be2889.ccr21.cle04.atlas.cogentco.com (154.54.47.49)
15 253.00 ms be2717.ccr41.ord01.atlas.cogentco.com (154.54.6.221)
16 257.00 ms be2831.ccr21.mci01.atlas.cogentco.com (154.54.42.165)
17 266.00 ms be3035.ccr21.den01.atlas.cogentco.com (154.54.5.89)
18 277.00 ms be3037.ccr21.slc01.atlas.cogentco.com (154.54.41.145)
19 294.00 ms be3109.ccr21.sfo01.atlas.cogentco.com (154.54.44.137)
20 293.00 ms be3178.ccr21.sjc01.atlas.cogentco.com (154.54.43.70)
21 295.00 ms be2063.rcr21.b001848-1.sjc01.atlas.cogentco.com (154.54.1.162)
22 291.00 ms 38.142.11.154
23 307.00 ms if-1-4.csw5-fnc1.linode.com (173.230.159.81)
24 287.00 ms scanme.nmap.org (45.33.32.156)
Nmap done: 1 IP address (1 host up) scanned in 15.82 seconds

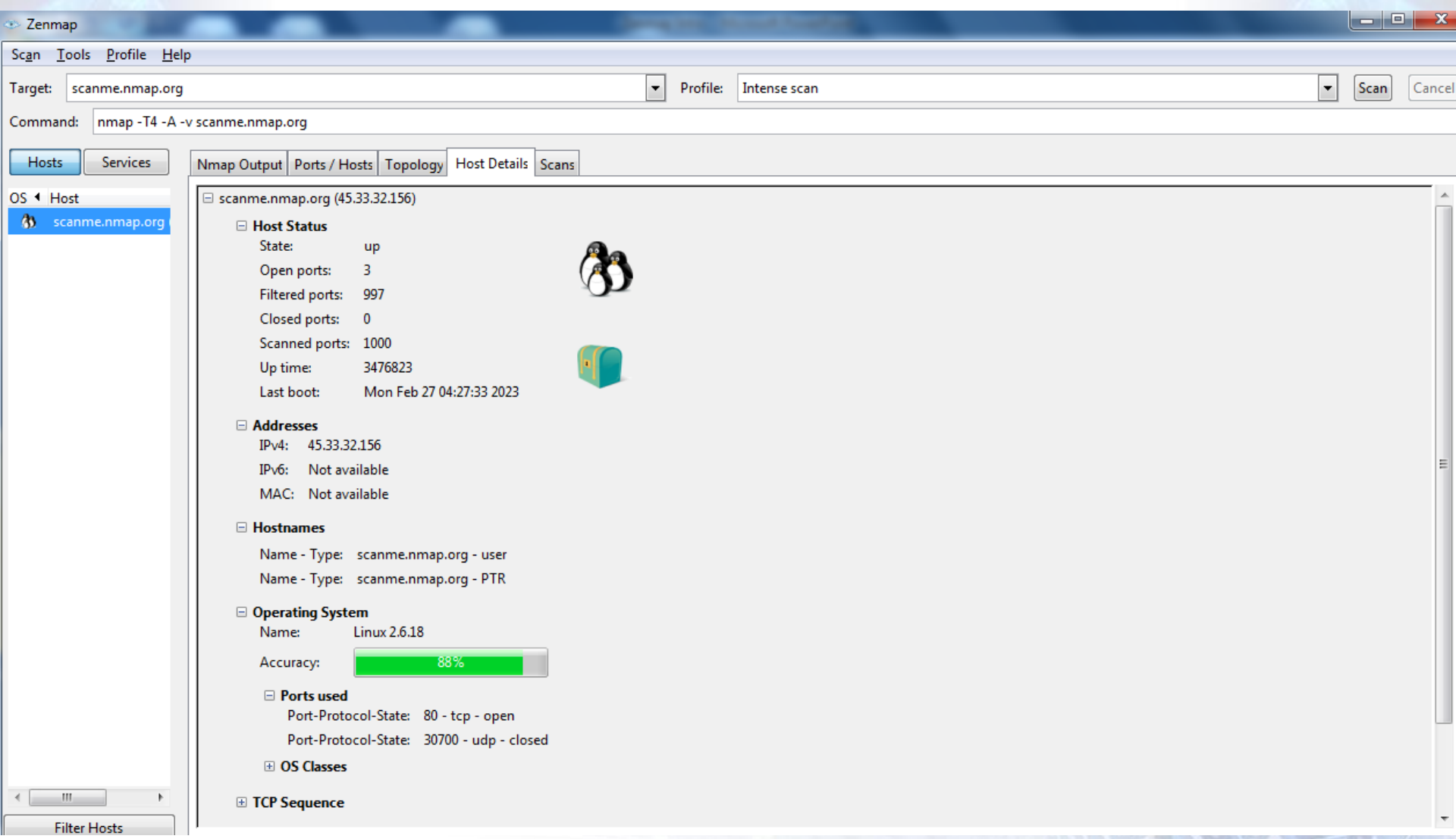

Zenmap
Scan Tools Profile Help
Target: scanme.nmap.org
Profile: Quick scan
Scan
Cancel
Command: nmap -T4 -F scanme.nmap.org
Hosts
Services
OS Host
scanme.nmap.org
www.vu.edu.pk (11
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -F scanme.nmap.org
Details
Starting Nmap 7.93 (https://nmap.org) at 2023-04-08 10:08 Pakistan Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.29s latency).
Not shown: 99 filtered tcp ports (no-response)
PORT STATE SERVICE
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 8.17 seconds

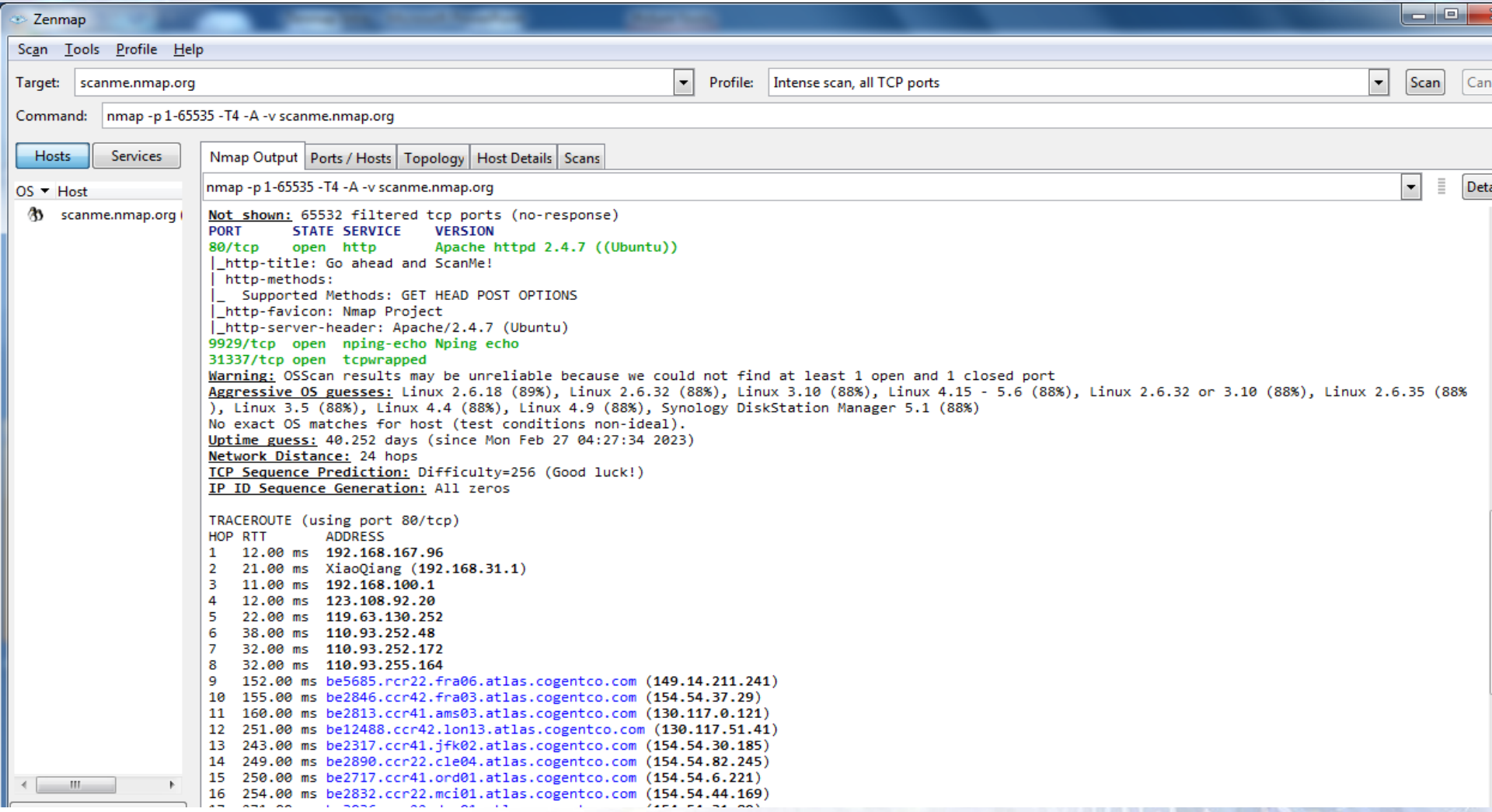

Zenmap
Scan Tools Profile Help
Target: scanme.nmap.org
Profile: Intense scan, no ping
Scan
Cancel
Command: nmap -T4 -A -v -Pn scanme.nmap.org
Hosts
Services
OS Host
scanme.nmap.org
www.vu.edu.pk (11
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -A -v -Pn scanme.nmap.org
Details
NSE: Script scanning 45.33.32.156.
Initiating NSE at 10:10
Completed NSE at 10:10, 6.04s elapsed
Initiating NSE at 10:10
Completed NSE at 10:10, 1.31s elapsed
Initiating NSE at 10:10
Completed NSE at 10:10, 0.00s elapsed
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.23s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.4.7 ((Ubuntu))
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-title: Go ahead and ScanMe!
|_http-favicon: Nmap Project
|_http-server-header: Apache/2.4.7 (Ubuntu)
9929/tcp open nping-echo Nping echo
31337/tcp open tcpwrapped
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 2.6.32 (88%), Linux 3.10 (88%), Linux 2.6.18 (88%), Linux 4.15 - 5.6 (87%), Linux 2.6.32 or 3.10 (87%), Linux 2.6.35 (87%), Linux 2.6.39 (87%), Linux 3.10 - 3.12 (87%), Linux 3.4 (87%), Linux 3.5 (87%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 40.238 days (since Mon Feb 27 04:27:33 2023)
Network Distance: 24 hops
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: All zeros
TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 3.00 ms 192.168.167.96
2 11.00 ms XiaoQiang (192.168.31.1)
3 12.00 ms 192.168.100.1
4 12.00 ms 123.108.92.20
5 15.00 ms 119.63.130.252
6 23.00 ms 110.93.252.48

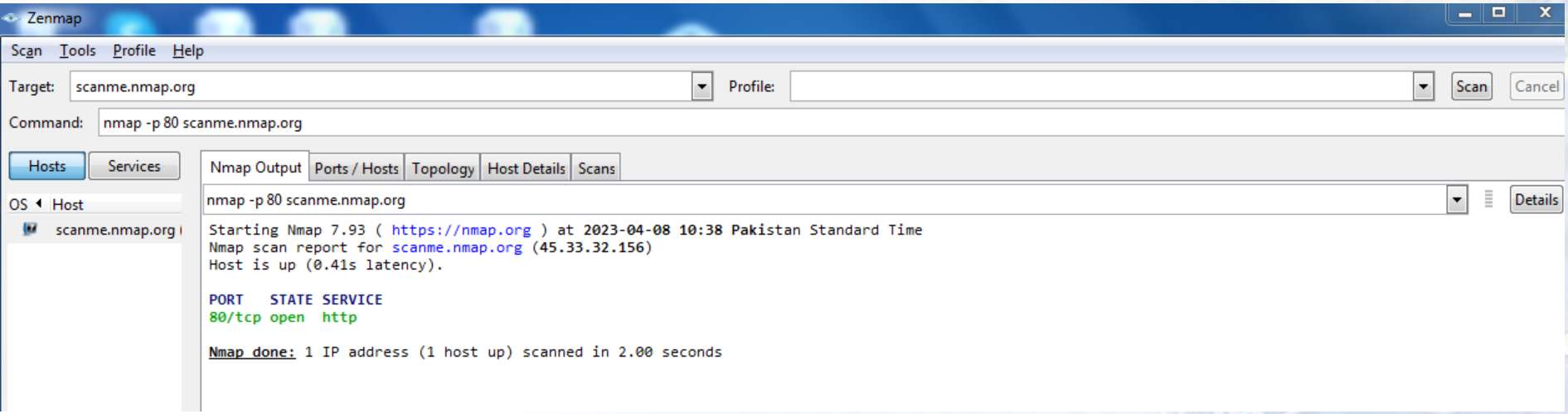

Zenmap
Scan Tools Profile Help
Target:
Profile:
Scan
Cancel
Command: nmap -V
Hosts
Services
OS Host
scanme.nmap.org
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap --version
Details
Nmap version 7.93 (https://nmap.org)
Platform: i686-pc-windows-windows
Compiled with: nmap-liblua-5.3.6 openssl-3.0.5 nmap-libssh2-1.10.0 nmap-libz-1.2.12 nmap-libpcre-7.6 Npcap-1.72 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: iocp poll select

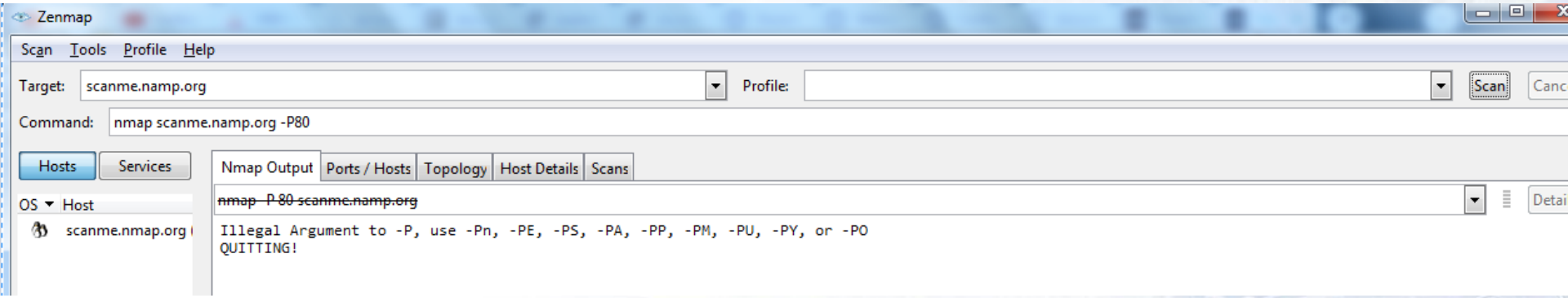

Zenmap
Scan Tools Profile Help
Target: scanme.nmap.org
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v scanme.nmap.org
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Service
http
nping-echo
tcpwrapped
Hostname
Port
Protocol
State
Version
scanme.nmap.org (45.33.32.156)
80
tcp
open
Apache httpd 2.4.7 ((Ubuntu))

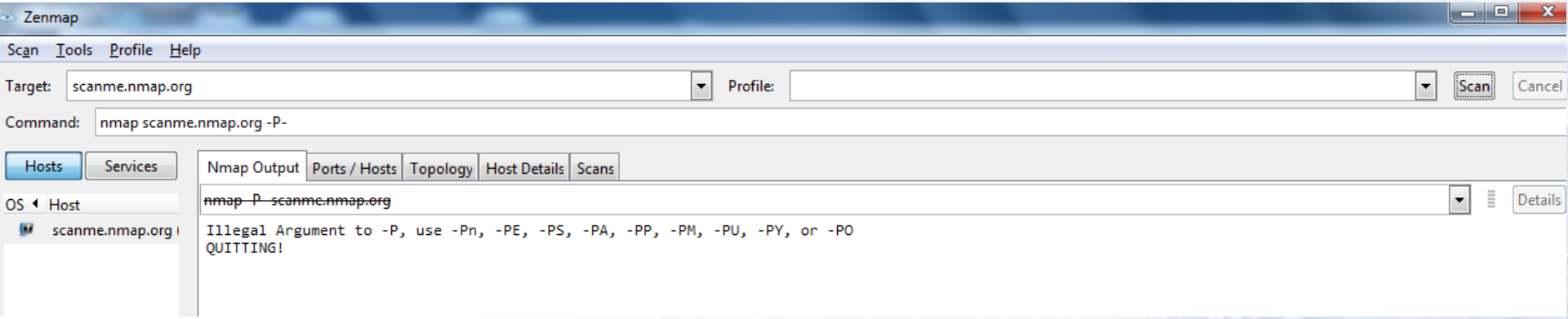

Zenmap
Scan Tools Profile Help
Target: scanme.nmap.org
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v scanme.nmap.org
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Service
http
nping-echo
tcpwrapped
Hosts Viewer
Fisheye
Controls
Legend
Save Graphic
be2814.ccr42.ams03.atlas.cogentco.com
be2846.ccr42.fra03.atlas.cogentco.com
be5685.rcr22.fra06.atlas.cogentco.com
110.93.255.164
110.93.252.146
110.93.255.26
110.93.254.84
119.63.130.252
123.108.92.20
192.168.100.1
XiaoQiang
192.168.167.96
localhost

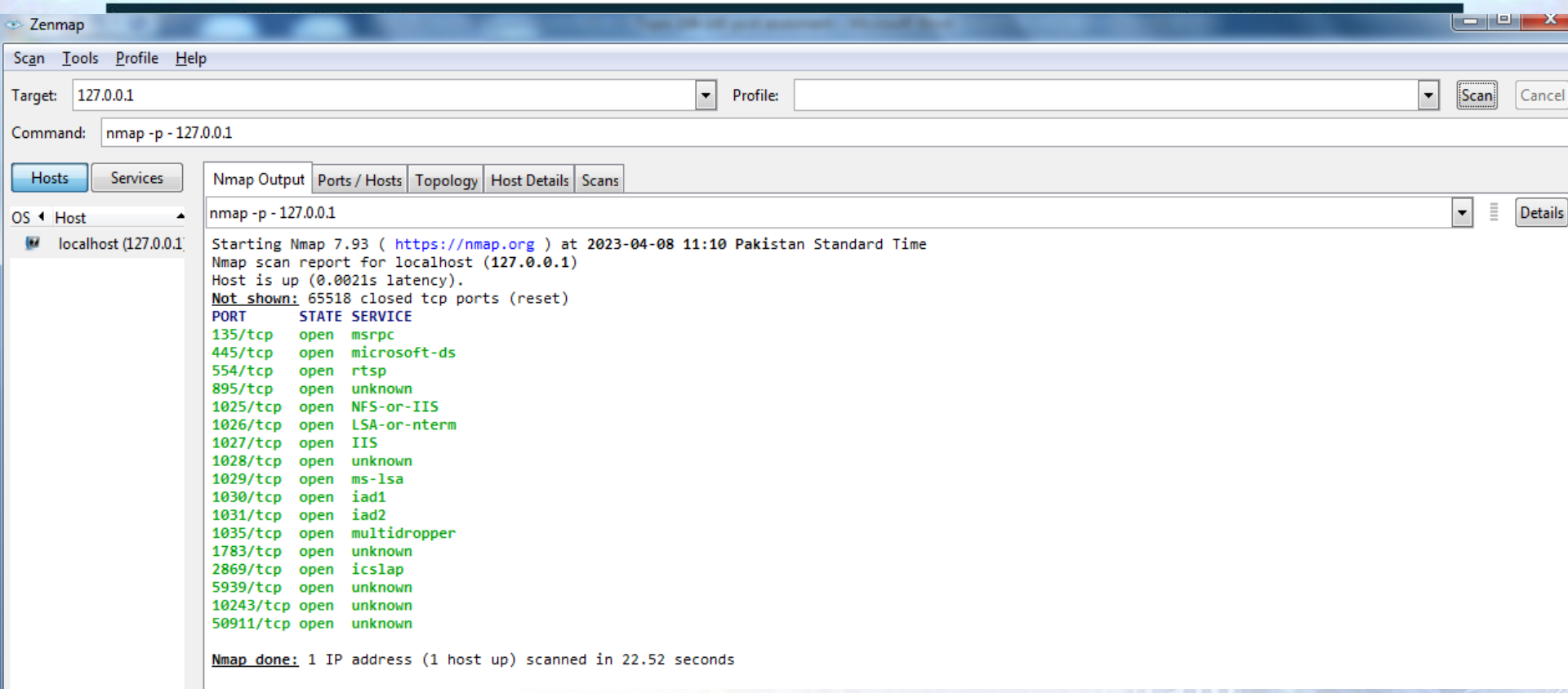

Zenmap
Scan Tools Profile Help
Target: scanme.nmap.org
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v scanme.nmap.org
Hosts
Services
OS Host
scanme.nmap.org
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
scanme.nmap.org (45.33.32.156)
Host Status
State: up
Open ports: 3
Filtered ports: 997
Closed ports: 0
Scanned ports: 1000
Up time: 3476823
Last boot: Mon Feb 27 04:27:33 2023
Addresses
IPv4: 45.33.32.156
IPv6: Not available
MAC: Not available
Hostnames
Name - Type: scanme.nmap.org - user
Name - Type: scanme.nmap.org - PTR
Operating System
Name: Linux 2.6.18
Accuracy: 88%
Ports used
Port-Protocol-State: 80 - tcp - open
Port-Protocol-State: 30700 - udp - closed
OS Classes
TCP Sequence

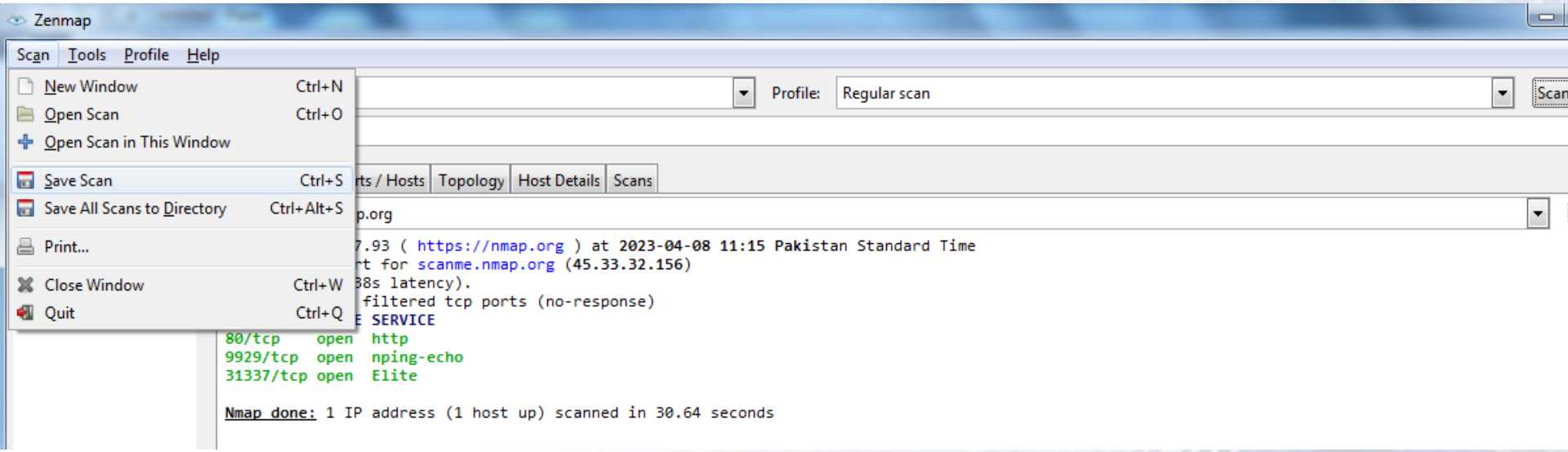

Zenmap
Scan Tools Profile Help
Target: scanme.nmap.org
Profile: Intense scan, all TCP ports
Scan
Command: nmap -p 1-65535 -T4 -A -v scanme.nmap.org
Hosts
Services
OS Host
scanme.nmap.org
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -p 1-65535 -T4 -A -v scanme.nmap.org
Not shown: 65532 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.4.7 ((Ubuntu))
|_http-title: Go ahead and ScanMe!
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-favicon: Nmap Project
|_http-server-header: Apache/2.4.7 (Ubuntu)
9929/tcp open nping-echo Nping echo
31337/tcp open tcpwrapped
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 2.6.18 (89%), Linux 2.6.32 (88%), Linux 3.10 (88%), Linux 4.15 - 5.6 (88%), Linux 2.6.32 or 3.10 (88%), Linux 2.6.35 (88%), Linux 3.5 (88%), Linux 4.4 (88%), Linux 4.9 (88%), Synology DiskStation Manager 5.1 (88%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 40.252 days (since Mon Feb 27 04:27:34 2023)
Network Distance: 24 hops
TCP Sequence Prediction: Difficulty=256 (Good luck!)
IP ID Sequence Generation: All zeros
TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 12.00 ms 192.168.167.96
2 21.00 ms XiaoQiang (192.168.31.1)
3 11.00 ms 192.168.100.1
4 12.00 ms 123.108.92.20
5 22.00 ms 119.63.130.252
6 38.00 ms 110.93.252.48
7 32.00 ms 110.93.252.172
8 32.00 ms 110.93.255.164
9 152.00 ms be5685.rcr22.fra06.atlas.cogentco.com (149.14.211.241)
10 155.00 ms be2846.ccr42.fra03.atlas.cogentco.com (154.54.37.29)
11 160.00 ms be2813.ccr41.ams03.atlas.cogentco.com (130.117.0.121)
12 251.00 ms be12488.ccr42.lon13.atlas.cogentco.com (130.117.51.41)
13 243.00 ms be2317.ccr41.jfk02.atlas.cogentco.com (154.54.30.185)
14 249.00 ms be2890.ccr22.cle04.atlas.cogentco.com (154.54.82.245)
15 250.00 ms be2717.ccr41.ord01.atlas.cogentco.com (154.54.6.221)
16 254.00 ms be2832.ccr22.mci01.atlas.cogentco.com (154.54.44.169)


Zenmap
Scan Tools Profile Help
Target: scanme.nmap.org
Profile:
Scan
Cancel
Command: nmap -p 80 scanme.nmap.org
Hosts
Services
OS Host
scanme.nmap.org
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -p 80 scanme.nmap.org
Details
Starting Nmap 7.93 (https://nmap.org) at 2023-04-08 10:38 Pakistan Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.41s latency).
PORT STATE SERVICE
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 2.00 seconds


Zenmap
Scan Tools Profile Help
Target: scanme.namp.org
Profile:
Scan
Command: nmap scanme.namp.org -P80
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS Host
scanme.nmap.org
nmap -P 80 scanme.namp.org
Illegal Argument to -P, use -Pn, -PE, -PS, -PA, -PP, -PM, -PU, -PY, or -PO
QUITTING!


Zenmap
Scan Tools Profile Help
Target: scanme.nmap.org
Profile:
Scan
Cancel
Command: nmap scanme.nmap.org -P-
Hosts
Services
OS Host
scanme.nmap.org
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -P- scanme.nmap.org
Details
Illegal Argument to -P, use -Pn, -PE, -PS, -PA, -PP, -PM, -PU, -PY, or -PO
QUITTING!

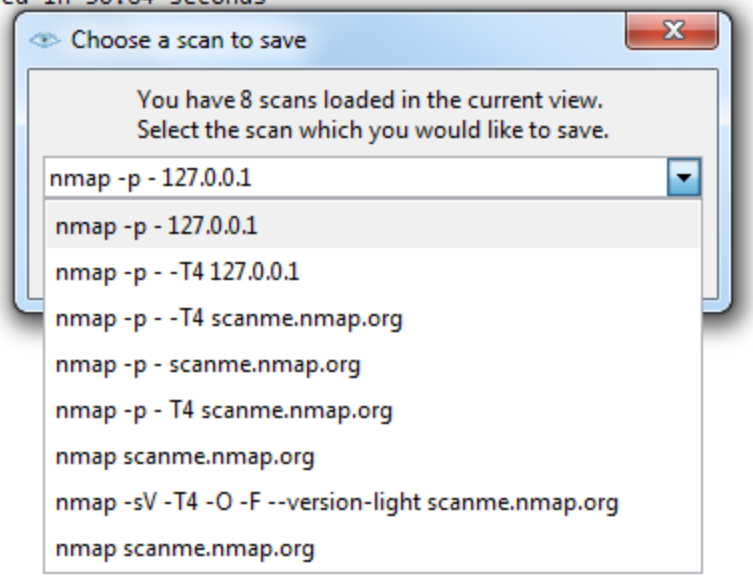

Zenmap
Scan Tools Profile Help
Target: 127.0.0.1
Profile:
Scan
Cancel
Command: nmap -p - 127.0.0.1
Hosts
Services
OS Host
localhost (127.0.0.1)
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -p - 127.0.0.1
Details
Starting Nmap 7.93 (https://nmap.org) at 2023-04-08 11:10 Pakistan Standard Time
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0021s latency).
Not shown: 65518 closed tcp ports (reset)
PORT STATE SERVICE
135/tcp open msrpc
445/tcp open microsoft-ds
554/tcp open rtsp
895/tcp open unknown
1025/tcp open NFS-or-IIS
1026/tcp open LSA-or-nterm
1027/tcp open IIS
1028/tcp open unknown
1029/tcp open ms-lsa
1030/tcp open iad1
1031/tcp open iad2
1035/tcp open multidropper
1783/tcp open unknown
2869/tcp open icslap
5939/tcp open unknown
10243/tcp open unknown
50911/tcp open unknown
Nmap done: 1 IP address (1 host up) scanned in 22.52 seconds


Zenmap
Scan Tools Profile Help
New Window Ctrl+N
Open Scan Ctrl+O
Open Scan in This Window
Save Scan Ctrl+S
Save All Scans to Directory Ctrl+Alt+S
Print...
Close Window Ctrl+W
Quit Ctrl+Q
Profile: Regular scan
Scan
Topology
Host Details
Scans
7.93 (https://nmap.org) at 2023-04-08 11:15 Pakistan Standard Time
for scanme.nmap.org (45.33.32.156)
filtered tcp ports (no-response)
SERVICE
80/tcp open http
9929/tcp open nping-echo
31337/tcp open Elite
Nmap done: 1 IP address (1 host up) scanned in 30.64 seconds

nmap scanme.nmap.org

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-08 11:15 Pakistan Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.38s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

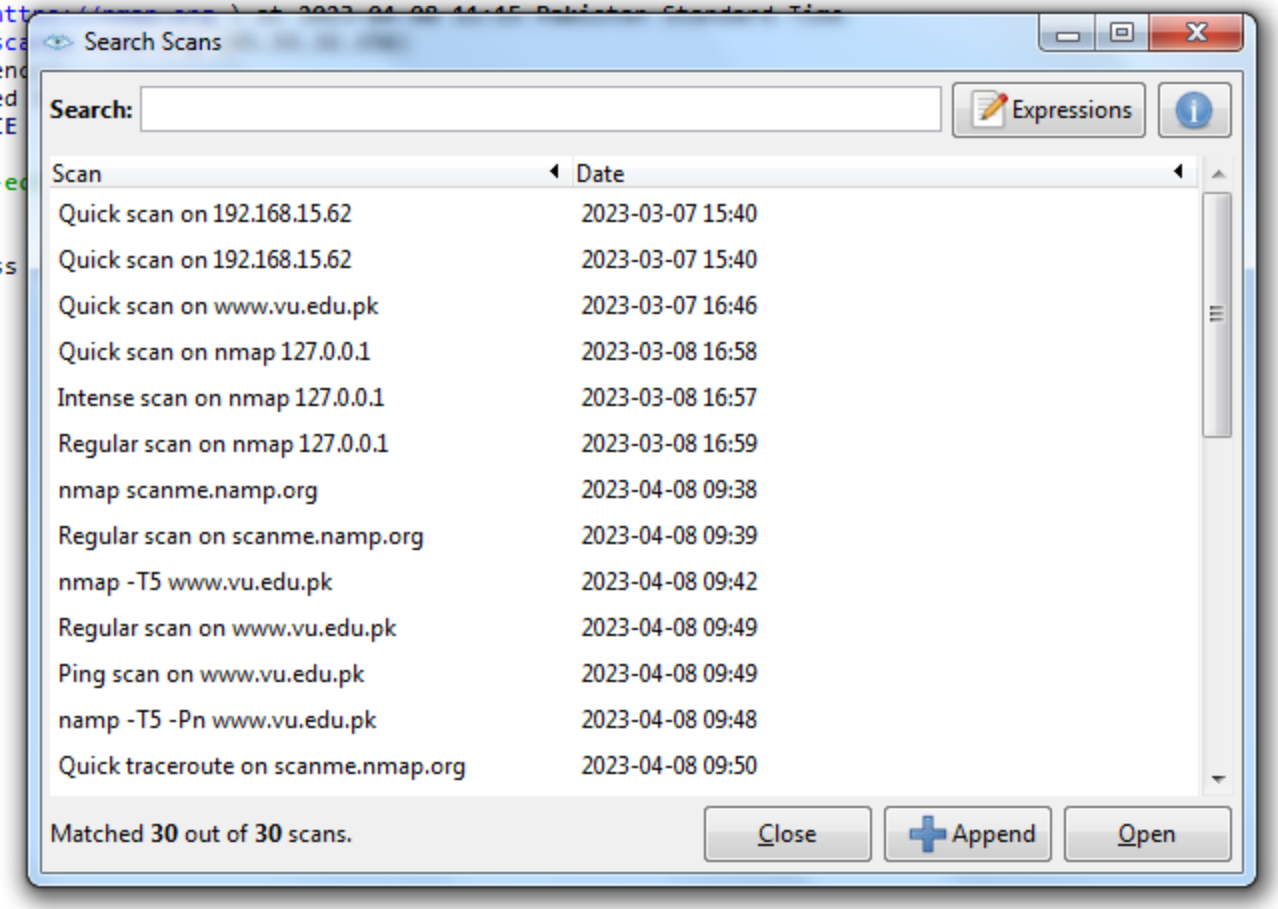
Nmap done: 1 IP address (1 host up) scanned in 30.64 seconds
```

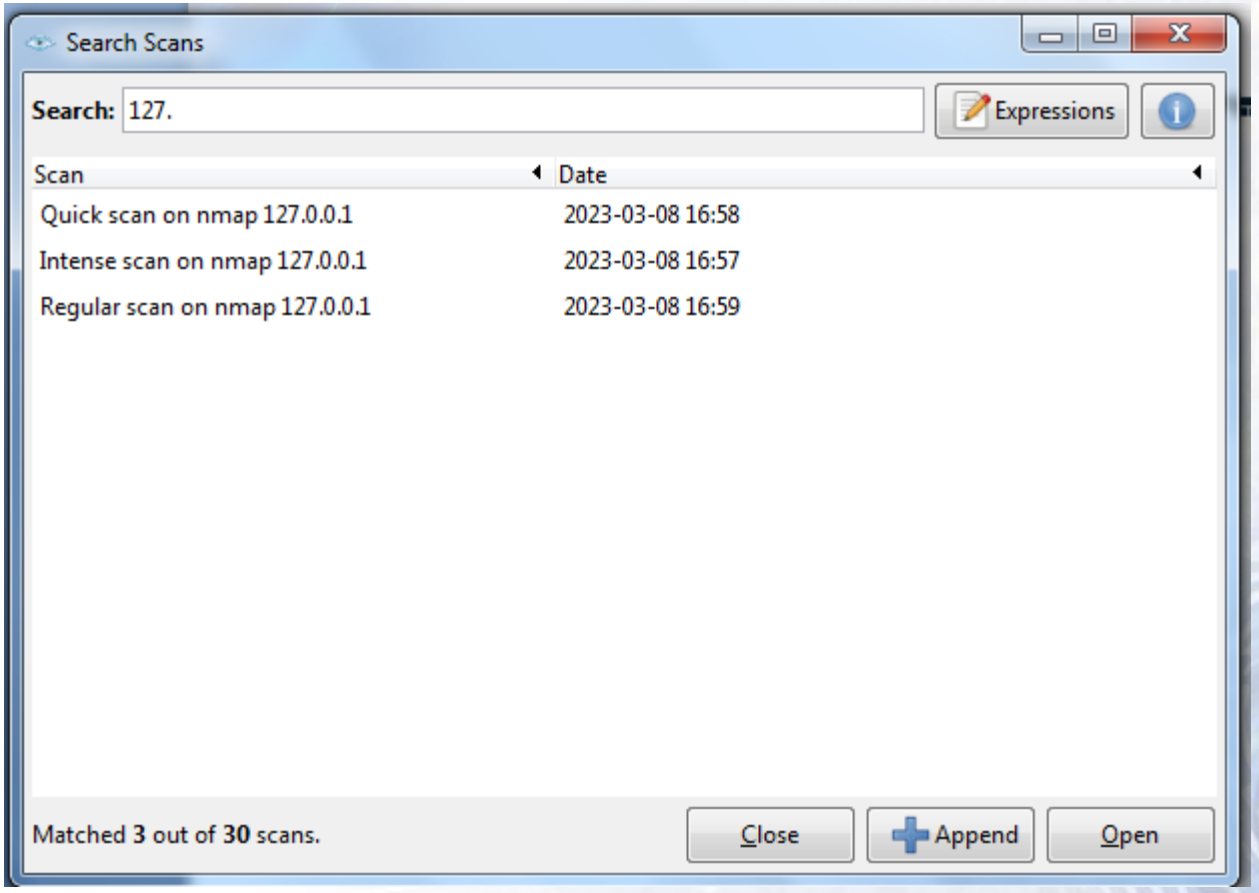


nmap scanme.nmap.org

```
Starting Nmap 7.93 ( http
Nmap scan report for sca
Host is up (0.38s laten
Not shown: 997 filtered
PORT      STATE SERVICE
80/tcp    open  http
9929/tcp  open  nping-e
31337/tcp open  Elite

Nmap done: 1 IP address
```

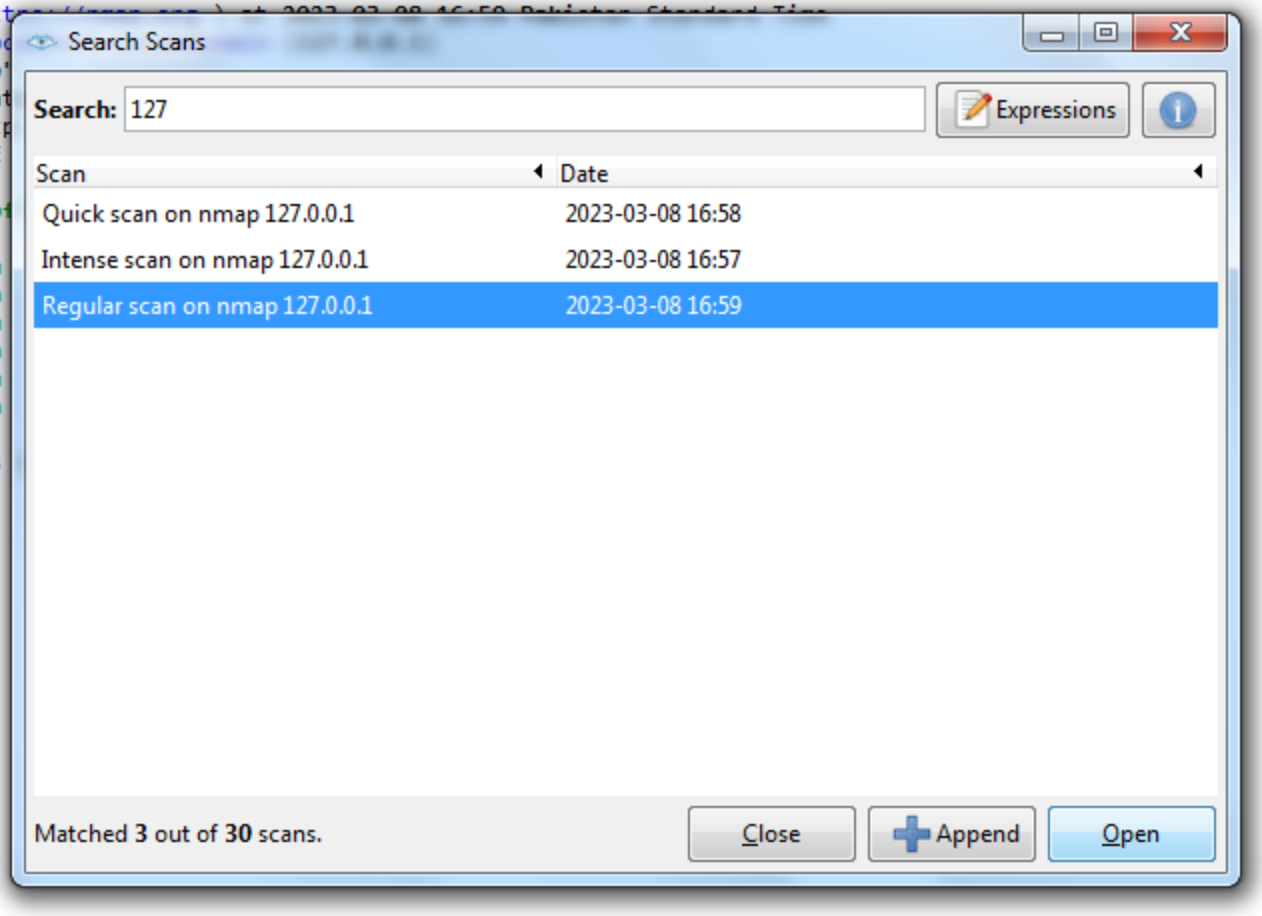


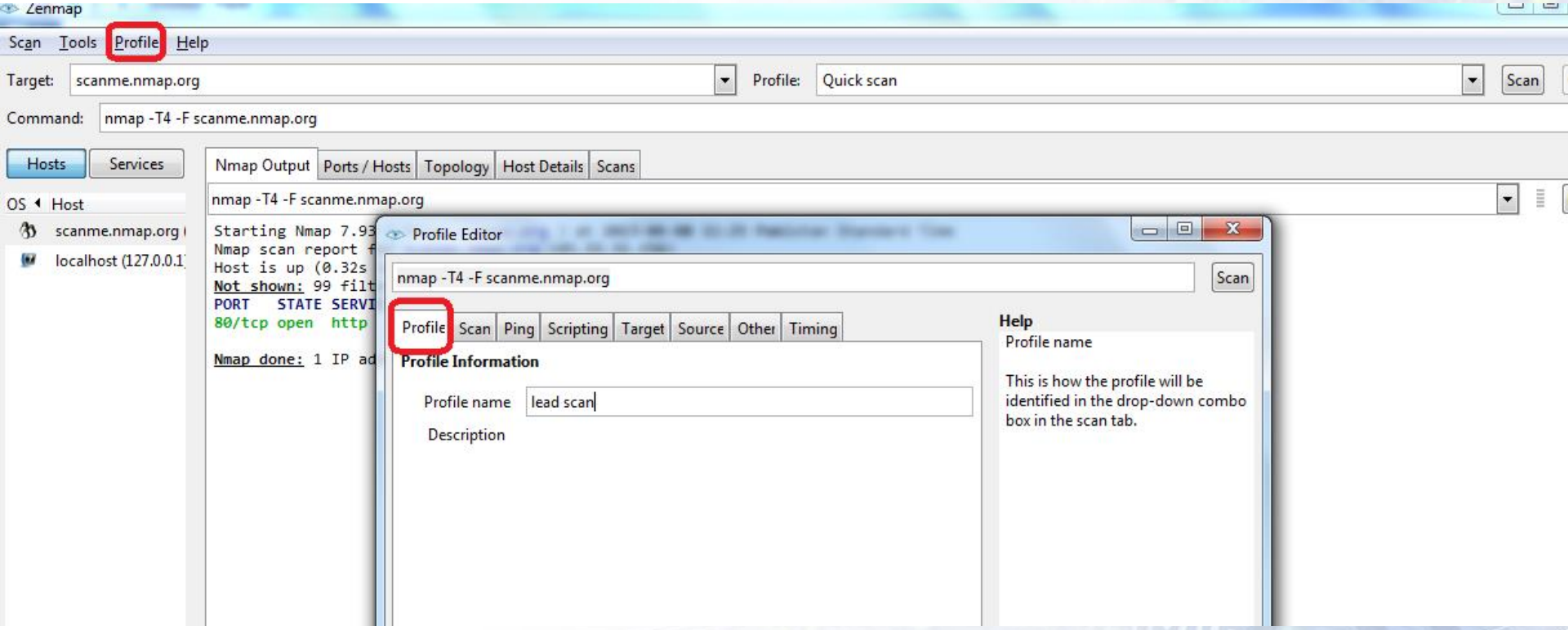

Search Scans
Search: 127.
Expressions
Scan
Date
Quick scan on nmap 127.0.0.1
2023-03-08 16:58
Intense scan on nmap 127.0.0.1
2023-03-08 16:57
Regular scan on nmap 127.0.0.1
2023-03-08 16:59
Matched 3 out of 30 scans.
Close
Append
Open

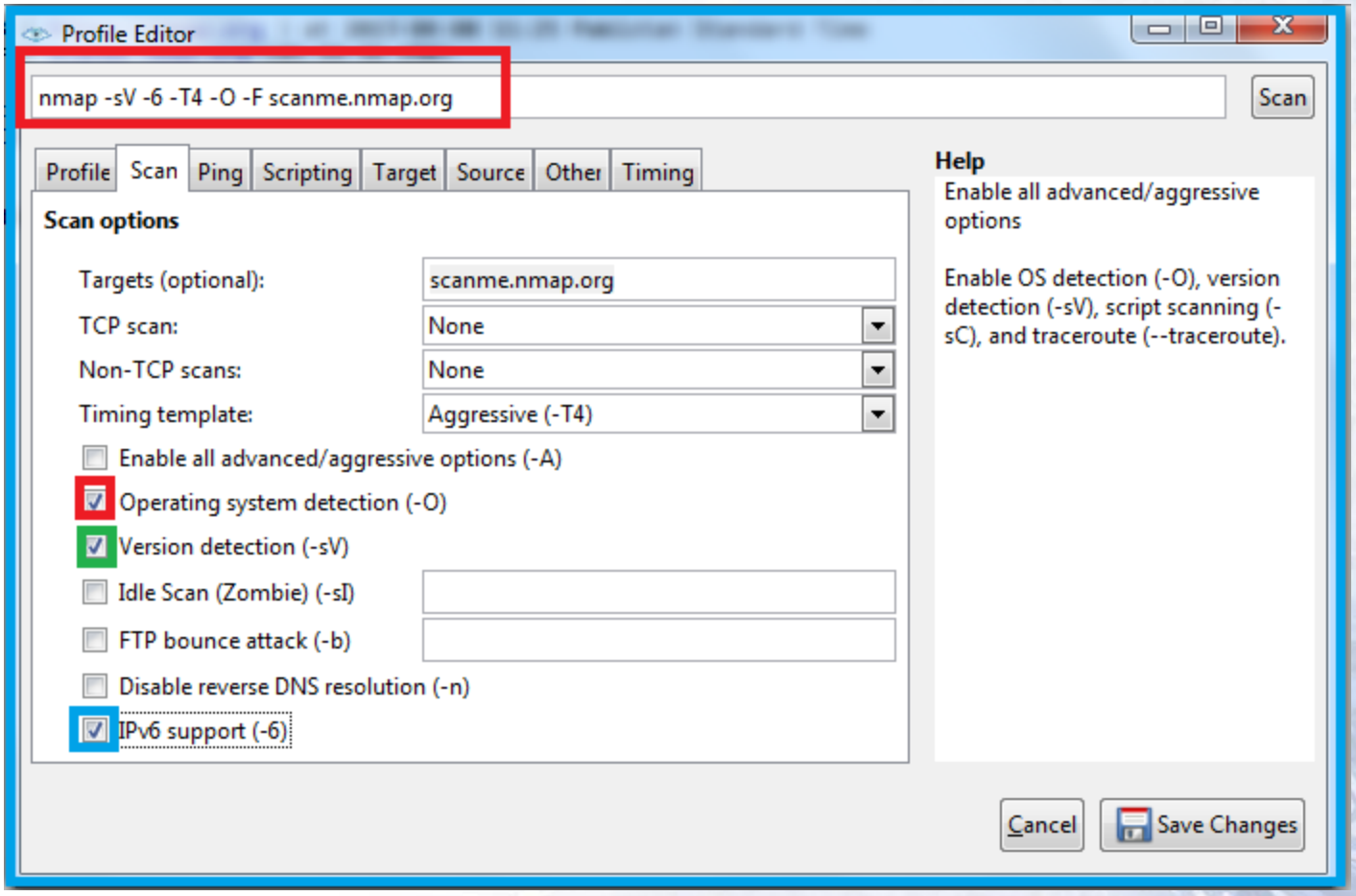
nmap -F nmap 127.0.0.1

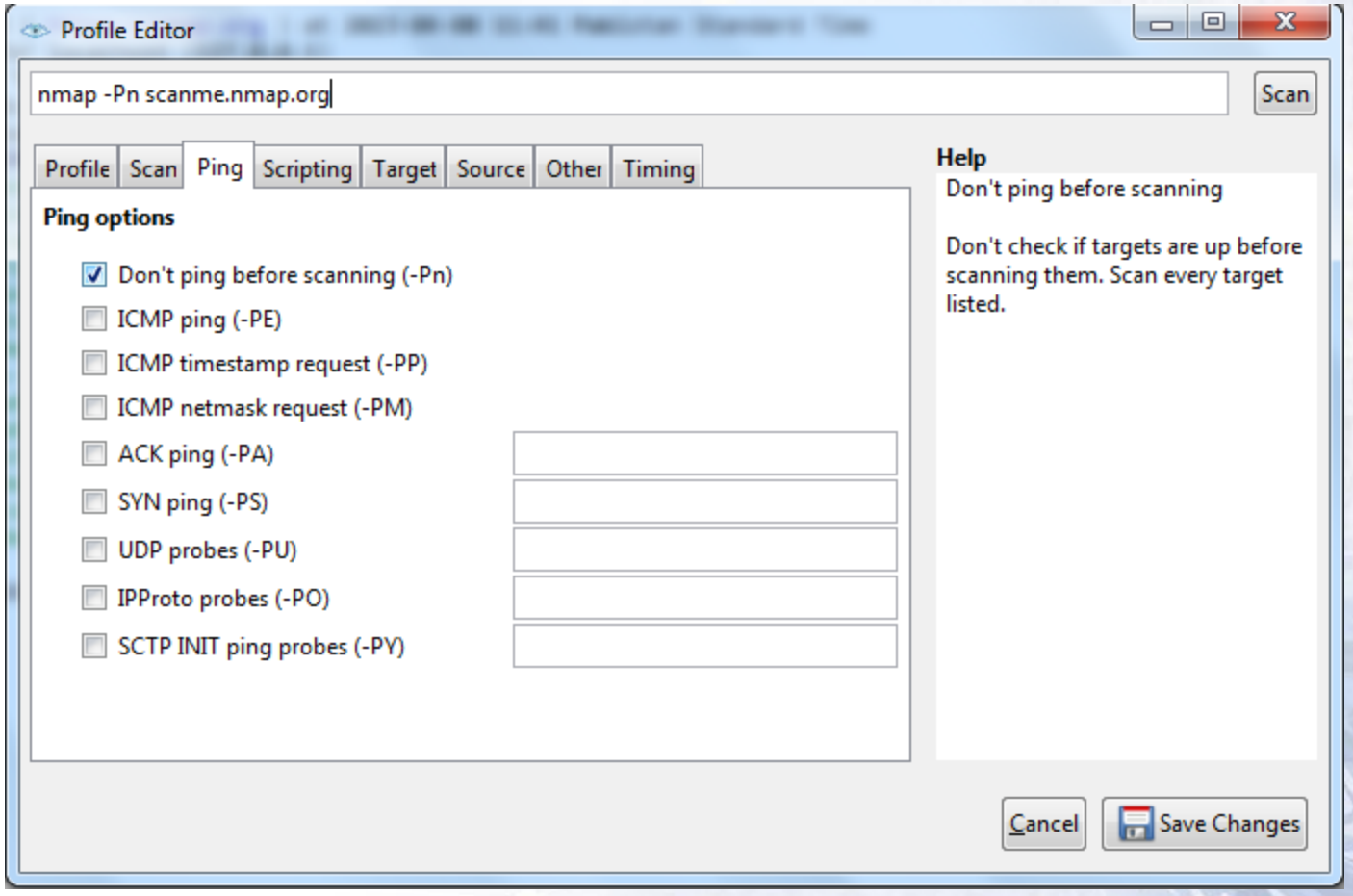
```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-08 16:59 Pakistan Standard Time
Nmap scan report for localhost (127.0.0.1)
Failed to resolve "nmap".
Host is up (0.00015s latency).
Not shown: 91 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

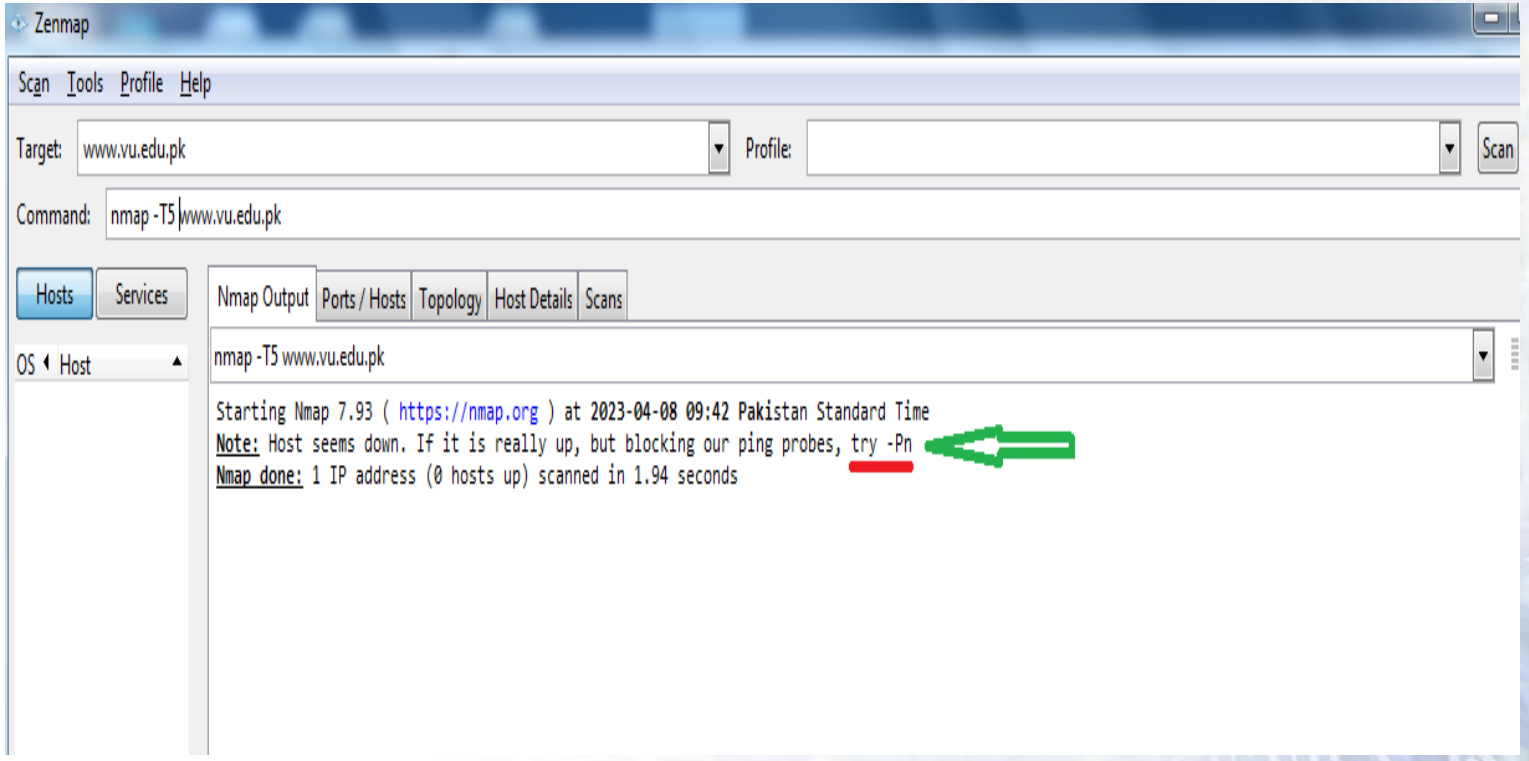
Nmap done: 1 IP address
```



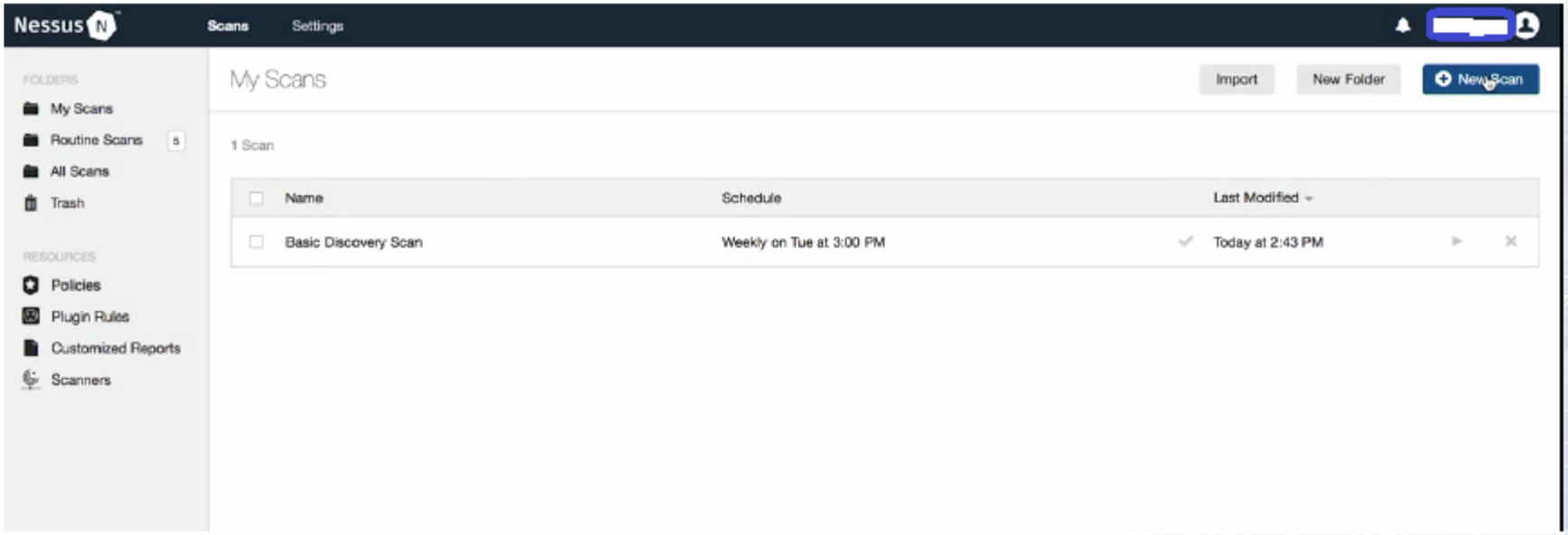

Zenmap
Scan Tools Profile Help
Target: scanme.nmap.org
Profile: Quick scan
Scan
Command: nmap -T4 -F scanme.nmap.org
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -F scanme.nmap.org
OS Host
scanme.nmap.org
localhost (127.0.0.1)
Starting Nmap 7.93
Nmap scan report f
Host is up (0.32s
Not shown: 99 filt
PORT STATE SERVI
80/tcp open http
Nmap done: 1 IP ad
Profile Editor
nmap -T4 -F scanme.nmap.org
Scan
Profile Scan Ping Scripting Target Source Other Timing
Profile Information
Profile name lead scan
Description
Help
Profile name
This is how the profile will be identified in the drop-down combo box in the scan tab.

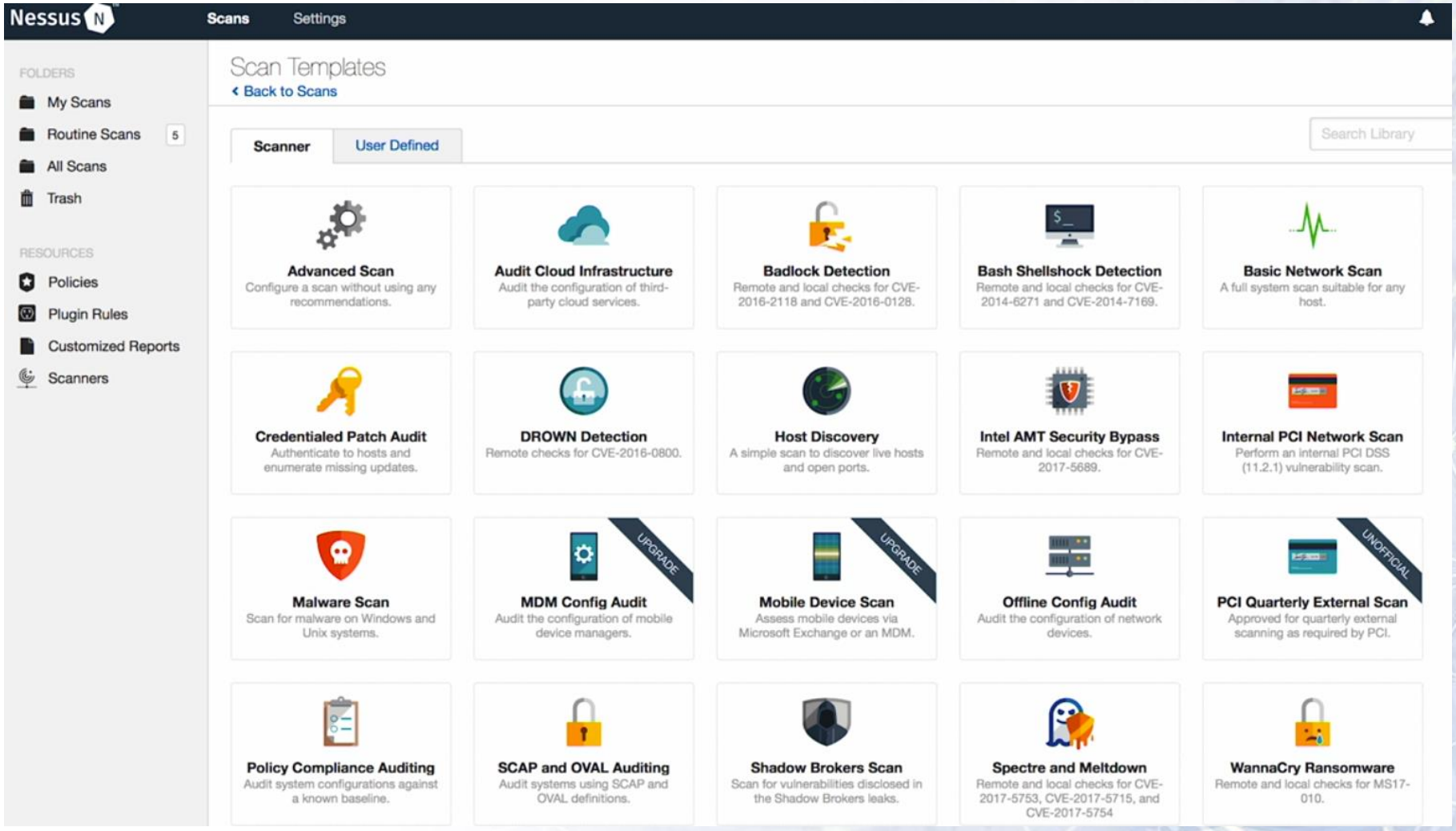

Profile Editor
nmap -sV -6 -T4 -O -F scanme.nmap.org
Scan
Profile
Scan
Ping
Scripting
Target
Source
Other
Timing
Scan options
Targets (optional):
scanme.nmap.org
TCP scan:
None
Non-TCP scans:
None
Timing template:
Aggressive (-T4)
Enable all advanced/aggressive options (-A)
Operating system detection (-O)
Version detection (-sV)
Idle Scan (Zombie) (-sI)
FTP bounce attack (-b)
Disable reverse DNS resolution (-n)
IPv6 support (-6)
Help
Enable all advanced/aggressive options
Enable OS detection (-O), version detection (-sV), script scanning (-sC), and traceroute (--traceroute).
Cancel
Save Changes

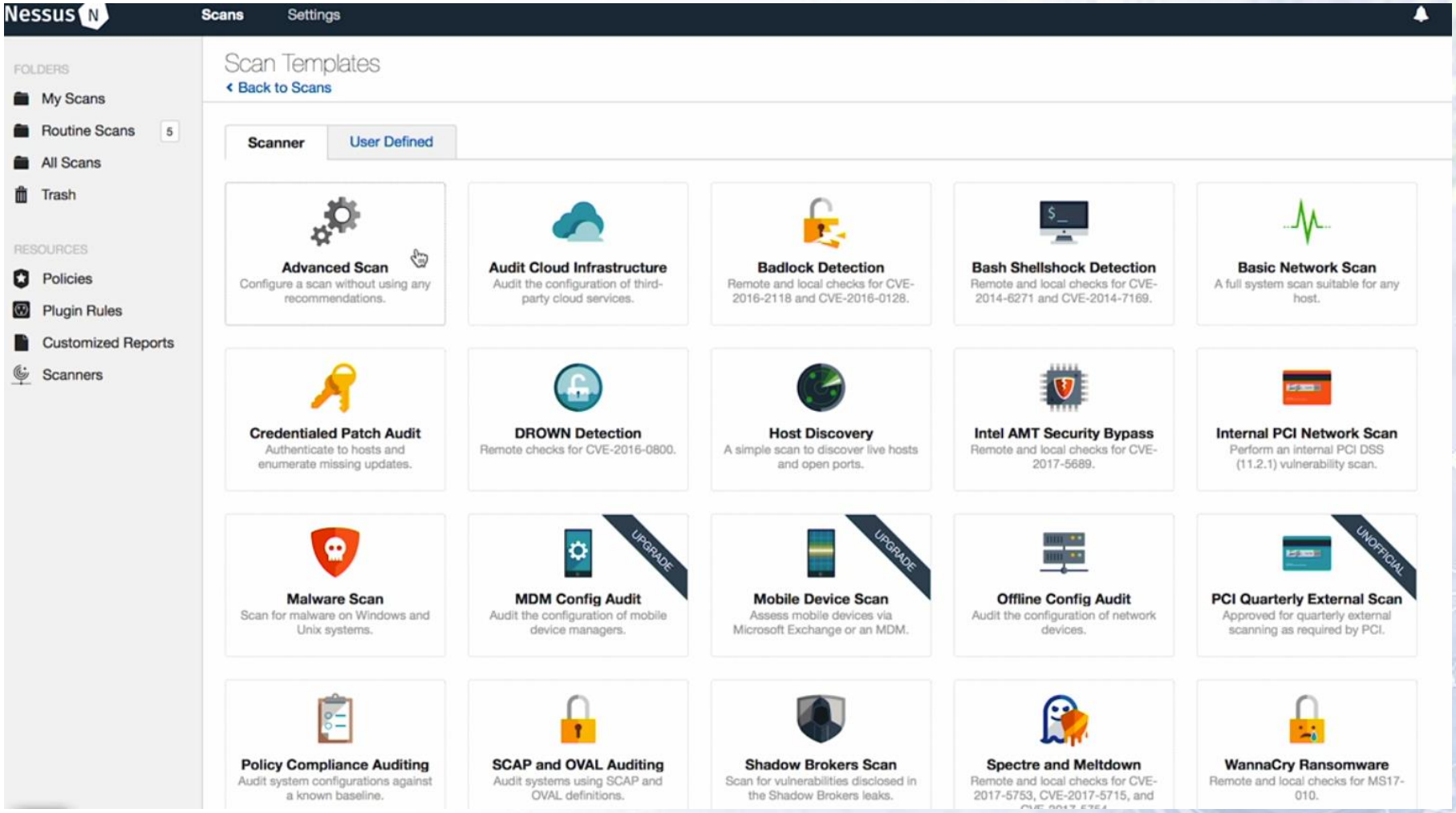

Profile Editor
nmap -Pn scanme.nmap.org
Scan
Profile
Scan
Ping
Scripting
Target
Source
Other
Timing
Ping options
Don't ping before scanning (-Pn)
ICMP ping (-PE)
ICMP timestamp request (-PP)
ICMP netmask request (-PM)
ACK ping (-PA)
SYN ping (-PS)
UDP probes (-PU)
IPProto probes (-PO)
SCTP INIT ping probes (-PY)
Help
Don't ping before scanning
Don't check if targets are up before scanning them. Scan every target listed.
Cancel
Save Changes

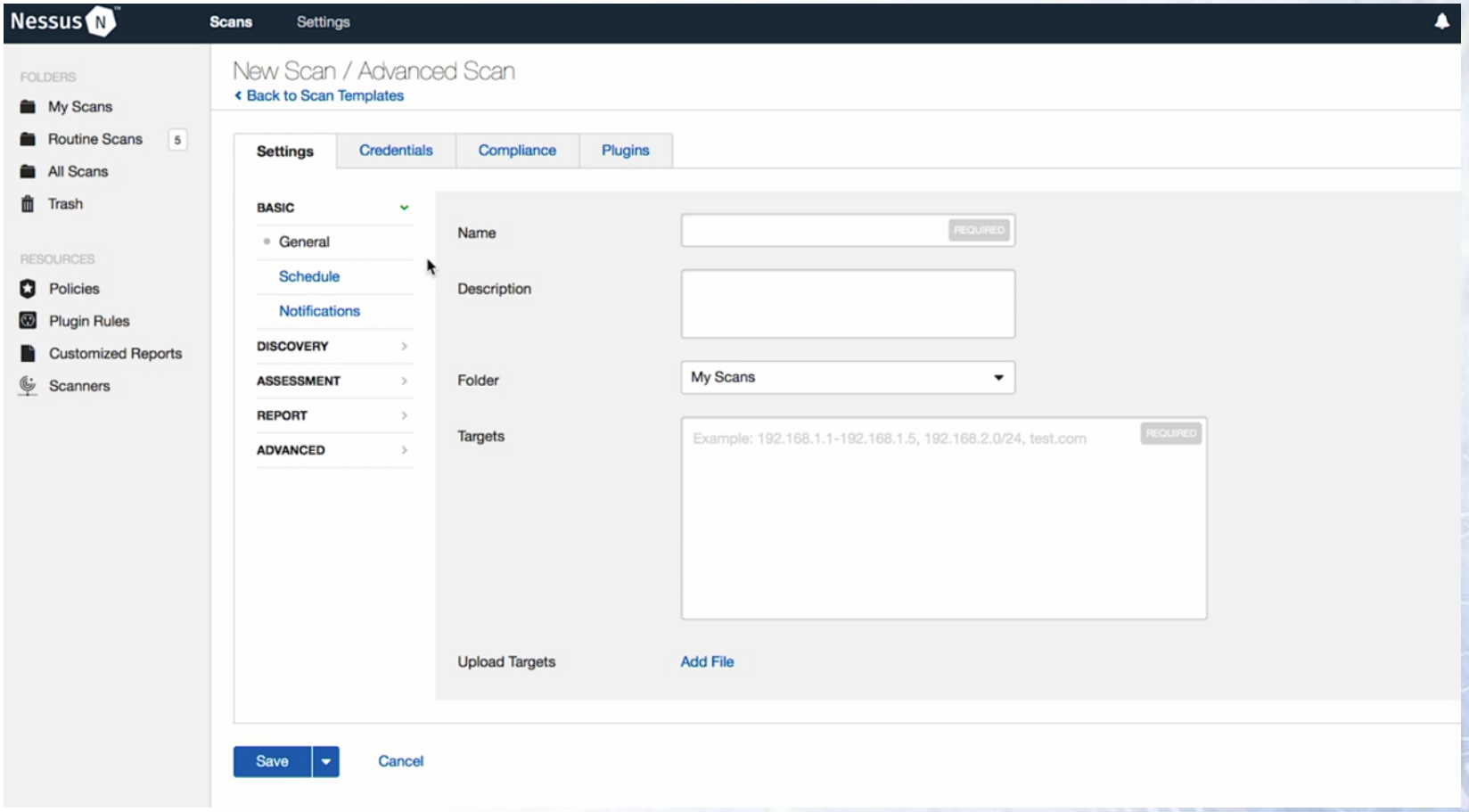

Zenmap
Scan Tools Profile Help
Target: www.vu.edu.pk
Profile:
Scan
Command: nmap -T5 www.vu.edu.pk
Hosts
Services
OS Host
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T5 www.vu.edu.pk
Starting Nmap 7.93 (https://nmap.org) at 2023-04-08 09:42 Pakistan Standard Time
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.94 seconds

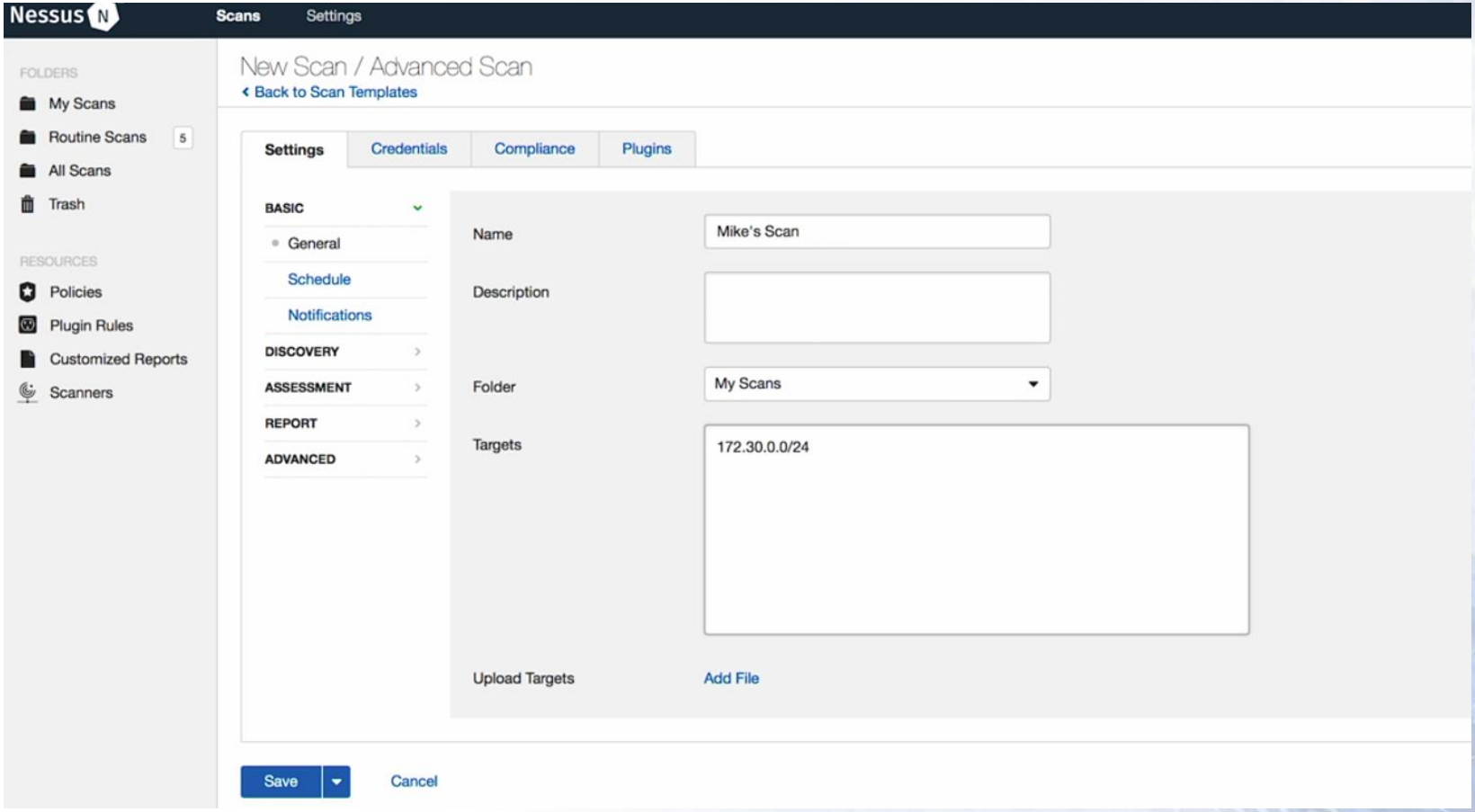
Nessus New scan

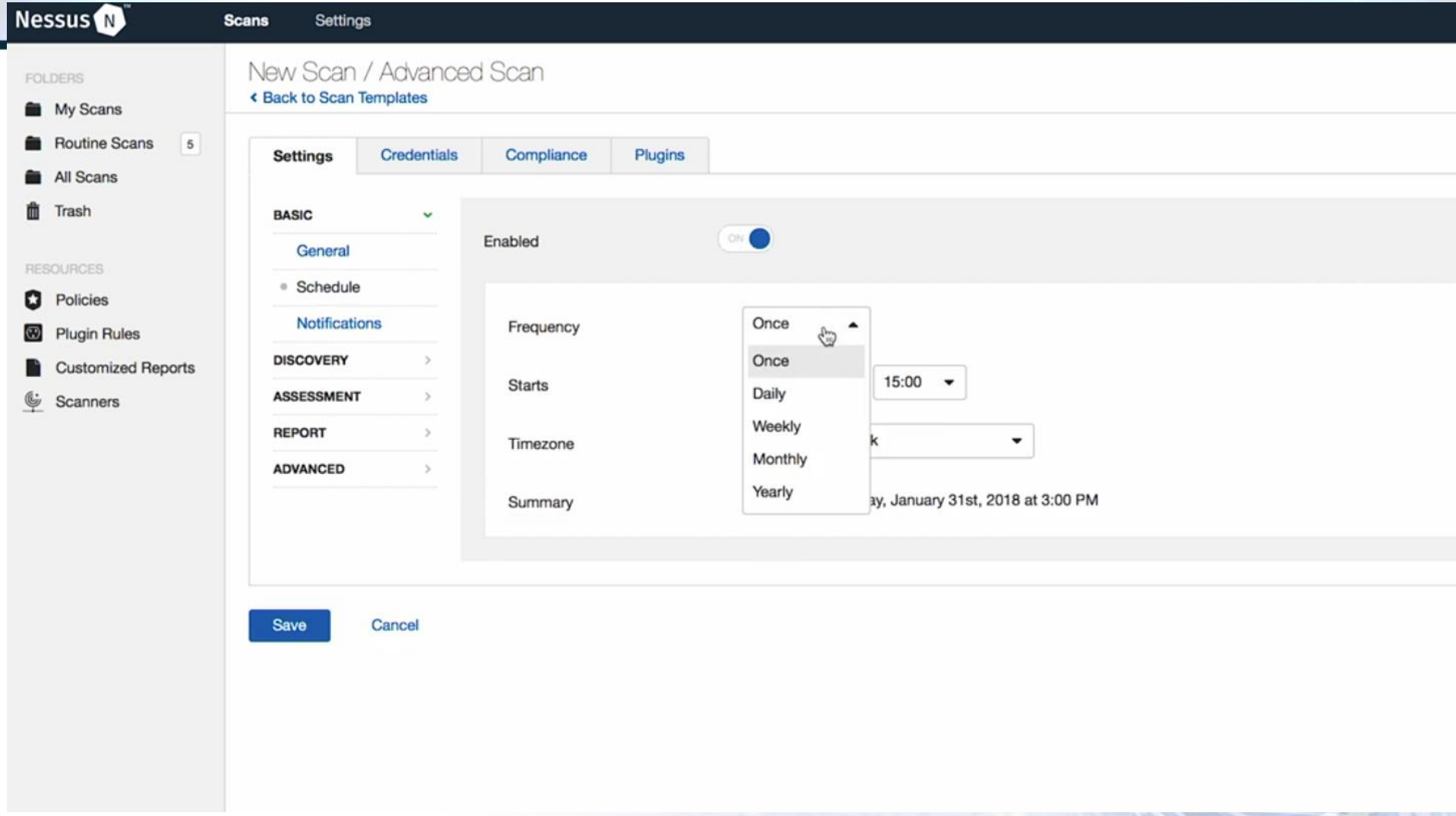

Nessus
Scans
Settings
FOLDERS
My Scans
Routine Scans
5
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
My Scans
Import
New Folder
New Scan
1 Scan
Name
Schedule
Last Modified
Basic Discovery Scan
Weekly on Tue at 3:00 PM
Today at 2:43 PM

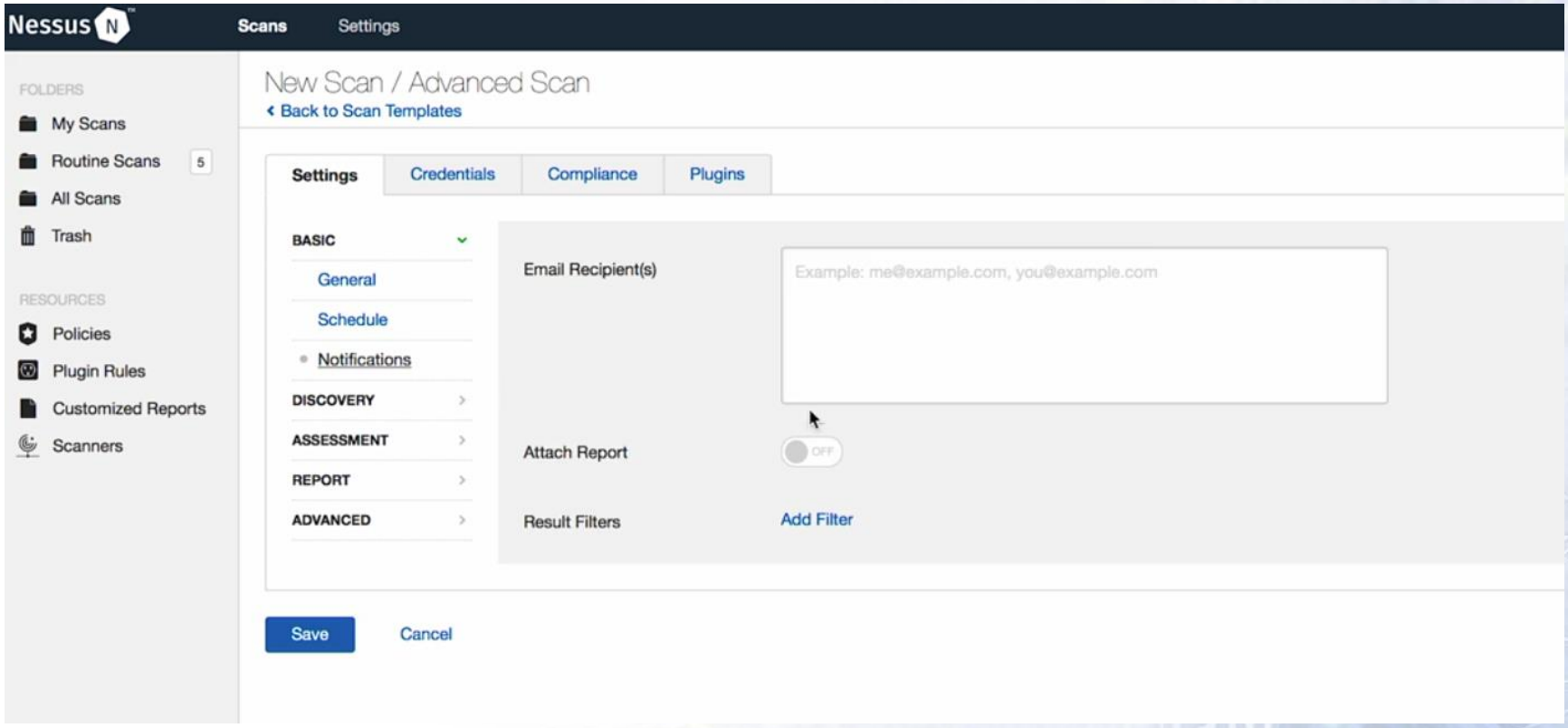

Nessus
Scans
Settings
FOLDERS
My Scans
Routine Scans
5
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
Scan Templates
Back to Scans
Scanner
User Defined
Search Library
Advanced Scan
Configure a scan without using any recommendations.
Audit Cloud Infrastructure
Audit the configuration of third-party cloud services.
Badlock Detection
Remote and local checks for CVE-2016-2118 and CVE-2016-0128.
Bash Shellshock Detection
Remote and local checks for CVE-2014-6271 and CVE-2014-7169.
Basic Network Scan
A full system scan suitable for any host.
Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.
DROWN Detection
Remote checks for CVE-2016-0800.
Host Discovery
A simple scan to discover live hosts and open ports.
Intel AMT Security Bypass
Remote and local checks for CVE-2017-5689.
Internal PCI Network Scan
Perform an internal PCI DSS (11.2.1) vulnerability scan.
Malware Scan
Scan for malware on Windows and Unix systems.
UPGRADE
MDM Config Audit
Audit the configuration of mobile device managers.
UPGRADE
Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.
Offline Config Audit
Audit the configuration of network devices.
UNOFFICIAL
PCI Quarterly External Scan
Approved for quarterly external scanning as required by PCI.
Policy Compliance Auditing
Audit system configurations against a known baseline.
SCAP and OVAL Auditing
Audit systems using SCAP and OVAL definitions.
Shadow Brokers Scan
Scan for vulnerabilities disclosed in the Shadow Brokers leaks.
Spectre and Meltdown
Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754
WannaCry Ransomware
Remote and local checks for MS17-010.

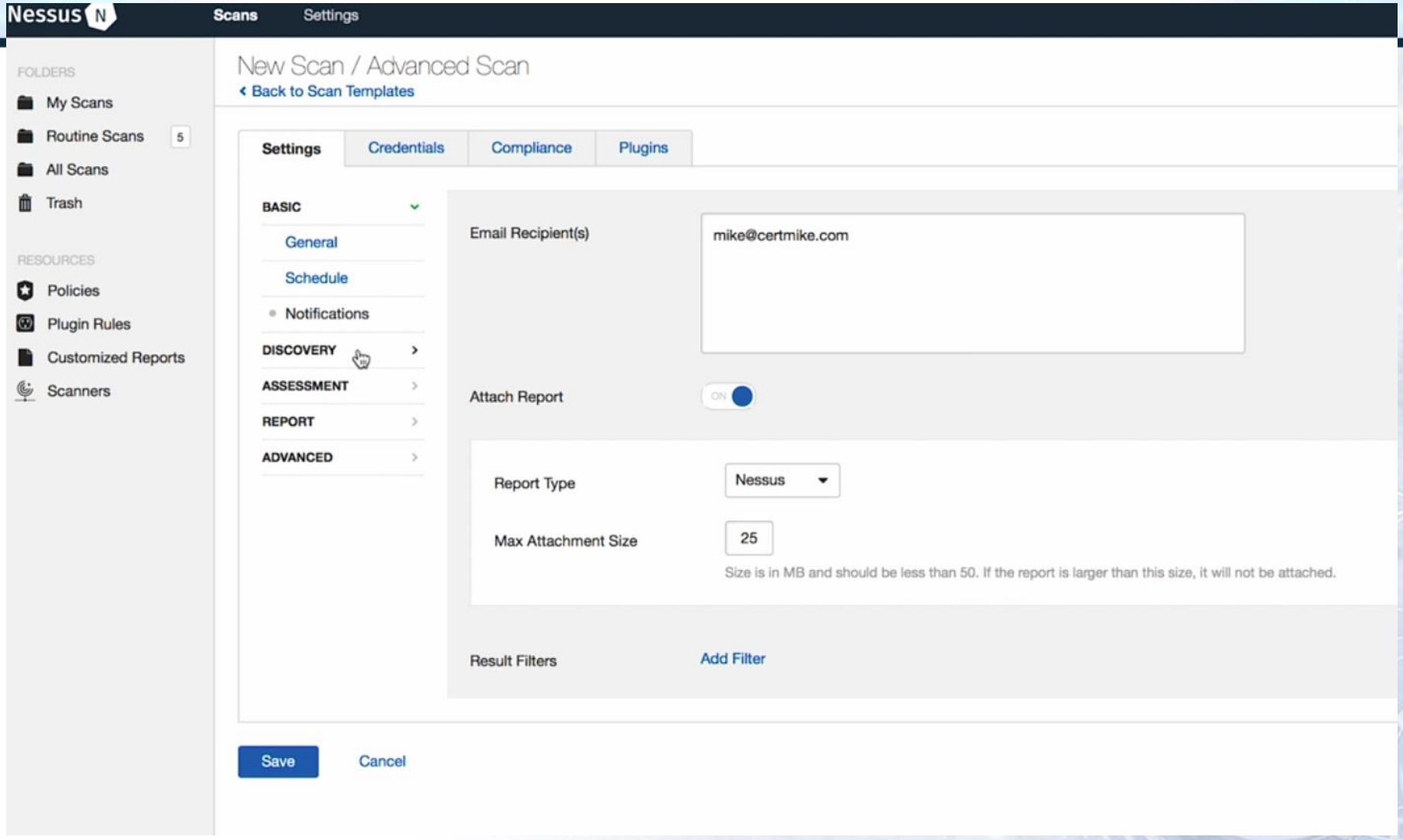

Nessus
Scans
Settings
FOLDERS
My Scans
Routine Scans
5
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
Scan Templates
Back to Scans
Scanner
User Defined
Advanced Scan
Configure a scan without using any recommendations.
Audit Cloud Infrastructure
Audit the configuration of third-party cloud services.
Badlock Detection
Remote and local checks for CVE-2016-2118 and CVE-2016-0128.
Bash Shellshock Detection
Remote and local checks for CVE-2014-6271 and CVE-2014-7169.
Basic Network Scan
A full system scan suitable for any host.
Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.
DROWN Detection
Remote checks for CVE-2016-0800.
Host Discovery
A simple scan to discover live hosts and open ports.
Intel AMT Security Bypass
Remote and local checks for CVE-2017-5689.
Internal PCI Network Scan
Perform an internal PCI DSS (11.2.1) vulnerability scan.
Malware Scan
Scan for malware on Windows and Unix systems.
MDM Config Audit
Audit the configuration of mobile device managers.
UPGRADE
Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.
UPGRADE
Offline Config Audit
Audit the configuration of network devices.
PCI Quarterly External Scan
Approved for quarterly external scanning as required by PCI.
UNOFFICIAL
Policy Compliance Auditing
Audit system configurations against a known baseline.
SCAP and OVAL Auditing
Audit systems using SCAP and OVAL definitions.
Shadow Brokers Scan
Scan for vulnerabilities disclosed in the Shadow Brokers leaks.
Spectre and Meltdown
Remote and local checks for CVE-2017-5753, CVE-2017-5715, and
WannaCry Ransomware
Remote and local checks for MS17-010.

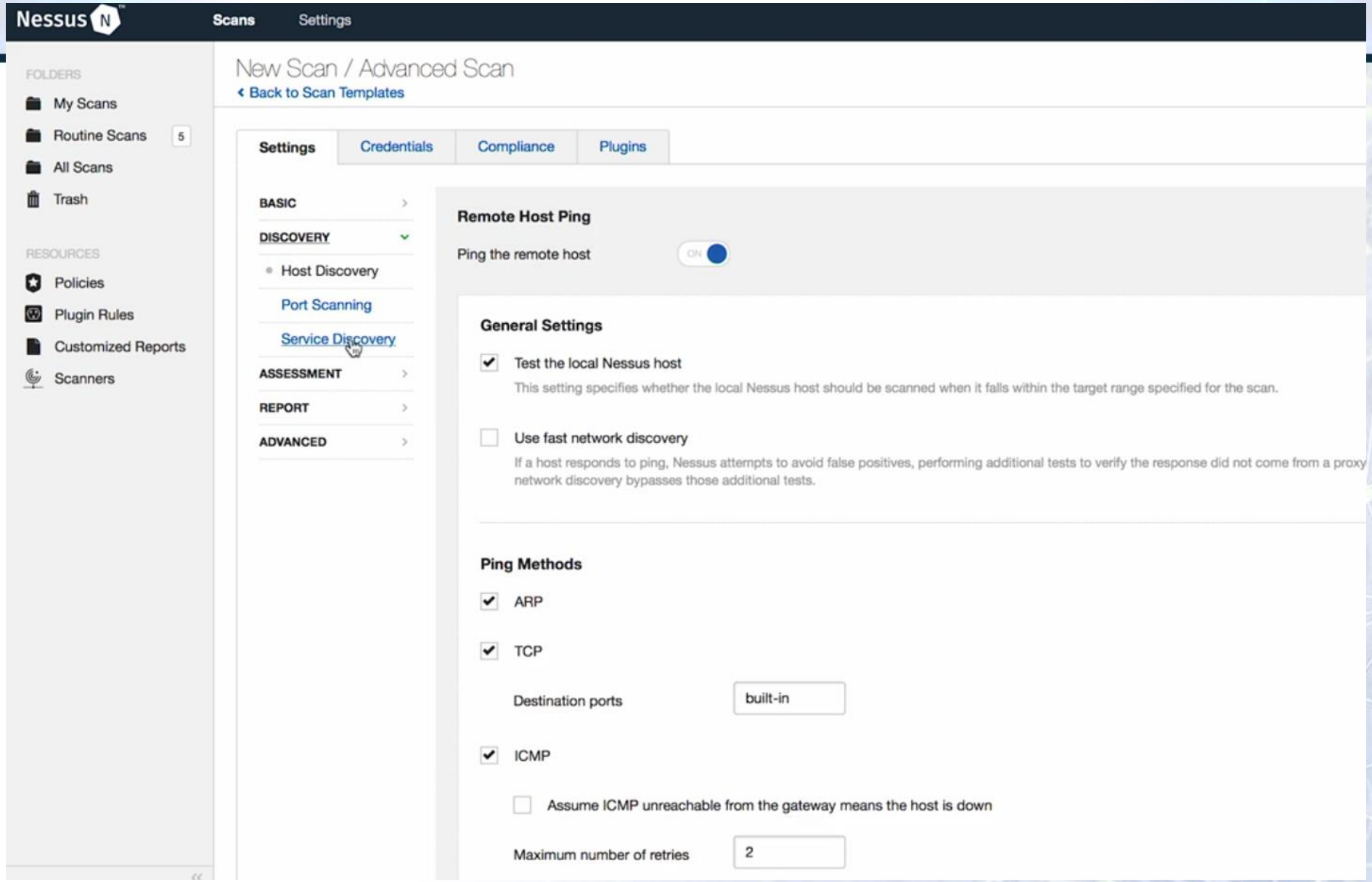

Nessus
Scans
Settings
FOLDERS
My Scans
Routine Scans
5
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
New Scan / Advanced Scan
Back to Scan Templates
Settings
Credentials
Compliance
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
REQUIRED
Description
Folder
My Scans
Targets
Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com
REQUIRED
Upload Targets
Add File
Save
Cancel

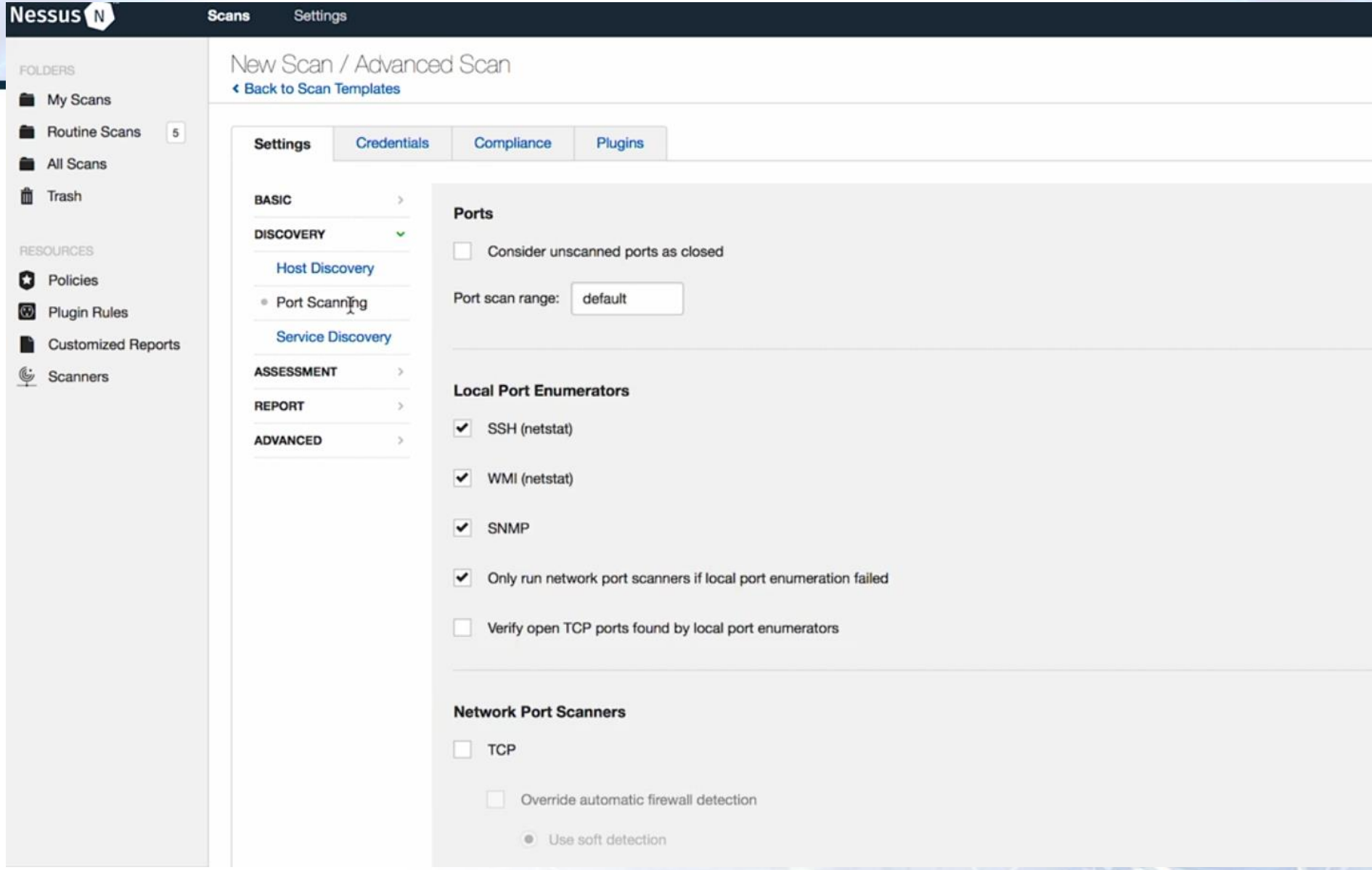

Nessus
Scans
Settings
FOLDERS
My Scans
Routine Scans
5
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
New Scan / Advanced Scan
Back to Scan Templates
Settings
Credentials
Compliance
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
Mike's Scan
Description
Folder
My Scans
Targets
172.30.0.0/24
Upload Targets
Add File
Save
Cancel

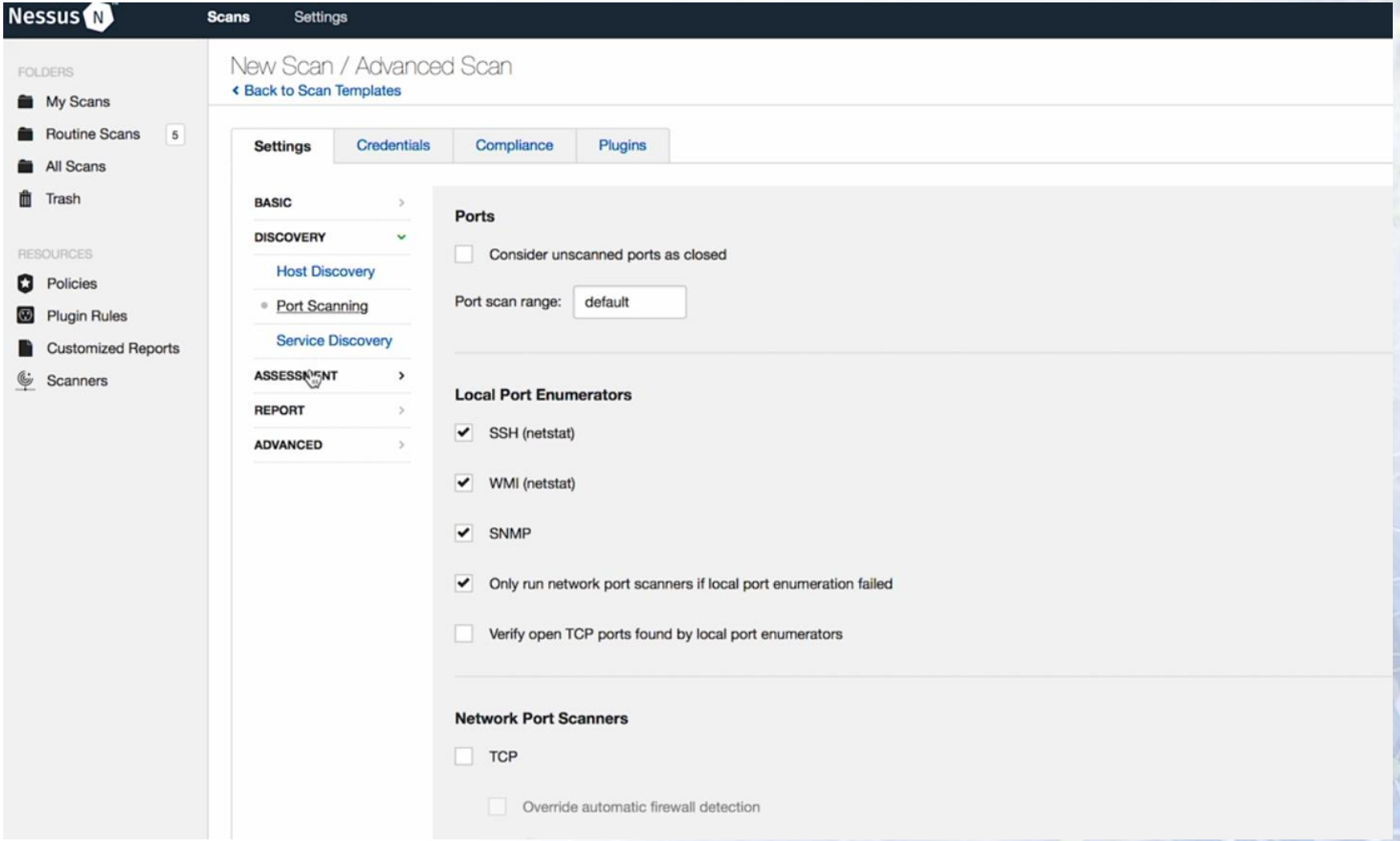

Nessus
Scans
Settings
FOLDERS
My Scans
Routine Scans
5
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
New Scan / Advanced Scan
Back to Scan Templates
Settings
Credentials
Compliance
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Enabled
ON
Frequency
Once
Once
Daily
Weekly
Monthly
Yearly
Starts
15:00
Timezone
Summary
ay, January 31st, 2018 at 3:00 PM
Save
Cancel

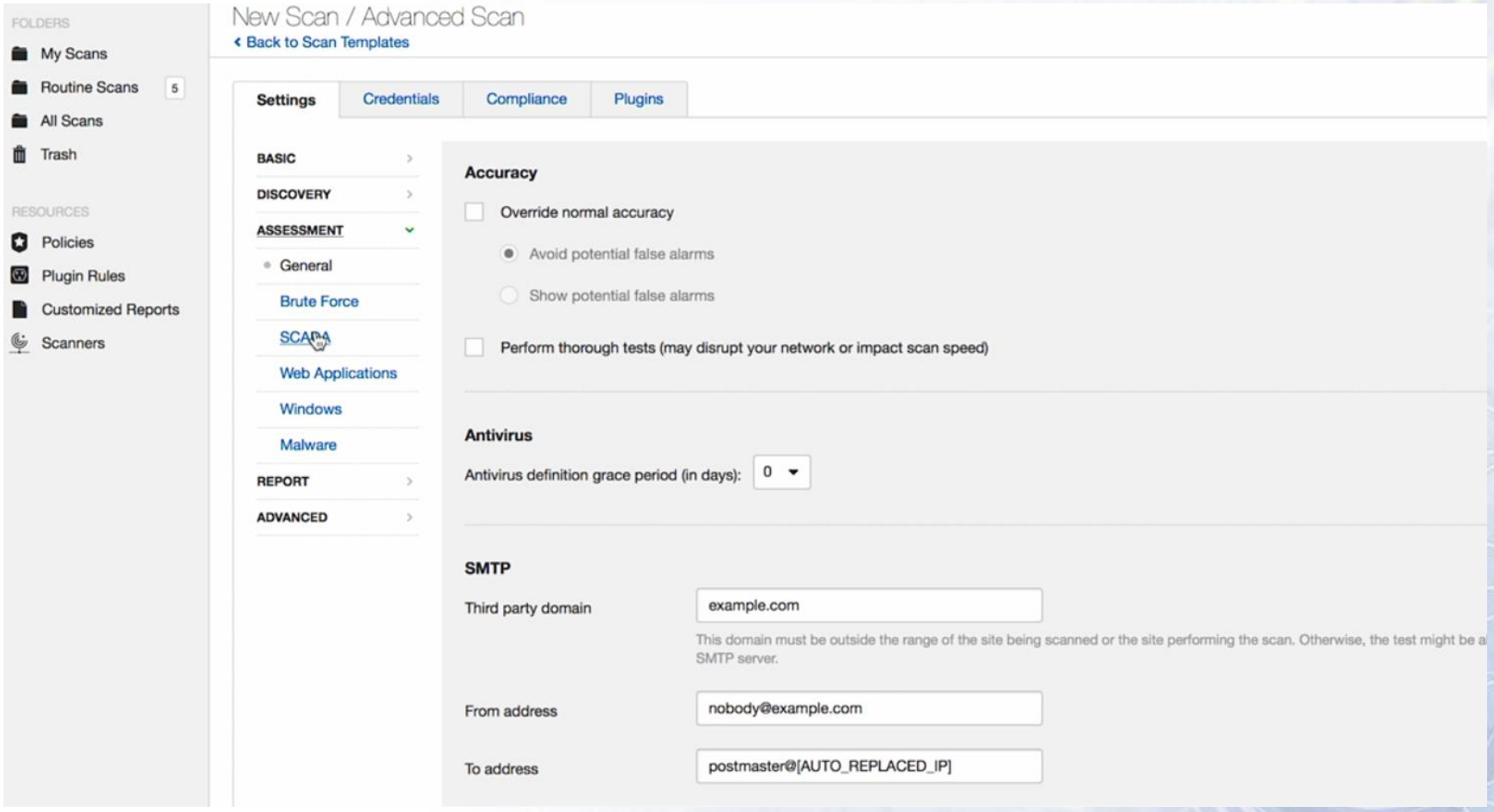

Nessus
Scans
Settings
FOLDERS
My Scans
Routine Scans
5
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
New Scan / Advanced Scan
Back to Scan Templates
Settings
Credentials
Compliance
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Email Recipient(s)
Example: me@example.com, you@example.com
Attach Report
OFF
Result Filters
Add Filter
Save
Cancel

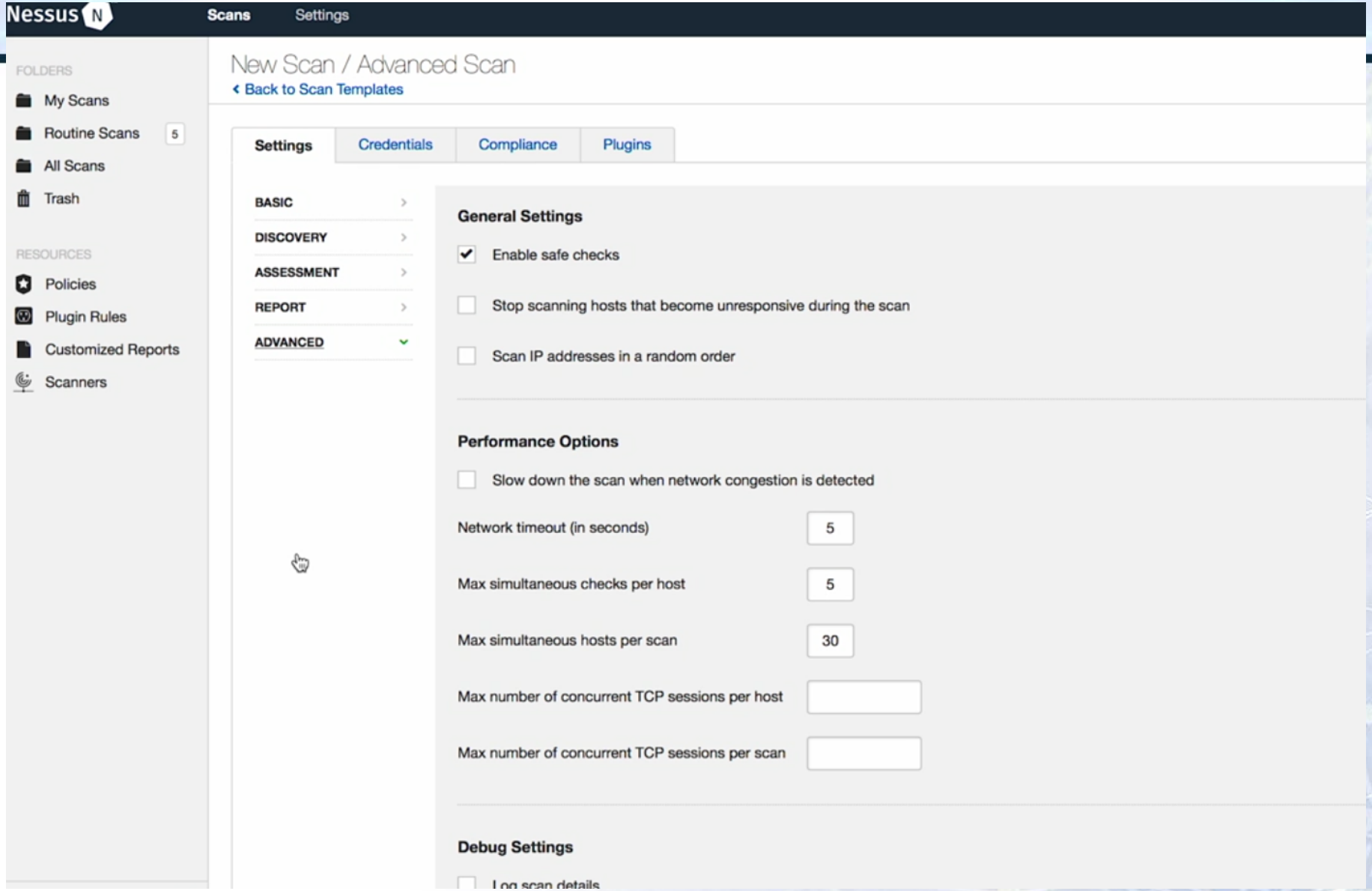

Nessus
Scans
Settings
FOLDERS
My Scans
Routine Scans
5
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
New Scan / Advanced Scan
Back to Scan Templates
Settings
Credentials
Compliance
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Email Recipient(s)
mike@certmike.com
Attach Report
ON
Report Type
Nessus
Max Attachment Size
25
Size is in MB and should be less than 50. If the report is larger than this size, it will not be attached.
Result Filters
Add Filter
Save
Cancel

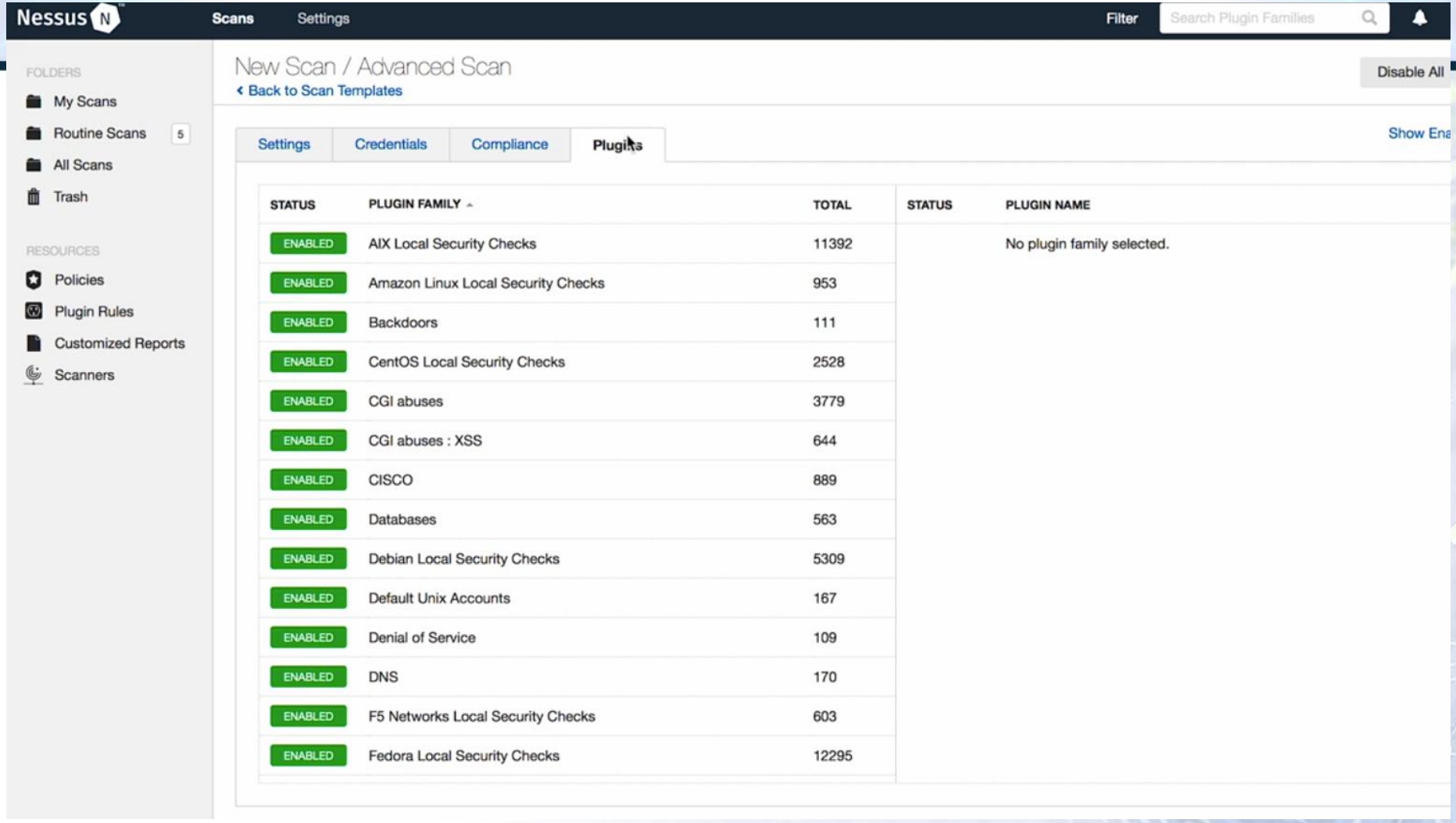

Nessus
Scans
Settings
FOLDERS
My Scans
Routine Scans
5
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
New Scan / Advanced Scan
Back to Scan Templates
Settings
Credentials
Compliance
Plugins
BASIC
DISCOVERY
Host Discovery
Port Scanning
Service Discovery
ASSESSMENT
REPORT
ADVANCED
Remote Host Ping
Ping the remote host
ON
General Settings
Test the local Nessus host
This setting specifies whether the local Nessus host should be scanned when it falls within the target range specified for the scan.
Use fast network discovery
If a host responds to ping, Nessus attempts to avoid false positives, performing additional tests to verify the response did not come from a proxy network discovery bypasses those additional tests.
Ping Methods
ARP
TCP
Destination ports
built-in
ICMP
Assume ICMP unreachable from the gateway means the host is down
Maximum number of retries
2

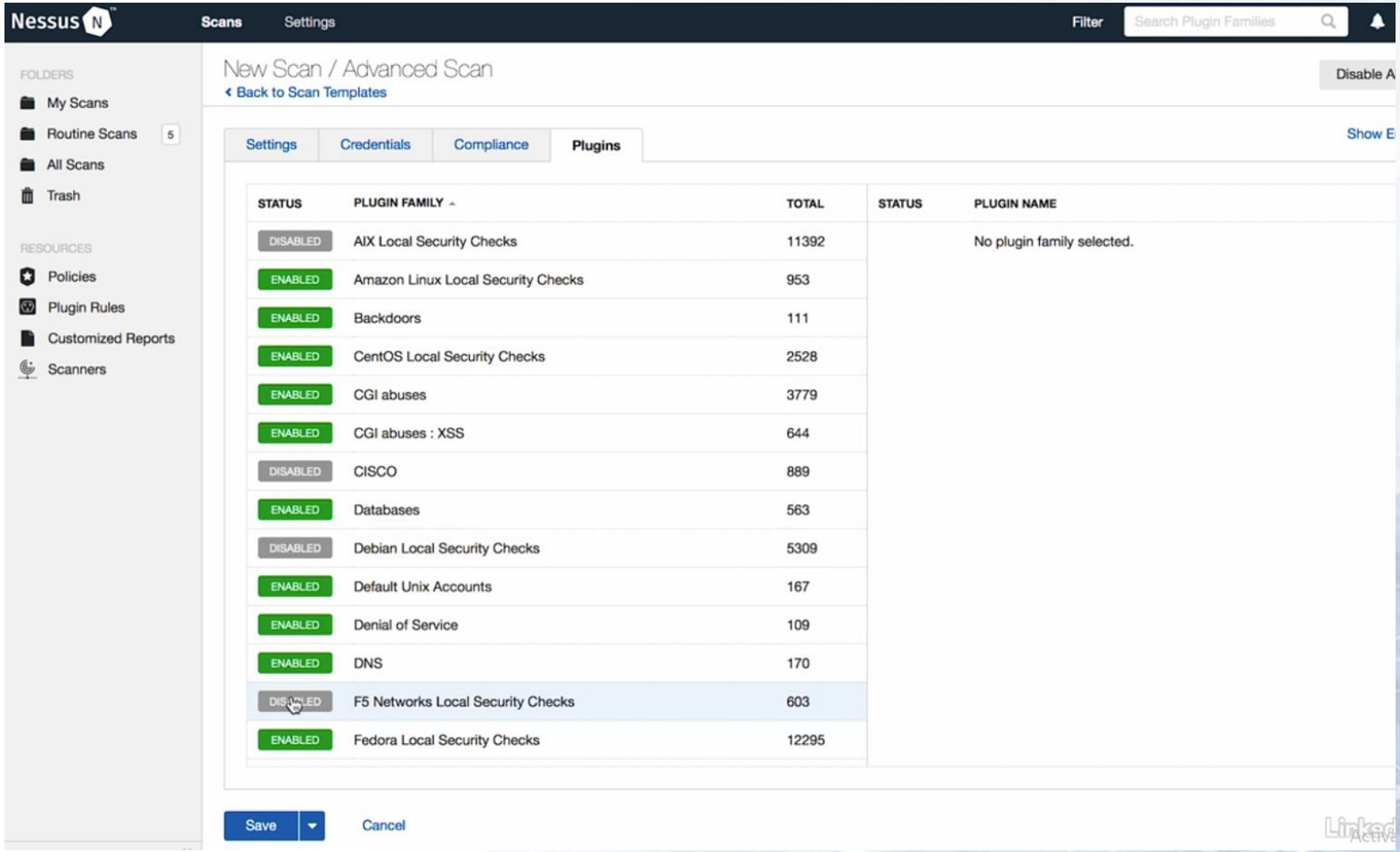

Nessus
Scans
Settings
FOLDERS
My Scans
Routine Scans
5
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
New Scan / Advanced Scan
Back to Scan Templates
Settings
Credentials
Compliance
Plugins
BASIC
DISCOVERY
Host Discovery
Port Scanning
Service Discovery
ASSESSMENT
REPORT
ADVANCED
Ports
Consider unscanned ports as closed
Port scan range:
default
Local Port Enumerators
SSH (netstat)
WMI (netstat)
SNMP
Only run network port scanners if local port enumeration failed
Verify open TCP ports found by local port enumerators
Network Port Scanners
TCP
Override automatic firewall detection
Use soft detection

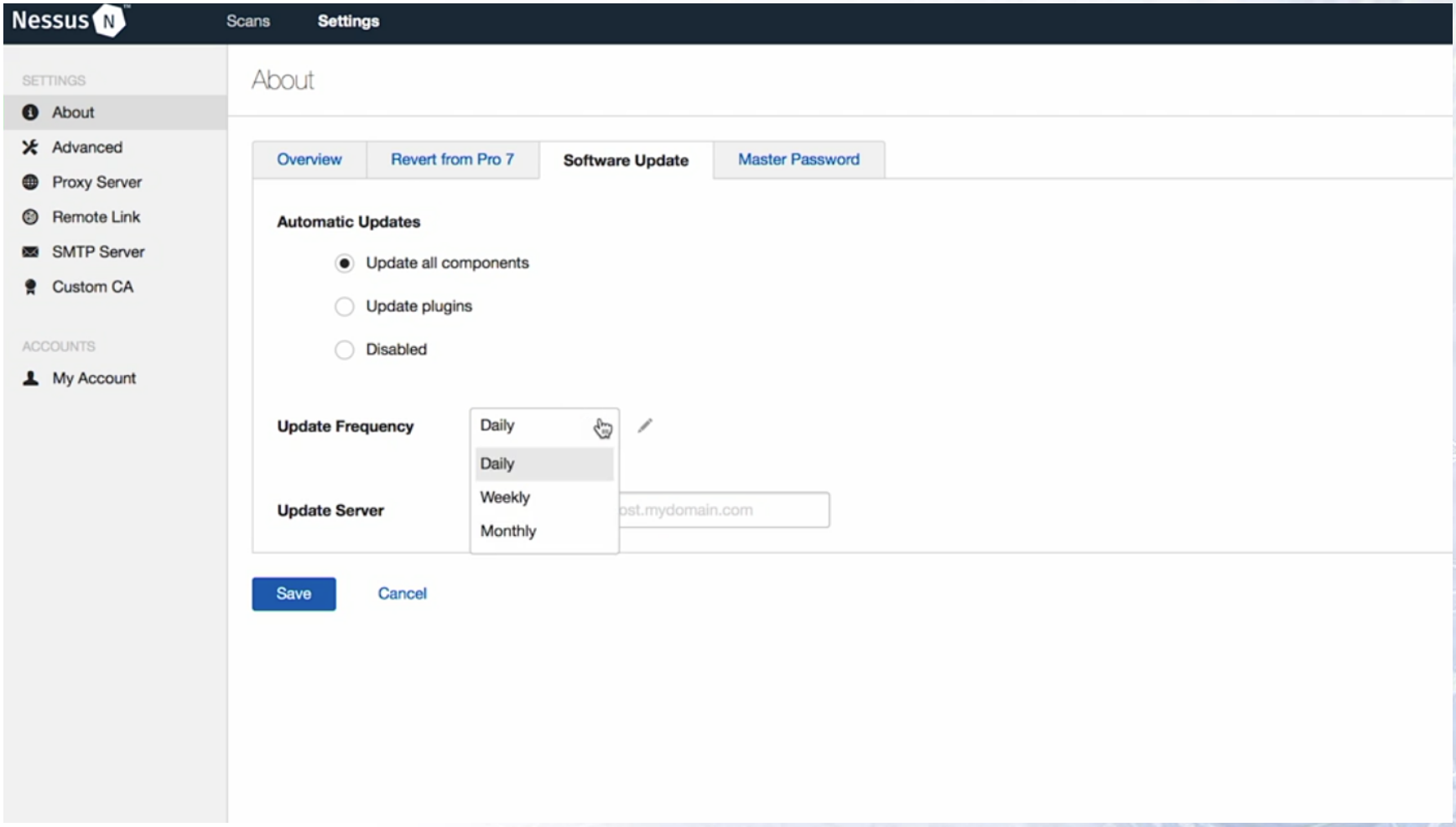

Nessus
Scans
Settings
FOLDERS
My Scans
Routine Scans
5
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
New Scan / Advanced Scan
Back to Scan Templates
Settings
Credentials
Compliance
Plugins
BASIC
DISCOVERY
Host Discovery
Port Scanning
Service Discovery
ASSESSMENT
REPORT
ADVANCED
Ports
Consider unscanned ports as closed
Port scan range:
default
Local Port Enumerators
SSH (netstat)
WMI (netstat)
SNMP
Only run network port scanners if local port enumeration failed
Verify open TCP ports found by local port enumerators
Network Port Scanners
TCP
Override automatic firewall detection


FOLDERS
My Scans
Routine Scans 5
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
New Scan / Advanced Scan
Back to Scan Templates
Settings
Credentials
Compliance
Plugins
BASIC
DISCOVERY
ASSESSMENT
General
Brute Force
SCADA
Web Applications
Windows
Malware
REPORT
ADVANCED
Accuracy
Override normal accuracy
Avoid potential false alarms
Show potential false alarms
Perform thorough tests (may disrupt your network or impact scan speed)
Antivirus
Antivirus definition grace period (in days): 0
SMTP
Third party domain
example.com
This domain must be outside the range of the site being scanned or the site performing the scan. Otherwise, the test might be a
SMTP server.
From address
nobody@example.com
To address
postmaster@[AUTO_REPLACED_IP]


Nessus
Scans
Settings
FOLDERS
My Scans
Routine Scans
5
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
New Scan / Advanced Scan
Back to Scan Templates
Settings
Credentials
Compliance
Plugins
BASIC
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
General Settings
Enable safe checks
Stop scanning hosts that become unresponsive during the scan
Scan IP addresses in a random order
Performance Options
Slow down the scan when network congestion is detected
Network timeout (in seconds)
5
Max simultaneous checks per host
5
Max simultaneous hosts per scan
30
Max number of concurrent TCP sessions per host
Max number of concurrent TCP sessions per scan
Debug Settings
Log scan details


Nessus
Scans
Settings
Filter
Search Plugin Families
FOLDERS
My Scans
Routine Scans 5
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
New Scan / Advanced Scan
Back to Scan Templates
Disable All
Settings
Credentials
Compliance
Plugins
Show Ena
STATUS
PLUGIN FAMILY
TOTAL
STATUS
PLUGIN NAME
ENABLED AIX Local Security Checks 11392
ENABLED Amazon Linux Local Security Checks 953
ENABLED Backdoors 111
ENABLED CentOS Local Security Checks 2528
ENABLED CGI abuses 3779
ENABLED CGI abuses : XSS 644
ENABLED CISCO 889
ENABLED Databases 563
ENABLED Debian Local Security Checks 5309
ENABLED Default Unix Accounts 167
ENABLED Denial of Service 109
ENABLED DNS 170
ENABLED F5 Networks Local Security Checks 603
ENABLED Fedora Local Security Checks 12295
No plugin family selected.


Nessus
Scans
Settings
Filter
Search Plugin Families
FOLDERS
My Scans
Routine Scans 5
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
New Scan / Advanced Scan
Back to Scan Templates
Disable A
Settings
Credentials
Compliance
Plugins
Show E
STATUS
PLUGIN FAMILY
TOTAL
STATUS
PLUGIN NAME
DISABLED AIX Local Security Checks 11392
ENABLED Amazon Linux Local Security Checks 953
ENABLED Backdoors 111
ENABLED CentOS Local Security Checks 2528
ENABLED CGI abuses 3779
ENABLED CGI abuses : XSS 644
DISABLED CISCO 889
ENABLED Databases 563
DISABLED Debian Local Security Checks 5309
ENABLED Default Unix Accounts 167
ENABLED Denial of Service 109
ENABLED DNS 170
DISABLED F5 Networks Local Security Checks 603
ENABLED Fedora Local Security Checks 12295
No plugin family selected.
Save
Cancel


Nessus
Scans
Settings
SETTINGS
About
Advanced
Proxy Server
Remote Link
SMTP Server
Custom CA
ACCOUNTS
My Account
About
Overview
Revert from Pro 7
Software Update
Master Password
Automatic Updates
Update all components
Update plugins
Disabled
Update Frequency
Daily
Daily
Weekly
Monthly
Update Server
st.mydomain.com
Save
Cancel

Nessus Demo - 1

- Lets take a look at Nessus Demo
- https://www.tenable.com/products/nessus/nessus-professional/evaluate
- Download free 7 day trial
- Get activation key from website

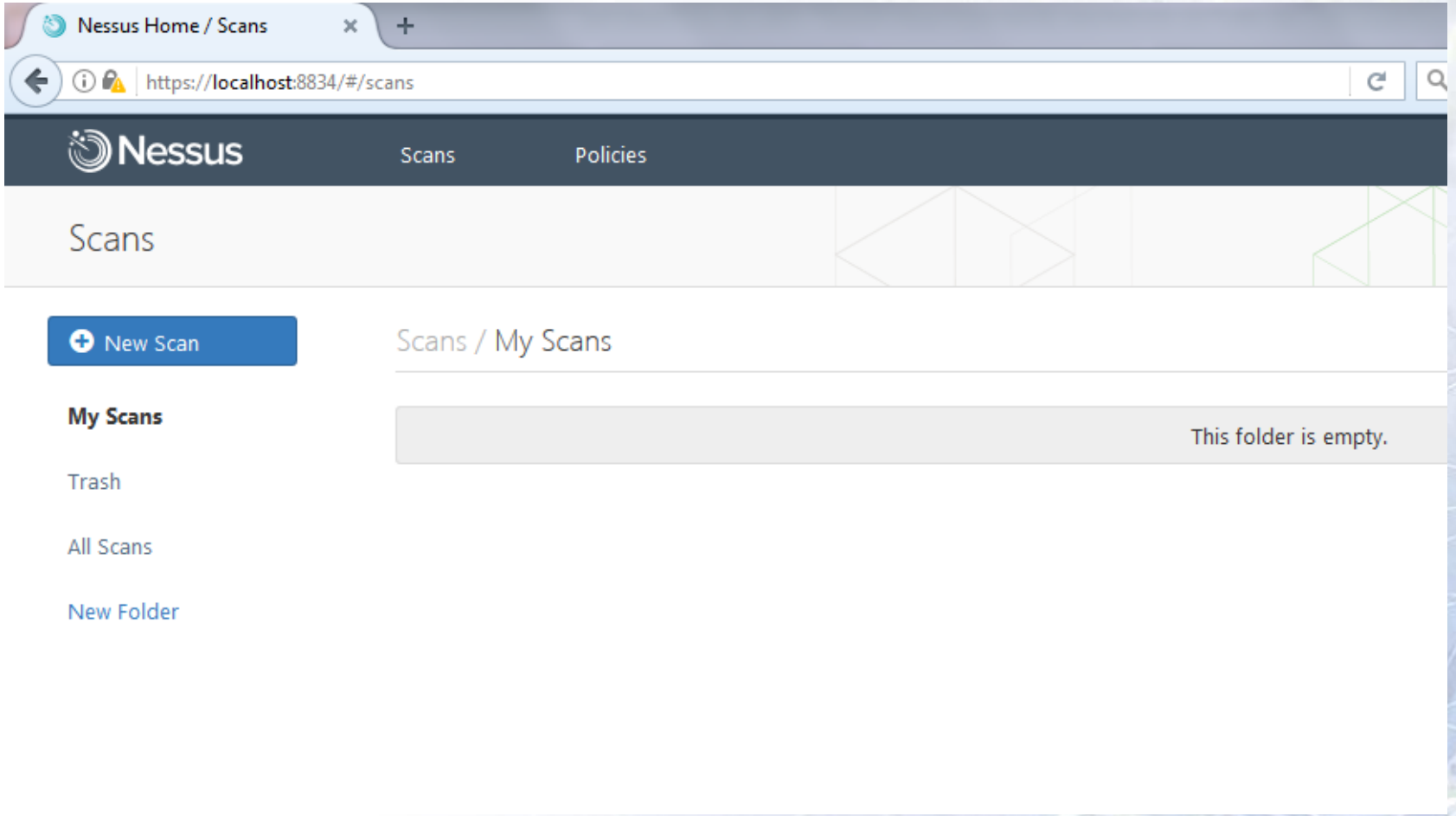
Nessus Demo - 1

LOGIN SCREEN



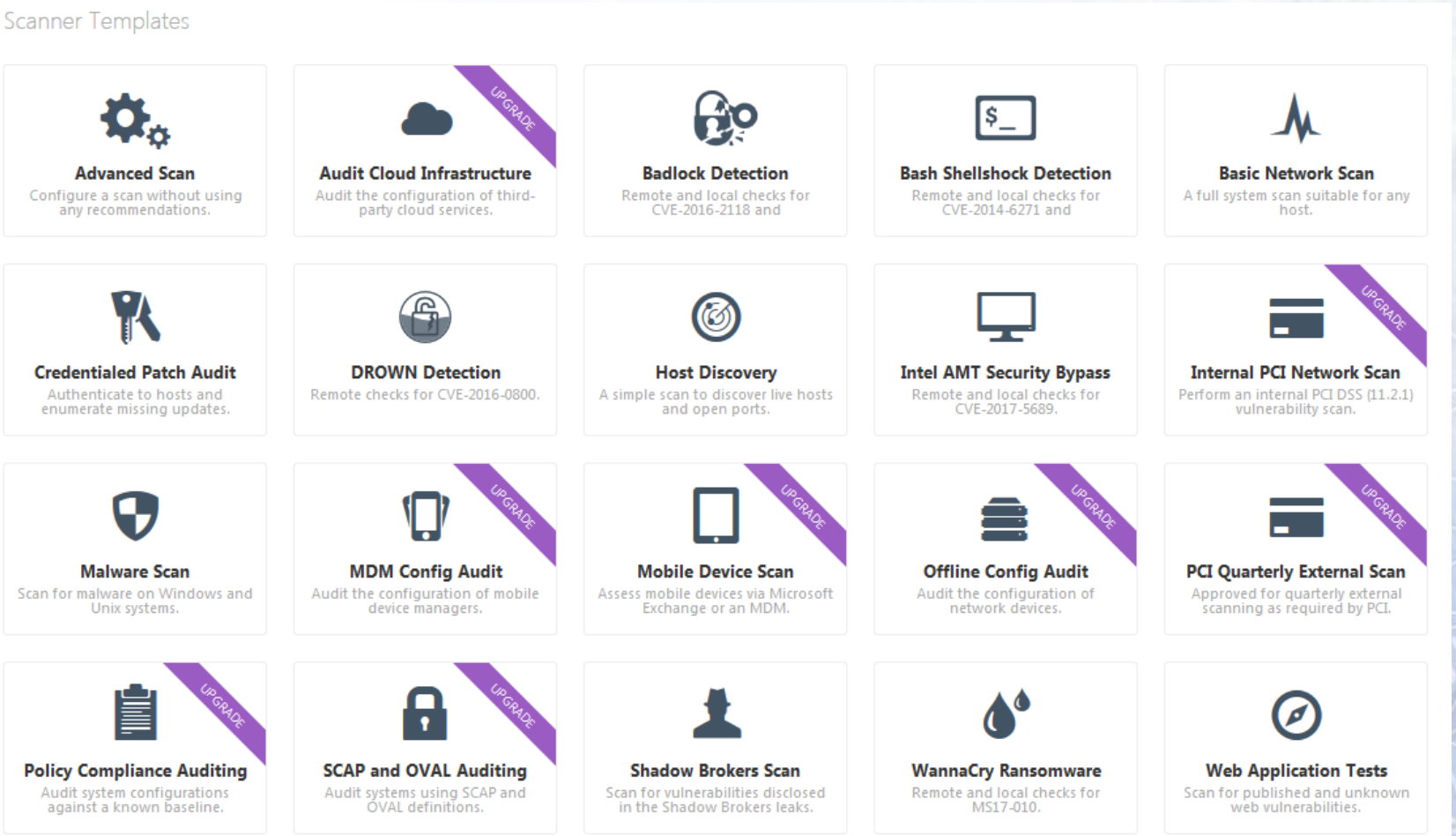
Nessus Demo - 1

DASHBOARD



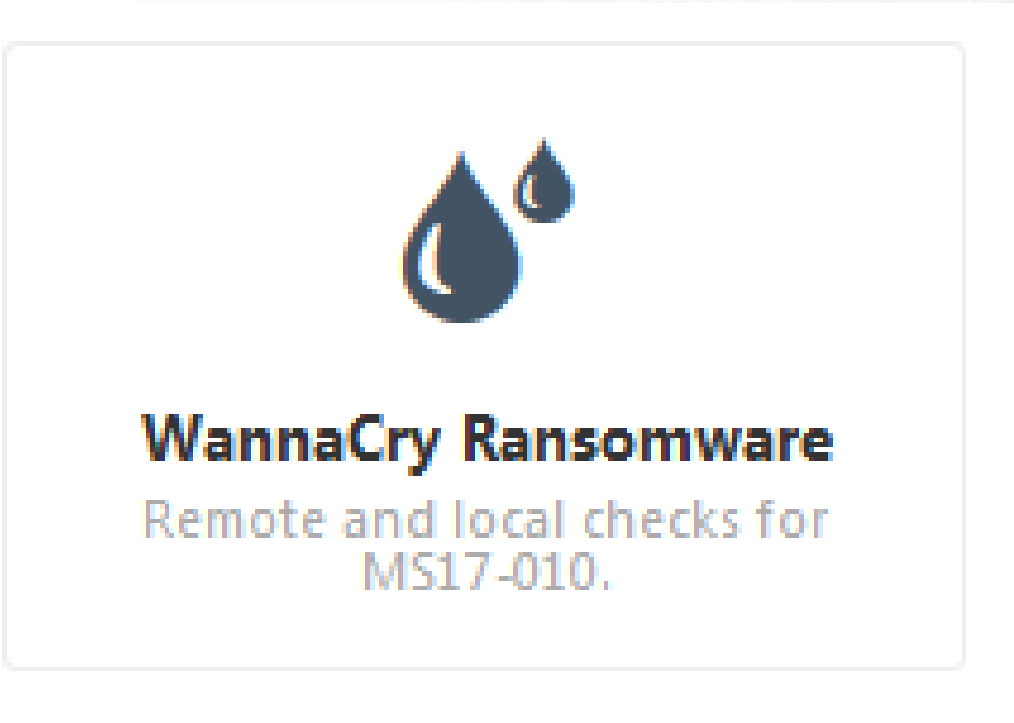
Nessus Demo - 1

NEW SCAN



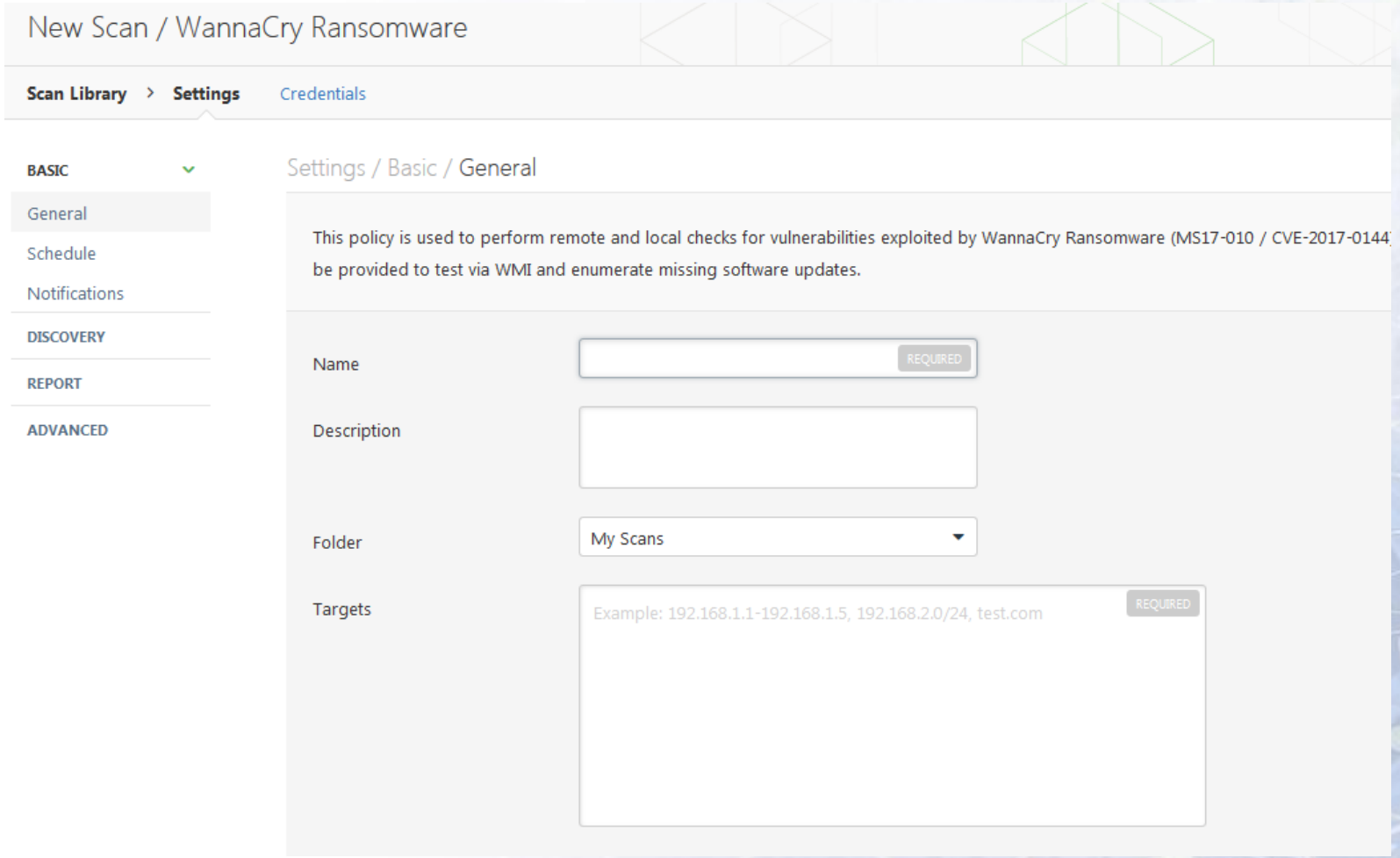
Nessus Demo - 1

WANNACRY RANSOMWARE SCAN



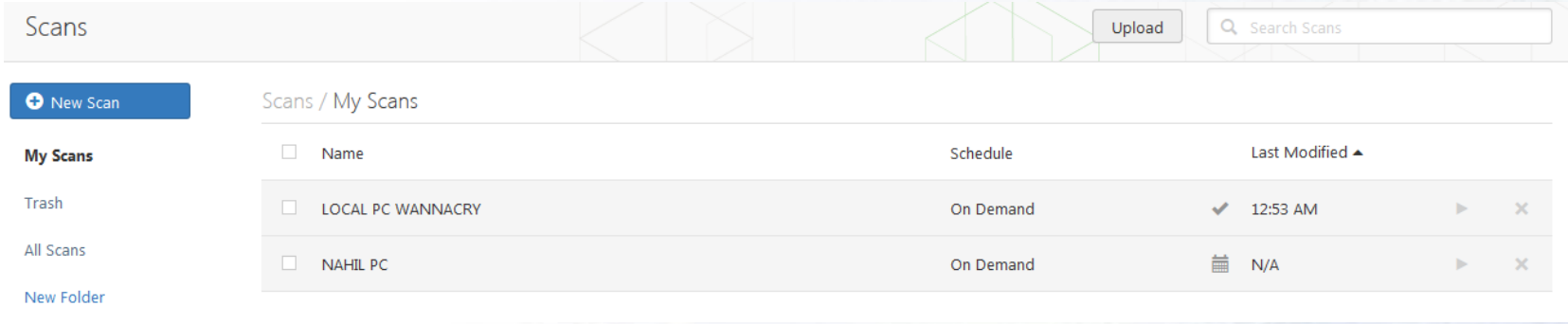
Nessus Demo - 1

NEW SCAN WINDOW



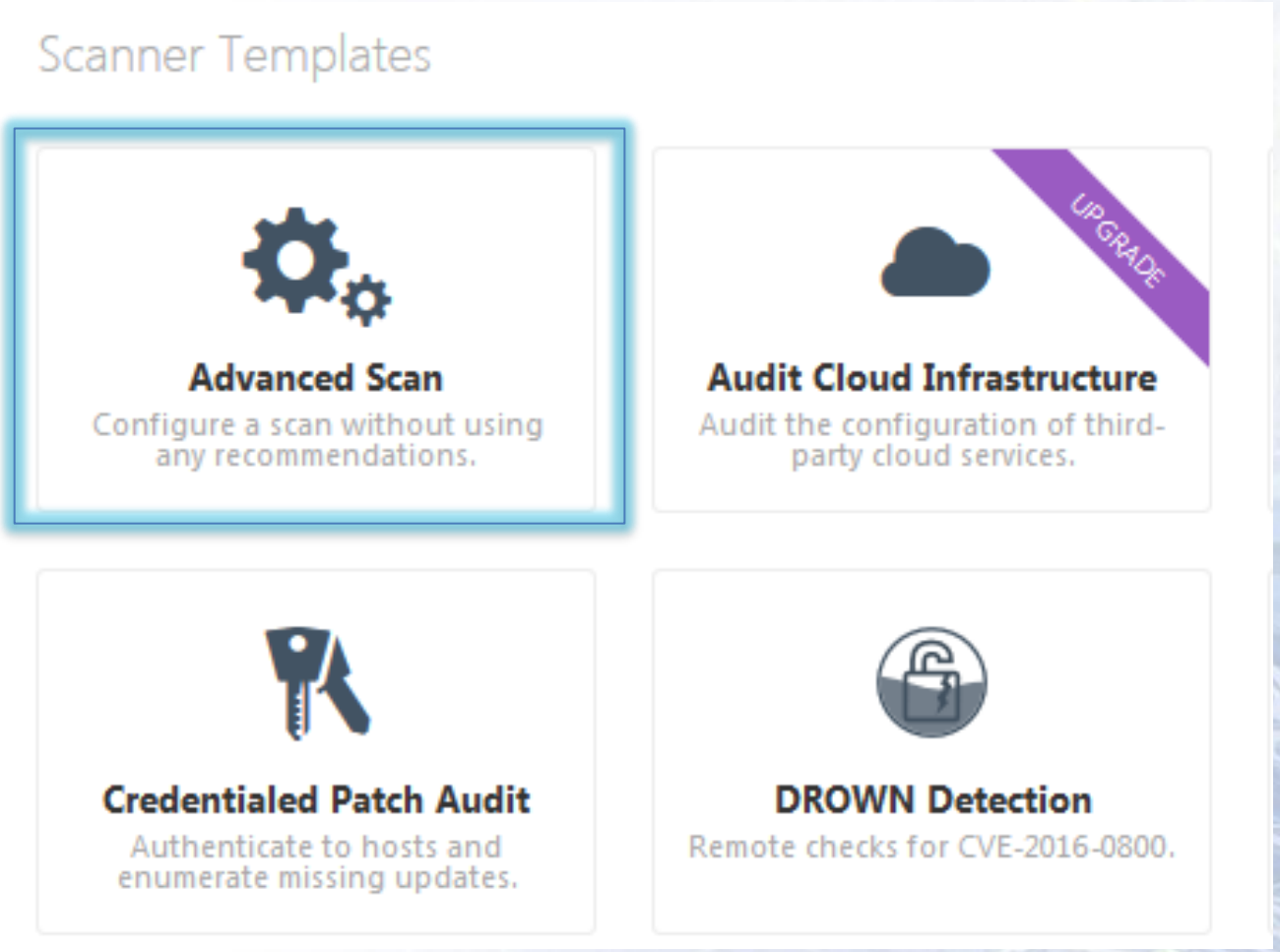
Nessus Demo - 1

DASHBOARD VIEW WITH SCANS



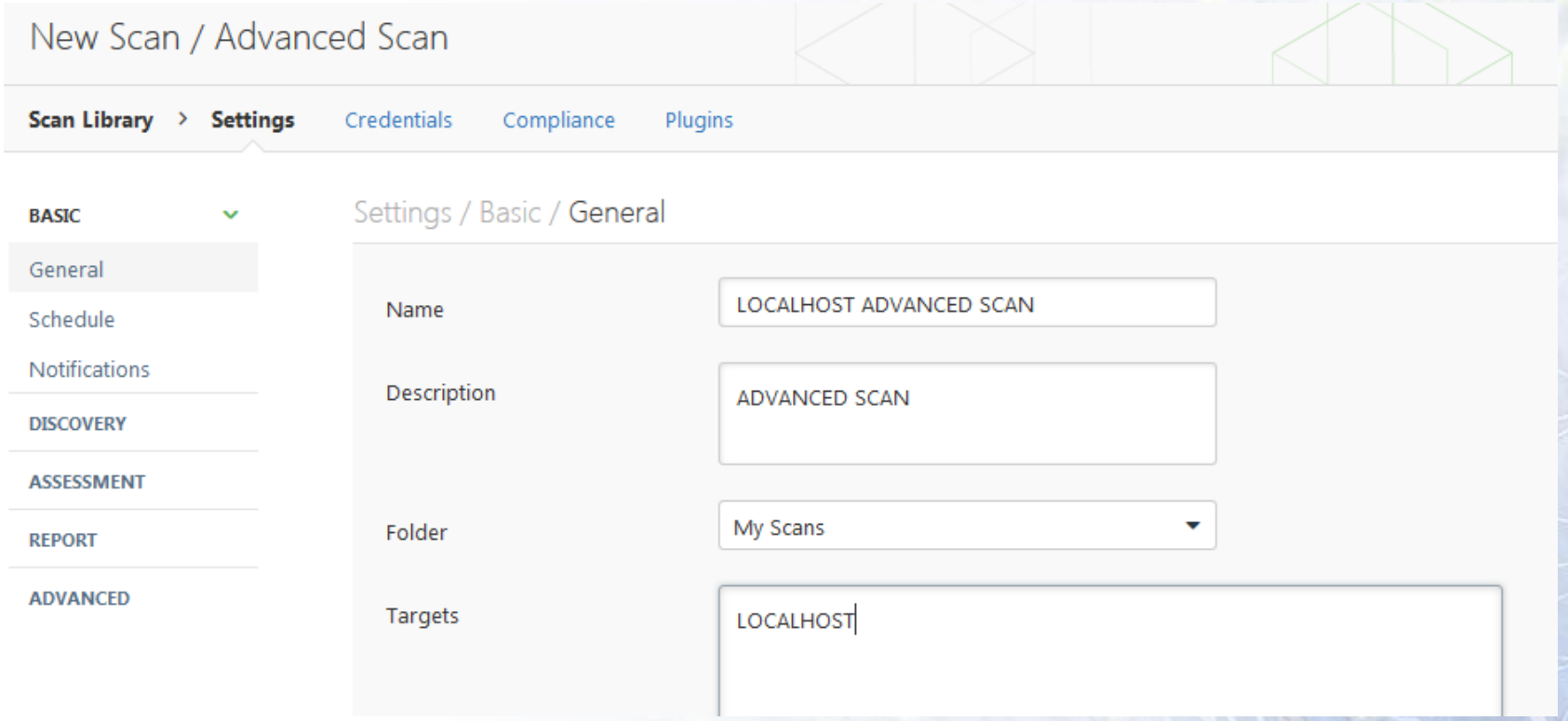
Nessus Demo - 1

NEW SCAN…



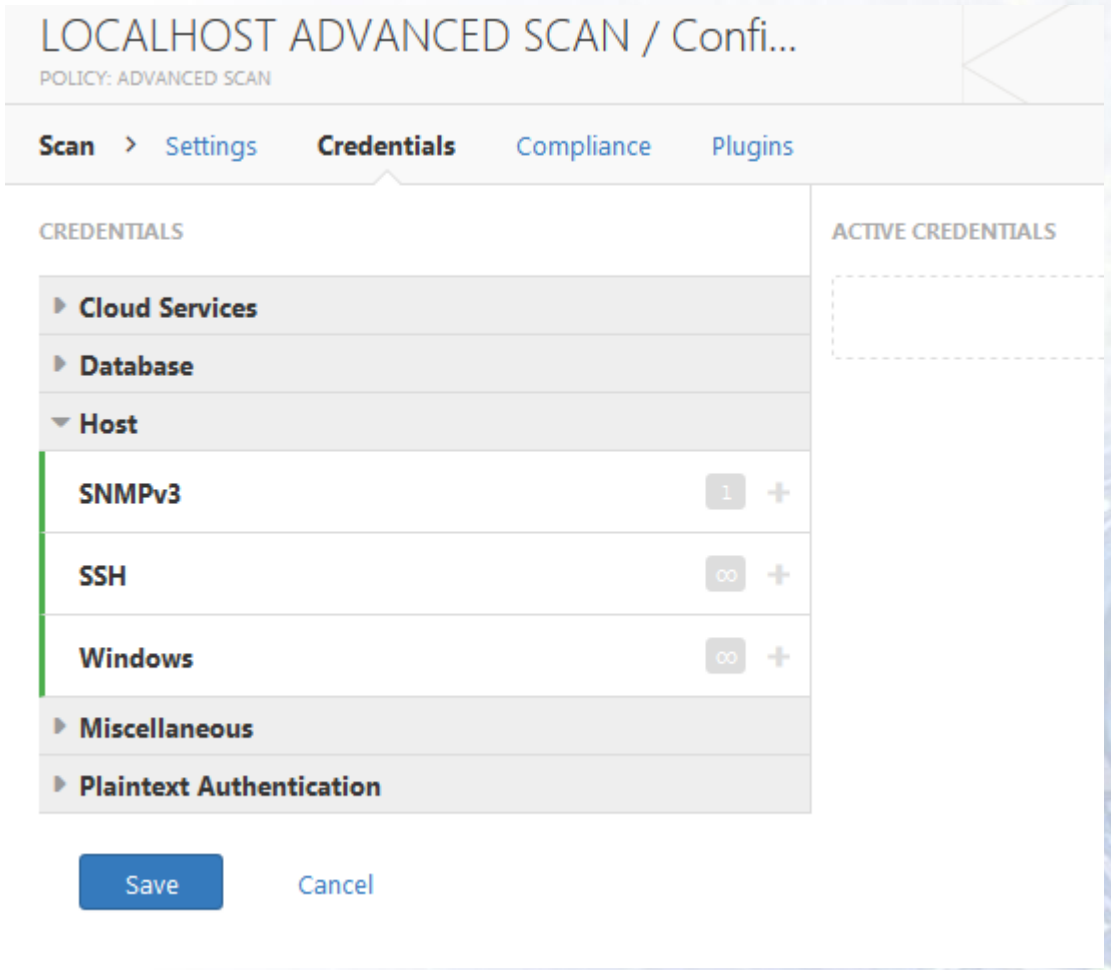
Nessus Demo - 1

ENTER SCAN DETAILS



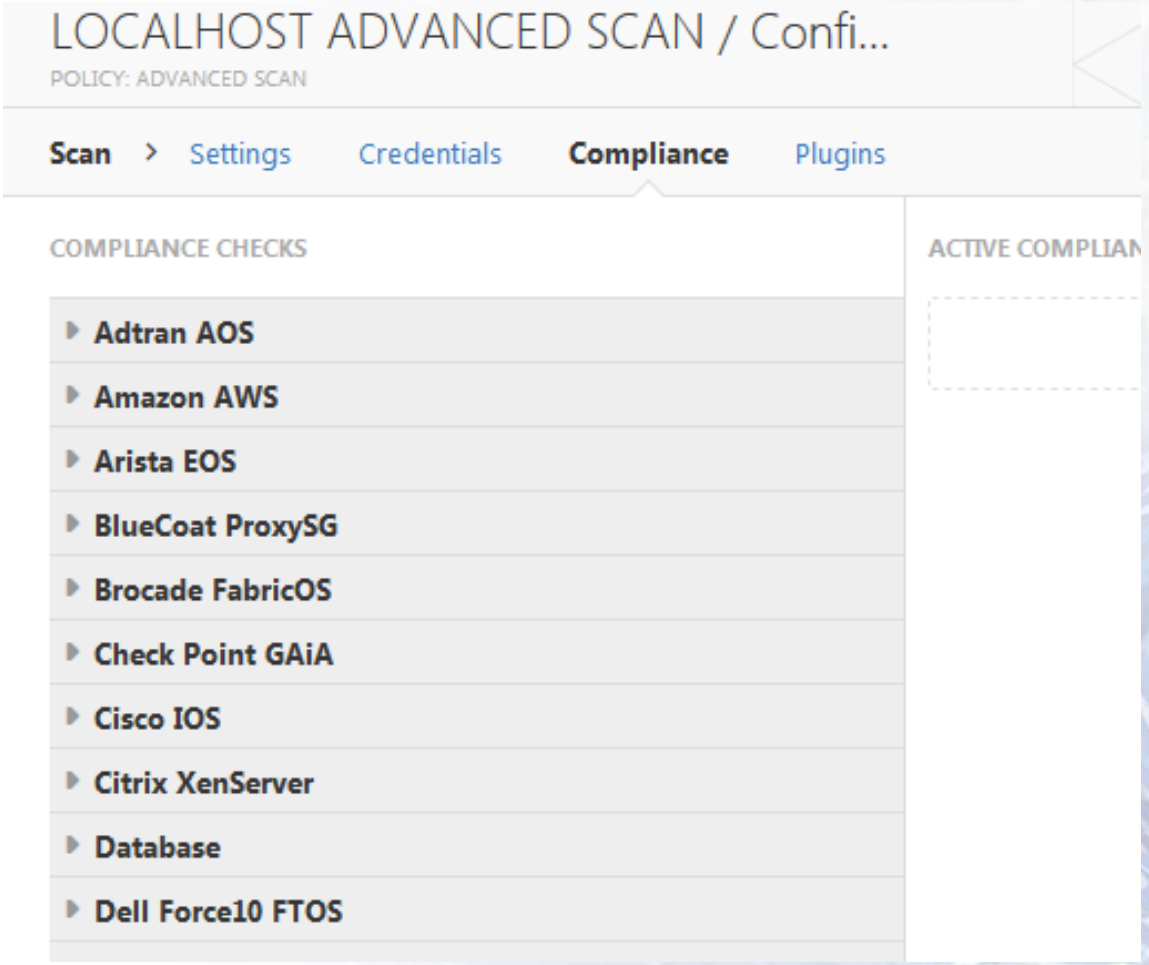
Nessus Demo - 1

CREDENTIAL SCAN



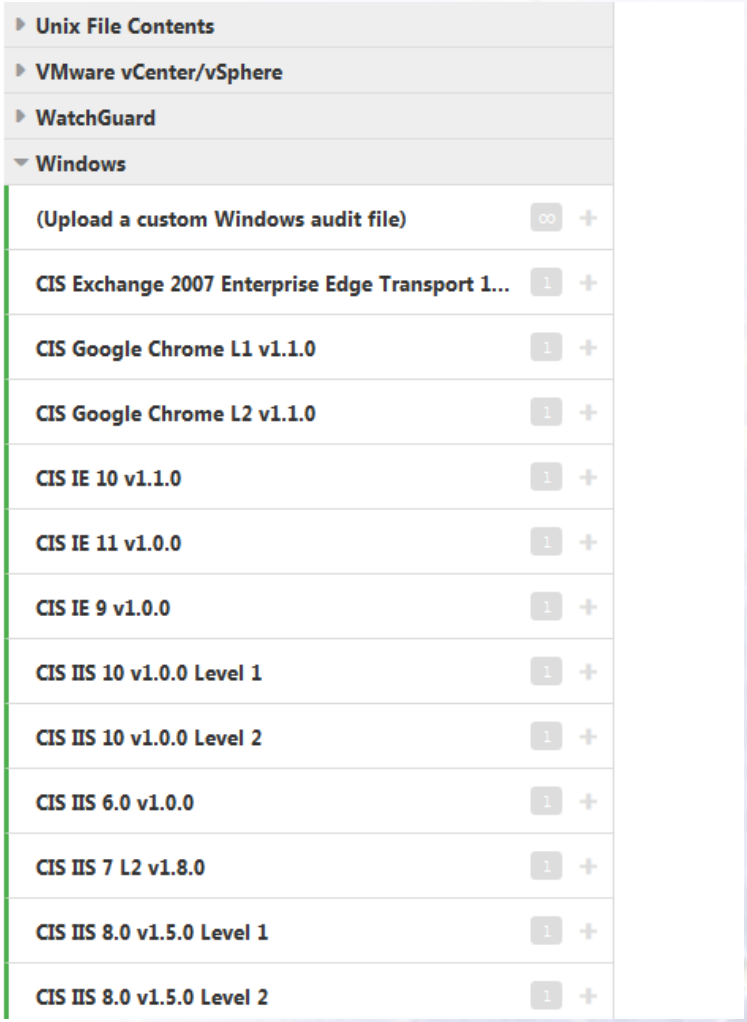
Nessus Demo - 1

COMPLIANCE SCAN



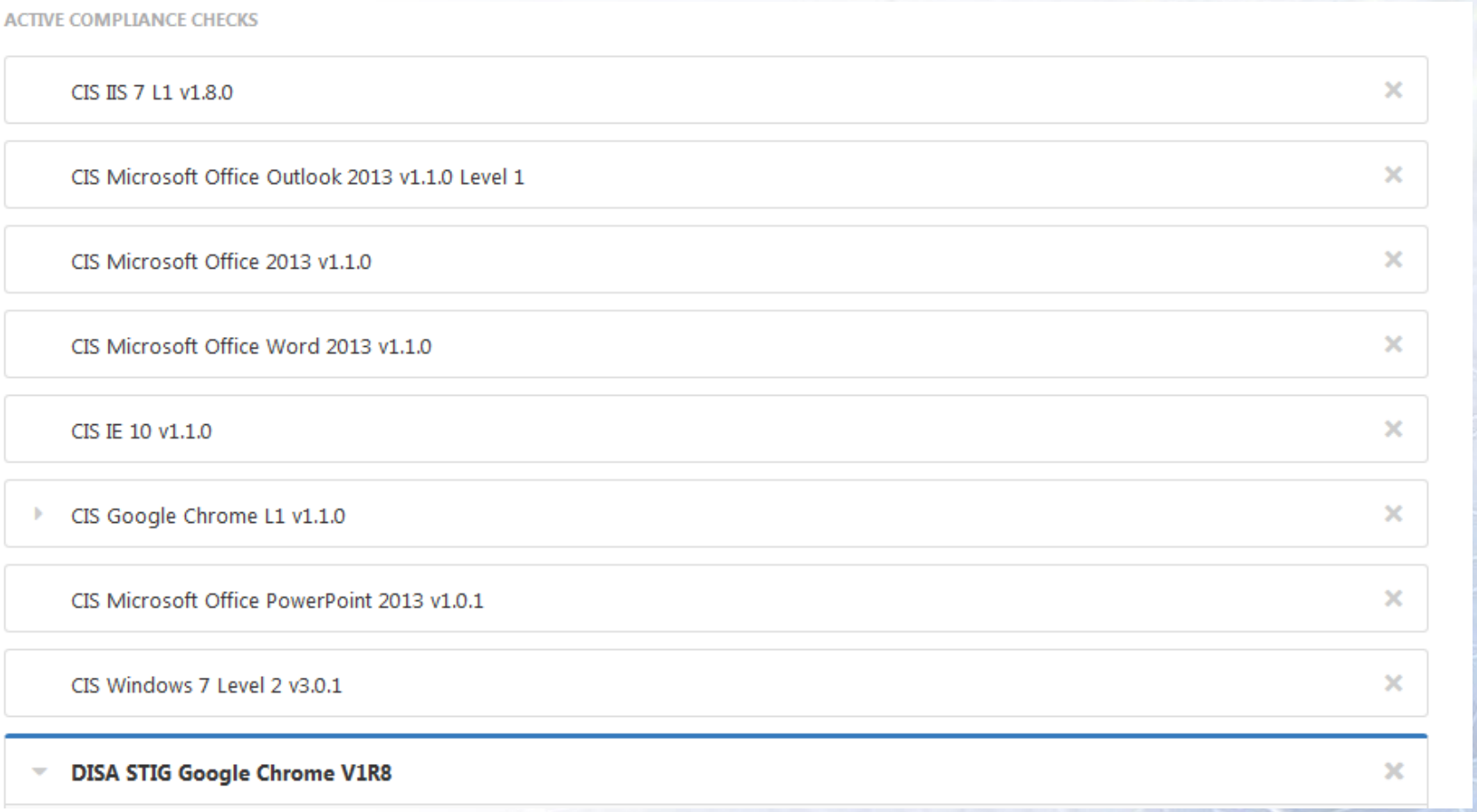
Nessus Demo - 1

WINDOWS COMPLIANCE MENU (CIS)



Nessus Demo - 1

WINDOWS COMPLIANCE MENU (CIS)…



Nessus Demo - 1

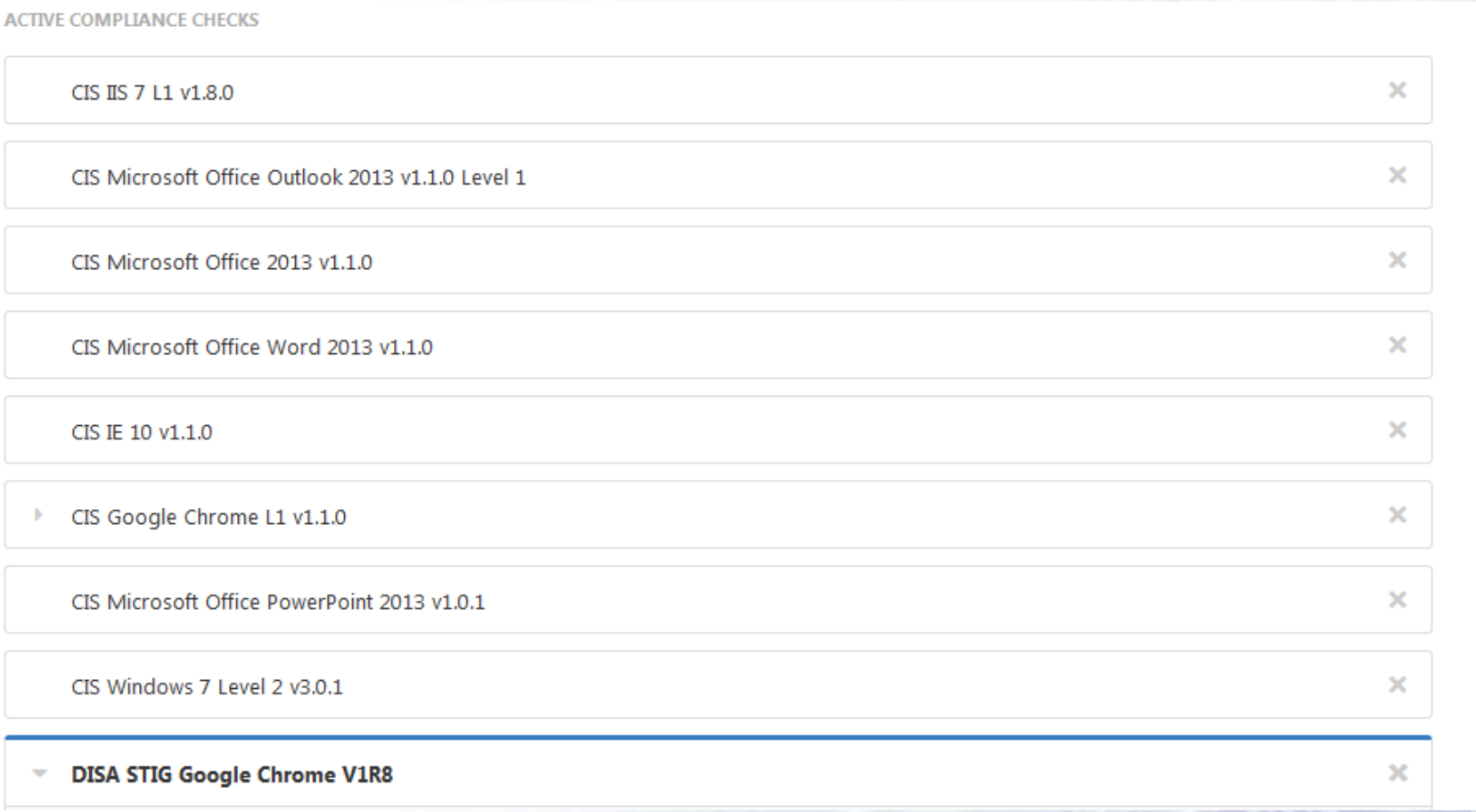
- Lets take a look at Nessus Demo
- https://www.tenable.com/products/nessus/nessus-professional/evaluate
- Download free 7 day trial
- Get activation key from website

Nessus Demo - 2

- Lets take a look at Nessus Demo
- https://www.tenable.com/products/nessus/nessus-professional/evaluate
- Download free 7 day trial
- Get activation key from website

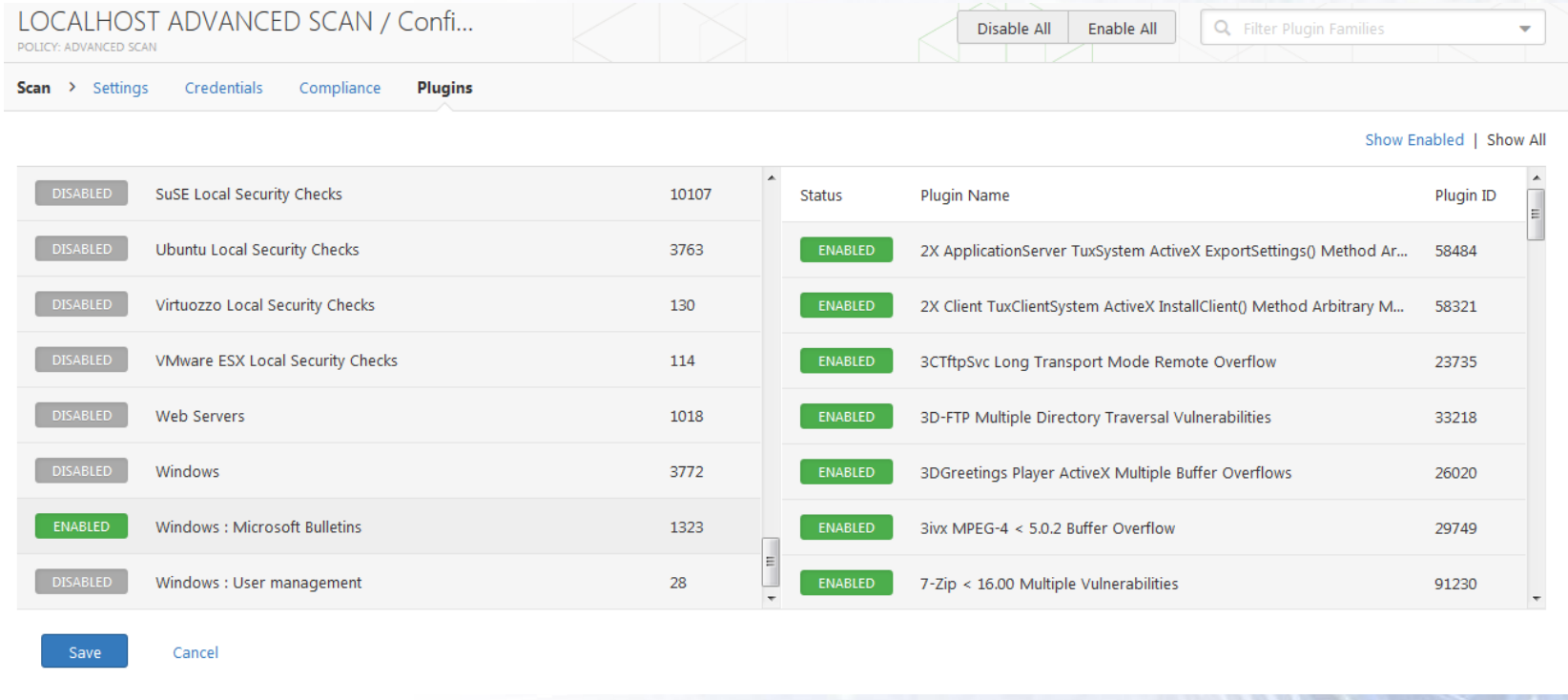
Nessus Demo - 2

ADVANCED SCAN / COMPLIANCE



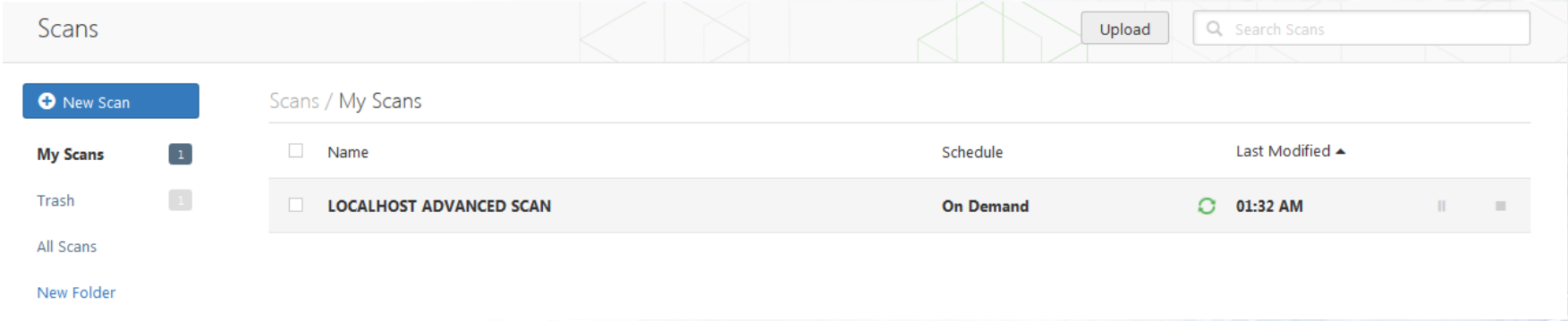
Nessus Demo - 2

ADVANCED SCAN / PLUG-INS



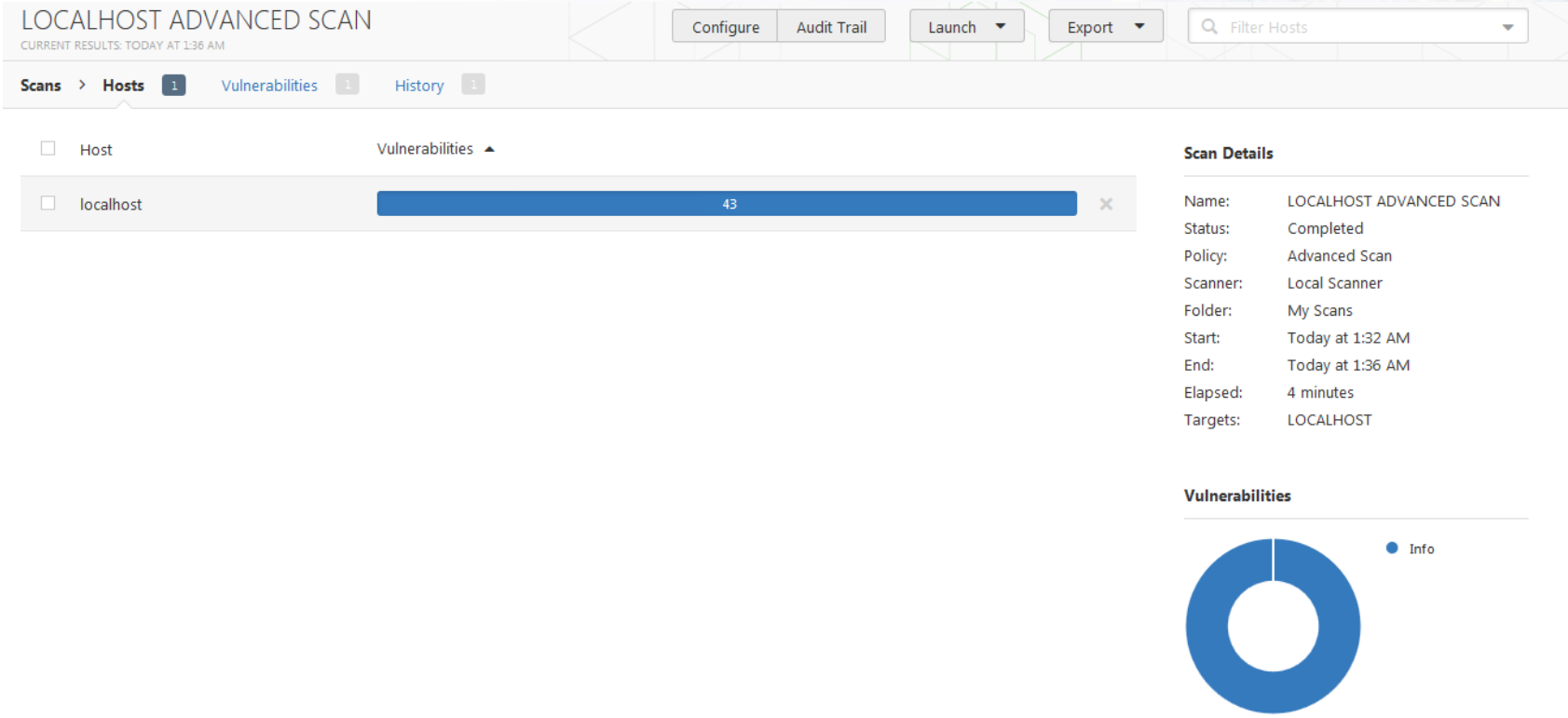
Nessus Demo - 2

SCAN…IN PROGRESS



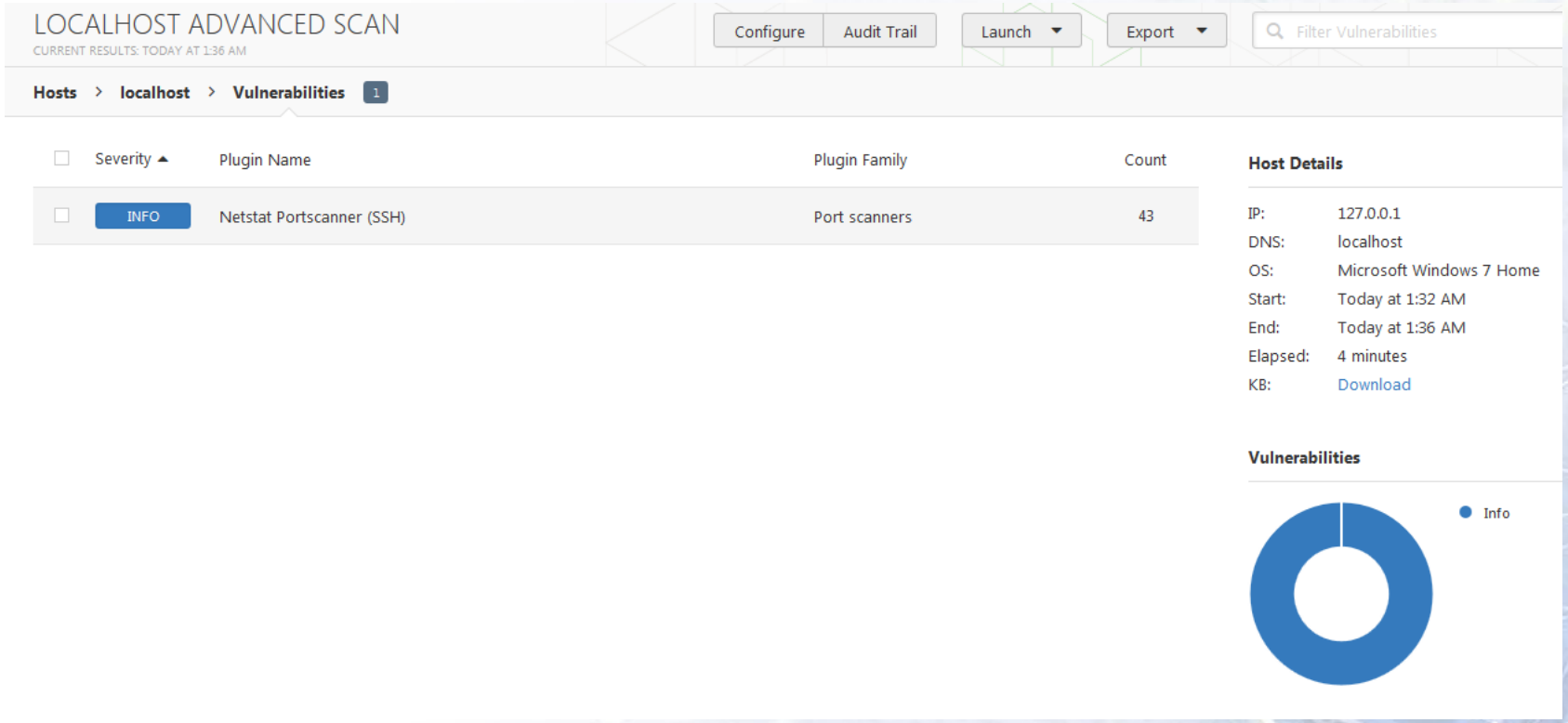
Nessus Demo - 2

SCAN REPORT [43 INFO]



Nessus Demo - 2

SCAN REPORT [DETAILS]



Nessus Demo - 2

SCAN REPORT [DETAILS…]

https://en.wikipedia.org/wiki/Netstat

Output

Port 68/udp was found to be open

Port	Hosts
68 / udp	localhost

Port 123/udp was found to be open

Port	Hosts
123 / udp	localhost

Port 135/tcp was found to be open

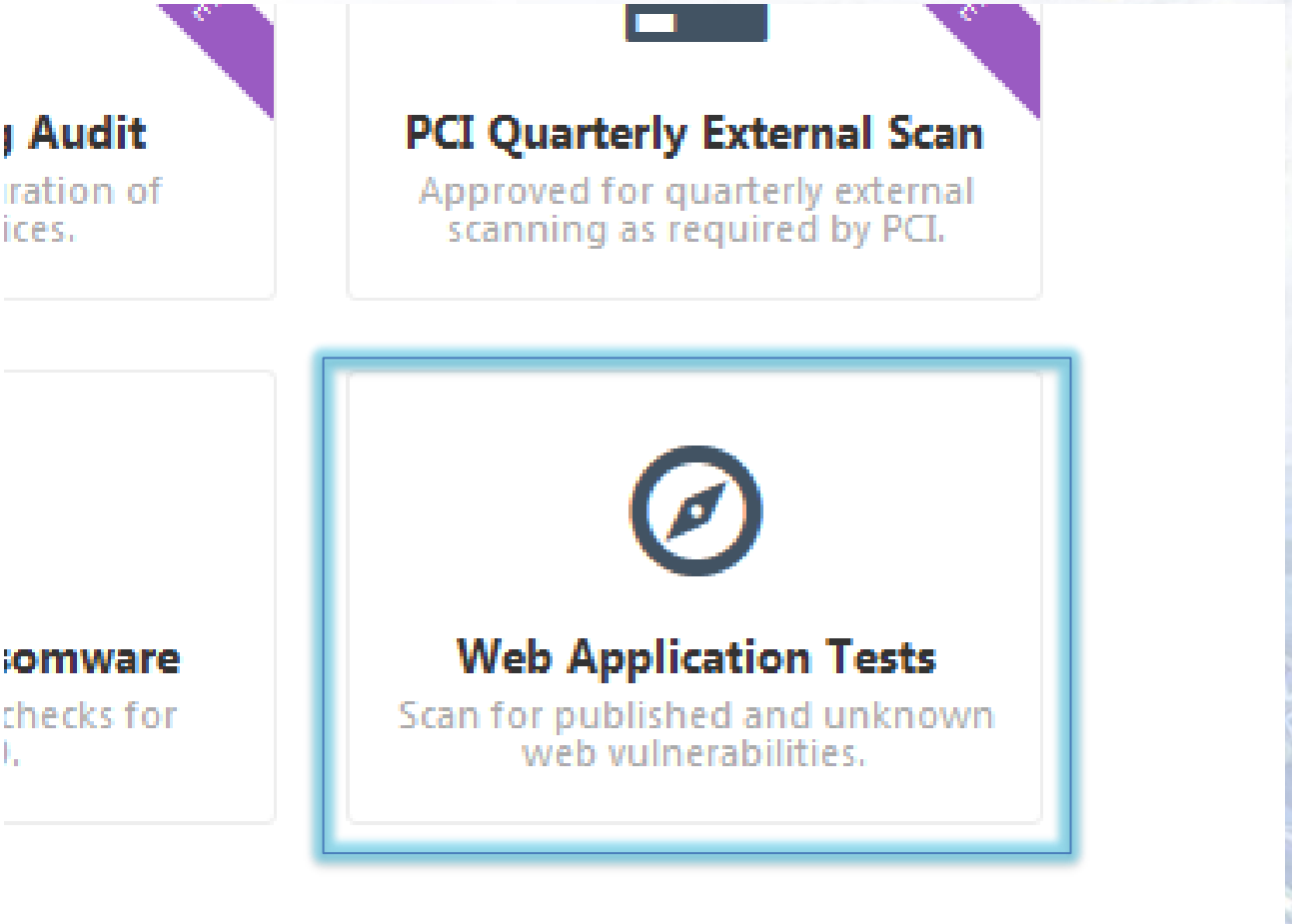
Port	Hosts
135 / tcp / epmap	localhost

Port 137/udp was found to be open

Port	Hosts
137 / udp	localhost

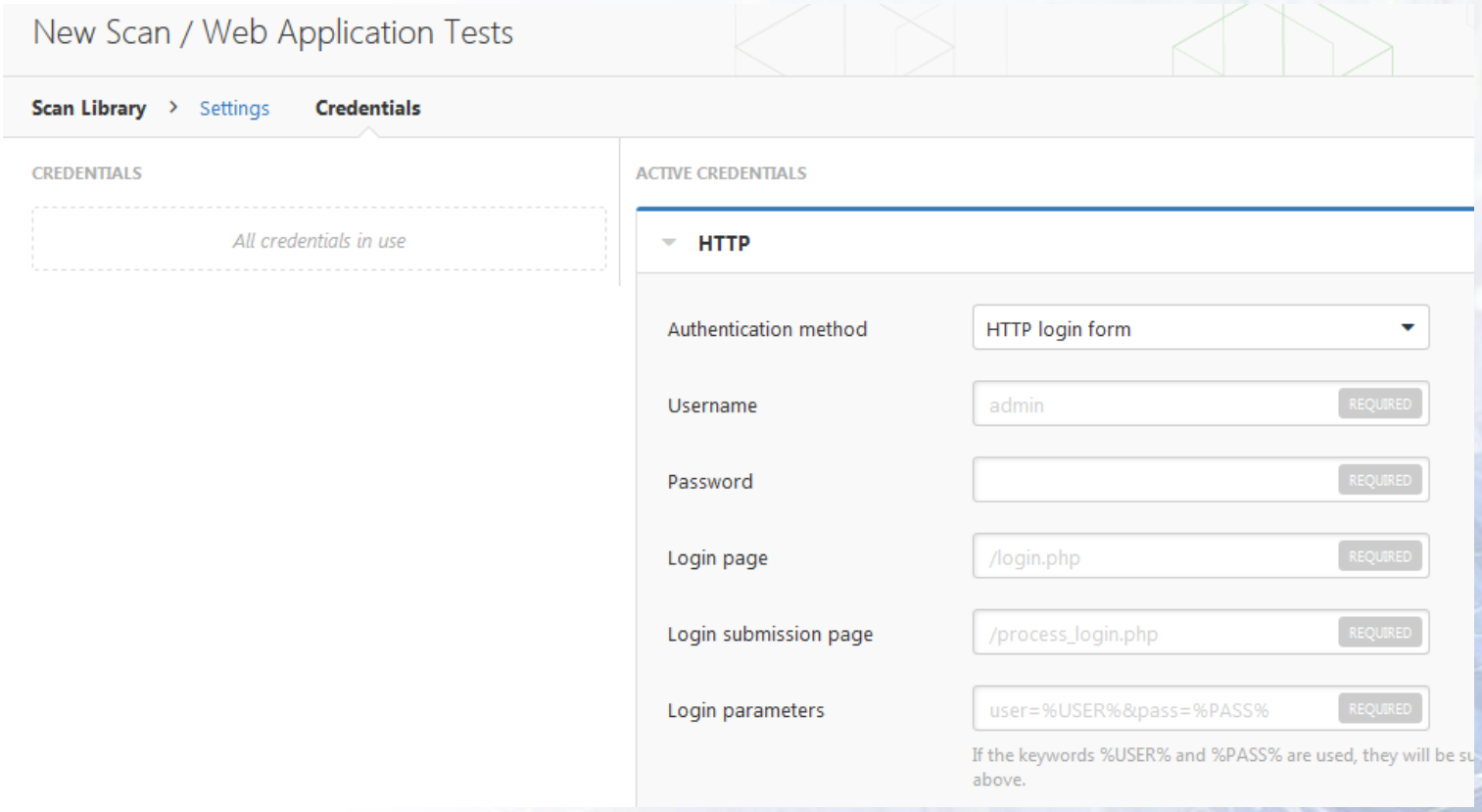
Nessus Demo - 2

WEB APPLICATION TEST



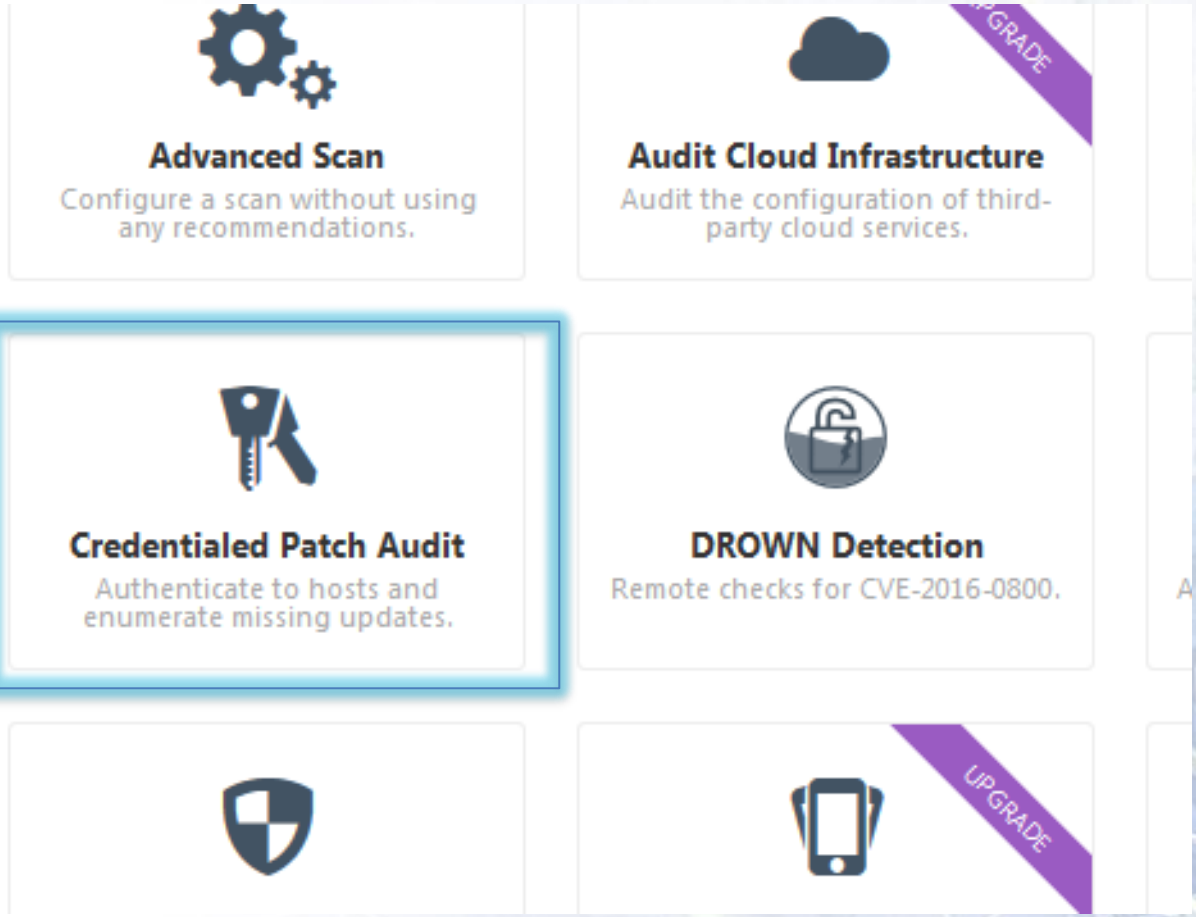
Nessus Demo - 2

WEB APPLICATION TEST - CREDENTIALS



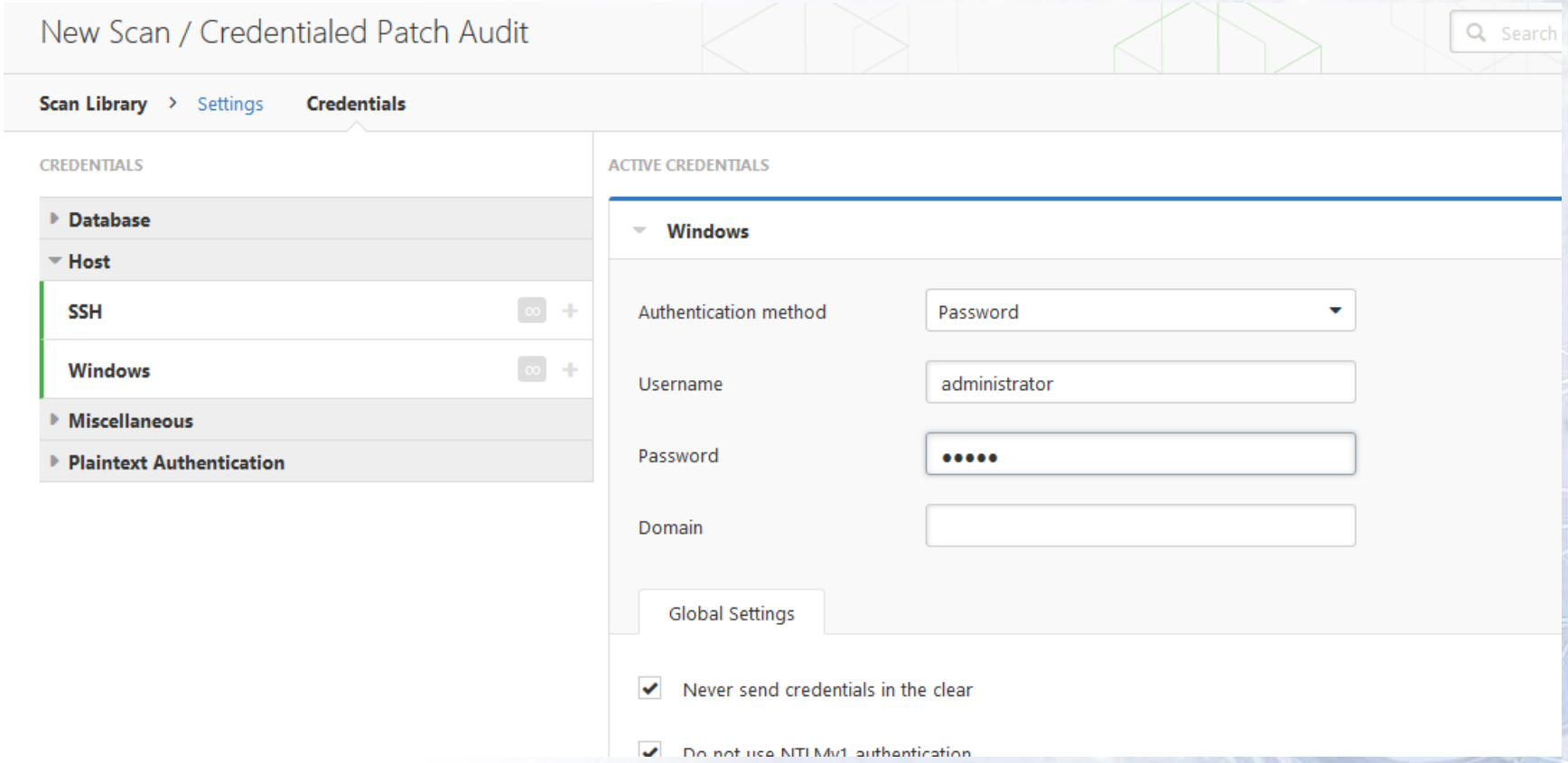
Nessus Demo - 2

CREDENTIALED PATCH AUDIT



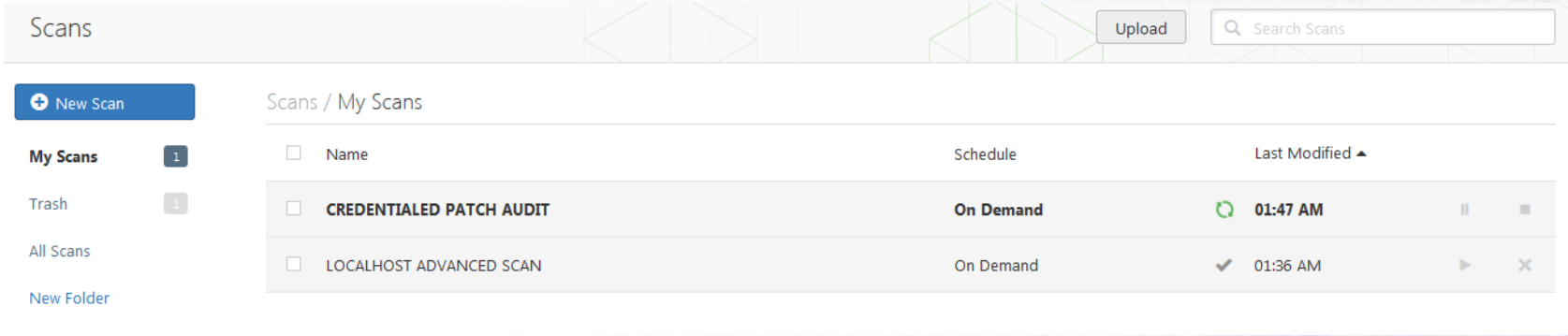
Nessus Demo - 2

CREDENTIALED PATCH AUDIT



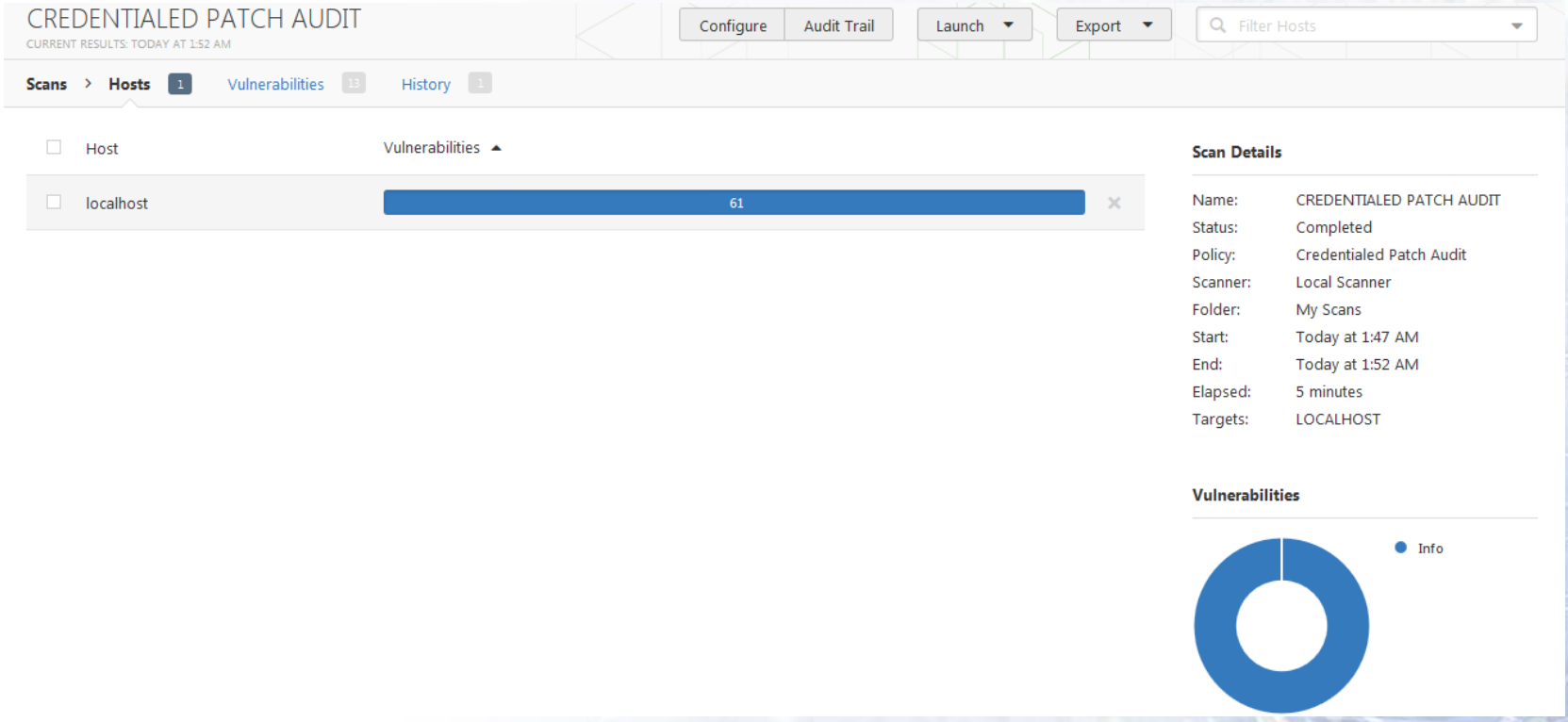
Nessus Demo - 2

SCANS DASHBOARD



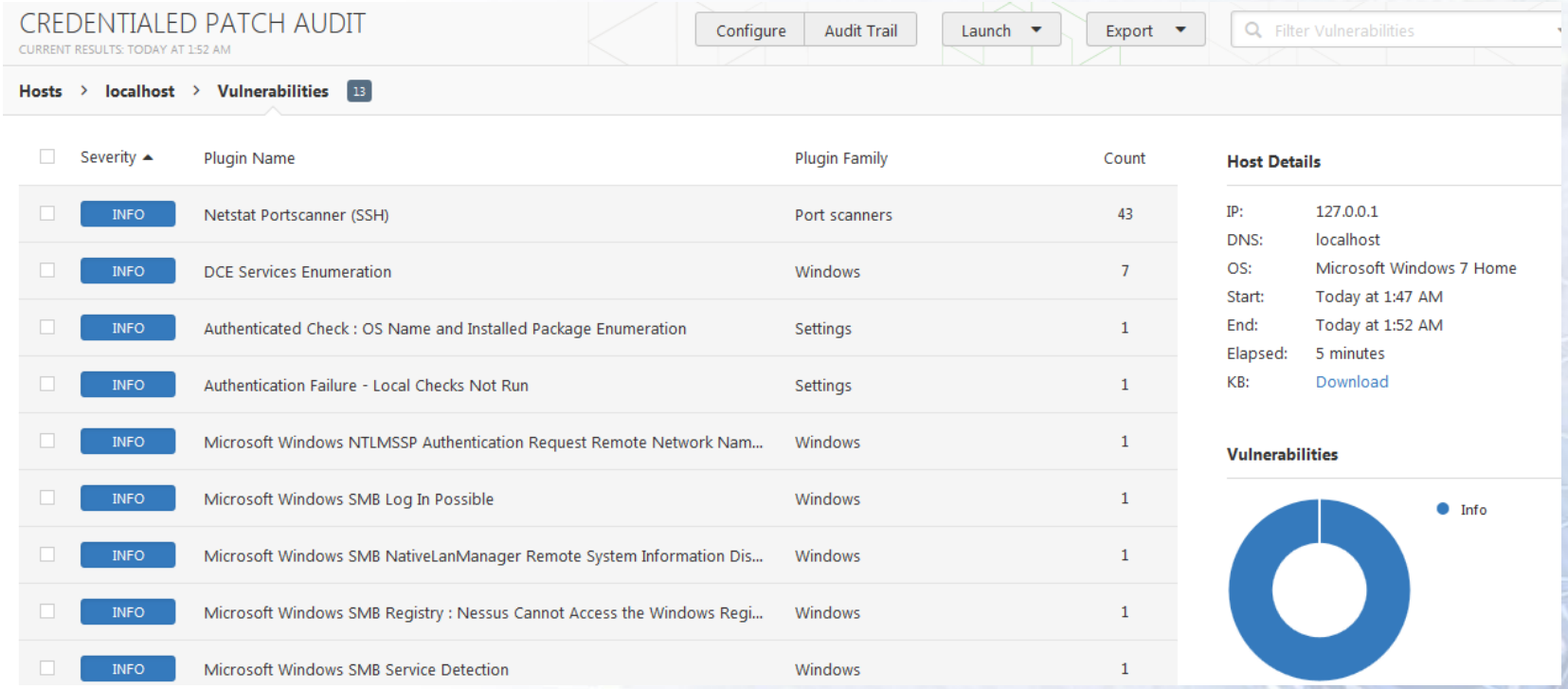
Nessus Demo - 2

CREDENTIALED AUDIT SCAN RESULTS [61 INFO]



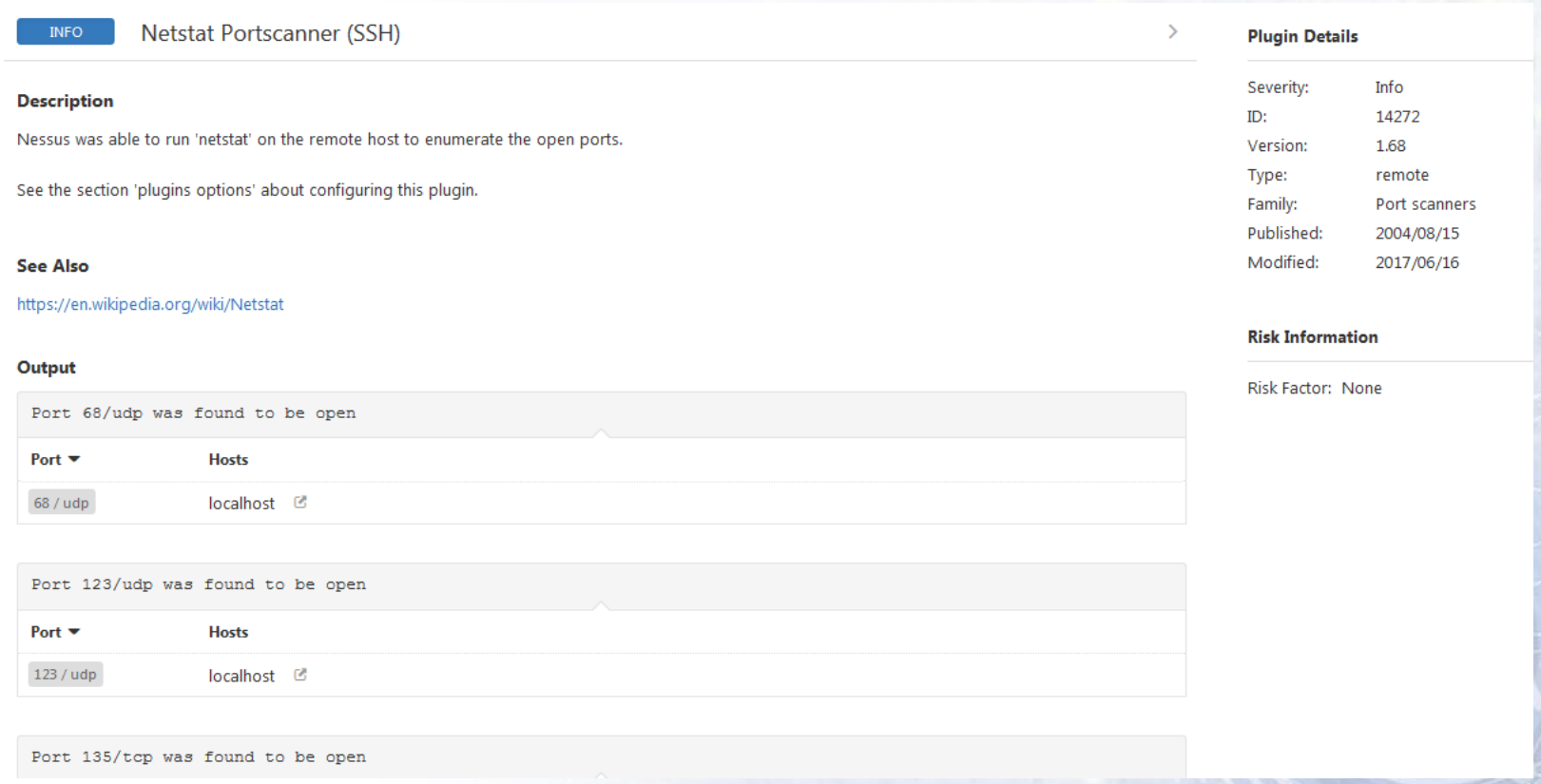
Nessus Demo - 2

CREDENTIALED AUDIT SCAN RESULTS [61 INFO]



Nessus Demo - 2

CREDENTIALED AUDIT SCAN RESULTS [DETAILS]



INFO Netstat Portscanner (SSH)

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See the section 'plugins options' about configuring this plugin.

See Also

https://en.wikipedia.org/wiki/Netstat

Output

```
Port 68/udp was found to be open
```

Port	Hosts
68 / udp	localhost

```
Port 123/udp was found to be open
```

Port	Hosts
123 / udp	localhost

```
Port 135/tcp was found to be open
```

Plugin Details

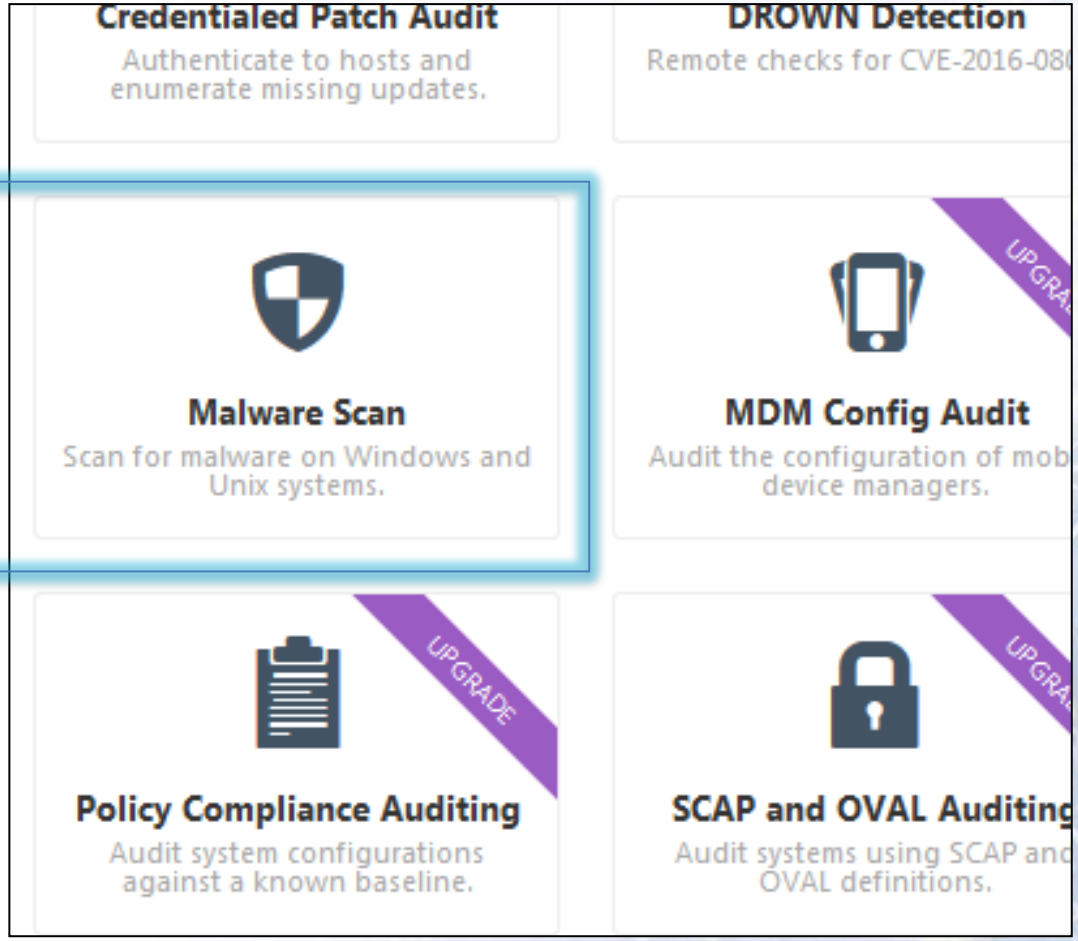
Severity:	Info
ID:	14272
Version:	1.68
Type:	remote
Family:	Port scanners
Published:	2004/08/15
Modified:	2017/06/16

Risk Information

Risk Factor: None

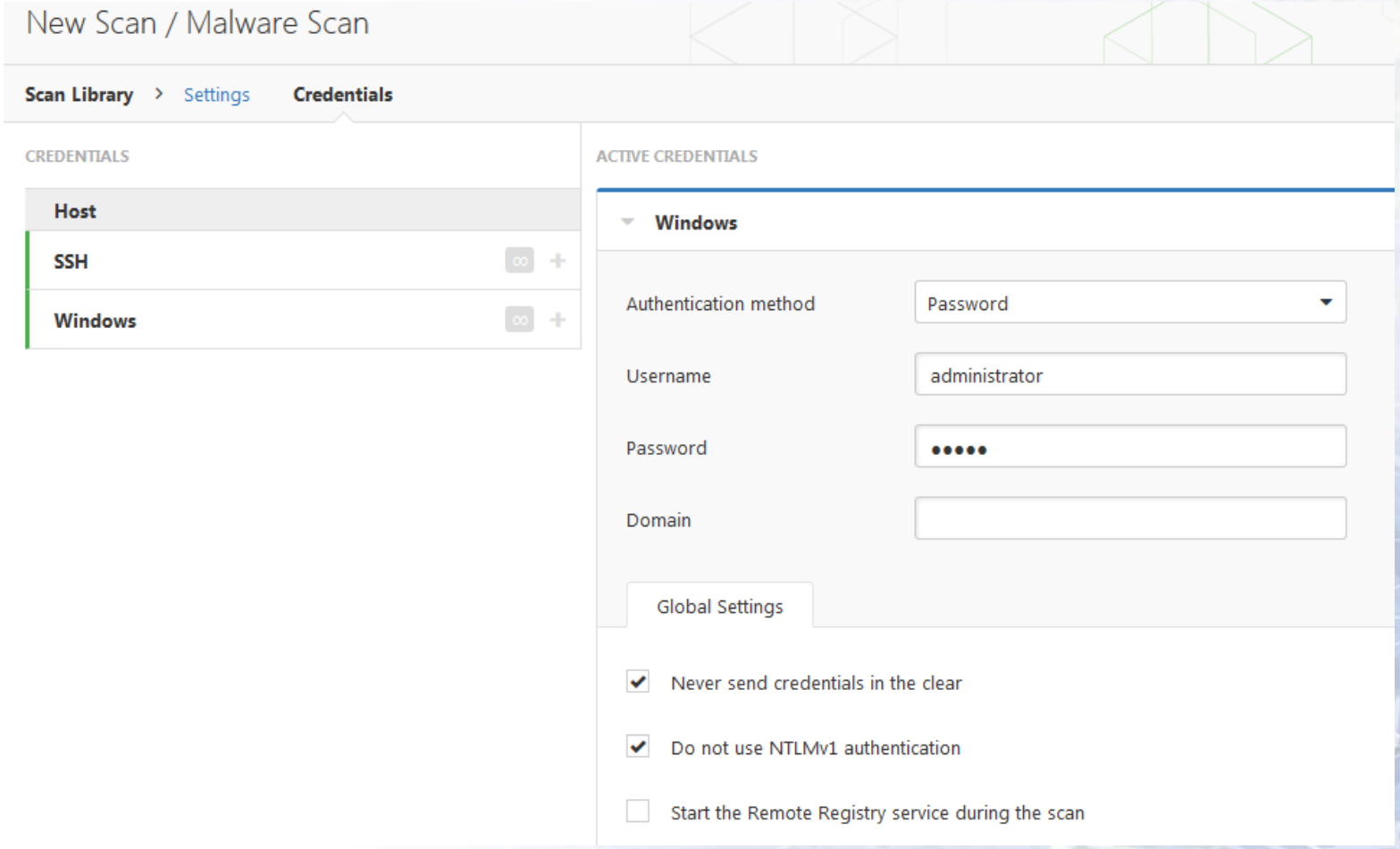
Nessus Demo - 2

SYSTEM MALWARE SCAN



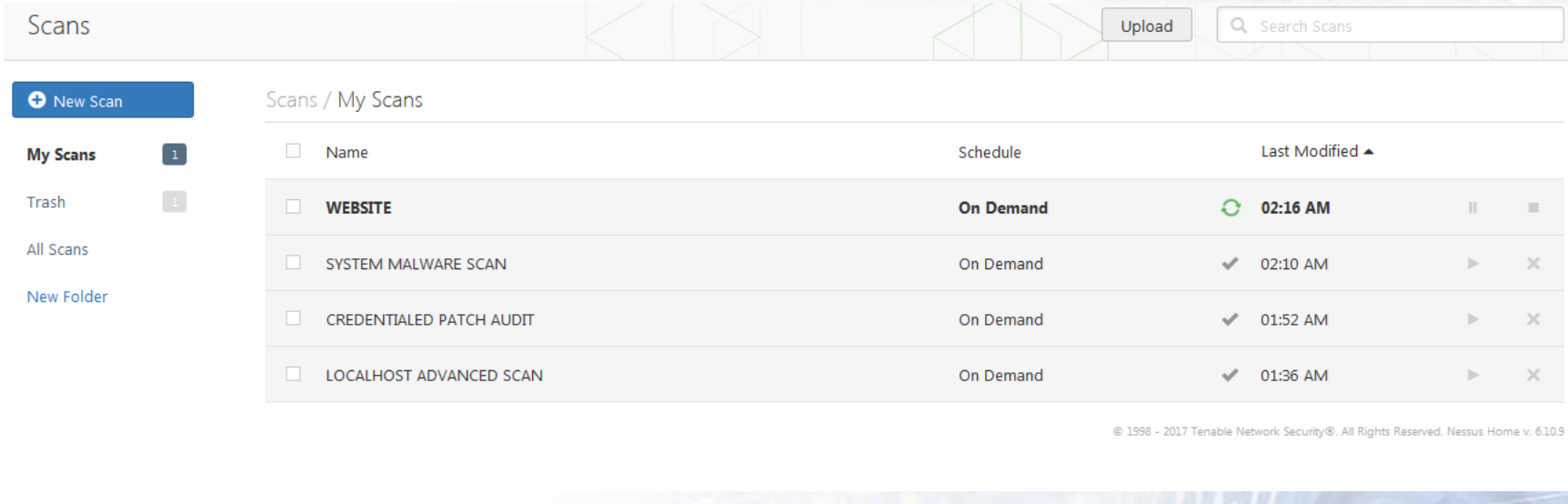
Nessus Demo - 2

SYSTEM MALWARE SCAN



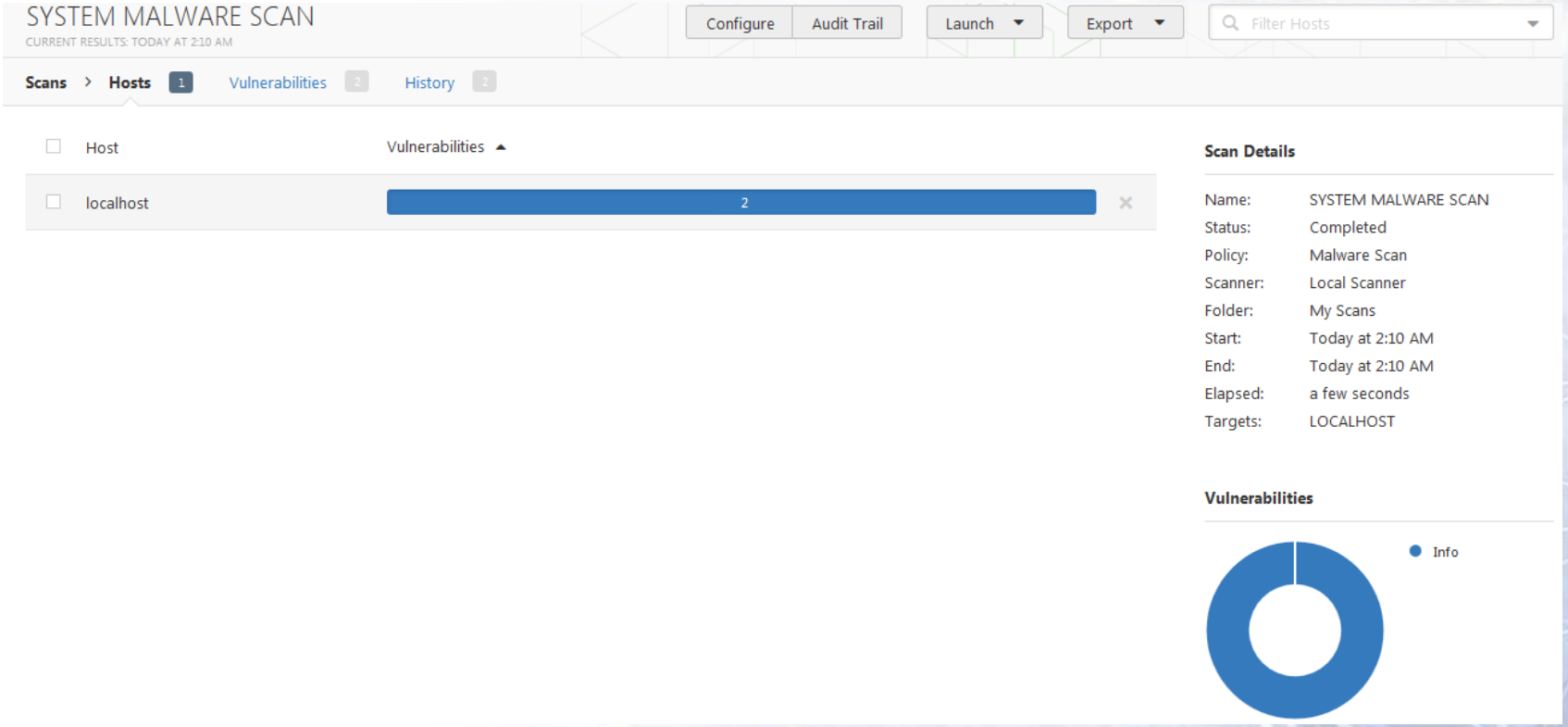
Nessus Demo - 2

SCAN DASHBOARD



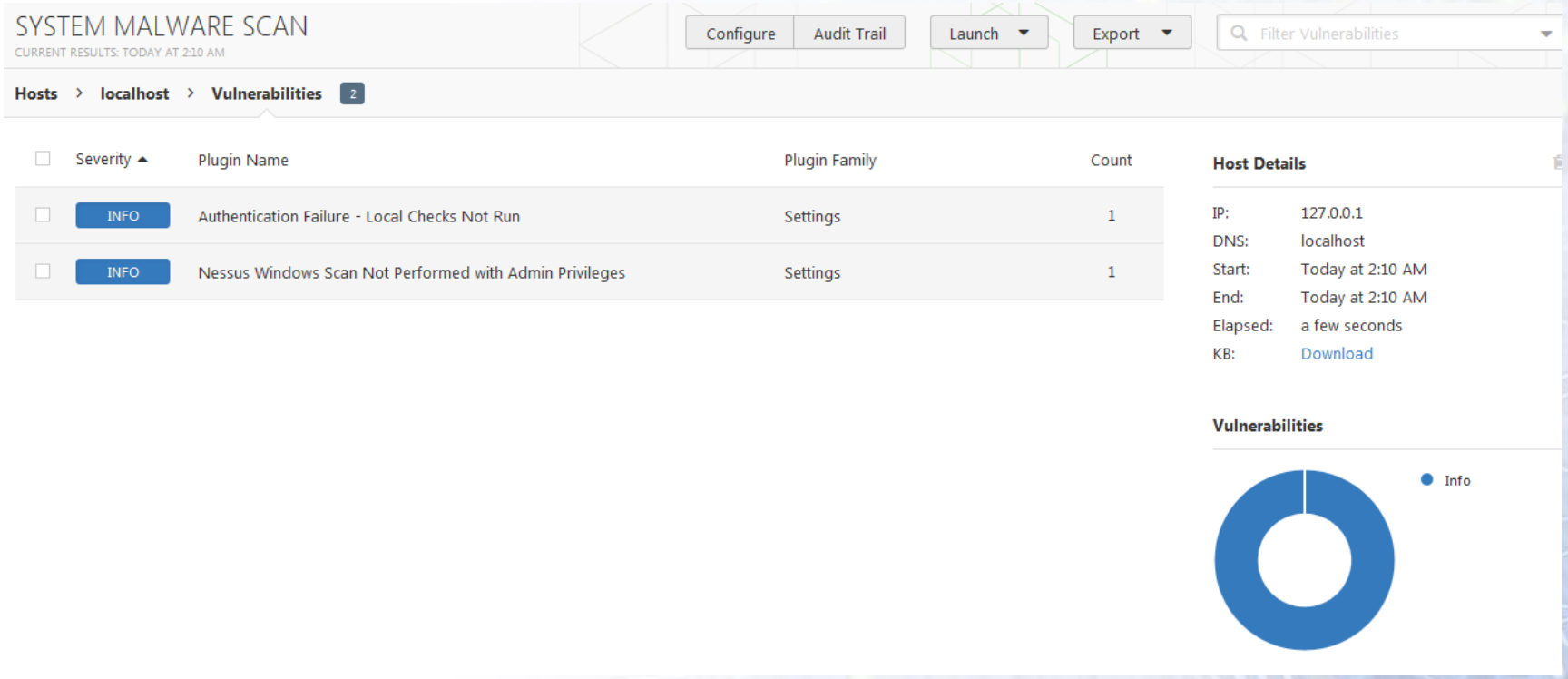
Nessus Demo - 2

SYSTEM MALWARE SCAN [2 INFO]



Nessus Demo - 2

SYSTEM MALWARE SCAN



Nessus Demo - 2

- Nessus is an easy to use and powerful scanner
- Dozens of scans on dashboard
- Setup a new scan
- Setup a profile as scan template
- Credentialed scan
- Thousands of plugins from CIS/DISA etc

END

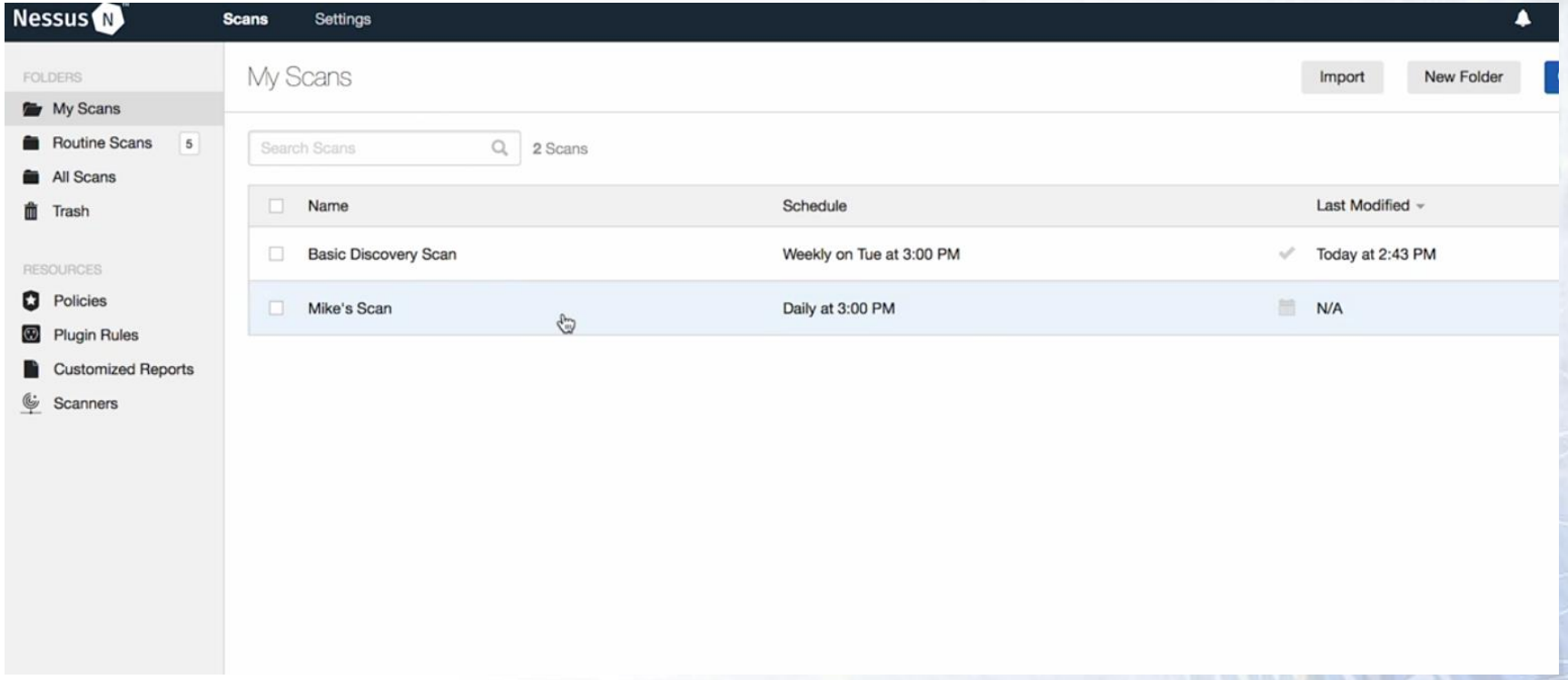
Nessus scan Types

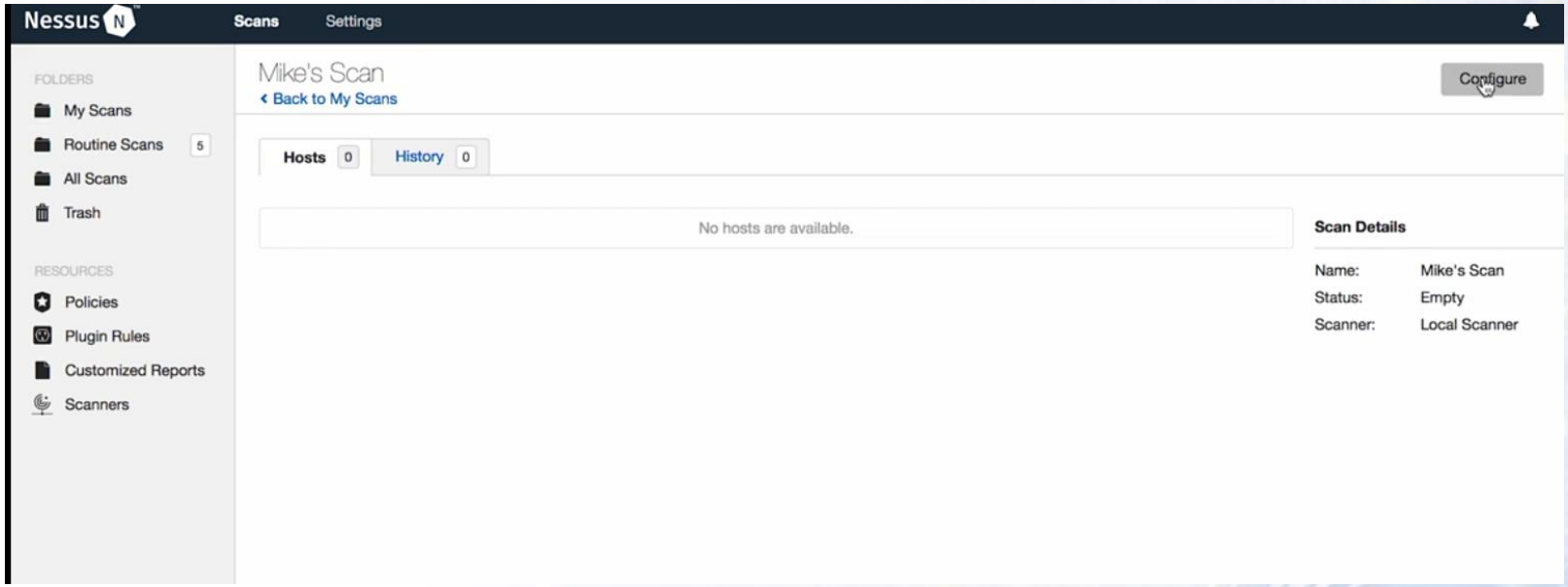
Nessus Credentailed scan

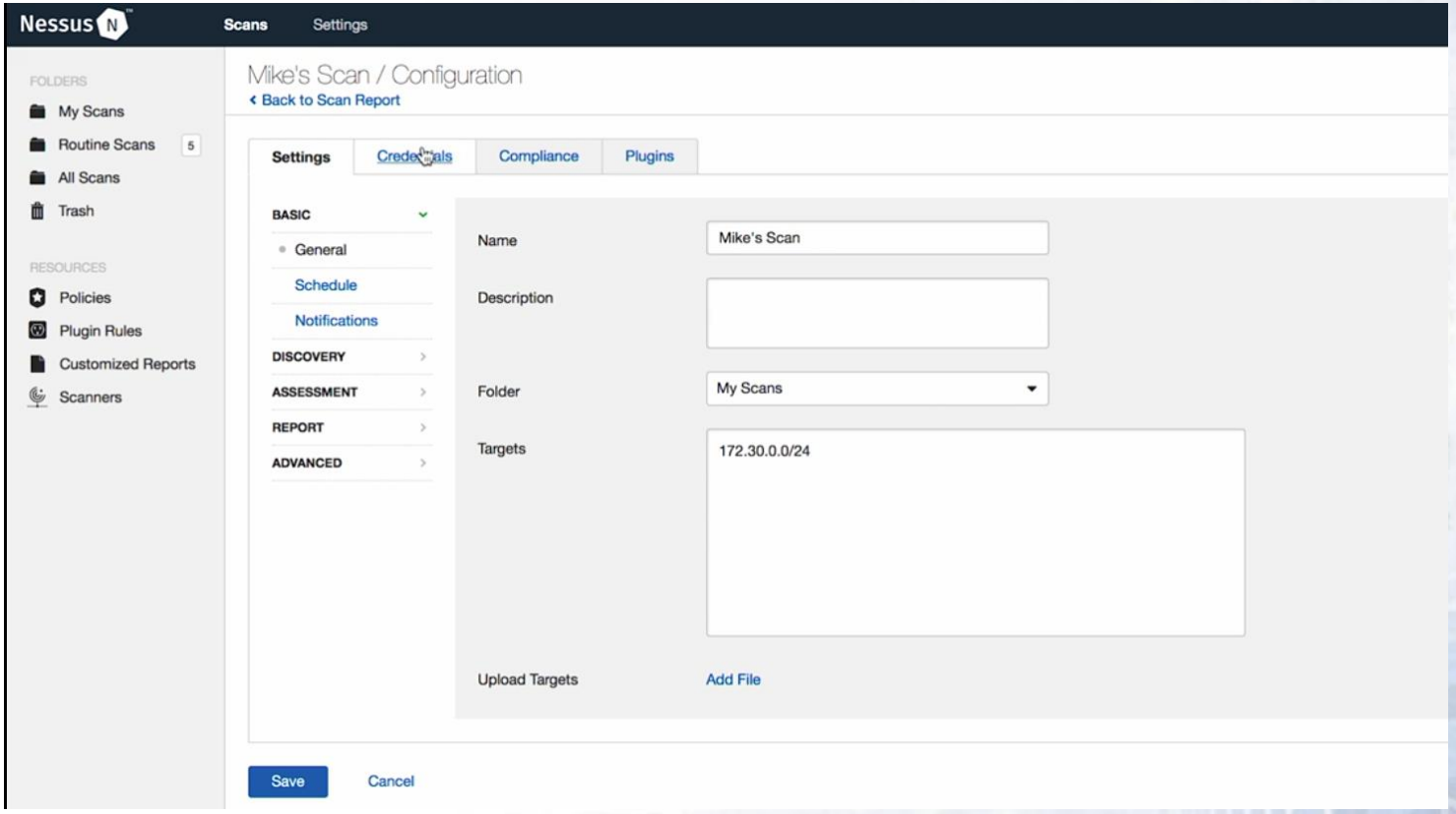


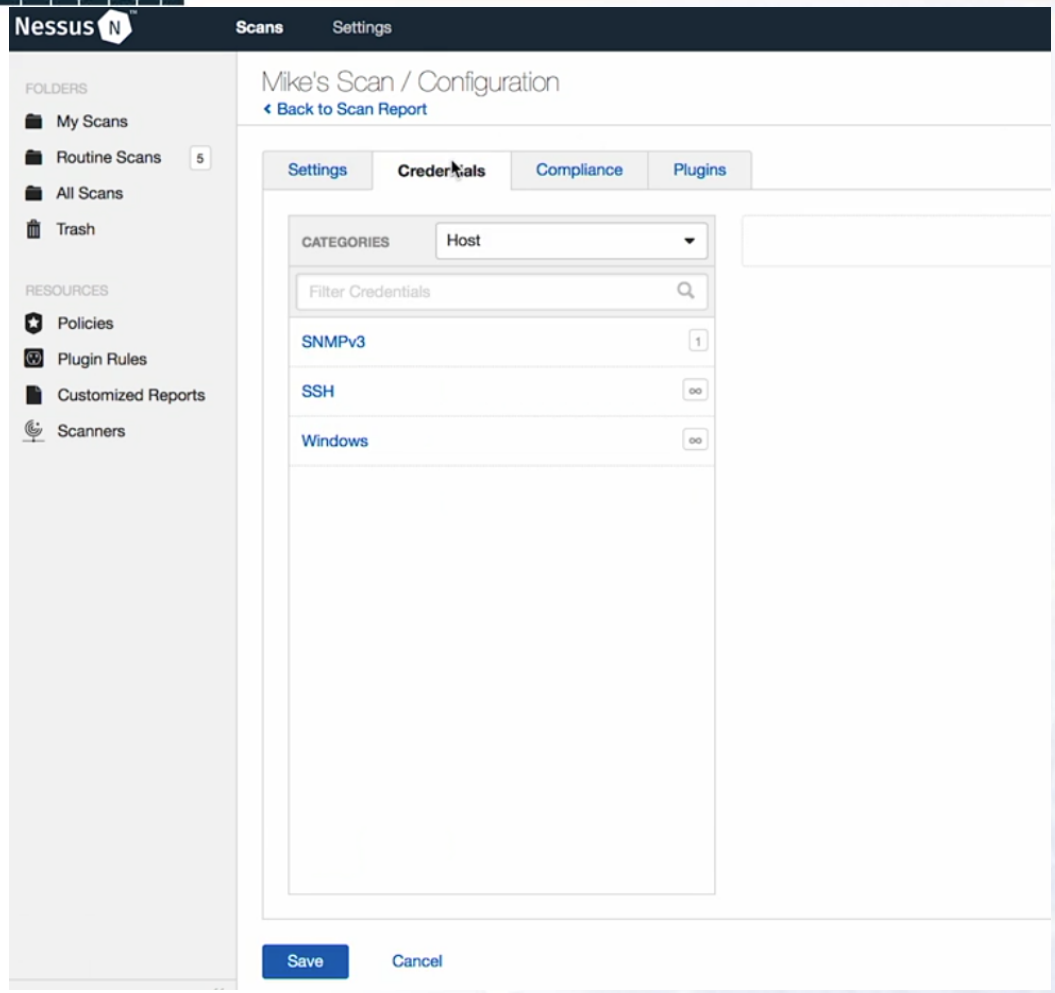
Credentialed Scanning

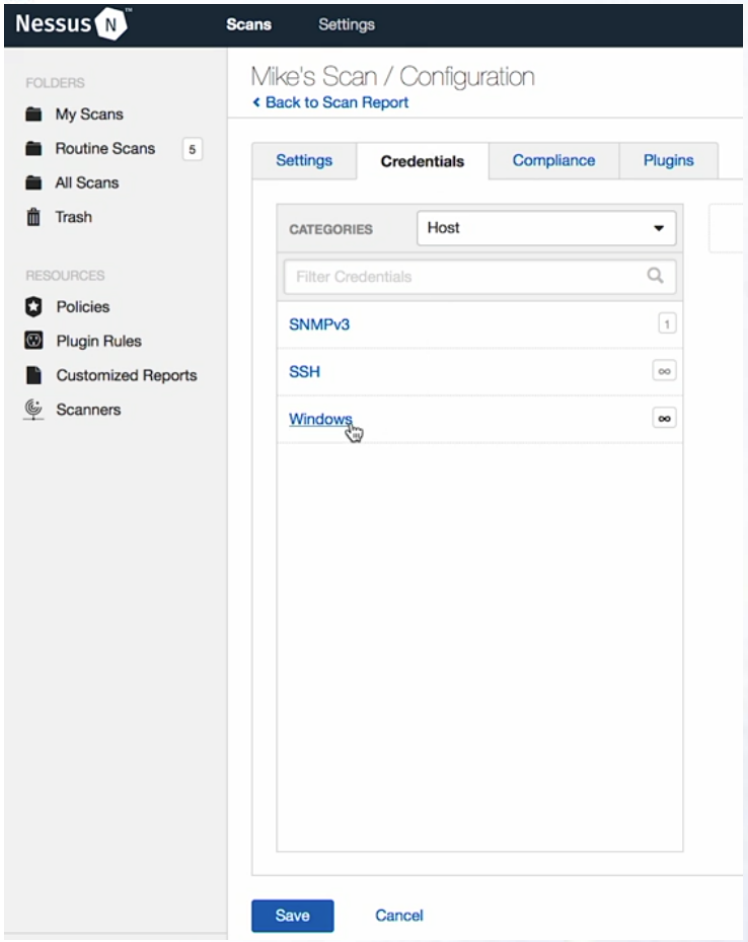
Uses passwords to log into systems

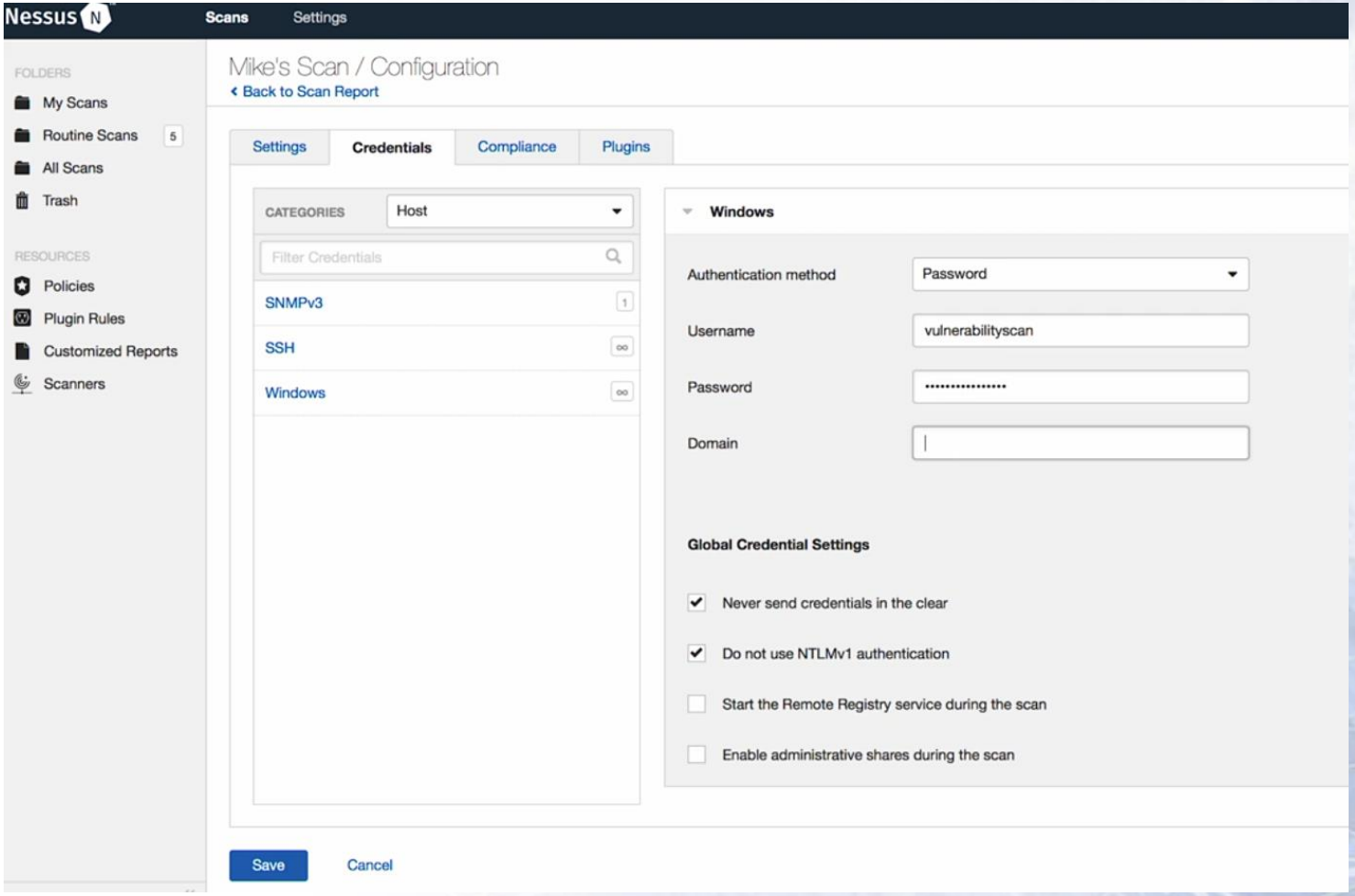

Nessus
Scans
Settings
FOLDERS
My Scans
Routine Scans
5
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
My Scans
Import
New Folder
Search Scans
2 Scans
Name
Schedule
Last Modified
Basic Discovery Scan
Weekly on Tue at 3:00 PM
Today at 2:43 PM
Mike's Scan
Daily at 3:00 PM
N/A


Nessus
Scans
Settings
FOLDERS
My Scans
Routine Scans 5
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
Mike's Scan
Back to My Scans
Configure
Hosts 0
History 0
No hosts are available.
Scan Details
Name: Mike's Scan
Status: Empty
Scanner: Local Scanner


Nessus
Scans
Settings
FOLDERS
My Scans
Routine Scans
5
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
Mike's Scan / Configuration
Back to Scan Report
Settings
Credentials
Compliance
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
Mike's Scan
Description
Folder
My Scans
Targets
172.30.0.0/24
Upload Targets
Add File
Save
Cancel


Nessus
Scans
Settings
FOLDERS
My Scans
Routine Scans
5
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
Mike's Scan / Configuration
Back to Scan Report
Settings
Credentials
Compliance
Plugins
CATEGORIES
Host
Filter Credentials
SNMPv3
1
SSH
Windows
Save
Cancel

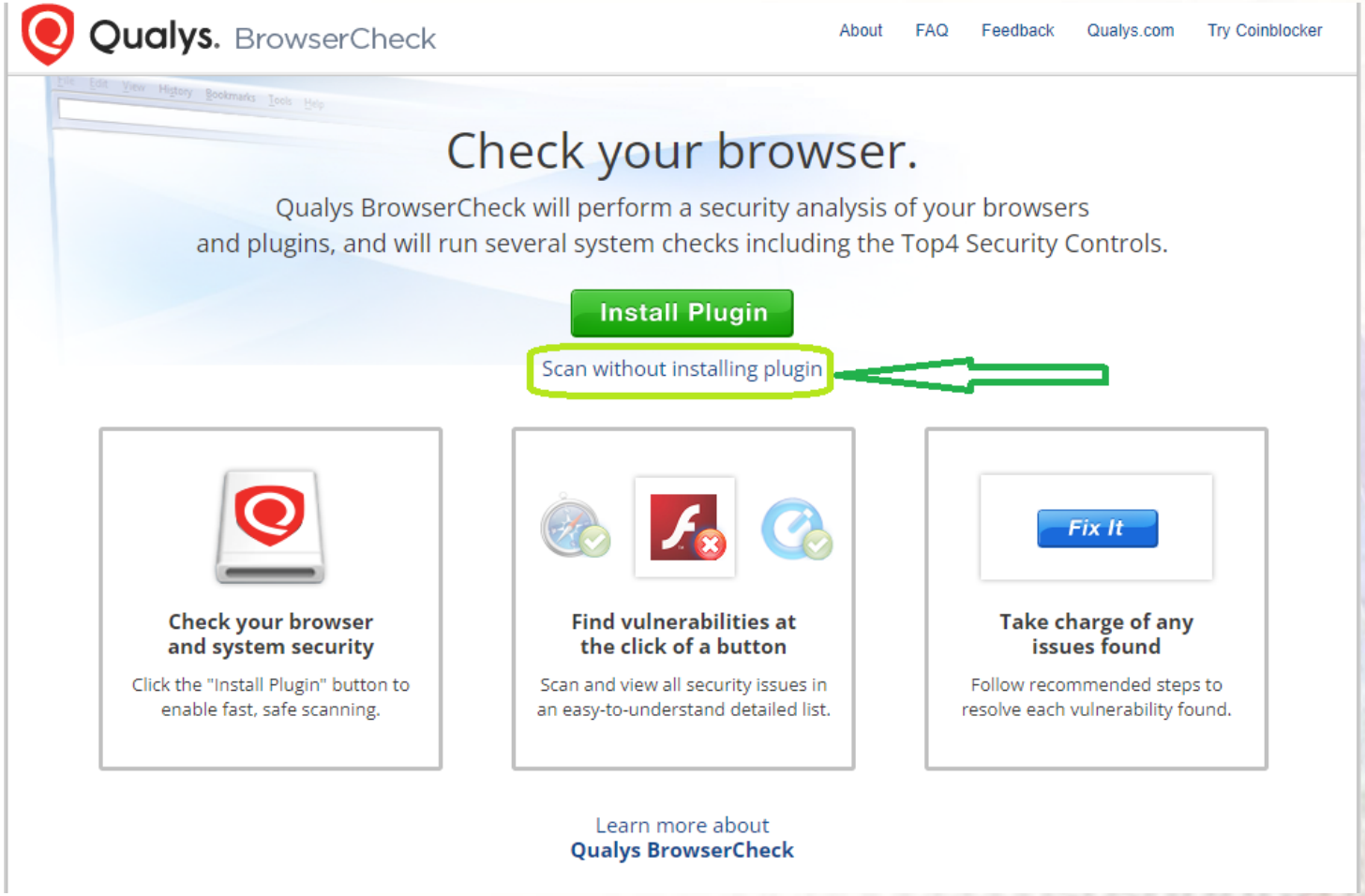

Nessus
Scans
Settings
FOLDERS
My Scans
Routine Scans
5
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
Mike's Scan / Configuration
Back to Scan Report
Settings
Credentials
Compliance
Plugins
CATEGORIES
Host
Filter Credentials
SNMPv3
1
SSH
Windows
Save
Cancel


Nessus
Scans
Settings
FOLDERS
My Scans
Routine Scans
5
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
Mike's Scan / Configuration
Back to Scan Report
Settings
Credentials
Compliance
Plugins
CATEGORIES
Host
Filter Credentials
SNMPv3
1
SSH
Windows
Windows
Authentication method
Password
Username
vulnerabilityscan
Password
Domain
Global Credential Settings
Never send credentials in the clear
Do not use NTLMv1 authentication
Start the Remote Registry service during the scan
Enable administrative shares during the scan
Save
Cancel

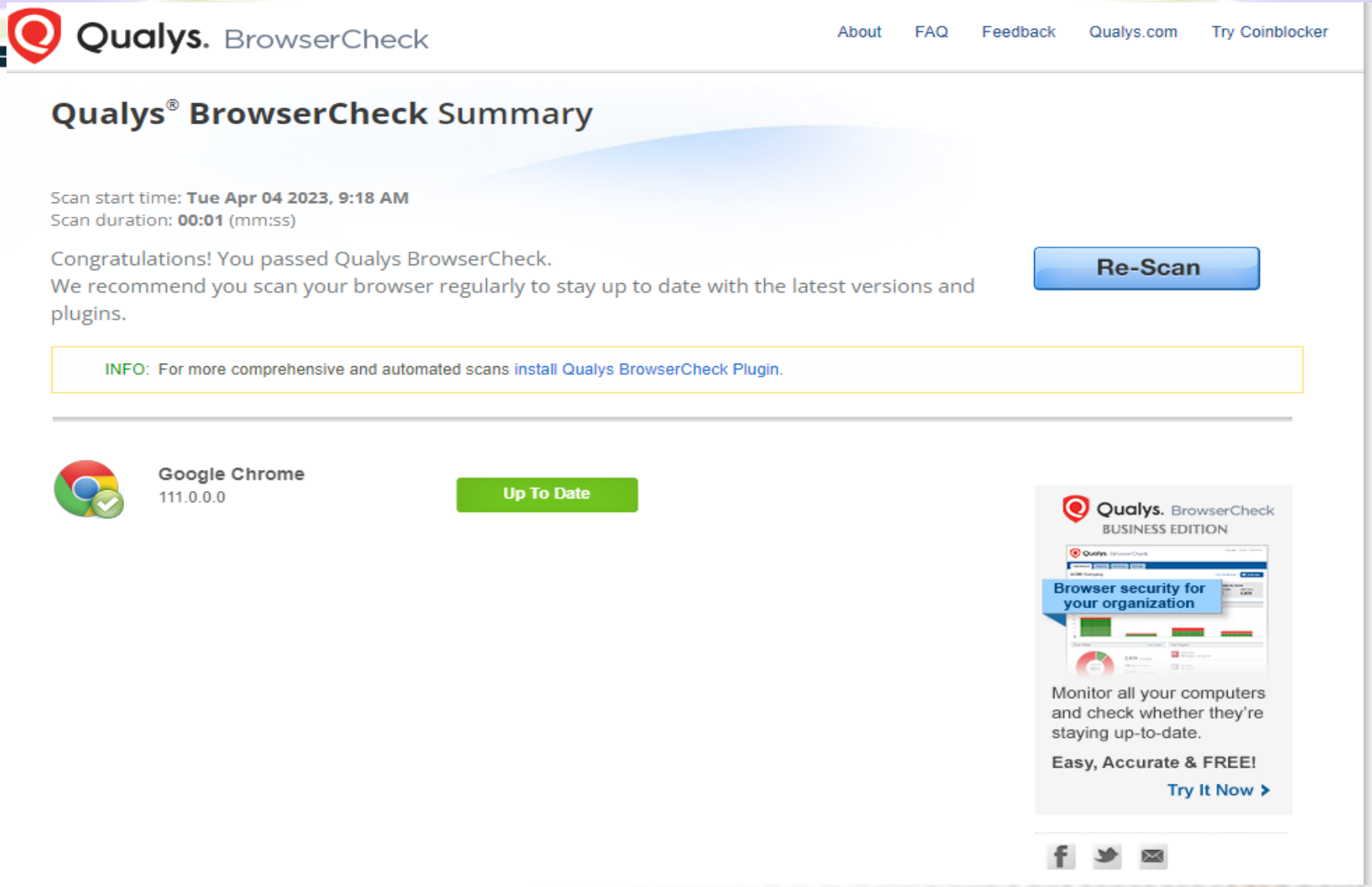
Qualys Demo - 1

- Lets take a look at Qualys Demo
- Free Qualys tools:
  - BrowserCheck
  - SSL
- Qualys FreeScan
  - Vulnerability
  - OWASP
  - Patch Tuesday
  - SCAP

Qualys Demo - 1



https://www.qualys.com/free-services/



https://www.qualys.com/free-services/

Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

HOW WELL DO YOU KNOW SSL?

If you want to learn more about the technology that protects the Internet, you've come to the right place.

Test your server »
Test your site's certificate and configuration

Test your browser »
Test your browser's SSL implementation

SSL Pulse »
See how other web sites are doing

Documentation »
Learn how to deploy SSL/TLS correctly

Books



Bulletproof SSL and TLS is a complete guide to deploying secure servers and web applications. This book, which provides comprehensive coverage of the ever-changing field of SSL/TLS and Web PKI, is intended for IT security professionals, system administrators, and developers, with the main focus on getting things done. MORE »

News

LinkedIn Faux Pas Shines Light on Certificate Management
May 24, 2019

Zombie POODLE and GOLDENDOODLE Vulnerabilities
April 22, 2019

PCI & SSL/Early TLS QIDs 38601, 42366
March 14, 2019

About SSL Labs

SSL Labs is a collection of documents, tools and thoughts related to SSL. It's an attempt to better understand how SSL is deployed, and an attempt to make it better. I hope that, in time, SSL Labs will grow into a forum where SSL will be discussed and improved.

SSL Labs is a non-commercial research effort, and we welcome participation from any individual and organization interested in SSL.

-- *Ivan Ristić, Qualys*

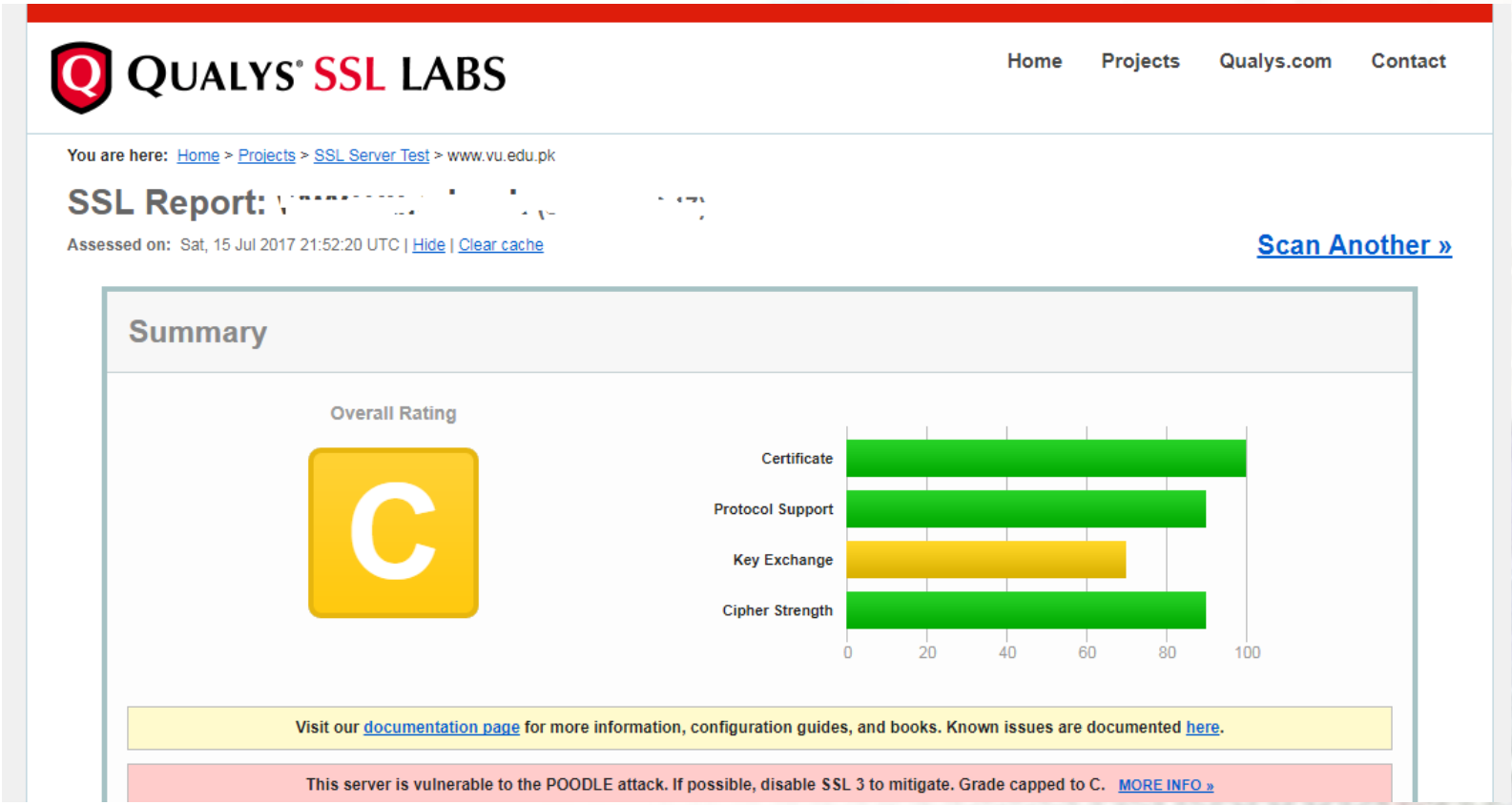
Copyright © 2009-2023 Qualys, Inc. All Rights Reserved.

Terms and Conditions

Try Qualys for free! Experience the award-winning Qualys Cloud Platform and the entire collection of Qualys Cloud Apps, including certificate security solutions.

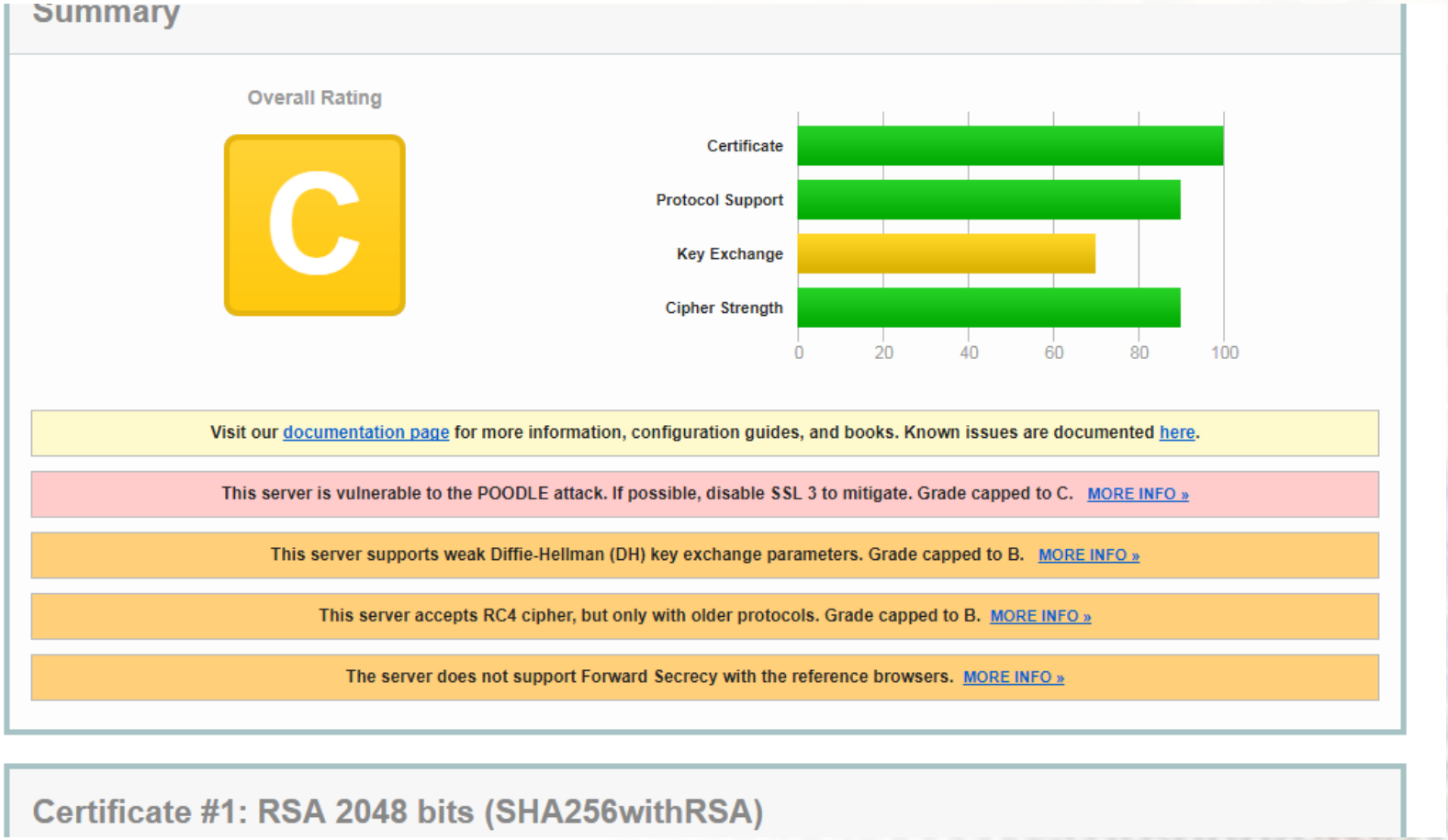
Qualys Demo - 1

SSL LABS REPORT



Qualys Demo - 1

SSL LABS REPORT



https://www.qualys.com/free-services/
https://www.ssllabs.com/

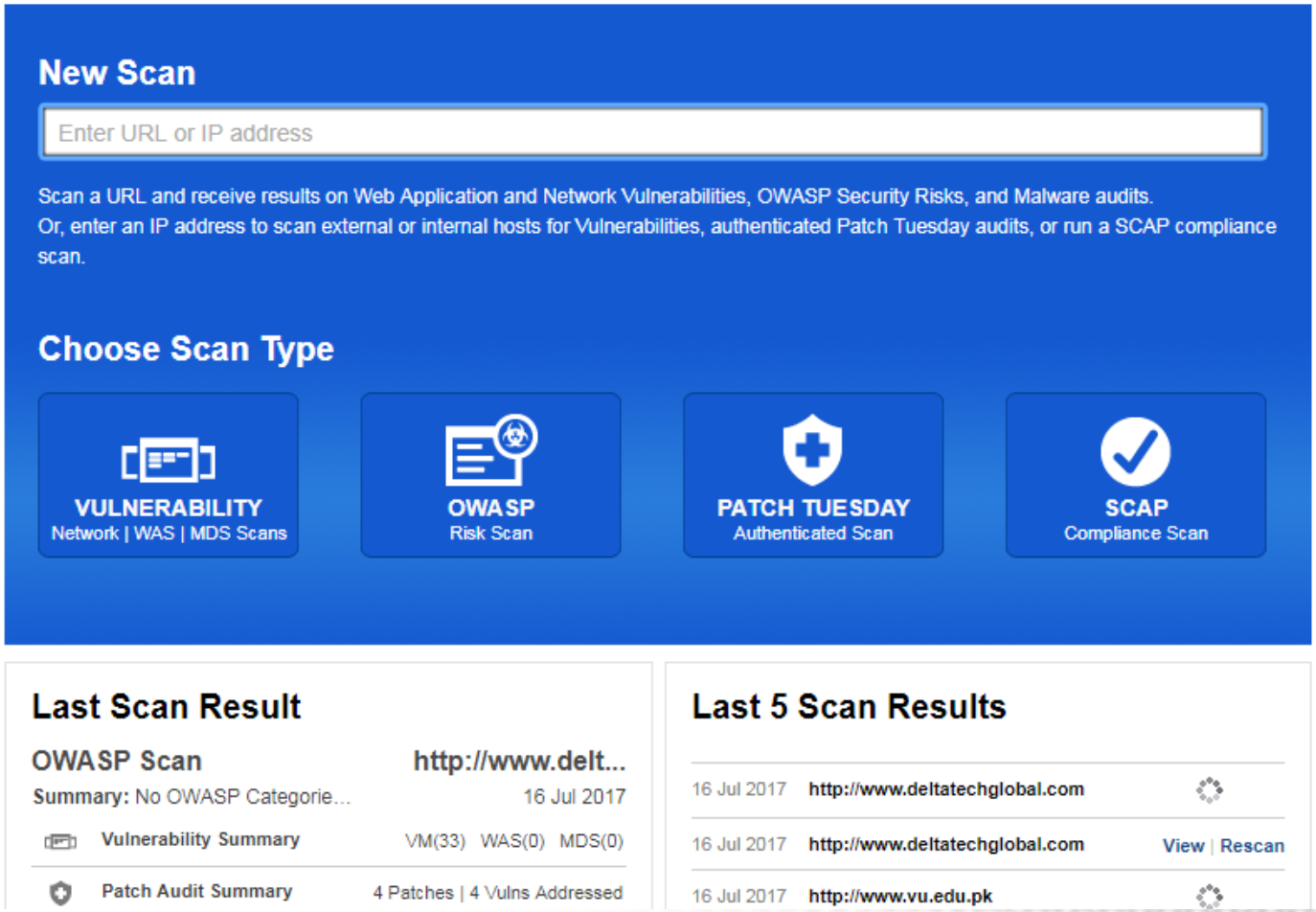
Qualys Demo - 1

PROTOCOL DETAILS

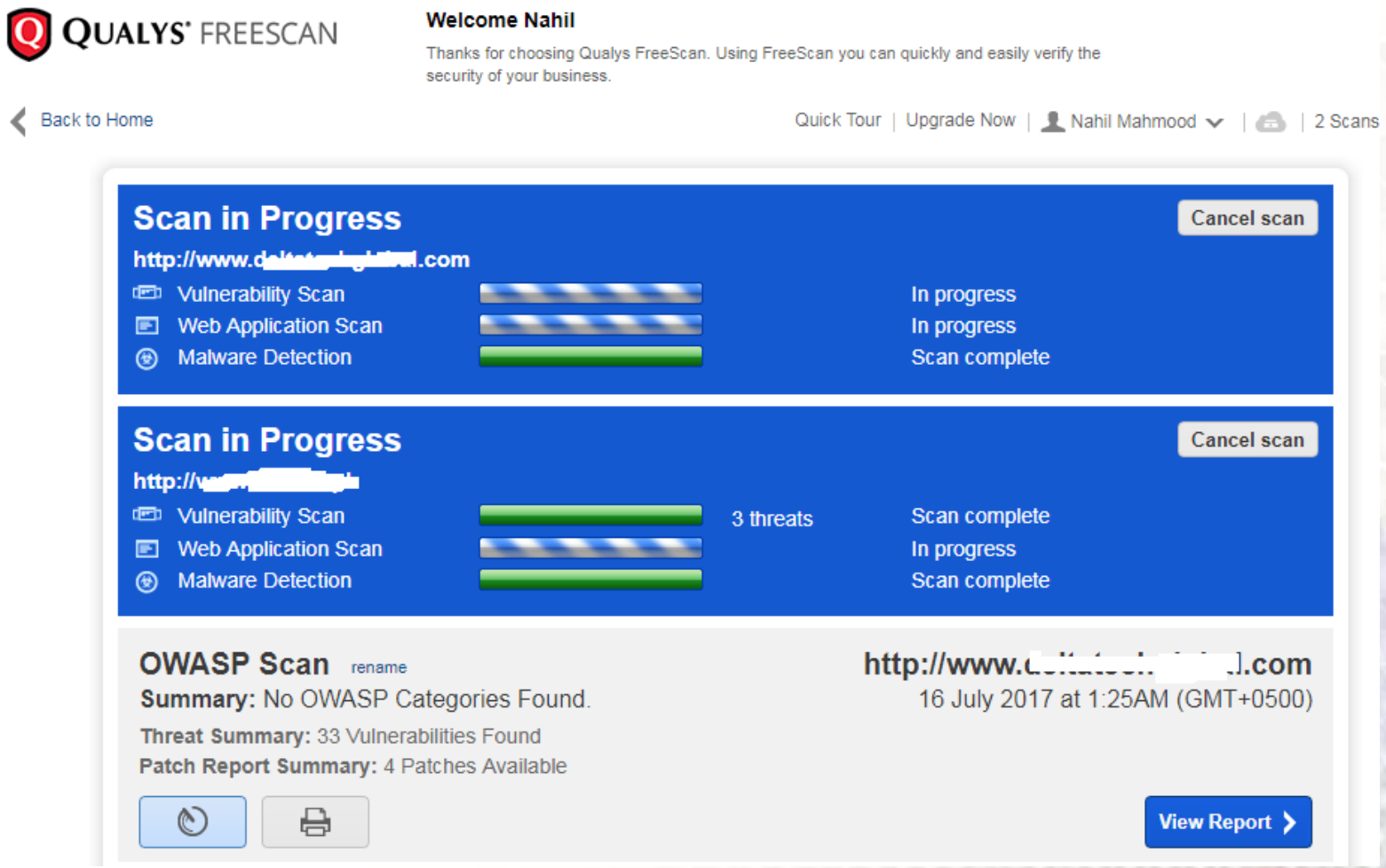
BEAST attack	Not mitigated server-side (more info) SSL 3: 0xa, TLS 1.0: 0xc014
POODLE (SSLv3)	Vulnerable INSECURE (more info) SSL 3: 0xa
POODLE (TLS)	No (more info)
Downgrade attack prevention	No, TLS_FALLBACK_SCSV not supported (more info)
SSL/TLS compression	No
RC4	Yes INSECURE (more info)
Heartbeat (extension)	No
Heartbleed (vulnerability)	No (more info)
Ticketbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)
Forward Secrecy	Weak key exchange WEAK
ALPN	No

Qualys Demo - 1

QUALYS FREESCAN

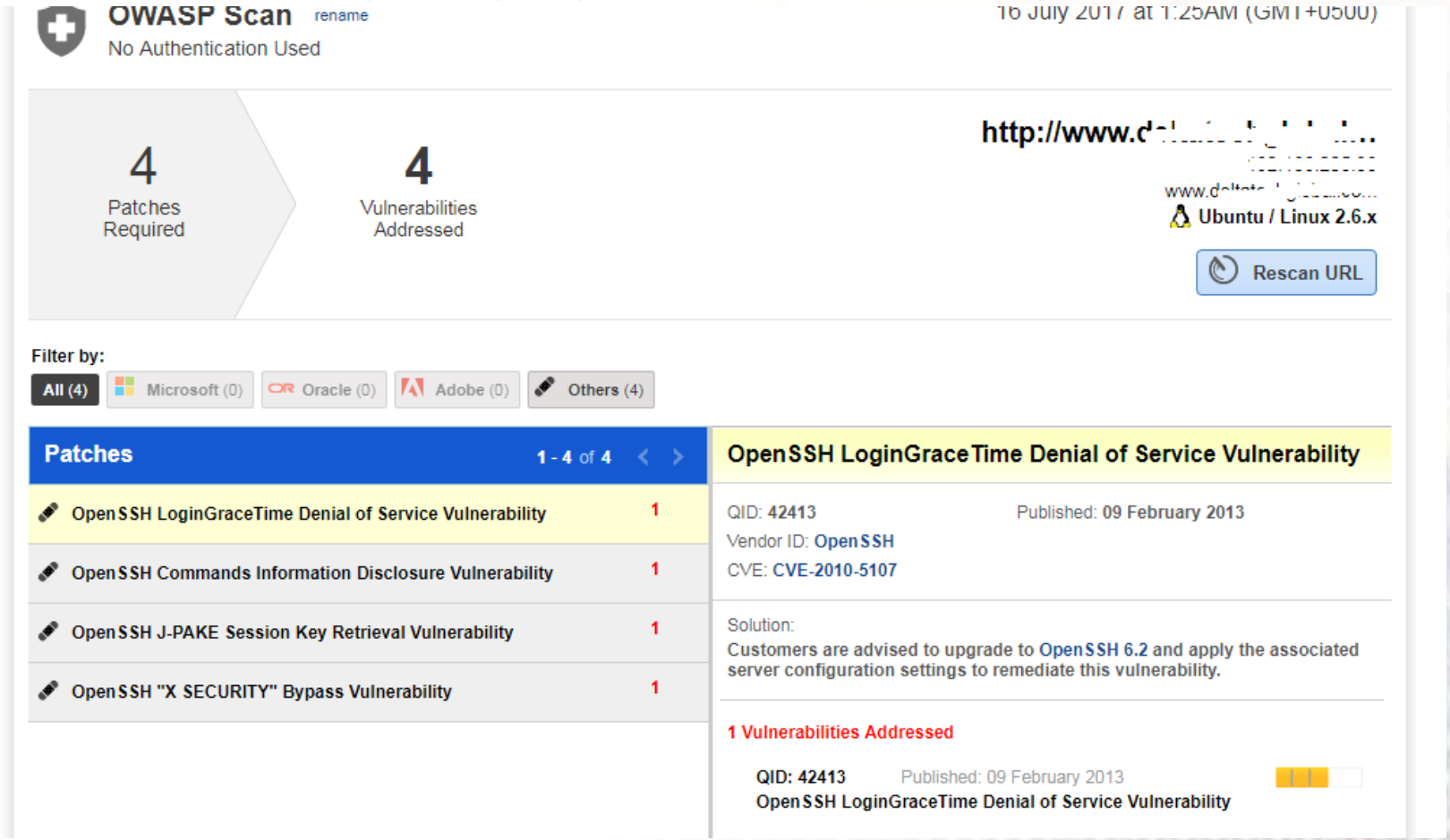


Qualys Demo - 1



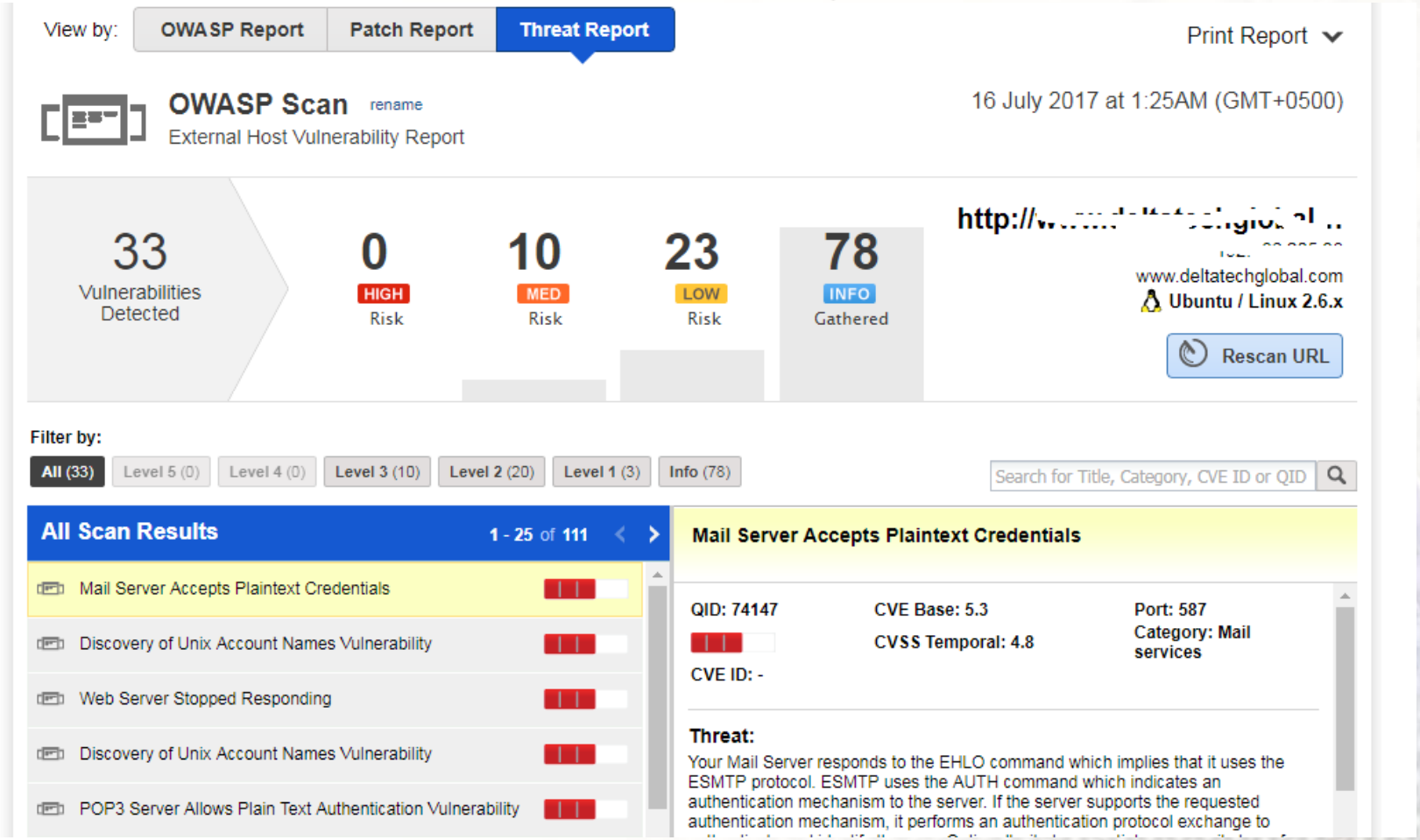
Qualys Demo - 1

OWASP SCAN PATCH REPORT



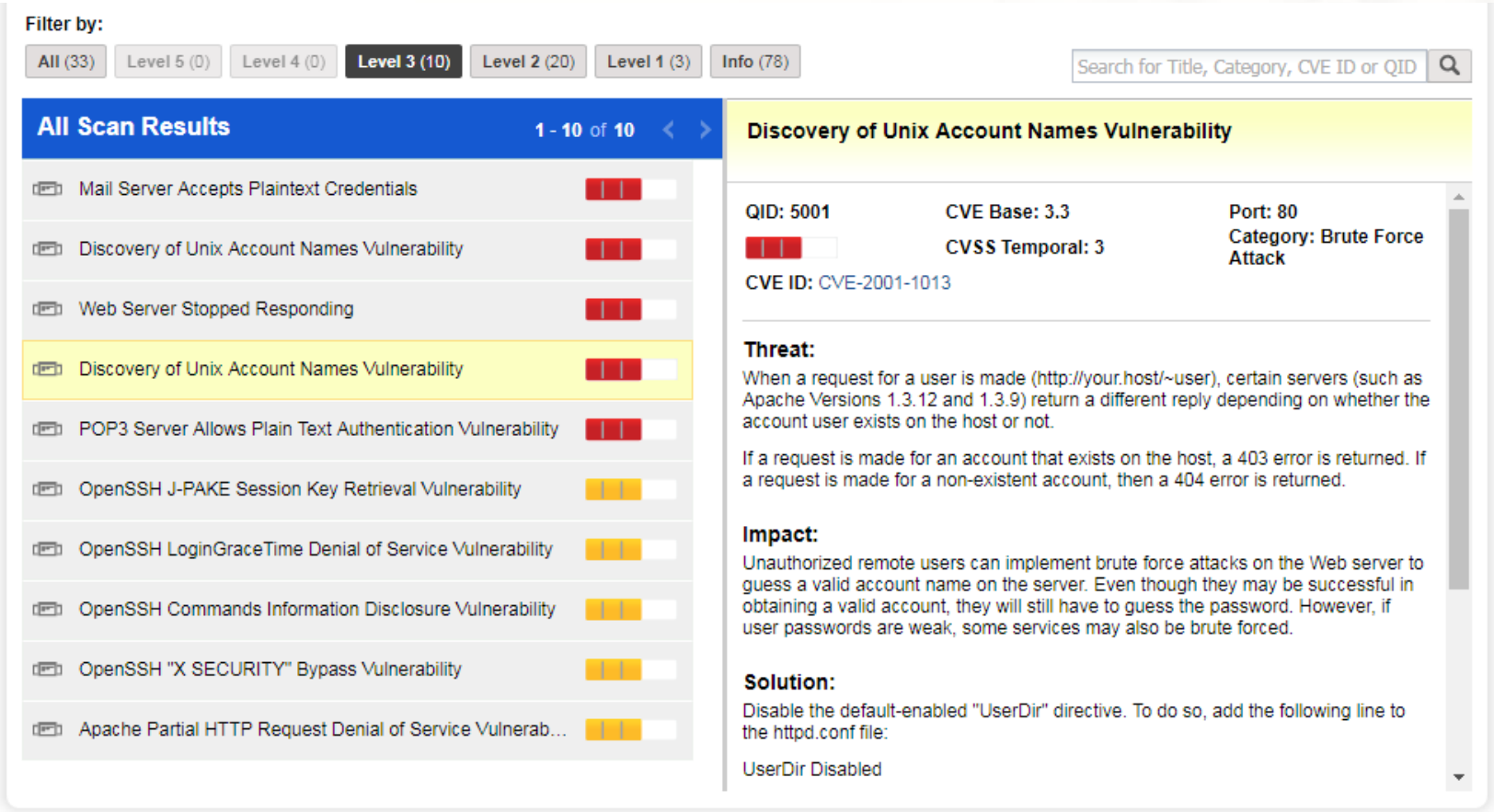
Qualys Demo - 1

THREAT REPORT



Qualys Demo - 1

THREAT REPORT



Qualys Demo - 1

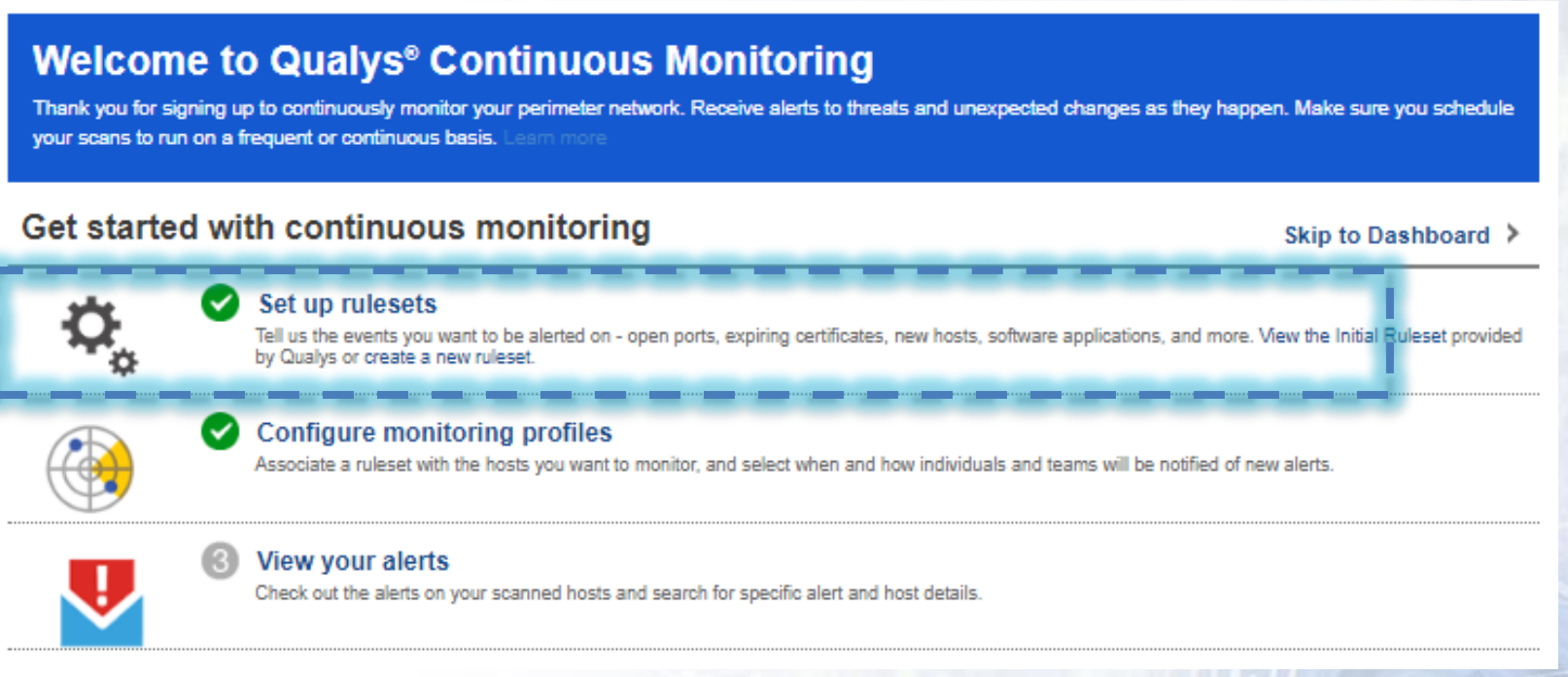
- Qualys is a powerful cloud-based vulnerability management tool
- Several online free tools
- Advanced web application security testing

END

QUALYS DEMO - PART 3

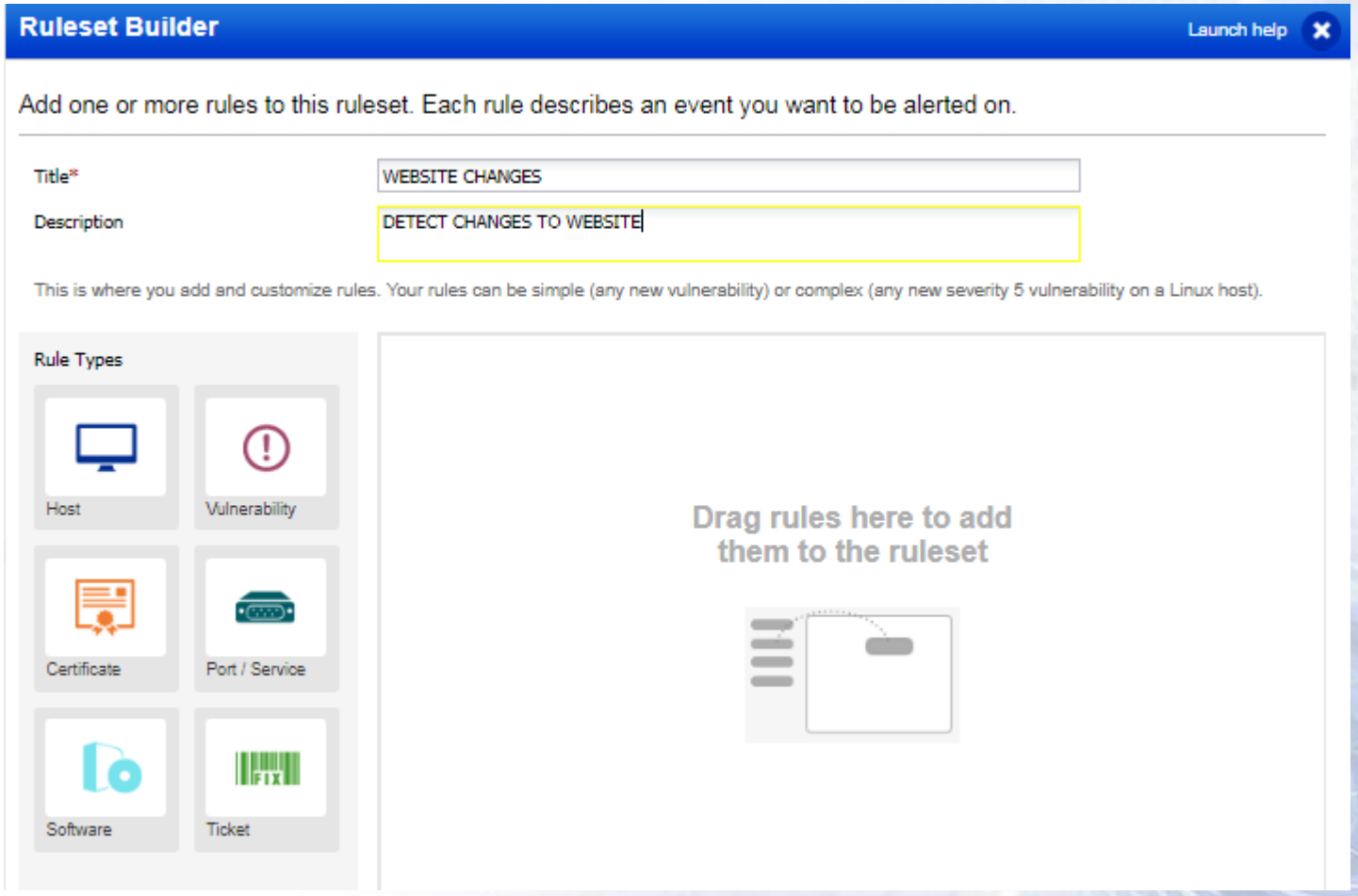
- Lets have a look at some further features of Qualys:
- Qualys Continuous Monitoring

QUALYS DEMO - PART 3



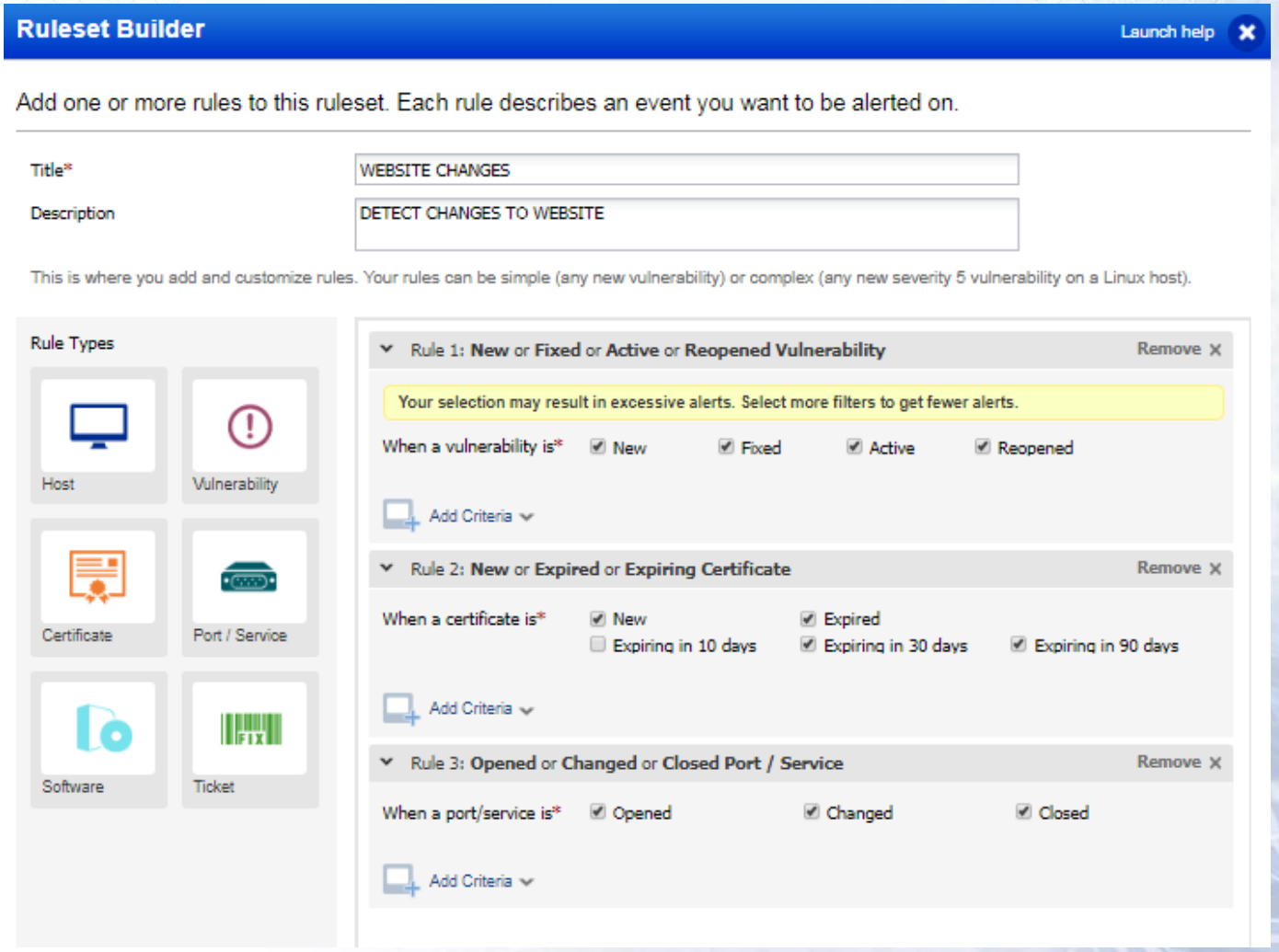
QUALYS CONTINUOUS MONITORING INTERFACE

QUALYS DEMO - PART 3



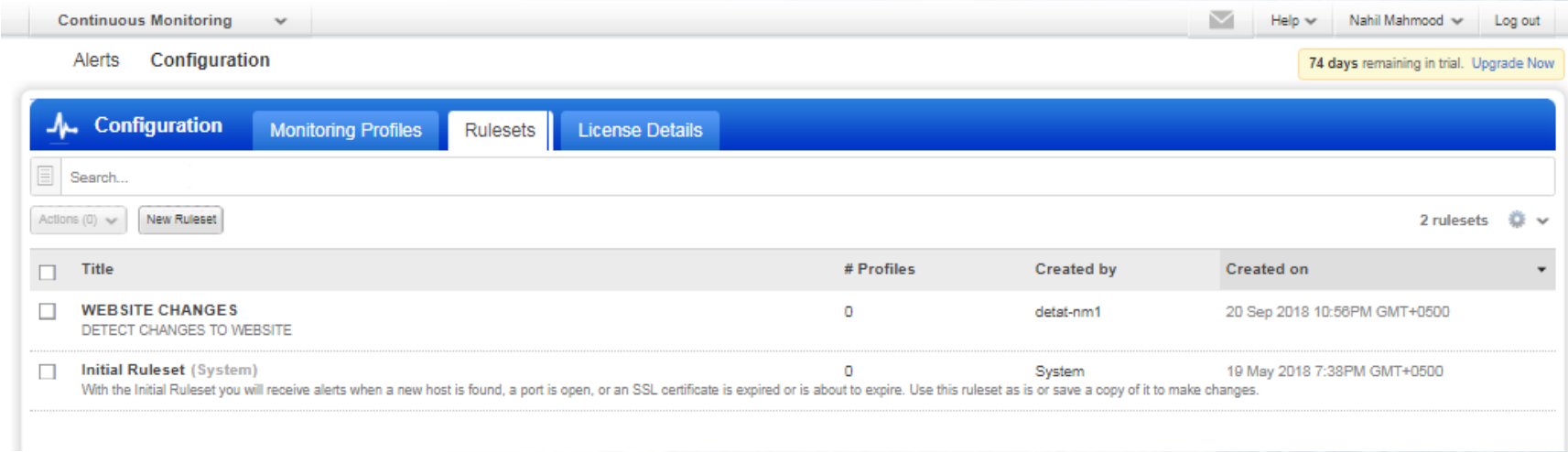
RULESET BUILDER

QUALYS DEMO - PART 3



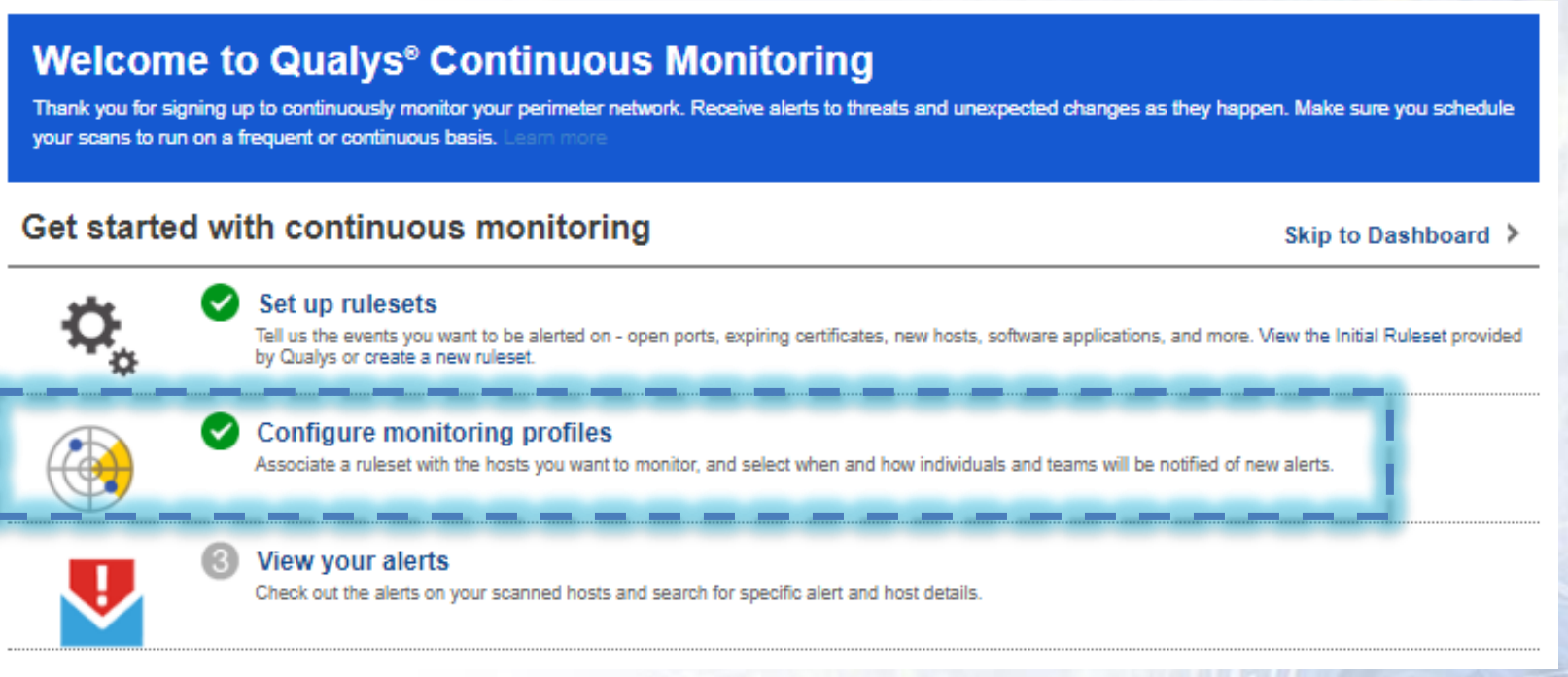
RULETYPES & CONFIGURATION

QUALYS DEMO - PART 3



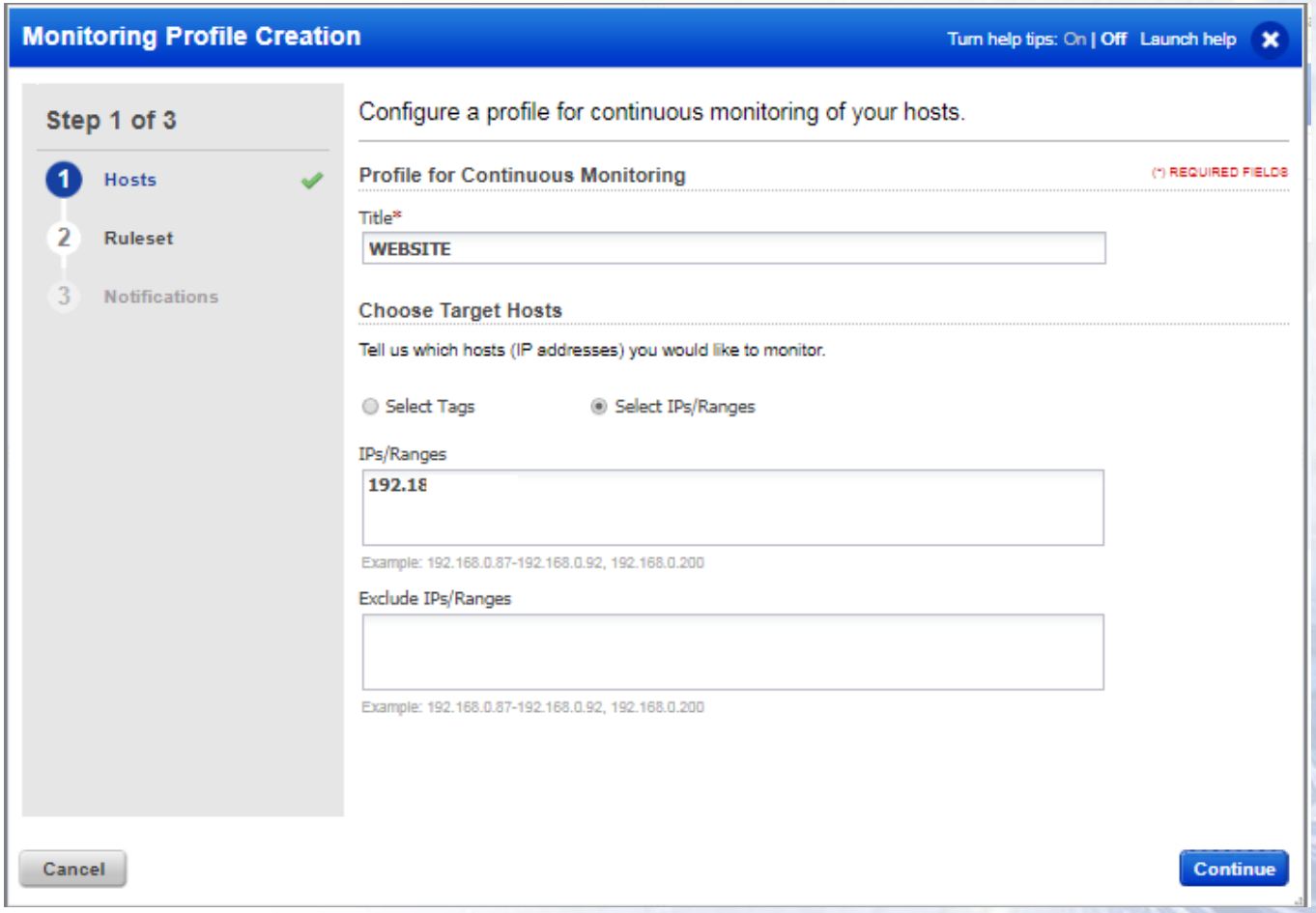
RULESETS INTERFACE

QUALYS DEMO - PART 3



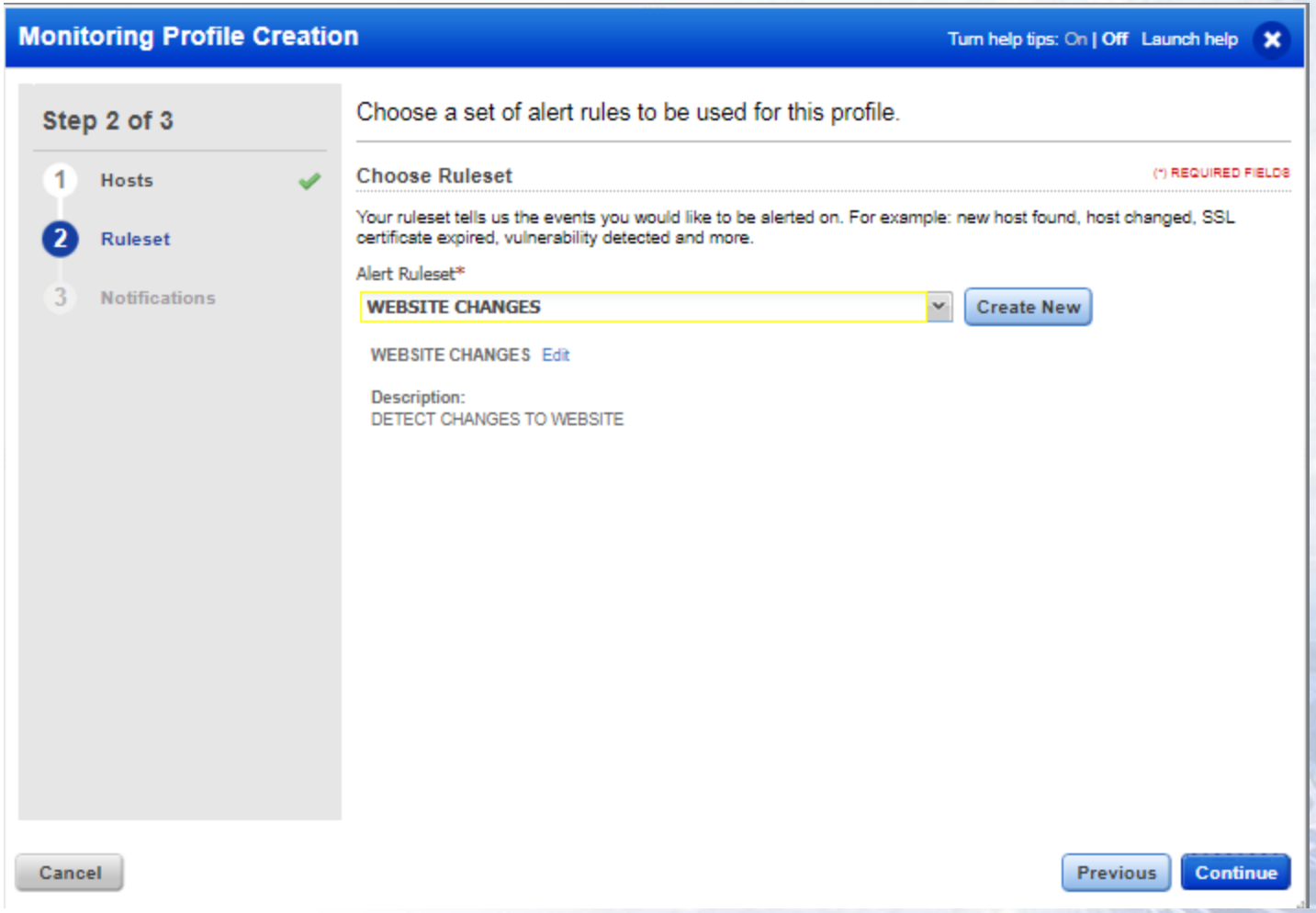
QUALYS CONTINUOUS MONITORING INTERFACE

QUALYS DEMO - PART 3



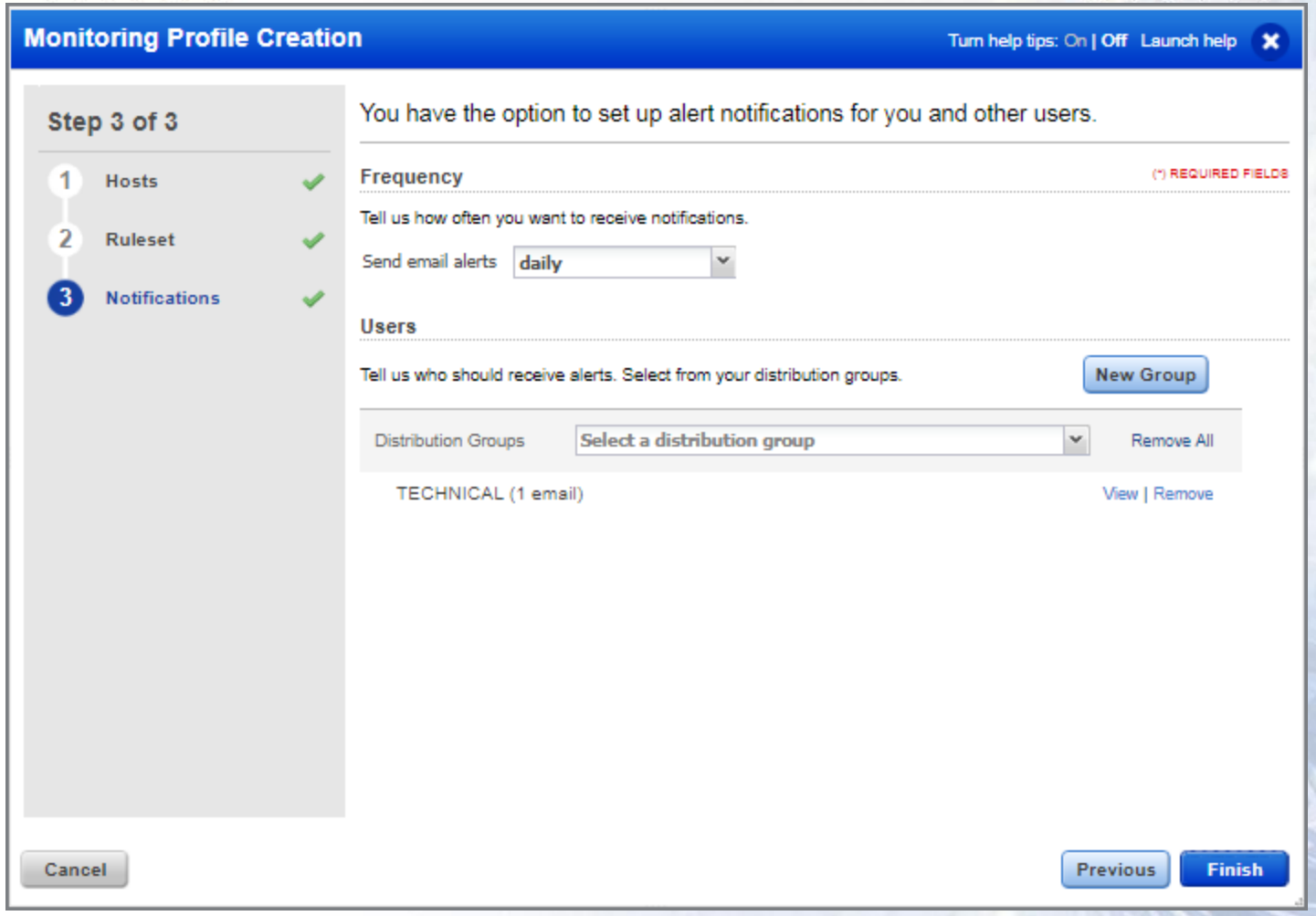
PROFILE CREATION

QUALYS DEMO - PART 3



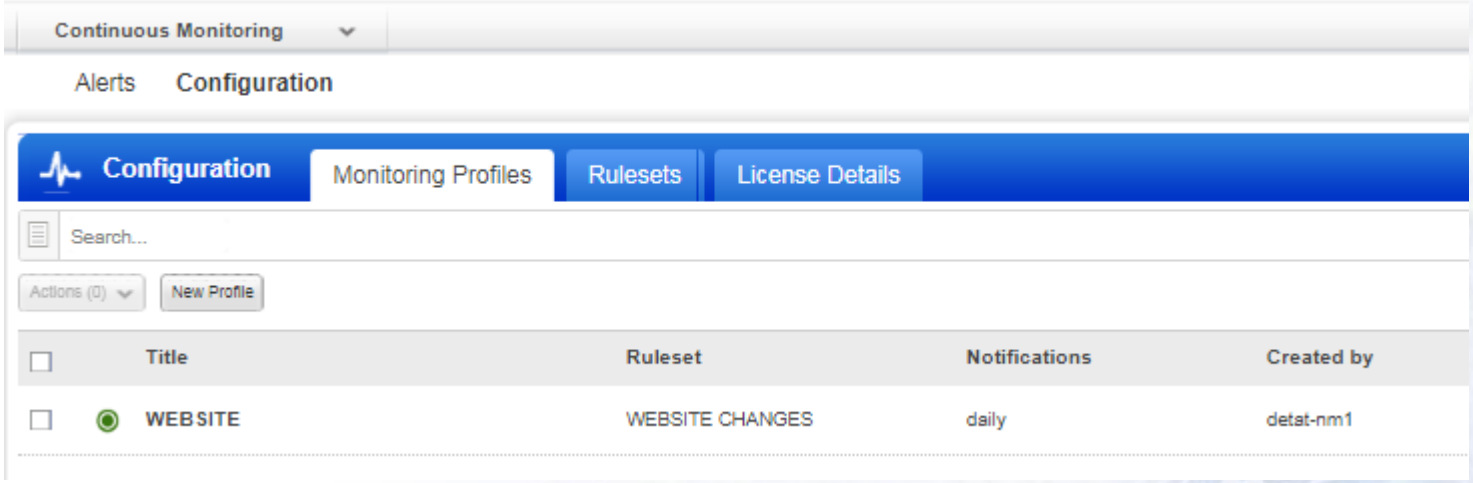
CHOOSE RULESET

QUALYS DEMO - PART 3



NOTIFICATIONS

QUALYS DEMO - PART 3



MONITORING PROFILE ACTIVE

QUALYS DEMO - PART 3

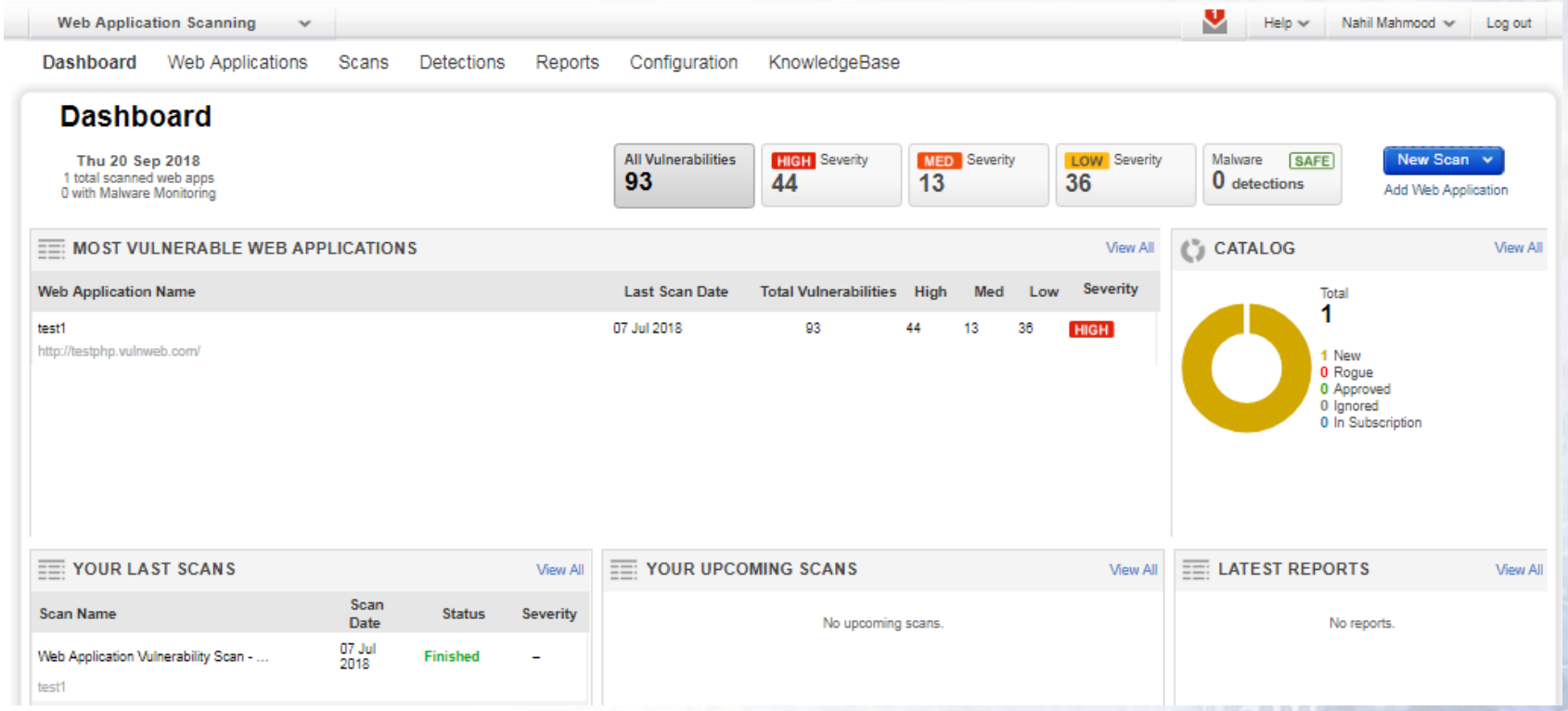
- Qualys Continuous Monitoring is very useful for watching critical changes that may impact security

END

QUALYS WEB APPLICATION SCANNING

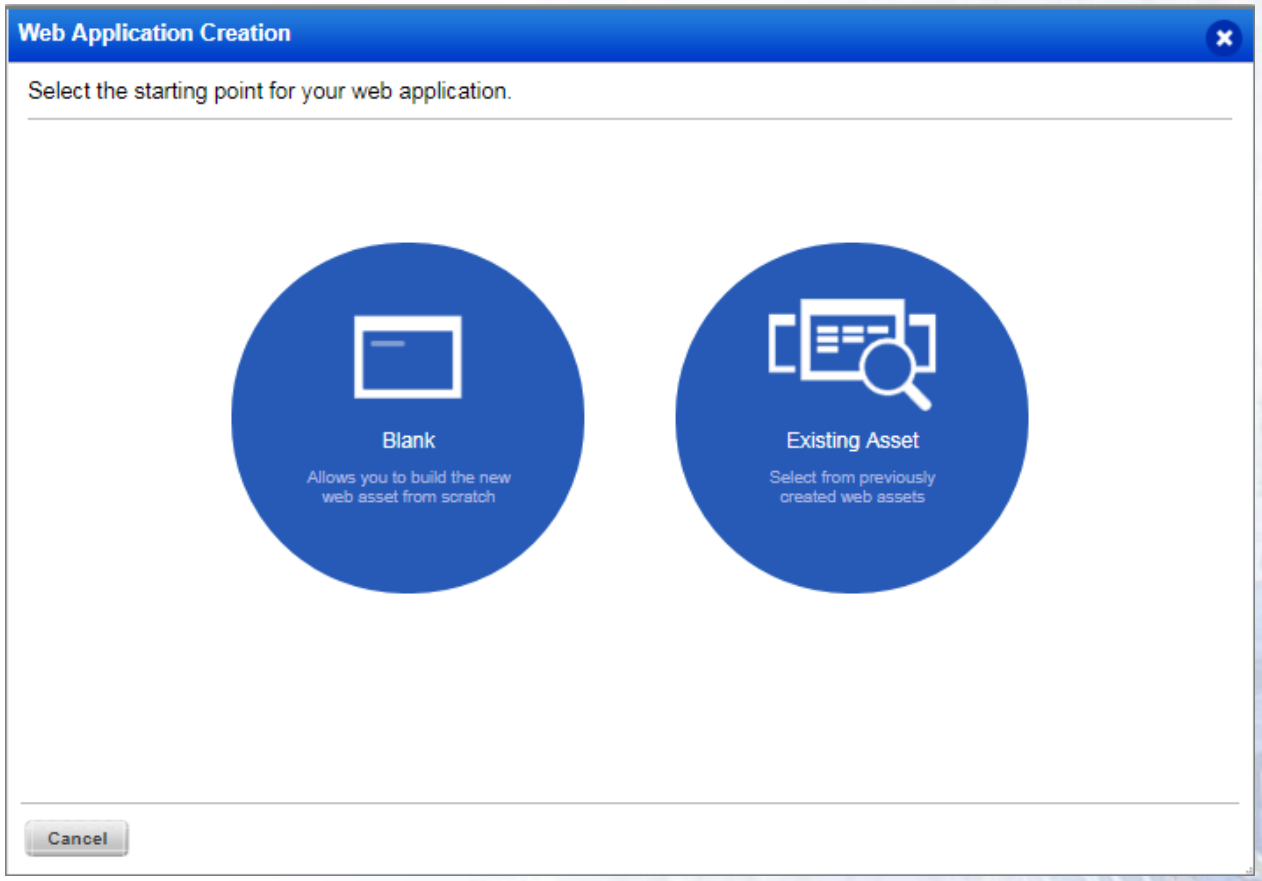
- Lets have a look at Qualys Web Application Scanning

QUALYS WEB APPLICATION SCANNING



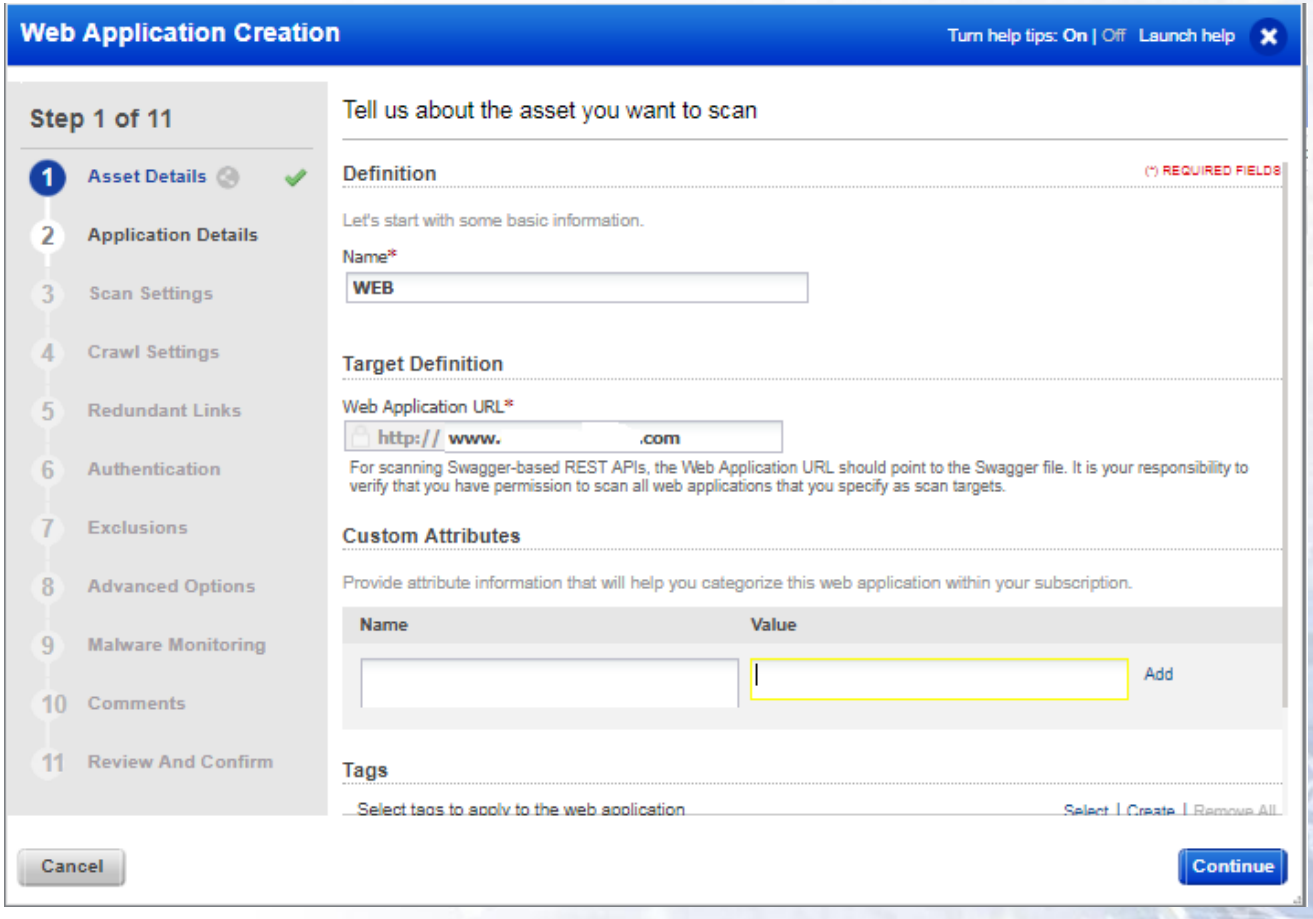
DASHBOARD

QUALYS WEB APPLICATION SCANNING



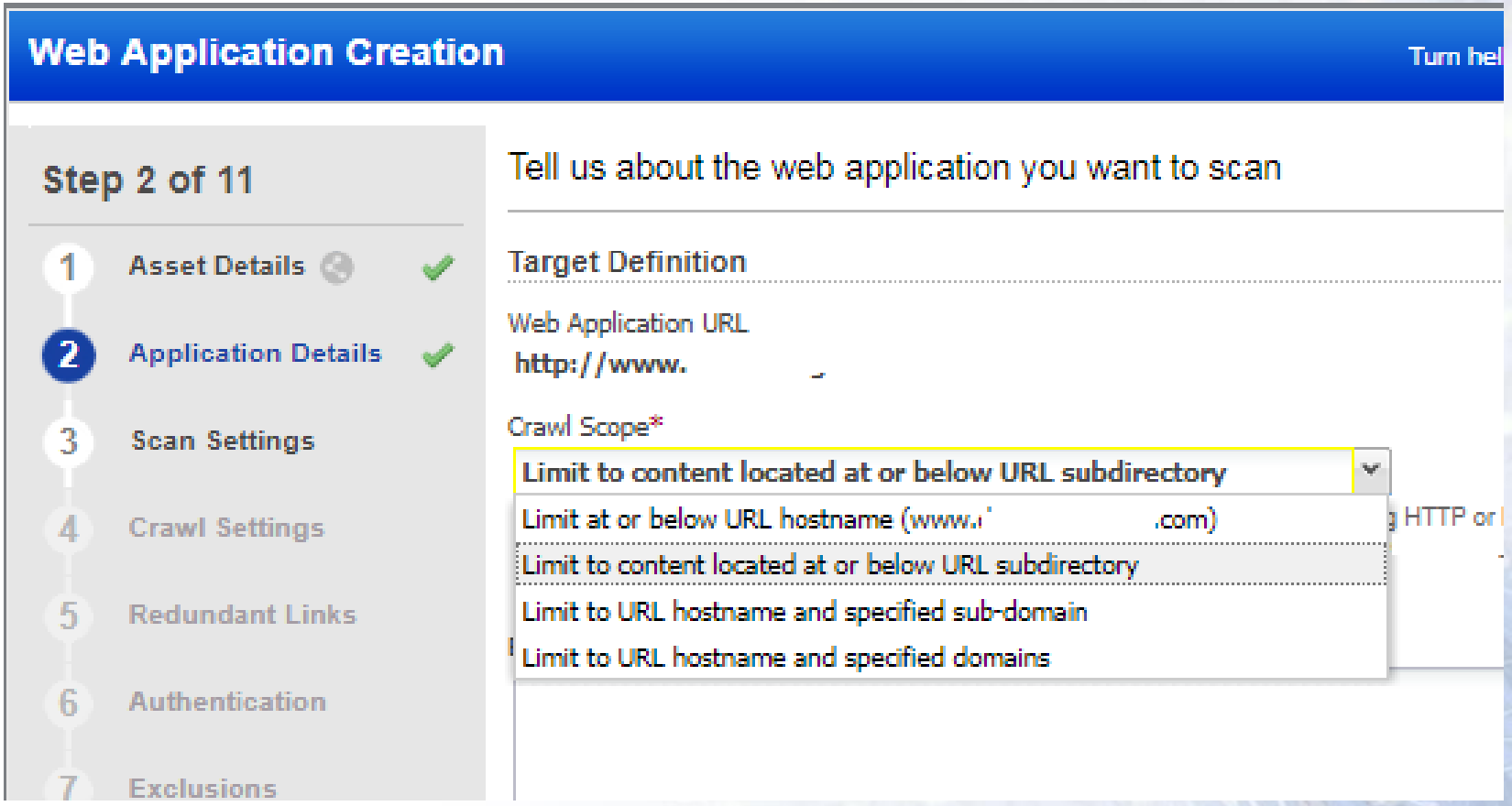
CREATION – BLANK OR EXISTING ASSET

QUALYS WEB APPLICATION SCANNING



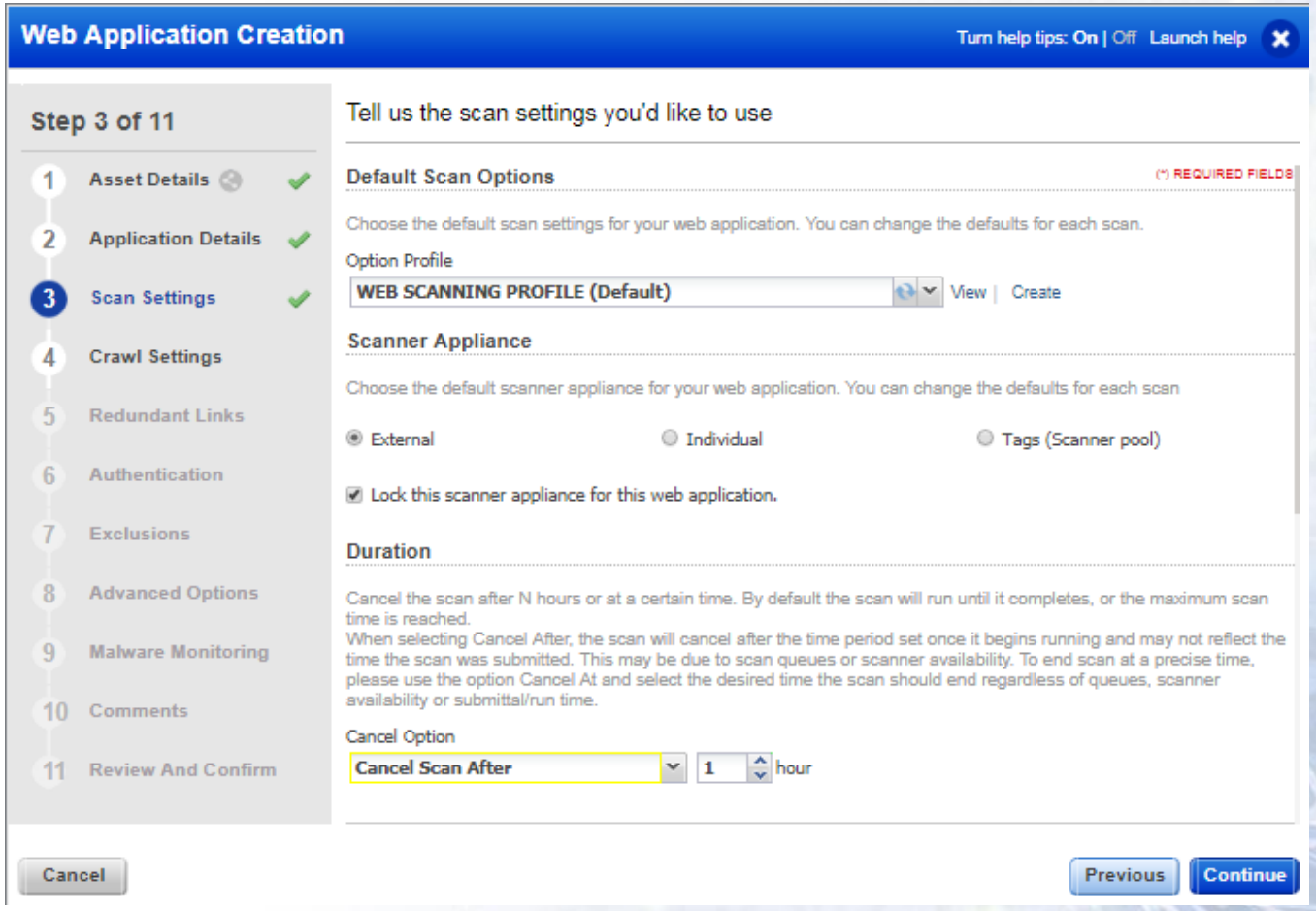
ASSET DETAILS

QUALYS WEB APPLICATION SCANNING



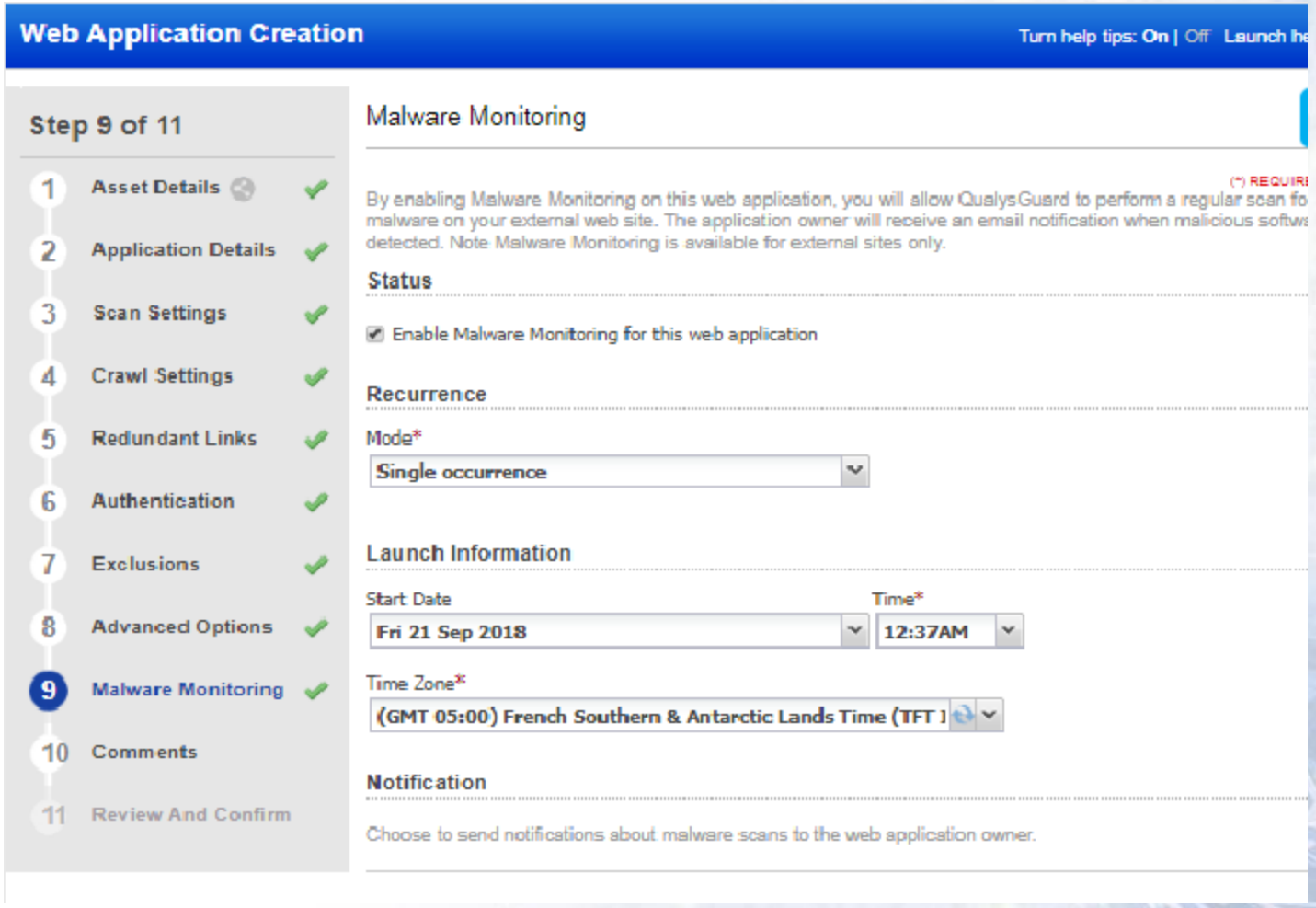
CRAWL SCOPE

QUALYS WEB APPLICATION SCANNING



SCAN SETTINGS

QUALYS WEB APPLICATION SCANNING

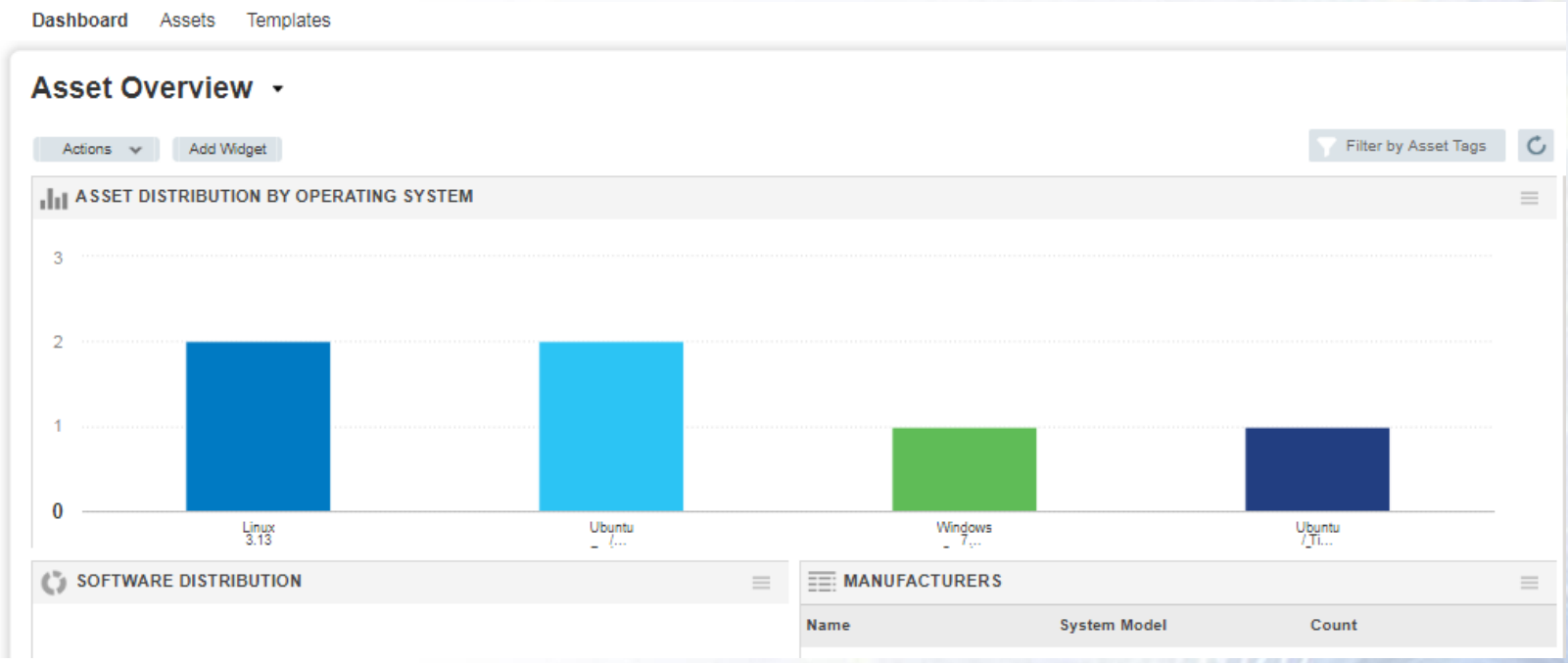


MALWARE MONITORING

ASSET MANAGEMENT THROUGH QUALYS

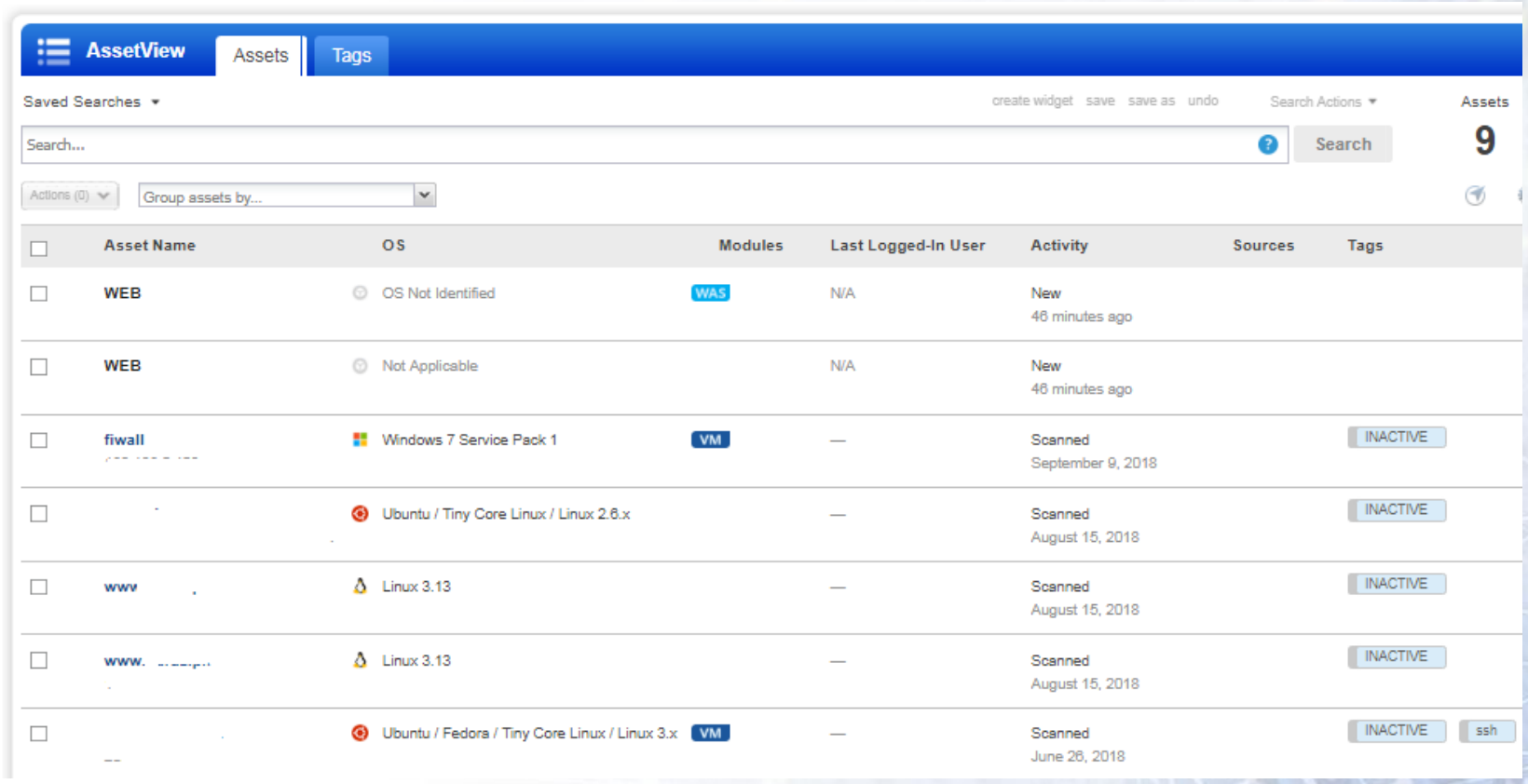
- Lets have a look at Qualys asset management capabilities

ASSET MANAGEMENT THROUGH QUALYS



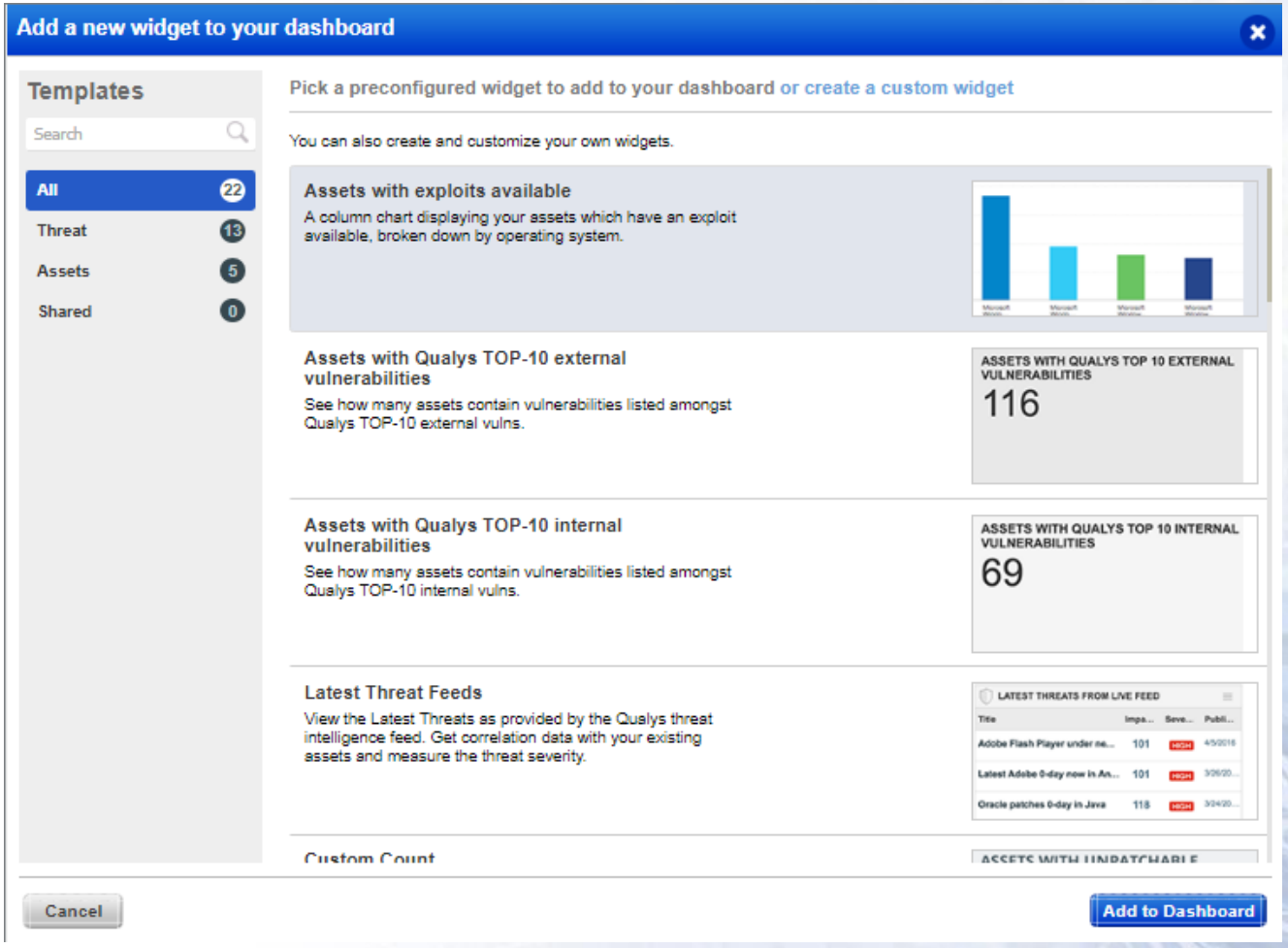
QUALYS ASSET OVERVIEW DASHBOARD

ASSET MANAGEMENT THROUGH QUALYS



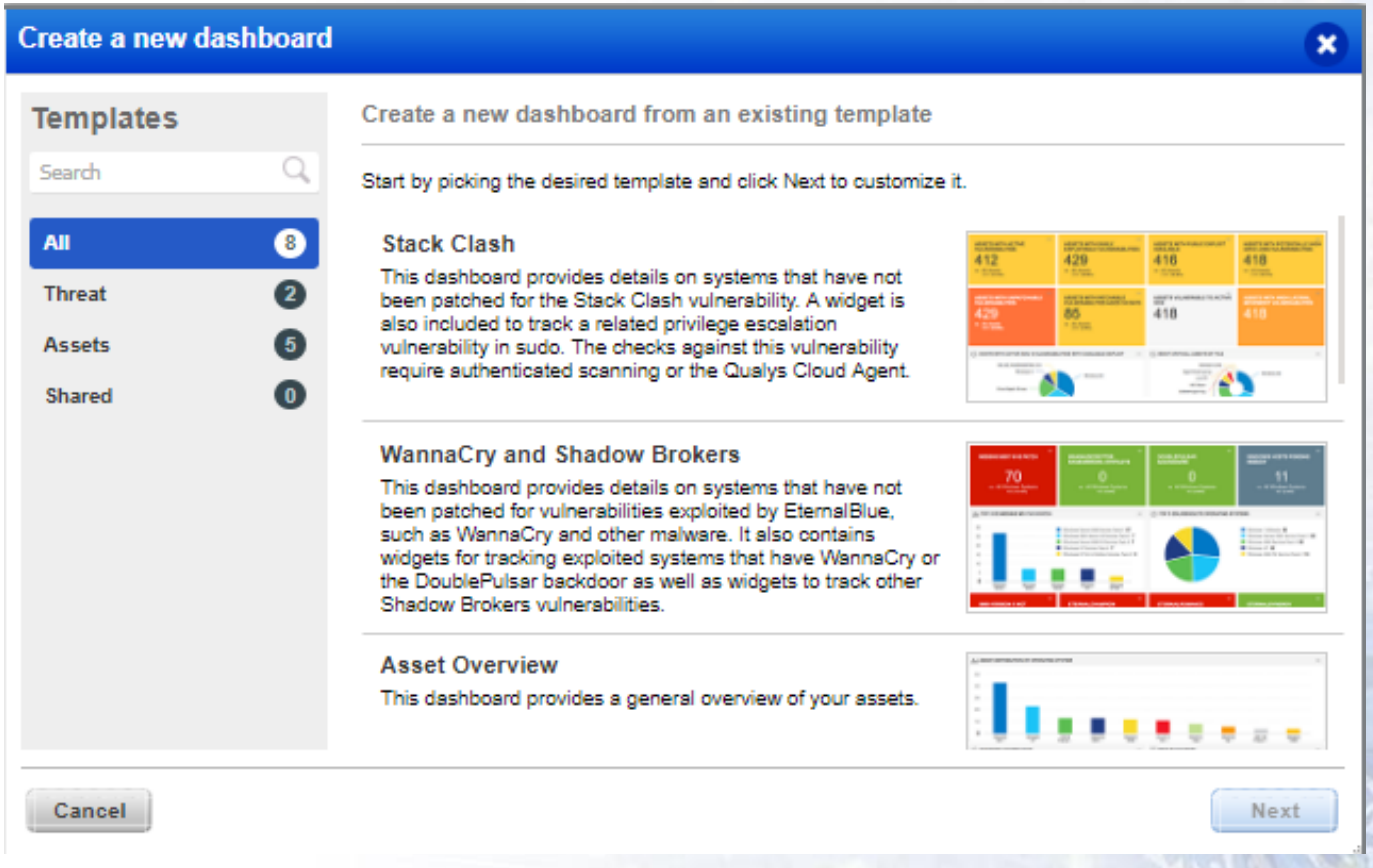
ASSETS LIST

ASSET MANAGEMENT THROUGH QUALYS



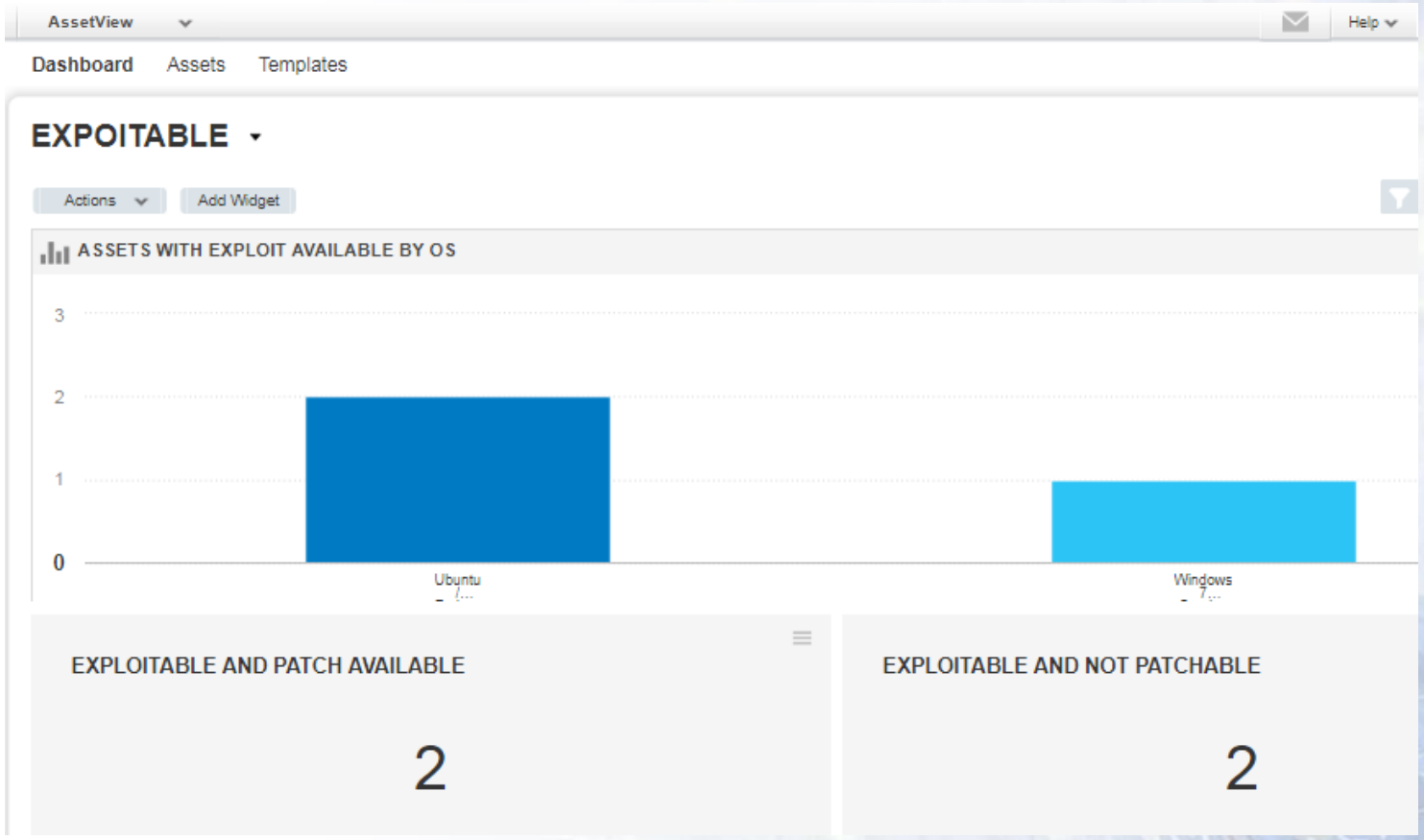
ADD NEW ASSET WIDGET TO DASHBOARD

ASSET MANAGEMENT THROUGH QUALYS



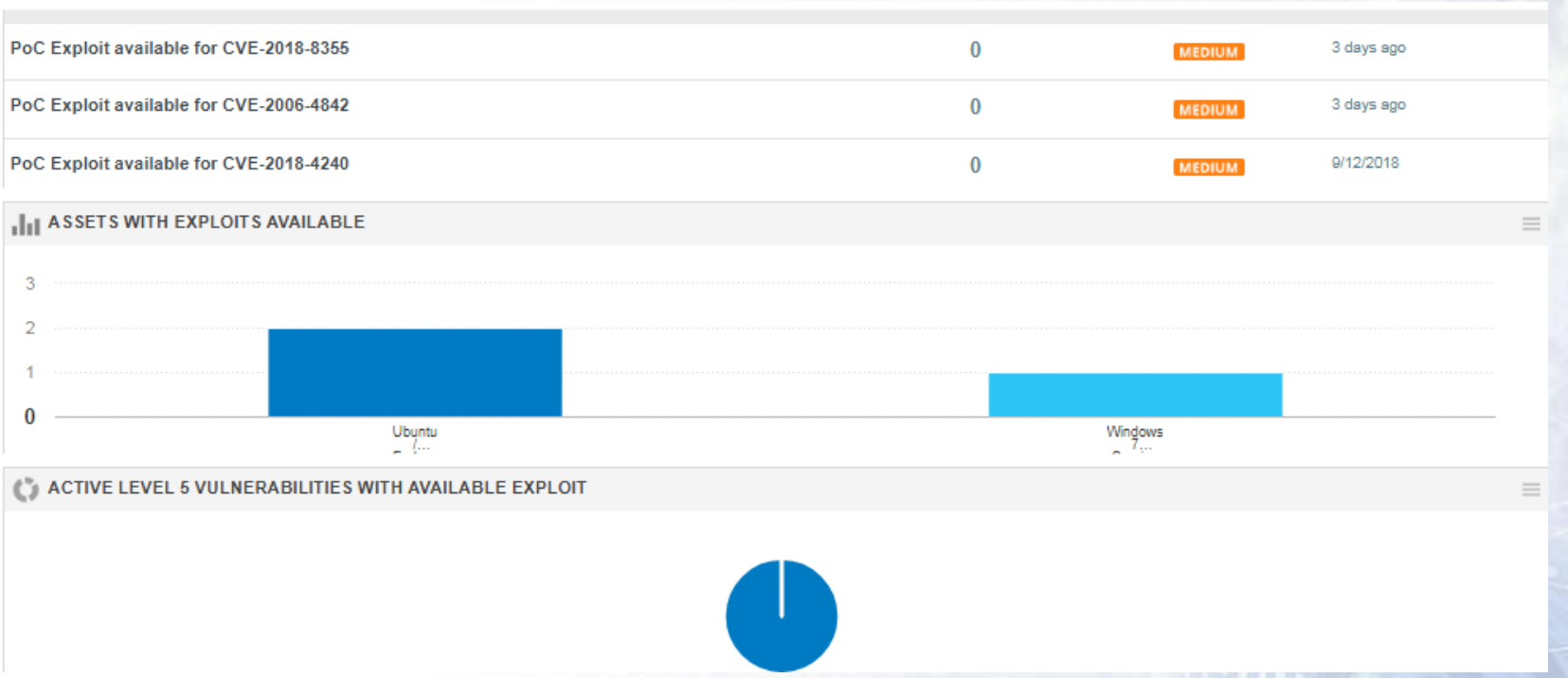
CREATE A NEW DASHBOARD

ASSET MANAGEMENT THROUGH QUALYS



NEW DASHBOARD CREATED

ASSET MANAGEMENT THROUGH QUALYS



ASSETS WITH EXPLOITS AVAILABLE

ASSET MANAGEMENT THROUGH QUALYS

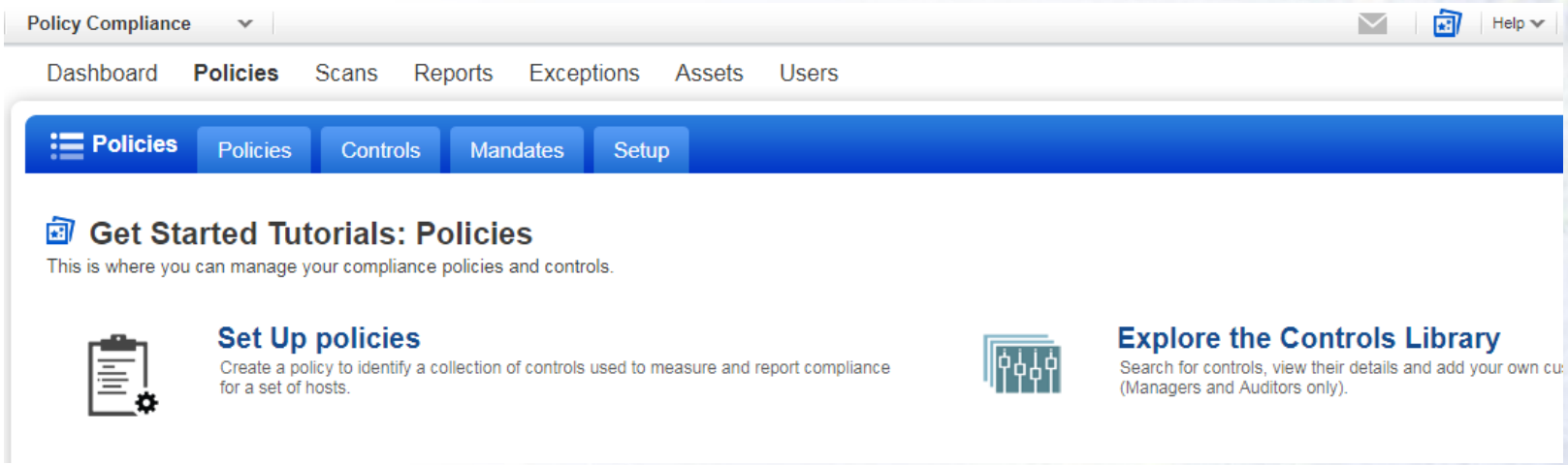
- Qualys allows various reporting and views on assets and their characteristics

END

QUALYS POLICY LIBRARIES

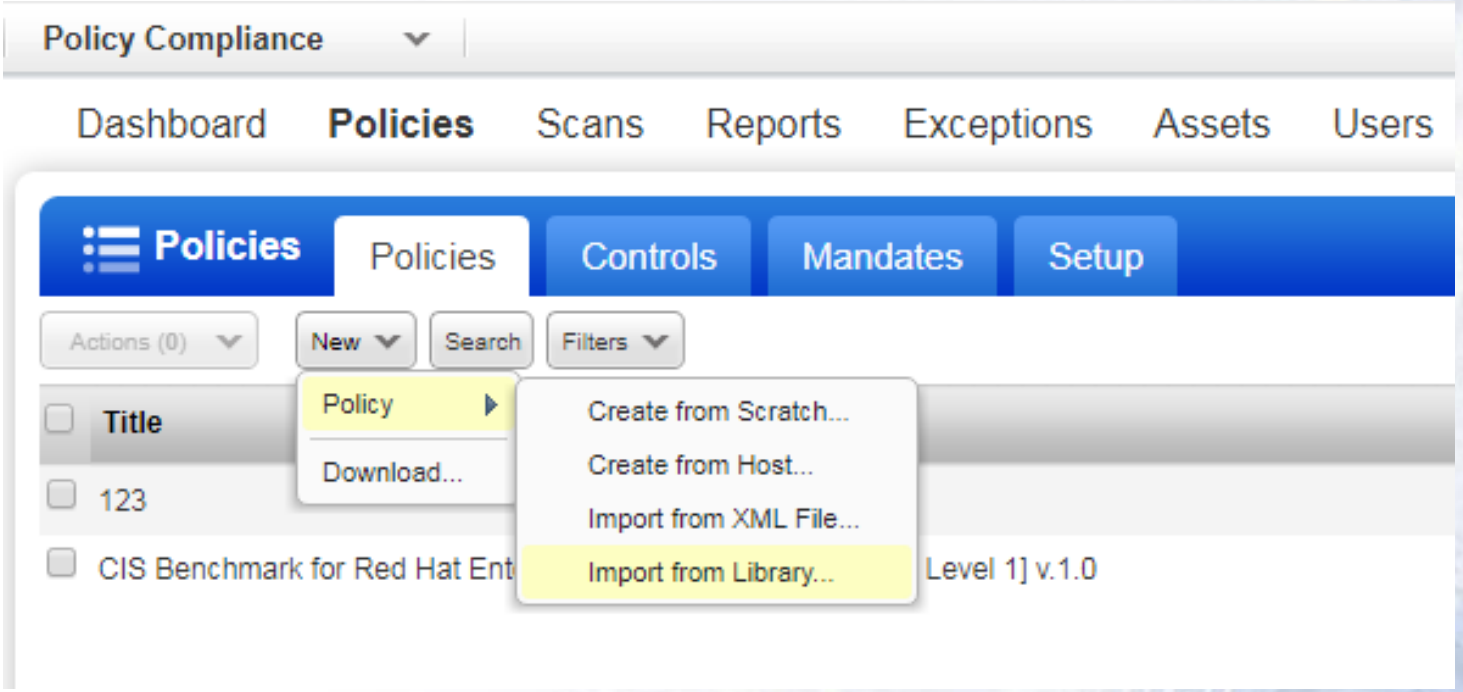
- Lets have a detailed look at Qualys built-in libraries for creating scanning policies
- CIS
- QUALYS
- MANDATE
- DISA
- VENDOR

QUALYS POLICY LIBRARIES



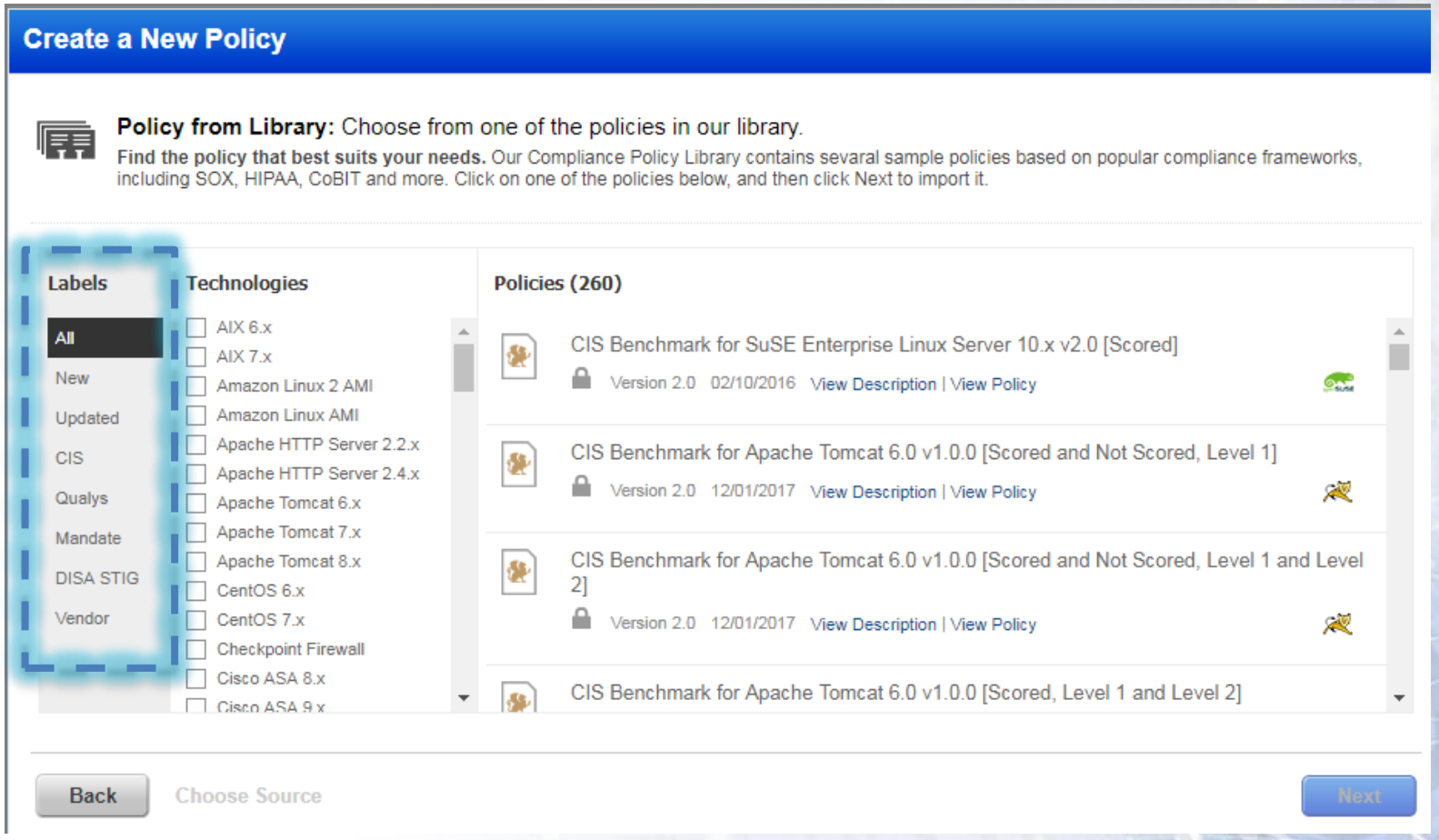
EXPLORE THE CONTROLS LIBRARY

QUALYS POLICY LIBRARIES



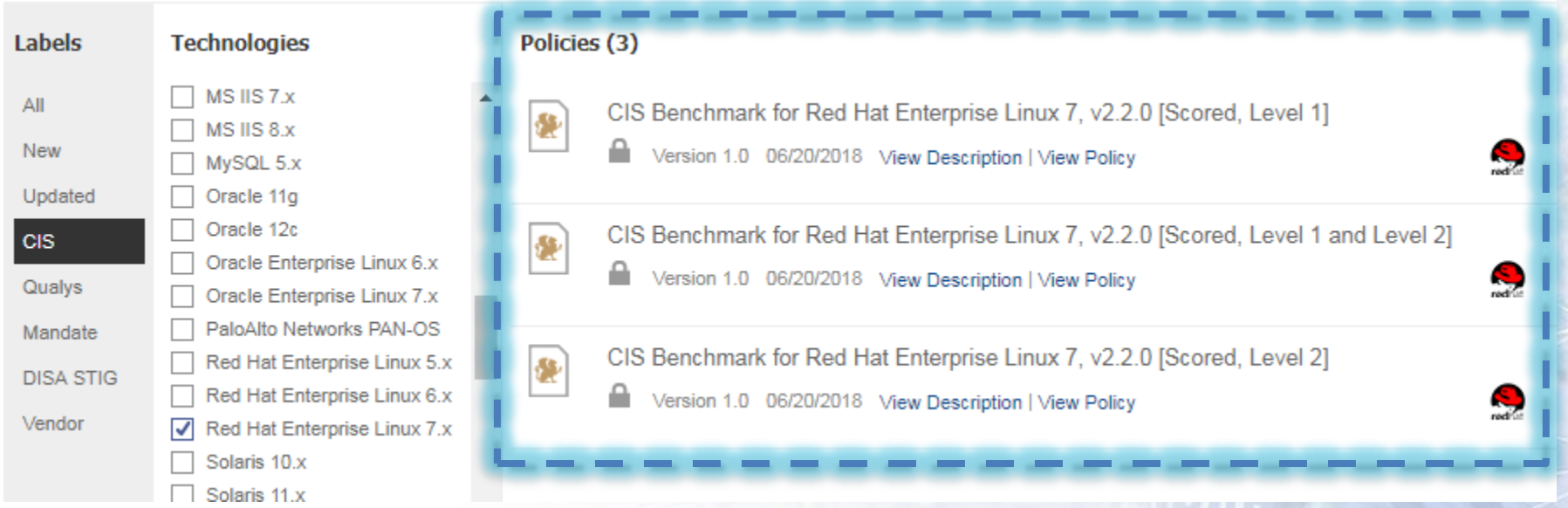
CREATE NEW POLICY > IMPORT FROM LIBRARY

QUALYS POLICY LIBRARIES



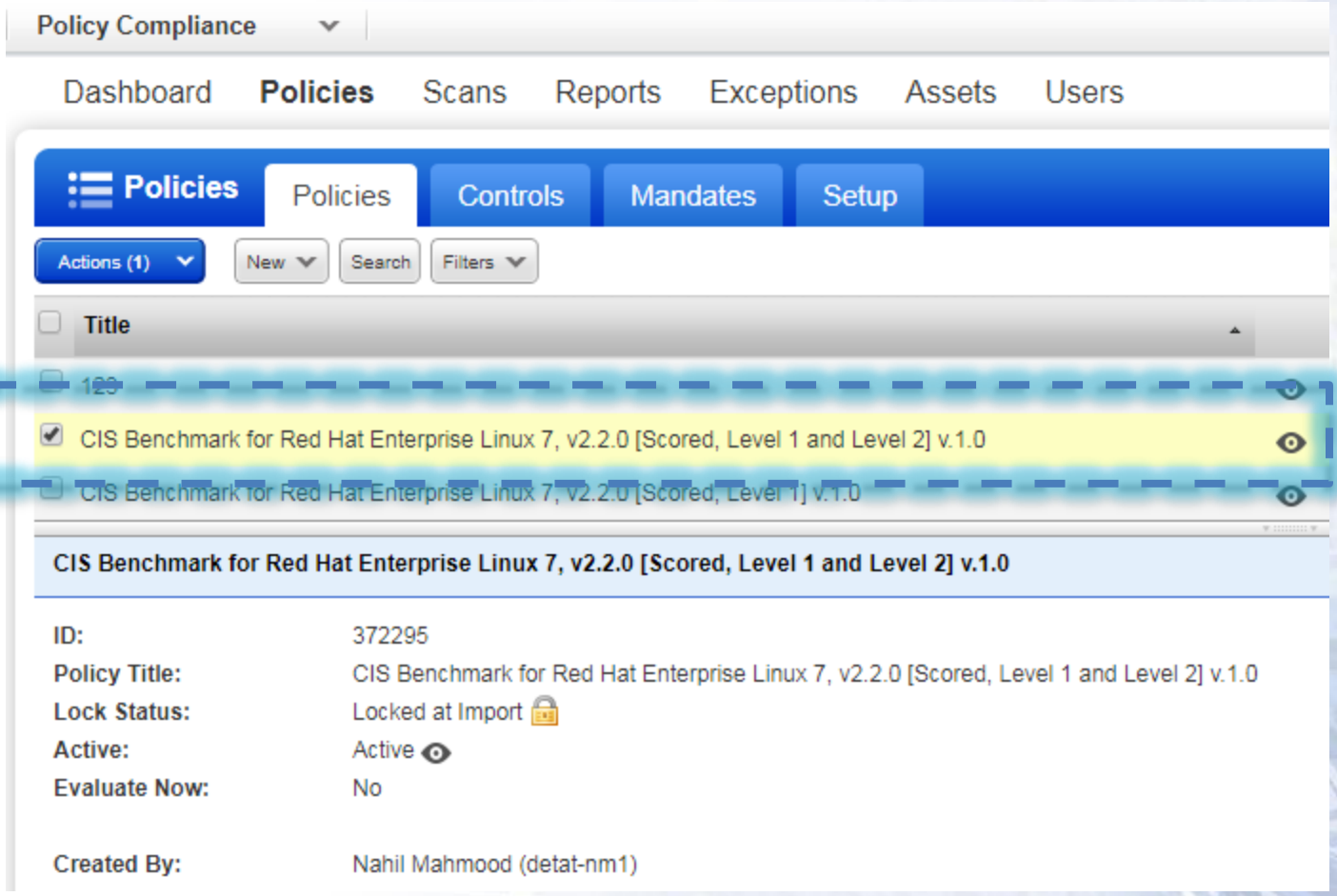
CREATE A NEW POLICY

QUALYS POLICY LIBRARIES



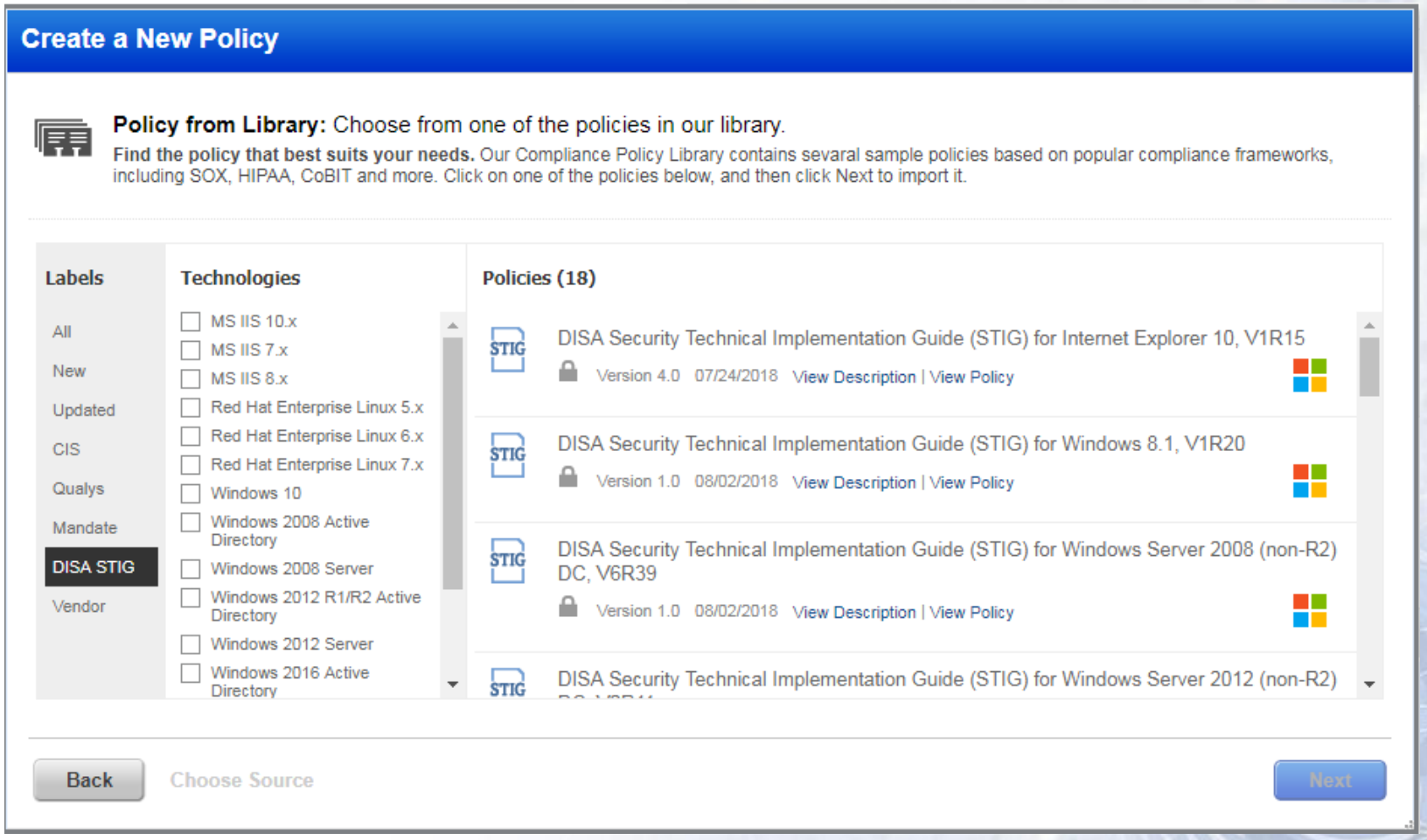
CIS > RED HAT ENT. LINUX 7.X

QUALYS POLICY LIBRARIES



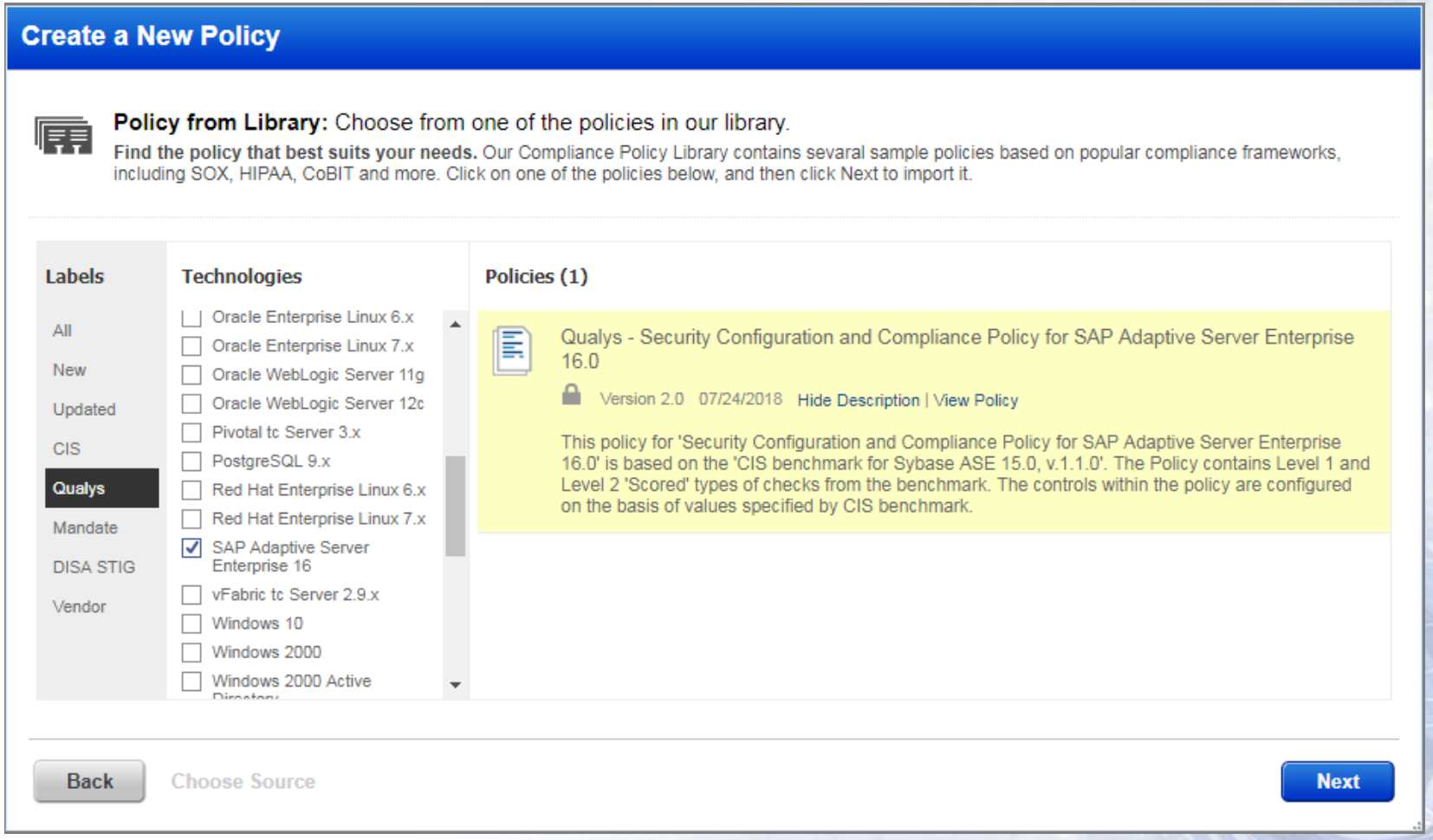
POLICIES DASHBOARD

QUALYS POLICY LIBRARIES



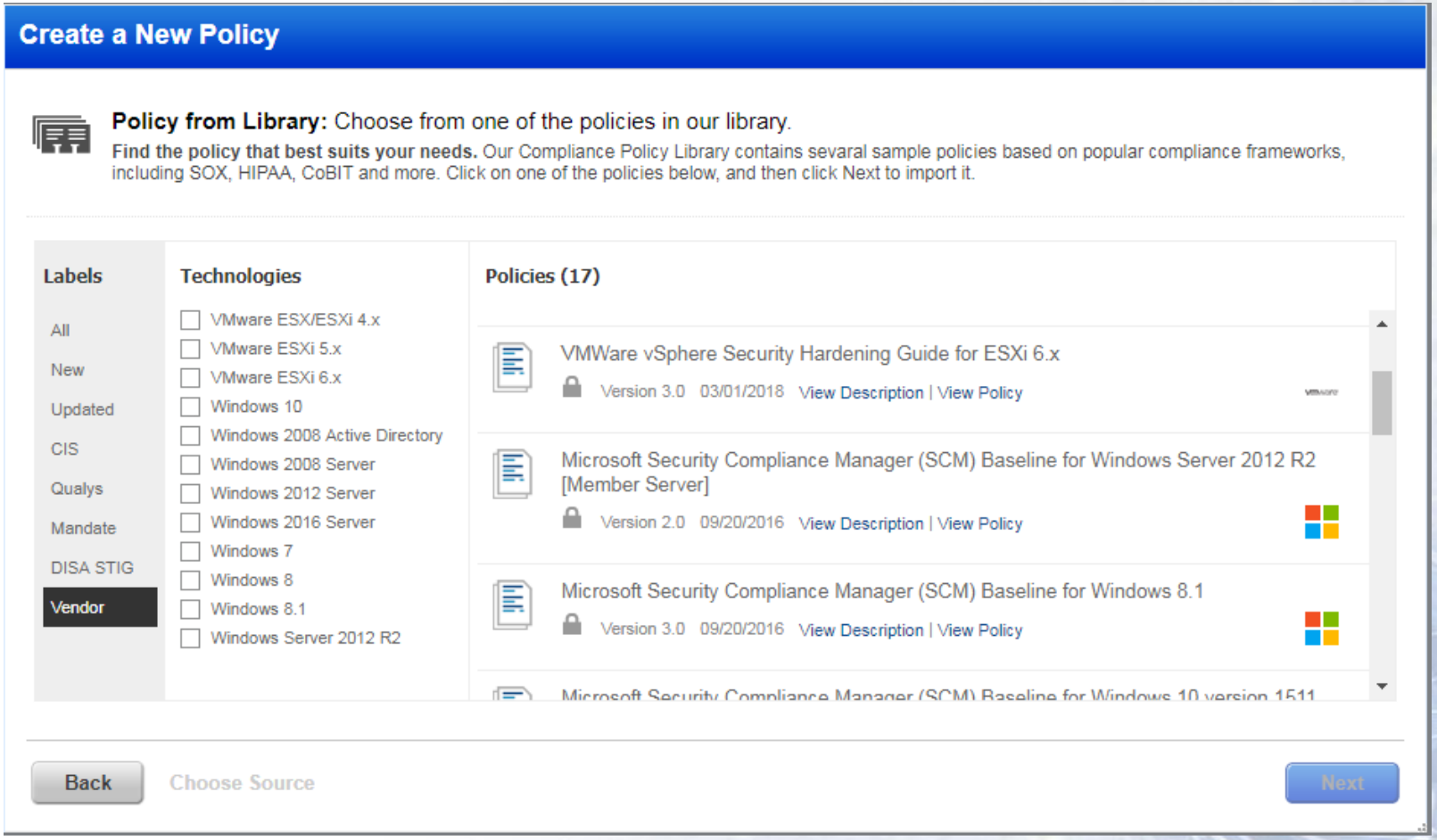
DISA STIG

QUALYS POLICY LIBRARIES



QUALYS SAP ADAPTIVE SERVER ENT 16

QUALYS POLICY LIBRARIES



VENDOR POLICIES

QUALYS POLICY LIBRARIES

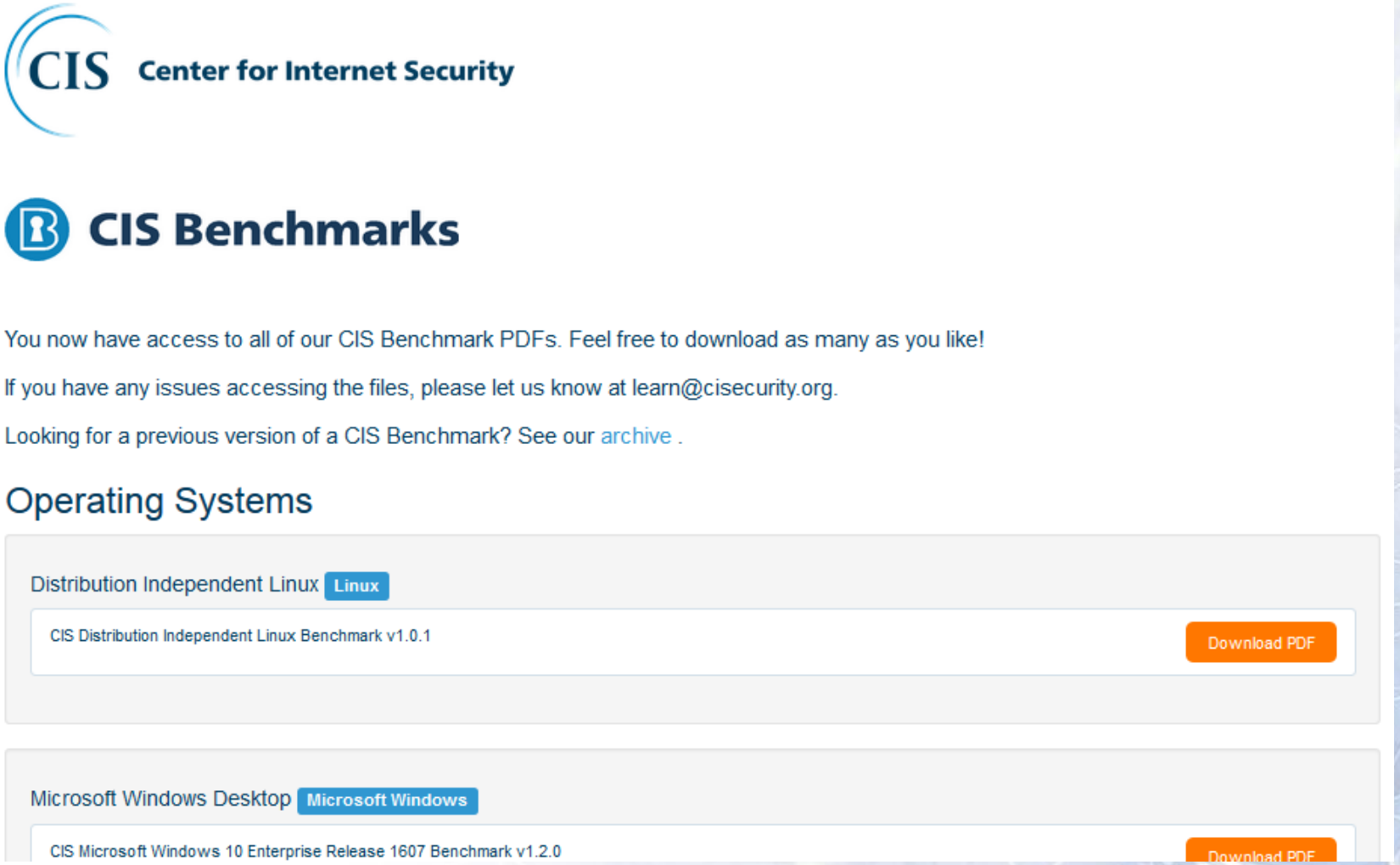
- Qualys has a vast number of options for Compliance Scans, and these should be fully explored through the Qualys trial

END

A Look At CIS Security Benchmarks (1)

- Center for Internet Security (CIS)
  - https://www.cisecurity.org/cis-benchmarks/
  - Fill out your details and will receive an email with link

A Look At CIS Security Benchmarks (1)



A Look At CIS Security Benchmarks (2)

#	OVERALL CIS BENCHMARK CATEGORIES	TOTAL
1	OPERATING SYSTEMS	36
2	SERVER SOFTWARE	33
3	CLOUD PROVIDERS	2
4	MOBILE DEVICES	8
5	NETWORK DEVICES	6
6	DESKTOP SOFTWARE	21
7	MULTIFUNCTION PRINT DEVICES	1
	GRAND TOTAL CIS BENCHMARKS	**107**

A Look At CIS Security Benchmarks (1)

#	OPERATING SYSTEMS	TOTAL
1	DISTRIBUTION INDEPENDENT LINUX	1
2	MICROSOFT WINDOWS DESKTOP	5
3	DEBIAN LINUX	2
4	UBUNTU LINUX	3
5	AMAZON LINUX	1
6	CENTOS LINUX	2
7	ORACLE LINUX	2

A Look At CIS Security Benchmarks (1)

#	OPERATING SYSTEMS (CONTD)…	TOTAL
8	REDHAT LINUX	3
9	SUSE LINUX	2
10	APPLE OS (UNIX)	5
11	IBM AIX (UNIX)	1
12	ORACLE SOLARIS (UNIX)	3
13	MS WINDOWS SERVER	6
	TOTAL BENCH MARKS OPERATING SYSTEMS	**36**

A Look At CIS Security Benchmarks (1)

Microsoft Windows Desktop **Microsoft Windows**

- CIS Microsoft Windows 10 Enterprise Release 1607 Benchmark v1.2.0
- CIS Microsoft Windows 8.1 Workstation Benchmark v2.2.1
- CIS Microsoft Windows 7 Workstation Benchmark v3.0.1
- CIS Microsoft Windows XP Benchmark v3.1.0
- CIS Microsoft Windows 8 Benchmark v1.0.0

A Look At CIS Security Benchmarks (1)

Microsoft Windows Server **Microsoft Windows**

- CIS Microsoft Windows Server 2016 RTM (Release 1607) Benchmark v1.0.0
- CIS Microsoft Windows Server 2008 (non-R2) Benchmark v3.0.1
- CIS Microsoft Windows Server 2008 R2 Benchmark v3.0.1
- CIS Microsoft Windows Server 2012 R2 Benchmark v2.2.1
- CIS Microsoft Windows Server 2012 (non-R2) Benchmark v2.0.1
- CIS Microsoft Windows Server 2003 Benchmark v3.1.0

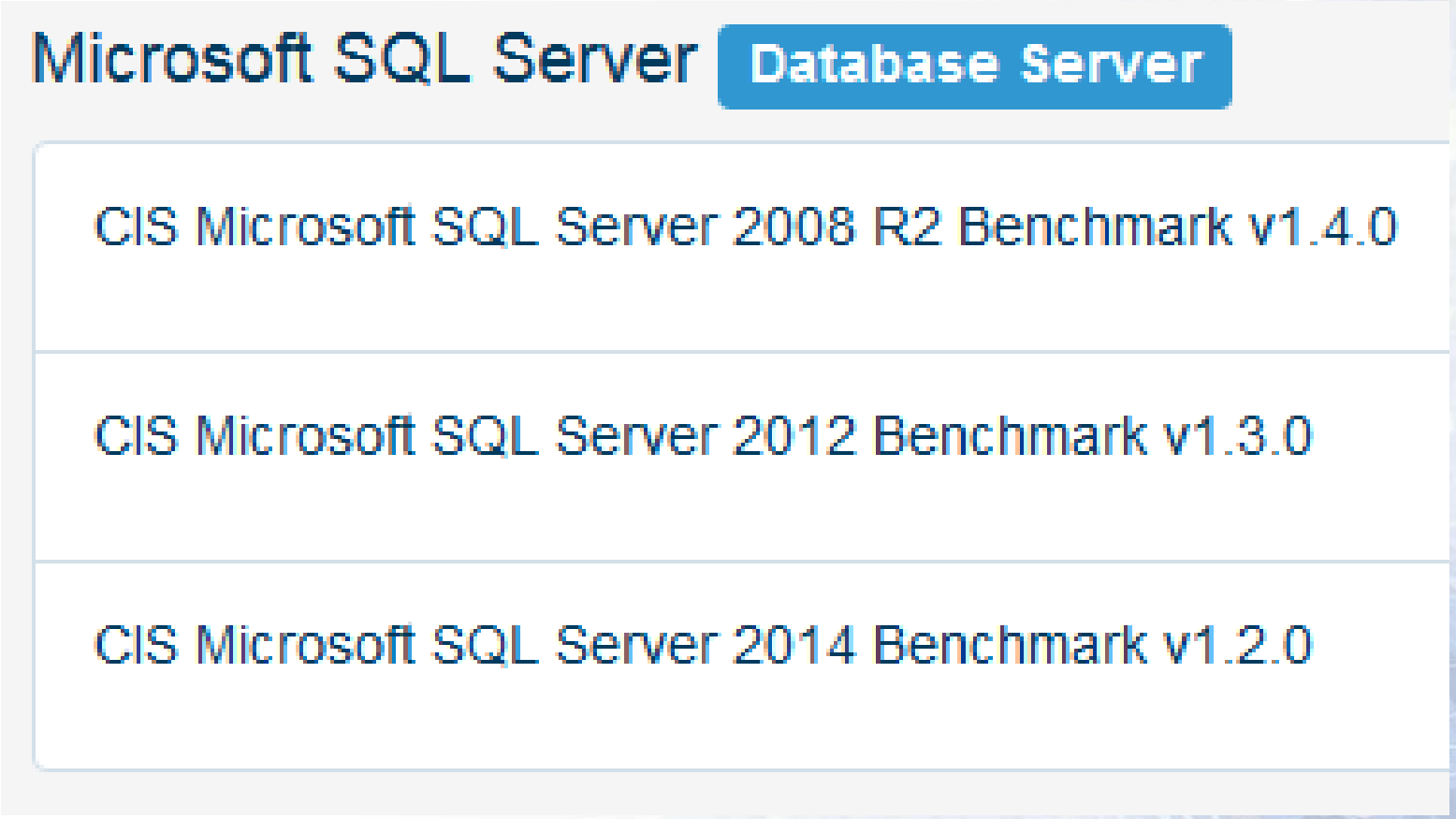
A Look At CIS Security Benchmarks (1)

#	SERVER SOFTWARE	TOTAL
1	MICROSOFT IIS (WEB SERVER)	3
2	VMWARE (VIRTUALIZATION)	2
3	MONGODB (DATABASE SERVER)	3
4	IBM DB2 (DATABASE SERVER)	3
5	BIND (DNS SERVER)	1
6	APACHE TOMCAT (WEB SERVER)	2
7	MICROSOFT SQL SERVER (DB SERVER)	3

A Look At CIS Security Benchmarks (1)

#	SERVER SOFTWARE (CONTD)…	TOTAL
8	APACHE (HTTP SERVER)	2
9	DOCKER (VIRTUALIZATION)	5
10	ORACLE (DATABASE SERVER)	3
11	KUBERNETES (VIRTUALIZATION)	1
12	MIT KERBEROS (AUTHENTICATION)	1
13	ORACLE MySQL (DB SERVER)	4
	TOTAL BENCH MARKS SERVER SOFTWARE	**33**

A Look At CIS Security Benchmarks (1)



A Look At CIS Security Benchmarks (1)

#	CLOUD PROVIDERS	TOTAL
1	AMAZON WEB SERVICES	2
	TOTAL CLOUD PROVIDERS	**2**

A Look At CIS Security Benchmarks (1)

- Next module…remaining categories

END

A Look At CIS Security Benchmarks (2)

- Mobile devices, network devices, desktop software, multifunction print devices

A Look At CIS Security Benchmarks (2)

#	MOBILE DEVICES	TOTAL
1	APPLE IOS	5
2	GOOGLE ANDROID	3
	TOTAL BENCH MARKS MOBILE DEVICES	**8**

A Look At CIS Security Benchmarks (2)

#	NETWORK DEVICES	TOTAL
1	CISCO	4
2	PALO ALTO NETWORKS	2
	TOTAL BENCH MARKS NETWORK DEVICES	**6**

A Look At CIS Security Benchmarks (2)

#	DESKTOP SOFTWARE	TOTAL
1	MICROSOFT OFFICE	13
2	GOOGLE CHROME (WEB BROWSER)	1
3	MS EXCHANGE SERVER	3
4	MS INTERNET EXPLORER	2
5	MOZILLA FIREFOX	2
	TOTAL BENCH MARKS DESKTOP SOFTWARE	**21**

A Look At CIS Security Benchmarks (2)

#	MULTIFUNCTION PRINT DEVICES	TOTAL
1	MULTIFUNCTION DEVICE	1
	TOTAL BENCH MARKS MULTIFUNCTION PRINT DEVICES	**1**

A Look At CIS Security Benchmarks (2)

Apple iOS

- CIS Apple iOS 10 Benchmark v2.0.0
- CIS Apple iOS 9 Benchmark v1.0.0
- CIS Apple iOS 8 Benchmark v1.0.0
- CIS Apple iOS 7 Benchmark v1.1.0
- CIS Apple iOS 6 Benchmark v1.0.0

A Look At CIS Security Benchmarks (2)

Google Android

- CIS Google Android 7 Benchmark v1.0.0
- CIS Google Android 4 Benchmark v1.0.0
- CIS Google Android 2.3 Benchmark v1.1.0

A Look At CIS Security Benchmarks (2)

Cisco

- CIS Cisco Firewall Benchmark v4.0.0
- CIS Cisco IOS 12 Benchmark v4.0.0
- CIS Cisco IOS 15 Benchmark v4.0.0
- CIS Cisco Wireless LAN Controller 7 Benchmark v1.1.0

A Look At CIS Security Benchmarks (2)

Microsoft Office **Productivity Software**

- CIS Microsoft Office 2016 Benchmark v1.1.0
- CIS Microsoft Office PowerPoint 2016 Benchmark v1.0.1
- CIS Microsoft Office PowerPoint 2013 Benchmark v1.0.1
- CIS Microsoft Office Excel 2016 Benchmark v1.0.1
- CIS Microsoft Office Excel 2013 Benchmark v1.0.1
- CIS Microsoft Office Access 2016 Benchmark v1.0.1
- CIS Microsoft Office Access 2013 Benchmark v1.0.1

A Look At CIS Security Benchmarks (2)

- CIS Microsoft Office 2013 Benchmark v1.1.0
- CIS Microsoft Office Word 2016 Benchmark v1.1.0
- CIS Microsoft Office Word 2013 Benchmark v1.1.0
- CIS Microsoft Office Outlook 2016 Benchmark v1.1.0
- CIS Microsoft Office Outlook 2013 Benchmark v1.1.0
- CIS Microsoft Outlook 2010 Benchmark v1.0.0

A Look At CIS Security Benchmarks (3)

- CIS Benchmarks example (Network Devices)

A Look At CIS Security Benchmarks (3)

#	OVERALL CIS BENCHMARK CATEGORIES	TOTAL
1	OPERATING SYSTEMS	36
2	SERVER SOFTWARE	33
3	CLOUD PROVIDERS	2
4	MOBILE DEVICES	8
5	NETWORK DEVICES	6
6	DESKTOP SOFTWARE	21
7	MULTIFUNCTION PRINT DEVICES	1
	GRAND TOTAL CIS BENCHMARKS	**107**

CIS Benchmarks

- The CIS Benchmarks are prescriptive configuration recommendations for more than 25+ vendor product families. They represent the consensus-based effort of cybersecurity experts globally to help you protect your systems against threats more confidently.

CIS Benchmarks

CIS Benchmarks from the Center of Internet Security (CIS)

- a set of globally recognized and consensus-driven best practices to help security practitioners implement and manage their cybersecurity defenses.
- Developed with a global community of security experts, the guidelines help organizations proactively safeguard against emerging risks.
- Companies implement the CIS Benchmark guidelines to limit configuration-based security vulnerabilities in their digital assets.

CIS Benchmarks

When you implement CIS Benchmarks, you can better secure your legacy systems against common and emerging risks by taking steps such as these:

- Disabling unused ports
- Removing unnecessary app permissions
- Limiting administrative privileges

CIS levels

- Level 1: Basic easily implementable configurations designed to lower the attack surface without impacting performance.

- Level 2: Configuration recommendations that may create system conflicts and are intended to provide "defense in depth" for environments that need enhanced security

Domain Controller& Memeber Server

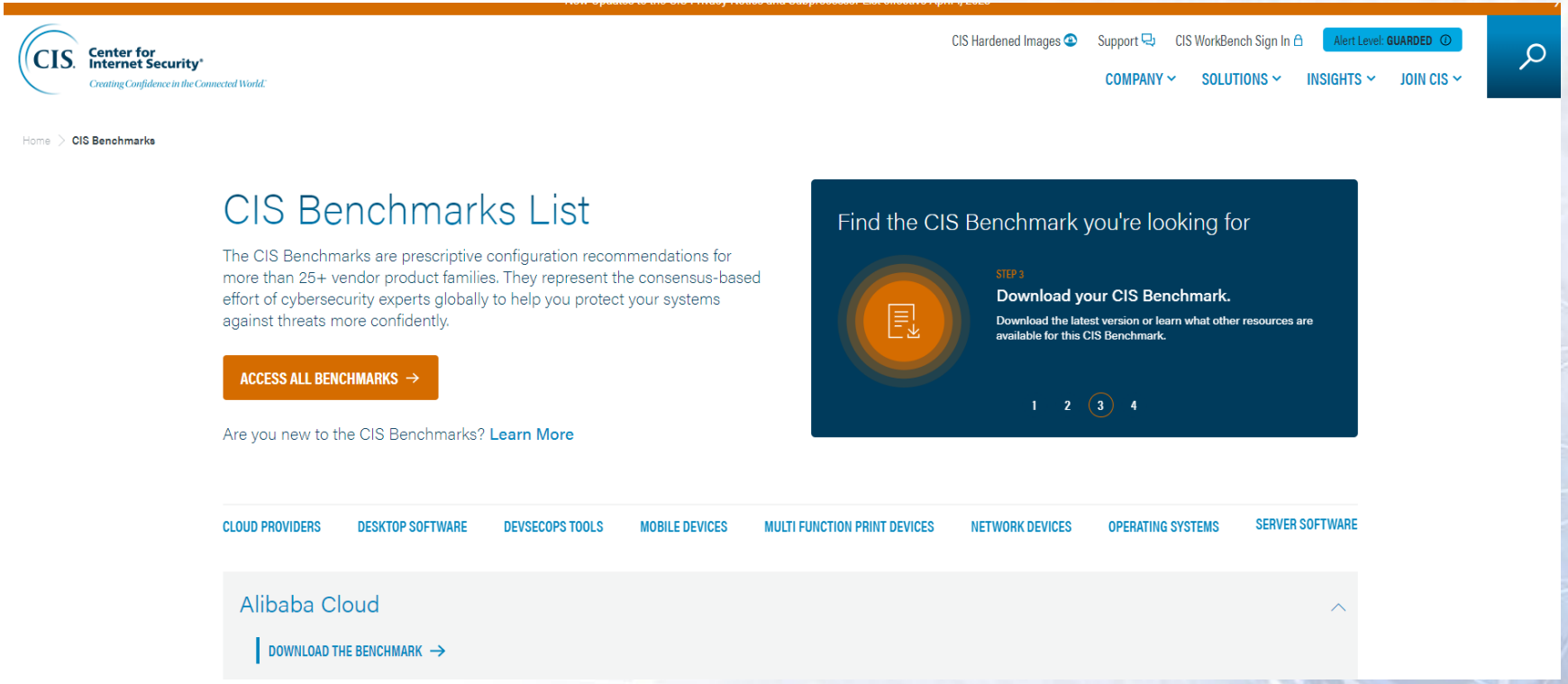
- A computer with a server OS and Active Directory installed is a Domain Controller.
- Any other computer with a server OS or for example with SQL Server installed, which works as a server and is joined to the domain can be called a member server. A member server does not have Active Directory installed.

- If a computer has DHCP or DNS, but not Active Directory, it's a member server.

Scored and Unscored

- Each recommendation is either 'scored' or 'not scored.
- 'Scored' recommendations are mandatory to achieve CIS compliance, and if not met, they lower the total benchmark score.

- Recommendations that are 'not scored' have no impact on the overall score of the benchmark.



https://www.cisecurity.org/cis-benchmarks

CIS Critical Security Controls

- Formerly the SANS Critical Security Controls (SANS Top 20) these are now officially called the CIS Critical Security Controls (CIS Controls).

- CIS Top 20 Critical Security Controls are a prioritized set of cybersecurity best practices that can help protect enterprises from the most pervasive and dangerous attacks.

- https://www.cisecurity.org/controls

- The CIS Critical Security Controls (CIS Controls) are a prescriptive, prioritized, and simplified set of best practices that you can use to strengthen your cybersecurity posture.

- Thousands of cybersecurity practitioners from around the world use the CIS Controls and/or contribute to their development via a community consensus process.

CIS-CAT

- CIS-CAT Pro Assessor evaluates the cybersecurity posture of a system against recommended policy settings. The tool helps organizations save time and resources by employing automated content with policy setting recommendations based on 100+ globally recognized CIS Benchmarks.
- The CIS Controls Self Assessment Tool (CSAT) is a companion tool that helps IT security teams track their implementation of every CIS Control and Sub-Control

- https://www.cisecurity.org/insights/blog/cis-csat-free-tool-assessing-implementation-of-cis-controls

There are two versions of CIS CSAT.

- The CIS-hosted CSAT is free to every organization for use in a non-commercial capacity.
- CIS CSAT Pro is an on-premises version that offers additional features and benefits and is only available to CIS SecureSuite Members.

A Look At CIS Security Benchmarks (4)

- CIS Benchmarks example (Operating Systems)
  - MS Windows Server 2012-R2

A Look At CIS Security Benchmarks (4)

#	OVERALL CIS BENCHMARK CATEGORIES	TOTAL
1	OPERATING SYSTEMS	36
2	SERVER SOFTWARE	33
3	CLOUD PROVIDERS	2
4	MOBILE DEVICES	8
5	NETWORK DEVICES	6
6	DESKTOP SOFTWARE	21
7	MULTIFUNCTION PRINT DEVICES	1
	GRAND TOTAL CIS BENCHMARKS	**107**

A Look At CIS Security Benchmarks (4)



- January 31, 2017
- 760 pages PDF doc

A Look At CIS Security Benchmarks (4)

- Profile applicability:
  - Level 1 domain controller
  - Level 1 member server
  - **Level 2 domain controller**
  - **Level 2 member server**

A Look At CIS Security Benchmarks (4)

- Level 1: Items in this profile intend to:
  - be practical and prudent;
  - provide a clear security benefit; and
  - not inhibit the utility of the technology beyond acceptable means

A Look At CIS Security Benchmarks (4)

- Level 2: extends the Level 1 - profile
  - intended for environments or use cases where security is paramount
  - acts as defense in depth measure
  - may negatively inhibit the utility or performance of the technology

A Look At CIS Security Benchmarks (4)

- Control content:
  - Profile applicability (ASA 8.X, ASA 9.X)
  - Description
  - Rationale
  - Audit
  - Remediation
  - **Impact**
  - Default value
  - References

A Look At CIS Security Benchmarks (4)

- 1.1.2 [L1]: *Ensure 'Maximum password age' is set to '60 or fewer days, but not 0' (Scored)*
  - *Profile applicability: Level 1 Domain Controller, Level 1 Member Server*

A Look At CIS Security Benchmarks (4)

- 1.1.2 [L1] Description:
  - This policy setting defines how long a user can use their password before it expires.
  - Values for this policy setting range from 0 to 999 days. If you set the value to 0, the password will never expire.

A Look At CIS Security Benchmarks (4)

- 1.1.2 [L1] Audit:
  - Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

A Look At CIS Security Benchmarks (4)

Remediation:

To establish the recommended configuration via GP, set the following UI path to `60 or fewer days, but not 0:`

```
Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Maximum password age
```

A Look At CIS Security Benchmarks (4)

- 1.1.2 [L1] Default Value: 42 days
- 1.1.2 [L1] Reference: CCE-37167-4
  - Common Configuration Enumeration (Unique identifiers for common system config issues)

END

A Look At CIS Security Benchmarks (3)



- June 29, 2016
- 174 pages PDF doc

A Look At CIS Security Benchmarks (3)

- Control content:
  - Profile applicability (ASA 8.X, ASA 9.X)
  - Description
  - Rationale
  - Audit
  - Remediation
  - Default value
  - References

A Look At CIS Security Benchmarks (3)

- 1.8 (page 88); Session Timeout
  - Profile applicability: Level 1, Cisco ASA9.X
  - Description: Sets the idle timeout for a console session before the security appliance terminates it.

A Look At CIS Security Benchmarks (3)

- 1.8 (page 88); Session Timeout
  - Rationale: Limiting session timeout prevents unauthorized users from using abandoned sessions to perform malicious activities.

A Look At CIS Security Benchmarks (3)

Audit:

- Step 1: Run the following command to show what the console timeout is set to

```
hostname#sh run console | in timeout.5
```

The output should look like

```
console timeout 5
```

Example:

```
Asa-fw#sh run console | in timeout.5
console timeout 5
```

Here the session timeout is 5 minutes

- Step 2: If an output is displayed, the system is compliant. If not, there is a finding.

A Look At CIS Security Benchmarks (3)

Remediation:

- Step 1: Run the following command to set the console timeout to less than or equal to 5 minutes

```
hostname(config)# console timeout 5
```

A Look At CIS Security Benchmarks (3)

- 1.8 (page 88); Session Timeout
  - Default Value: The default timeout is 0, which means the console session will not time out

A Look At CIS Security Benchmarks (3)

- 1.8 (page 88); Session Timeout
  - Reference: CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide, 9.1

A Look At DISA STIGs (1)

- Defense Information Systems Agency (DISA) provides technical guides referred to as Security Technical Implementation Guides (STIGs).

A Look At DISA STIGs (1)

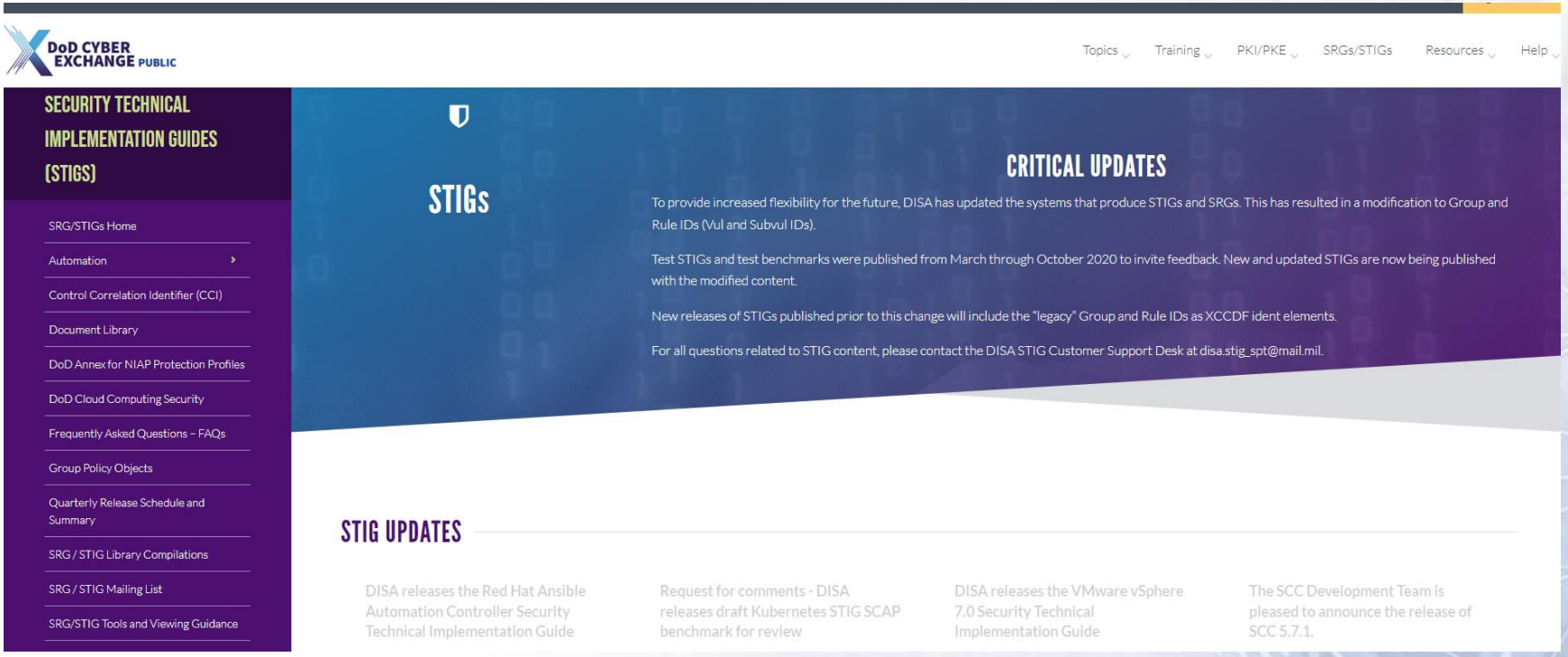
- USA DoD
- Security Technical Implementation Guides (STIGs)
- Most expansive security benchmarks available
- Most regularly updated
- 425 STIGs available

A Look At DISA STIGs (1)

- **STIGs master list (A-Z):**
  - https://public.cyber.mil/stigs/downloads/
  - **STIG viewer:**
  - https://public.cyber.mil/stigs/srg-stig-tools/

A Look At DISA STIGs (1)

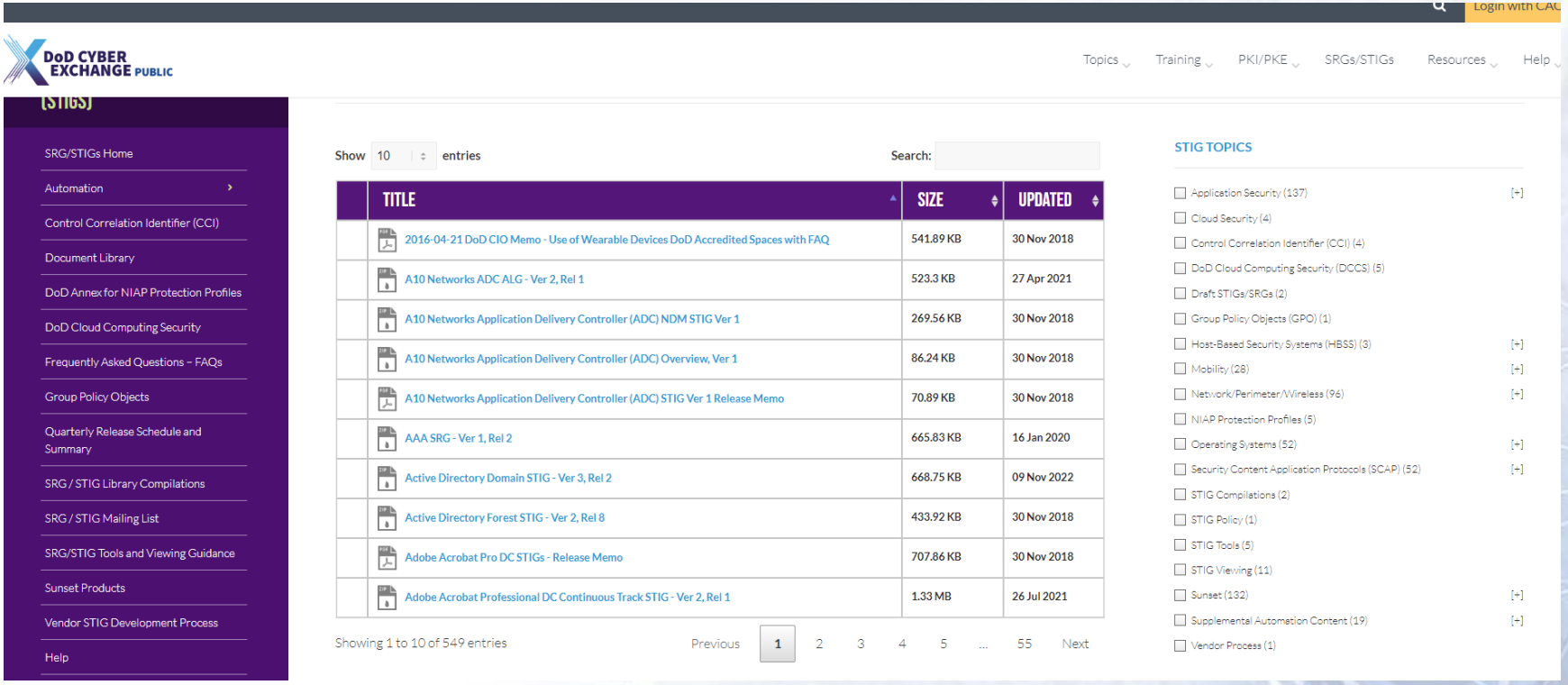
STIGs HOME



https://public.cyber.mil/stigs/

A Look At DISA STIGs (1)

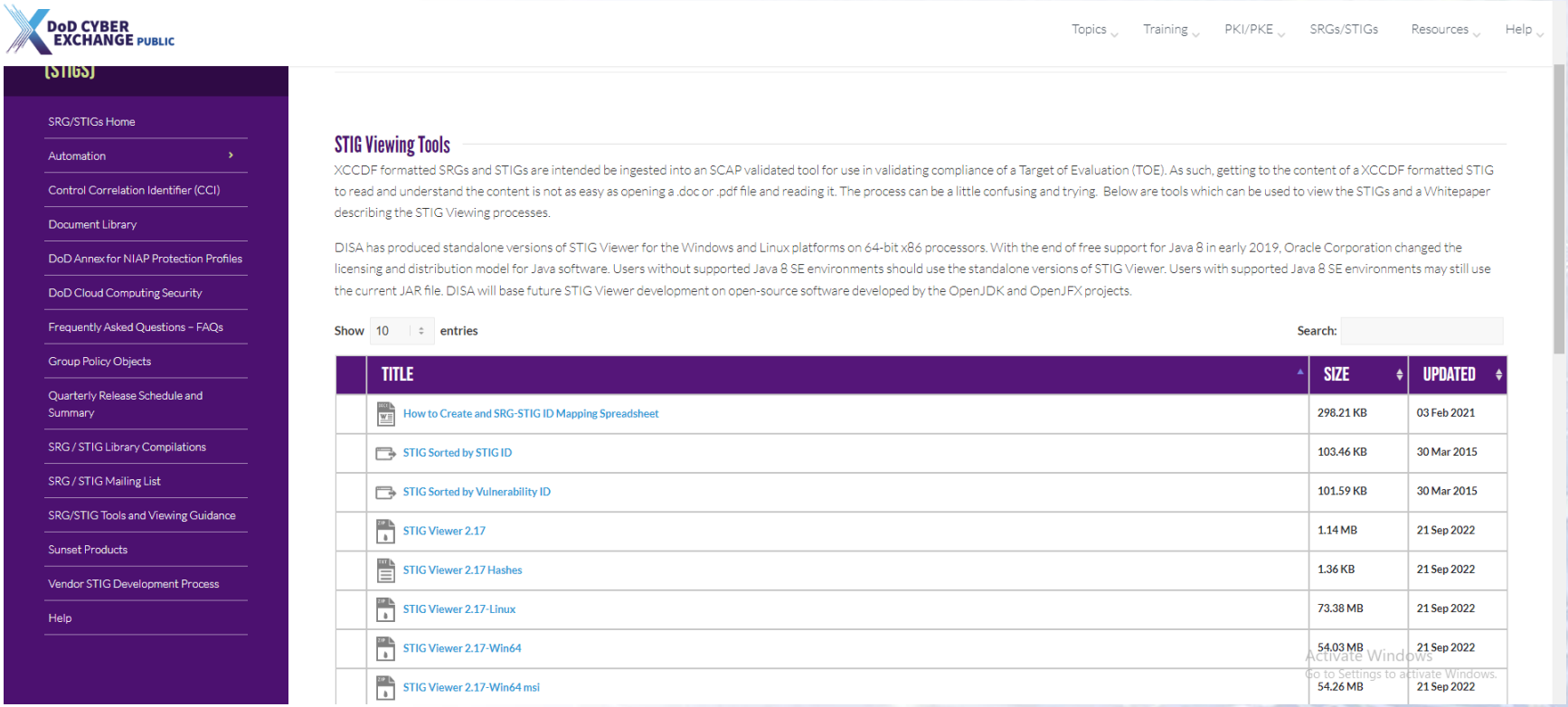
STIGs Master List



https://public.cyber.mil/stigs/downloads/

A Look At DISA STIGs (1)

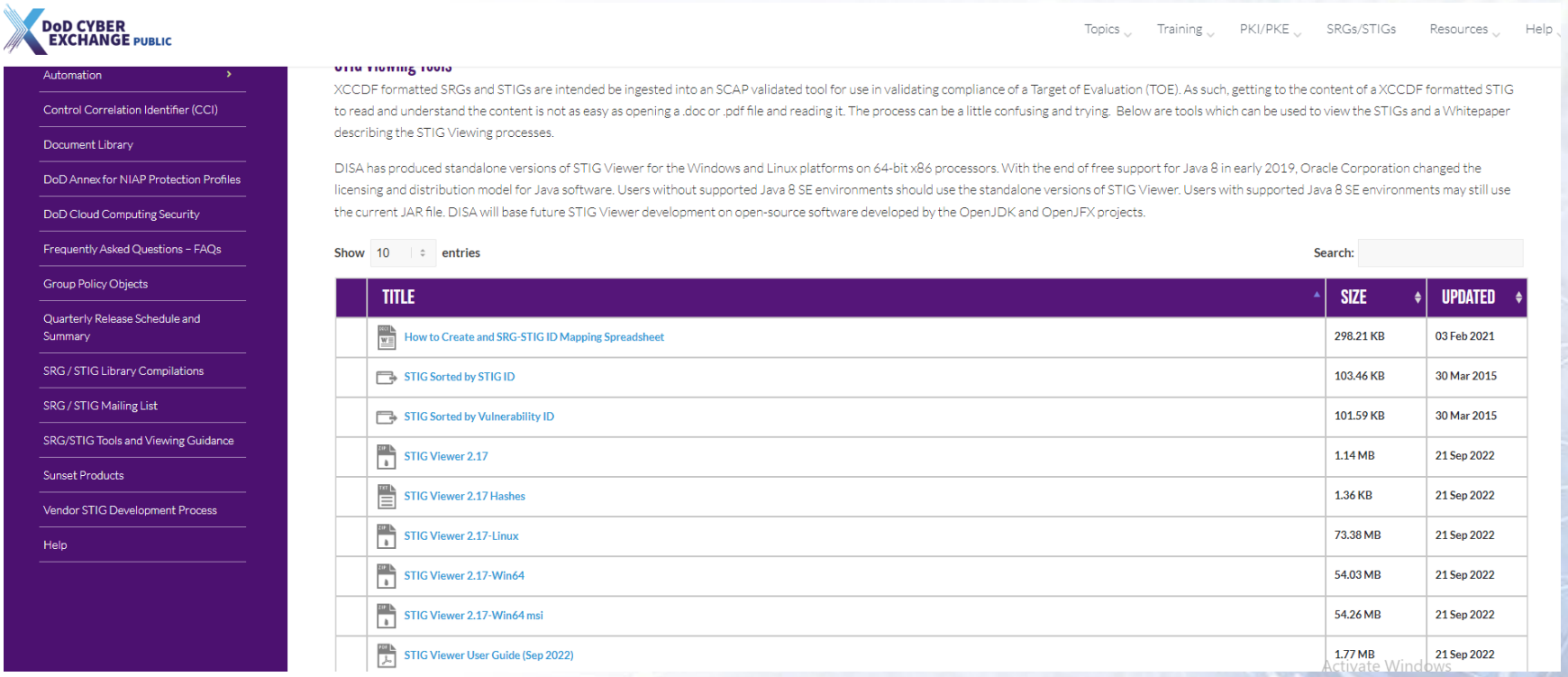
STIGs Viewer



https://public.cyber.mil/stigs/srg-stig-tools/

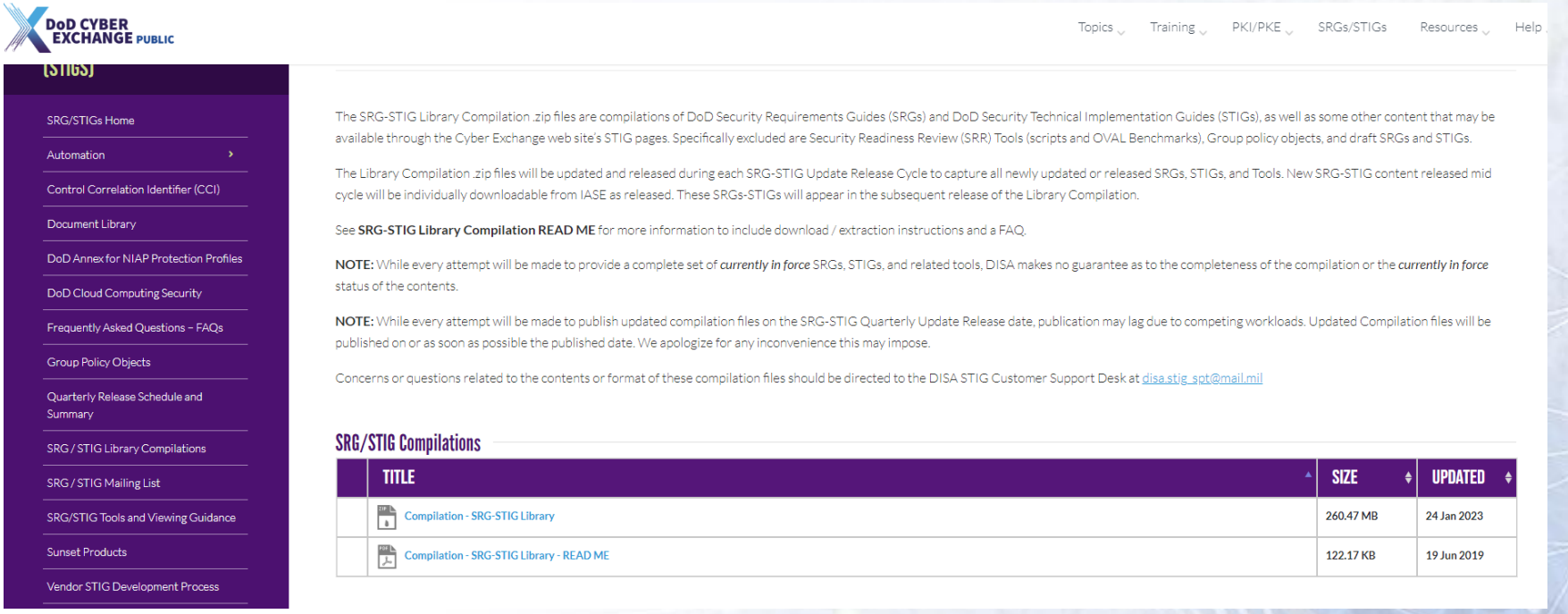
A Look At DISA STIGs (1)

STIG Viewer Download



A Look At DISA STIGs (1)

STIG Library Compilation

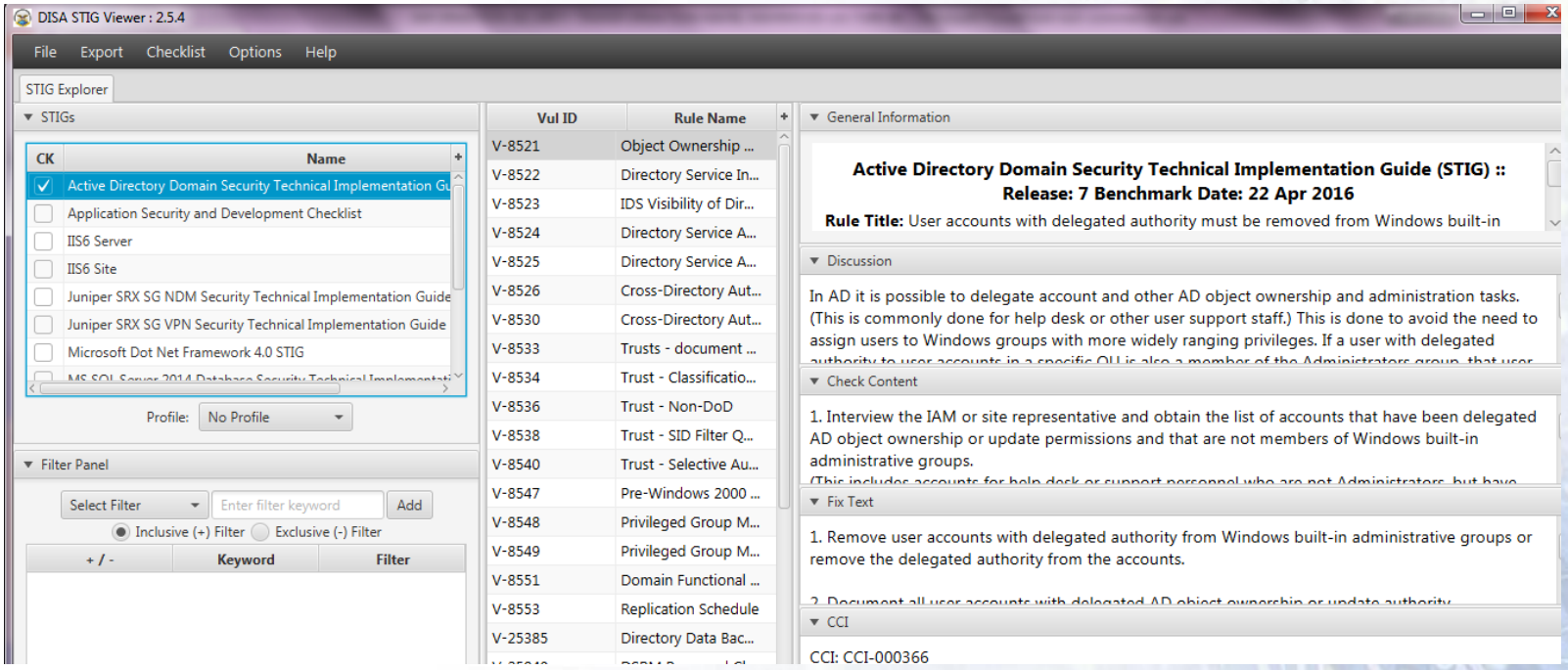


- There are three categories of severity, ranked on level of risk or vulnerability.
- These are known as Severity Category Codes (CAT), with CAT 1, CAT 2 and CAT 3 levels of risk.

- CAT 1 controls cover the most severe vulnerabilities and risks.
- CAT I weaknesses should receive the highest priority for correction or mitigation.

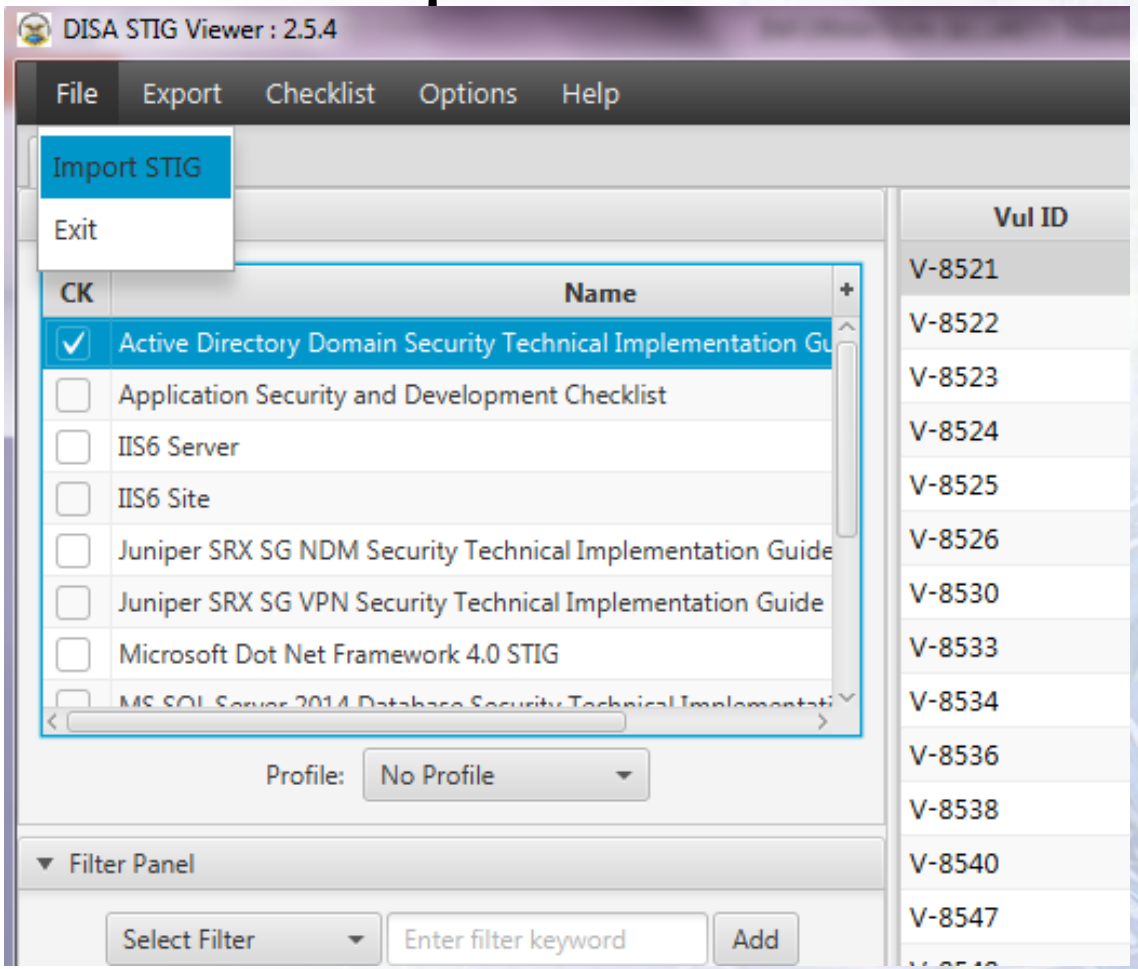
A Look At DISA STIGs (1)

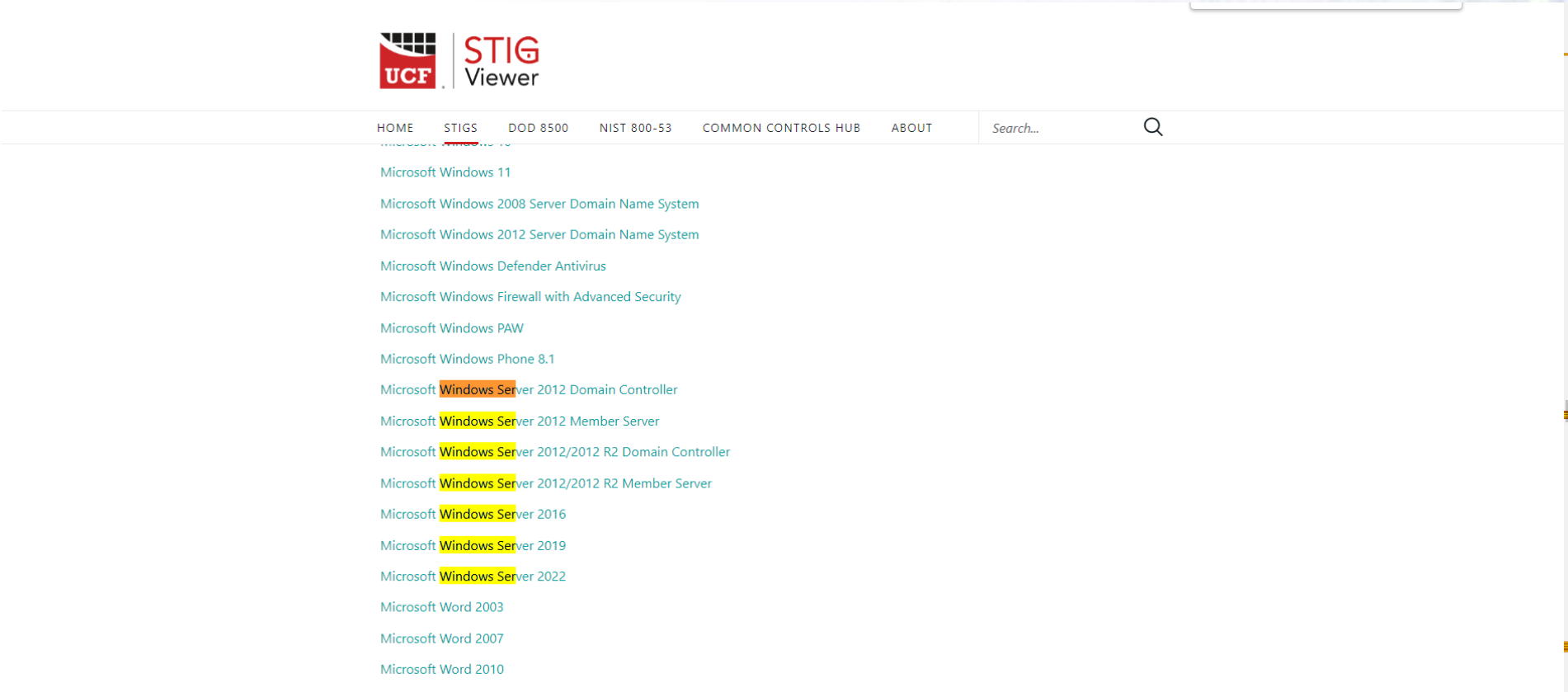
STIG Viewer Window



A Look At DISA STIGs (1)

Import STIG





https://www.stigviewer.com/stigs


UCF
STIG Viewer
HOME
STIGS
DOD 8500
NIST 800-53
COMMON CONTROLS HUB
ABOUT
Search...
Microsoft Windows Server 2012/2012 R2 Member Server Security Technical Implementation Guide
Overview
Version
Date
Finding Count (330)
Downloads
3
2022-09-06
CAT I (High): 33
CAT II (Med): 238
CAT III (Low): 59
Excel
JSON
XML
STIG Description
This Security Technical Implementation Guide is published as a tool to improve the security of Department of Defense (DoD) information systems. The requirements are derived from the National Institute of Standards and Technology (NIST) 800-53 and related documents. Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil.
Available Profiles


UCF
STIG
Viewer
HOME
STIGS
DOD 8500
NIST 800-53
COMMON CONTROLS HUB
ABOUT
Search...
Findings (MAC III - Administrative Sensitive)
Finding ID
Severity
Title
Description
V-225447
High
Anonymous access to the registry must be restricted.
The registry is integral to the function, security, and stability of the Windows system. Some processes may require anonymous access to the registry. This must be limited to properly protect the system.
V-225244
High
Administrative accounts must not be used with applications that access the Internet, such as web browsers, or with potential Internet sources, such as email.
Using applications that access the Internet or have potential Internet sources using administrative privileges exposes a system to compromise. If a flaw in an application is exploited while...
V-225258
High
The Windows 2012 / 2012 R2 system must use an anti-virus program.
Malicious software can establish a base on individual desktops and servers. Employing an automated mechanism to detect this type of software will aid in elimination of the software from the...
V-225547
High
The Act as part of the operating system user right must not be assigned to any groups or accounts.
Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities. Accounts with the "Act as part of the operating system" user right can assume the...
V-225438
High
File Transfer Protocol (FTP) servers must be configured to prevent access to the system drive.
The FTP service allows remote users to access shared files and directories. Access outside of the specific directories of shared data could provide access to system resources and compromise the system.
V-225449
High
Local accounts with blank passwords must be restricted to prevent access from the network.
An account without a password can allow unauthorized access to a system as only the username would be required. Password policies should prevent

A Look At DISA STIGs (1)

- Completely different mechanism for DISA STIGs

END

A Look At DISA STIGs (2)

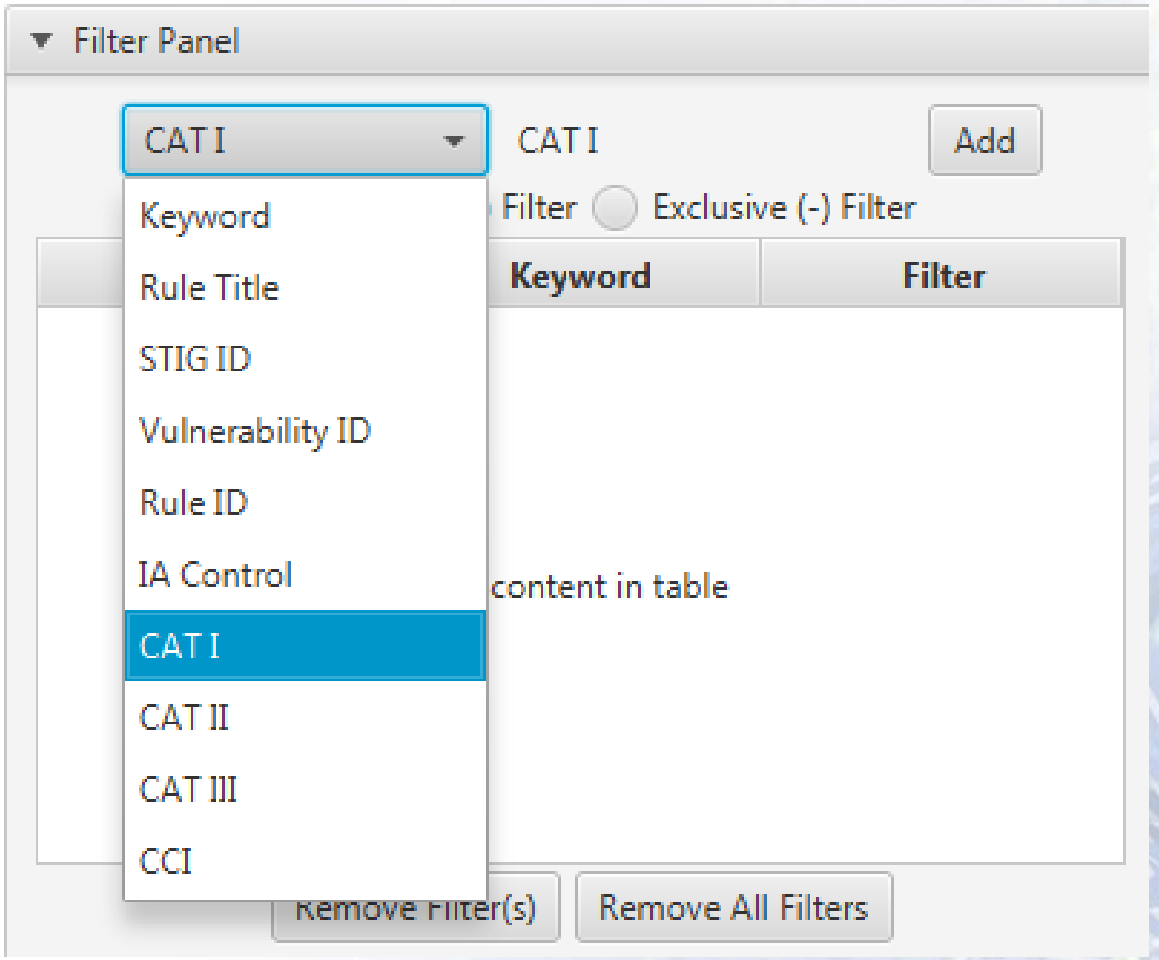
- STIG content:
  - General information (title)
  - Discussion
  - Check content
  - Fix text
  - CCI (References)

A Look At DISA STIGs (2)

SEVERITY	DISA CATEGORY CODE GUIDELINES
CAT 1	Any vulnerability, the exploitation of which will directly and immediately result in loss of Confidentiality, Availability, or Integrity.
CAT 2	Any vulnerability, the exploitation of which has a potential to result in loss of Confidentiality, Availability, or Integrity.
CAT 3	Any vulnerability, the existence of which degrades measures to protect against loss of Confidentiality, Availability, or Integrity

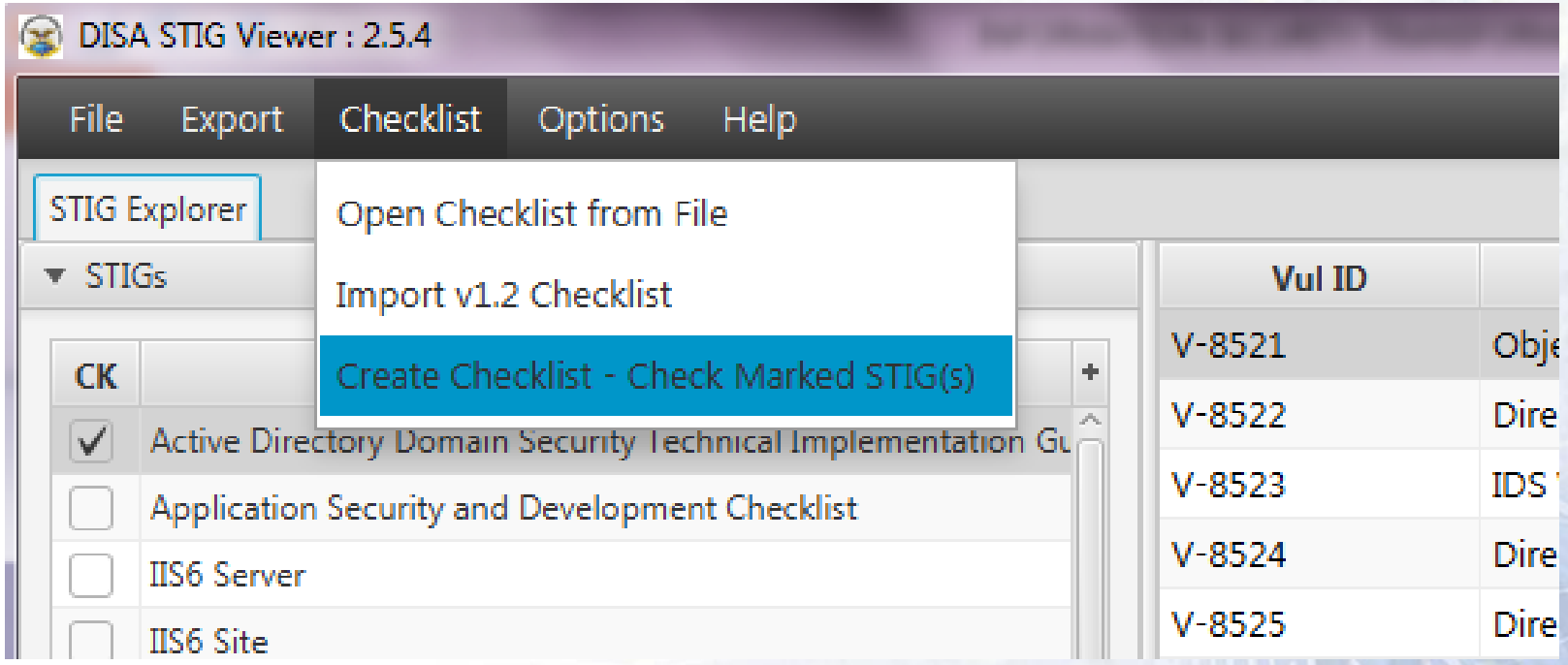
A Look At DISA STIGs (2)

FILTER PANEL



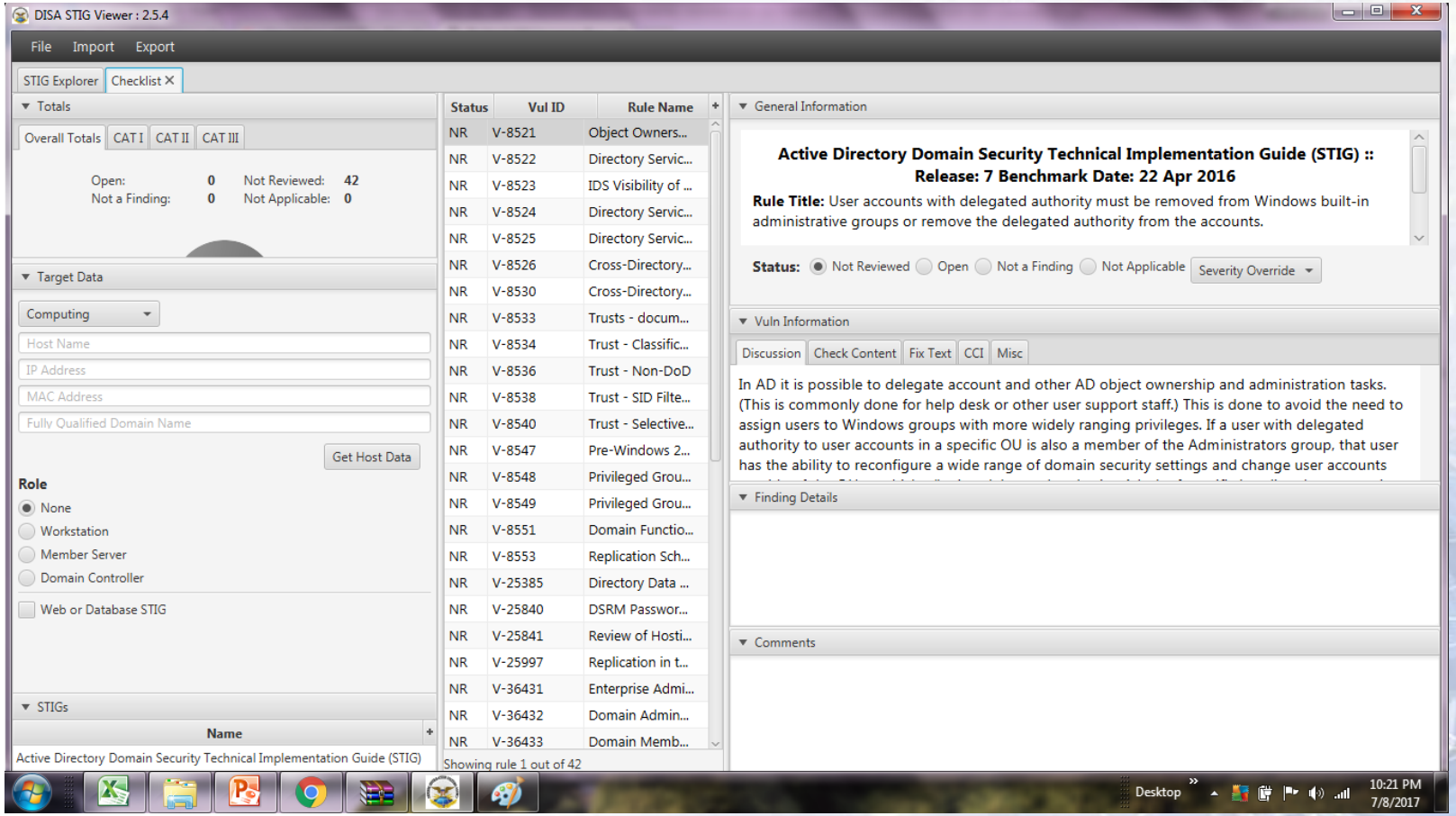
A Look At DISA STIGs (2)

CREATE CHECKLIST



A Look At DISA STIGs (2)

CHECKLIST



A Look At DISA STIGs (2)

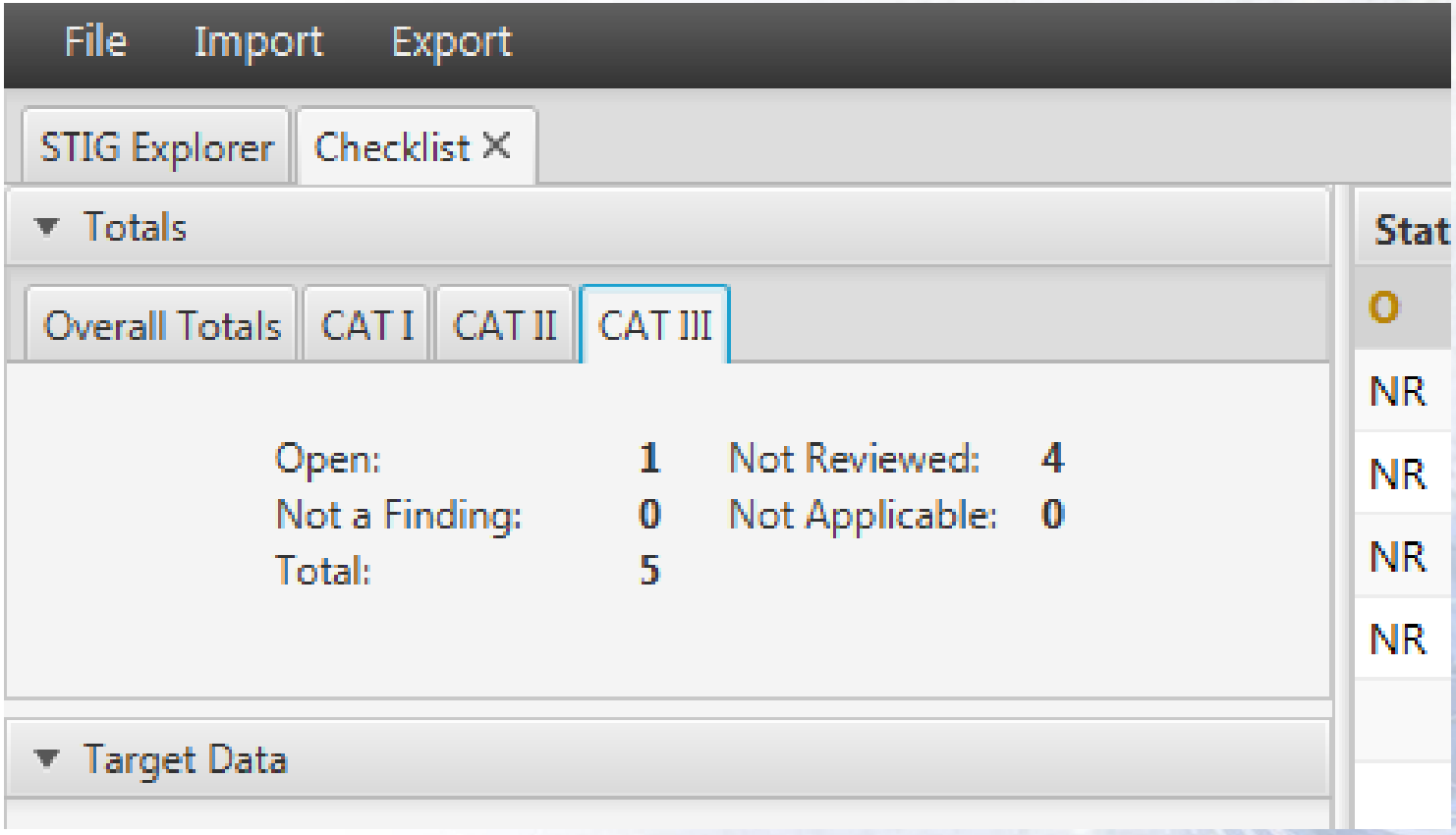
- Checklist screens:
  - Overall totals
  - Target data
  - Role
  - Finding details
  - Comments

A Look At DISA STIGs (2)

- Checklist screens (STATUS):
  - Not reviewed
  - Open
  - Not a finding
  - Not applicable

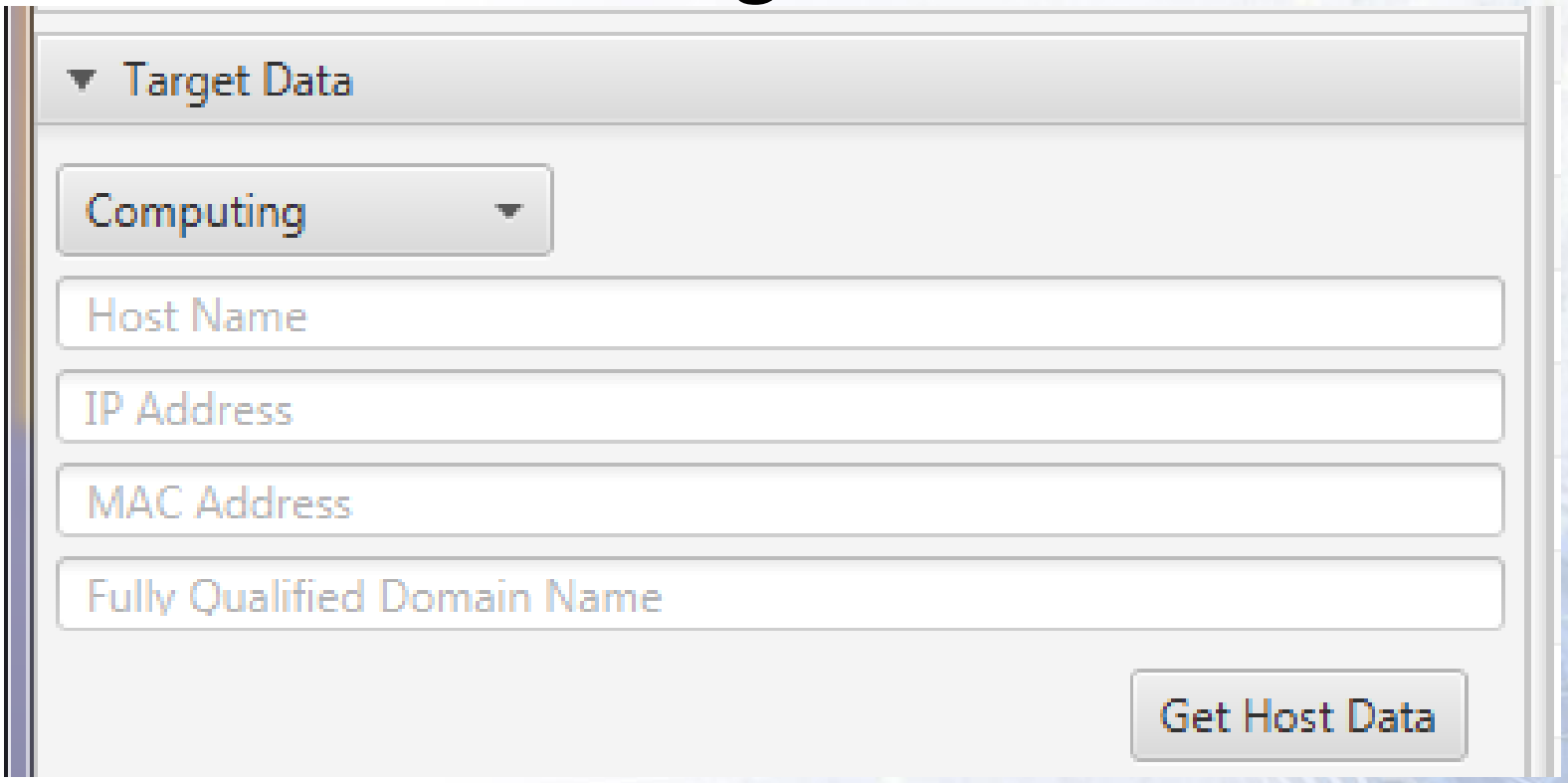
A Look At DISA STIGs (2)

Totals



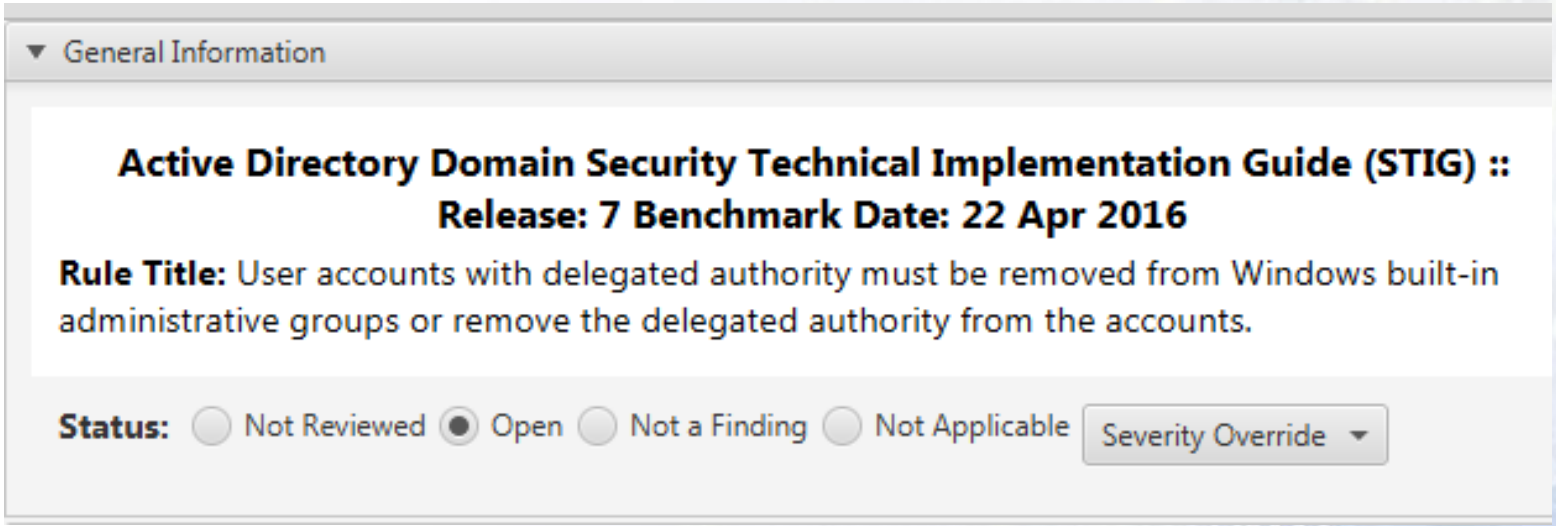
A Look At DISA STIGs (2)

Target Data



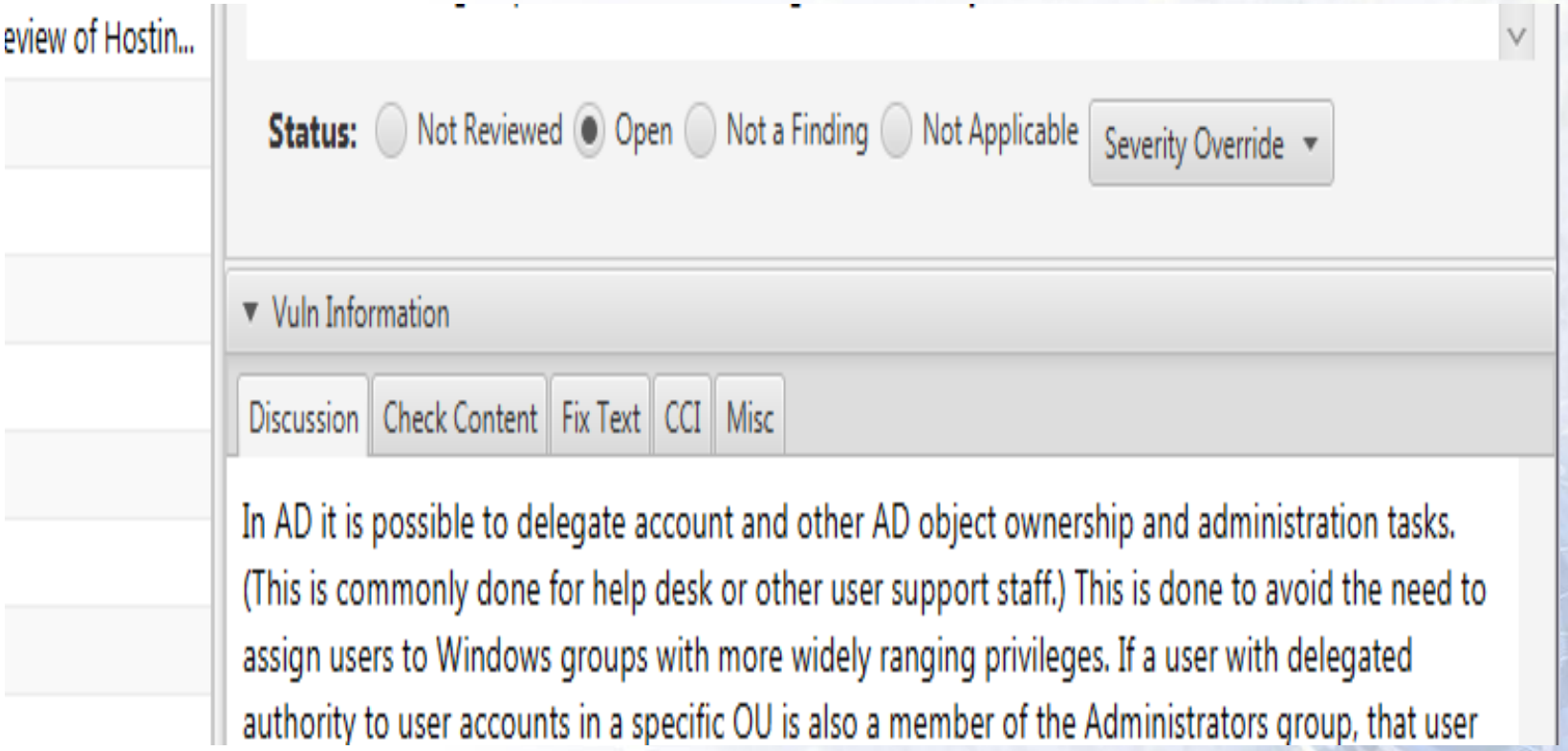
A Look At DISA STIGs (2)

Status



A Look At DISA STIGs (2)

Vuln Information



A Look At DISA STIGs (2)

- In the next module lets look at further details

END

A Look At STIGs Viewer

https://public.cyber.mil/stigs/srg-stig-tools/

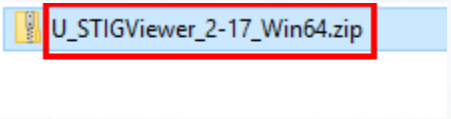
DoD CYBER EXCHANGE PUBLIC

- Frequently Asked Questions – FAQs
- Group Policy Objects
- Quarterly Release Schedule and Summary
- SRG / STIG Library Compilations
- SRG / STIG Mailing List
- SRG/STIG Tools and Viewing Guidance
- Sunset Products
- Vendor STIG Development Process
- Help

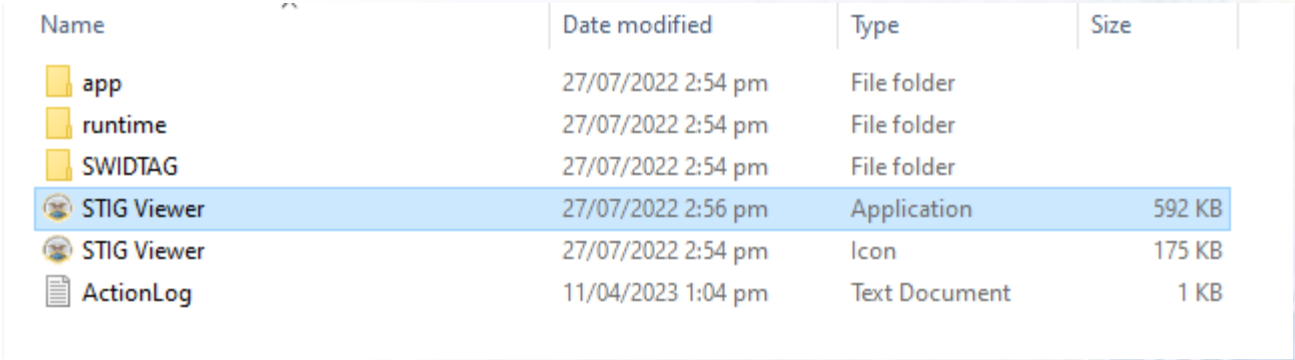
Show 10 entries

TITLE
How to Create and SRG-STIG ID Mapping Spreadsheet
STIG Sorted by STIG ID
STIG Sorted by Vulnerability ID
STIG Viewer 2.17
STIG Viewer 2.17 Hashes
STIG Viewer 2.17-Linux
STIG Viewer 2.17-Win64
STIG Viewer 2.17-Win64 msi
STIG Viewer User Guide (Sep 2022)
STIG Viewer Video

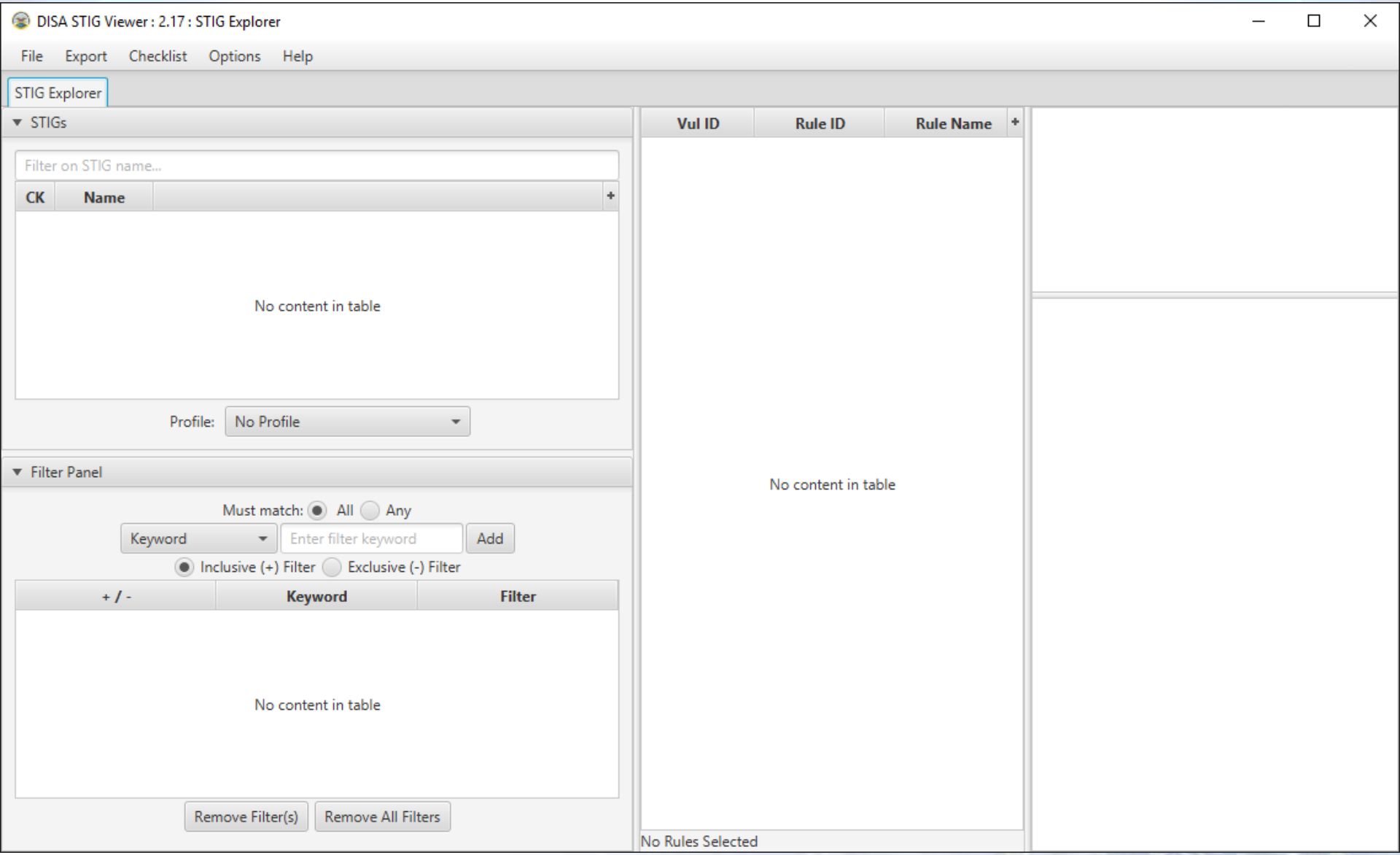
Showing 1 to 10 of 11 entries

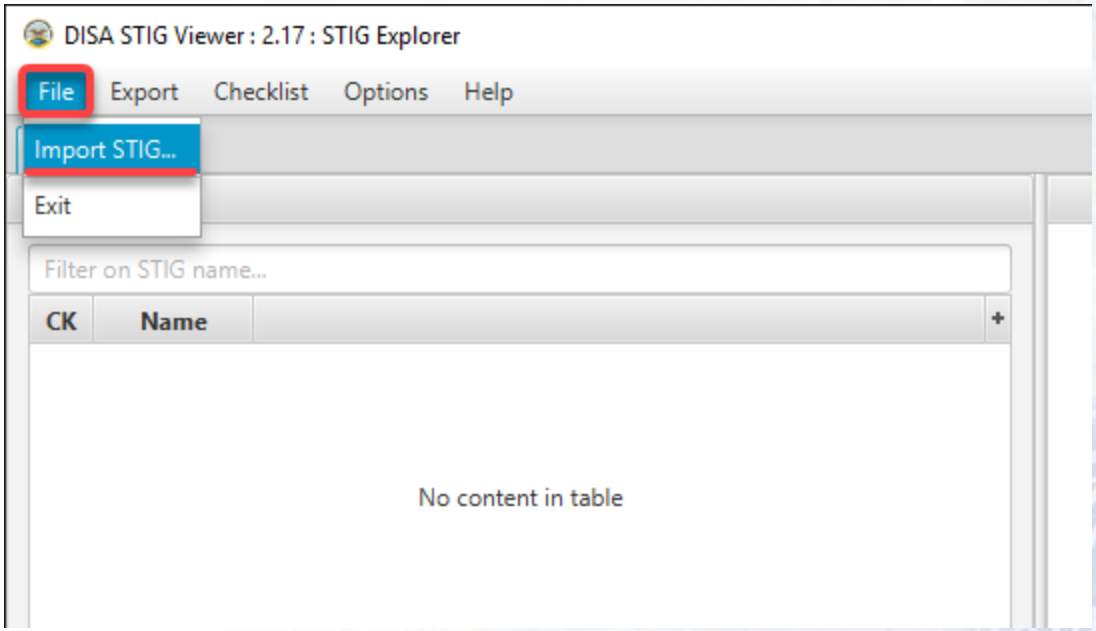


https://public.cyber.mil/stigs/srg-stig-tools/

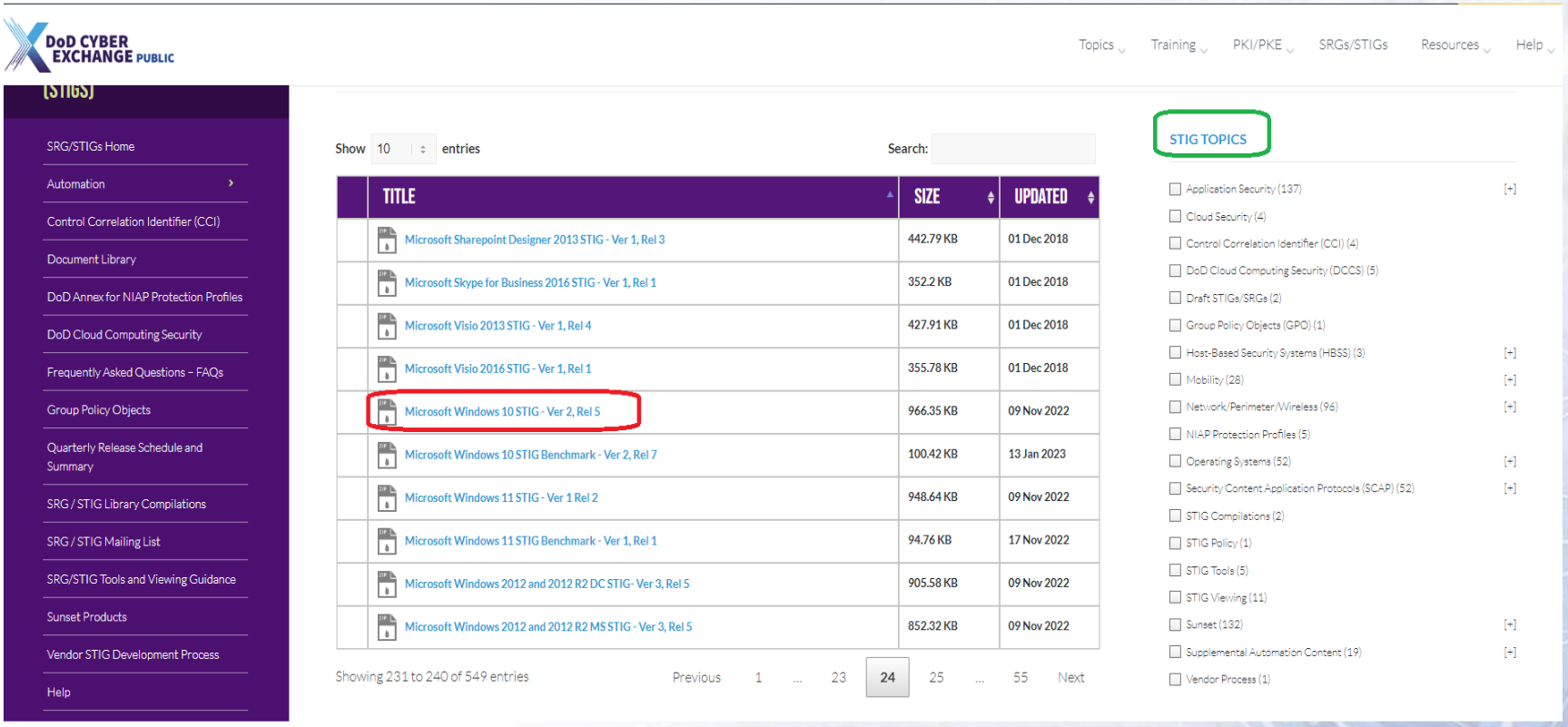


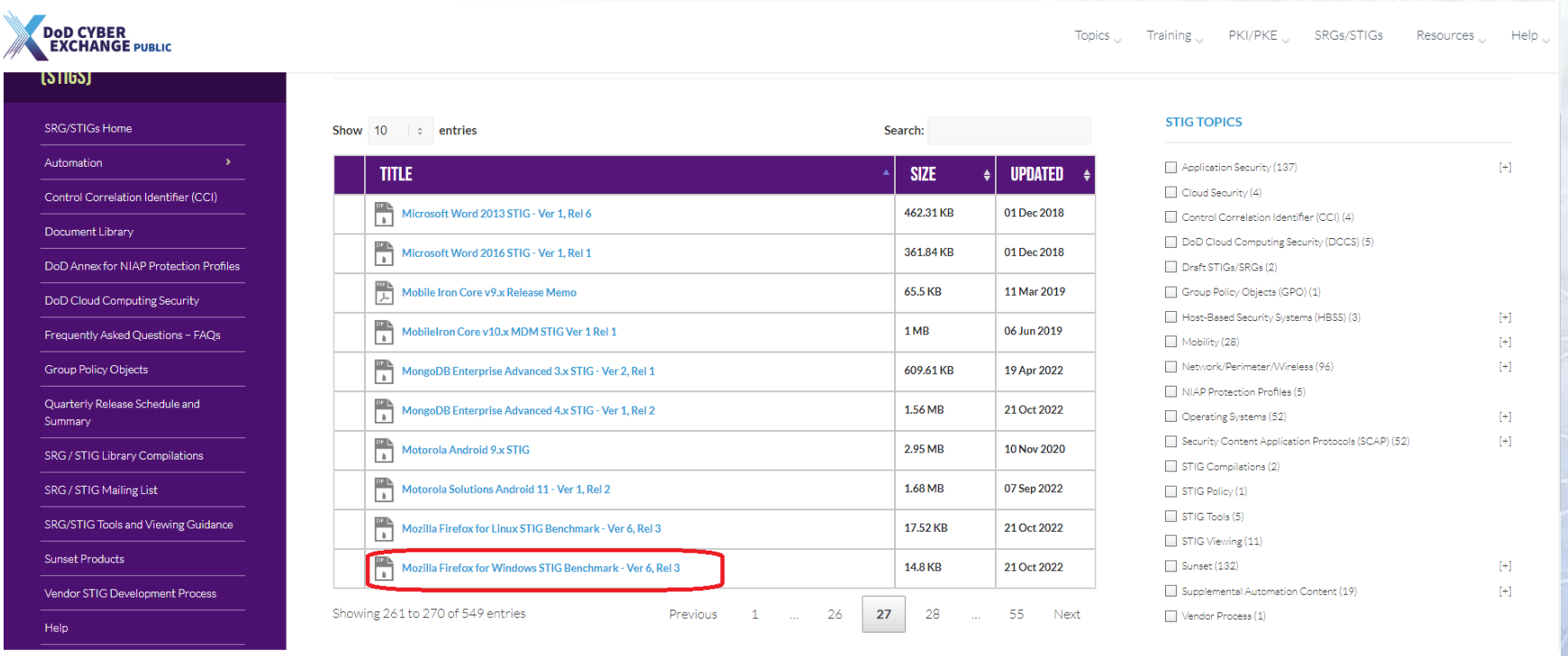
Name	Date modified	Type	Size
app	27/07/2022 2:54 pm	File folder	
runtime	27/07/2022 2:54 pm	File folder	
SWIDTAG	27/07/2022 2:54 pm	File folder	
STIG Viewer	27/07/2022 2:56 pm	Application	592 KB
STIG Viewer	27/07/2022 2:54 pm	Icon	175 KB
ActionLog	11/04/2023 1:04 pm	Text Document	1 KB

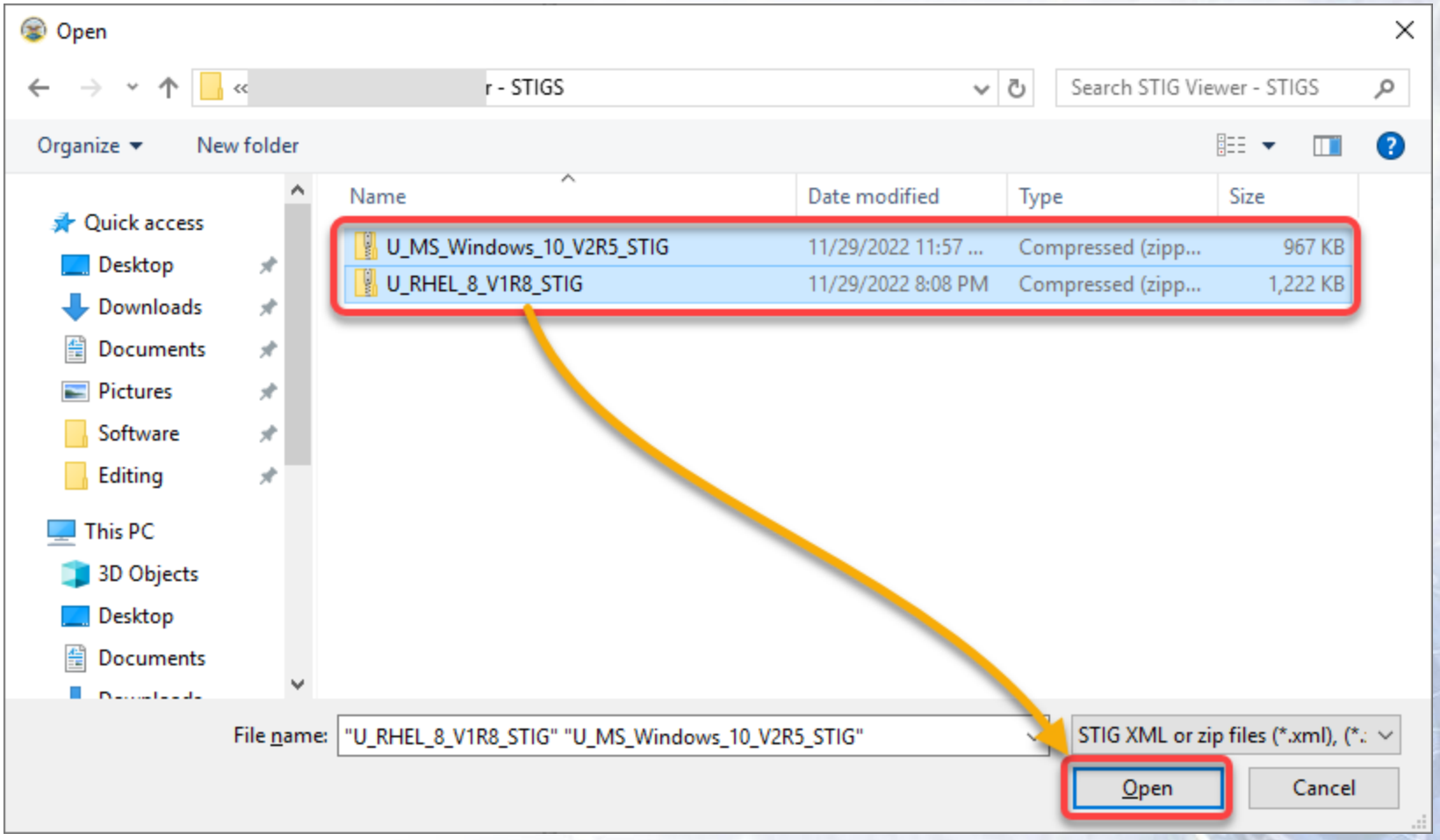

DISA STIG Viewer : 2.17 : STIG Explorer
File
Export
Checklist
Options
Help
STIG Explorer
STIGs
Filter on STIG name...
CK
Name
No content in table
Profile:
No Profile
Filter Panel
Must match:
All
Any
Keyword
Enter filter keyword
Add
Inclusive (+) Filter
Exclusive (-) Filter
+ / -
Keyword
Filter
No content in table
Remove Filter(s)
Remove All Filters
Vul ID
Rule ID
Rule Name
No content in table
No Rules Selected

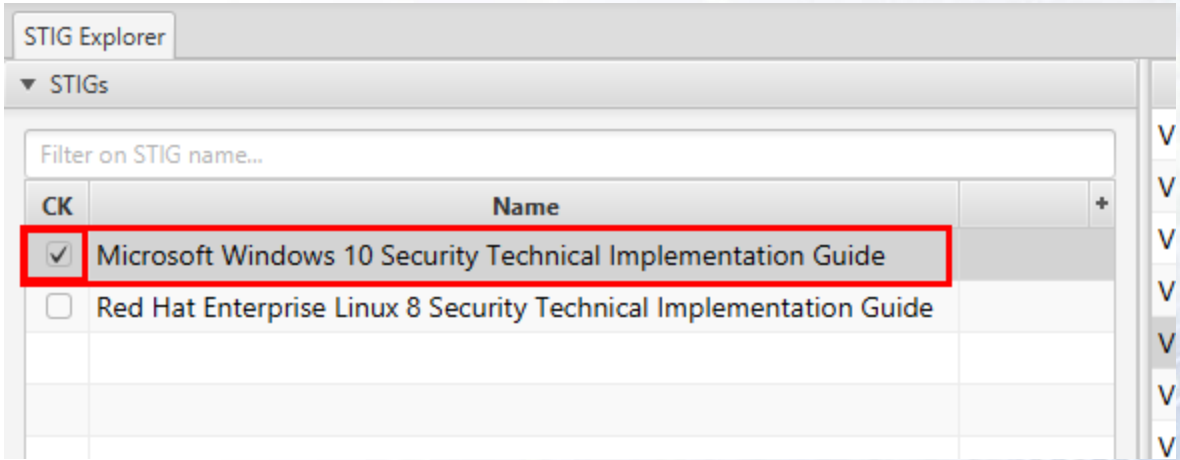

DISA STIG Viewer : 2.17 : STIG Explorer
File
Export
Checklist
Options
Help
Import STIG...
Exit
Filter on STIG name...
CK
Name
No content in table

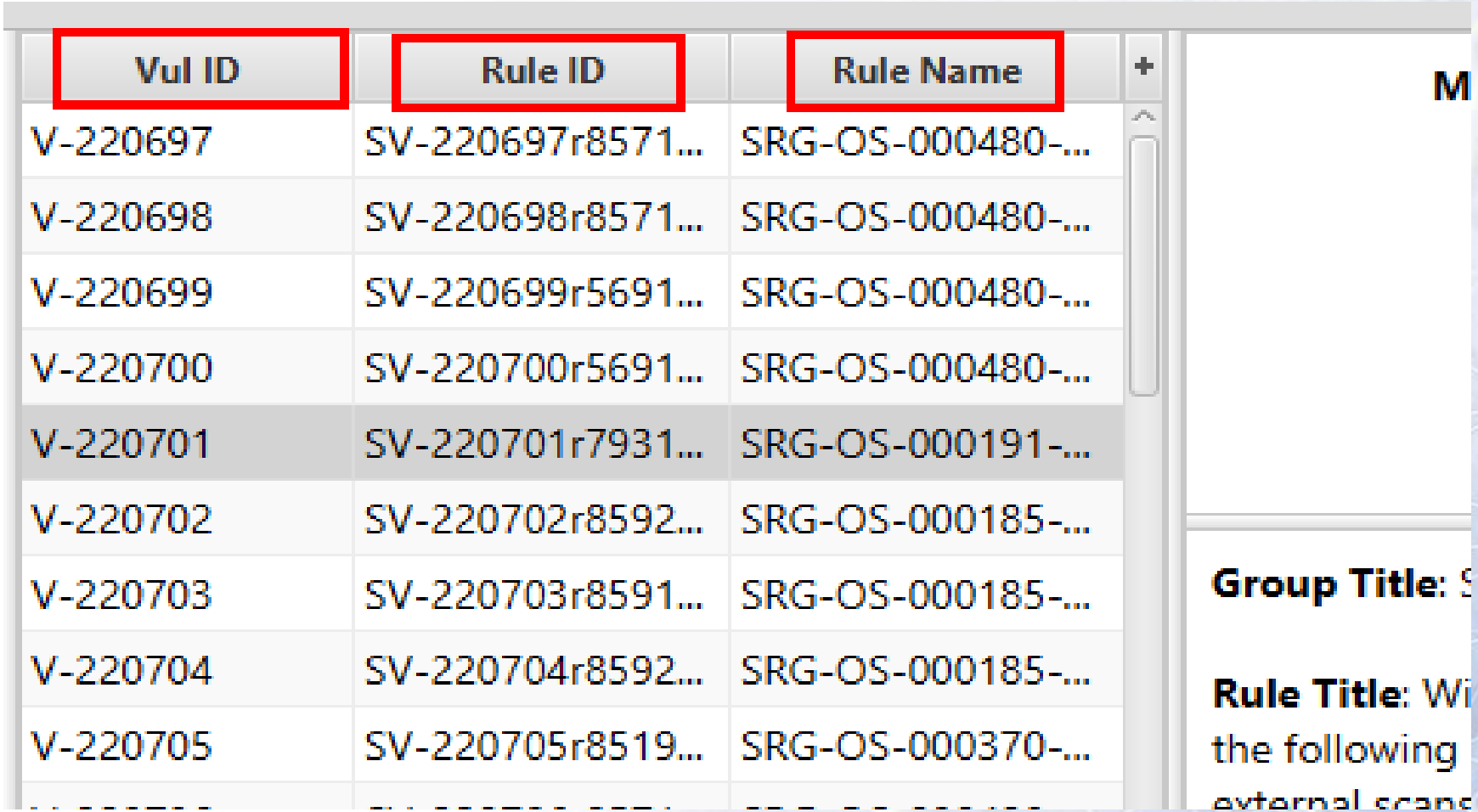
A Look At STIGs Viewer

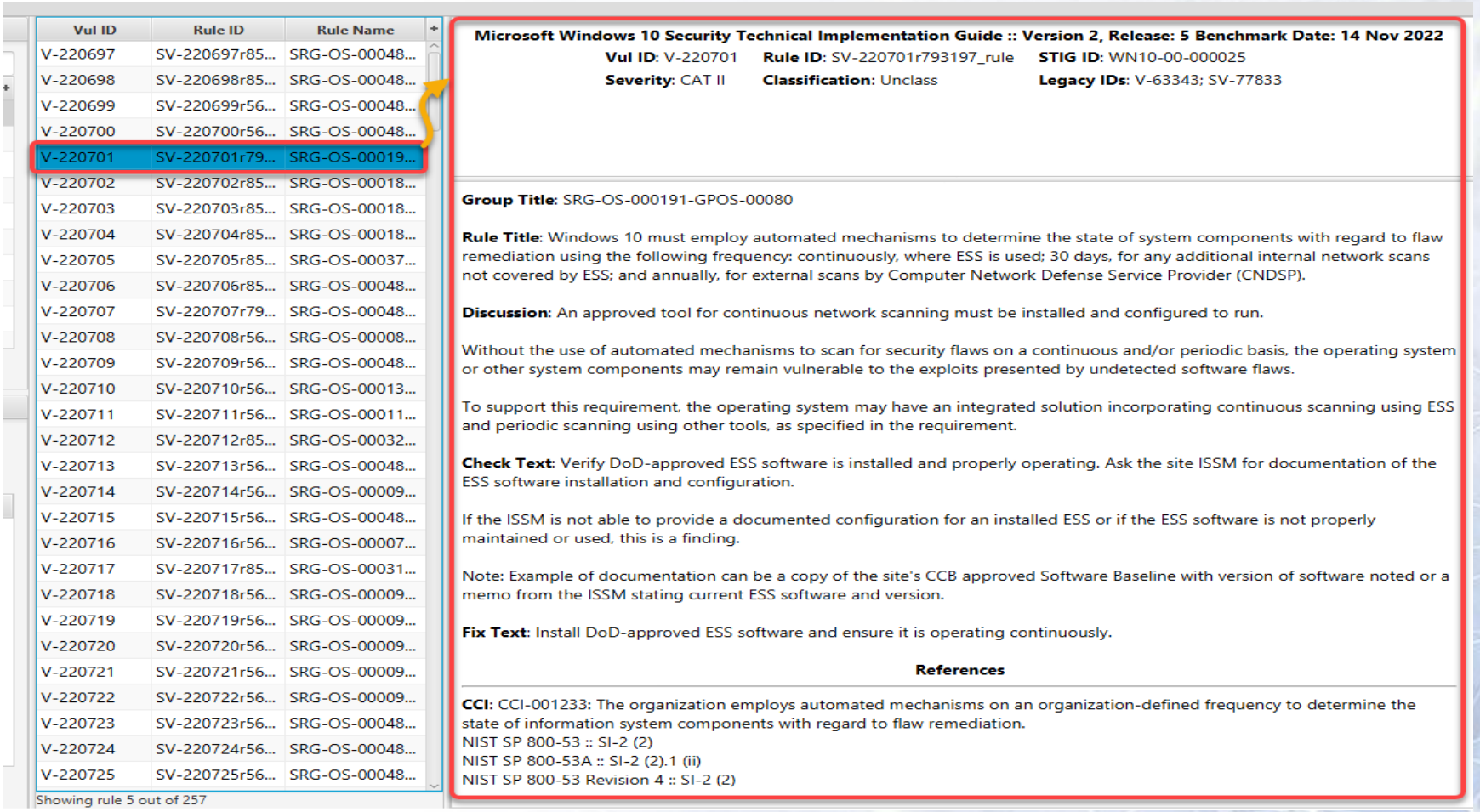



DoD CYBER EXCHANGE PUBLIC
Topics
Training
PKI/PKE
SRGs/STIGs
Resources
Help
(STIGS)
SRG/STIGs Home
Automation
Control Correlation Identifier (CCI)
Document Library
DoD Annex for NIAP Protection Profiles
DoD Cloud Computing Security
Frequently Asked Questions – FAQs
Group Policy Objects
Quarterly Release Schedule and Summary
SRG / STIG Library Compilations
SRG / STIG Mailing List
SRG/STIG Tools and Viewing Guidance
Sunset Products
Vendor STIG Development Process
Help
Show 10 entries
Search:
TITLE
SIZE
UPDATED
Microsoft Word 2013 STIG - Ver 1, Rel 6 462.31 KB 01 Dec 2018
Microsoft Word 2016 STIG - Ver 1, Rel 1 361.84 KB 01 Dec 2018
Mobile Iron Core v9.x Release Memo 65.5 KB 11 Mar 2019
MobileIron Core v10.x MDM STIG Ver 1 Rel 1 1 MB 06 Jun 2019
MongoDB Enterprise Advanced 3.x STIG - Ver 2, Rel 1 609.61 KB 19 Apr 2022
MongoDB Enterprise Advanced 4.x STIG - Ver 1, Rel 2 1.56 MB 21 Oct 2022
Motorola Android 9.x STIG 2.95 MB 10 Nov 2020
Motorola Solutions Android 11 - Ver 1, Rel 2 1.68 MB 07 Sep 2022
Mozilla Firefox for Linux STIG Benchmark - Ver 6, Rel 3 17.52 KB 21 Oct 2022
Mozilla Firefox for Windows STIG Benchmark - Ver 6, Rel 3 14.8 KB 21 Oct 2022
Showing 261 to 270 of 549 entries
Previous 1 ... 26 27 28 ... 55 Next
STIG TOPICS
Application Security (137) [+]
Cloud Security (4)
Control Correlation Identifier (CCI) (4)
DoD Cloud Computing Security (DCCS) (5)
Draft STIGs/SRGs (2)
Group Policy Objects (GPO) (1)
Host-Based Security Systems (HBSS) (3) [+]
Mobility (28) [+]
Network/Perimeter/Wireless (96) [+]
NIAP Protection Profiles (5)
Operating Systems (52) [+]
Security Content Application Protocols (SCAP) (52) [+]
STIG Compilations (2)
STIG Policy (1)
STIG Tools (5)
STIG Viewing (11)
Sunset (132) [+]
Supplemental Automation Content (19) [+]
Vendor Process (1)


Open
r - STIGS
Search STIG Viewer - STIGS
Organize
New folder
Quick access
Desktop
Downloads
Documents
Pictures
Software
Editing
This PC
3D Objects
Desktop
Documents
Name
Date modified
Type
Size
U_MS_Windows_10_V2R5_STIG
11/29/2022 11:57 ...
Compressed (zipp...
967 KB
U_RHEL_8_V1R8_STIG
11/29/2022 8:08 PM
Compressed (zipp...
1,222 KB
File name:
"U_RHEL_8_V1R8_STIG" "U_MS_Windows_10_V2R5_STIG"
STIG XML or zip files (*.xml), (*.
Open
Cancel


STIG Explorer
STIGs
Filter on STIG name...
CK
Name
Microsoft Windows 10 Security Technical Implementation Guide
Red Hat Enterprise Linux 8 Security Technical Implementation Guide


Vul ID
Rule ID
Rule Name
V-220697
SV-220697r8571...
SRG-OS-000480-...
V-220698
SV-220698r8571...
SRG-OS-000480-...
V-220699
SV-220699r5691...
SRG-OS-000480-...
V-220700
SV-220700r5691...
SRG-OS-000480-...
V-220701
SV-220701r7931...
SRG-OS-000191-...
V-220702
SV-220702r8592...
SRG-OS-000185-...
V-220703
SV-220703r8591...
SRG-OS-000185-...
V-220704
SV-220704r8592...
SRG-OS-000185-...
V-220705
SV-220705r8519...
SRG-OS-000370-...
Group Title:
Rule Title:
the following


Vul ID
Rule ID
Rule Name
V-220697 SV-220697r85... SRG-OS-00048...
V-220698 SV-220698r85... SRG-OS-00048...
V-220699 SV-220699r56... SRG-OS-00048...
V-220700 SV-220700r56... SRG-OS-00048...
V-220701 SV-220701r79... SRG-OS-00019...
V-220702 SV-220702r85... SRG-OS-00018...
V-220703 SV-220703r85... SRG-OS-00018...
V-220704 SV-220704r85... SRG-OS-00018...
V-220705 SV-220705r85... SRG-OS-00037...
V-220706 SV-220706r85... SRG-OS-00048...
V-220707 SV-220707r79... SRG-OS-00048...
V-220708 SV-220708r56... SRG-OS-00008...
V-220709 SV-220709r56... SRG-OS-00048...
V-220710 SV-220710r56... SRG-OS-00013...
V-220711 SV-220711r56... SRG-OS-00011...
V-220712 SV-220712r85... SRG-OS-00032...
V-220713 SV-220713r56... SRG-OS-00048...
V-220714 SV-220714r56... SRG-OS-00009...
V-220715 SV-220715r56... SRG-OS-00048...
V-220716 SV-220716r56... SRG-OS-00007...
V-220717 SV-220717r85... SRG-OS-00031...
V-220718 SV-220718r56... SRG-OS-00009...
V-220719 SV-220719r56... SRG-OS-00009...
V-220720 SV-220720r56... SRG-OS-00009...
V-220721 SV-220721r56... SRG-OS-00009...
V-220722 SV-220722r56... SRG-OS-00009...
V-220723 SV-220723r56... SRG-OS-00048...
V-220724 SV-220724r56... SRG-OS-00048...
V-220725 SV-220725r56... SRG-OS-00048...
Showing rule 5 out of 257
Microsoft Windows 10 Security Technical Implementation Guide :: Version 2, Release: 5 Benchmark Date: 14 Nov 2022
Vul ID: V-220701 Rule ID: SV-220701r793197_rule STIG ID: WN10-00-000025
Severity: CAT II Classification: Unclass Legacy IDs: V-63343; SV-77833
Group Title: SRG-OS-000191-GPOS-00080
Rule Title: Windows 10 must employ automated mechanisms to determine the state of system components with regard to flaw remediation using the following frequency: continuously, where ESS is used; 30 days, for any additional internal network scans not covered by ESS; and annually, for external scans by Computer Network Defense Service Provider (CNDSP).
Discussion: An approved tool for continuous network scanning must be installed and configured to run.
Without the use of automated mechanisms to scan for security flaws on a continuous and/or periodic basis, the operating system or other system components may remain vulnerable to the exploits presented by undetected software flaws.
To support this requirement, the operating system may have an integrated solution incorporating continuous scanning using ESS and periodic scanning using other tools, as specified in the requirement.
Check Text: Verify DoD-approved ESS software is installed and properly operating. Ask the site ISSM for documentation of the ESS software installation and configuration.
If the ISSM is not able to provide a documented configuration for an installed ESS or if the ESS software is not properly maintained or used, this is a finding.
Note: Example of documentation can be a copy of the site's CCB approved Software Baseline with version of software noted or a memo from the ISSM stating current ESS software and version.
Fix Text: Install DoD-approved ESS software and ensure it is operating continuously.
References
CCI: CCI-001233: The organization employs automated mechanisms on an organization-defined frequency to determine the state of information system components with regard to flaw remediation.
NIST SP 800-53 :: SI-2 (2)
NIST SP 800-53A :: SI-2 (2).1 (ii)
NIST SP 800-53 Revision 4 :: SI-2 (2)

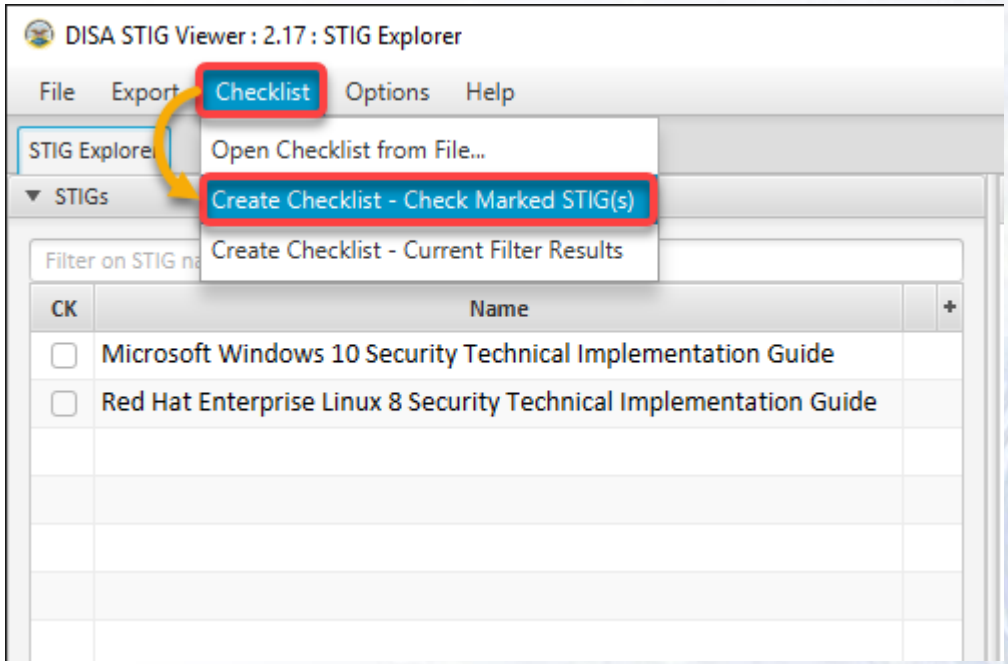
Microsoft Windows 10 Security Technical Implementation Guide :: Version 2, Release: 5 Benchmark Date: 14 Nov 2022

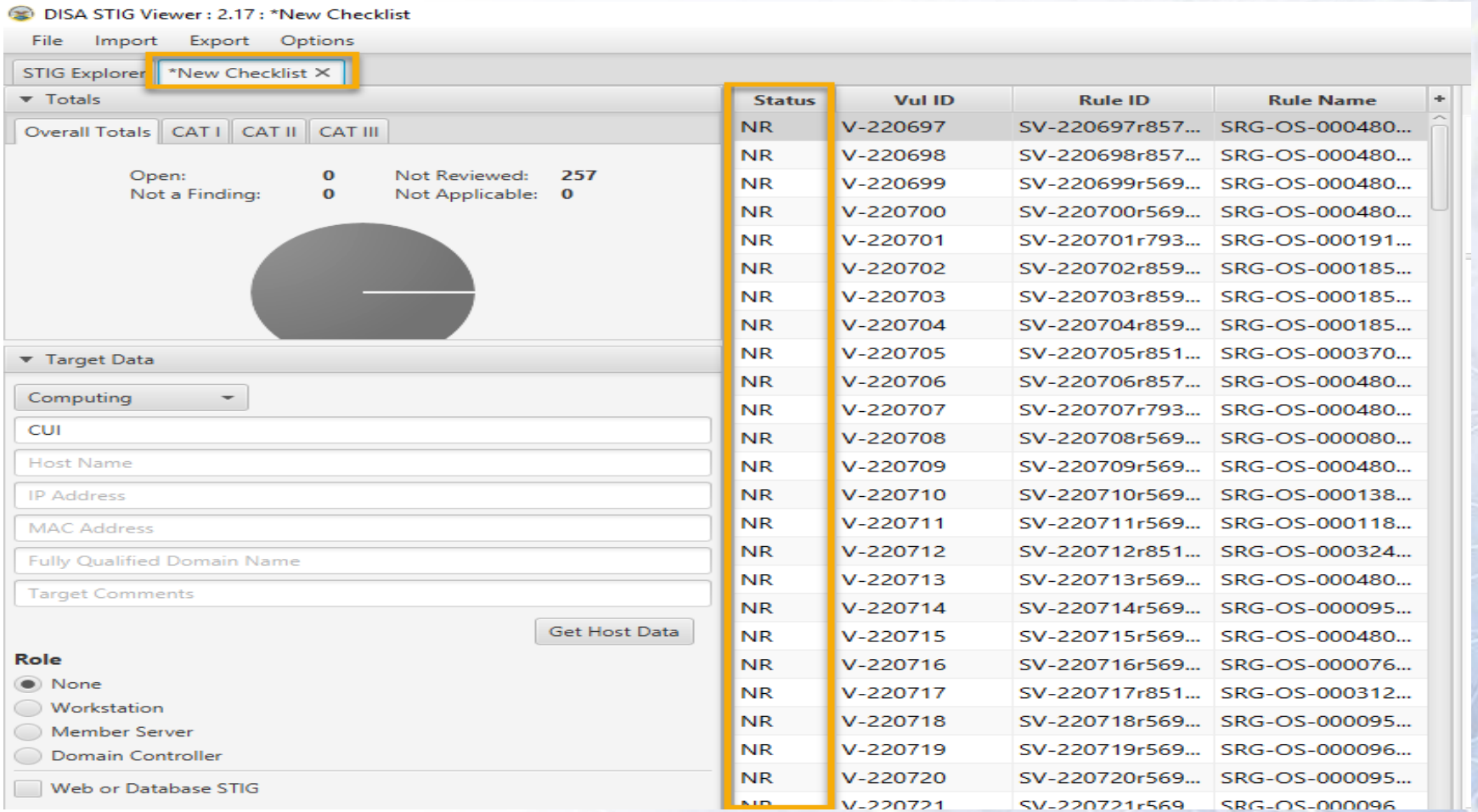
Vul ID: V-220701	**Rule ID**: SV-220701r793197_rule	**STIG ID**: WN10-00-000025
Severity: CAT II	**Classification**: Unclass	**Legacy IDs**: V-63343; SV-77833

Group Title: SRG-OS-000191-GPOS-00080

Rule Title: Windows 10 must employ automated mechanisms to determine the state of system components with regard to flaw remediation using the following frequency: continuously, where ESS is used; 30 days, for any additional internal network scans not covered by ESS; and annually, for external scans by Computer Network Defense Service Provider (CNDSP).

Discussion: An approved tool for continuous network scanning must be installed and configured to run.

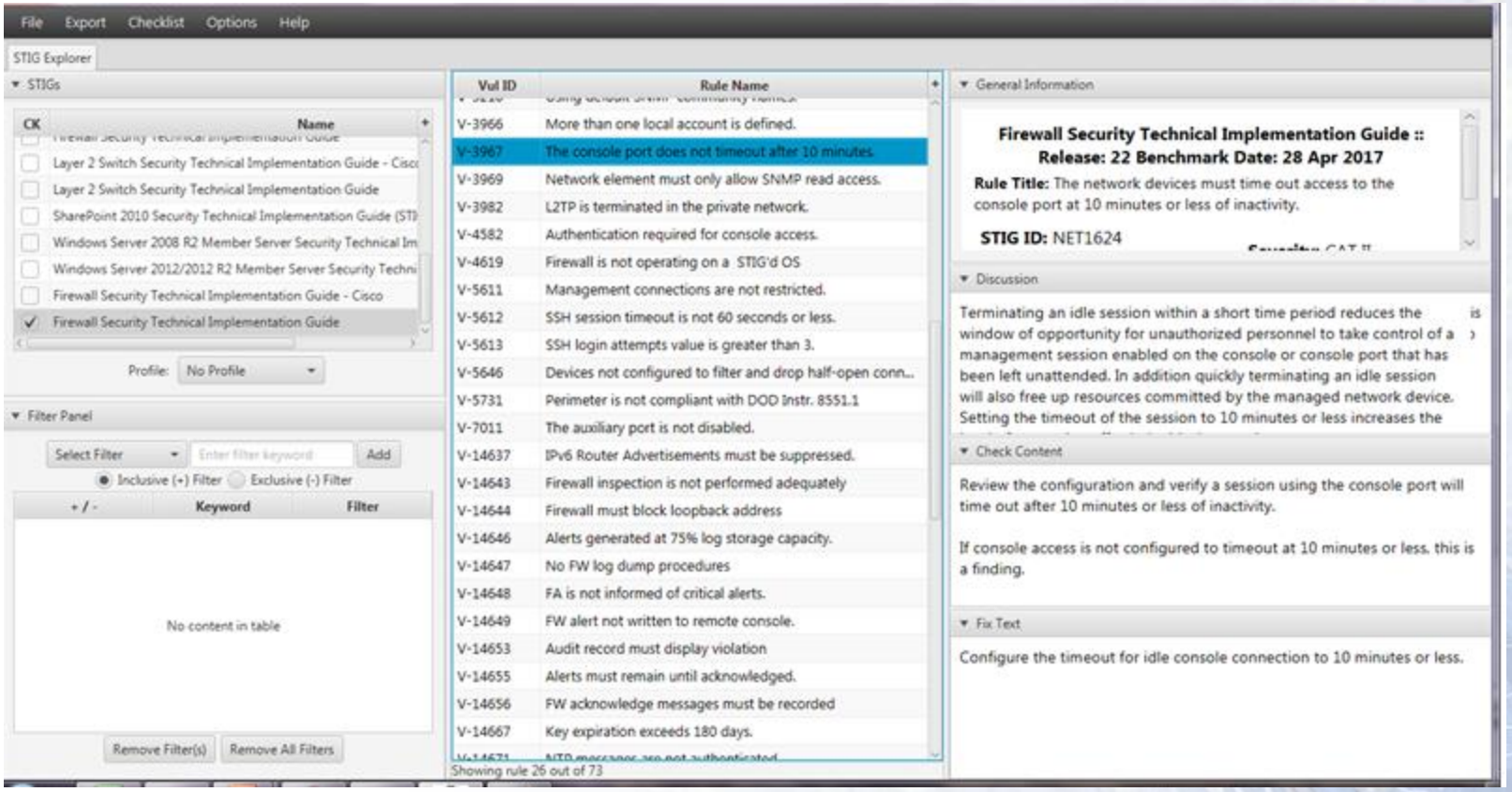

DISA STIG Viewer : 2.17 : STIG Explorer
File
Export
Checklist
Options
Help
STIG Explorer
Open Checklist from File...
Create Checklist - Check Marked STIG(s)
Create Checklist - Current Filter Results
STIGs
Filter on STIG na
CK
Name
Microsoft Windows 10 Security Technical Implementation Guide
Red Hat Enterprise Linux 8 Security Technical Implementation Guide


DISA STIG Viewer : 2.17 : *New Checklist
File
Import
Export
Options
STIG Explorer
*New Checklist
Totals
Overall Totals
CAT I
CAT II
CAT III
Open: 0
Not a Finding: 0
Not Reviewed: 257
Not Applicable: 0
Target Data
Computing
CUI
Host Name
IP Address
MAC Address
Fully Qualified Domain Name
Target Comments
Get Host Data
Role
None
Workstation
Member Server
Domain Controller
Web or Database STIG
Status
Vul ID
Rule ID
Rule Name
NR V-220697 SV-220697r857... SRG-OS-000480...
NR V-220698 SV-220698r857... SRG-OS-000480...
NR V-220699 SV-220699r569... SRG-OS-000480...
NR V-220700 SV-220700r569... SRG-OS-000480...
NR V-220701 SV-220701r793... SRG-OS-000191...
NR V-220702 SV-220702r859... SRG-OS-000185...
NR V-220703 SV-220703r859... SRG-OS-000185...
NR V-220704 SV-220704r859... SRG-OS-000185...
NR V-220705 SV-220705r851... SRG-OS-000370...
NR V-220706 SV-220706r857... SRG-OS-000480...
NR V-220707 SV-220707r793... SRG-OS-000480...
NR V-220708 SV-220708r569... SRG-OS-000080...
NR V-220709 SV-220709r569... SRG-OS-000480...
NR V-220710 SV-220710r569... SRG-OS-000138...
NR V-220711 SV-220711r569... SRG-OS-000118...
NR V-220712 SV-220712r851... SRG-OS-000324...
NR V-220713 SV-220713r569... SRG-OS-000480...
NR V-220714 SV-220714r569... SRG-OS-000095...
NR V-220715 SV-220715r569... SRG-OS-000480...
NR V-220716 SV-220716r569... SRG-OS-000076...
NR V-220717 SV-220717r851... SRG-OS-000312...
NR V-220718 SV-220718r569... SRG-OS-000095...
NR V-220719 SV-220719r569... SRG-OS-000096...
NR V-220720 SV-220720r569... SRG-OS-000095...

A Look At DISA STIGs (4)

- Firewall Security Technical Implementation Guide
- Vulnerability ID: V-3967
- Rule name: The console port does not timeout after 10 mins

A Look At DISA STIGs (4)



A Look At DISA STIGs (4)

- General Information:
  - **Rule Title:** The network devices must time out access to the console port at 10 minutes or less of inactivity
  - **STIG ID:** NET1624
  - **Severity:** CAT II

A Look At DISA STIGs (4)

- Discussion:
  - Terminating an idle session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console…

A Look At DISA STIGs (4)

- Discussion…:
  - port that has been left unattended. In addition quickly terminating an idle session will also free up resources committed by the managed network device. Setting the timeout of the session to 10 minutes

A Look At DISA STIGs (4)

- Discussion…:
  - or less increases the level of protection afforded critical network components

A Look At DISA STIGs (4)

- Check Content:
  - Review the configuration and verify a session using the console port will time out after 10 mins or less of inactivity.
  - If console access is not configured to timeout at 10 minutes or less, this is a finding.

A Look At DISA STIGs (4)

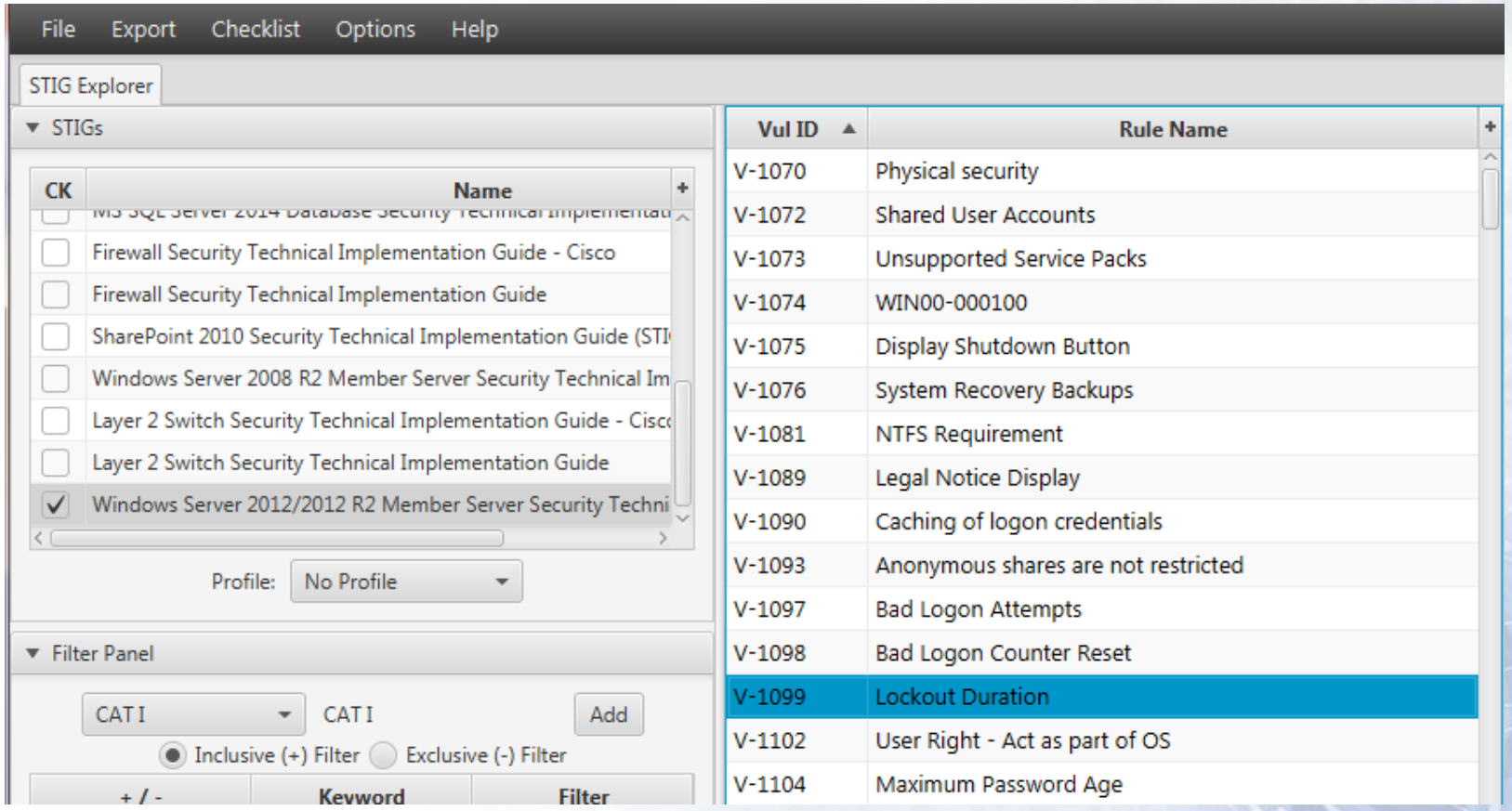
- Fix Text:
  - Configure the timeout for idle console connection to 10 minutes or less.

END

A Look At DISA STIGs (3)

- Windows Server 2012 R2 Member Server
  - Import STIG
  - V1099 (Lockout duration)

A Look At DISA STIGs (2)



A Look At DISA STIGs (2)

Vul ID	Rule Name
V-1070	Physical security
V-1072	Shared User Accounts
V-1073	Unsupported Service Packs
V-1074	WIN00-000100
V-1075	Display Shutdown Button
V-1076	System Recovery Backups
V-1081	NTFS Requirement
V-1089	Legal Notice Display
V-1090	Caching of logon credentials
V-1093	Anonymous shares are not restricted
V-1097	Bad Logon Attempts
V-1098	Bad Logon Counter Reset
V-1099	Lockout Duration
V-1102	User Right - Act as part of OS
V-1104	Maximum Password Age
V-1105	Minimum Password Age
V-1107	Password Uniqueness
V-1112	Dormant Accounts
V-1113	Disable Guest Account
V-1114	Rename Built-in Guest Account
V-1115	Rename Built-in Administrator Account

▼ General Information

Windows Server 2012/2012 R2 Member Server Security Technical Implementation Guide :: Release: 8 Benchmark Date: 28 Apr 2017

Rule Title: The lockout duration must be configured to require an

▼ Discussion

The account lockout feature, when enabled, prevents brute-force password attacks on the system. This parameter specifies the period of time that an account will remain locked after the specified number of failed logon attempts. A value of 0 will require an administrator to unlock the account.

▼ Check Content

Verify the effective setting in Local Group Policy Editor.
Run "gpedit.msc".

Navigate to Local Computer Policy -> Computer Configuration -> Windows Settings -> Security Settings -> Account Policies -> Account

▼ Fix Text

Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Account Policies -> Account Lockout Policy -> "Account lockout duration" to "0" minutes, "Account is locked out until administrator unlocks it".

▼ CCI

A Look At DISA STIGs (3)

- Rule Title:
  - The lockout duration must be configured to require an administrator to unlock an account
  - Severity: CAT II

A Look At DISA STIGs (3)

- Discussion:
  - The account lockout feature, when enabled, prevents brute-force password attacks on the system. This parameter specifies the period of time that an account will remain locked after the specified number

A Look At DISA STIGs (3)

- Discussion…:
  - of failed logon attempts. A value of 0 will require an administrator to unlock the account.

A Look At DISA STIGs (3)

- Check Content:
  - Verify the effective setting in Local Group Policy Editor.
    Run "gpedit.msc".

A Look At DISA STIGs (3)

- Check Content:
  - Navigate to Local Computer Policy -> Computer Configuration -> Windows Settings -> Security Settings -> Account Policies -> Account Lockout Policy.

A Look At DISA STIGs (3)

- Check Content…:
  - If the "Account lockout duration" is not set to "0", requiring an administrator to unlock the account, this is a finding.

A Look At DISA STIGs (3)

- Fix Text:
  - Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Account Policies -> Account Lockout Policy -> "Account lockout duration" to "0" minutes,

A Look At DISA STIGs (3)

- Fix Text…..:
  - "Account is locked out until administrator unlocks it".
- CCI: NIST SP 800-53 Revision 4 :: AC-7 b

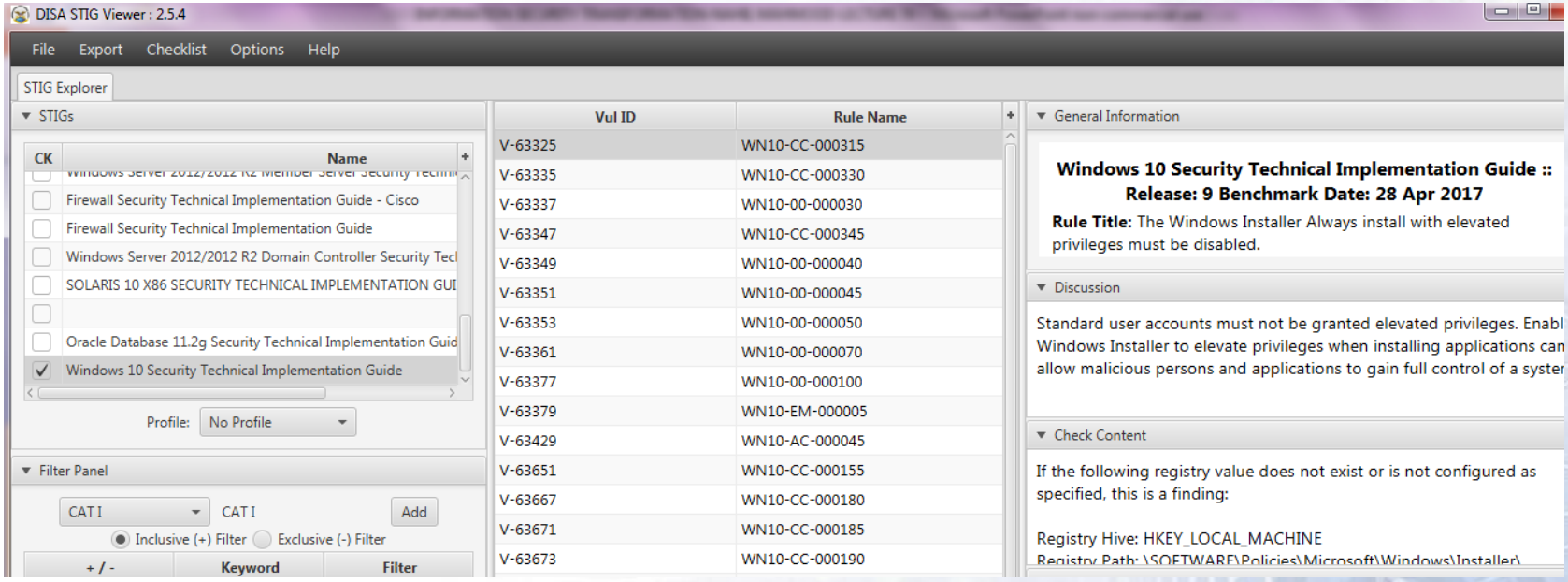
END

Security Hardening – Case Study – Win 10

- Windows 10
- DISA, Release 9
  - 28 April 2017

Security Hardening – Case Study – Win 10

STIGVIEWER WINDOW



Security Hardening – Case Study – Win 10

- General Information:
  - **Rule Title:** The antivirus program must be configured to update signature files on a daily basis.
  - **STIG ID**: WN10-00-000046
  - **Severity**: CAT I

Security Hardening – Case Study – Win 10

- Discussion:
  - Virus scan programs are a primary line of defense against the introduction of viruses and malicious code that can destroy data and even render a computer inoperable. Using a virus scan program provides the ability to…

Security Hardening – Case Study – Win 10

- Discussion…:
  - …detect malicious code before extensive damage occurs. Updated virus scan data files help protect a system, as constantly changing malware is identified by the antivirus software vendors

Security Hardening – Case Study – Win 10

- Check Content:
  - This requirement is NA if McAfee VirusScan Enterprise (VSE) is used. It will be addressed with the corresponding McAfee VSE STIG.
  - Configurations will vary depending on the product.

Security Hardening – Case Study – Win 10

- Fix Text:
  - Configure the antivirus program to update signature files at least daily. Ensure the updates are occurring on timely basis and are not more than a week old.

Security Hardening – Case Study – Win 10

END

- CCI (Control Correlation Identifier):
  - CCI: 000366
    The org implements the security config settings.
    NIST SP 800-53 :: CM-6 b
    NIST SP 800-53A :: CM-6.1 (iv)
    NIST SP 800-53 Revision 4 :: CM-6

Comparison of CIS Vs DISA

Comparison of CIS Vs DISA

- Many controls are common
- Approaches are different
- Organization styles are different

Comparison of CIS Vs DISA

FEATURE	CIS	DISA
CONTROL COVERAGE	GOOD	EXCELLENT
ORG SUITABILITY	SMALL AND MEDIUM ORGS	LARGE ORGS
USER FRIENDLINESS	GOOD	SATISFACTORY
UNUSABLE TERMINOLOGY	NO	YES
CONTROL DETAIL	GOOD	SATISFACTORY
TOOLS	CAT (COMMERCIAL)	SCAP (MILITARY USE)

Comparison of CIS Vs DISA

FEATURE	CIS	DISA
CONTROL PRIORITIZATION	LEVEL 1, LEVEL 2	CAT I - CAT III
TRACKING EASE	CAT TOOL (COMMERCIAL)	FREE STIG VIEWER (CHECKLIST)
FREQUENCY OF UPDATES	FAIR	QUARTERLY
INDUSTRY CREDIBILITY	HIGH	VERY HIGH
INDUSTRY ADOPTION	HIGH	MODERATE

Comparison of CIS Vs DISA

- How to select CIS/DISA:
  - Size of organization
  - IT infrastructure extent
  - Nature of business
  - Security program goals
  - Maturity of IT & security staff

Comparison of CIS Vs DISA

- Rule of thumb:
  - Smaller orgs use CIS
  - Larger orgs use DISA
  - CIS is part of Homeland Security, DISA is part of US Military
  - DISA more frequently updated and maintained with wider coverage

END

ISMS:Leading InfoSec Governance Framework

- ISO27001:2013 (ISMS)
  - Specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system
  - Ten short clauses
  - Long annex

ISMS:Leading InfoSec Governance Framework

ISO27001:2013 MANDATORY CLAUSES

Reference		Description
Mandatory	Clause 4	Context of the organization
	Clause 5	Leadership
	Clause 6	Planning
	Clause 7	Support
	Clause 8	Operation
	Clause 9	Performance evaluation
	Clause 10	Improvement

https://chapters.theiia.org/bermuda/Events/ChapterDocuments/Information%20Security%20Management%20System%20%28ISMS%29%20Overview.pdf

ISMS:Leading InfoSec Governance Framework

ISO27001:2013 DISCRETIONARY CONTROLS

Reference		Description	Control Total
Discretionary	A5	Information security policies	2
	A6	Organization of information security	7
	A7	Human resource security	6
	A8	Asset management	10
	A9	Access control	13
	A10	Cryptography	2
	A11	Physical and environmental security	15
	A12	Operations security	14
	A13	Communications security	7
	A14	System acquisition, development and maintenance	13
	A15	Supplier relationships	5
	A16	Information security incident management	7
	A17	Information security aspects of business continuity management	4
	A18	Compliance	8

TOTAL: 113

https://chapters.theiia.org/bermuda/Events/ChapterDocuments/Information%20Security%20Management%20System%20%28ISMS%29%20Overview.pdf

ISMS:Leading InfoSec Governance Framework

- Merits of ISO27001:2013 (ISMS):
  - Exceptional framework with comprehensive coverage of mandatory requirements (clauses 4-10) and discretionary controls (annex)

ISMS:Leading InfoSec Governance Framework

- Merits of ISO27001:2013 (ISMS):
  - Highly beneficial as a framework for security program
  - Covers all domain areas
  - Provides a structure and organized sequence for security controls

ISMS:Leading InfoSec Governance Framework

- Merits of ISO27001:2013 (ISMS):
  - Complements security transformation model as serves as a reference and guideline for activities and controls

ISMS:Leading InfoSec Governance Framework

- **De-merits** of ISO27001:2013 (ISMS):
  - Very broad
  - Generic framework – leaves it to organization how to implement the measures and controls
  - Not suited for orgs that are new to security program

ISMS:Leading InfoSec Governance Framework

- How to best use advantages of ISO27001:2013 (ISMS):
  - Implement security transformational model
  - Cap off security transformation project with ISO27001:2013 (ISMS) certification

ISMS:Leading InfoSec Governance Framework

- How to best use advantages of ISO27001:2013 (ISMS):
  - ISMS as a complementary reference and checklist rather than main framework

How to Use ISO27002:2013

- What is ISO27002:2013 ?
  - Information technology -- Security techniques -- Code of practice for information security controls
  - Renamed from ISO 17799

How to Use ISO27002:2013

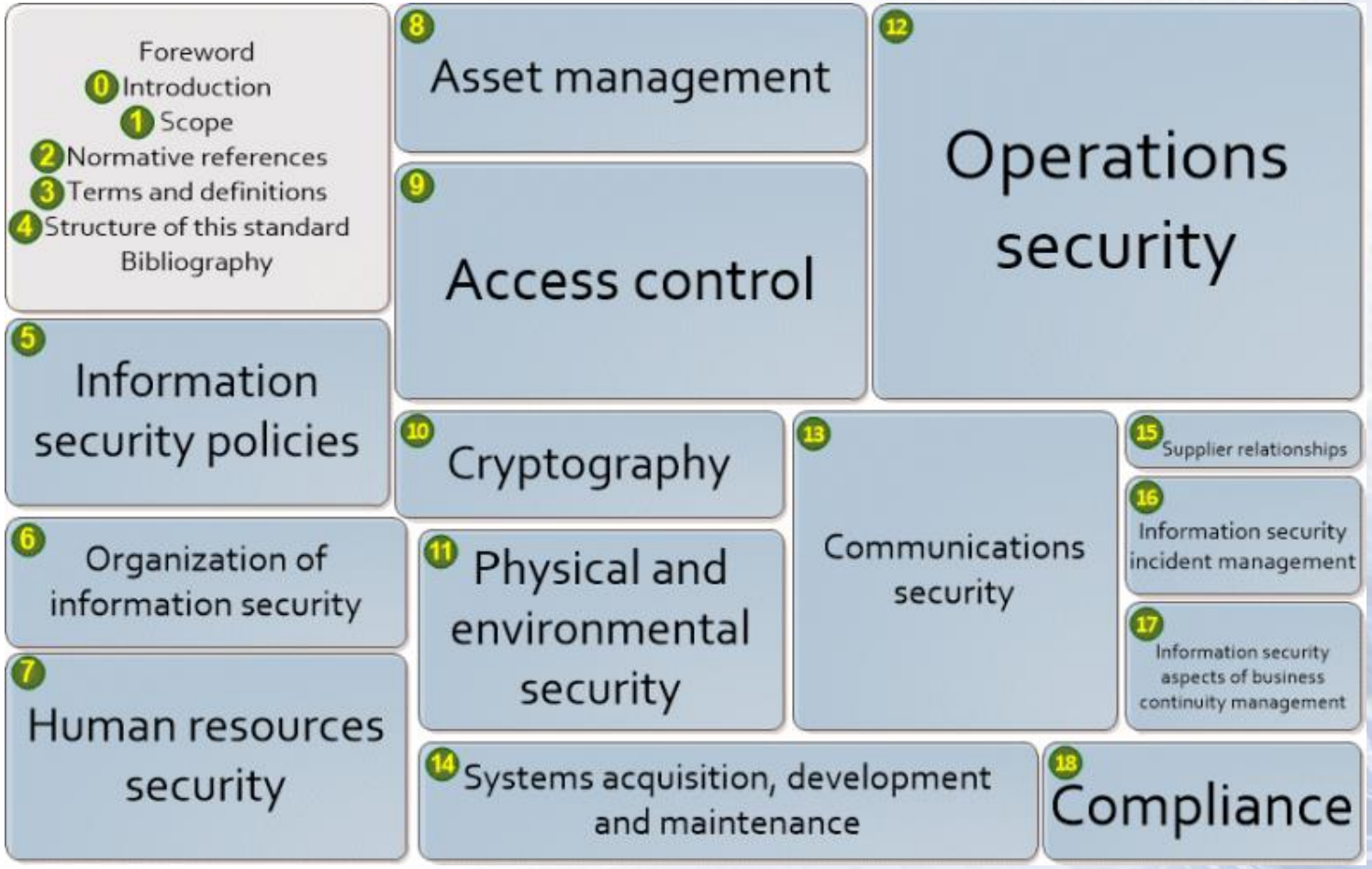
- 0.1 Background & Context
  - This Int'l Standard is designed for orgs to use as a **reference** for selecting controls within the process of implementing an Information Security Management System (ISMS) based on ISO/IEC 27001;

How to Use ISO27002:2013

- 0.1 Background & Context
  - or as a **guidance document** for organizations implementing commonly accepted information security controls.

How to Use ISO27002:2013

STRUCTURE OF ISO27002:2013



http://www.iso27001security.com/html/27002.html

How to Use ISO27002:2013

- Lets have a look at control A.5.1.2 (**Review Of The Policies Of Information Security**)

How to Use ISO27002:2013

ISO27001:2013

A.5.1.2	REVIEW OF THE POLICIES FOR INFORMATION SECURITY	***Control:*** The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

How to Use ISO27002:2013

ISO27002:2013

TITLE

5.1.2 Review of the policies for information security

Control

The policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

Implementation guidance

Each policy should have an owner who has approved management responsibility for the development, review and evaluation of the policies. The review should include assessing opportunities for improvement of the organization's policies and approach to managing information security in response to changes to the organizational environment, business circumstances, legal conditions or technical environment.

How to Use ISO27002:2013

ISO27002:2013

CONTROL

5.1.2 Review of the policies for information security

Control

The policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

Implementation guidance

Each policy should have an owner who has approved management responsibility for the development, review and evaluation of the policies. The review should include assessing opportunities for improvement of the organization's policies and approach to managing information security in response to changes to the organizational environment, business circumstances, legal conditions or technical environment.

How to Use ISO27002:2013

ISO27002:2013

5.1.2 Review of the policies for information security

Control

The policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

Implementation guidance

Each policy should have an owner who has approved management responsibility for the development, review and evaluation of the policies. The review should include assessing opportunities for improvement of the organization's policies and approach to managing information security in response to changes to the organizational environment, business circumstances, legal conditions or technical environment.

27002 IMPLEMENTATION GUIDANCE

How to Use ISO27002:2013

ISO27002:2013

A.5.1.2	REVIEW OF THE POLICIES FOR INFOSEC	***27002: Implementation Guidance:*** Each policy should have an owner who has approved mngmt responsibility for the development, review and evaluation of the policies. The review should include assessing opportunities for improvement of the org's policies and approach to managing Infosec in response to changes to the org environment, business circumstances, legal conditions or tech environment.

How to Use ISO27002:2013

- Practically:
  - ISO27001:2013 controls are brief and generic
  - **27002 clarifies further what is being referred to, gives further context & very useful implementation guidance**

END

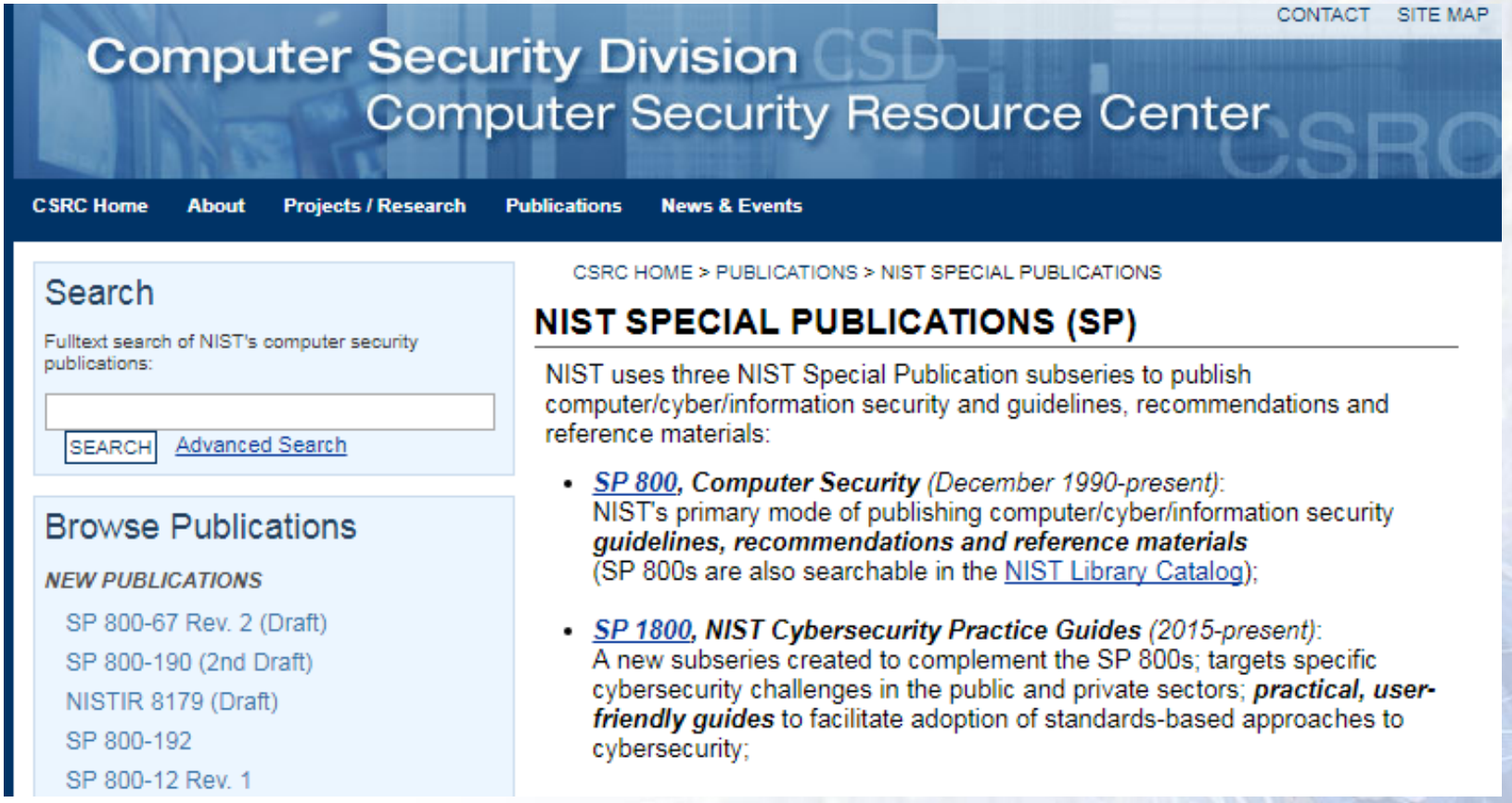
NIST FRAMEWORK

- The Computer Security Resource Center (CSRC) website guides users to NIST resources on **computer, cyber, and information security and privacy.**

NIST FRAMEWORK

- Its content includes **publications, projects, research, news and events** from the NIST Information Technology Laboratory's (ITL) two security divisions

NIST FRAMEWORK



CONTACT SITE MAP

Computer Security Division
Computer Security Resource Center

CSRC Home | About | Projects / Research | Publications | News & Events

Search

Fulltext search of NIST's computer security publications:

SEARCH Advanced Search

Browse Publications

NEW PUBLICATIONS

- SP 800-67 Rev. 2 (Draft)
- SP 800-190 (2nd Draft)
- NISTIR 8179 (Draft)
- SP 800-192
- SP 800-12 Rev. 1

CSRC HOME > PUBLICATIONS > NIST SPECIAL PUBLICATIONS

NIST SPECIAL PUBLICATIONS (SP)

NIST uses three NIST Special Publication subseries to publish computer/cyber/information security and guidelines, recommendations and reference materials:

- ***SP 800*, Computer Security** *(December 1990-present)*:
  NIST's primary mode of publishing computer/cyber/information security ***guidelines, recommendations and reference materials***
  (SP 800s are also searchable in the NIST Library Catalog);

- ***SP 1800*, NIST Cybersecurity Practice Guides** *(2015-present)*:
  A new subseries created to complement the SP 800s; targets specific cybersecurity challenges in the public and private sectors; ***practical, user-friendly guides*** to facilitate adoption of standards-based approaches to cybersecurity;

NIST FRAMEWORK

- ***SP 800*, Computer Security** *(December 1990-present)*:
  NIST's primary mode of publishing computer/cyber/information security ***guidelines, recommendations and reference materials***
  (SP 800s are also searchable in the NIST Library Catalog);

NIST FRAMEWORK

PUBLICATIONS BY TOPIC/PROJECT

Browse FIPS, Special Publications, NISTIRs and ITL Bulletins ***by topic or project***:

Security Concepts
General IT Security
Audit & Accountability
Authentication
Awareness & Training
Certification & Accreditation
Contingency Planning
Cryptography
Digital Signatures
Incident Response
Maintenance
Personal Identity Verification (PIV)
Planning
Privacy
Public Key Infrastructure (PKI)
Research
Risk Assessment
Security Automation
Services & Acquisition
Threats & Vulnerability Management
Usability

Technologies
Biometrics
Cloud Computing & Virtualization
Communications & Wireless
Mobile
Smart Cards

Applications
Cyber-Physical Systems / Smart Grid
Forensics
Healthcare
Internet of Things (IoT)
Public Safety
Supply Chain
Voting

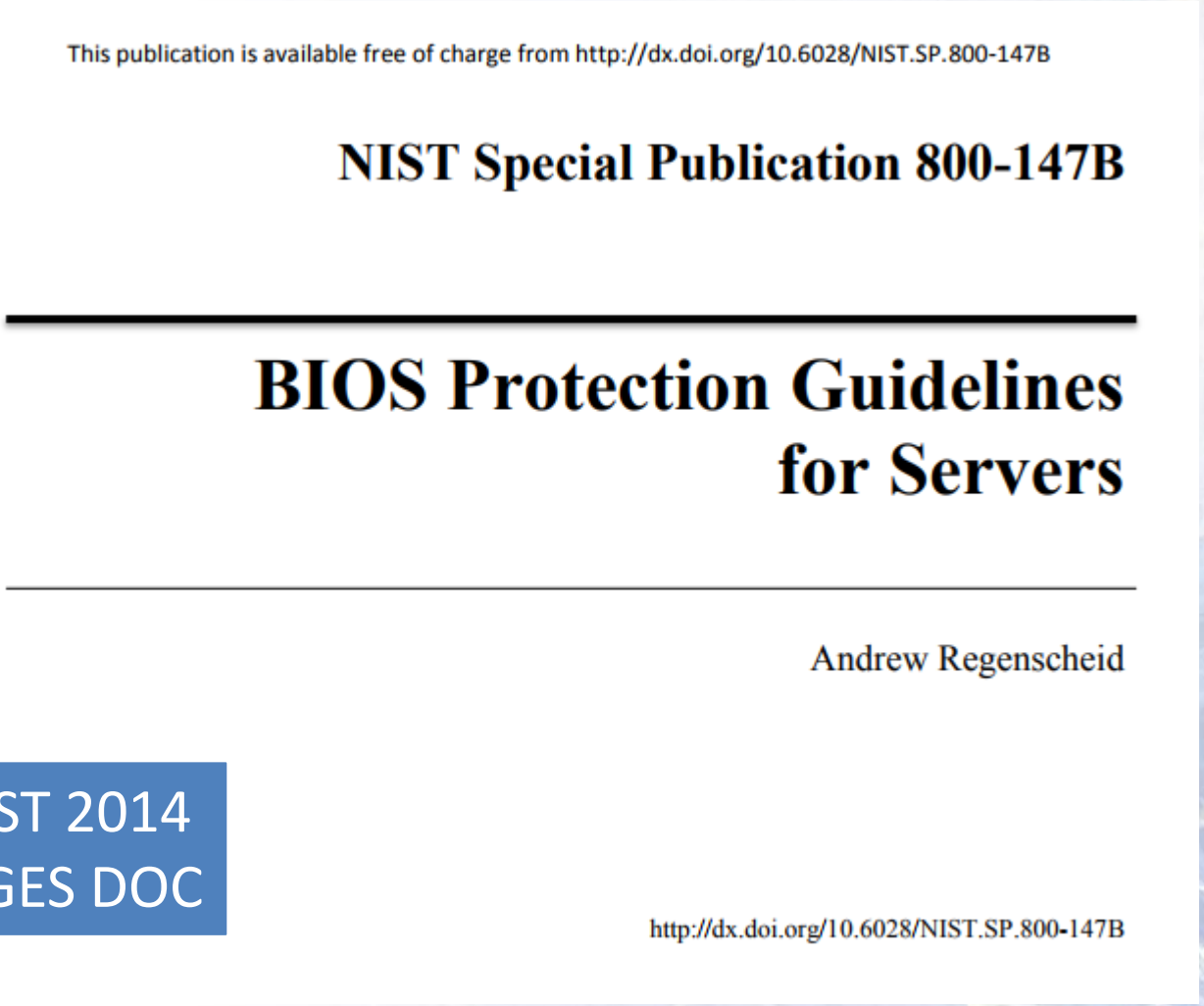
Activities
Annual Reports
Conferences & Workshops

NIST FRAMEWORK

SP 800s - Computer Security

Number	Date	Title
SP 800-193 (Draft)	May 2017	**DRAFT Platform Firmware Resiliency Guidelines** Announcement and Draft Publication
SP 800-192	June 2017	**Verification and Test Methods for Access Control Policies/Models** SP 800-192 FAQ doi:10.6028/NIST.SP.800-192 [Direct Link]
SP 800-190 (Draft)	July 2017	**DRAFT Application Container Security Guide (2nd Draft)** Announcement and Draft Publication
SP 800-188 (Draft)	December 2016	**DRAFT De-Identifying Government Datasets (2nd Draft)** Announcement and Draft Publication
SP 800-187 (Draft)	November 2016	**DRAFT Guide to LTE Security** Announcement and Draft Publication
SP 800-185	December 2016	**SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash, and ParallelHash** SP 800-185 FAQ doi:10.6028/NIST.SP.800-185 [Direct Link] Comments Received on Draft SP 800-185
SP 800-184	December	**Guide for Cybersecurity Event Recovery**

NIST FRAMEWORK



This publication is available free of charge from http://dx.doi.org/10.6028/NIST.SP.800-147B

NIST Special Publication 800-147B

BIOS Protection Guidelines for Servers

Andrew Regenscheid

http://dx.doi.org/10.6028/NIST.SP.800-147B

AUGUST 2014
32 PAGES DOC

NIST FRAMEWORK

- NIST has a tremendous library of free documentation on a diverse range of topics
- **Relevance is often average, however, depth and detail of material is extra-ordinary**

END

PCI DSS V3

- PCI Data Security Standard (DSS):
  - Designed to ensure that ALL companies that accept, process, store or transmit credit card info maintain a secure environment
  - Managed by Security Standards Council

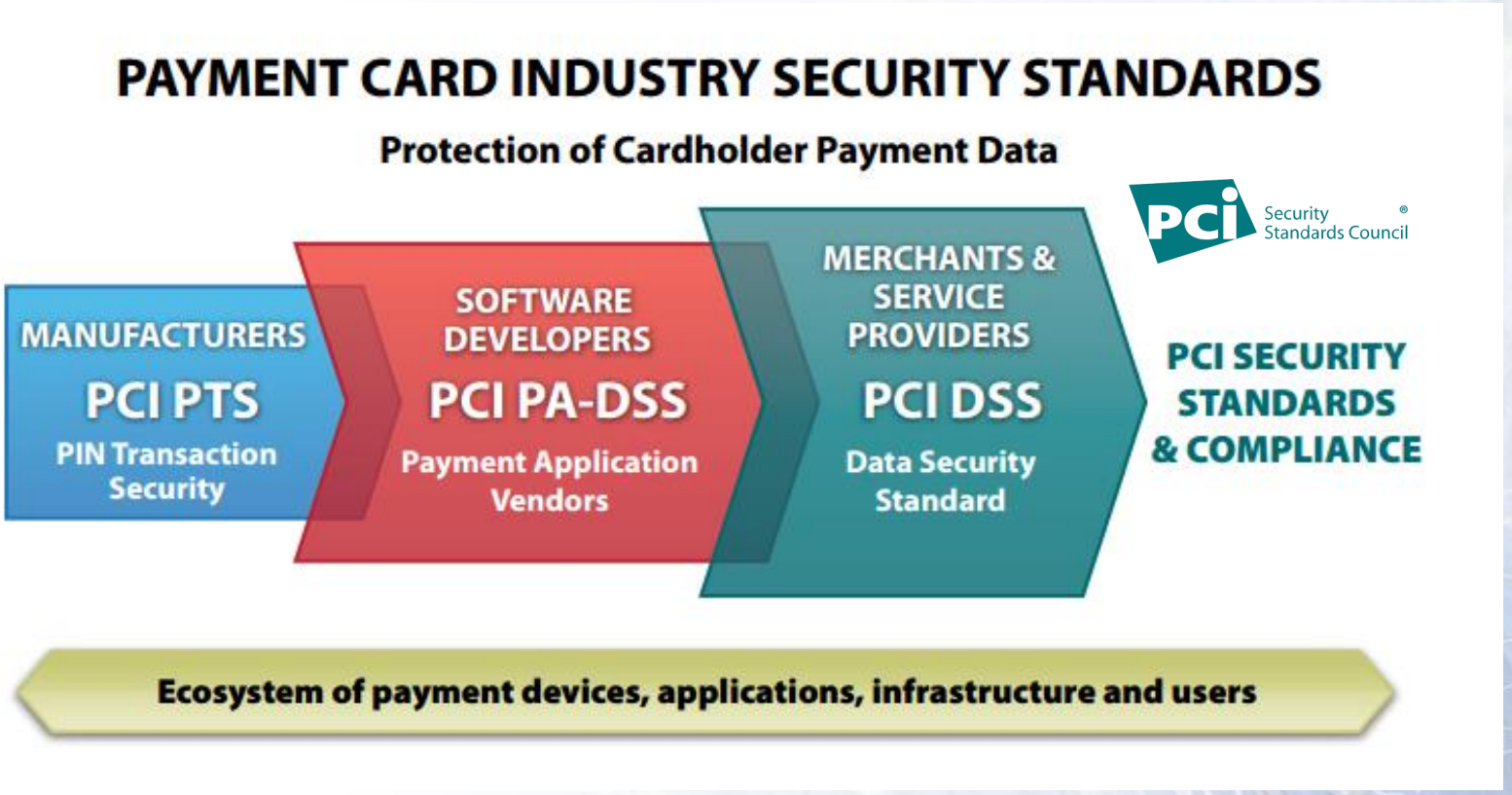
https://www.pcicomplianceguide.org/pci-faqs-2/

PCI DSS V3

- PCI DSS:
  - SSC is an independent body that was created by the major payment card brands (Visa, MasterCard, American Express, Discover and JCB
  - 6 Broad goals and 12 requirements

REF: PCI Best Practices For Implementing Security Awareness; https://www.pcisecuritystandards.org/documents/

PCI DSS V3



https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf

PCI DSS V3

Goals	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data a public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

PCI Security Standards Council

https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf

PCI DSS V3

PCI DSS Requirements	Testing Procedures	Guidance
	1.1.1.c Identify a sample of actual changes made to firewall and router configurations, compare to the change records, and interview responsible personnel to verify the changes were approved and tested.	PCI Security Standards Council
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	1.1.2.a Examine diagram(s) and observe network configurations to verify that a current network diagram exists and that it documents all connections to cardholder data, including any wireless networks.	Network diagrams describe how networks are configured, and identify the location of all network devices. Without current network diagrams, devices could be overlooked and be unknowingly left out of the security controls implemented for PCI DSS and thus be vulnerable to compromise.
	1.1.2.b Interview responsible personnel to verify that the diagram is kept current.	

REQUIREMENT

PCI DSS V3

PCI DSS Requirements	Testing Procedures	Guidance
	1.1.1.c Identify a sample of actual changes made to firewall and router configurations, compare to the change records, and interview responsible personnel to verify the changes were approved and tested.	PCI Security Standards Council
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	1.1.2.a Examine diagram(s) and observe network configurations to verify that a current network diagram exists and that it documents all connections to cardholder data, including any wireless networks. 1.1.2.b Interview responsible personnel to verify that the diagram is kept current.	Network diagrams describe how networks are configured, and identify the location of all network devices. Without current network diagrams, devices could be overlooked and be unknowingly left out of the security controls implemented for PCI DSS and thus be vulnerable to compromise.

TESTING PROCEDURES

PCI DSS V3

PCI DSS Requirements	Testing Procedures	Guidance
	1.1.1.c Identify a sample of actual changes made to firewall and router configurations, compare to the change records, and interview responsible personnel to verify the changes were approved and tested.	PCI Security Standards Council
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	**1.1.2.a** Examine diagram(s) and observe network configurations to verify that a current network diagram exists and that it documents all connections to cardholder data, including any wireless networks.	Network diagrams describe how networks are configured, and identify the location of all network devices. Without current network diagrams, devices could be overlooked and be unknowingly left out of the security controls implemented for PCI DSS and thus be vulnerable to compromise.
	1.1.2.b Interview responsible personnel to verify that the diagram is kept current.	

GUIDANCE

PCI DSS V3

REQMT	TEST PROCEDURES	GUIDANCE
7.1.4 Require documented approval by authorized parties specifying required privileges.	**7.1.4** Select a sample of user IDs & compare with documented approvals to verify that: -Documented approval exists for the assigned privileges -The approval was by authorized parties -That specified privileges match the roles assigned to the individual.	Documented approval (for example, in writing or electronically) assures that those with access and privileges are known and authorized by management, and that their access is necessary for their job function.

PCI DSS V3

REQMT	TEST PROCEDURES	GUIDANCE
8.1.4 Remove/ disable inactive user accounts within 90 days.	**8.1.4** Observe user accounts to verify that any inactive accounts over 90 days old are either removed or disabled.	Accounts that are not used regularly are often targets of attack since it is less likely that any changes (such as a changed password) will be noticed. As such, these accounts may be more easily exploited and used to access cardholder data.

PCI DSS V3

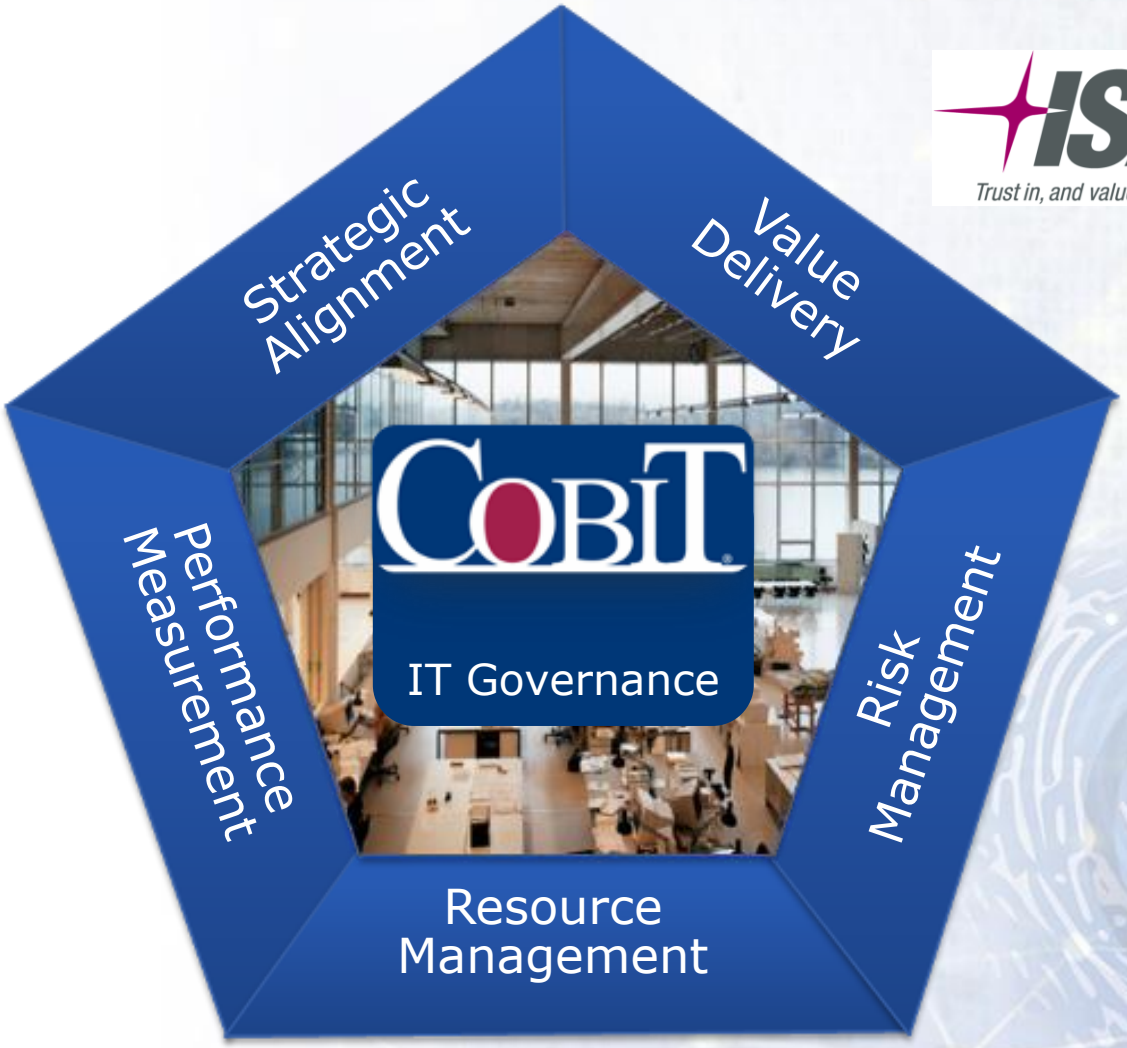
- PCI is specific to the card environment to protect cardholder data
- PCI controls are very specific and in-depth compared to generic and high-level controls of ISO27001

END

COBIT

- COBIT:
  - ISACA framework for IT Governance
  - COBIT 5 helps enterprises to create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resource use (ISACA)

COBIT

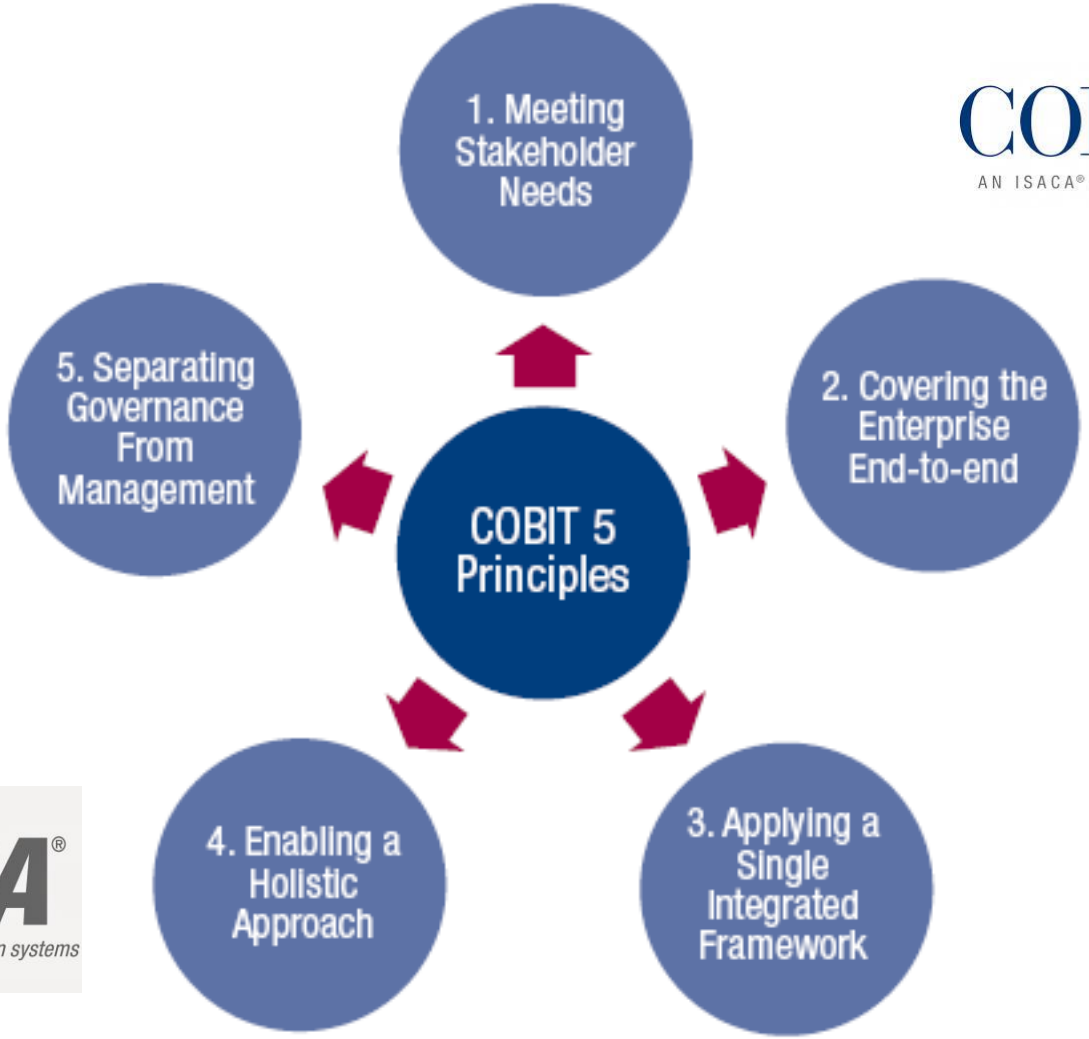


ISACA®
Trust in, and value from, information systems

COBIT

- COBIT 5 brings together **five principles** that allow the enterprise to build an effective governance and management framework (ISACA)
- Based on a holistic set of **seven enablers** that optimises IT investment and use for the benefit of stakeholders (ISACA)

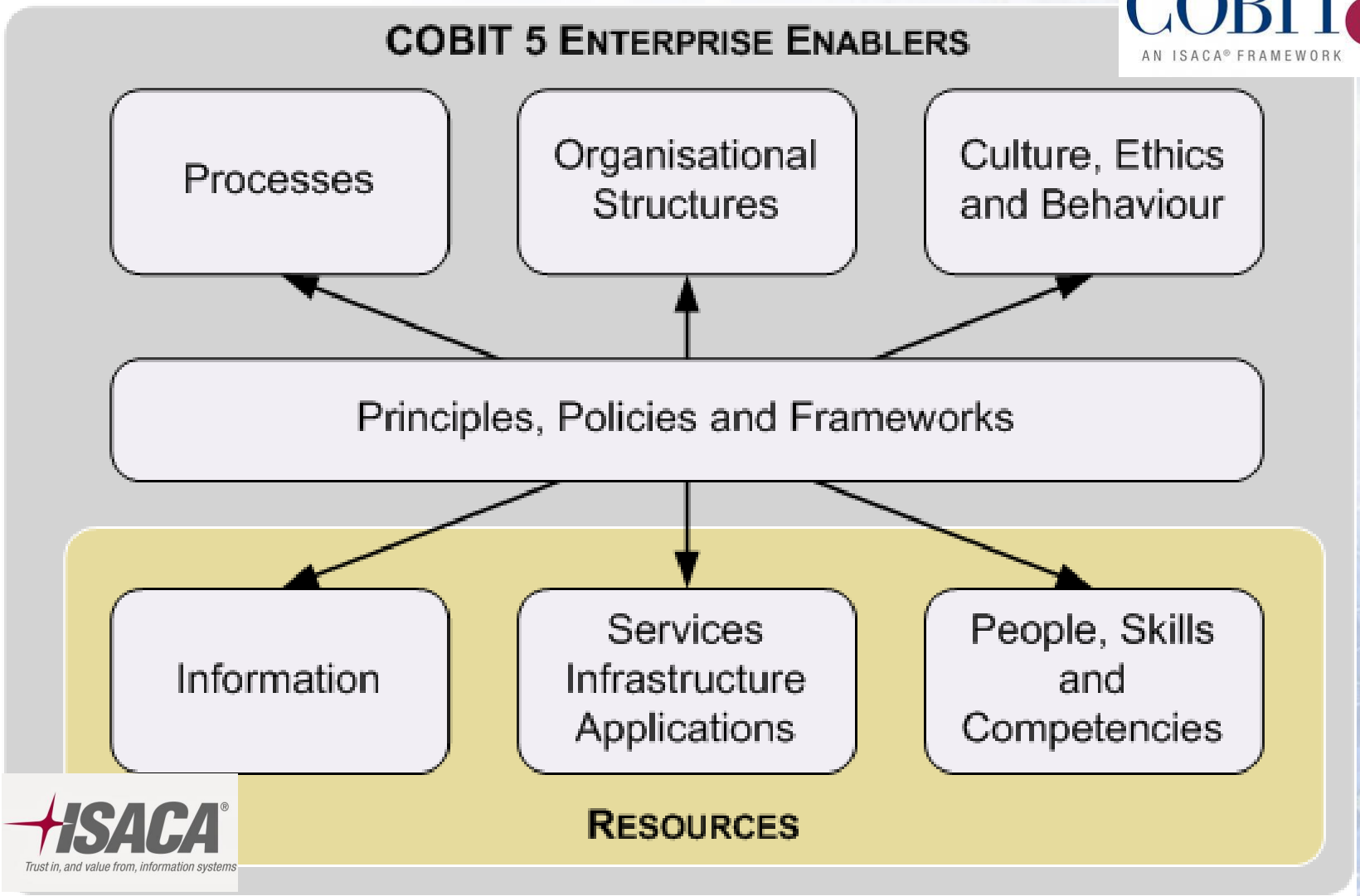
COBIT



COBIT 5
AN ISACA® FRAMEWORK

ISACA®
Trust in, and value from, information systems

COBIT


COBIT 5 ENTERPRISE ENABLERS
Processes
Organisational Structures
Culture, Ethics and Behaviour
Principles, Policies and Frameworks
Information
Services Infrastructure Applications
People, Skills and Competencies
RESOURCES

COBIT

- **Governance** ensures that enterprise objectives are achieved by **evaluating** stakeholder needs, conditions & options; setting **direction** through prioritisation & decision making;

COBIT

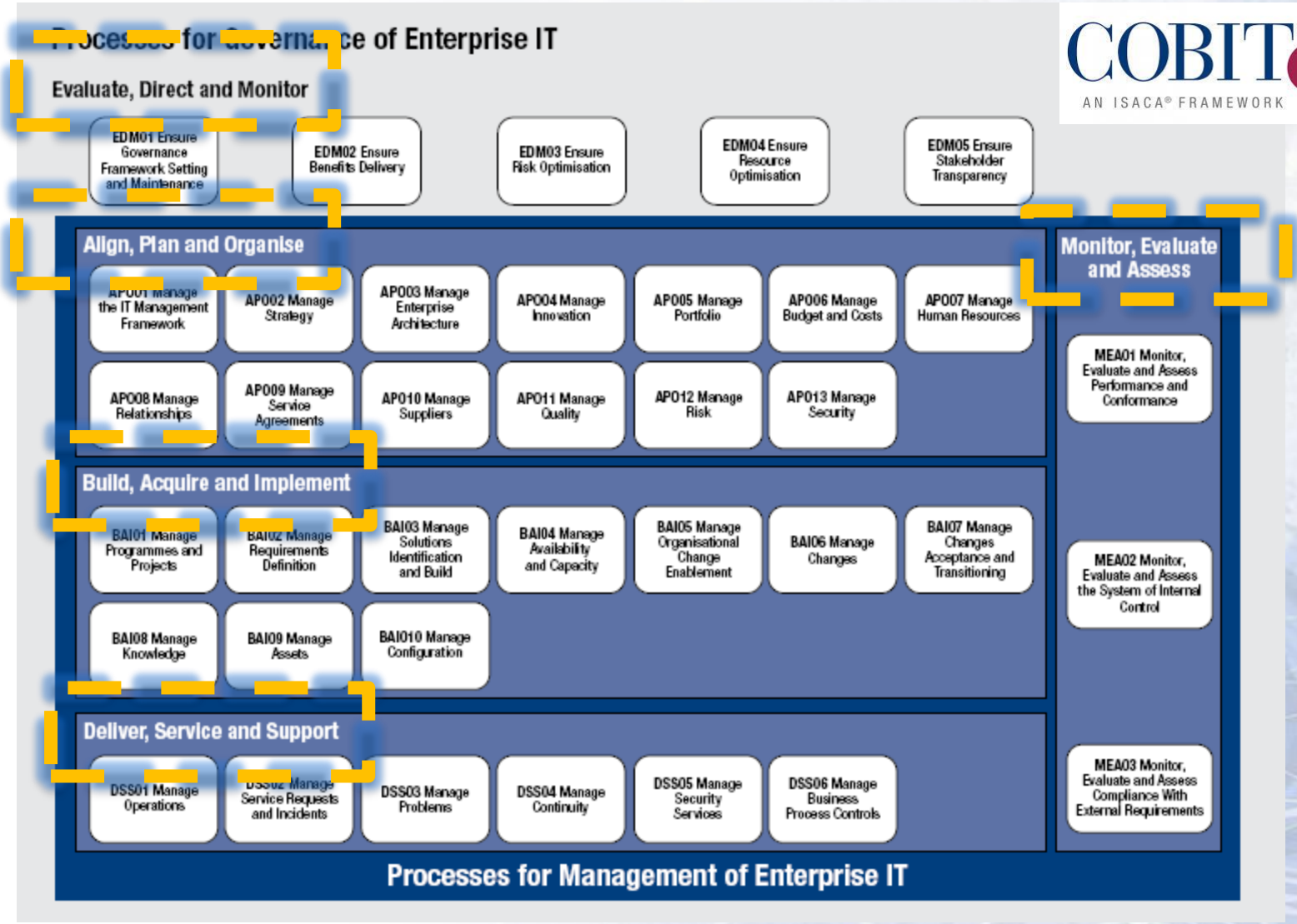
- … & **monitoring** performance, compliance and progress against agreed direction and objectives **(EDM)**



COBIT

- **Management plans, builds, runs** and **monitors** activities in alignment with the direction set by the governance body to achieve the enterprise objectives **(PBRM)**

COBIT


Processes for Governance of Enterprise IT
COBIT 5
AN ISACA® FRAMEWORK
Evaluate, Direct and Monitor
EDM01 Ensure Governance Framework Setting and Maintenance
EDM02 Ensure Benefits Delivery
EDM03 Ensure Risk Optimisation
EDM04 Ensure Resource Optimisation
EDM05 Ensure Stakeholder Transparency
Align, Plan and Organise
APO01 Manage the IT Management Framework
APO02 Manage Strategy
APO03 Manage Enterprise Architecture
APO04 Manage Innovation
APO05 Manage Portfolio
APO06 Manage Budget and Costs
APO07 Manage Human Resources
APO08 Manage Relationships
APO09 Manage Service Agreements
APO10 Manage Suppliers
APO11 Manage Quality
APO12 Manage Risk
APO13 Manage Security
Build, Acquire and Implement
BAI01 Manage Programmes and Projects
BAI02 Manage Requirements Definition
BAI03 Manage Solutions Identification and Build
BAI04 Manage Availability and Capacity
BAI05 Manage Organisational Change Enablement
BAI06 Manage Changes
BAI07 Manage Changes Acceptance and Transitioning
BAI08 Manage Knowledge
BAI09 Manage Assets
BAI010 Manage Configuration
Deliver, Service and Support
DSS01 Manage Operations
DSS02 Manage Service Requests and Incidents
DSS03 Manage Problems
DSS04 Manage Continuity
DSS05 Manage Security Services
DSS06 Manage Business Process Controls
Monitor, Evaluate and Assess
MEA01 Monitor, Evaluate and Assess Performance and Conformance
MEA02 Monitor, Evaluate and Assess the System of Internal Control
MEA03 Monitor, Evaluate and Assess Compliance With External Requirements
Processes for Management of Enterprise IT

COBIT

- COBIT 5 is a detailed framework for IT governance developed by ISACA which has principles, enablers, and processes
- These tools assist implementers and customer organizations to successfully deploy the framework
- Certifiable framework

END

MALWARE

MALICIOUS SOFTWARE

Malware

- Malicious software
- Rogue software
- Rogue
  - Large, destructive, anomalous or unpredictable
  - Operating outside normal or desirable controls

Malware

- Malware (a portmanteau for malicious software) is any software intentionally designed to cause disruption to a computer, server, client, or computer network, leak private information, gain unauthorized access to information or systems, deprive access to information, or which unknowingly interferes with the user's computer security and privacy.
- Researchers tend to classify malware into one or more sub-types (i.e. computer viruses, worms, Trojan horses, ransomware, spyware, adware, rogue software, wiper and keyloggers).
- Malware poses serious problems to individuals and businesses on the Internet.
- According to Symantec's 2018 Internet Security Threat Report (ISTR), malware variants number has increased to 669,947,865 in 2017, which is twice as many malware variants as in 2016.
- Cybercrime, which includes malware attacks as well as other crimes committed by computer, was predicted to cost the world economy $6 trillion USD in 2021, and is increasing at a rate of 15% per year.
- Since 2021, malware has been designed to target computer systems that run critical infrastructure such as the electricity distribution network.
- The defense strategies against malware differ according to the type of malware but most can be thwarted by installing antivirus software, firewalls, applying regular patches to reduce zero-day attacks, securing networks from intrusion, having regular backups and isolating infected systems.
- Malware is now being designed to evade antivirus software detection algorithms.

Malware Types

- Virus
- Worm
- Trojan
- Logic bomb
- Time bomb
- Drive-by download
- Backdoor
- PUPs(Potentially Unwanted Program)
- Spyware
- Adware
- Scareware
- Ransomware
- FakeAV / Rogue security software
- Malvertising
- APT
- Fileless malware

Software versus Malware

- Writing a typical software
  - Software application (word processor, spreadsheet, graphics)
  - Higher-level programming language
  - Usually independent of OS

- Writing a virus
  - Detailed knowledge of OS

Computer Virus

- Biological virus
  - Latin → Poison
  - Shell filled with genetic material that it injects into a living cell, thereby infecting it
  - The cell then starts manufacturing copies of virus

- Computer virus behaves similarly
  - Injects its contents, a short computer program / instructions, into a host computer and infecting it
  - When the computer executes the virus code, it replicates the code, performs some task(s), usually of a malicious nature

- A computer virus is a type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its own code into those programs.
- Computer viruses generally require a host program.
- The virus writes its own code into the host program.
- When the program runs, the written virus program is executed first, causing infection and damage.

- By contrast, a computer worm does not need a host program, as it is an independent program or code chunk.

- Therefore, it is not restricted by the host program, but can run independently and actively carry out attacks.

- Any virus will by definition make unauthorised changes to a computer, which is undesirable even if no damage is done or intended.

- The first page of Dr Solomon's Virus Encyclopaedia explains the undesirability of viruses, even those that do nothing but reproduce.

- The first academic work on the theory of self-replicating computer programs was done in 1949 by John von Neumann who gave lectures at the University of Illinois about the "Theory and Organization of Complicated Automata".
- The work of von Neumann was later published as the "Theory of self-reproducing automata".
- In his essay von Neumann described how a computer program could be designed to reproduce itself.
- Von Neumann's design for a self-reproducing computer program is considered the world's first computer virus, and he is considered to be the theoretical "father" of computer virology.

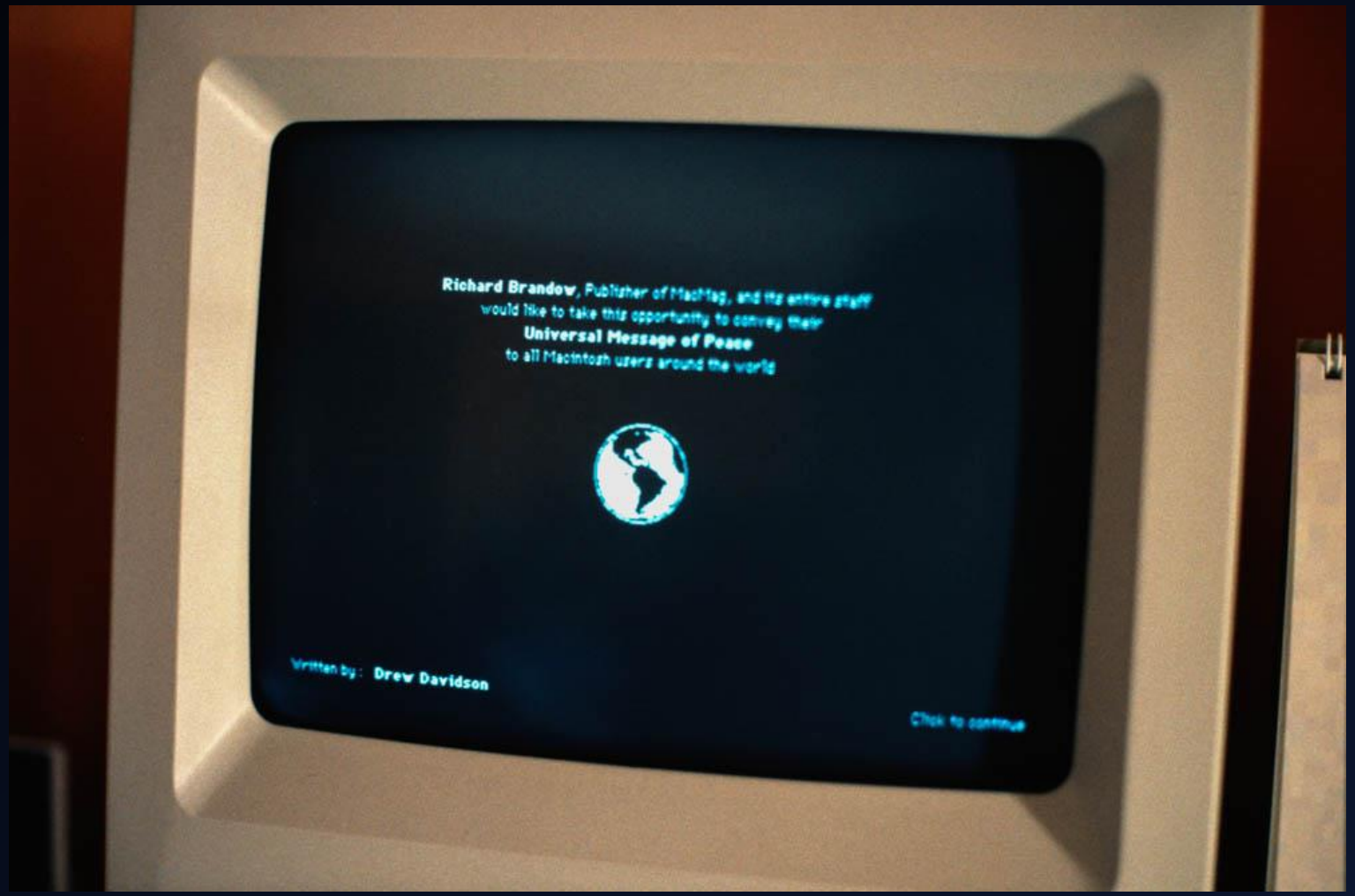
- In 1972, Veith Risak directly building on von Neumann's work on self-replication, published his article "Selbstreproduzierende Automaten mit minimaler Informationsübertragung" (Self-reproducing automata with minimal information exchange).
- The article describes a fully functional virus written in assembler programming language for a SIEMENS 4004/35 computer system.
- In 1980 Jürgen Kraus wrote his diplom thesis "Selbstreproduktion bei Programmen" (Self-reproduction of programs) at the University of Dortmund.
- In his work Kraus postulated that computer programs can behave in a way similar to biological viruses.

Creeper / Reaper

- The Creeper virus was first detected on ARPANET, the forerunner of the Internet, in the early 1970s.
- Creeper was an experimental self-replicating program written by Bob Thomas at BBN Technologies in 1971.
- Creeper used the ARPANET to infect DEC PDP-10 computers running the TENEX operating system.
- Creeper gained access via the ARPANET and copied itself to the remote system where the message, "I'M THE CREEPER. CATCH ME IF YOU CAN!" was displayed.
- The Reaper program was created to delete Creeper.

- In 1984 Fred Cohen from the University of Southern California wrote his paper "Computer Viruses – Theory and Experiments".
- It was the first paper to explicitly call a self-reproducing program a "virus", a term introduced by Cohen's mentor Leonard Adleman.

This is the MacMag virus 'Universal Peace' message, as displayed on my Mac in March of 1988.



Brain virus

- 26 September 1988: front cover of Time magazine
- Title: “Invasion of the data snatchers”

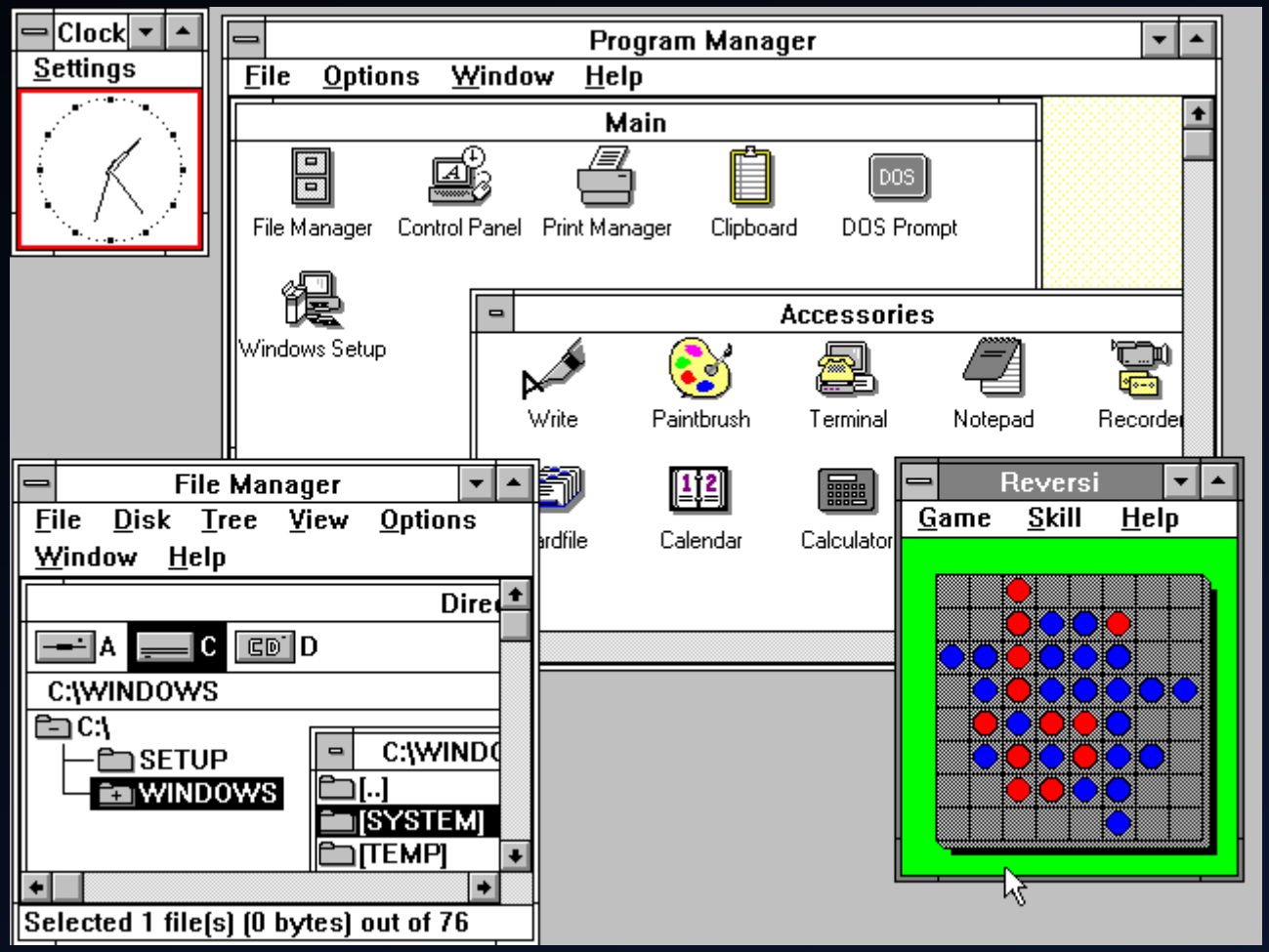
- The first IBM PC compatible virus in the "wild" was a boot sector virus dubbed (c)Brain, created in 1986 and was released in 1987 by Amjad Farooq Alvi and Basit Farooq Alvi in Lahore, Pakistan, reportedly to deter unauthorized copying of the software they had written.

Hex dump of the Brain virus, generally regarded as the first computer virus for the IBM Personal Computer (IBM PC) and compatibles



Displacement	Hex codes	ASCII value
0000(0000)	FA E9 4A 01 34 12 00 07 14 00 01 00 00 00 00 20	-0J04↕●╥0
0016(0010)	20 20 20 20 20 20 57 65 6C 63 6F 6D 65 20 74 6F	Welcome to
0032(0020)	20 74 68 65 20 44 75 6E 67 65 6F 6E 20 20 20 20	the Dungeon
0048(0030)	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	
0064(0040)	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	
0080(0050)	20 28 63 29 20 31 39 38 36 20 42 61 73 69 74 20	(c) 1986 Basit
0096(0060)	26 20 41 6D 6A 61 64 20 28 70 76 74 29 20 4C 74	& Amjad (put) Lt
0112(0070)	64 2E 20 20 20 20 20 20 20 20 20 20 20 20 20 20	d.
0128(0080)	20 42 52 41 49 4E 20 43 4F 4D 50 55 54 45 52 20	BRAIN COMPUTER
0144(0090)	53 45 52 56 49 43 45 53 2E 2E 37 33 30 20 4E 49	SERVICES.. 730 NI
0160(00A8)	5A 41 4D 20 42 4C 4F 43 4B 20 41 4C 4C 41 4D 41	ZAM BLOCK ALLAMA
0176(00B0)	20 49 51 42 41 4C 20 54 4F 57 4E 20 20 20 20 20	.IQBAL TOWN
0192(00C0)	20 20 20 20 20 20 20 20 20 20 20 4C 41 48 4F 52	LAHDR
0208(0BD0)	45 2D 50 41 4B 49 53 54 41 4E 2E 2E 50 48 4F 4E	E-PAKISTAN..PHJN
0224(00E0)	45 20 3A 34 33 30 37 39 31 2C 34 34 33 32 34 3B	E :430791,443248
0240(00F0)	2C 32 38 30 35 33 30 2E 20 20 20 20 20 20 20 20	,280530.

The first virus to specifically target Microsoft Windows, WinVir was discovered in April 1992, two years after the release of Windows 3.0.



Parts of a Virus

- A computer virus generally contains three parts:
  - the infection mechanism, which finds and infects new files
  - the payload, which is the malicious code to execute
  - the trigger, which determines when to activate the payload

Computer worm

- A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers.
- It often uses a computer network to spread itself, relying on security failures on the target computer to access it.
- It will use this machine as a host to scan and infect other computers.
- When these new worm-invaded computers are controlled, the worm will continue to scan and infect other computers using these computers as hosts, and this behaviour will continue.

Computer worm

- Computer worms use recursive methods to copy themselves without host programs and distribute themselves based on exploiting the advantages of exponential growth, thus controlling and infecting more and more computers in a short time.
- Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.
- Many worms are designed only to spread, and do not attempt to change the systems they pass through.
- However, as the Morris worm and Mydoom showed, even these "payload-free" worms can cause major disruption by increasing network traffic and other unintended effects.

Hex dump of the Blaster worm, showing a message left for Microsoft CEO Bill Gates by the worm's creator



Ransomware

- Ransomware is a type of malware from cryptovirology that threatens to publish the victim's personal data or permanently block access to it unless a ransom is paid off.
- While some simple ransomware may lock the system without damaging any files, more advanced malware uses a technique called cryptoviral extortion.
- It encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.


CryptoLocker
Payment for private key
Choose a convenient payment method and click «Next»:
Bitcoin (most cheap option)
bitcoin
Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.
You have to send 2 BTC to Bitcoin address
[redacted]
and specify the Transaction ID on the next page, which will be verified and confirmed.
Home Page
Getting started with Bitcoin
Private key will be destroyed on
10/13/2013
1:21 PM
Time left
71 : 33 : 17
<< Back
Next >>


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

Trojan horse

- In computing, a Trojan horse is any malware that misleads users of its true intent by disguising itself as a standard program.

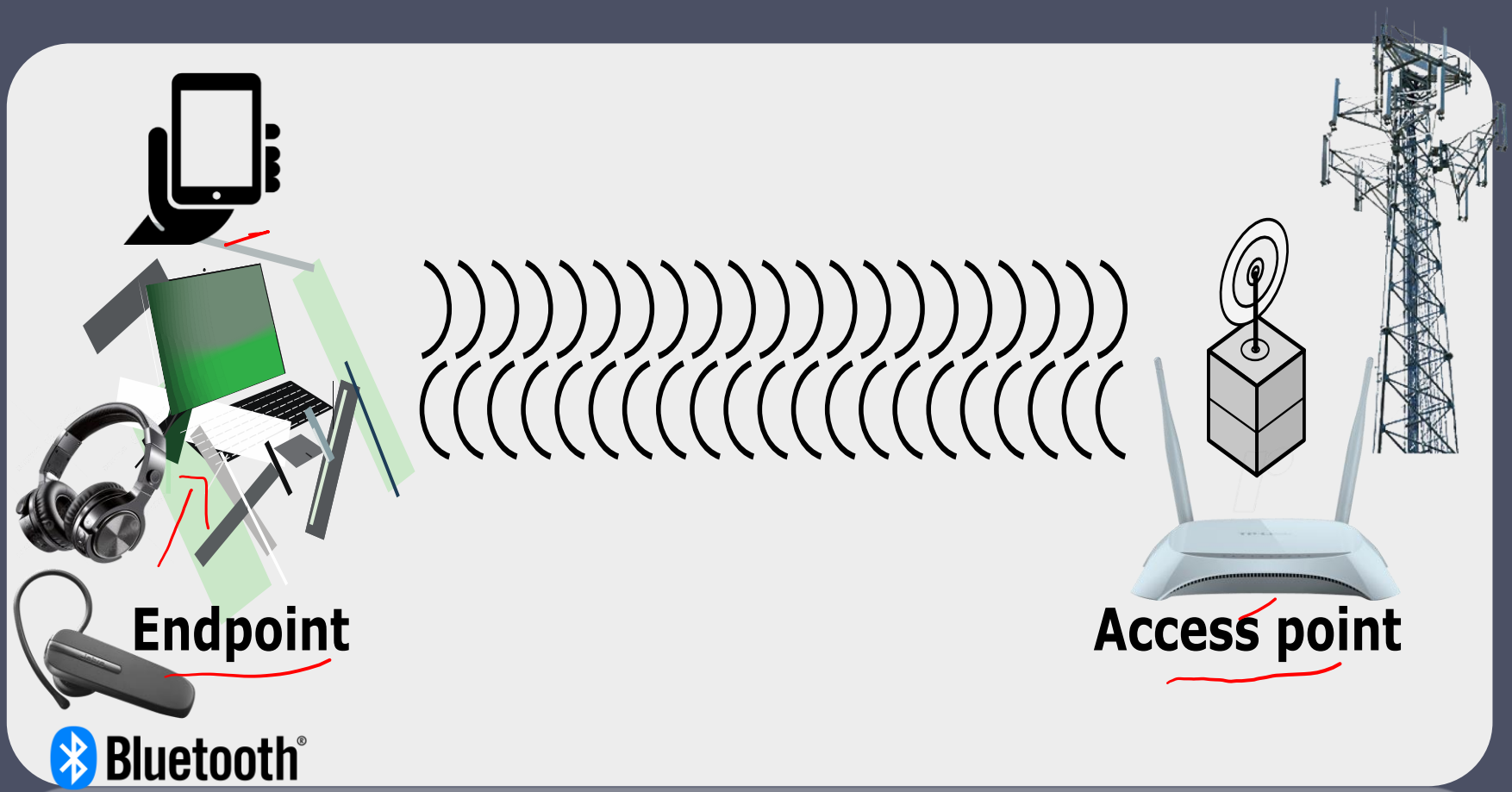
- The term is derived from the ancient Greek story of the deceptive Trojan Horse that led to the fall of the city of Troy.

- Once installed, Trojans may perform a range of malicious actions.
- Many tend to contact one or more Command and Control (C2) servers across the Internet and await instruction.
- Since individual Trojans typically use a specific set of ports for this communication, it can be relatively simple to detect them.



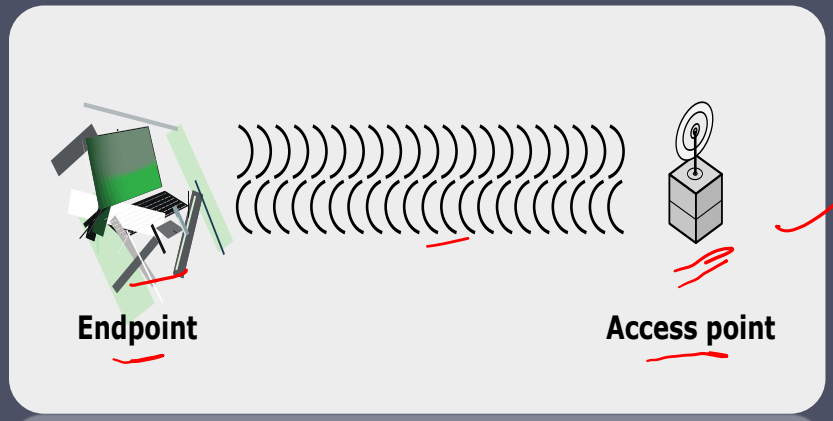
Wireless Network Security

Wireless Networking Components



Wireless Security

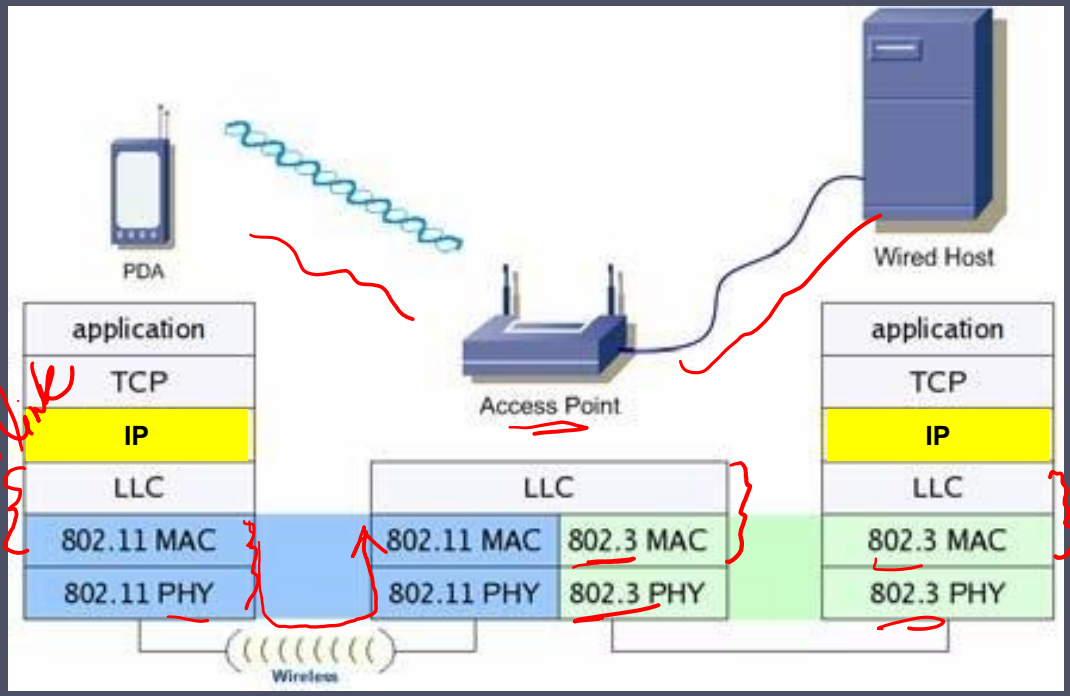
- Key factors contributing to higher security risk of wireless networks compared to wired networks include:
- **Channel**
  - Wireless networking typically involves broadcast communications, which is far more susceptible to eavesdropping and jamming than wired networks
  - Wireless networks are also more vulnerable to active attacks that exploit vulnerabilities in communications protocols
- **Mobility**
  - Wireless devices are far more portable and mobile, thus resulting in a number of risks
- **Limited Resources**
  - Some wireless devices, such as smartphones and tablets, have sophisticated operating systems but limited memory and processing resources with which to counter threats, including denial of service and malware
- **Accessibility**
  - Some wireless devices, such as sensors and robots, may be left unattended in remote and/or hostile locations, thus greatly increasing their vulnerability to physical attacks



IEEE 802.11 Standard

Wired and Wireless LANs

- LANs are designed for use in a **small area** (offices, campuses)
- IEEE has defined the specifications for a
  - wired LAN, called IEEE 802.3
  - wireless LAN, called IEEE 802.11,
- These specifications are concerning the physical and data link layers.



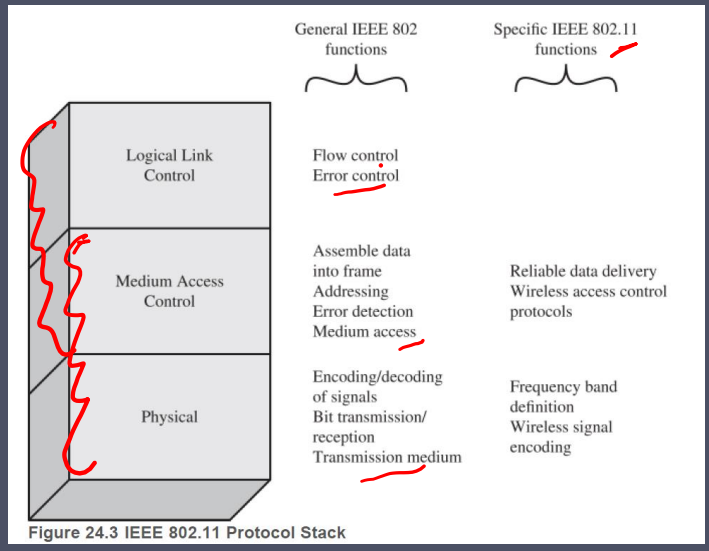


Figure 24.3 IEEE 802.11 Protocol Stack

Brief History of IEEE 802

- Since there are various types of computer system manufacturers, the IEEE's computer society started a project in 1985 called **Project 802** to enable standard communication between various devices.

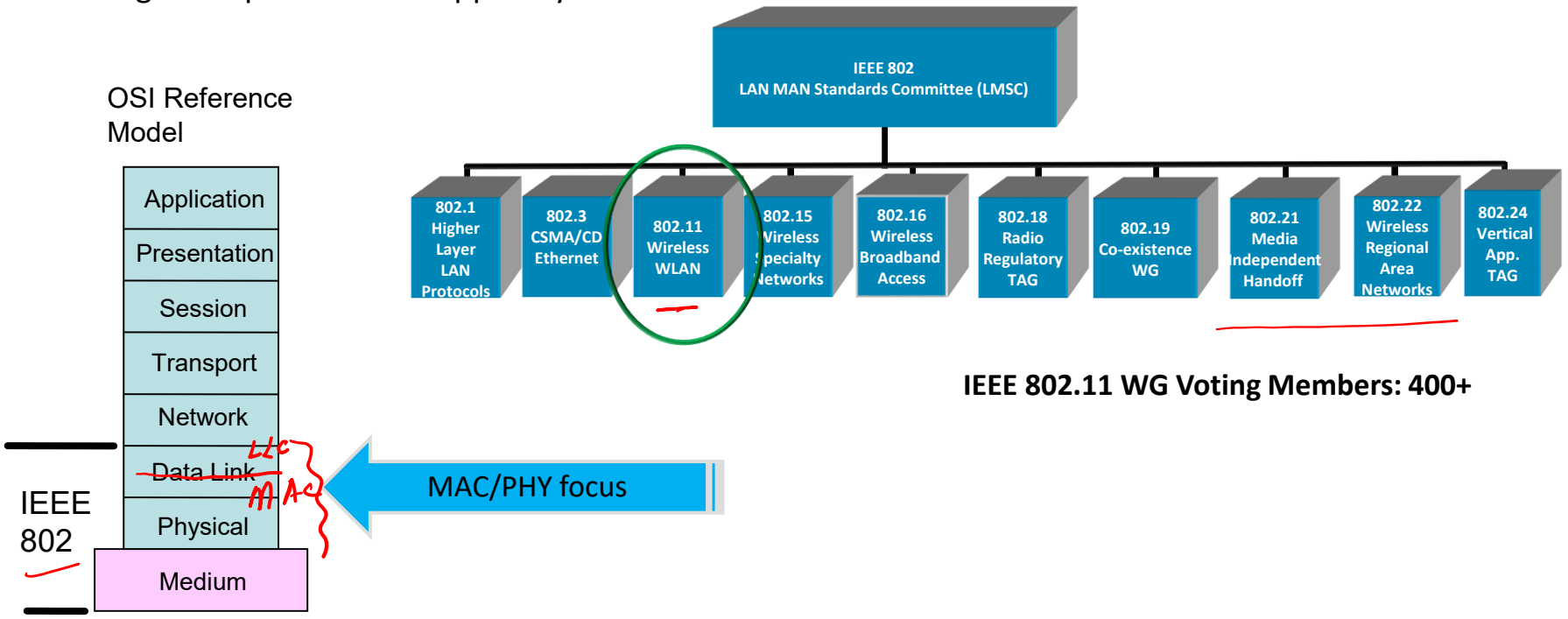


- The **IEEE 802 LAN/MAN Standards Committee (LMSC)** develops and maintains networking standards and recommended practices for **local, metropolitan, and other area networks**, using an open and accredited process, and advocates them on a global basis.

https://www.ieee802.org/

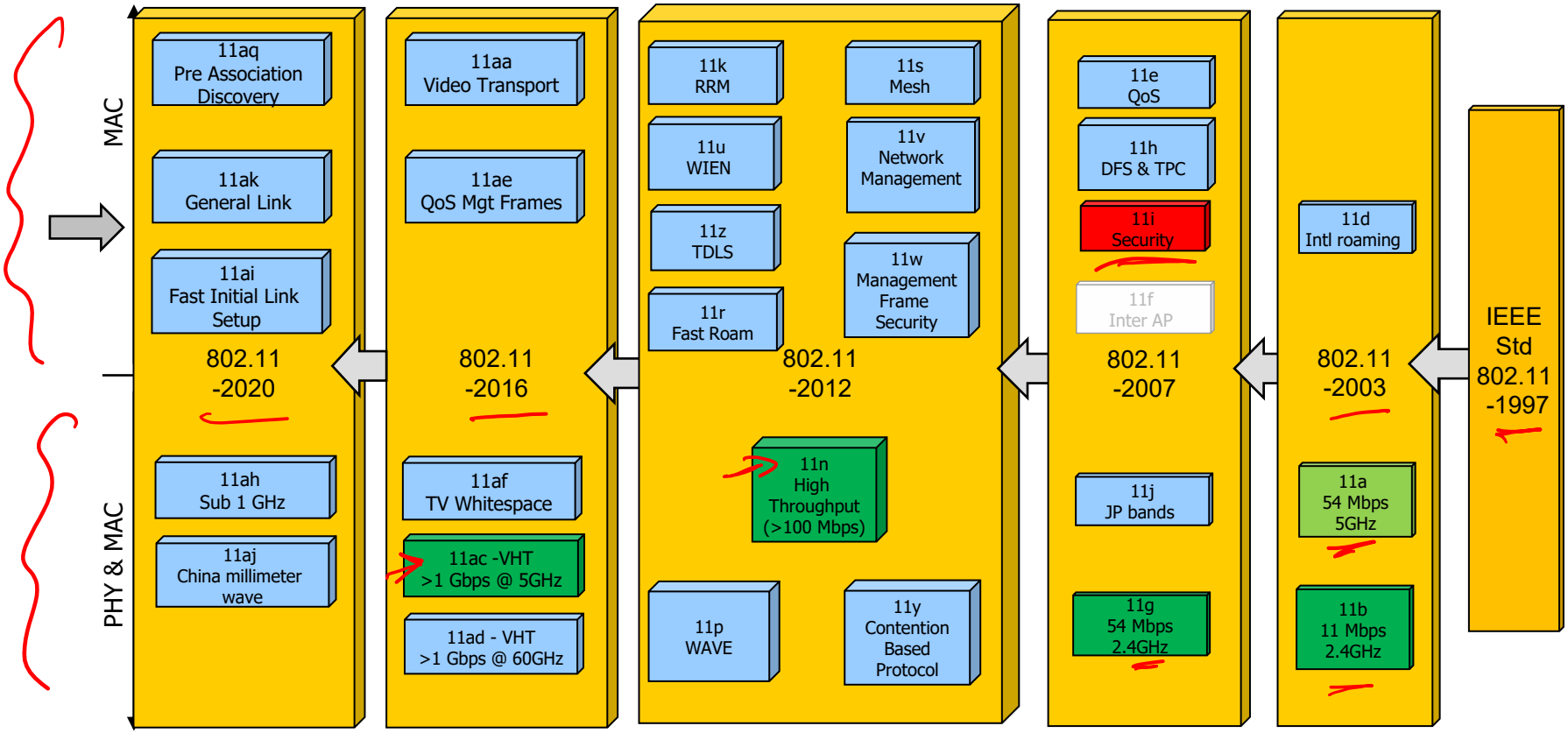
The IEEE 802.11 Working Group is one of the most active WGs in 802

- The 802.11 Working Group was established in 1990.
- Focus on **link and physical layers** of the network stack
- Leverage IETF protocols for upper layers

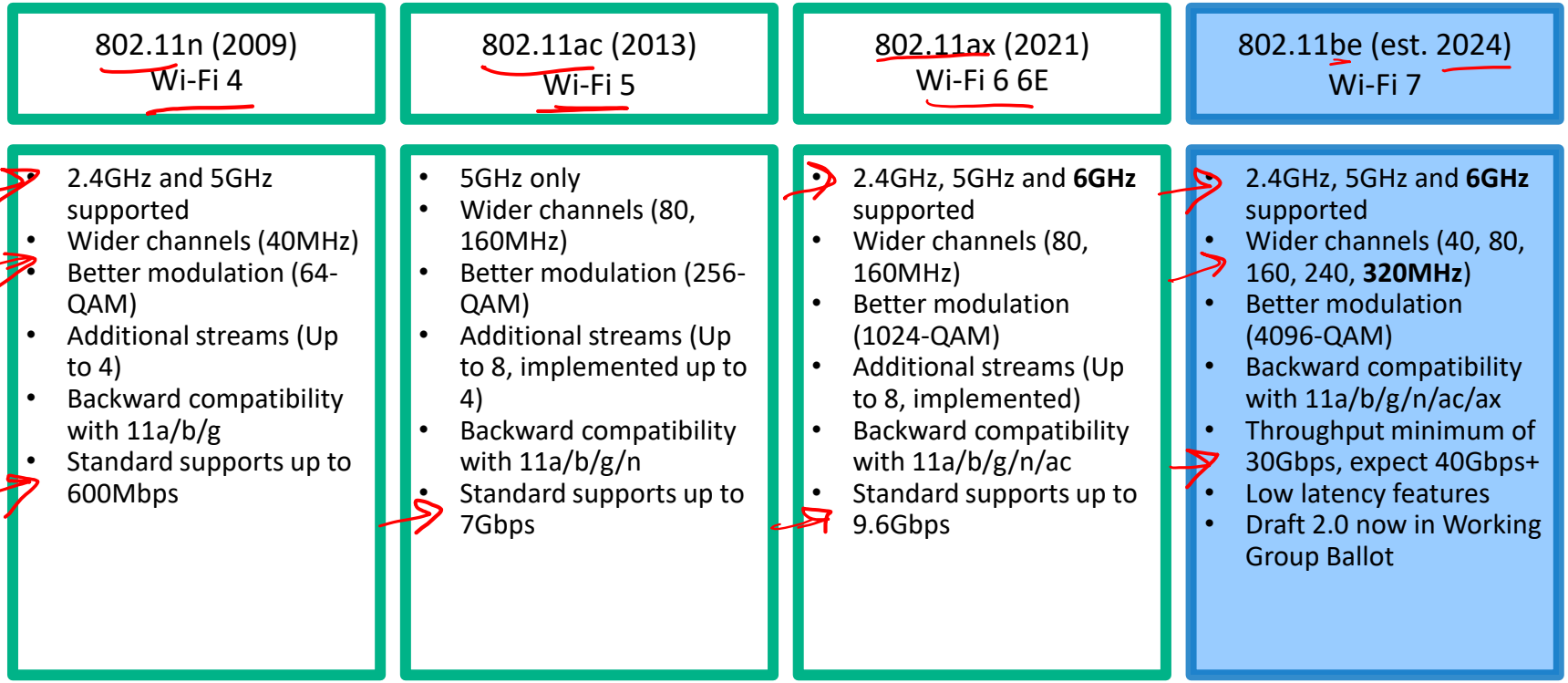


IEEE 802.11 WG Voting Members: 400+

Development of the IEEE 802.11 Standard is ongoing since 1997



IEEE802.11 Wi-Fi standard evolution: 802.11be is under development

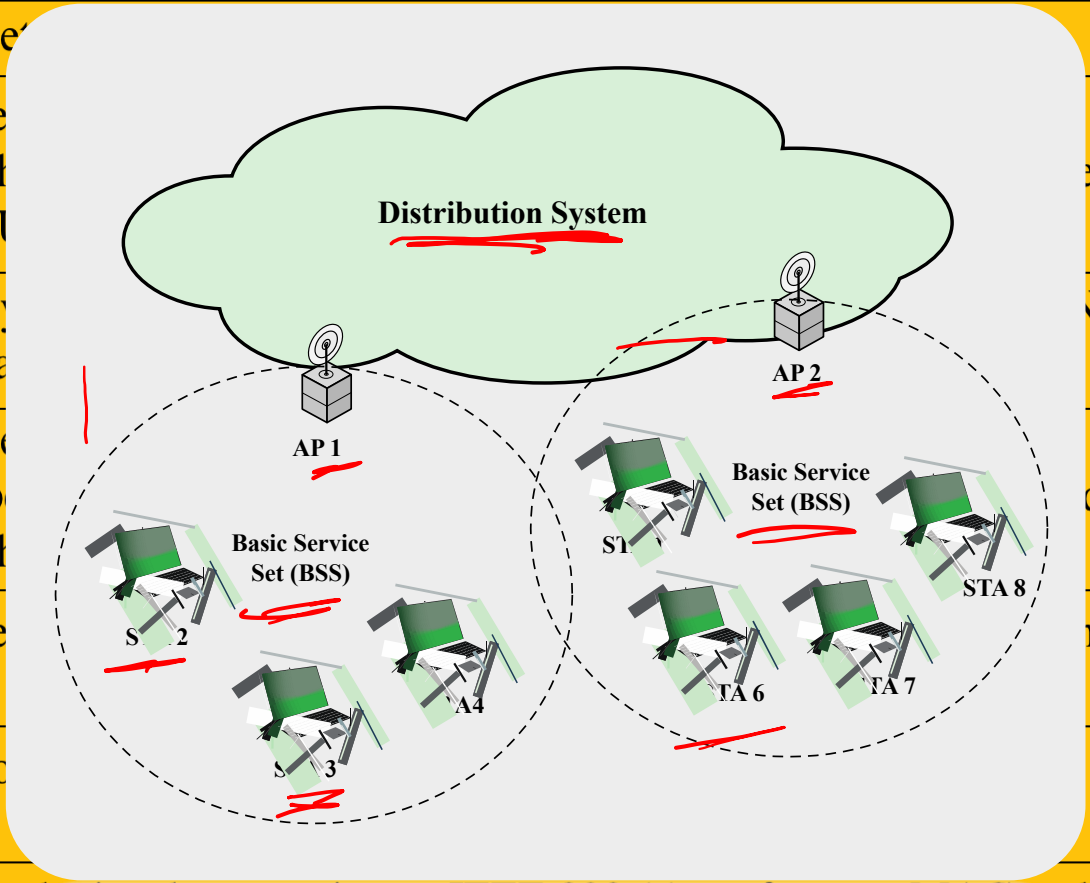


(Ratification date) Products available in the market typically ~2 years prior

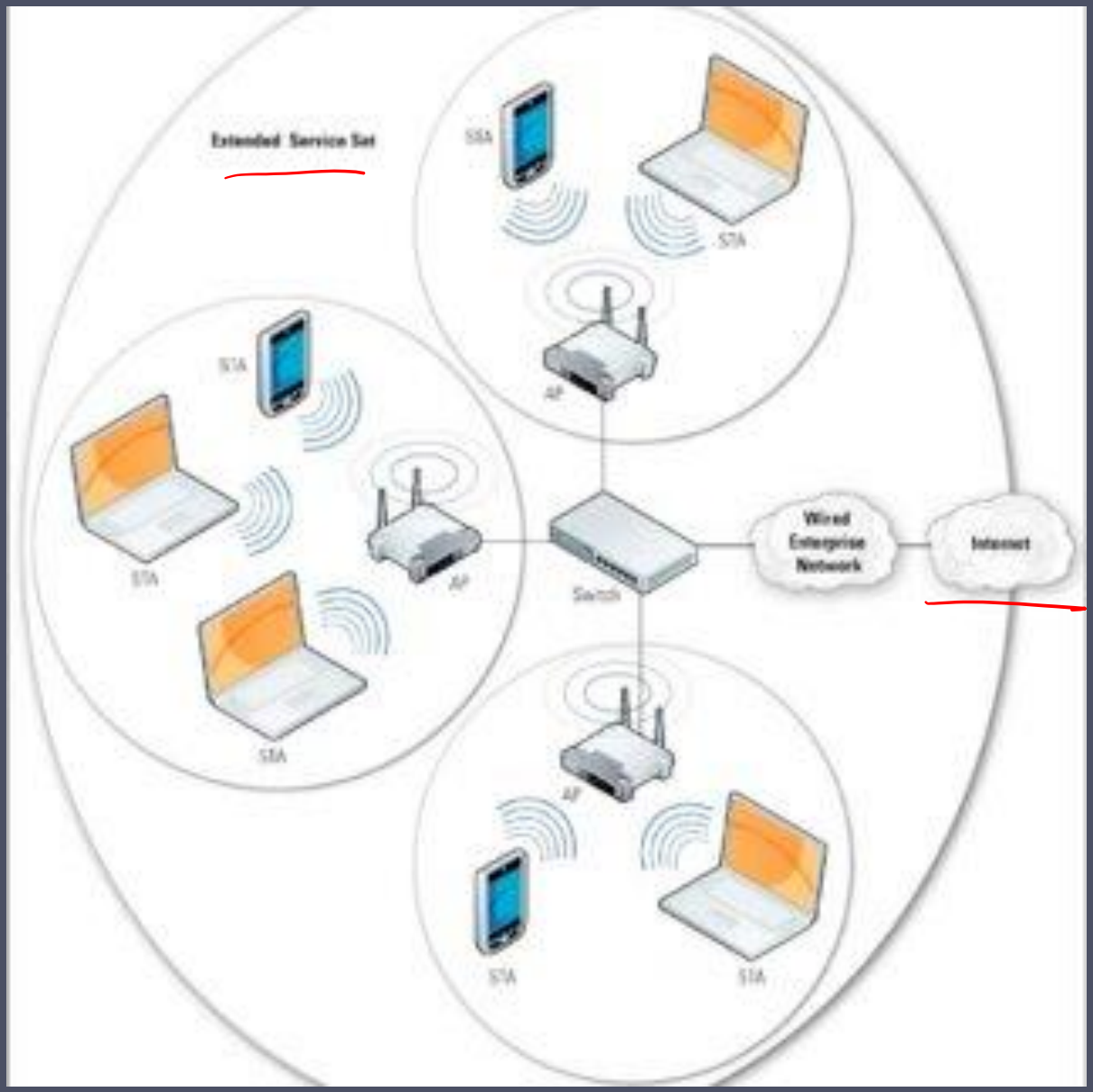
IEEE 802.11 Terminology

IEEE 802.11 Terminology

Access point (AP)	Any entity that has station functionality and provides access to the distribution system via the wireless medium for associated stations.
Basic service set (BSS)	A se
Coordination function	The with PDU
Distribution system (DS)	A sy crea
Extended service set (ESS)	A se app with
MAC protocol data unit (MPDU)	The the
MAC service data unit (MSDU)	Info
Station	Any device that contains an IEEE 802.11 conformant MAC and physical layer.



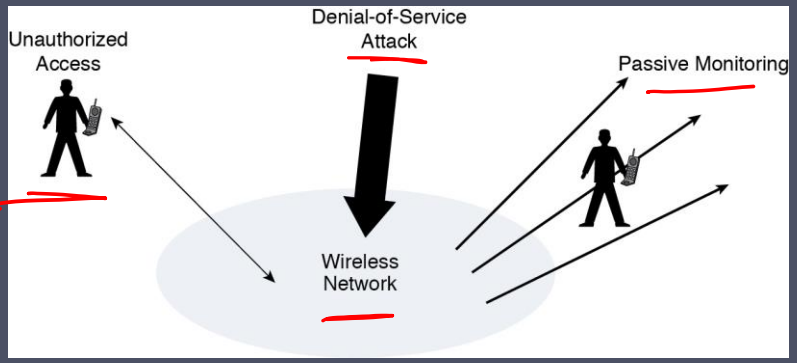
IEEE 802.11 Extended Service Set Example

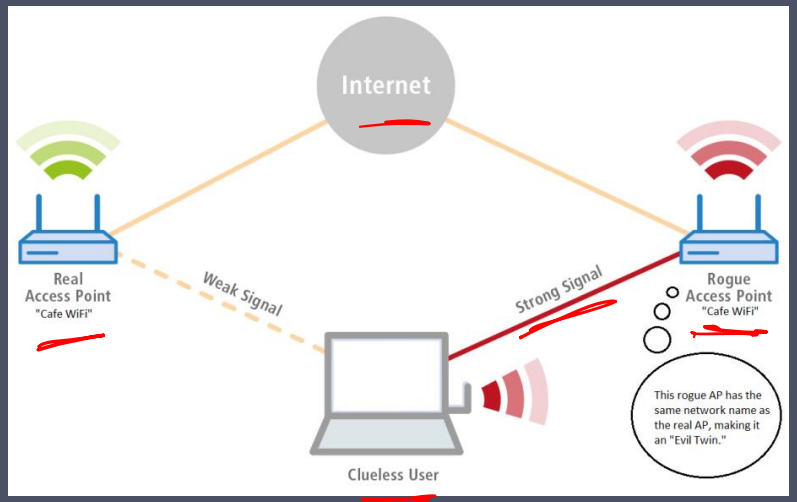


IEEE 802.1x Standard

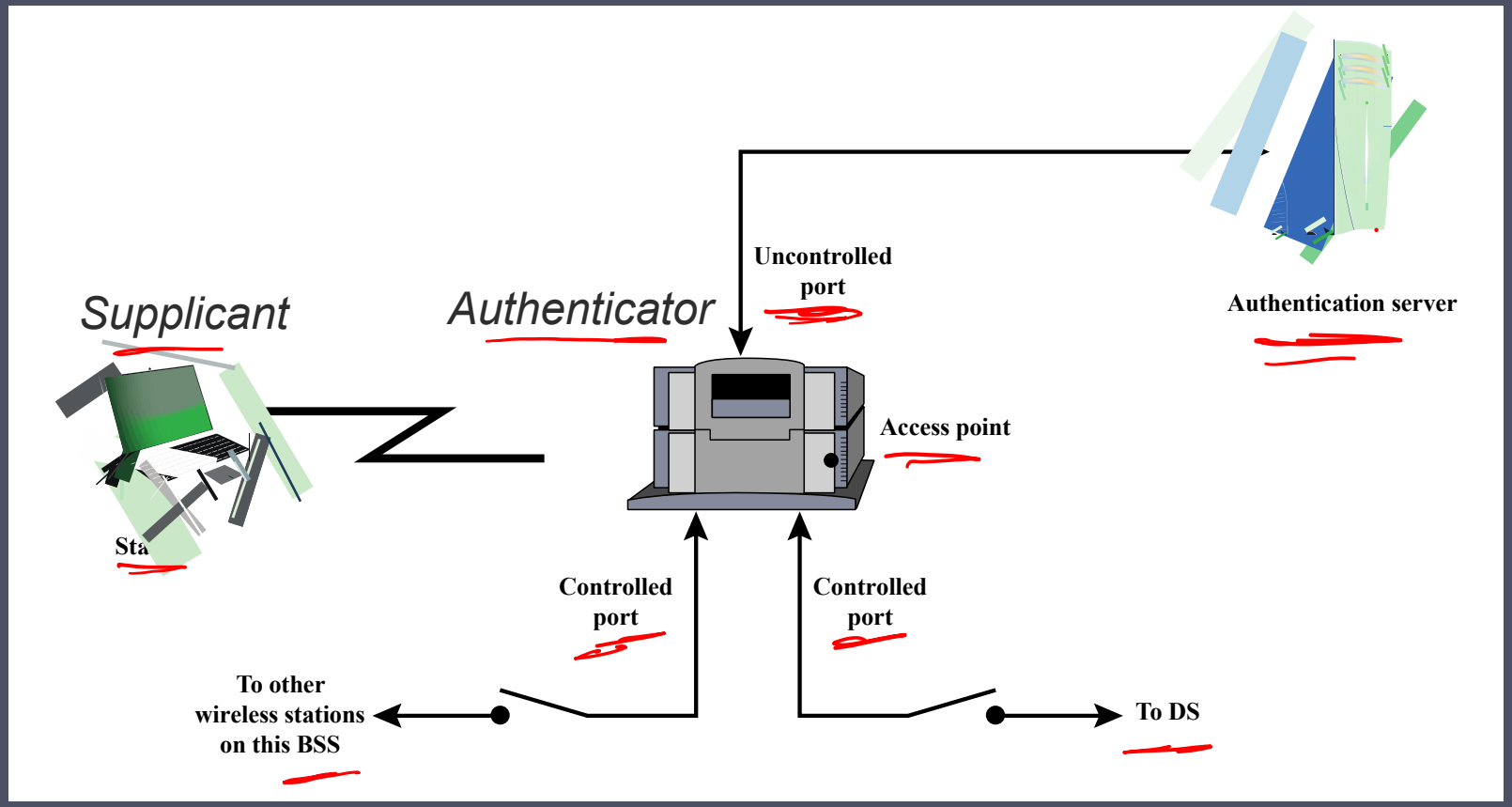
Securing Wireless Networks

- The main threat involving wireless access points is unauthorized access to the network
- Principal approach for preventing such access is the IEEE 802.1X standard for port-based network access control
  - The standard provides an authentication mechanism for devices wishing to attach to a LAN or wireless network
- Use of 802.1X can prevent rogue access points and other unauthorized devices from becoming insecure backdoors

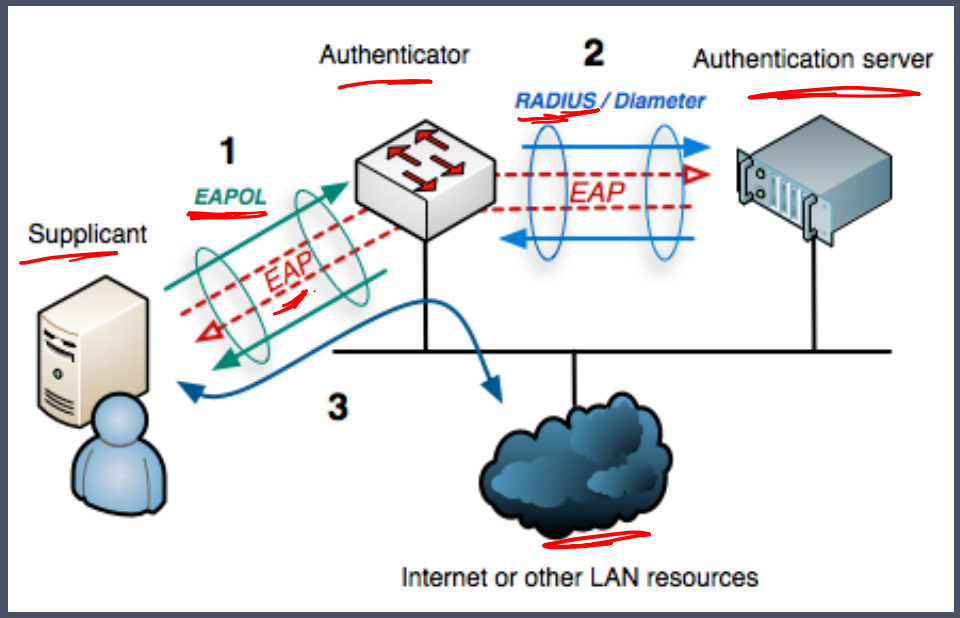




802.1X Access Control



IEEE 802.1X standard for Securing Wired/Wireless Networks



Extensible Authentication Protocol (EAP) originally designed for Point-to-Point Protocol (PPP)

EAPoL (EAP over LAN)

EAPoW (EAP over Wireless)

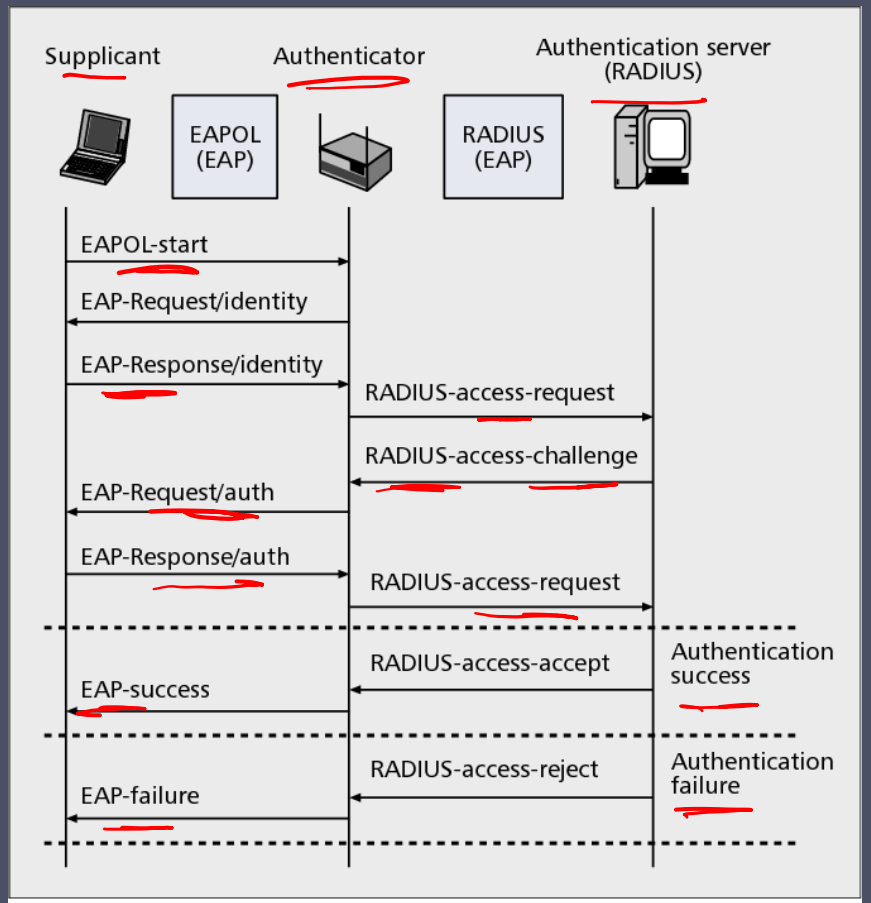


FIGURE 4. *A typical 802.1x message flow.*

Wireless Fidelity (Wi-Fi) Alliance

Wireless Fidelity (Wi-Fi) Alliance

https://www.wi-fi.org/

- The Wi-Fi Alliance is a non-profit organization that owns the Wi-Fi trademark.
  - Manufacturers may use the trademark to brand products certified for Wi-Fi interoperability.
- 802.11b
  - First 802.11 standard to gain broad industry acceptance
- Wireless Ethernet Compatibility Alliance (WECA)
  - Industry consortium formed in 1999 to address the concern of products from different vendors successfully interoperating
  - Later renamed the Wi-Fi Alliance in 2002
- Term used for certified 802.11b products is *Wi-Fi* in 1999
- In 2018, the Wi-Fi Alliance introduced simplified Wi-Fi generational numbering to indicate supported 802.11 standard by the equipment e.g.
- Other programs
  - Wi-Fi Direct: In October 2010, the Alliance began to certify Wi-Fi Direct
  - Wi-Fi Easy Connect protocol via QR Code
  - Wi-Fi Passpoint : Wi-Fi Passpoint, alternatively known as Hotspot 2.0
  - and may others…

Year	WiFi Versions/Protocols	Old name	New name
1999	First Generation	WiFi 802.11b	WiFI 1
1999	Second Generation	WiFi 802.11a	WiFi 2
2003	Third Generation	WiFI 802.11g	WiFi 3
2009	Four Generation	WiFi 802.11n	WiFi 4
2014	Fifth Generation	WiFi 802.11ac	WiFi 5
2019	Sixth Generation	WiFi 802.11ax	WiFi 6

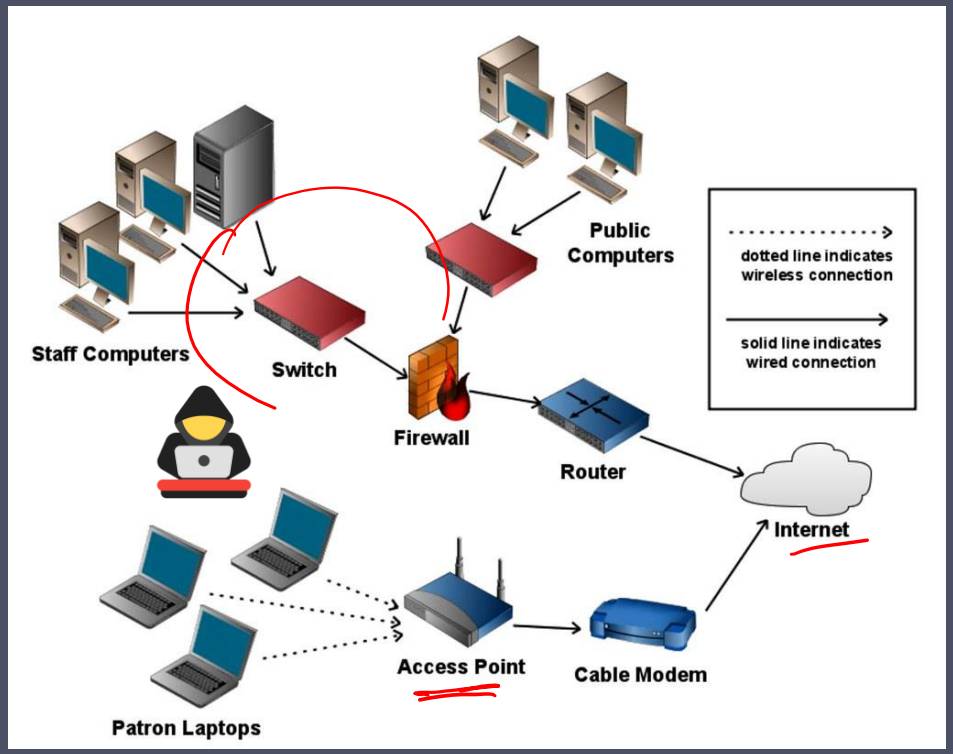


Demo Wi-Fi Info…

Wireless LAN Security

Wireless LAN Security

- There are two characteristics of a wired LAN that are not inherent in a wireless LAN.
  - In order to transmit over a wired LAN, a station must be physically connected to the LAN, which is not the case in Wireless…
  - Similarly, in order to receive a transmission from a station that is part of a wired LAN, the receiving station also must be attached to the wired LAN, which is not the case in Wireless...



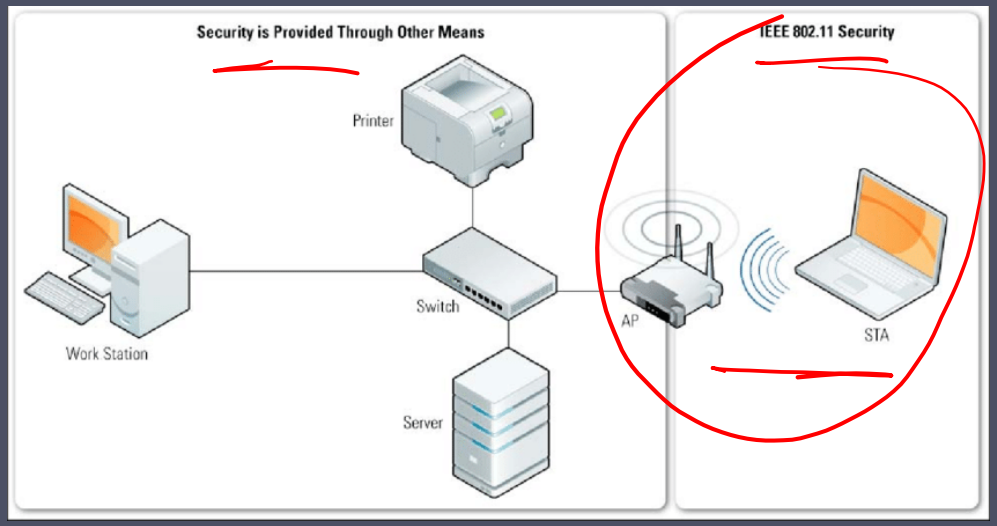
Wireless LAN Security

- The following security measures are often considered as trivial solutions for risk mitigation:
  - Disable the SSID broadcast
  - Maintain a list of authorized MAC addresses and block unauthorized ones from the network
  - Select AP locations in the middle of the building (not close to windows), use directional antennas and line walls and windows with metal foil to minimize the signal leakage to the outside of the building
- How much security do these measures bring?
- Need something more…real security solutions

Demo AP Setting…

Wireless LAN Security

- The original 802.11 specification included a set of security features for privacy and authentication that were quite weak.
  - For privacy, 802.11 defined the Wired Equivalent Privacy (WEP) algorithm.
  - The privacy portion of the 802.11 standard contained major weaknesses.
- Subsequently, the 802.11i task group has developed a set of capabilities to address the WLAN security issues. In order to accelerate the introduction of strong security into WLANs, the Wi-Fi Alliance promulgated Wi-Fi Protected Access (WPA) as a Wi-Fi standard.
  - WPA is a set of security mechanisms that eliminates most 802.11 security issues and was based on the trimmed down version of 802.11i standard.
- The final form of the 802.11i standard is referred to as Robust Security Network (RSN).
  - The Wi-Fi Alliance certifies vendors in compliance with the full 802.11i specification under the WPA2 program.



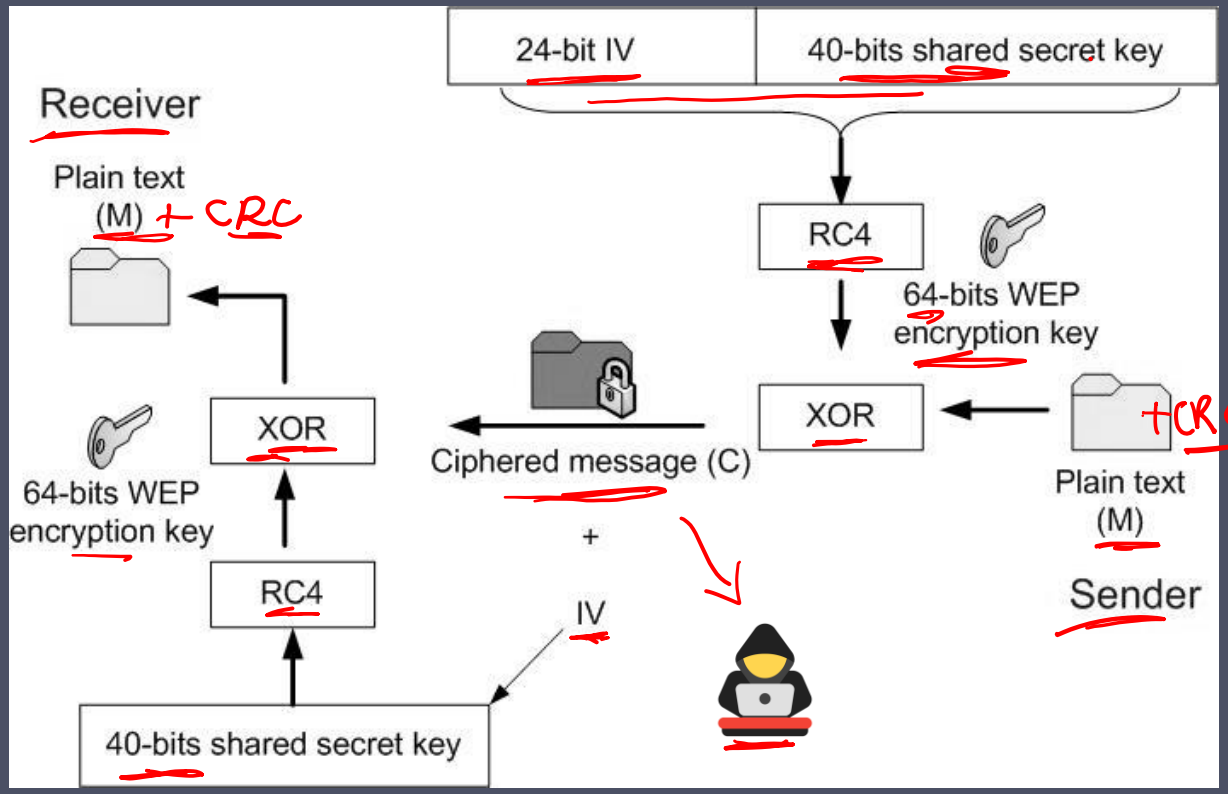
Demo Wi-Fi Info...

Wired Equivalent Privacy (WEP) Algorithm

Wired Equivalent Privacy (WEP) Algorithm

WEP was part of the IEEE 802.11 standard ratified in 1997.

Provide Support for
- Authentication
- Confidentiality
- Integrity



WEP is notoriously weak…

Wi-Fi Protected Access (WPA)

Brief History of Wi-Fi Protected Access (WPA)

- As WEP was not secure…
- Subsequently, the 802.11i task group has developed a set of capabilities to address the WLAN security issues.
  - In order to accelerate the introduction of strong security into WLANs, the Wi-Fi Alliance promulgated Wi-Fi Protected Access (WPA) as a Wi-Fi standard.
- WPA is a set of security mechanisms that eliminates most 802.11 security issues and was based on trimmed down version of 802.11i standard…initially released in 2003.
  - No new/specialized equipment was required…just firmware update
  - Based on TKIP / CCMP for encryption
    - TKIP - Temporal Key Integrity Protocol (TKIP)
    - CCMP - Counter mode CBC-MAC Protocol
- WPA2 is improved version of original WPA released in 2004.
  - Based on CCMP for encryption
- WPA3 comes as a successor to WPA2 - introduced in 2018
  - after July 2020, all Wi-Fi devices that are certified must support it.

WPA2

The Wi-Fi Alliance certifies vendors in compliance with the full 802.11i specification under the WPA2 program.

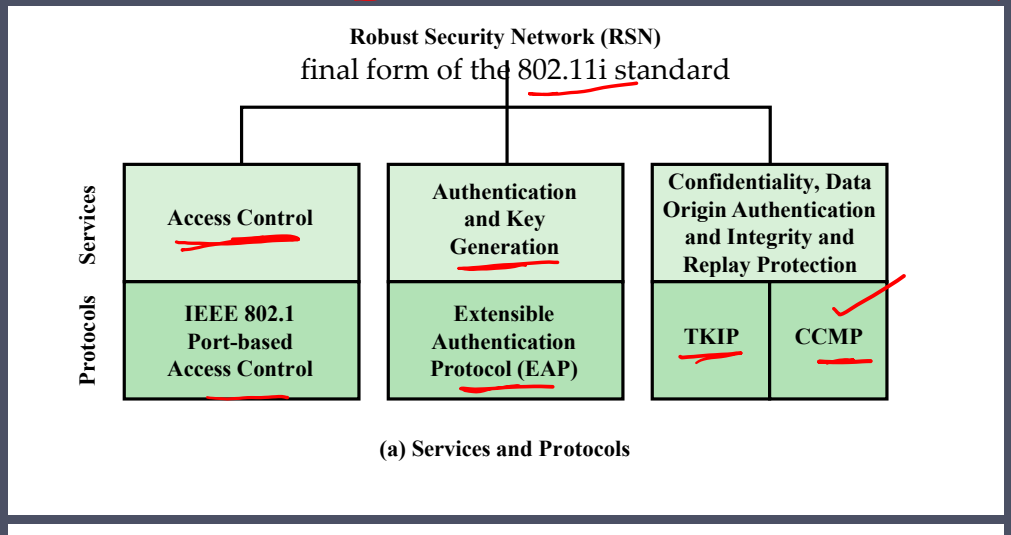


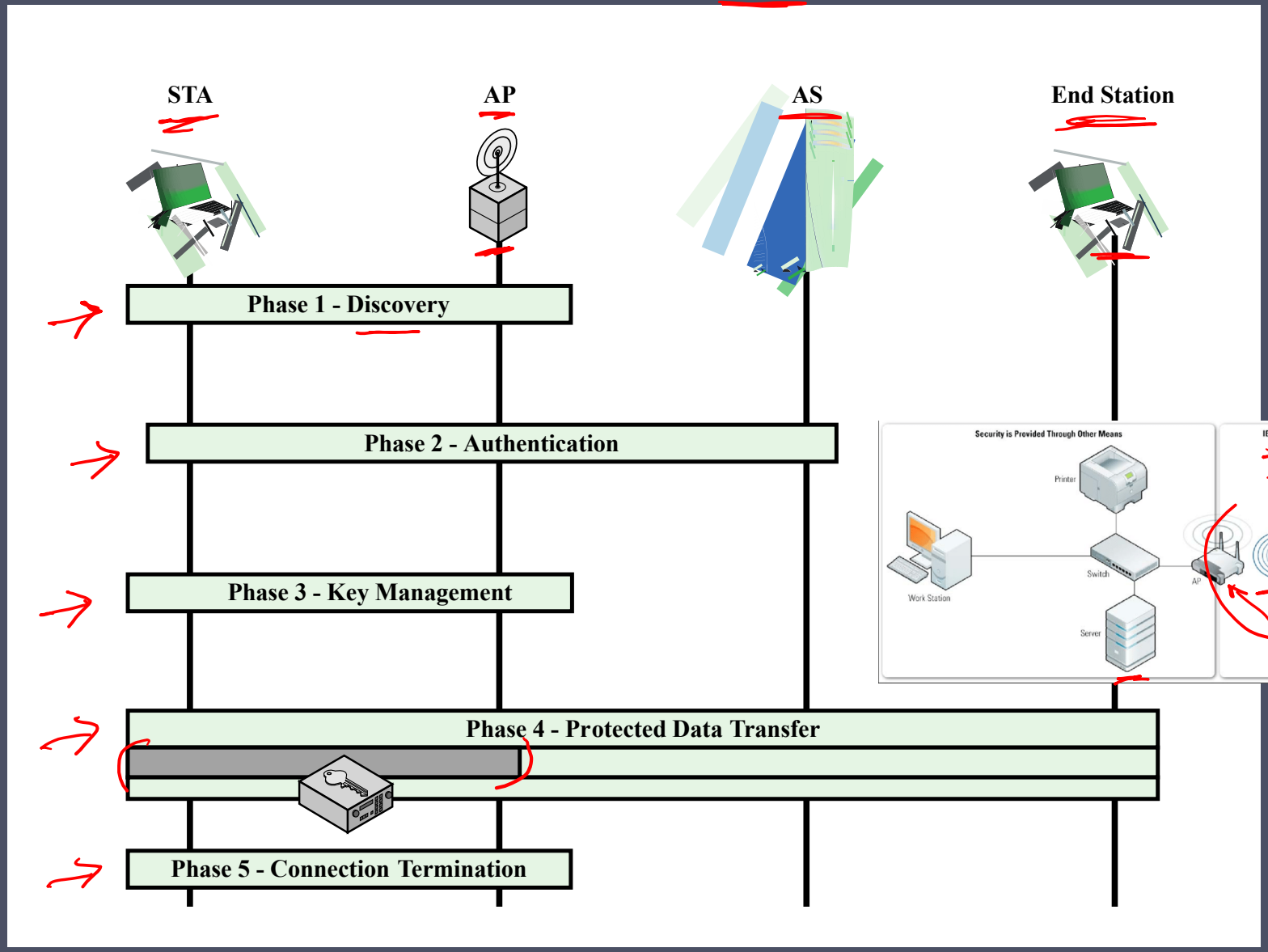
Figure 24.6 Elements of IEEE 802.11i

IEEE 802.11i Standard

Phases of Operation

IEEE 802.11i Phases of Operation

Essentially the working WPA2 protocol

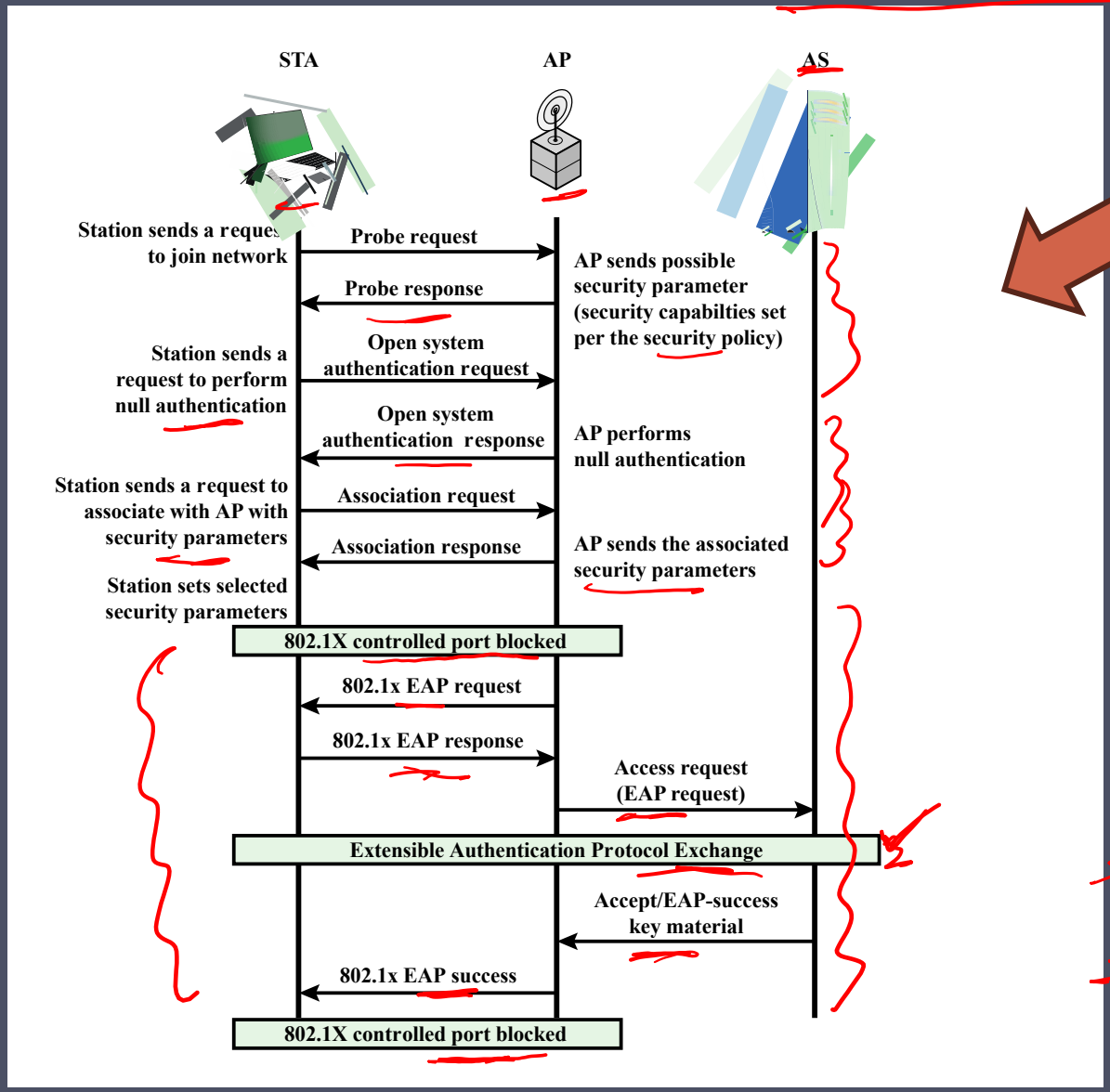


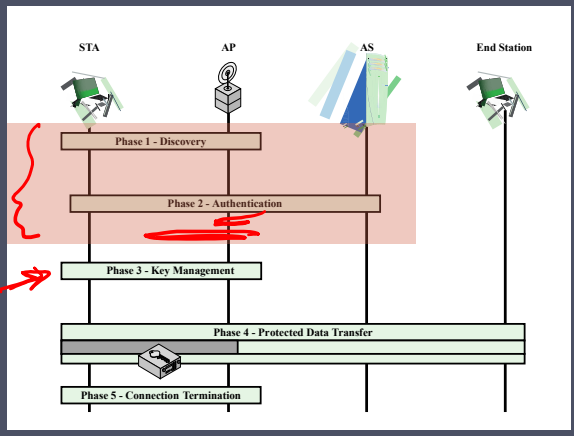
IEEE 802.11i Standard Phases of Operation

Capability Discovery, Association, and Authentication

IEEE 802.11i Phases of Operation

Essentially the working WPA2 protocol



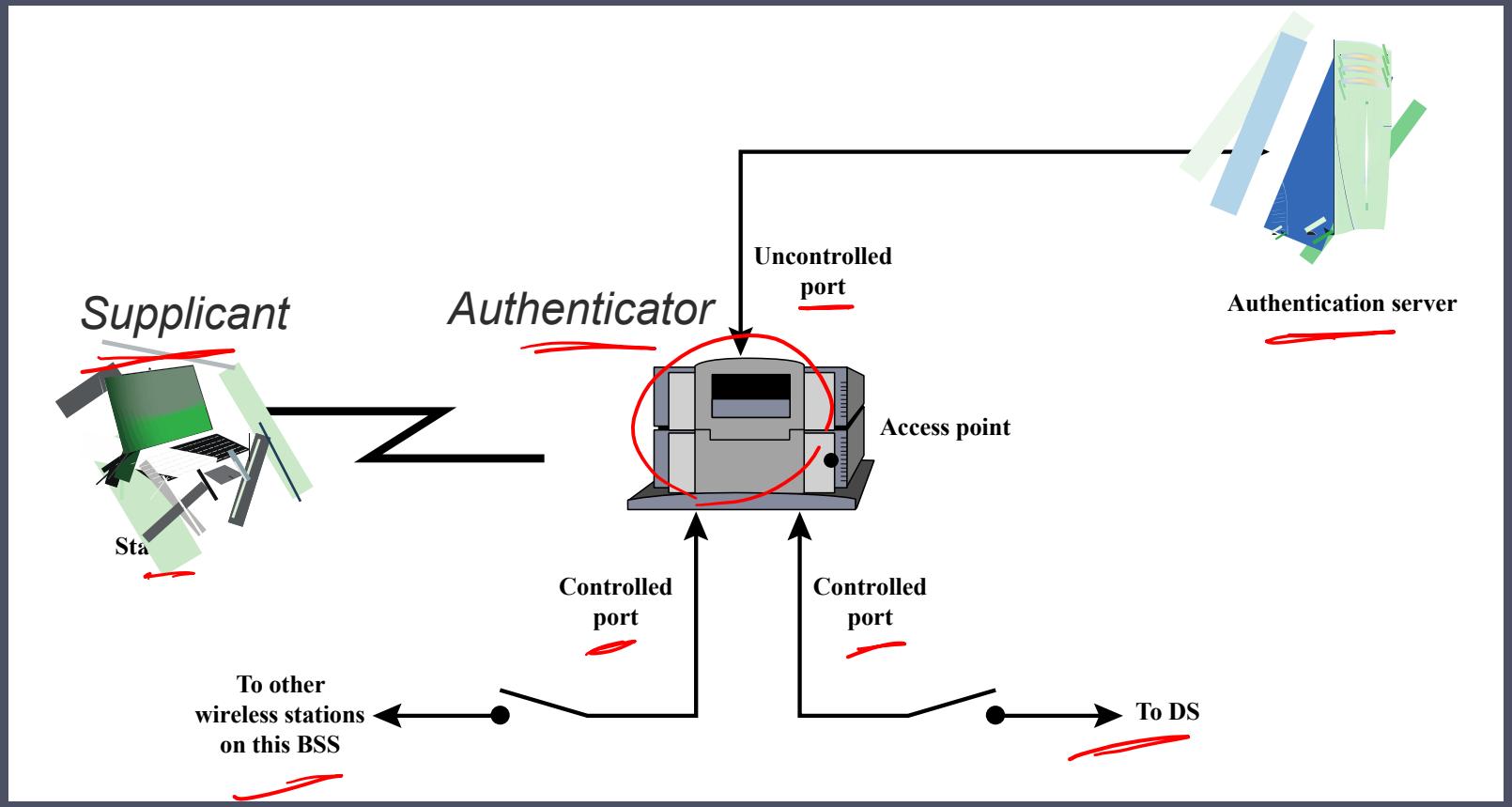


Capability Discovery, Association, and Authentication

Authentication phase consists of three phases:

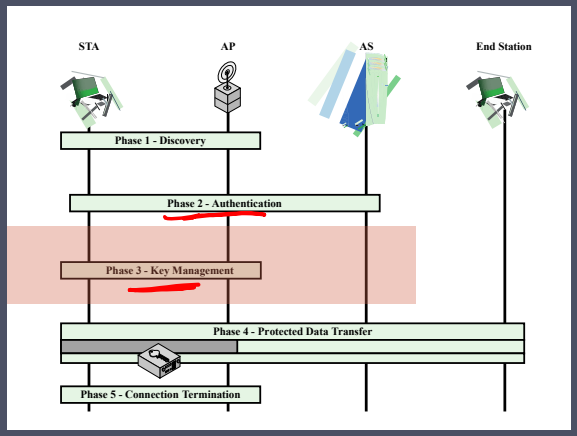
- **Connect to AS**
  - The STA sends a request to its AS through AP
- **EAP exchange**
  - Authenticates the STA and AS to each other
- **Secure key delivery**
  - On success, the AS generates a Master Session Key and sends it to the STA

802.1X Access Control

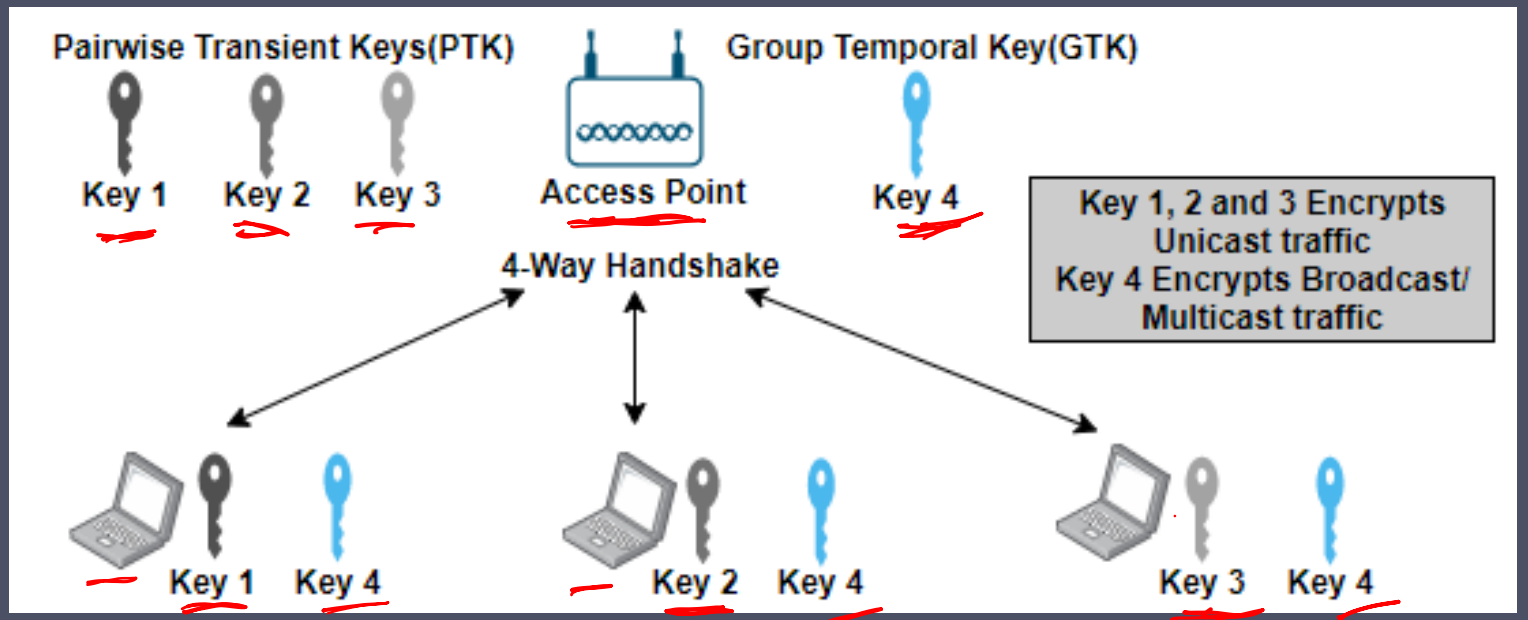


IEEE 802.11i
Key Hierarchies

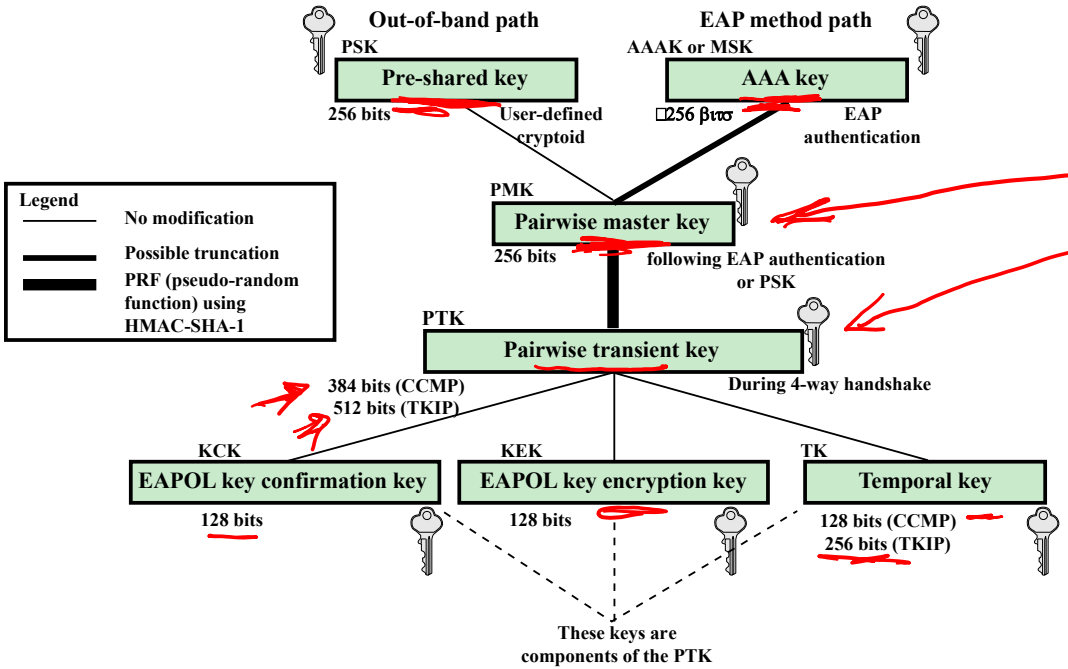
IEEE 802.11i Key Hierarchies



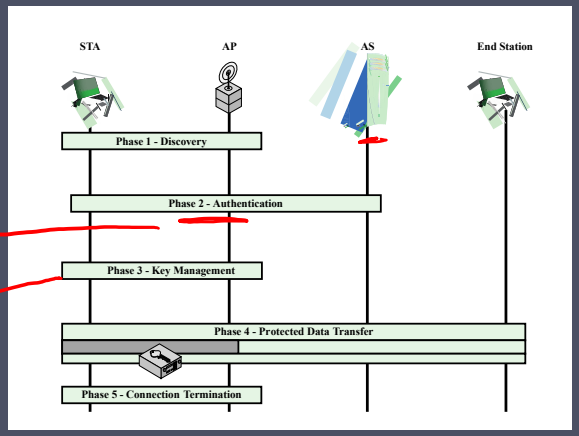
Pairwise keys and Group keys

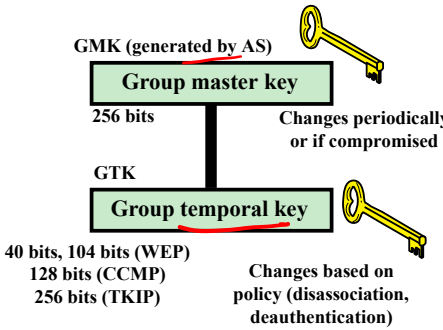


IEEE 802.11i Key Hierarchies



(a) Pairwise key hierarchy





(b) Group key hierarchy

Abbrev-iation	Name	Description / Purpose	Size (bits)	Type
AAA Key	Authentication, Accounting, and Authorization Key	Used to derive the PMK. Used with the IEEE 802.1X authentication and key management approach. Same as MMSK.	≥ 256	Key generation key, root key
PSK	Pre-Shared Key	Becomes the PMK in pre-shared key environments.	256	Key generation key, root key
PMK	Pairwise Master Key	Used with other inputs to derive the PTK.	256	Key generation key
GMK	Group Master Key	Used with other inputs to derive the GTK.	128	Key generation key
PTK	Pair-wise Transient Key	Derived from the PMK. Comprises the EAPOL-KCK, EAPOL-KEK, and TK and (for TKIP) the MIC key.	512 (TKIP) 384 (CCMP)	Composite key
TK	Temporal Key	Used with TKIP or CCMP to provide confidentiality and integrity protection for unicast user traffic.	256 (TKIP) 128 (CCMP)	Traffic key
GTK	Group Temporal Key	Derived from the GMK. Used to provide confidentiality and integrity protection for multicast/broadcast user traffic.	256 (TKIP) 128 (CCMP) 40, 104 (WEP)	Traffic key
MIC Key	Message Integrity Code Key	Used by TKIP's Michael MIC to provide integrity protection of messages.	64	Message integrity key
EAPOL-KCK	EAPOL-Key Confirmation Key	Used to provide integrity protection for key material distributed during the 4-Way Handshake.	128	Message integrity key
EAPOL-KEK	EAPOL-Key Encryption Key	Used to ensure the confidentiality of the GTK and other key material in the 4-Way Handshake.	128	Traffic key / key encryption key
WEP Key	Wired Equivalent Privacy Key	Used with WEP.	40, 104	Traffic key

IEEE 802.11i Keys for Data Confidentiality and Integrity Protocols

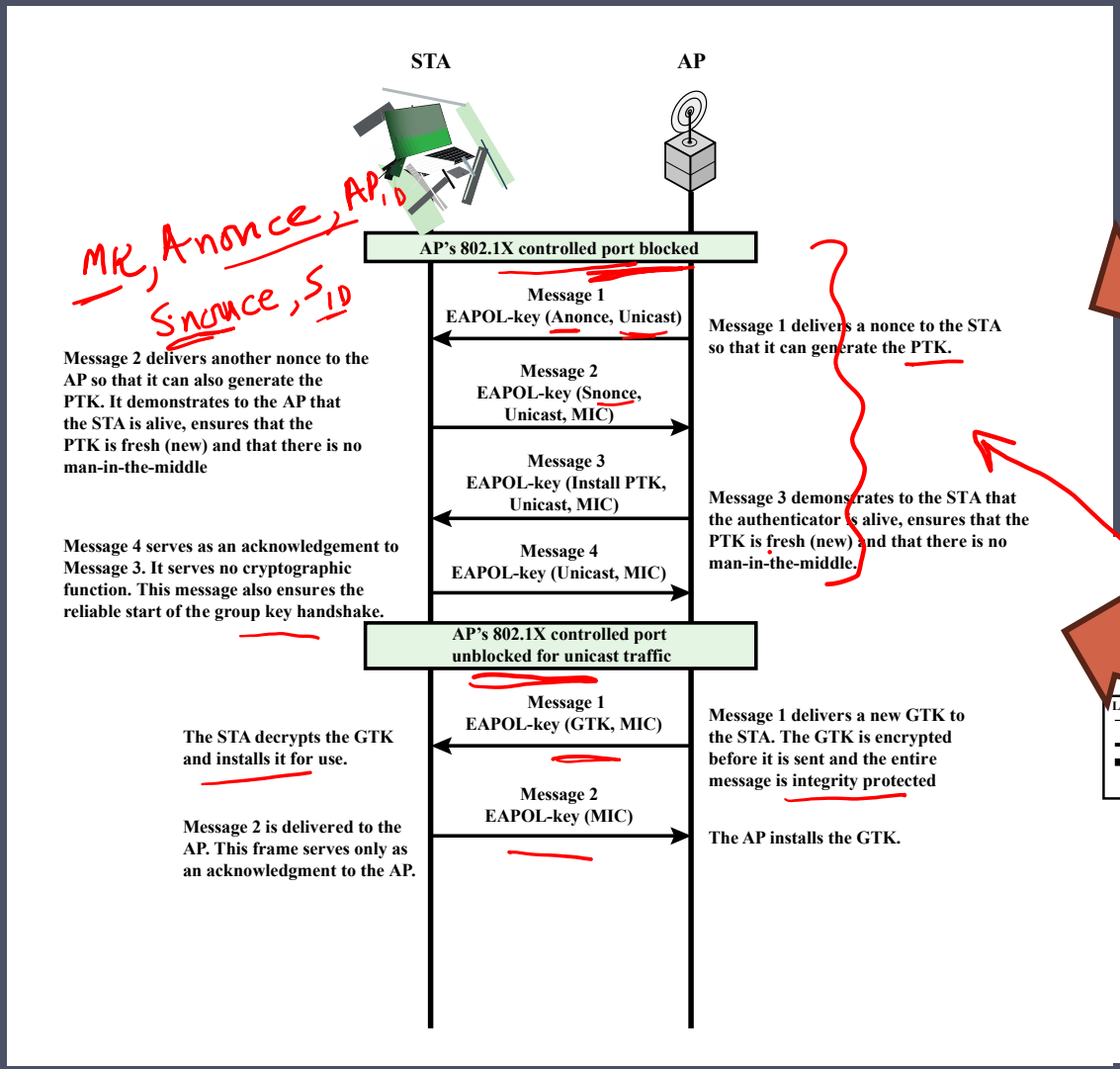
IEEE 802.11i Standard Phases of Operation

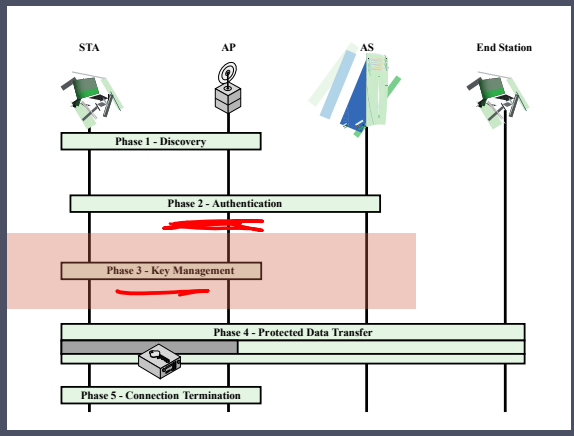
4-Way Handshake and Group Key Handshake

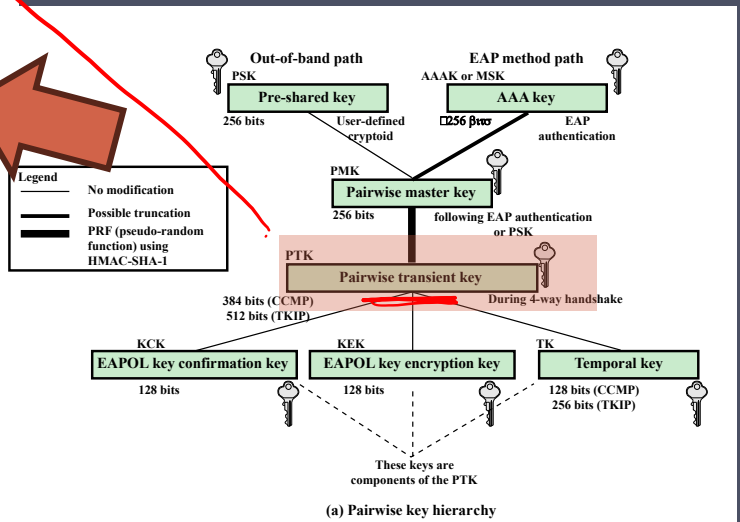
IEEE 802.11i Phases of Operation

Essentially the working WPA2 protocol

4-Way Handshake and Group Key Handshake







(a) Pairwise key hierarchy

About Strength of WPA2

- WPA2 ensures that data sent or received over your wireless network is encrypted,
  - only people with your network password have access to it.
- WPA2 use AES to replace the more vulnerable TKIP algorithm used in the original WPA protocol.
- WPA2 uses dynamic key encryption,
  - Regularly changes the key PTK and makes it more difficult to crack.
- However, Pre-Shared Key is derived from passphrase (Wi-Fi password)
  - This is common in Home networks… Enterprise networks use AS and are more safe…
- Weak Wif-Fi passwords can easily be cracked
  - All you need is to capture 4-way handshake exchange messages **"airodump-ng"**
  - Then use offline dictionary attacks…to crack the password **"aircrack-ng"**
- That's why we have WPA3 coming as a successor to WPA2…

Buffer Overflow Attacks

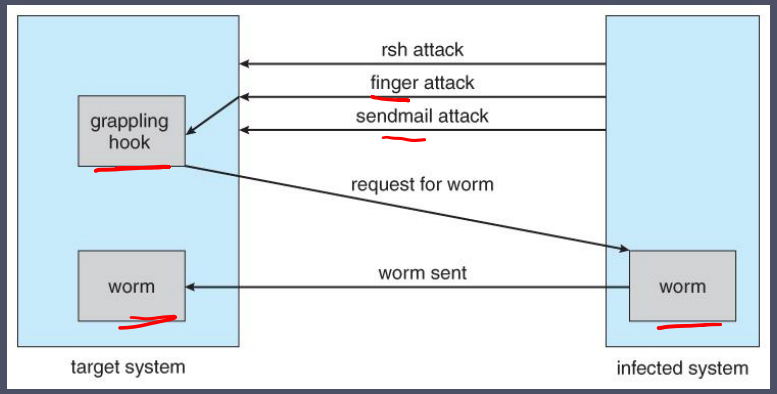
A Brief History of Some Buffer Overflow Attacks

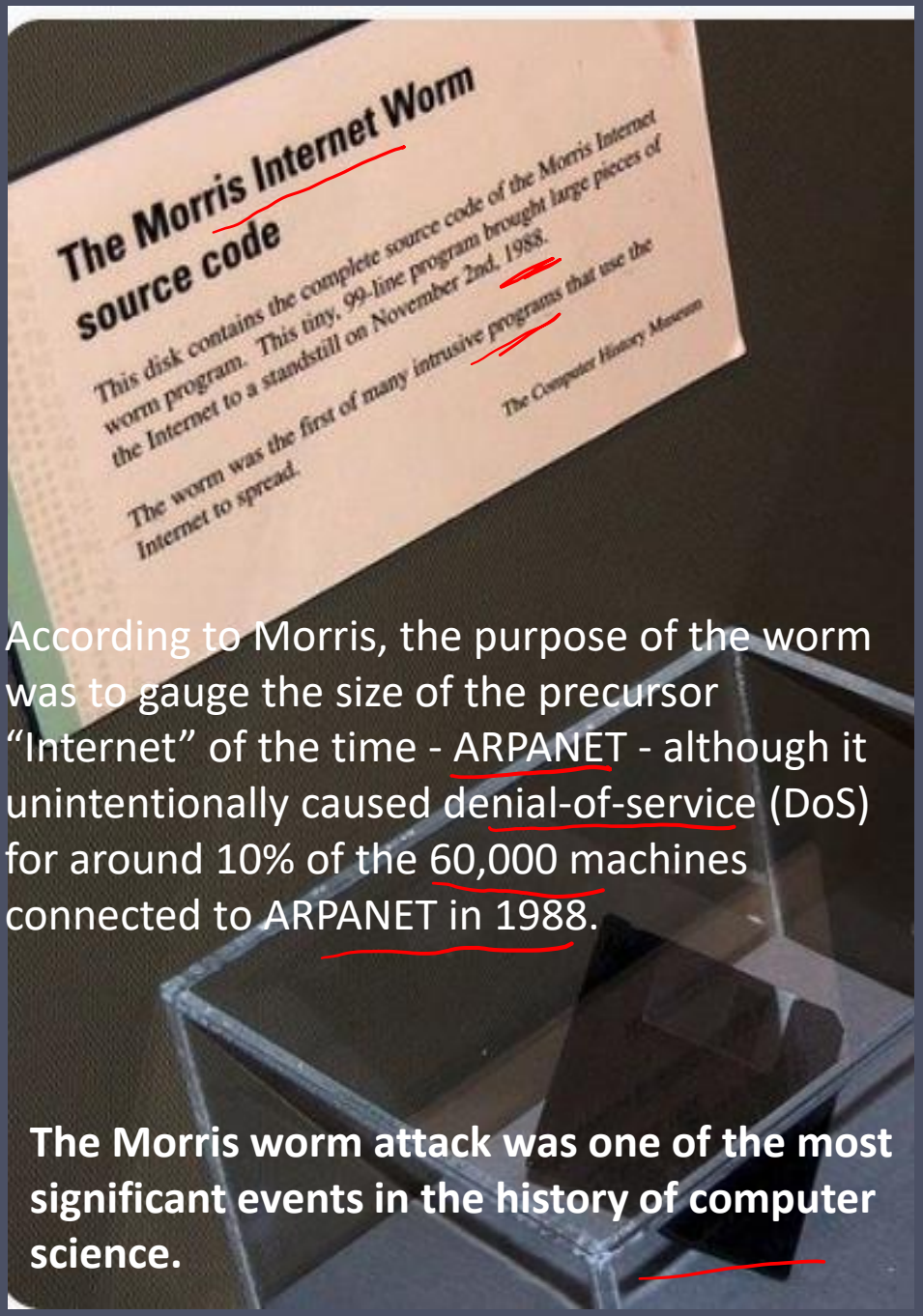
...



Robert Tappan Morris

The Morris worm functioned as a denial-of-service (DoS) attack.
The Morris worm spread by exploiting vulnerabilities in UNIX sendmail (using a backdoor), finger (through buffer overflow), and rsh/rexec (to explore whether it could operate).





According to Morris, the purpose of the worm was to gauge the size of the precursor "Internet" of the time - ARPANET - although it unintentionally caused denial-of-service (DoS) for around 10% of the 60,000 machines connected to ARPANET in 1988.

The Morris worm attack was one of the most significant events in the history of computer science.



Code Red was a computer worm observed on the Internet on July 15, 2001.

This worm targeted Windows-based systems with Microsoft IIS (Internet Information Services for Windows Server) installed exploiting **buffer overflow**.

The front page of an infected server might have been changed by the worm to following:

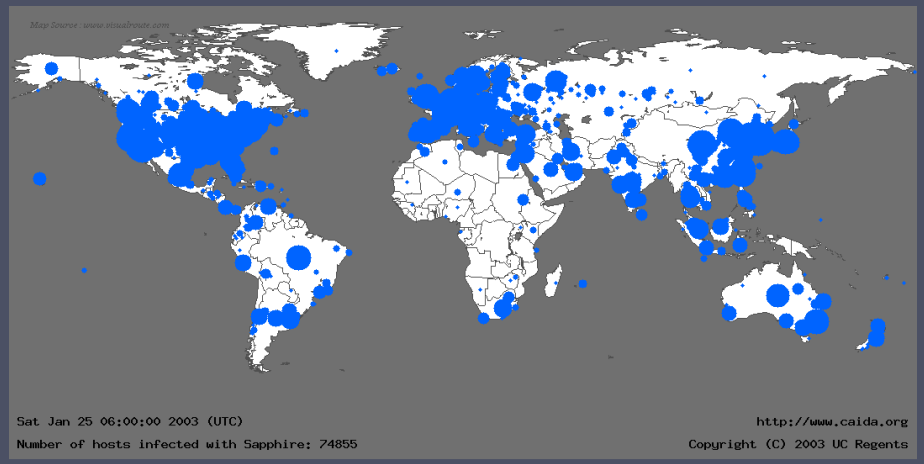


The Code Red worm has three phases

- Discovery and propagation… between day 1 and day 19 of any month
- Attack …between day 20 and day 27 of any month…DDoS attack on White House Web site
- Dormancy…From day 28 to the end of the month



SQL Slammer is a 2003 computer worm that caused a denial of service on some Internet hosts and dramatically slowed general Internet traffic and crashing routers all around the world. It spread rapidly, infecting most of its 75,000 victims within 10 minutes.



Slammer exploited a buffer overflow vulnerability in Microsoft SQL server 2000 in order to propagate.



Buffer overflow vulnerability in **WhatsApp**

On May 14, 2019, a buffer overflow vulnerability was identified in WhatsApp.

The vulnerability allows a remote attacker to execute arbitrary code on the target system.

The vulnerability exists due to a boundary error within the WhatsApp VOIP stack when processing SRTCP packets.

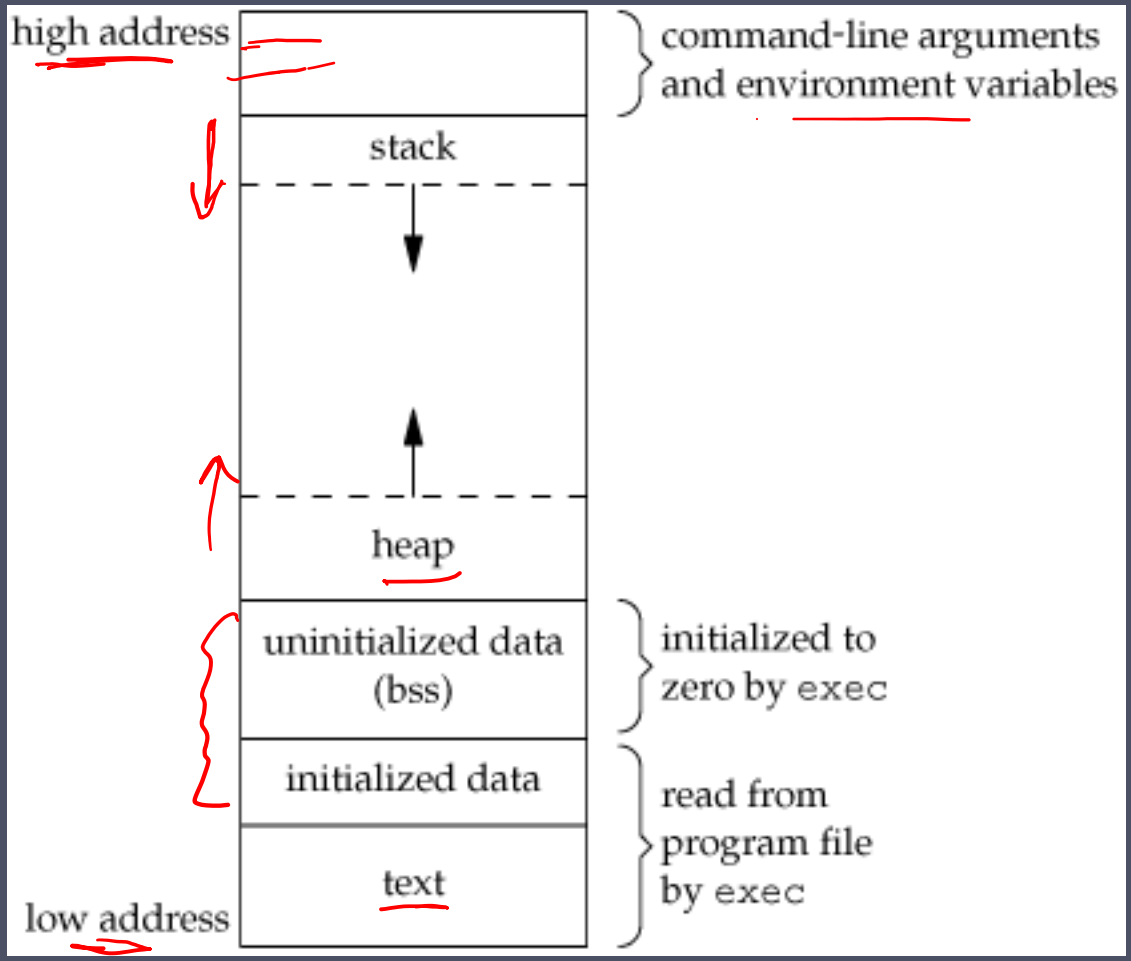
A remote attacker can send a series of specially crafted SRTCP packets sent to a target phone number, trigger buffer overflow and execute arbitrary code on the target device.

Successful exploitation of this vulnerability may result in complete compromise of vulnerable system.

https://www.whatsapp.com/security/advisories/archive?lang=en_US

Program Memory Layout and Stack Buffer

Memory Layout of a C Program

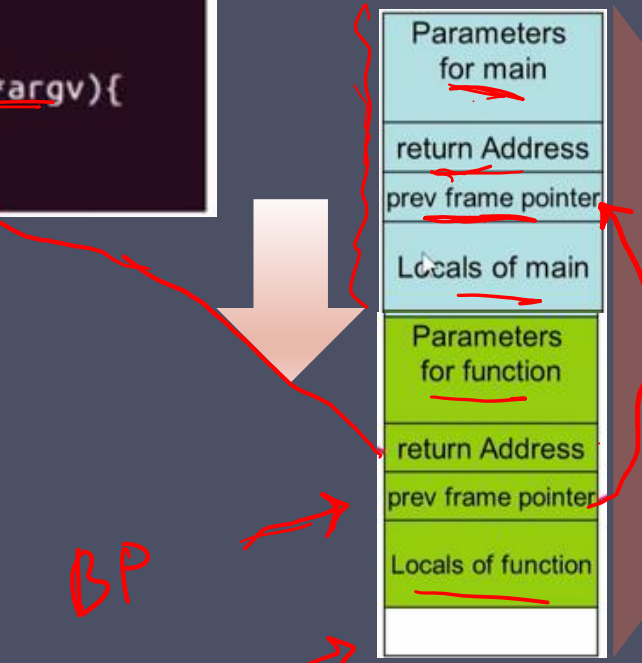


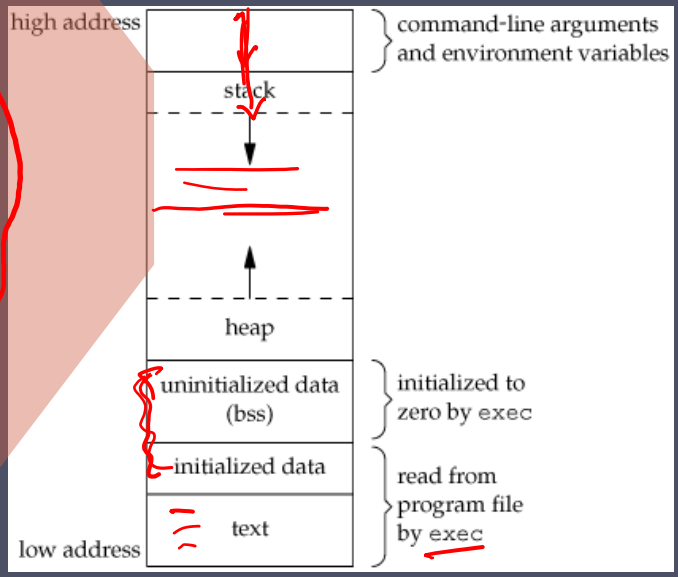
Stack in Program

(when functions are executing)

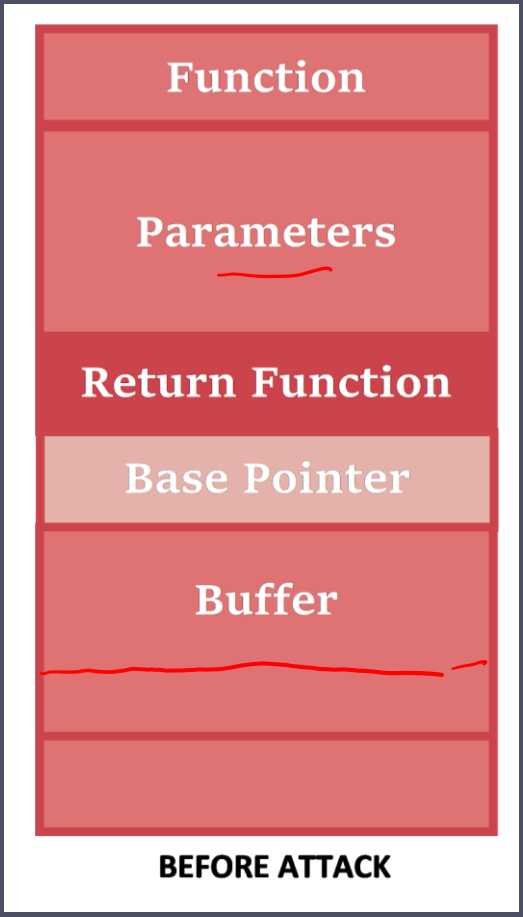
```
void function(int a, int b, int c){
  char buffer1[5];
  char buffer2[10];
}

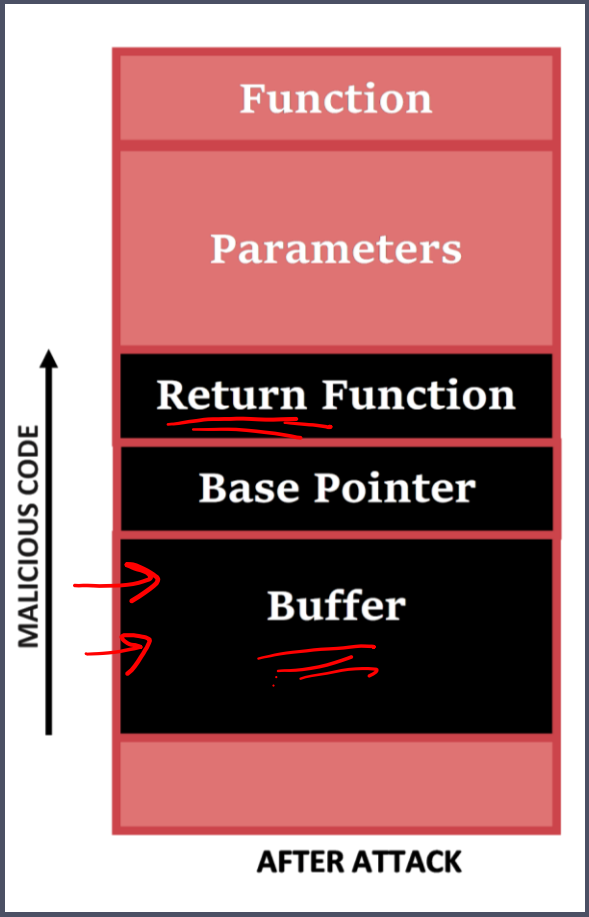
int main(int argc, char **argv){
  function(1,2,3);
}
```





Buffer Overflow Attack





Buffer Overflow Attack

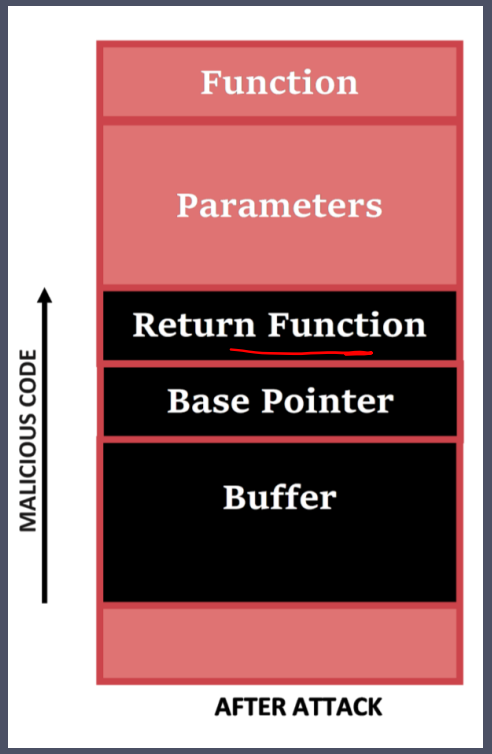
Buffer Overflow Attack

- A very common attack mechanism
  - First widely used by the Morris Worm in 1988
- Prevention techniques known
- Still of major concern
  - Legacy of buggy code in widely deployed operating systems and applications
  - Continued careless programming practices by programmers

Buffer Overflow

A buffer overflow, also known as a buffer overrun, is defined in the NIST *Glossary of Key Information Security Terms* as follows:

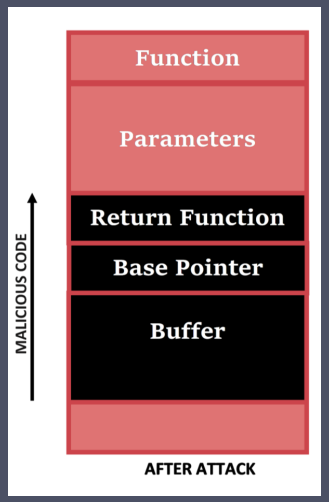
"A condition at an interface under which more input can be placed into a buffer or data holding area than the capacity allocated, overwriting other information. Attackers exploit such a condition to crash a system or to insert specially crafted code that allows them to gain control of the system."

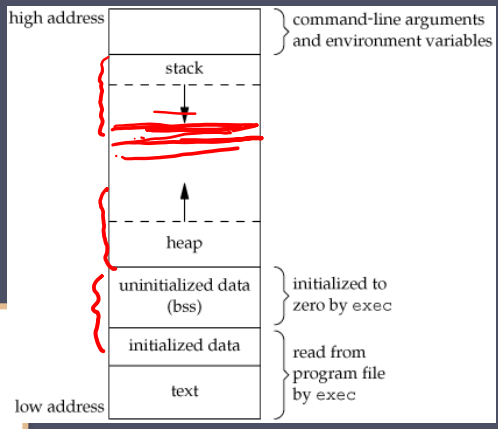


NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Buffer Overflow Basics

- Programming error when a process attempts to store data beyond the limits of a fixed-sized buffer
- Overwrites adjacent memory locations
  - Locations could hold other program variables, parameters, or program control flow data
- Buffer could be located on the stack, in the heap, or in the data section of the process





Consequences:

- **Corruption of program data**
- **Unexpected transfer of control**
- **Memory access violations**
- **Execution of code chosen by attacker**

Buffer Overflow Attacks

- To exploit a buffer overflow an attacker needs:
  - To identify a buffer overflow vulnerability in some program that can be triggered using externally sourced data under the attacker's control
  - To understand how that buffer is stored in memory and determine potential for corruption
- Identifying vulnerable programs can be done by:
  - Inspection of program source
  - Tracing the execution of programs as they process oversized input
  - Using tools such as fuzzing to automatically identify potentially vulnerable programs

Buffer Overflows Made Easy - YouTube

By The Cyber Mentor

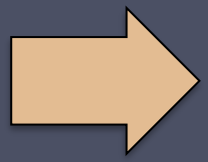
Role of Programming Language in Handling Buffer Overflow Attacks

Programming Language

- At the machine level data manipulated by machine instructions executed by the computer processor are stored in either the processor's registers or in memory
- Assembly language programmer is responsible for the correct interpretation of any saved data value

Modern high-level languages have a strong notion of type and valid operations

- **Not vulnerable to buffer overflows**
- **Does incur overhead, some limits on use**



C and related languages have high-level control structures, but allow direct access to memory

- **Hence are vulnerable to buffer overflow**
- **Have a large legacy of widely used, unsafe, and hence vulnerable code**

Basic Buffer Overflow Example

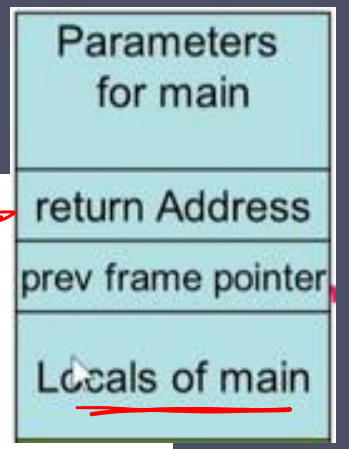
```
int main(int argc, char *argv[]) {
    int valid = FALSE;
    char str1[8];
    char str2[8];

    next_tag(str1);
    gets(str2);
    if (strncmp(str1, str2, 8) == 0)
        valid = TRUE;
    printf("buffer1: str1(%s), str2(%s), valid(%d)\n", str1, str2, valid);
}
```

(a) Basic buffer overflow C code

```
$ cc -g -o buffer1 buffer1.c
$ ./buffer1
START
buffer1: str1(START), str2(START), valid(1)
$ ./buffer1
EVILINPUTVALUE
buffer1: str1(TVALUE), str2(EVILINPUTVALUE), valid(0)
$ ./buffer1
BADINPUTBADINPUT
buffer1: str1(BADINPUT), str2(BADINPUTBADINPUT), valid(1)
```

(b) Basic buffer overflow example runs



Memory Address	Before gets(str2)	After gets(str2)	Contains Value of
. . . .	. . . .	. . . .	
bffffbf4	34fcffbf 4 . . .	34fcffbf 3 . . .	argv
bffffbf0	01000000	01000000	argc
bffffbec	c6bd0340 . . . @	c6bd0340 . . . @	return addr
bffffbe8	08fcffbf	08fcffbf	old base ptr
bffffbe4	00000000	01000000	valid
bffffbe0	80640140 . d . @	00640140 . d . @	
bffffbdc	54001540 T . . @	4e505554 N P U T	str1[4-7]
bffffbd8	53544152 S T A R	42414449 B A D I	str1[0-3]
bffffbd4	00850408	4e505554 N P U T	str2[4-7]
bffffbd0	30561540 0 V . @	42414449 B A D I	str2[0-3]
. . . .	. . . .	. . . .	

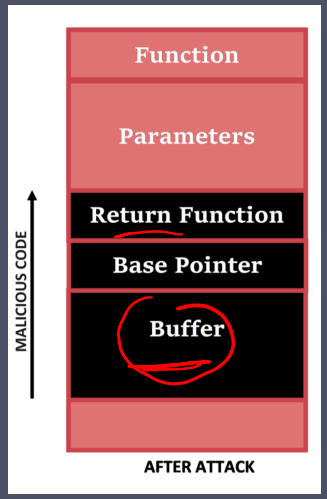
Some Common Unsafe C Standard Library Routines

`gets(char *str)`	read line from standard input into str
`sprintf(char *str, char *format, ...)`	create str according to supplied format and variables
`strcat(char *dest, char *src)`	append contents of string src to string dest
`strcpy(char *dest, char *src)`	copy contents of string src to string dest
`vsprintf(char *str, char *fmt, va_list ap)`	create str according to supplied format and variables

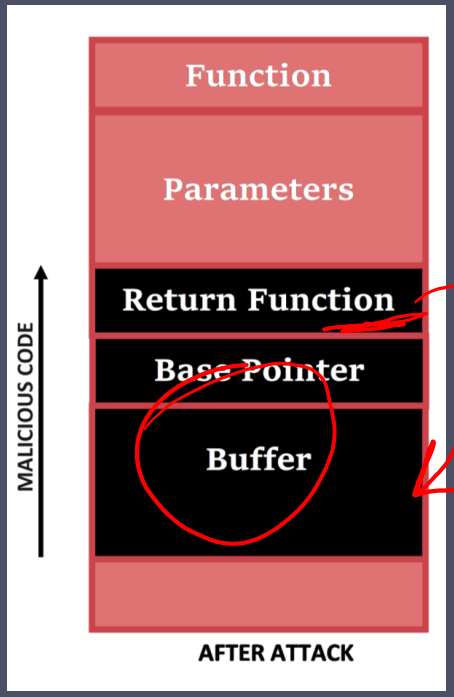
Demo in Visual Studio…

Shellcode

Shellcode



- Code supplied by attacker
  - Often saved in buffer being overflowed
  - Traditionally transferred control to a user command-line interpreter (shell)
- Machine code
  - Specific to processor and operating system
  - Traditionally needed good assembly language skills to create
  - More recently a number of sites and tools have been developed that automate this process
- Metasploit Project
  - Provides useful information to people who perform penetration, IDS signature development, and exploit research



Example UNIX Shellcode

```
int main(int argc, char *argv[])
{
   char *sh;
   char *args[2];

   sh = "/bin/sh";
   args[0] = sh;
   args[1] = NULL;
   execve(sh, args, NULL);
}
```

(a) Desired shellcode code in C

```
      nop
      nop                  // end of nop sled
      jmp    find          // jump to end of code
cont:  pop    %esi          // pop address of sh off stack into %esi
      xor    %eax,%eax     // zero contents of EAX
      mov    %al,0x7(%esi)  // copy zero byte to end of string sh (%esi)
      lea    (%esi),%ebx    // load address of sh (%esi) into %ebx
      mov    %ebx,0x8(%esi)  // save address of sh in args[0] (%esi+8)
      mov    %eax,0xc(%esi)  // copy zero to args[1] (%esi+c)
      mov    $0xb,%al       // copy execve syscall number (11) to AL
      mov    %esi,%ebx      // copy address of sh (%esi) t0 %ebx
      lea    0x8(%esi),%ecx  // copy address of args (%esi+8) to %ecx
      lea    0xc(%esi),%edx  // copy address of args[1] (%esi+c) to %edx
      int    $0x80          // software interrupt to execute syscall
find:  call   cont           // call cont which saves next address on stack
sh:    .string "/bin/sh "     // string constant
args:  .long 0               // space used for args array
      .long 0               // args[1] and also NULL for env array
```

(b) Equivalent position-independent x86 assembly code

```
90 90 eb 1a 5e 31 c0 88 46 07 8d 1e 89 5e 08 89
46 0c b0 0b 89 f3 8d 4e 08 8d 56 0c cd 80 e8 e1
ff ff ff 2f 62 69 6e 2f 73 68 20 20 20 20 20 20
```

(c) Hexadecimal values for compiled x86 machine code

Stack Overflow Variants

Target program can be:

- A trusted system utility
- Network service daemon
- Commonly used library code

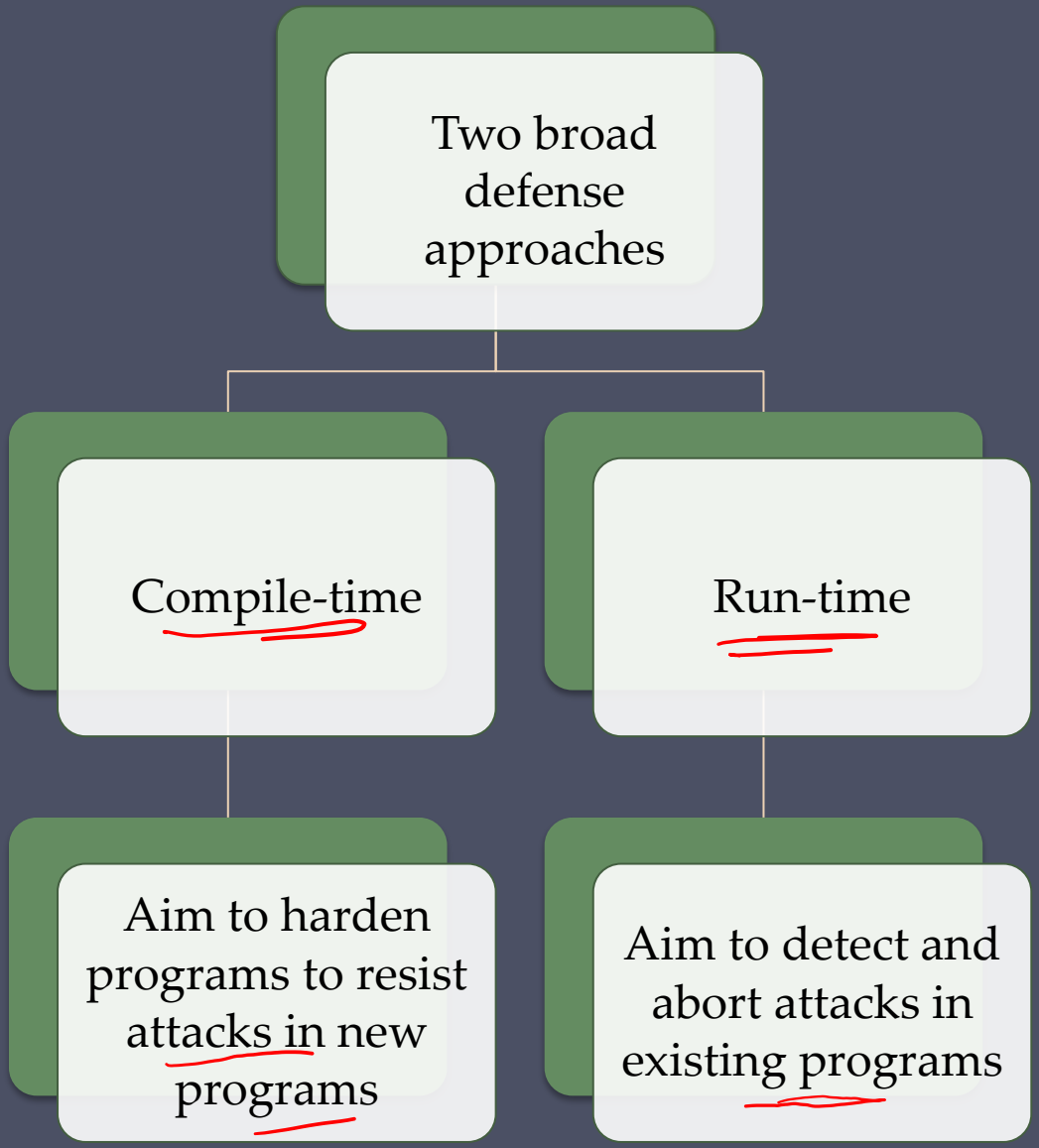
Shellcode functions

- **Launch a remote shell when connected to**
- **Create a reverse shell that connects back to the hacker**
- **Use local exploits that establish a shell**
- **Flush firewall rules that currently block other attacks**
- **Break out of a chroot (restricted execution) environment, giving full access to the system**

Buffer Overflow Defenses

Buffer Overflow Defenses

- Buffer overflows are widely exploited



Compile-Time Defenses: Programming Language

- Use a modern high-level language
  - Not vulnerable to buffer overflow attacks
  - Compiler enforces range checks and permissible operations on variables

Disadvantages

- Additional code must be executed at run time to impose checks
- Flexibility and safety comes at a cost in resource use
- Distance from the underlying machine language and architecture means that access to some instructions and hardware resources is lost
- Limits their usefulness in writing code, such as device drivers, that must interact with such resources

Compile-Time Defenses: Safe Coding Techniques

- C designers placed much more emphasis on space efficiency and performance considerations than on type safety
  - Assumed programmers would exercise due care in writing code
- Programmers need to inspect the code and rewrite any unsafe coding
  - An example of this is the OpenBSD project
- Programmers have audited the existing code base, including the operating system, standard libraries, and common utilities
  - This has resulted in what is widely regarded as one of the safest operating systems in widespread use

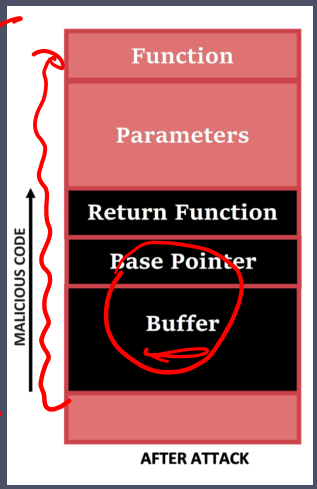
Run-Time Defenses: Executable Address Space Protection

Use virtual memory support to make some regions of memory non-executable

- Requires support from memory management unit (MMU)
- Long existed on SPARC / Solaris systems
- Recent on x86 Linux/Unix/Windows systems

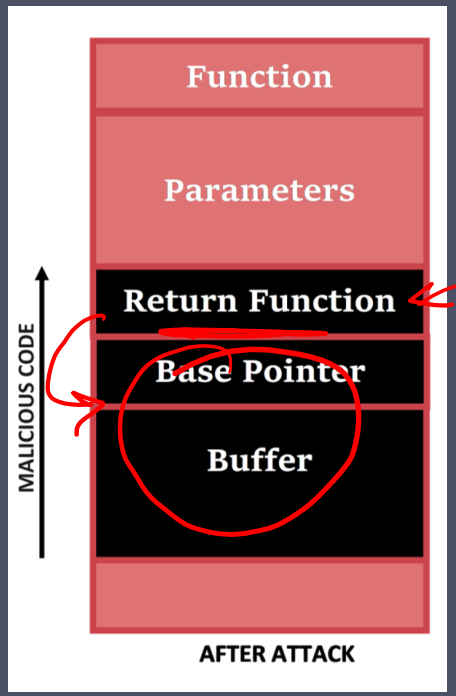
Issues

- Support for executable stack code
- Special provisions are needed



Run-Time Defenses: Address Space Randomization

- Manipulate location of key data structures
  - Stack, heap, global data
  - Using random shift for each process
  - Large address range on modern systems means wasting some has negligible impact
- Randomize location of heap buffers
- Random location of standard library functions



Software Security

CWE/SANS TOP 25 Most Dangerous Software Errors (2011)

Software Error Category: Insecure Interaction Between Components

Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
Unrestricted Upload of File with Dangerous Type
Cross-Site Request Forgery (CSRF)
URL Redirection to Untrusted Site ('Open Redirect')

Software Error Category: Risky Resource Management

Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
Download of Code Without Integrity Check
Inclusion of Functionality from Untrusted Control Sphere
Use of Potentially Dangerous Function
Incorrect Calculation of Buffer Size
Uncontrolled Format String
Integer Overflow or Wraparound

Software Error Category: Porous Defenses

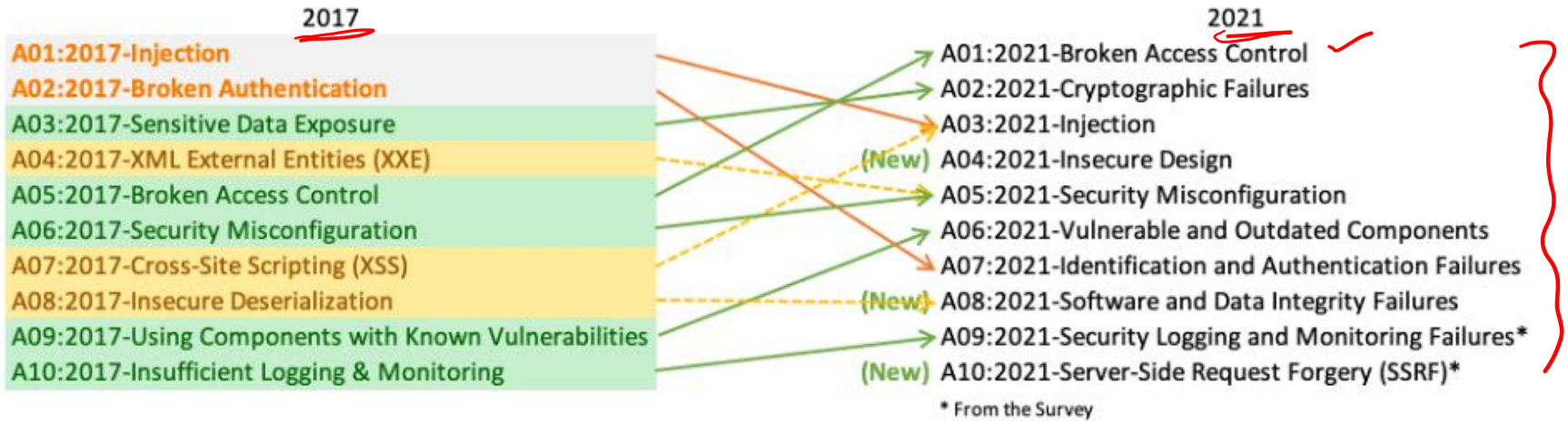
Missing Authentication for Critical Function
Missing Authorization
Use of Hard-coded Credentials
Missing Encryption of Sensitive Data
Reliance on Untrusted Inputs in a Security Decision
Execution with Unnecessary Privileges
Incorrect Authorization
Incorrect Permission Assignment for Critical Resource
Use of a Broken or Risky Cryptographic Algorithm
Improper Restriction of Excessive Authentication Attempts
Use of a One-Way Hash without a Salt

https://cwe.mitre.org/top25/archive/2023/2023_top25_list.html

OWASP Top 10 Web Application Security Risks

Open Web Application Security Project (OWASP)

There are three new categories, four categories with naming and scoping changes, and some consolidation in the Top 10 for 2021.



https://owasp.org/www-project-top-ten/

Security Flaws

- Critical Web application security flaws include five related to insecure software code
  - Unvalidated input
  - Cross-site scripting
  - Buffer overflow
  - Injection flaws
  - Improper error handling
- These flaws occur as a consequence of insufficient checking and validation of data and error codes in programs
- Awareness of these issues is a critical initial step in writing more secure program code
- Emphasis should be placed on the need for software developers to address these known areas of concern

Reducing Software Vulnerabilities

Reducing Software Vulnerabilities

- The NIST report NISTIR 8151 presents a range of approaches to reduce the number of software vulnerabilities
- It recommends:
  - Stopping vulnerabilities before they occur by using improved methods for specifying and building software
  - Finding vulnerabilities before they can be exploited by using better and more efficient testing techniques
  - Reducing the impact of vulnerabilities by building more resilient architectures

Software Security, Quality and Reliability

Software Security, Quality and Reliability





- Software quality and reliability

- Software Security

Software Security, Quality and Reliability

- Software quality and reliability:
  - Concerned with the accidental failure of program as a result of some theoretically random, unanticipated input, system interaction, or use of incorrect code
  - Improve using structured design and testing to identify and eliminate as many bugs as possible from a program
  - Concern is not how many bugs, but how often they are triggered

- Software security:
  - Attacker chooses probability distribution, specifically targeting bugs that result in a failure that can be exploited by the attacker
  - Triggered by inputs that differ dramatically from what is usually expected
  - Unlikely to be identified by common testing approaches

Defensive Programming

Defensive Programming

- Designing and implementing software so that it continues to function even when under attack
- Requires attention to all aspects of program execution, environment, and type of data it processes
- Software is able to detect erroneous conditions resulting from some attack
- Also referred to as secure programming
- Key rule is to never assume anything, check all assumptions and handle any possible error states

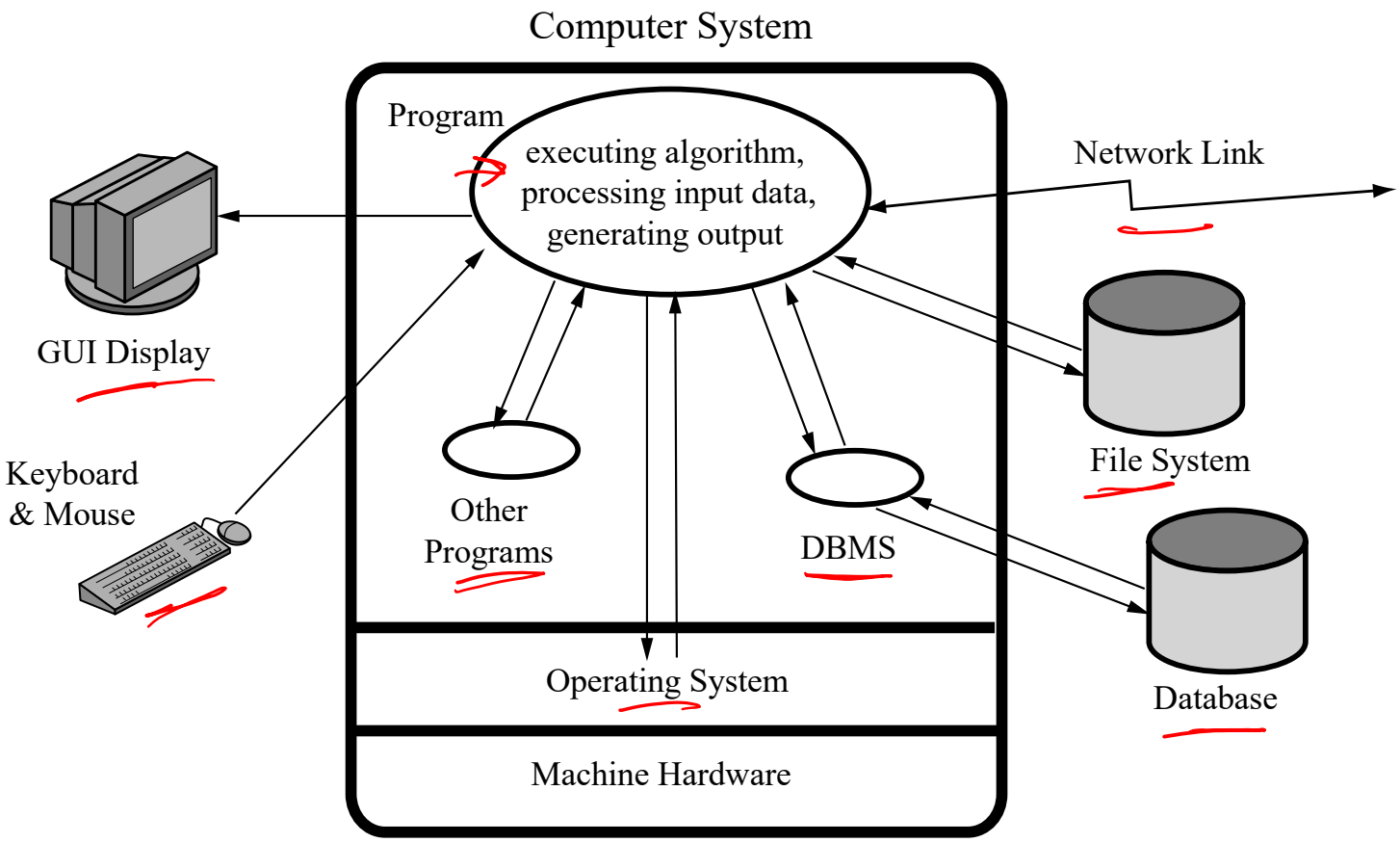


Figure 11.1 Abstract View of Program

Defensive Programming

- Programmers often make assumptions about the type of inputs a program will receive and the environment it executes in
  - Assumptions need to be validated by the program and all potential failures handled gracefully and safely
- Requires a changed mindset to traditional programming practices
  - Programmers have to understand how failures can occur and the steps needed to reduce the chance of them occurring in their programs
- Conflicts with business pressures to keep development times as short as possible to maximize market advantage

Handling Program Input

Handling Program Input

Incorrect handling of input data is a very common failing

Input is any source of data from outside and whose value is not explicitly known by the programmer when the code was written

Must identify all data sources

Explicitly validate assumptions on size and type of values before use

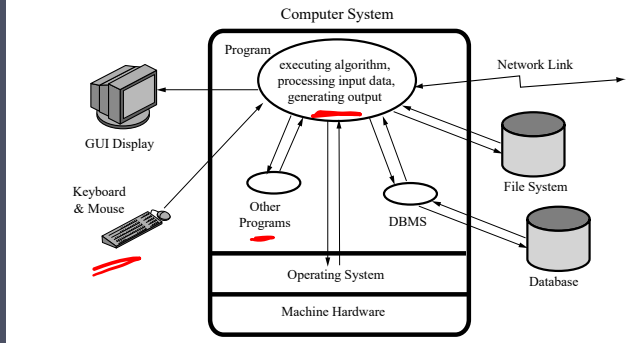


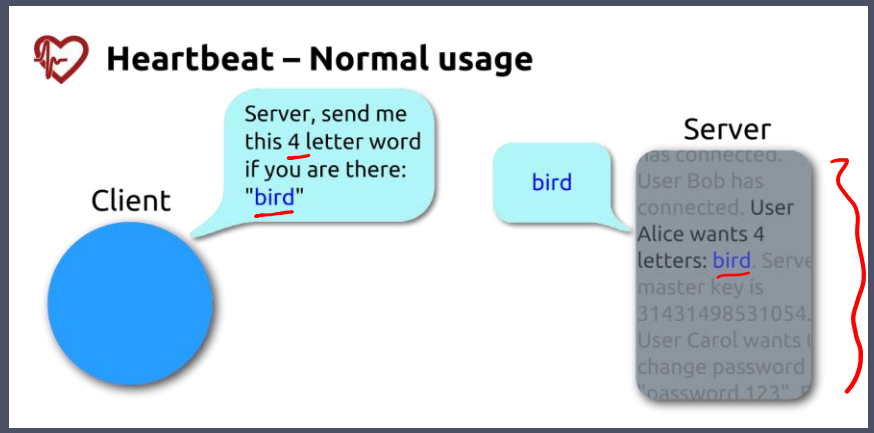
Figure 11.1 Abstract View of Program

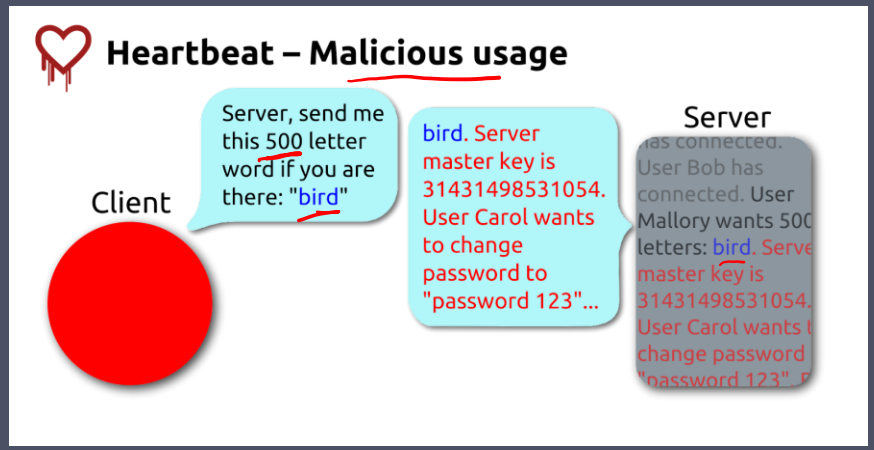
Input Size & Buffer Overflow

- Programmers often make assumptions about the maximum expected size of input
  - Allocated buffer size is not confirmed
  - Resulting in buffer overflow
- Testing may not identify vulnerability
  - Test inputs are unlikely to include large enough inputs to trigger the overflow
- Safe coding treats all input as dangerous

Interpretation of Program Input

- Program input may be binary or text
  - Binary interpretation depends on encoding and is usually application specific
- There is an increasing variety of character sets being used
  - Care is needed to identify just which set is being used and what characters are being read
- Failure to validate may result in an exploitable vulnerability
- 2014 Heartbleed OpenSSL bug is a recent example of a failure to check the validity of a binary input value





Injection Attacks

Injection Attacks

- Flaws relating to invalid handling of input data, specifically when program input data can accidentally or deliberately influence the flow of execution of the program

Most often occur in scripting languages

- Encourage reuse of other programs and system utilities where possible to save coding effort

```
$name = $ REQUEST['name'];
$query = "SELECT * FROM suppliers WHERE name = '" . $name . "';"
$result = mysql_query($query);
```

(a) Vulnerable PHP code

```
$name = $_REQUEST['name'];
$query = "SELECT * FROM suppliers WHERE name = '" .
     mysql_real_escape_string($name) . "';"
$result = mysql_query($query);
```

(b) Safer PHP code

Figure 11.3 SQL Injection Example

SQL Injection Attack Demo

https://www.codingame.com/playgrounds/154/sql-injection-demo/sql-injection

```
$name = $_REQUEST['name'];
$query = "SELECT * FROM suppliers WHERE name = '" . $name . "';"
$result = mysql_query($query);
```

(a) Vulnerable PHP code

```
$name = $_REQUEST['name'];
$query = "SELECT * FROM suppliers WHERE name = '" .
     mysql_real_escape_string($name) . "';"
$result = mysql_query($query);
```

(b) Safer PHP code

Figure 11.3 SQL Injection Example

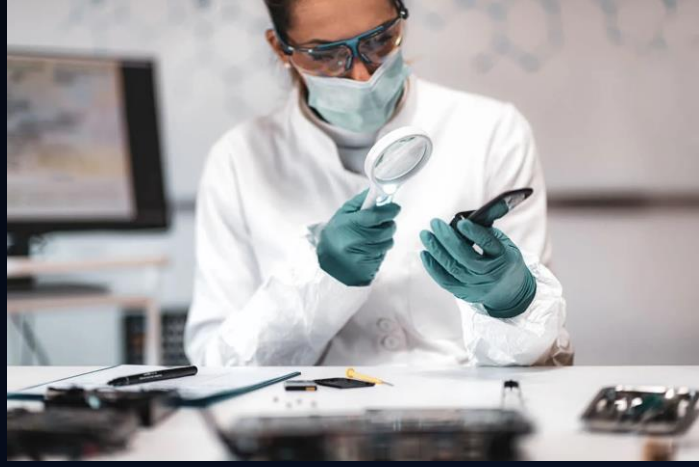
```
query = "SELECT name FROM user where username = '" + username + "' and password = '" + password  + "'";

query = "SELECT name FROM user where username = 'admin' and password = 'admin123' ";

query = "SELECT name FROM user where username = 'any' and password = '123' or '1'='1'";
```

Injected SQL

Forensic Science



- Forensic science, also known as criminalistics, is the application of science to criminal and civil laws.
- During criminal investigation in particular, it is governed by the legal standards of admissible evidence and criminal procedure.
- It is a broad field utilizing numerous practices such as the analysis of DNA, fingerprints, bloodstain patterns, firearms, ballistics, and toxicology.
- Forensic scientists collect, preserve, and analyze scientific evidence during the course of an investigation.
- While some forensic scientists travel to the scene of the crime to collect the evidence themselves, others occupy a laboratory role, performing analysis on objects brought to them by other individuals.
- Still others are involved in analysis of financial, banking, or other numerical data for use in financial crime investigation, and can be employed as consultants from private firms, academia, or as government employees.
- In addition to their laboratory role, forensic scientists testify as expert witnesses in both criminal and civil cases and can work for either the prosecution or the defense.

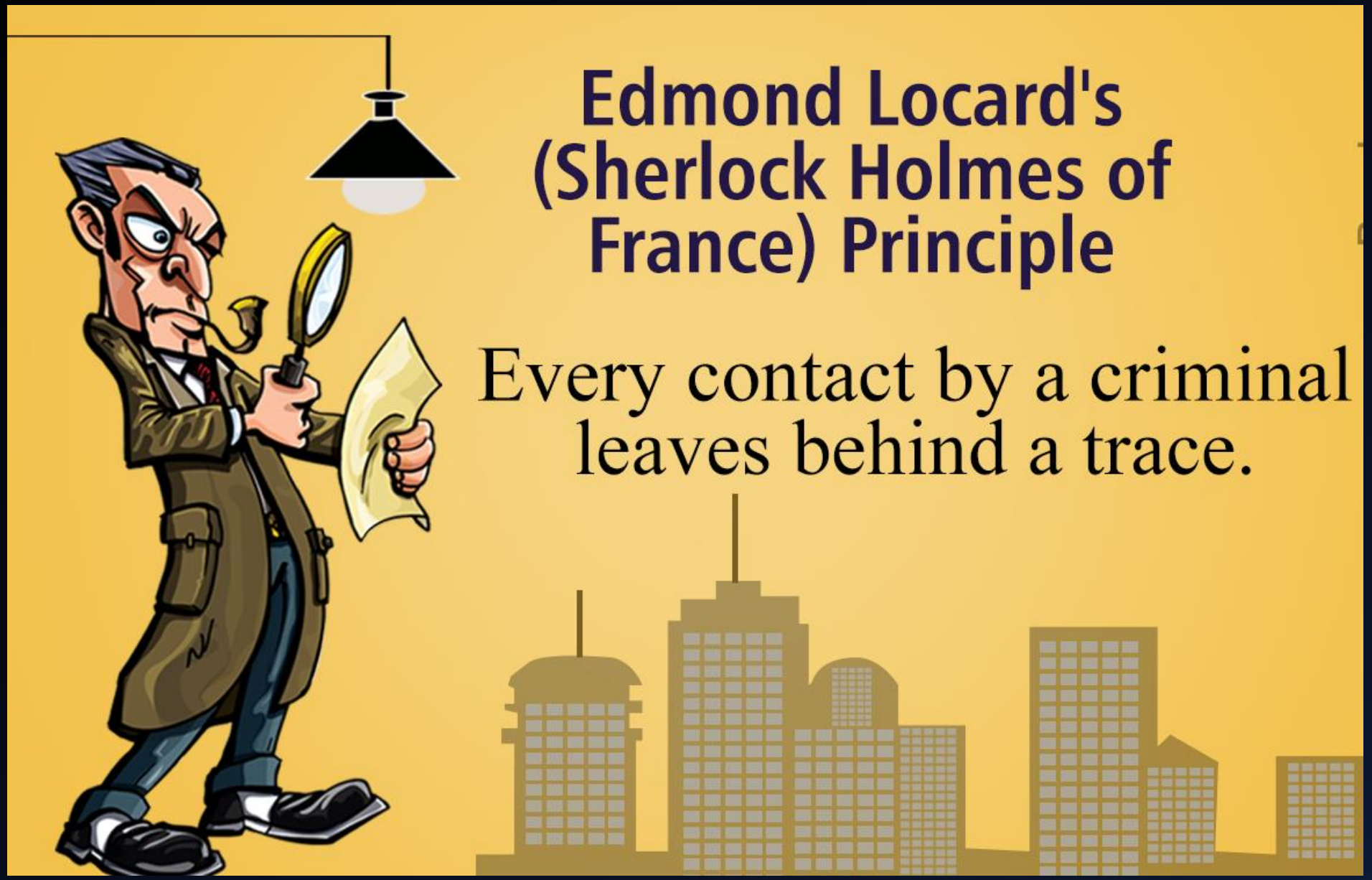
Origins of forensic science and early methods

- The ancient world lacked standardized forensic practices, which enabled criminals to escape punishment.
- Criminal investigations and trials relied heavily on forced confessions and witness testimony.
- However, ancient sources do contain several accounts of techniques that foreshadow concepts in forensic science developed centuries later.

Locard’s Exchange Principle

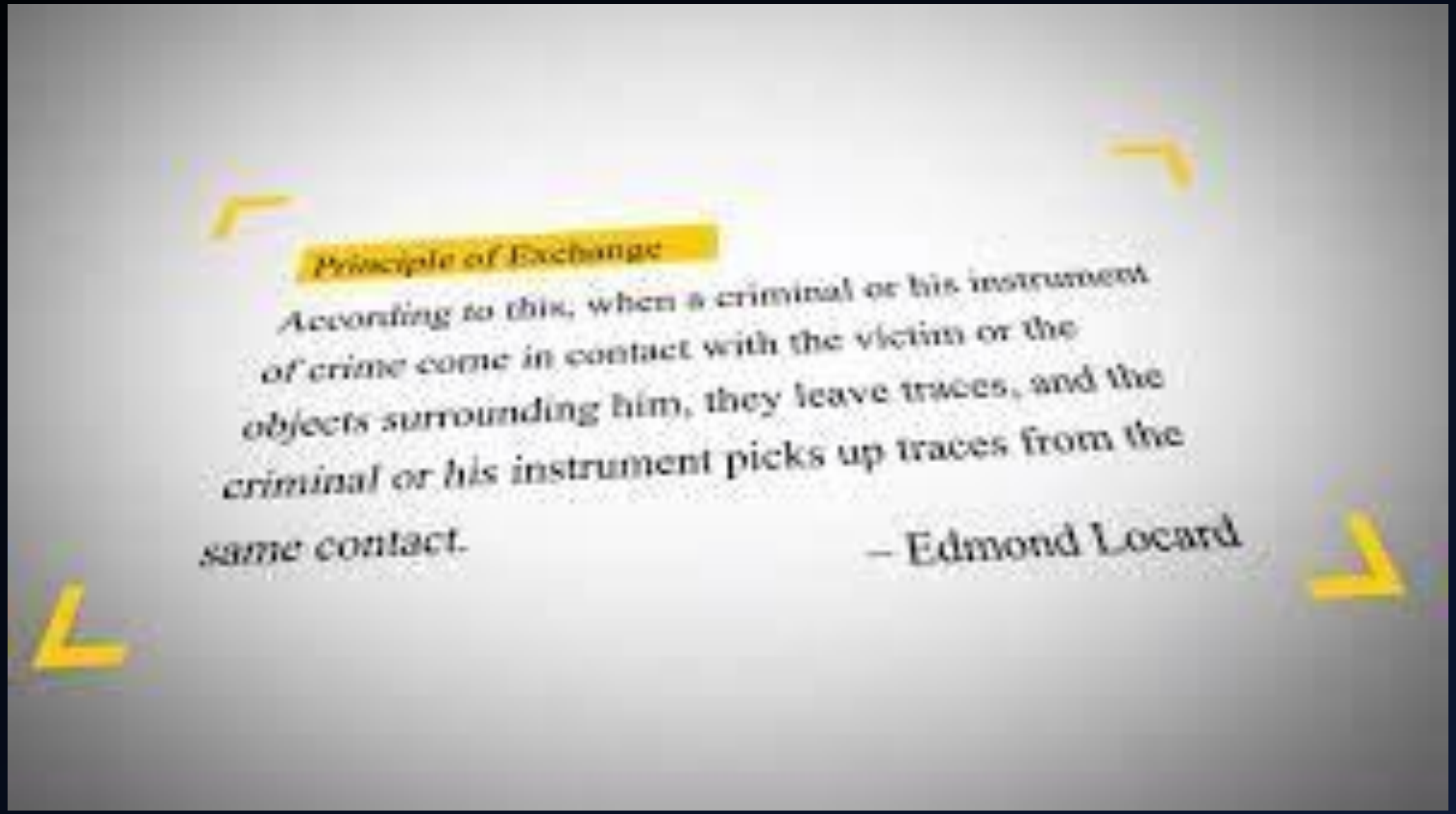
- In forensic science, Locard's principle holds that the perpetrator of a crime will bring something into the crime scene and leave with something from it, and that both can be used as forensic evidence.
- Dr. Edmond Locard (1877–1966) was a pioneer in forensic science who became known as the Sherlock Holmes of Lyon, France.
- He formulated the basic principle of forensic science as: "Every contact leaves a trace".
- It is generally understood as "with contact between two items, there will be an exchange."
- Paul L. Kirk expressed the principle as follows:
  - Wherever he steps, whatever he touches, whatever he leaves, even unconsciously, will serve as a silent witness against him.
  - Not only his fingerprints or his footprints, but his hair, the fibres from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects.
  - All of these and more, bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study and understand it, can diminish its value.

https://sciencestruck.com/locards-exchange-principle-in-forensic-science



- Fragmentary or trace evidence is any type of material left at (or taken from) a crime scene, or the result of contact between two surfaces, such as shoes and the floor covering or soil, or fibres from where someone sat on an upholstered chair.
- When a crime is committed, fragmentary (or trace) evidence needs to be collected from the scene.
- A team of specialised police technicians goes to the scene of the crime and seals it off.
- They record video and take photographs of the crime scene, victim/s (if there are any) and items of evidence.
- If necessary, they undertake ballistics examinations.
- They check for foot, shoe, and tire mark impressions, plus hair as well as examine any vehicles and check for fingerprints – whole or partial.

https://www.facebook.com/evidigators/videos/principle-of-exchange-locards-law/1061852050665075/



What is computer/digital/cyber forensics?

- Cyber forensics is the discovery, analysis, and reconstruction of evidence extracted from any element of Computer systems, Computer networks, Computer media, and Computer peripherals that allow investigators to solve a crime.
- Digital forensics (sometimes known as digital forensic science) is a branch of forensic science encompassing the recovery, investigation, examination, and analysis of material found in digital devices, often in relation to mobile devices and computer crime.
- The term "digital forensics" was originally used as a synonym for computer forensics but has expanded to cover investigation of all devices capable of storing digital data.



Media types used for computer forensic analysis: a Fujifilm FinePix digital camera, two flash memory cards, a USB flash drive, a 5GB iPod, a CD-R or DVD recordable, and a Mini CD.

https://en.wikipedia.org/wiki/File:PersonalStorageDevices.agr.jpg



https://dxhub.calpoly.edu/challenges/digital-evidence/




Menu
Home
Preferences
System
11:59
Search
HEALTH DEPT.: WARNS OF DANGERS RELATED TO FLOODING
1 new message
12:42
13:45
14:59
NICOLAS
Hey Nicolas!
Hey! Whats up? Are you ready for the party?
I'm ready! and you?
Search




10:15
mobile
STOCK EXCHANGE



Nature of Digital Evidence

- Physical Form
- Virtual Locations / Paths
- Volatile vs Non-volatile

Application and Uses



- Digital forensics investigations have a variety of applications.
- The most common is to support or refute a hypothesis before criminal or civil courts.
- Criminal cases involve the alleged breaking of laws that are defined by legislation and enforced by the police and prosecuted by the state, such as murder, theft, and assault against the person.
- Civil cases, on the other hand, deal with protecting the rights and property of individuals (often associated with family disputes), but may also be concerned with contractual disputes between commercial entities where a form of digital forensics referred to as electronic discovery (ediscovery) may be involved.
- Forensics may also feature in the private sector, such as during internal corporate investigations or intrusion investigations (a special probe into the nature and extent of an unauthorized network intrusion).
- As well as identifying direct evidence of a crime, digital forensics can be used to attribute evidence to specific suspects, confirm alibis or statements, determine intent, identify sources (for example, in copyright cases), or authenticate documents.
- Investigations are much broader in scope than other areas of forensic analysis (where the usual aim is to provide answers to a series of simpler questions), often involving complex time-lines or hypotheses.



- Digital forensics is commonly used in both criminal law and private investigation.
- Traditionally it has been associated with criminal law, where evidence is collected to support or oppose a hypothesis before the courts.
- As with other areas of forensics this is often a part of a wider investigation spanning a number of disciplines.
- In some cases, the collected evidence is used as a form of intelligence gathering, used for other purposes than court proceedings (for example to locate, identify or halt other crimes).
- In civil litigation or corporate matters digital forensics forms part of the electronic discovery (or eDiscovery) process.
- Forensic procedures are similar to those used in criminal investigations, often with different legal requirements and limitations.
- Outside of the courts digital forensics can form a part of internal corporate investigations.
- A common example might be following unauthorized network intrusion.
- A specialist forensic examination into the nature and extent of the attack is performed as a damage limitation exercise, both to establish the extent of any intrusion and in an attempt to identify the attacker.

Subdivisions and Branches

- Digital forensics is the application of proven scientific methods and techniques in order to recover data from electronic / digital media. Digital Forensic specialists work in the field as well as in the lab.
- Digital forensics investigation is not restricted to retrieve data merely from the computer, as laws are breached by the criminals and small digital devices (e.g. tablets, smartphones, flash drives) are now extensively used.
- Some of these devices have volatile memory while some have non-volatile memory.
- Sufficient methodologies are available to retrieve data from volatile memory, however, there is lack of detailed methodology or a framework for data retrieval from non-volatile memory sources.
- Also, the technical aspect of an investigation is divided into several sub-branches related to the type of digital devices involved:
  - computer forensics, network forensics, forensic data analysis, and mobile device forensics, router forensics.
- Depending on the type of devices, media or artifacts, digital forensics investigation is branched into various types.

Digital Forensic Categories / Subdivisions / Branches

- Computer Forensics
- Mobile Device Forensics
- Network Forensics [Logs]
- Forensic Data Analysis
- Digital Image Forensics
- Database Forensics
- Cloud Forensics
- IoT Forensics
- Dark Web Forensics
- Audio Analysis/Forensics
- Video Analysis/Forensics
- E-Mail Forensics

- Computer forensics
  - The goal of computer forensics is to explain the current state of a digital artifact; such as a computer system, storage medium or electronic document.
  - The discipline usually covers computers, embedded systems (digital devices with rudimentary computing power and onboard memory) and static memory (such as USB pen drives).
  - Computer forensics can deal with a broad range of information; from logs (such as internet history) through to the actual files on the drive.
  - In 2007 prosecutors used a spreadsheet recovered from the computer of Joseph Edward Duncan to show premeditation and secure the death penalty.
  - Sharon Lopatka's killer was identified in 2006 after email messages from him detailing torture and death fantasies were found on her computer.

- Mobile device forensics
  - Mobile device forensics is a sub-branch of digital forensics relating to recovery of digital evidence or data from a mobile device.
  - Mobile device forensics is the scientific examination and evaluation of evidence found in mobile phones, e.g. Call History and Deleted SMS, and includes SIM Card Forensics.
  - It differs from Computer forensics in that a mobile device will have an inbuilt communication system (e.g. GSM) and, usually, proprietary storage mechanisms.
  - Investigations usually focus on simple data such as call data and communications (SMS/Email) rather than in-depth recovery of deleted data.
  - SMS data from a mobile device investigation helped to exonerate Patrick Lumumba in the murder of Meredith Kercher.
  - Mobile devices are also useful for providing location information; either from inbuilt gps/location tracking or via cell site logs, which track the devices within their range.
  - Such information was used to track down the kidnappers of Thomas Onofri in 2006.

- Network forensics
  - Network forensics is concerned with the monitoring and analysis of computer network traffic, both local and WAN/internet, for the purposes of information gathering, evidence collection, or intrusion detection.
  - Traffic is usually intercepted at the packet level, and either stored for later analysis or filtered in real-time.
  - Unlike other areas of digital forensics network data is often volatile and rarely logged, making the discipline often reactionary.

- Forensic data analysis
  - Forensic Data Analysis is a branch of digital forensics. It examines structured data with the aim to discover and analyze patterns of fraudulent activities resulting from financial crime.
- Digital image forensics
  - Digital image forensics (or forensic image analysis) is a branch of digital forensics that deals with examination and verification of an image's authenticity and content.
  - These can range from Stalin-era airbrushed photos to elaborate deepfake videos.
  - This has broad implications for a wide variety of crimes, for determining the validity of information presented in civil and criminal trials, and for verifying images and information that are circulated through news and social media.
- Forensic video analysis is the scientific examination, comparison and evaluation of video in legal matters.

- Database forensics
  - Database forensics is a branch of digital forensics relating to the forensic study of databases and their metadata.
  - Investigations use database contents, log files and in-RAM data to build a timeline or recover relevant information.
- IoT Forensics
  - IoT forensics is a branch of Digital forensics that has the goal of identifying and extracting digital information from devices belonging to the Internet of things field, to be used for forensics investigations as potential source of evidence.

Digital Forensic Standards & Frameworks

- Since 2000, in response to the need for standardization, various bodies and agencies have published guidelines for digital forensics.

1. The Scientific Working Group on Digital Evidence (SWGDE) produced a 2002 paper, Best practices for Computer Forensics.
2. This was followed, in 2005, by the publication of an ISO standard (ISO 17025, General requirements for the competence of testing and calibration laboratories).
3. NIST

Forensic Lab Setup

- Laws & Regulations
- Types of Incidents
- Important Numbers / Emergency Contacts
- Physical Location
- Team Members & Personnel
- Forensic Expertise
- HVAC & Lighting
- Building Structure
- Tools
  - Hardware
    - Forensic Machines
    - Cables & Connectors
  - Software
  - Write Blocker
  - Duplicator
  - Storage
    - Data & Equipment

Digital Forensic Process

- The typical forensic process encompasses the seizure, forensic imaging (acquisition), and analysis of digital media, followed with the production of a report of the collected evidence.



https://www.uco.edu/programs/microcredentials/digital-evidence

- A digital forensic investigation commonly consists of 3 stages:
  - acquisition or imaging of exhibits, analysis, and reporting.
- Ideally acquisition involves capturing an image of the computer's volatile memory (RAM) and creating an exact sector level duplicate (or "forensic duplicate") of the media, often using a write blocking device to prevent modification of the original.
  - However, the growth in size of storage media and developments such as cloud computing have led to more use of 'live' acquisitions whereby a 'logical' copy of the data is acquired rather than a complete image of the physical storage device.
  - Both acquired image (or logical copy) and original media/data are hashed (using an algorithm such as SHA-1 or MD5) and the values compared to verify the copy is accurate.
- During the analysis phase an investigator recovers evidence material using a number of different methodologies and tools.
  - In 2002, an article in the International Journal of Digital Evidence referred to this step as "an in-depth systematic search of evidence related to the suspected crime."
  - In 2006, forensics researcher Brian Carrier described an "intuitive procedure" in which obvious evidence is first identified and then "exhaustive searches are conducted to start filling in the holes."
  - The actual process of analysis can vary between investigations, but common methodologies include conducting keyword searches across the digital media (within files as well as unallocated and slack space), recovering deleted files and extraction of registry information (for example to list user accounts, or attached USB devices).
  - The evidence recovered is analysed to reconstruct events or actions and to reach conclusions, work that can mostly be performed by specialised staff.
- When an investigation is complete the data is presented, usually in the form of a written report, in lay persons' terms.

DIGITAL FORENSICS

Identification

Where is the evidence? In which country?
Which device(s) does it need to be gathered from?
Is the data "at rest" or "in transit"?



Preservation

How will the data be accessed? Which legislation applies?
Is the action proportionate, lawful, accountable and necessary?

Analysis

Are the required technical and people skills available to acquire, analyse and exploit the evidence in a timely manner with full chain-of-custody?



Documentation

Ensure EVERYTHING is documented to prevent losing evidence due to legal or procedural mistakes



Presentation

Evidence should be presented accurately, concisely and clearly. Can the judge and/or jury understand it?
Can it be tested and challenged by the defence?

An example of an image's Exif metadata that might be used to prove its origin

https://en.wikipedia.org/wiki/File:En_exif_data.png

Camera manufacturer	Canon
Camera model	Canon EOS 400D DIGITAL
Exposure time	1/60 sec (0.016666666666667)
F-number	f/4.5
ISO speed rating	400
Date and time of data generation	11:06, August 27, 2010
Lens focal length	31 mm
Show extended details	

Forensic Report

- Title Page [Case number/title, reporting date, number of pages, examiner name]
- Case Summary
- Evidence Details or Particulars
- Tools Used
- Methodology / Steps
- Forensic Analysis & Findings
- Forensic Investigator/Examiner Signature
- Images of Evidentiary Items
- Chain of Custody

Development of Digital Forensic Tools

- During the 1980s, very few specialized digital forensic tools existed.
- Consequently, investigators often performed live analysis on media, examining computers from within the operating system using existing sysadmin tools to extract evidence.
- This practice carried the risk of modifying data on the disk, either inadvertently or otherwise, which led to claims of evidence tampering.
- A number of tools were created during the early 1990s to address the problem.
- The need for such software was first recognized in 1989 at the Federal Law Enforcement Training Center, resulting in the creation of IMDUMP (by Michael White) and in 1990, SafeBack (developed by Sydex).
- Similar software was developed in other countries; DIBS (a hardware and software solution) was released commercially in the UK in 1991, and Rob McKemmish released Fixed Disk Image free to Australian law enforcement.
- These tools allowed examiners to create an exact copy of a piece of digital media to work on, leaving the original disk intact for verification.
- By the end of the 1990s, as demand for digital evidence grew, more advanced commercial tools such as EnCase and FTK were developed, allowing analysts to examine copies of media without using any live forensics.
- More recently, a trend towards "live memory forensics" has grown, resulting in the availability of tools such as WindowsSCOPE.
- The same progression of tool development has occurred for mobile devices; initially investigators accessed data directly on the device, but soon specialist tools such as Cellebrite, XRY or Radio Tactics Aceso appeared.

https://interworks.com/blog/bstephens/2016/02/05/what-digital-forensics/



Digital Forensic Tools

- Building Structure
- Tools
  - Hardware
    - Forensic Machines
    - Cables & Connectors
  - Software
  - Write Blocker
  - Duplicator
  - Storage
    - Data & Equipment

Mobile phones in an Evidence bag
https://en.wikipedia.org/wiki/File:Mobiles.JPG



A portable Tableau write-blocker attached to a hard drive
https://en.wikipedia.org/wiki/File:Portable_forensic_tableau.JPG



Limitations

- Encryption
  - One major limitation to a forensic investigation is the use of encryption; this disrupts initial examination where pertinent evidence might be located using keywords.
  - Laws to compel individuals to disclose encryption keys are still relatively new and controversial but always more frequently there are solutions to brute force passwords or bypass encryption, such as in smartphones or PCs where by means of bootloader techniques the content of the device can be first acquired and later forced in order to find the password or encryption key.
- Steganography
- Cloud Computing/Forensics
  - Jurisdiction
  - Virtualization
  - Elasticity

Anti-Forensic Techniques

- Passwords
- Encryption
- Jurisdiction
- Proxy Chaining
- Steganography
- NTFS Data Streams

Data hiding

- Data hiding is the process of making data difficult to find while also keeping it accessible for future use.
- "Obfuscation and encryption of data give an adversary the ability to limit identification and collection of evidence by investigators while allowing access and use to themselves."
- Some of the more common forms of data hiding include encryption, steganography and other various forms of hardware/software based data concealment.
- Each of the different data hiding methods makes digital forensic examinations difficult.
- When the different data hiding methods are combined, they can make a successful forensic investigation nearly impossible.
- Encryption
- Steganography
- Other forms of data hiding

Data hiding: Encryption

- One of the more commonly used techniques to defeat computer forensics is data encryption.
- In a presentation given on encryption and anti-forensic methodologies, the Vice President of Secure Computing, Paul Henry, referred to encryption as a "forensic expert's nightmare".
- The majority of publicly available encryption programs allow the user to create virtual encrypted disks which can only be opened with a designated key.
  - Through the use of modern encryption algorithms and various encryption techniques these programs make the data virtually impossible to read without the designated key.
- File level encryption encrypts only the file contents.
  - This leaves important information such as file name, size and timestamps unencrypted.
  - Parts of the content of the file can be reconstructed from other locations, such as temporary files, swap file and deleted, unencrypted copies.
- Most encryption programs have the ability to perform a number of additional functions that make digital forensic efforts increasingly difficult.
  - Some of these functions include the use of a keyfile, full-volume encryption, and plausible deniability.
  - The widespread availability of software containing these functions has put the field of digital forensics at a great disadvantage.

Data hiding: Steganography

- Steganography is a technique where information or files are hidden within another file in an attempt to hide data by leaving it in plain sight.
- "Steganography produces dark data that is typically buried within light data (e.g., a non-perceptible digital watermark buried within a digital photograph).“
- While some experts have argued that the use of steganography techniques is not very widespread and therefore the subject shouldn't be given a lot of thought, most experts agree that steganography has the capability of disrupting the forensic process when used correctly.
- According to Jeffrey Carr, a 2007 edition of Technical Mujahid (a bi-monthly terrorist publication) outlined the importance of using a steganography program called Secrets of the Mujahideen. According to Carr, the program was touted as giving the user the capability to avoid detection by current steganalysis programs. It did this through the use of steganography in conjunction with file compression.

Data hiding: Other forms of data hiding

- Other forms of data hiding involve the use of tools and techniques to hide data throughout various locations in a computer system.
  - Some of these places can include "memory, slack space, hidden directories, bad blocks, alternate data streams, (and) hidden partitions."
- One of the more well known tools that is often used for data hiding is called Slacker (part of the Metasploit framework).
  - Slacker breaks up a file and places each piece of that file into the slack space of other files, thereby hiding it from the forensic examination software.
- Another data hiding technique involves the use of bad sectors.
  - To perform this technique, the user changes a particular sector from good to bad and then data is placed onto that particular cluster.
  - The belief is that forensic examination tools will see these clusters as bad and continue on without any examination of their contents.

Artifact wiping

- The methods used in artifact wiping are tasked with permanently eliminating particular files or entire file systems.
- This can be accomplished through the use of a variety of methods that include disk cleaning utilities, file wiping utilities and disk degaussing/destruction techniques.
- Disk cleaning utilities
- File wiping utilities
- Disk degaussing / destruction techniques

Artifact wiping: Disk cleaning utilities

- Disk cleaning utilities use a variety of methods to overwrite the existing data on disks .
- The effectiveness of disk cleaning utilities as anti-forensic tools is often challenged as some believe they are not completely effective.
- Experts who don't believe that disk cleaning utilities are acceptable for disk sanitization base their opinions of current DOD policy, which states that the only acceptable form of sanitization is degaussing.
- Disk cleaning utilities are also criticized because they leave signatures that the file system was wiped, which in some cases is unacceptable.
- Some of the widely used disk cleaning utilities include DBAN, srm, BCWipe Total WipeOut, KillDisk, PC Inspector and CyberScrubs cyberCide.
- Another option which is approved by the NIST and the NSA is CMRR Secure Erase, which uses the Secure Erase command built into the ATA specification.

Artifact wiping: File wiping utilities

- File wiping utilities are used to delete individual files from an operating system.
- The advantage of file wiping utilities is that they can accomplish their task in a relatively short amount of time as opposed to disk cleaning utilities which take much longer.
- Another advantage of file wiping utilities is that they generally leave a much smaller signature than disk cleaning utilities.
- There are two primary disadvantages of file wiping utilities, first they require user involvement in the process and second some experts believe that file wiping programs don't always correctly and completely wipe file information.
- Some of the widely used file wiping utilities include BCWipe, R-Wipe & Clean, Eraser, Aevita Wipe & Delete and CyberScrubs PrivacySuite.
- On Linux tools like shred and srm can be also used to wipe single files.
- SSDs are by design more difficult to wipe, since the firmware can write to other cells therefore allowing data recovery.
- In these instances ATA Secure Erase should be used on the whole drive, with tools like hdparm that support it.

Artifact wiping: Disk degaussing / destruction techniques

- Disk degaussing is a process by which a magnetic field is applied to a digital media device.
- The result is a device that is entirely clean of any previously stored data.
- Degaussing is rarely used as an anti-forensic method despite the fact that it is an effective means to ensure data has been wiped.
- This is attributed to the high cost of degaussing machines, which are difficult for the average consumer to afford.
- A more commonly used technique to ensure data wiping is the physical destruction of the device.
- The NIST recommends that "physical destruction can be accomplished using a variety of methods, including disintegration, incineration, pulverizing, shredding and melting.

Trail obfuscation

- The purpose of trail obfuscation is to confuse, disorient, and divert the forensic examination process.
- Trail obfuscation covers a variety of techniques and tools that include "log cleaners, spoofing, misinformation, backbone hopping, zombied accounts, trojan commands."
- One of the more widely known trail obfuscation tools is Timestomp (part of the Metasploit Framework).
  - Timestomp gives the user the ability to modify file metadata pertaining to access, creation and modification times/dates.
  - By using programs such as Timestomp, a user can render any number of files useless in a legal setting by directly calling into question the files' credibility.
- Another well known trail-obfuscation program is Transmogrify (also part of the Metasploit Framework).
  - In most file types the header of the file contains identifying information.
  - A (.jpg) would have header information that identifies it as a (.jpg), a (.doc) would have information that identifies it as (.doc) and so on.
  - Transmogrify allows the user to change the header information of a file, so a (.jpg) header could be changed to a (.doc) header.
  - If a forensic examination program or operating system were to conduct a search for images on a machine, it would simply see a (.doc) file and skip over it.

Attacks against computer forensics

- In the past anti-forensic tools have focused on attacking the forensic process by destroying data, hiding data, or altering data usage information.
- Anti-forensics has recently moved into a new realm where tools and techniques are focused on attacking forensic tools that perform the examinations.
- These new anti-forensic methods have benefited from a number of factors to include well documented forensic examination procedures, widely known forensic tool vulnerabilities, and digital forensic examiners' heavy reliance on their tools.
- During a typical forensic examination, the examiner would create an image of the computer's disks.
  - This keeps the original computer (evidence) from being tainted by forensic tools.
  - Hashes are created by the forensic examination software to verify the integrity of the image.
  - One of the recent anti-tool techniques targets the integrity of the hash that is created to verify the image.
  - By affecting the integrity of the hash, any evidence that is collected during the subsequent investigation can be challenged.

Forensic Jobs

- Government, Military, Law Enforcement Agencies
- Private sector companies
- Designations:
  - Forensic Examiner / Specialist / Scientist / Manager
- Relevant Degree, Certifications and Experience



Digital Forensic Certifications

- There are several computer forensics certifications available, such as the ISFCE Certified Computer Examiner, Digital Forensics Investigation Professional (DFIP) and IACRB Certified Computer Forensics Examiner.
- The top vendor independent certification (especially within EU) is considered the CCFP - Certified Cyber Forensics Professional.
- Others, worth to mention for USA or APAC are: The International Association of Computer Investigative Specialists offers the Certified Computer Examiner program. The International Society of Forensic Computer Examiners offers the Certified Computer Examiner program.
- Many commercial based forensic software companies are now also offering proprietary certifications on their products.
  - For example, Guidance Software offering the (EnCE) certification on their tool EnCase, AccessData offering (ACE) certification on their tool FTK, PassMark Software offering certification on their tool OSForensics, and X-Ways Software Technology offering (X-PERT) certification for their software, X-Ways Forensics.
- Tool Specific: EnCase, AccessData FTK, Cellebrite
- General: CHFI (Certified Hacking Forensic Investigator by EC-Council), Mile2, eLearnSecurity, SANS GIAC and many more

DIGITAL FORENSICS

Computer forensics (also known as computer forensic science) is a branch of digital forensic science pertaining to evidence found in computers and digital storage media. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information.

Although it is most often associated with the investigation of a wide variety of computer crime, computer forensics may also be used in civil proceedings. The discipline involves similar techniques and principles to data recovery, but with additional guidelines and practices designed to create a legal audit trail.

Evidence from computer forensics investigations is usually subjected to the same guidelines and practices of other digital evidence. It has been used in a number of high-profile cases and is accepted as reliable within U.S. and European court systems.

Overview

In the early 1980s, personal computers became more accessible to consumers, leading to their increased use in criminal activity (for example, to help commit fraud). At the same time, several new "computer crimes" were recognized (such as cracking). The discipline of computer forensics emerged during this time as a method to recover and investigate digital evidence for use in court. Since then, computer crime and computer-related crime has grown, with the FBI reporting a suspected 791,790 internet crimes alone in 2020, a 69% increase over the amount reported in 2019. Today, computer forensics is used to investigate a wide variety of crime, including child pornography, fraud, espionage, cyberstalking, murder, and rape. The discipline also features in civil proceedings as a form of information gathering (for example, Electronic discovery)

Forensic techniques and expert knowledge are used to explain the current state of a digital artifact, such as a computer system, storage medium (e.g., hard disk or CD-ROM), or an electronic document (e.g., an email message or JPEG image). The scope of a forensic analysis can vary from simple information retrieval to reconstructing a series of events. In a 2002 book, Computer Forensics, authors Kruse and Heiser define computer forensics as involving "the preservation, identification, extraction, documentation and interpretation of computer data". They go on to describe the discipline as "more of an art than a science", indicating that forensic methodology is backed by flexibility and extensive domain knowledge. However, while several methods can be used to extract evidence from a given computer, the strategies used by law enforcement are fairly rigid and lack the flexibility found in the civilian world.

Digital forensics

Digital forensics (sometimes known as digital forensic science) is a branch of forensic science encompassing the recovery, investigation, examination, and analysis of material found in digital devices, often in relation to mobile devices and computer crime. The term "digital forensics" was originally used as a synonym for computer forensics but has expanded to cover investigation of all

devices capable of storing digital data. With roots in the personal computing revolution of the late 1970s and early 1980s, the discipline evolved in a haphazard manner during the 1990s, and it was not until the early 21st century that national policies emerged.

Digital forensics investigations have a variety of applications. The most common is to support or refute a hypothesis before criminal or civil courts. Criminal cases involve the alleged breaking of laws that are defined by legislation and enforced by the police and prosecuted by the state, such as murder, theft, and assault against the person. Civil cases, on the other hand, deal with protecting the rights and property of individuals (often associated with family disputes), but may also be concerned with contractual disputes between commercial entities where a form of digital forensics referred to as electronic discovery (ediscovery) may be involved.

Forensics may also feature in the private sector, such as during internal corporate investigations or intrusion investigations (a special probe into the nature and extent of an unauthorized network intrusion).

The technical aspect of an investigation is divided into several sub-branches related to the type of digital devices involved: computer forensics, network forensics, forensic data analysis, and mobile device forensics. The typical forensic process encompasses the seizure, forensic imaging (acquisition), and analysis of digital media, followed with the production of a report of the collected evidence.

As well as identifying direct evidence of a crime, digital forensics can be used to attribute evidence to specific suspects, confirm alibis or statements, determine intent, identify sources (for example, in copyright cases), or authenticate documents. Investigations are much broader in scope than other areas of forensic analysis (where the usual aim is to provide answers to a series of simpler questions), often involving complex time-lines or hypotheses.

History

Prior to the 1970s, crimes involving computers were dealt with using existing laws. The first computer crimes were recognized in the 1978 Florida Computer Crimes Act, which included legislation against the unauthorized modification or deletion of data on a computer system. Over the next few years, the range of computer crimes being committed increased, and laws were passed to deal with issues of copyright, privacy/harassment (e.g., cyber bullying, happy slapping, cyber stalking, and online predators), and child pornography. It was not until the 1980s that federal laws began to incorporate computer offences. Canada was the first country to pass legislation in 1983. This was followed by the US Federal Computer Fraud and Abuse Act in 1986, Australian amendments to their crimes acts in 1989, and the British Computer Misuse Act in 1990.

1980s–1990s: Growth of the field

The growth in computer crime during the 1980s and 1990s caused law enforcement agencies to begin establishing specialized groups, usually at the national level, to handle the technical aspects of investigations. For example, in 1984, the FBI launched a Computer Analysis and Response Team and the following year a computer crime department was set up within the British Metropolitan Police fraud squad. As well as being law enforcement professionals, many of the early members of these groups were also computer hobbyists and became responsible for the field's initial research and direction.

One of the first practical (or at least publicized) examples of digital forensics was Cliff Stoll's pursuit of hacker Markus Hess in 1986. Stoll, whose investigation made use of computer and network forensic techniques, was not a specialized examiner. Many of the earliest forensic examinations followed the same profile.

Throughout the 1990s, there was high demand for these new, and basic, investigative resources. The strain on central units lead to the creation of regional, and even local, level groups to help handle the load. For example, the British National Hi-Tech Crime Unit was set up in 2001 to provide a national infrastructure for computer crime, with personnel located both centrally in London and with the various regional police forces (the unit was folded into the Serious Organised Crime Agency (SOCA) in 2006).

During this period, the science of digital forensics grew from the ad-hoc tools and techniques developed by these hobbyist practitioners. This is in contrast to other forensics disciplines, which developed from work by the scientific community. It was not until 1992 that the term "computer forensics" was used in academic literature (although prior to this, it had been in informal use); a paper by Collier and Spaul attempted to justify this new discipline to the forensic science world. This swift development resulted in a lack of standardization and training. In his 1995 book, High-Technology Crime: Investigating Cases Involving Computers, K. Rosenblatt wrote the following:

Seizing, preserving, and analyzing evidence stored on a computer is the greatest forensic challenge facing law enforcement in the 1990s. Although most forensic tests, such as fingerprinting and DNA testing, are performed by specially trained experts the task of collecting and analyzing computer evidence is often assigned to patrol officers and detectives.

2000s: Developing standards

Since 2000, in response to the need for standardization, various bodies and agencies have published guidelines for digital forensics. The Scientific Working Group on Digital Evidence (SWGDE) produced a 2002 paper, Best practices for Computer Forensics, this was followed, in 2005, by the publication of an ISO standard (ISO 17025, General requirements for the competence of testing and calibration laboratories). A European-led international treaty, the Convention on Cybercrime, came into force in 2004 with the aim of reconciling national computer crime laws, investigative techniques, and international co-operation. The treaty has been signed by 43 nations (including the US, Canada, Japan, South Africa, UK, and other European nations) and ratified by 16.

The issue of training also received attention. Commercial companies (often forensic software developers) began to offer certification programs, and digital forensic analysis was included as a topic at the UK specialist investigator training facility, Centrex.

In the late 1990s, mobile devices became more widely available, advancing beyond simple communication devices, and were found to be rich forms of information, even for crime not traditionally associated with digital forensics. Despite this, digital analysis of phones has lagged behind traditional computer media, largely due to problems over the proprietary nature of devices.

Focus has also shifted onto internet crime, particularly the risk of cyber warfare and cyberterrorism. A February 2010 report by the United States Joint Forces Command concluded the following:

Through cyberspace, enemies will target industry, academia, government, as well as the military in the air, land, maritime, and space domains. In much the same way that airpower transformed the

battlefield of World War II, cyberspace has fractured the physical barriers that shield a nation from attacks on its commerce and communication.

The field of digital forensics still faces unresolved issues. A 2009 paper, "Digital Forensic Research: The Good, the Bad and the Unaddressed" by Peterson and Shenoi, identified a bias towards Windows operating systems in digital forensics research. In 2010, Simson Garfinkel identified issues facing digital investigations in the future, including the increasing size of digital media, the wide availability of encryption to consumers, a growing variety of operating systems and file formats, an increasing number of individuals owning multiple devices, and legal limitations on investigators. The paper also identified continued training issues, as well as the prohibitively high cost of entering the field.

Development of forensic tools

During the 1980s, very few specialized digital forensic tools existed. Consequently, investigators often performed live analysis on media, examining computers from within the operating system using existing sysadmin tools to extract evidence. This practice carried the risk of modifying data on the disk, either inadvertently or otherwise, which led to claims of evidence tampering. A number of tools were created during the early 1990s to address the problem.

The need for such software was first recognized in 1989 at the Federal Law Enforcement Training Center, resulting in the creation of IMDUMP (by Michael White) and in 1990, SafeBack (developed by Sydex). Similar software was developed in other countries; DIBS (a hardware and software solution) was released commercially in the UK in 1991, and Rob McKemmish released Fixed Disk Image free to Australian law enforcement. These tools allowed examiners to create an exact copy of a piece of digital media to work on, leaving the original disk intact for verification. By the end of the 1990s, as demand for digital evidence grew, more advanced commercial tools such as EnCase and FTK were developed, allowing analysts to examine copies of media without using any live forensics. More recently, a trend towards "live memory forensics" has grown, resulting in the availability of tools such as WindowsSCOPE.

More recently, the same progression of tool development has occurred for mobile devices; initially investigators accessed data directly on the device, but soon specialist tools such as XRY or Radio Tactics Aceso appeared.

Cybersecurity

Computer forensics is often confused with cybersecurity. Cybersecurity is about prevention and protection, while computer forensics is more reactionary and active, involving activities such as tracking and exposing. System security usually encompasses two teams, cybersecurity and computer forensics, which work together. A cybersecurity team creates systems and programs to protect data; if these fail, then the computer forensics team recovers the data and performs the investigation into the intrusion and theft. Both areas require knowledge of computer science.

Computer-related crimes

Computer forensics are used to convict those involved in physical and digital crimes. Some of these computer-related crimes include interruption, interception, copyright infringement, and fabrication. Interruption relates to the destruction and stealing of computer parts and digital files. Interception is the unauthorized access of files and information stored on technological devices. Copyright Infringement is using, reproducing, and distributing copyrighted information, including software piracy. Fabrication is accusing someone of using false data and information put in the system through an unauthorized source. Examples of interceptions are the Bank NSP case, Sony.Sambandh.com case, and business email compromise scams.

Use as evidence

In court, computer forensic evidence is subject to the usual requirements for digital evidence. This requires that information be authentic, reliably obtained, and admissible. Different countries have specific guidelines and practices for evidence recovery. In the United Kingdom, examiners often follow Association of Chief Police Officers guidelines that help ensure the authenticity and integrity of evidence. While voluntary, the guidelines are widely accepted in British courts.

Computer forensics has been used as evidence in criminal law since the mid-1980s, some notable examples include:

- BTK Killer: Dennis Rader was convicted of a string of serial killings that occurred over a period of sixteen years. Towards the end of this period, Rader sent letters to the police on a floppy disk. Metadata within the documents implicated an author named "Dennis" at "Christ Lutheran Church"; this evidence helped lead to Rader's arrest.
- Joseph Edward Duncan: A spreadsheet recovered from Duncan's computer contained evidence that showed him planning his crimes. Prosecutors used this to show premeditation and secure the death penalty.
- Sharon Lopatka: Hundreds of emails on Lopatka's computer lead investigators to her killer, Robert Glass.
- Corcoran Group: This case confirmed parties' duties to preserve digital evidence when litigation has commenced or is reasonably anticipated. Hard drives were analyzed by a computer forensics expert who could not find relevant emails the Defendants should have had. Though the expert found no evidence of deletion on the hard drives, evidence came out that the defendants were found to have intentionally destroyed emails, and misled and failed to disclose material facts to the plaintiffs and the court.
- Dr. Conrad Murray: Dr. Conrad Murray, the doctor of the deceased Michael Jackson, was convicted partially by digital evidence on his computer. This evidence included medical documentation showing lethal amounts of propofol.

Forensic process

Computer forensic investigations usually follow the standard digital forensic process or phases: acquisition, examination, analysis, and reporting. Investigations are performed on static data (i.e. acquired images) rather than "live" systems. This is a change from early forensic practices where a lack of specialist tools led to investigators commonly working on live data.

Forensic process

A digital forensic investigation commonly consists of 3 stages: acquisition or imaging of exhibits, analysis, and reporting. Ideally acquisition involves capturing an image of the computer's volatile memory (RAM) and creating an exact sector level duplicate (or "forensic duplicate") of the media, often using a write blocking device to prevent modification of the original. However, the growth in size of storage media and developments such as cloud computing have led to more use of 'live' acquisitions whereby a 'logical' copy of the data is acquired rather than a complete image of the physical storage device. Both acquired image (or logical copy) and original media/data are hashed (using an algorithm such as SHA-1 or MD5) and the values compared to verify the copy is accurate.

An alternative (and patented) approach (that has been dubbed 'hybrid forensics' or 'distributed forensics') combines digital forensics and ediscovery processes. This approach has been embodied in a commercial tool called ISEEK that was presented together with test results at a conference in 2017.

During the analysis phase an investigator recovers evidence material using a number of different methodologies and tools. In 2002, an article in the International Journal of Digital Evidence referred to this step as "an in-depth systematic search of evidence related to the suspected crime." In 2006, forensics researcher Brian Carrier described an "intuitive procedure" in which obvious evidence is first identified and then "exhaustive searches are conducted to start filling in the holes."

The actual process of analysis can vary between investigations, but common methodologies include conducting keyword searches across the digital media (within files as well as unallocated and slack space), recovering deleted files and extraction of registry information (for example to list user accounts, or attached USB devices).

The evidence recovered is analysed to reconstruct events or actions and to reach conclusions, work that can often be performed by less specialised staff. When an investigation is complete the data is presented, usually in the form of a written report, in lay persons' terms.

Application

Digital forensics is commonly used in both criminal law and private investigation. Traditionally it has been associated with criminal law, where evidence is collected to support or oppose a hypothesis before the courts. As with other areas of forensics this is often a part of a wider investigation spanning a number of disciplines. In some cases, the collected evidence is used as a form of intelligence gathering, used for other purposes than court proceedings (for example to locate, identify or halt other crimes). As a result, intelligence gathering is sometimes held to a less strict forensic standard.

In civil litigation or corporate matters digital forensics forms part of the electronic discovery (or eDiscovery) process. Forensic procedures are similar to those used in criminal investigations, often

with different legal requirements and limitations. Outside of the courts digital forensics can form a part of internal corporate investigations.

A common example might be following unauthorized network intrusion. A specialist forensic examination into the nature and extent of the attack is performed as a damage limitation exercise, both to establish the extent of any intrusion and in an attempt to identify the attacker. Such attacks were commonly conducted over phone lines during the 1980s, but in the modern era are usually propagated over the Internet.

The main focus of digital forensics investigations is to recover objective evidence of a criminal activity (termed actus reus in legal parlance). However, the diverse range of data held in digital devices can help with other areas of inquiry.

- **Attribution**
- Meta data and other logs can be used to attribute actions to an individual. For example, personal documents on a computer drive might identify its owner.
- **Alibis and statements**
- Information provided by those involved can be cross checked with digital evidence. For example, during the investigation into the Soham murders the offender's alibi was disproved when mobile phone records of the person he claimed to be with showed she was out of town at the time.
- **Intent**
- As well as finding objective evidence of a crime being committed, investigations can also be used to prove the intent (known by the legal term mens rea). For example, the Internet history of convicted killer Neil Entwistle included references to a site discussing How to kill people.
- **Evaluation of source**
- File artifacts and meta-data can be used to identify the origin of a particular piece of data; for example, older versions of Microsoft Word embedded a Global Unique Identifier into files which identified the computer it had been created on. Proving whether a file was produced on the digital device being examined or obtained from elsewhere (e.g., the Internet) can be very important.
- **Document authentication**
- Related to "Evaluation of source," meta data associated with digital documents can be easily modified (for example, by changing the computer clock you can affect the creation date of a file). Document authentication relates to detecting and identifying falsification of such details.

Limitations

One major limitation to a forensic investigation is the use of encryption; this disrupts initial examination where pertinent evidence might be located using keywords. Laws to compel individuals to disclose encryption keys are still relatively new and controversial. but always more frequently there are solutions to brute force passwords or bypass encryption, such as in smartphones or PCs where by means of bootloader techniques the content of the device can be first acquired and later forced in order to find the password or encryption key.

Legal considerations

The examination of digital media is covered by national and international legislation. For civil investigations, in particular, laws may restrict the abilities of analysts to undertake examinations. Restrictions against network monitoring, or reading of personal communications often exist. During criminal investigation, national laws restrict how much information can be seized. For example, in the United Kingdom seizure of evidence by law enforcement is governed by the PACE act. During its existence early in the field, the "International Organization on Computer Evidence" (IOCE) was one agency that worked to establish compatible international standards for the seizure of evidence.

In the UK the same laws covering computer crime can also affect forensic investigators. The 1990 Computer Misuse Act legislates against unauthorised access to computer material; this is a particular concern for civil investigators who have more limitations than law enforcement.

An individual's right to privacy is one area of digital forensics which is still largely undecided by courts. The US Electronic Communications Privacy Act places limitations on the ability of law enforcement or civil investigators to intercept and access evidence. The act makes a distinction between stored communication (e.g. email archives) and transmitted communication (such as VOIP). The latter, being considered more of a privacy invasion, is harder to obtain a warrant for. The ECPA also affects the ability of companies to investigate the computers and communications of their employees, an aspect that is still under debate as to the extent to which a company can perform such monitoring.

Article 5 of the European Convention on Human Rights asserts similar privacy limitations to the ECPA and limits the processing and sharing of personal data both within the EU and with external countries. The ability of UK law enforcement to conduct digital forensics investigations is legislated by the Regulation of Investigatory Powers Act.

Digital evidence

When used in a court of law digital evidence falls under the same legal guidelines as other forms of evidence; courts do not usually require more stringent guidelines. In the United States the Federal Rules of Evidence are used to evaluate the admissibility of digital evidence, the United Kingdom PACE and Civil Evidence acts have similar guidelines and many other countries have their own laws. US federal laws restrict seizures to items with only obvious evidential value. This is acknowledged as not always being possible to establish with digital media prior to an examination.

Laws dealing with digital evidence are concerned with two issues: integrity and authenticity. Integrity is ensuring that the act of seizing and acquiring digital media does not modify the evidence (either the original or the copy). Authenticity refers to the ability to confirm the integrity of information; for example that the imaged media matches the original evidence. The ease with which digital media can be modified means that documenting the chain of custody from the crime scene, through analysis and, ultimately, to the court, (a form of audit trail) is important to establish the authenticity of evidence.

Attorneys have argued that because digital evidence can theoretically be altered it undermines the reliability of the evidence. US judges are beginning to reject this theory, in the case US v. Bonallo the court ruled that "the fact that it is possible to alter data contained in a computer is plainly insufficient to establish untrustworthiness." In the United Kingdom guidelines such as those issued by ACPO are followed to help document the authenticity and integrity of evidence.

Digital investigators, particularly in criminal investigations, have to ensure that conclusions are based upon factual evidence and their own expert knowledge. In the US, for example, Federal Rules of Evidence state that a qualified expert may testify “in the form of an opinion or otherwise” so long as:

(1) the testimony is based upon sufficient facts or data,

(2) the testimony is the product of reliable principles and methods, and

(3) the witness has applied the principles and methods reliably to the facts of the case.

The sub-branches of digital forensics may each have their own specific guidelines for the conduct of investigations and the handling of evidence. For example, mobile phones may be required to be placed in a Faraday shield during seizure or acquisition to prevent further radio traffic to the device. In the UK forensic examination of computers in criminal matters is subject to ACPO guidelines. There are also international approaches to providing guidance on how to handle electronic evidence. The "Electronic Evidence Guide" by the Council of Europe offers a framework for law enforcement and judicial authorities in countries who seek to set up or enhance their own guidelines for the identification and handling of electronic evidence.

Investigative tools

The admissibility of digital evidence relies on the tools used to extract it. In the US, forensic tools are subjected to the Daubert standard, where the judge is responsible for ensuring that the processes and software used were acceptable. In a 2003 paper Brian Carrier argued that the Daubert guidelines required the code of forensic tools to be published and peer reviewed. He concluded that "open source tools may more clearly and comprehensively meet the guideline requirements than would closed source tools." In 2011 Josh Brunty stated that the scientific validation of the technology and software associated with performing a digital forensic examination is critical to any laboratory process. He argued that "the science of digital forensics is founded on the principles of repeatable processes and quality evidence therefore knowing how to design and properly maintain a good validation process is a key requirement for any digital forensic examiner to defend their methods in court." "

Computer forensics lab

The computer forensic lab is a safe and protected zone where electronic data can be managed, preserved, and accessed in a controlled environment. There, there is a very much reduced risk of damage or modification to the evidence. Computer forensic examiners have the resources needed to elicit meaningful data from the devices that they are examining.

Techniques

A number of techniques are used during computer forensics investigations, and these include the following:

- Cross-drive analysis

    - This is a forensic technique that correlates information found on multiple hard drives, and has been used to identify social networks and perform anomaly detection.
- Live analysis
    - The examination of computers from within the operating system using custom forensics or existing sysadmin tools to extract evidence. The practice is useful when dealing with Encrypting File Systems, for example, where the encryption keys may be collected and, in some instances, the logical hard drive volume may be imaged (known as a live acquisition) before the computer is shut down.
- Deleted files
    - A common technique used in computer forensics is the recovery of deleted files. Modern forensic software have their own tools for recovering or carving out deleted data. Most operating systems and file systems do not always erase physical file data, allowing investigators to reconstruct it from the physical disk sectors. File carving involves searching for known file headers within the disk image and reconstructing deleted materials.
- Stochastic forensics
    - A method which uses stochastic properties of the computer system to investigate activities lacking digital artifacts. Its chief use is to investigate data theft.
- Steganography
    - One of the techniques used to hide data is via steganography, the process of hiding data inside of a picture or digital image. An example would be to hide pornographic images of children or other information that a given criminal does not want to have discovered. Computer forensics professionals can fight this by looking at the hash of the file and comparing it to the original image (if available.) While the images appear identical upon visual inspection, the hash changes as the data changes.

Mobile device forensics

- **Phone Logs**: Phone companies usually keep logs of calls received, which can be helpful when creating timelines and gathering the locations of persons when the crime occurred.
- **Contacts**: Contact lists help narrow down the suspect pool due to their connections with the victim or suspect.
- **Text messages**: Messages contain timestamps and remain in company servers indefinitely, even if deleted on the original device. Because of this, messages act as crucial records of communication that can be used to convict suspects.
- **Photos**: Photos can be critical in either supporting or disproving alibis by displaying a location or scene along with a timestamp of when the photo was taken.
- **Audio Recordings**: Some victims might have been able to record pivotal moments of the struggle, like the voice of their attacker or extensive context of the situation.

Branches

Digital forensics investigation is not restricted to retrieve data merely from the computer, as laws are breached by the criminals and small digital devices (e.g. tablets, smartphones, flash drives) are now extensively used. Some of these devices have volatile memory while some have non-volatile memory.

Sufficient methodologies are available to retrieve data from volatile memory, however, there is lack of detailed methodology or a framework for data retrieval from non-volatile memory sources. Depending on the type of devices, media or artifacts, digital forensics investigation is branched into various types.

- **Computer forensics**
- The goal of computer forensics is to explain the current state of a digital artifact; such as a computer system, storage medium or electronic document. The discipline usually covers computers, embedded systems (digital devices with rudimentary computing power and onboard memory) and static memory (such as USB pen drives).
- Computer forensics can deal with a broad range of information; from logs (such as internet history) through to the actual files on the drive. In 2007 prosecutors used a spreadsheet recovered from the computer of Joseph Edward Duncan to show premeditation and secure the death penalty. Sharon Lopatka's killer was identified in 2006 after email messages from him detailing torture and death fantasies were found on her computer.

- **Mobile device forensics**
- Mobile device forensics is a sub-branch of digital forensics relating to recovery of digital evidence or data from a mobile device. It differs from Computer forensics in that a mobile device will have an inbuilt communication system (e.g. GSM) and, usually, proprietary storage mechanisms. Investigations usually focus on simple data such as call data and communications (SMS/Email) rather than in-depth recovery of deleted data. SMS data from a mobile device investigation helped to exonerate Patrick Lumumba in the murder of Meredith Kercher.
- Mobile devices are also useful for providing location information; either from inbuilt gps/location tracking or via cell site logs, which track the devices within their range. Such information was used to track down the kidnappers of Thomas Onofri in 2006.

- **Network forensics**
- Network forensics is concerned with the monitoring and analysis of computer network traffic, both local and WAN/internet, for the purposes of information gathering, evidence collection, or intrusion detection. Traffic is usually intercepted at the packet level, and either stored for later analysis or filtered in real-time. Unlike other areas of digital forensics network data is often volatile and rarely logged, making the discipline often reactionary.
- In 2000 the FBI lured computer hackers Aleksey Ivanov and Gorshkov to the United States for a fake job interview. By monitoring network traffic from the pair's computers, the FBI identified passwords allowing them to collect evidence directly from Russian-based computers.

- **Forensic data analysis**
- Forensic Data Analysis is a branch of digital forensics. It examines structured data with the aim to discover and analyze patterns of fraudulent activities resulting from financial crime.

- **Digital image forensics**
- Digital image forensics (or forensic image analysis) is a branch of digital forensics that deals with examination and verification of an image's authenticity and content. These can range from Stalin-era airbrushed photos to elaborate deepfake videos. This has broad implications for a wide variety of crimes, for determining the validity of information presented in civil and criminal trials, and for verifying images and information that are circulated through news and social media.

- **Database forensics**
- Database forensics is a branch of digital forensics relating to the forensic study of databases and their metadata. Investigations use database contents, log files and in-RAM data to build a timeline or recover relevant information.

- **IoT Forensics**
- IoT forensics is a branch of Digital forensics that has the goal of identifying and extracting digital information from devices belonging to the Internet of things field, to be used for forensics investigations as potential source of evidence.

Volatile data

Volatile data is any data that is stored in memory, or exists in transit, that will be lost when the computer loses power or is turned off. Volatile data resides in registries, cache, and random access memory (RAM). The investigation of this volatile data is called “live forensics”.

When seizing evidence, if the machine is still active, any information stored solely in RAM that is not recovered before powering down may be lost. One application of "live analysis" is to recover RAM data (for example, using Microsoft's COFEE tool, WinDD, WindowsSCOPE) prior to removing an exhibit. CaptureGUARD Gateway bypasses Windows login for locked computers, allowing for the analysis and acquisition of physical memory on a locked computer.

RAM can be analyzed for prior content after power loss, because the electrical charge stored in the memory cells takes time to dissipate, an effect exploited by the cold boot attack. The length of time that data is recoverable is increased by low temperatures and higher cell voltages. Holding unpowered RAM below −60 °C helps preserve residual data by an order of magnitude, improving the chances of successful recovery. However, it can be impractical to do this during a field examination.

Some of the tools needed to extract volatile data, however, require that a computer be in a forensic lab, both to maintain a legitimate chain of evidence, and to facilitate work on the machine. If necessary, law enforcement applies techniques to move a live, running desktop computer. These include a mouse jiggler, which moves the mouse rapidly in small movements and prevents the computer from going to sleep accidentally. Usually, an uninterruptible power supply (UPS) provides power during transit.

However, one of the easiest ways to capture data is by actually saving the RAM data to disk. Various file systems that have journaling features such as NTFS and ReiserFS keep a large portion of the RAM

data on the main storage media during operation, and these page files can be reassembled to reconstruct what was in RAM at that time.

Analysis tools

A number of open source and commercial tools exist for computer forensics investigation. Typical forensic analysis includes a manual review of material on the media, reviewing the Windows registry for suspect information, discovering and cracking passwords, keyword searches for topics related to the crime, and extracting e-mail and pictures for review. Autopsy (software), Belkasoft Evidence Center, COFEE, EnCase are the some of tools used in Digital forensics.

Jobs in computer forensics

Digital forensics analyst

A digital forensics analyst is responsible for preserving digital evidence, cataloging collected evidence, analyzing evidence in a manner relevant to the ongoing case, responding to cyber breaches (usually in a corporate context), writing reports containing findings, and testifying in court. A digital forensic analyst may alternatively be referred to as a computer forensic analyst, digital forensic examiner, cyber forensic analyst, forensic technician, or other similarly named titles, although these roles perform the same duties.

Certifications

There are several computer forensics certifications available, such as the ISFCE Certified Computer Examiner, Digital Forensics Investigation Professional (DFIP) and IACRB Certified Computer Forensics Examiner.

The top vendor independent certification (especially within EU) is considered the CCFP - Certified Cyber Forensics Professional.

Others, worth to mention for USA or APAC are: The International Association of Computer Investigative Specialists offers the Certified Computer Examiner program.

The International Society of Forensic Computer Examiners offers the Certified Computer Examiner program.

Many commercial based forensic software companies are now also offering proprietary certifications on their products. For example, Guidance Software offering the (EnCE) certification on their tool EnCase, AccessData offering (ACE) certification on their tool FTK, PassMark Software offering certification on their tool OSForensics, and X-Ways Software Technology offering (X-PERT) certification for their software, X-Ways Forensics.

Anti–computer forensics

Anti–computer forensics or counter-forensics are techniques used to obstruct forensic analysis.

Definition

Anti-forensics has only recently been recognized as a legitimate field of study.

One of the more widely known and accepted definitions comes from Marc Rogers of One of the earliest detailed presentations of anti-forensics, in Phrack Magazine in 2002, defines anti-forensics as "the removal, or hiding, of evidence in an attempt to mitigate the effectiveness of a forensics investigation".

A more abbreviated definition is given by Scott Berinato in his article entitled, The Rise of Anti-Forensics. "Anti-forensics is more than technology. It is an approach to criminal hacking that can be summed up like this: Make it hard for them to find you and impossible for them to prove they found you." Neither author takes into account using anti-forensics methods to ensure the privacy of one's personal data.

Sub-categories

Anti-forensics methods are often broken down into several sub-categories to make classification of the various tools and techniques simpler. One of the more widely accepted subcategory breakdowns was developed by Dr. Marcus Rogers. He has proposed the following sub-categories: data hiding, artifact wiping, trail obfuscation and attacks against the CF (computer forensics) processes and tools. Attacks against forensics tools directly has also been called counter-forensics.

Purpose and goals

Within the field of digital forensics there is much debate over the purpose and goals of anti-forensic methods. The conventional wisdom is that anti-forensic tools are purely malicious in intent and design. Others believe that these tools should be used to illustrate deficiencies in digital forensic procedures, digital forensic tools, and forensic examiner education. This sentiment was echoed at the 2005 Blackhat Conference by anti-forensic tool authors, James Foster and Vinnie Liu. They stated that by exposing these issues, forensic investigators will have to work harder to prove that collected evidence is both accurate and dependable. They believe that this will result in better tools and education for the forensic examiner. Also, counter-forensics has significance for defence against espionage, as recovering information by forensic tools serves the goals of spies equally as well as investigators.

Data hiding

Data hiding is the process of making data difficult to find while also keeping it accessible for future use. "Obfuscation and encryption of data give an adversary the ability to limit identification and collection of evidence by investigators while allowing access and use to themselves."

Some of the more common forms of data hiding include encryption, steganography and other various forms of hardware/software based data concealment. Each of the different data hiding methods makes digital forensic examinations difficult. When the different data hiding methods are combined, they can make a successful forensic investigation nearly impossible.

Encryption

One of the more commonly used techniques to defeat computer forensics is data encryption. In a presentation given on encryption and anti-forensic methodologies, the Vice President of Secure Computing, Paul Henry, referred to encryption as a "forensic expert's nightmare".

The majority of publicly available encryption programs allow the user to create virtual encrypted disks which can only be opened with a designated key. Through the use of modern encryption algorithms and various encryption techniques these programs make the data virtually impossible to read without the designated key.

File level encryption encrypts only the file contents. This leaves important information such as file name, size and timestamps unencrypted. Parts of the content of the file can be reconstructed from other locations, such as temporary files, swap file and deleted, unencrypted copies.

Most encryption programs have the ability to perform a number of additional functions that make digital forensic efforts increasingly difficult. Some of these functions include the use of a keyfile, full-volume encryption, and plausible deniability. The widespread availability of software containing these functions has put the field of digital forensics at a great disadvantage.

Steganography

Steganography is a technique where information or files are hidden within another file in an attempt to hide data by leaving it in plain sight. "Steganography produces dark data that is typically buried within light data (e.g., a non-perceptible digital watermark buried within a digital photograph)."While some experts have argued that the use of steganography techniques is not very widespread and therefore the subject shouldn't be given a lot of thought, most experts agree that steganography has the capability of disrupting the forensic process when used correctly.

According to Jeffrey Carr, a 2007 edition of Technical Mujahid (a bi-monthly terrorist publication) outlined the importance of using a steganography program called Secrets of the Mujahideen. According to Carr, the program was touted as giving the user the capability to avoid detection by current steganalysis programs. It did this through the use of steganography in conjunction with file compression.

Other forms of data hiding

Other forms of data hiding involve the use of tools and techniques to hide data throughout various locations in a computer system. Some of these places can include "memory, slack space, hidden directories, bad blocks, alternate data streams, (and) hidden partitions."

One of the more well known tools that is often used for data hiding is called Slacker (part of the Metasploit framework). Slacker breaks up a file and places each piece of that file into the slack space of other files, thereby hiding it from the forensic examination software. Another data hiding technique involves the use of bad sectors. To perform this technique, the user changes a particular sector from good to bad and then data is placed onto that particular cluster. The belief is that forensic examination tools will see these clusters as bad and continue on without any examination of their contents.

Artifact wiping

The methods used in artifact wiping are tasked with permanently eliminating particular files or entire file systems. This can be accomplished through the use of a variety of methods that include disk cleaning utilities, file wiping utilities and disk degaussing/destruction techniques.

Disk cleaning utilities

Disk cleaning utilities use a variety of methods to overwrite the existing data on disks. The effectiveness of disk cleaning utilities as anti-forensic tools is often challenged as some believe they are not completely effective. Experts who don't believe that disk cleaning utilities are acceptable for disk sanitization base their opinions of current DOD policy, which states that the only acceptable form of sanitization is degaussing. Disk cleaning utilities are also criticized because they leave signatures that the file system was wiped, which in some cases is unacceptable. Some of the widely used disk cleaning utilities include DBAN, srm, BCWipe Total WipeOut, KillDisk, PC Inspector and CyberScrubs cyberCide. Another option which is approved by the NIST and the NSA is CMRR Secure Erase, which uses the Secure Erase command built into the ATA specification.

File wiping utilities

File wiping utilities are used to delete individual files from an operating system. The advantage of file wiping utilities is that they can accomplish their task in a relatively short amount of time as opposed to disk cleaning utilities which take much longer. Another advantage of file wiping utilities is that they generally leave a much smaller signature than disk cleaning utilities. There are two primary disadvantages of file wiping utilities, first they require user involvement in the process and second some experts believe that file wiping programs don't always correctly and completely wipe file information. Some of the widely used file wiping utilities include BCWipe, R-Wipe & Clean, Eraser, Aevita Wipe & Delete and CyberScrubs PrivacySuite. On Linux tools like shred and srm can be also used to wipe single files. SSDs are by design more difficult to wipe, since the firmware can write to other cells therefore allowing data recovery. In these instances ATA Secure Erase should be used on the whole drive, with tools like hdparm that support it.

Disk degaussing / destruction techniques

Disk degaussing is a process by which a magnetic field is applied to a digital media device. The result is a device that is entirely clean of any previously stored data. Degaussing is rarely used as an anti-forensic method despite the fact that it is an effective means to ensure data has been wiped. This is attributed to the high cost of degaussing machines, which are difficult for the average consumer to afford.

A more commonly used technique to ensure data wiping is the physical destruction of the device. The NIST recommends that "physical destruction can be accomplished using a variety of methods, including disintegration, incineration, pulverizing, shredding and melting."

Trail obfuscation

The purpose of trail obfuscation is to confuse, disorient, and divert the forensic examination process. Trail obfuscation covers a variety of techniques and tools that include "log cleaners, spoofing, misinformation, backbone hopping, zombied accounts, trojan commands."

One of the more widely known trail obfuscation tools is Timestomp (part of the Metasploit Framework). Timestomp gives the user the ability to modify file metadata pertaining to access, creation and modification times/dates. By using programs such as Timestomp, a user can render any number of files useless in a legal setting by directly calling into question the files' credibility.

Another well known trail-obfuscation program is Transmogrify (also part of the Metasploit Framework). In most file types the header of the file contains identifying information. A (.jpg) would have header information that identifies it as a (.jpg), a (.doc) would have information that identifies it as (.doc) and so on. Transmogrify allows the user to change the header information of a file, so a (.jpg) header could be changed to a (.doc) header. If a forensic examination program or operating system were to conduct a search for images on a machine, it would simply see a (.doc) file and skip over it.

Attacks against computer forensics

In the past anti-forensic tools have focused on attacking the forensic process by destroying data, hiding data, or altering data usage information. Anti-forensics has recently moved into a new realm where tools and techniques are focused on attacking forensic tools that perform the examinations. These new anti-forensic methods have benefited from a number of factors to include well documented forensic examination procedures, widely known forensic tool vulnerabilities, and digital forensic examiners' heavy reliance on their tools.

During a typical forensic examination, the examiner would create an image of the computer's disks. This keeps the original computer (evidence) from being tainted by forensic tools. Hashes are created by the forensic examination software to verify the integrity of the image. One of the recent anti-tool techniques targets the integrity of the hash that is created to verify the image. By affecting the integrity of the hash, any evidence that is collected during the subsequent investigation can be challenged.

Physical

To prevent physical access to data while the computer is powered on (from a grab-and-go theft for instance, as well as seizure from Law Enforcement), there are different solutions that could be implemented:

- Software frameworks like USBGuard or USBKill implements USB authorization policies and method of use policies. If the software is triggered, by insertion or removal of USB devices, a specific action can be performed. After the arrest of Silk Road's administrator Ross Ulbricht, a number of proof of concept anti-forensic tools have been created to detect seizing of the computer from the owner to shut it down, therefore making the data inaccessible if full disk encryption is used.
- Hardware cable anchors using the Kensington Security Slot to prevent stealing by opportunistic thieves.
- Hardware kill cables like BusKill that lock, shutdown, or wipe data when ejected

- Use of chassis intrusion detection feature in computer case or a sensor (such as a photodetector) rigged with explosives for self-destruction. In some jurisdictions this method could be illegal since it could seriously maim or kill an unauthorized user and could consist in destruction of evidence.
- Battery could be removed from a laptop to make it work only while attached to the power supply unit. If the cable is removed, shutdown of the computer will occur immediately causing data loss. In the event of a power surge the same will occur though.

Some of these methods rely on shutting the computer down, while the data might be retained in the RAM from a couple of seconds up to a couple minutes, theoretically allowing for a cold boot attack. Cryogenically freezing the RAM might extend this time even further and some attacks on the wild have been spotted. Methods to counteract this attack exist and can overwrite the memory before shutting down. Some anti-forensic tools even detect the temperature of the RAM to perform a shutdown when below a certain threshold.

Attempts to create a tamper-resistant desktop computer has been made (as of 2020, the ORWL model is one of the best examples). However, security of this particular model is debated by security researcher and Qubes OS founder Joanna Rutkowska.

Use by criminals

While the study and applications of anti-forensics are generally available to protect users from forensic attacks of their confidential data by their adversaries (eg investigative journalists, human rights defenders, activists, corporate or government espionage), Mac Rogers of Purdue University notes that anti-forensics tools can also be used by criminals.

Rogers uses a more traditional "crime scene" approach when defining anti-forensics. "Attempts to negatively affect the existence, amount and/or quality of evidence from a crime scene, or make the analysis and examination of evidence difficult or impossible to conduct."

Effectiveness of anti-forensics

Anti-forensic methods rely on several weaknesses in the forensic process including: the human element, dependency on tools, and the physical/logical limitations of computers. By reducing the forensic process's susceptibility to these weaknesses, an examiner can reduce the likelihood of anti-forensic methods successfully impacting an investigation. This may be accomplished by providing increased training for investigators, and corroborating results using multiple tools.

FTPS (File Transfer Protocol Secure)

Ensuring Secure and Reliable File Transfers

Introduction to FTPS

- FTPS is a secure file transfer protocol that combines the traditional FTP protocol with the security features of SSL/TLS encryption.
- It provides a secure and reliable method for transferring files over a network, ensuring data integrity and confidentiality.
- FTPS is widely used in various industries, including banking, healthcare, and e-commerce, where secure file transfers are crucial.



How FTPS Works?

- FTPS utilizes SSL/TLS encryption to secure the communication between the client and the server.
- SSL/TLS establishes a secure and encrypted connection, preventing unauthorized access and eavesdropping.
- FTPS supports both implicit and explicit modes, offering flexibility in choosing the level of security required.

FTPS working



Key Features of FTPS

- **Encryption**: FTPS uses SSL/TLS encryption to protect data during transit, safeguarding it from interception and tampering.
- **Authentication**: FTPS provides strong authentication mechanisms, ensuring that only authorized users can access and transfer files.
- **Data Integrity**: Through SSL/TLS, FTPS guarantees the integrity of transferred files, detecting any unauthorized modifications.
- **Portability**: FTPS is supported by various operating systems and FTP client software, making it widely compatible and accessible.

Benefits of Using FTPS

Enhanced Security: FTPS offers a higher level of security compared to standard FTP, making it suitable for sensitive data transfers.

Compliance with Regulations: FTPS helps organizations meet regulatory requirements for data protection, such as HIPAA and GDPR.

Reliability: FTPS ensures the reliable delivery of files, minimizing errors and interruptions during transfers.

Flexibility: With implicit and explicit modes, FTPS allows organizations to choose the level of security that best suits their needs.

Use Cases for FTPS

- **Banking and Finance**: FTPS enables secure transfer of financial data, such as transactions, statements, and sensitive customer information.
- **Healthcare**: FTPS is used for transferring confidential patient records, medical images, and other sensitive healthcare data.
- **E-commerce**: FTPS ensures secure exchange of product information, inventory updates, and customer data between online retailers and suppliers.







Best Practices for FTPS Implementation

1. **Use Strong Authentication**: Implement strong username/password combinations or consider additional authentication methods like certificates.
2. **Regularly Update SSL/TLS Certificates**: Keep SSL/TLS certificates up to date to maintain the security of the FTPS server.
3. **Employ Access Controls**: Restrict FTPS access to authorized users and employ granular permissions to limit access to specific files and directories.
4. **Monitor and Audit**: Implement logging and monitoring mechanisms to track FTPS activities and detect any suspicious or unauthorized actions.

Conclusion

- FTPS is a secure and reliable file transfer protocol that combines the benefits of FTP with SSL/TLS encryption.
- By implementing FTPS, organizations can ensure the confidentiality, integrity, and secure transfer of sensitive data.
- With its wide compatibility and industry adoption, FTPS remains a trusted solution for secure file transfers in various sectors.

HTTPS (Hypertext Transfer Protocol Secure)
Securing Web Communication

Introduction to HTTPS

- HTTPS (Hypertext Transfer Protocol Secure) is a secure version of the HTTP protocol used for communication between web browsers and web servers.
- HTTPS adds an extra layer of security by encrypting data exchanged between the client and server, ensuring confidentiality and integrity.



How HTTPS Works

HTTPS utilizes the SSL/TLS (Secure Sockets Layer/Transport Layer Security) protocol to establish a secure connection:

Client Request: The client (web browser) initiates a request to the server using the HTTPS protocol.

Server Response: The server responds by presenting its SSL/TLS certificate to the client.

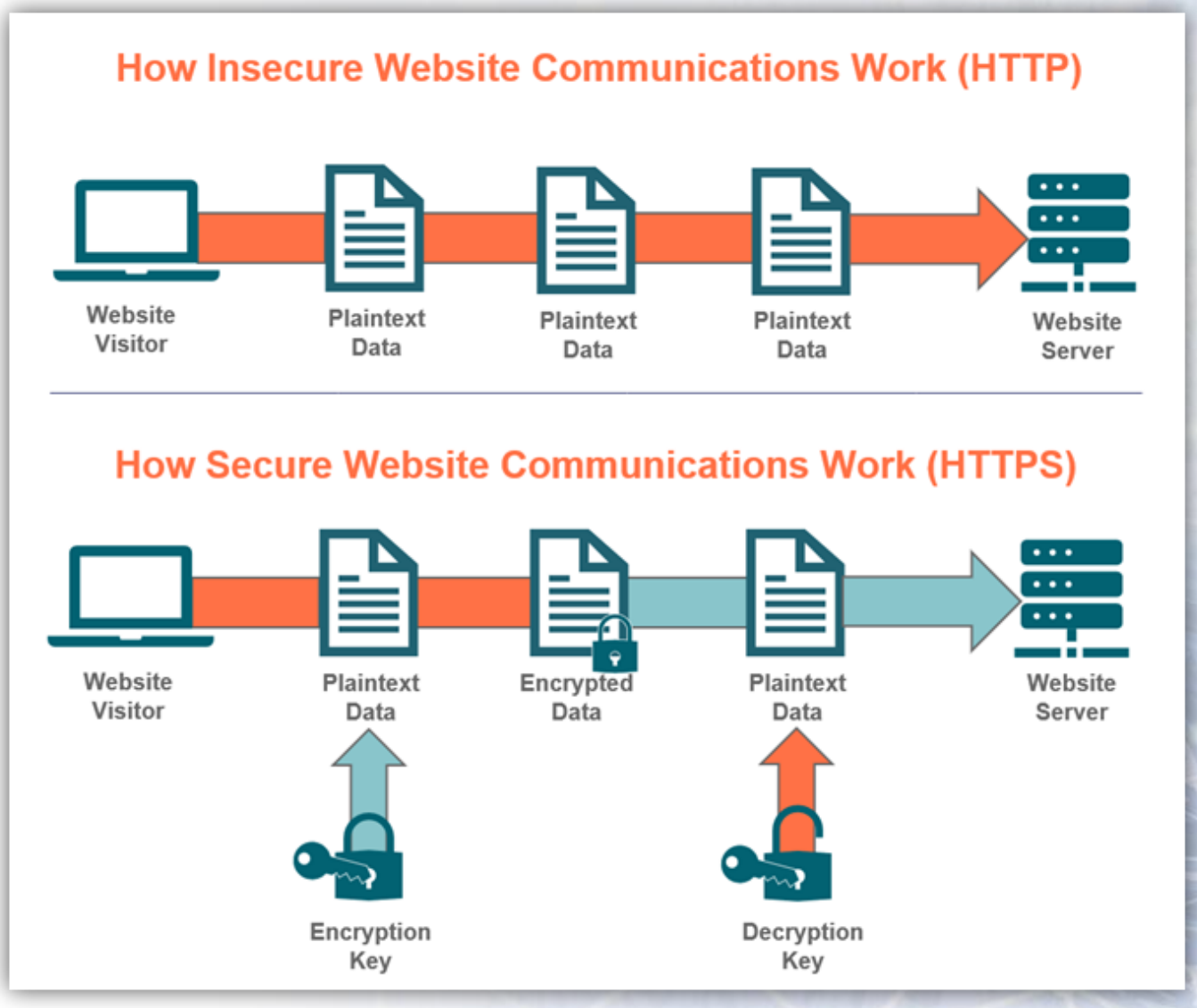
Certificate Verification: The client verifies the authenticity of the server's certificate using trusted Certificate Authorities (CAs).

Secure Connection: Once the certificate is validated, a secure connection is established, and data exchange occurs over an encrypted channel.

Encryption and Decryption: The client and server encrypt and decrypt data using symmetric encryption algorithms and a shared session key.

Secure Data Transfer: All subsequent data exchanged between the client and server remains encrypted, protecting it from eavesdropping and tampering.

HTTPS Working



Benefits of HTTPS

HTTPS offers numerous benefits for secure web communication:

- **Data Confidentiality**: HTTPS encrypts sensitive information, such as passwords, credit card details, and personal data, preventing unauthorized access.
- **Data Integrity**: HTTPS ensures that data remains intact during transmission, detecting any modifications or tampering attempts.
- **Authentication**: HTTPS verifies the identity of the server through SSL/TLS certificates, preventing impersonation or man-in-the-middle attacks.
- **Trust and User Confidence**: Displaying the padlock symbol and "https" in the URL instills trust in users and reassures them about the security of the website.
- **SEO Benefits**: Search engines consider HTTPS as a ranking signal, incentivizing website owners to implement HTTPS for improved search engine visibility.

Implementing HTTPS

Steps to implement HTTPS on a website:

1. Obtain an SSL/TLS certificate from a trusted Certificate Authority (CA).
2. Install the SSL/TLS certificate on the web server.
3. Configure the server to redirect HTTP traffic to HTTPS.
4. Ensure all web content (images, scripts, stylesheets, etc.) is loaded securely using HTTPS.
5. Test the HTTPS implementation to verify proper functioning and resolve any issues.

HTTPS Best Practices

Best practices for implementing and maintaining HTTPS:

- Use the latest version of the SSL/TLS protocol supported by your infrastructure.
- Enable strong cipher suites and prioritize secure encryption algorithms.
- Implement HTTP Strict Transport Security (HSTS) to enforce HTTPS usage and prevent downgrade attacks.
- Regularly renew and update SSL/TLS certificates to prevent expiration or revocation.
- Perform security audits and vulnerability scans to identify and address any weaknesses in the HTTPS configuration.

Conclusion

- HTTPS is a crucial technology for securing web communication and protecting sensitive information.
- It ensures data confidentiality, integrity, and authenticity, building trust with users and search engines.
- By implementing HTTPS correctly and following best practices, organizations can enhance the security of their websites and safeguard user data.

IPsec (Internet Protocol Security) - Securing Network Communications

Introduction to IPsec

- IPsec (Internet Protocol Security) is a suite of protocols and cryptographic techniques used to secure network communications at the IP layer.
- It provides a robust framework for ensuring the confidentiality, integrity, and authenticity of IP packets transmitted over a network.

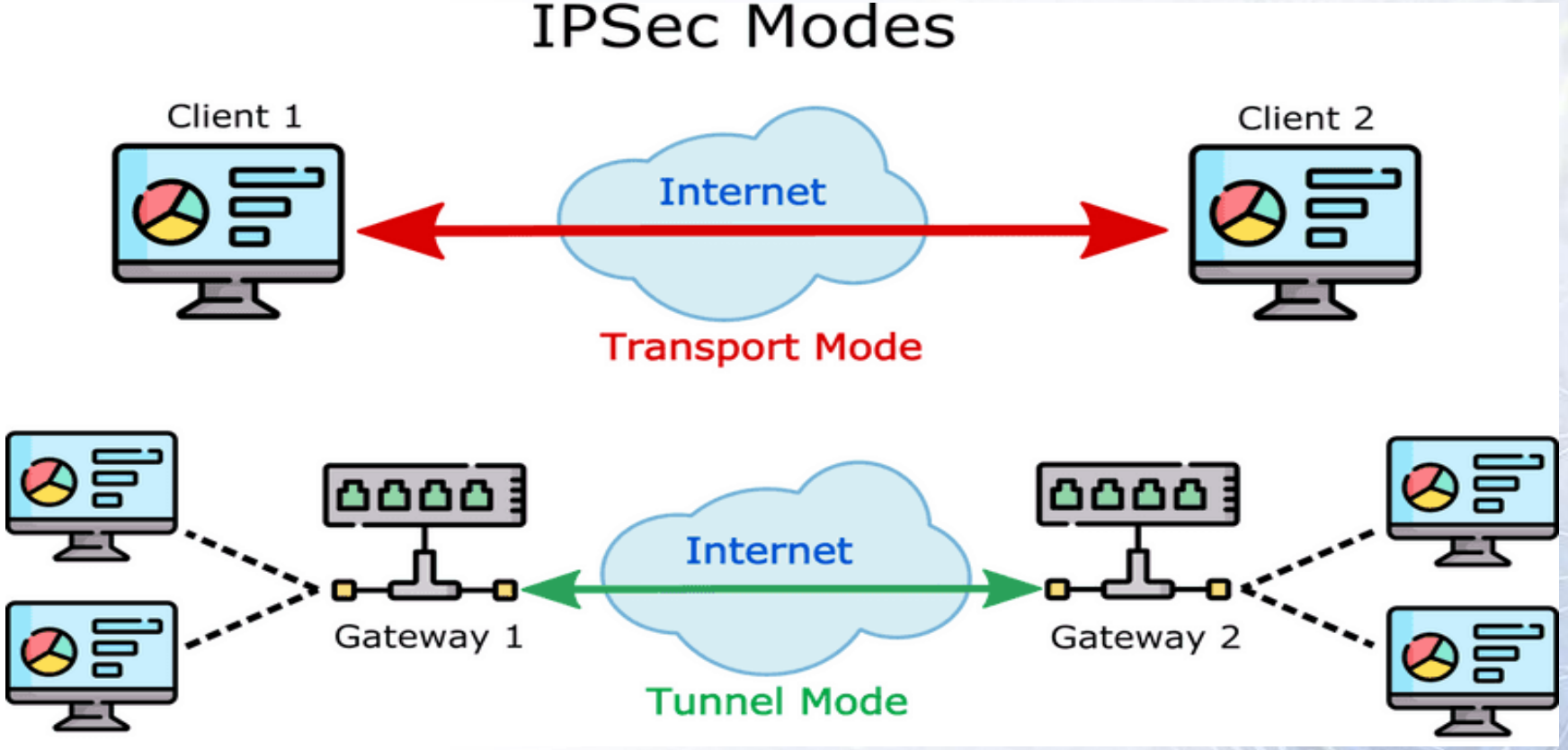


How IPsec Works?

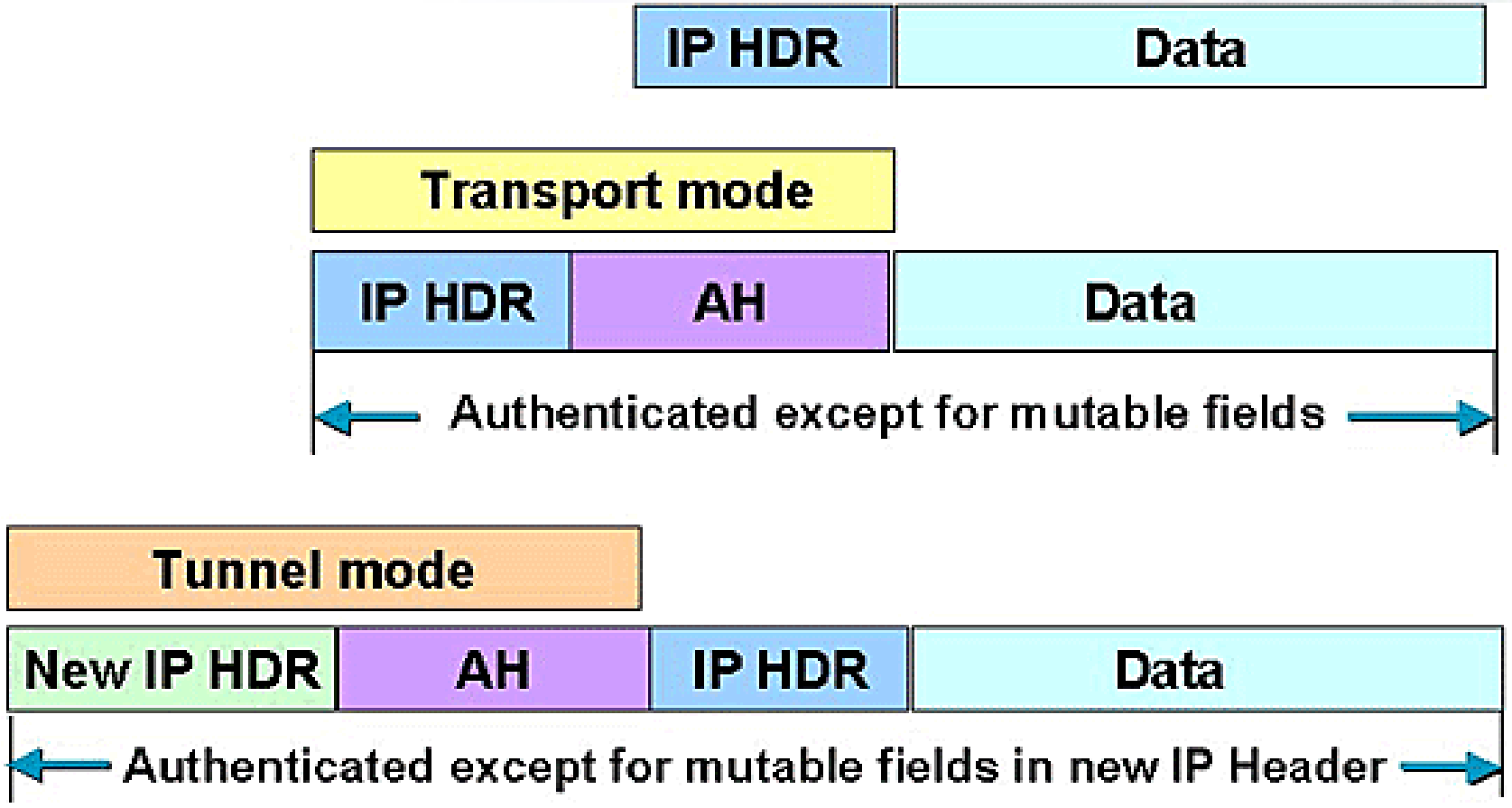
IPsec operates in two main modes: Transport mode and Tunnel mode:

1. **Transport Mode**: Protects the data payload of IP packets, leaving the original IP header intact. It is typically used for end-to-end communication within a network.
2. **Tunnel Mode**: Encrypts the entire IP packet, including the original IP header, and encapsulates it within a new IP packet. It is often used for secure communication between networks.

IPsec Working



IPsec Modes

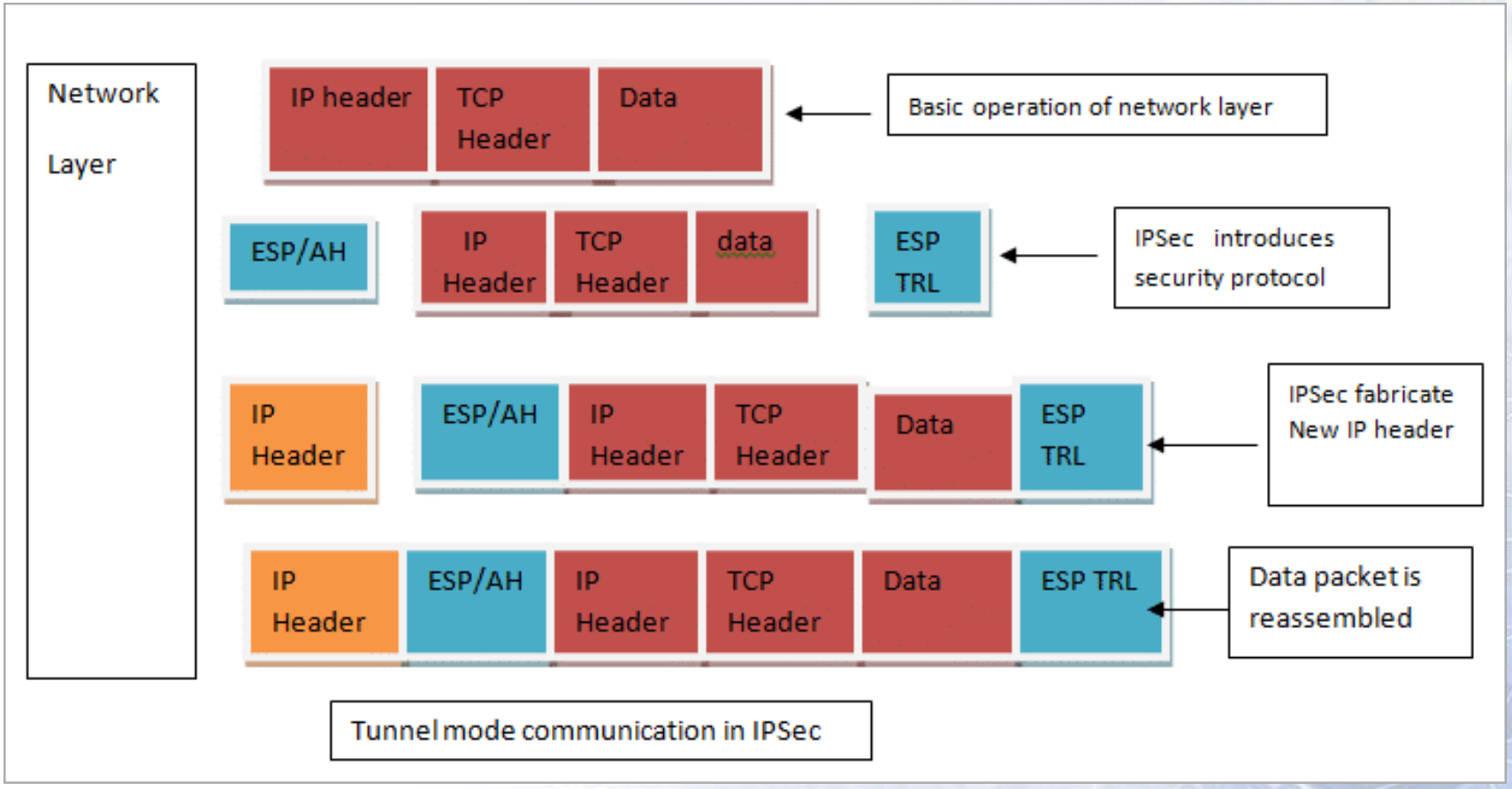

IP HDR
Data
Transport mode
IP HDR
AH
Data
Authenticated except for mutable fields
Tunnel mode
New IP HDR
AH
IP HDR
Data
Authenticated except for mutable fields in new IP Header

Components of IPsec

IPsec consists of several key components:

1. **Authentication Header (AH)**: Provides data integrity and authentication of IP packets.
2. **Encapsulating Security Payload (ESP)**: Offers data confidentiality, integrity, and authentication through encryption and encapsulation.
3. **Security Associations (SA)**: Establishes the security parameters, including encryption algorithms, authentication methods, and key management, between two communicating entities.
4. **Key Management**: Involves the secure exchange, generation, and management of cryptographic keys used by IPsec for encryption and authentication.

Tunnel Mode Detail



Benefits of IPsec

IPsec offers numerous advantages for securing network communications:

1. **Confidentiality**: Encrypts IP packets, preventing unauthorized access and eavesdropping of sensitive data.
2. **Integrity**: Verifies the integrity of IP packets, ensuring they have not been tampered with during transit.
3. **Authentication**: Authenticates the source of IP packets, preventing spoofing and unauthorized access.
4. **Seamless Integration**: IPsec can be implemented at the network layer, providing security for all applications and protocols that use IP.
5. **Interoperability**: IPsec is a widely supported standard, allowing secure communication between different vendors and platforms.

IPsec Implementation

Steps to implement IPsec in a network:

1. **Assess Network Requirements**: Determine the specific security needs and objectives of the network.
2. **Plan IPsec Policy**: Define security policies, including encryption algorithms, authentication methods, and key management approaches.
3. **Configure IPsec Devices**: Configure IPsec parameters on network devices, such as routers, firewalls, or VPN concentrators, based on the defined policies.
4. **Test and Monitor**: Perform thorough testing to ensure IPsec is functioning correctly and continuously monitor the network for any potential issues or vulnerabilities.

Conclusion

- IPsec is a powerful security protocol suite that protects network communications at the IP layer, ensuring confidentiality, integrity, and authenticity.
- By implementing IPsec correctly and following best practices, organizations can secure their network infrastructure and protect sensitive data from unauthorized access.

SHTTPS (Secure Hypertext Transfer Protocol Secure) - Strengthening Web Security

Introduction to SHTTPS

- SHTTPS (Secure Hypertext Transfer Protocol Secure) is an enhanced version of HTTPS that integrates additional security measures.
- It combines the secure communication features of HTTPS with additional mechanisms to protect against various web security threats.



Why SHTTPS?

- Traditional HTTPS provides secure communication between clients and servers, but SHTTPS further strengthens web security by addressing specific vulnerabilities and attacks.
- SHTTPS aims to mitigate risks related to website tampering, data integrity, and man-in-the-middle attacks.

Key Features of SHTTPS

SHTTPS incorporates the following key features to enhance web security:

- **Subresource Integrity (SRI):**
  - SRI ensures that external resources, such as scripts and stylesheets, loaded by a webpage are not tampered with during transit.
  - It uses cryptographic hashes to verify the integrity of the resources, allowing the browser to block or warn if any modifications are detected.

- **Certificate Transparency (CT):**
  - CT is a framework that provides public auditing and monitoring of SSL/TLS certificates issued by Certificate Authorities (CAs).
  - It aims to detect and mitigate misissued or fraudulent certificates, enhancing trust and accountability in the certificate ecosystem.

- **HTTP Public Key Pinning (HPKP):**
  - HPKP allows website operators to specify a list of cryptographic hashes of their SSL/TLS public keys in the HTTP response header.
  - This helps protect against rogue or compromised CAs by instructing the browser to only accept specific public keys for future connections to the website.

Benefits of SHTTPS

SHTTPS offers several advantages for web security:

- **Enhanced Protection:** SHTTPS strengthens the overall security of websites by addressing specific vulnerabilities and threats.
- **Tamper Detection:** SRI helps ensure the integrity of external resources and prevents unauthorized modifications.
- **Certificate Accountability:** CT provides transparency and oversight of SSL/TLS certificates, reducing the risk of misissued or fraudulent certificates.
- **Key Validation:** HPKP allows website operators to enforce the use of specific public keys, protecting against compromised or unauthorized certificates.
- **User Trust:** Implementing SHTTPS demonstrates a commitment to web security, enhancing user confidence and trust in the website.

Implementing SHTTPS

Steps to implement SHTTPS on a website:

- **Enable HTTPS:** Ensure that your website is already using HTTPS for secure communication.
- **Subresource Integrity (SRI):** Implement SRI by adding integrity attributes to external resource references (e.g., script and stylesheet tags) in your web pages.
- **Certificate Transparency (CT):** Utilize CT logs and monitoring services to track and validate SSL/TLS certificates issued for your website.
- **HTTP Public Key Pinning (HPKP):** Carefully consider the implications of HPKP, as it requires careful management of public keys and potential risks associated with pinning.

Conclusion

- SHTTPS is an advanced approach to web security, integrating additional measures to strengthen HTTPS and protect against specific vulnerabilities.
- By implementing SHTTPS and leveraging its features, website owners can enhance the integrity, trustworthiness, and overall security of their web presence.

SSH (Secure Shell) - Secure Remote Access and File Transfer

Introduction to SSH

- SSH (Secure Shell) is a cryptographic network protocol that provides secure remote access and file transfer between two systems.
- It offers a secure alternative to traditional remote access protocols like Telnet and FTP.
- SSH ensures the confidentiality, integrity, and authenticity of data exchanged between client and server.

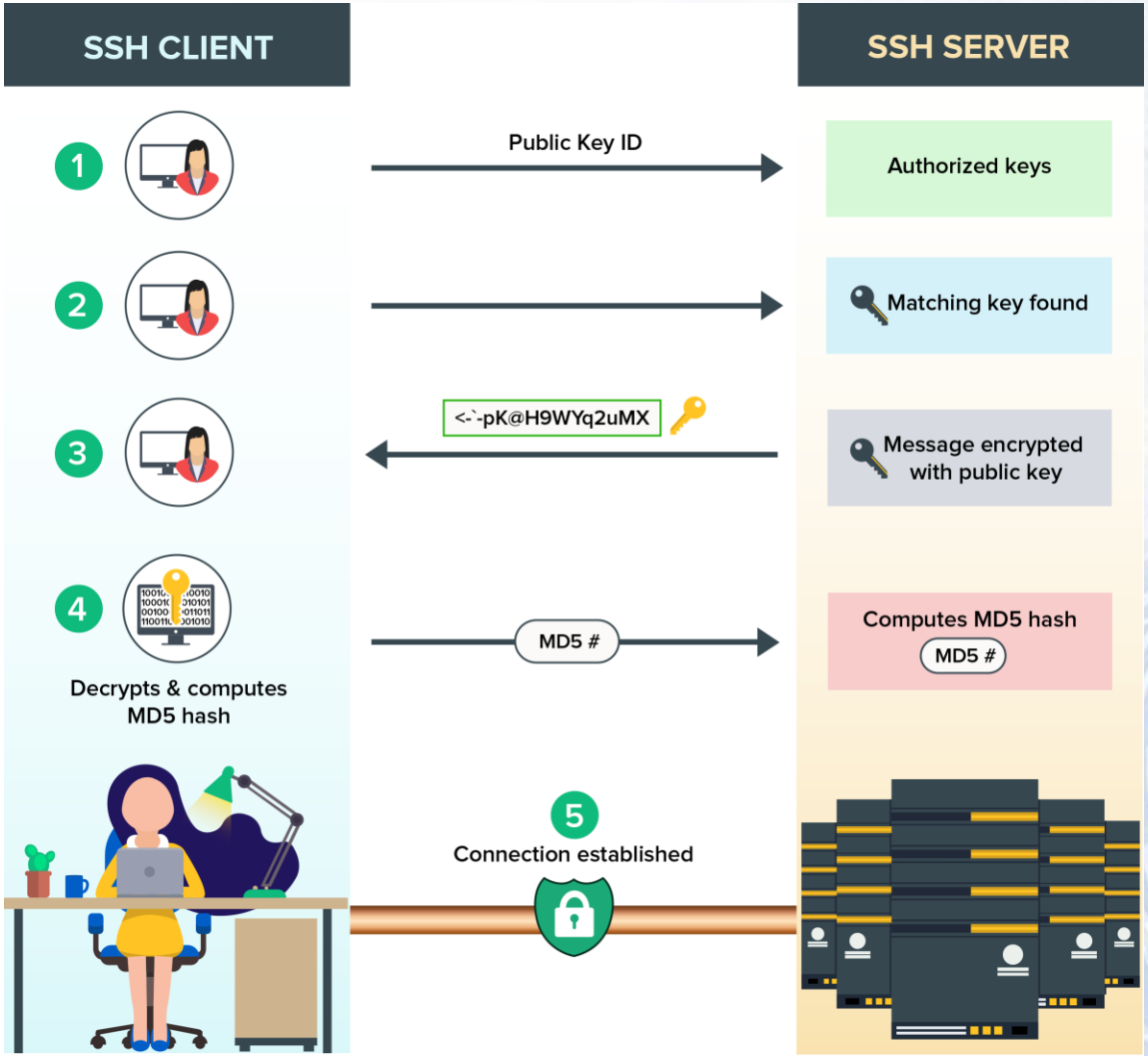


How SSH Works

SSH uses public-key cryptography and encryption to establish a secure connection:

1. **Client Authentication:** The client initiates a connection to the server using SSH and provides its public key.
2. **Server Authentication:** The server presents its public key to the client, which the client verifies to ensure the authenticity of the server.
3. **Session Key Exchange:** Both client and server agree on a session key, which is used for symmetric encryption and decryption of data during the session.
4. **Secure Data Exchange:** All subsequent data exchanged between the client and server is encrypted using the session key.
5. **Command Execution and File Transfer:** The client can securely execute remote commands or transfer files to and from the server.

HTTPS Working



Benefits of SSH

SSH offers several advantages for secure remote access and file transfer:

- **Encryption:** All data transmitted over SSH is encrypted, protecting it from unauthorized access or interception.
- **Authentication:** SSH uses public-key cryptography for user authentication, ensuring secure access to remote systems.
- **Data Integrity:** SSH verifies the integrity of data during transmission, preventing tampering or unauthorized modification.
- **Port Forwarding:** SSH allows secure tunneling of other protocols, enabling remote access to services running on a server's local network.
- **Cross-Platform Compatibility:** SSH is available on various operating systems, making it widely accessible for remote administration.

SSH Implementation

Steps to implement SSH for remote access and file transfer:

1. Install an SSH server on the remote system you want to access.
2. Generate an SSH key pair on the client machine.
3. Configure the SSH server to allow remote access using the generated SSH public key.
4. Use an SSH client (e.g., OpenSSH, PuTTY) to establish a secure connection to the remote system using the SSH key pair.

SSH Best Practices

Best practices for implementing and using SSH:

- Use strong and unique SSH key pairs for authentication.
- Disable password-based authentication to enhance security.
- Regularly update SSH software and apply security patches.
- Implement firewall rules to allow SSH access only from trusted IP addresses.
- Monitor SSH logs for suspicious activity and enable two-factor authentication for added security.

Conclusion

- SSH is a critical protocol for secure remote access and file transfer.
- It provides encryption, authentication, and data integrity, ensuring secure communication between client and server.
- By implementing SSH correctly and following best practices, organizations can protect sensitive information and maintain secure remote administration.

SSL (Secure Sockets Layer) - Ensuring Secure Communication

Introduction to SSL

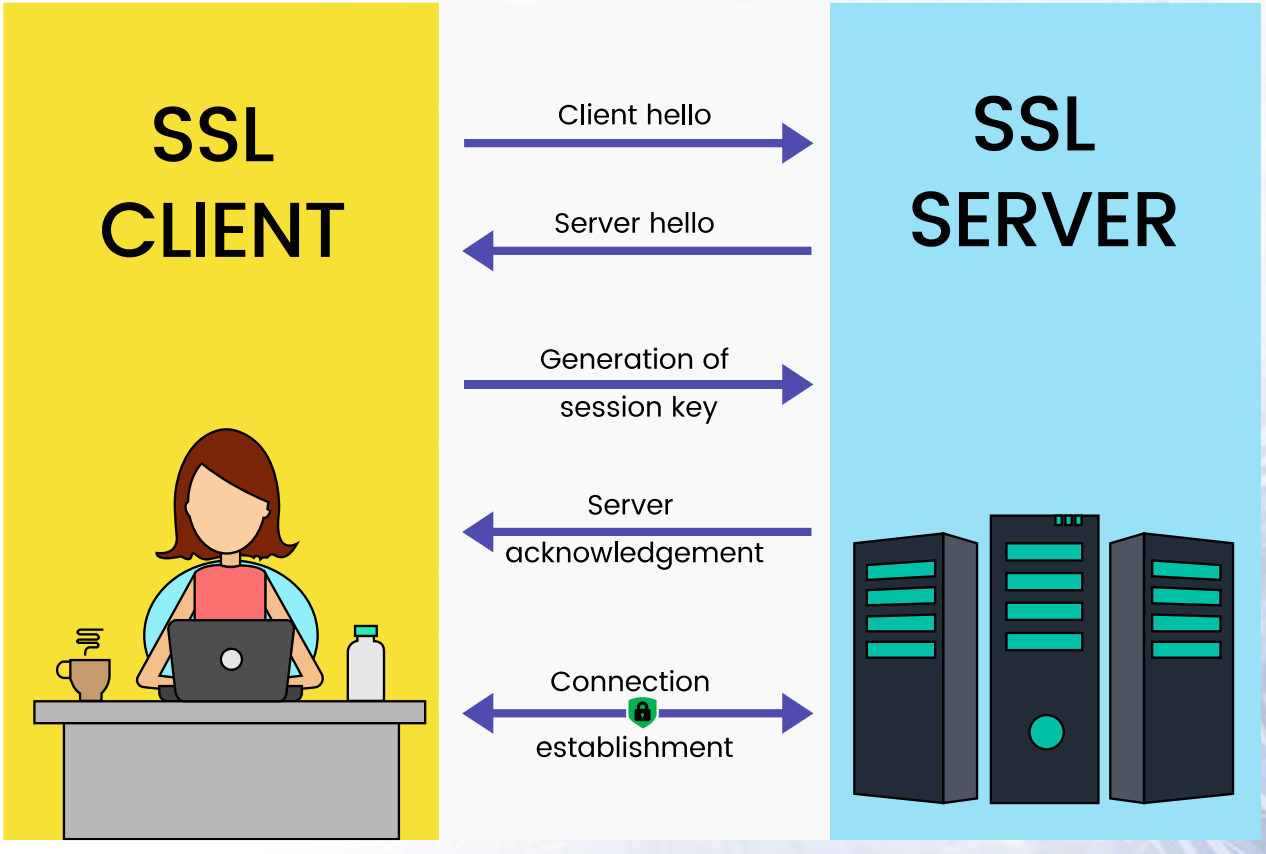
- SSL (Secure Sockets Layer) is a cryptographic protocol that provides secure communication over the internet.
- It ensures the confidentiality, integrity, and authenticity of data transmitted between clients and servers.
- SSL has been succeeded by Transport Layer Security (TLS), but the term "SSL" is still commonly used.



How SSL Works

- SSL handshake process:
- **Client Hello**: The client initiates a connection request to the server, presenting its supported SSL/TLS versions and cipher suites.
- **Server Hello**: The server responds by selecting the appropriate SSL/TLS version and cipher suite from the client's options.
- **Certificate Exchange**: The server sends its SSL certificate to the client, containing the server's public key and digitally signed by a trusted Certificate Authority (CA).
- **Client Authentication**: If required, the client presents its own SSL certificate to the server for authentication.
- **Session Key Exchange**: The client and server establish a session key for symmetric encryption and decryption of data during the session.
- **Secure Data Exchange**: All subsequent data exchanged between the client and server is encrypted using the session key.
- **Session Closure**: When the session ends, the client and server exchange closure messages to properly terminate the connection.

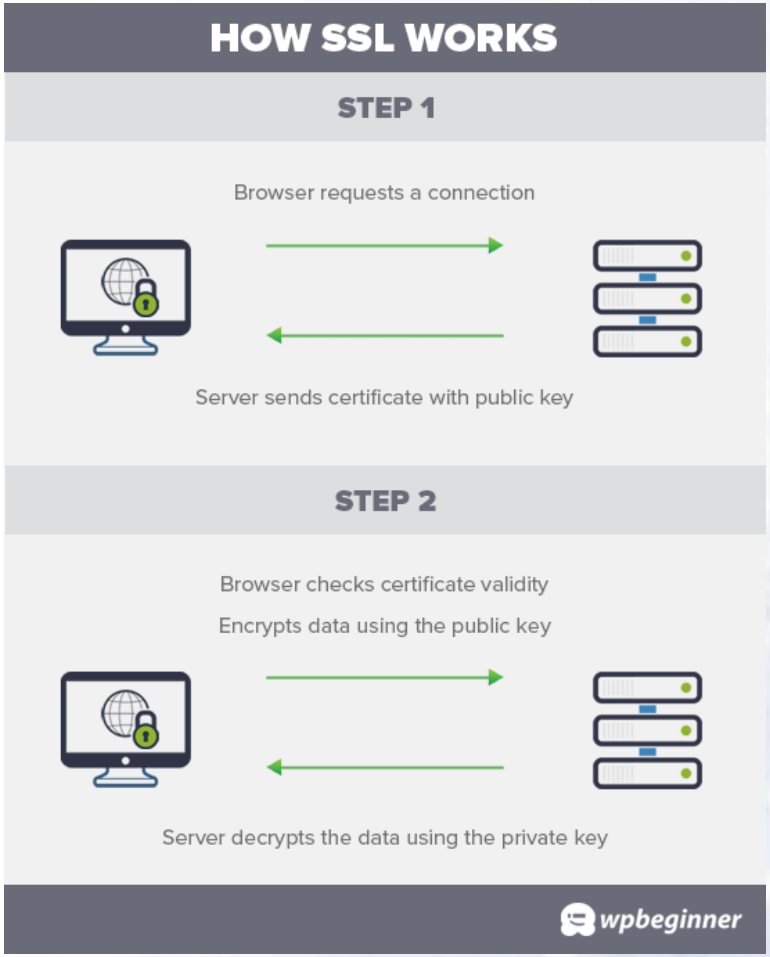
SSL Working


SSL
CLIENT
Client hello
Server hello
Generation of
session key
Server
acknowledgement
Connection
establishment
SSL
SERVER

SSL Certificate

- SSL certificates play a crucial role in SSL/TLS communication:
- They are digital files that bind an organization's identity with a public key.
- Issued by trusted Certificate Authorities (CAs), SSL certificates provide authenticity and trust to the SSL/TLS connection.
- SSL certificates contain information such as the domain name, organization name, CA's digital signature, and the public key.

SSL Working with certificate



Benefits of SSL

- SSL provides several advantages for secure communication:

- **Data Encryption**: SSL encrypts sensitive information, such as login credentials and financial details, ensuring their confidentiality.
- **Data Integrity**: SSL ensures that data remains intact during transmission, preventing unauthorized modification.
- **Authentication**: SSL certificates verify the identity of the server, assuring users that they are connecting to the intended website and not an imposter.
- **Trust and User Confidence**: Displaying the padlock symbol and "https" in the URL enhances trust and reassures users about the security of the website.
- **Compliance**: SSL is often required to meet regulatory and compliance standards, such as PCI DSS for secure payment processing.

SSL Implementation

Steps to implement SSL on a website:

- Obtain an SSL certificate from a trusted CA.
- Install the SSL certificate on the web server.
- Configure the server to use SSL/TLS protocols and enable HTTPS.
- Test the SSL implementation to ensure it is functioning correctly.

SSL Best Practices

Best practices for SSL implementation and management:

- Keep SSL certificates up to date and renew them before expiration.
- Use strong encryption algorithms and secure cipher suites.
- Implement HTTP Strict Transport Security (HSTS) to enforce HTTPS usage.
- Regularly monitor and audit SSL configurations for vulnerabilities.
- Educate users on how to identify SSL indicators, such as padlock symbols and "https" in URLs.

Conclusion

- SSL is a vital technology for ensuring secure communication over the internet.
- It provides data encryption, authentication, and integrity, fostering trust and user confidence.
- By implementing SSL correctly and following best practices, organizations can enhance the security of their online services and protect sensitive information.

TLS (Transport Layer Security) - Ensuring Secure Communication

Introduction to TLS

- TLS (Transport Layer Security) is a cryptographic protocol that provides secure communication over the internet.
- It is the successor to SSL (Secure Sockets Layer) and offers enhanced security features.
- TLS ensures the confidentiality, integrity, and authenticity of data transmitted between clients and servers.

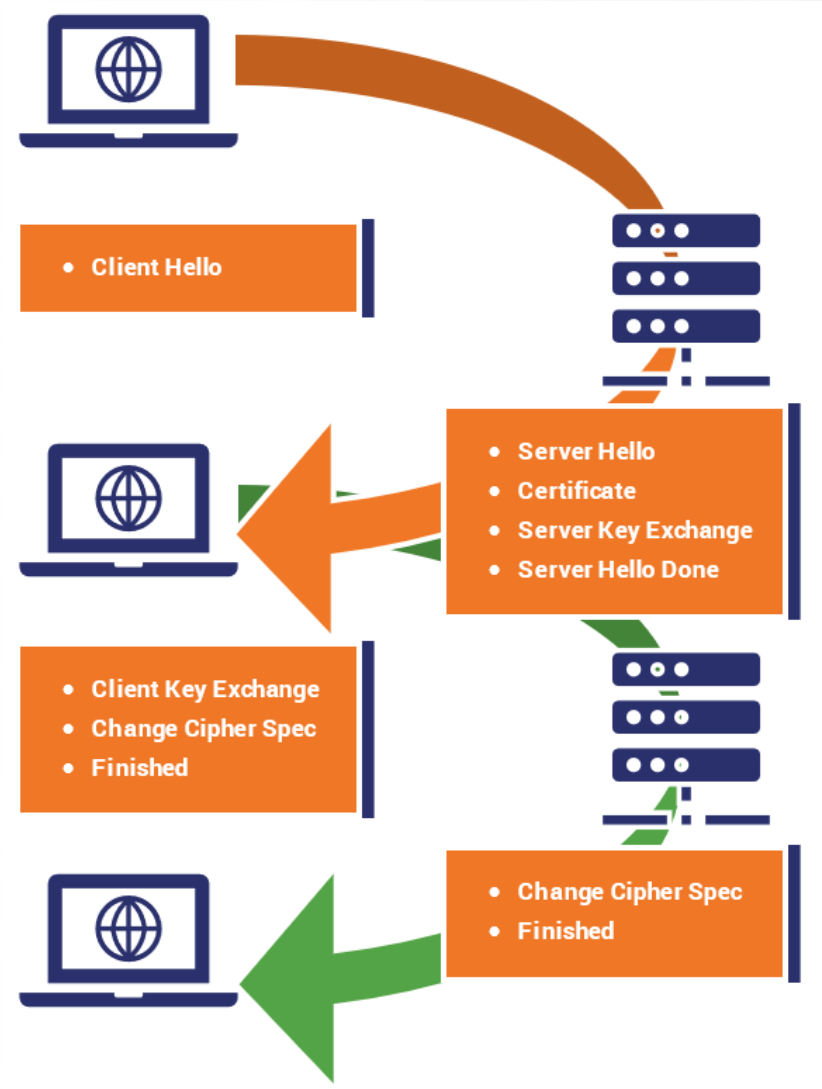


How TLS Works

TLS handshake process:

1. **Client Hello**: The client initiates a connection request to the server, presenting its supported TLS versions and cipher suites.
2. **Server Hello**: The server responds by selecting the appropriate TLS version and cipher suite from the client's options.
3. **Certificate Exchange**: The server sends its TLS certificate to the client, containing the server's public key and digitally signed by a trusted Certificate Authority (CA).
4. **Client Authentication**: If required, the client presents its own TLS certificate to the server for authentication.
5. **Key Exchange**: The client and server negotiate a shared secret key for symmetric encryption and decryption of data during the session.
6. **Secure Data Exchange**: All subsequent data exchanged between the client and server is encrypted using the shared secret key.
7. **Session Closure**: When the session ends, the client and server exchange closure messages to properly terminate the connection.

TSL Working


Client Hello
Server Hello
Certificate
Server Key Exchange
Server Hello Done
Client Key Exchange
Change Cipher Spec
Finished
Change Cipher Spec
Finished

TLS Versions and Cipher Suites

TLS supports various versions and cipher suites to ensure secure communication:

- **TLS versions**: TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3 (the latest version).
- **Cipher suites**: Combinations of encryption algorithms, authentication methods, and key exchange protocols.

Benefits of TLS

TLS provides several advantages for secure communication:

- **Strong Encryption**: TLS uses robust encryption algorithms to protect data from unauthorized access.
- **Data Integrity**: TLS ensures that data remains intact during transmission and detects any tampering attempts.
- **Authentication**: TLS certificates verify the identity of the server, assuring users they are connecting to the correct website.
- **Forward Secrecy**: TLS supports forward secrecy, ensuring that even if a private key is compromised, past communications remain secure.
- **Compatibility**: TLS is widely supported by modern web browsers and applications, enabling secure communication across platforms.

TLS Implementation

Steps to implement TLS on a website:

1. Obtain a TLS certificate from a trusted CA.
2. Install the TLS certificate on the web server.
3. Configure the server to use TLS protocols and enable HTTPS.
4. Regularly update TLS software and libraries to stay protected against vulnerabilities.

TLS Best Practices

Best practices for TLS implementation and management:

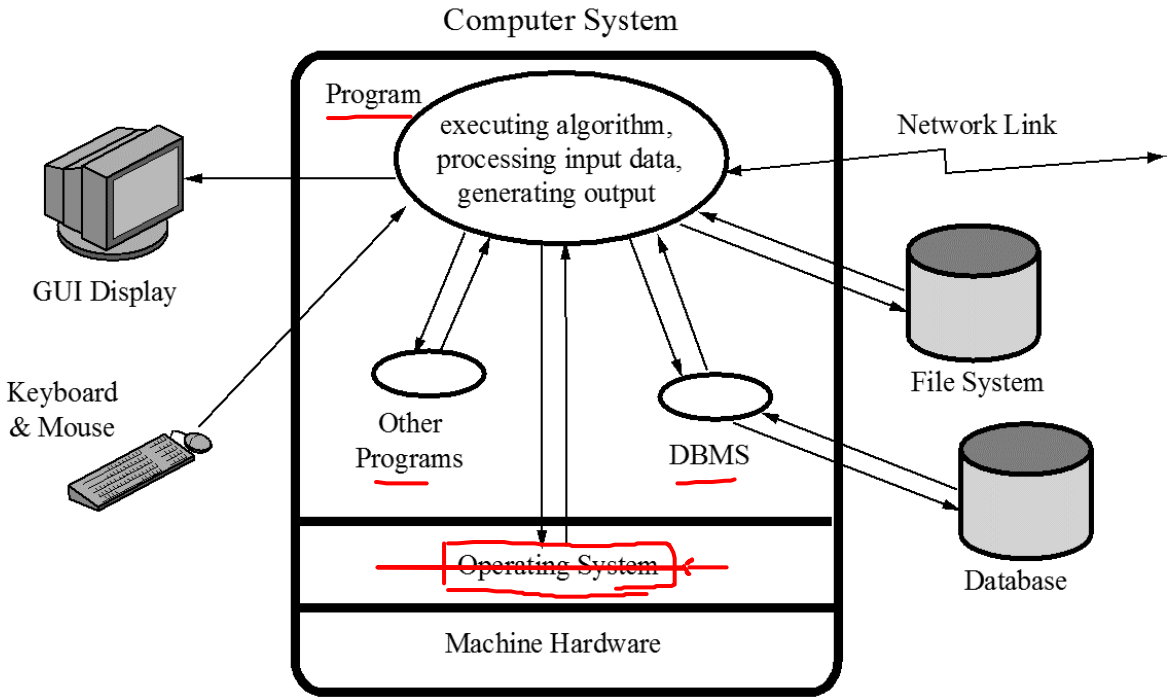
- Use the latest TLS version supported by your infrastructure.
- Select strong cipher suites that prioritize security and performance.
- Enable Perfect Forward Secrecy (PFS) to enhance security.
- Implement strict certificate validation and revocation checking.
- Regularly monitor and audit TLS configurations for vulnerabilities.

Conclusion

- TLS is a critical technology for ensuring secure communication over the internet.
- It offers strong encryption, data integrity, and authentication, enhancing the overall security of online services.
- By implementing TLS correctly and following best practices, organizations can protect sensitive information and establish trust with their users.

Operating System Security

Recall… Abstract View of Program



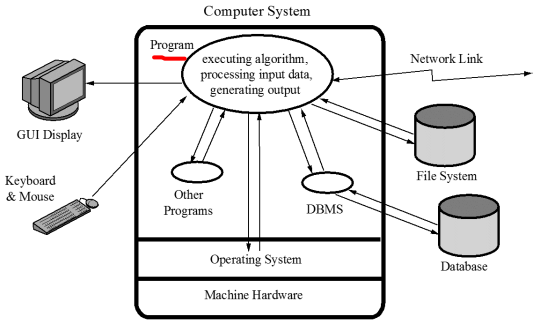
Operating System Security

Computer are rarely used in isolation
- Usually connected to some kind of network, Internet etc.

Networked computers
- ensure secure operation in networked environment

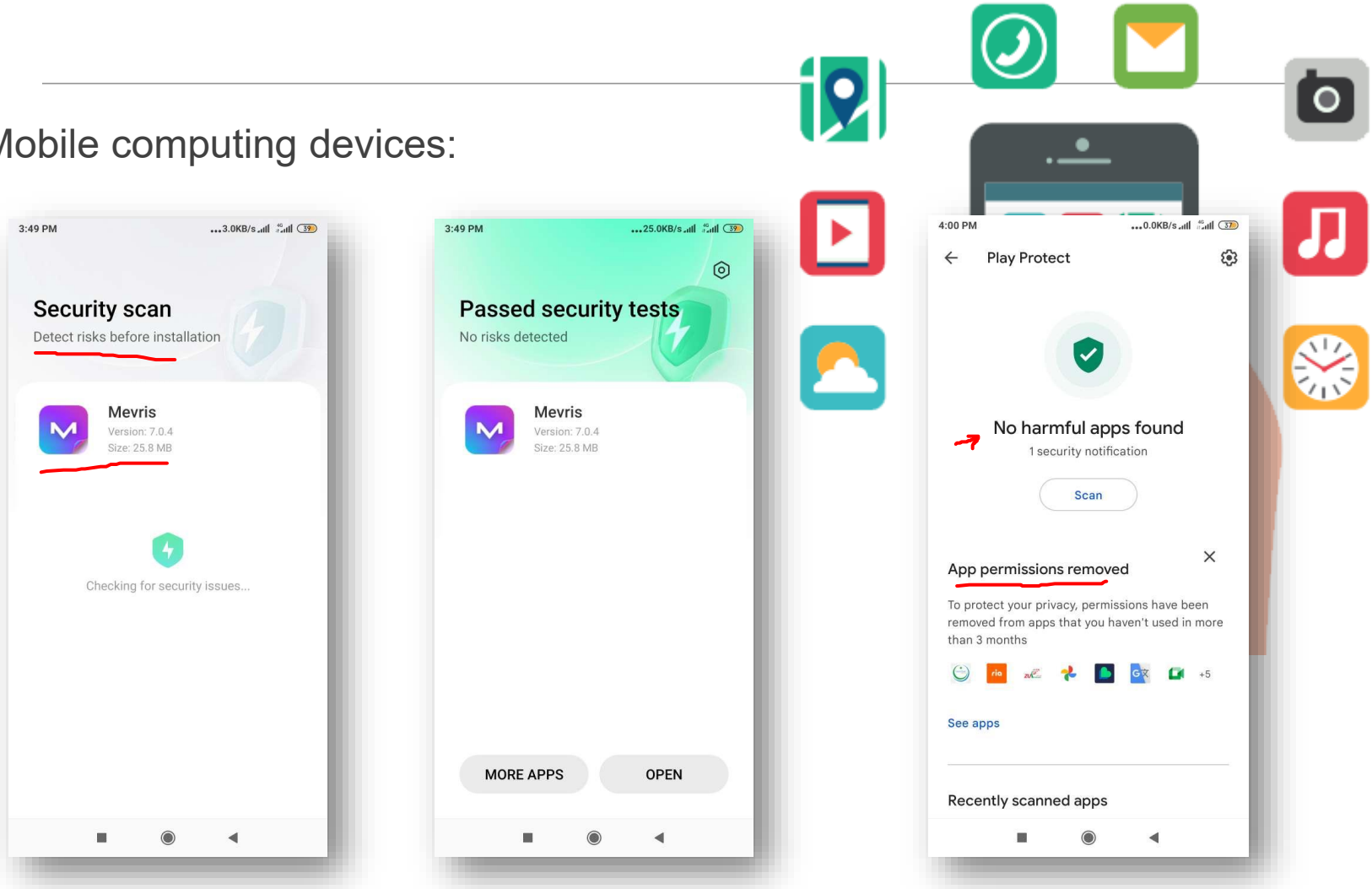
New threat?
- Attackers coming from the network.
- Network-facing programs on computers may be buggy.
- Users may be hurt via online communication.

Security mechanisms
- Authentication; Access Control
- Secure Communication (using cryptography)
- Logging & Auditing
- Intrusion Prevention and Detection



Mobile Operating System Security

Mobile computing devices:

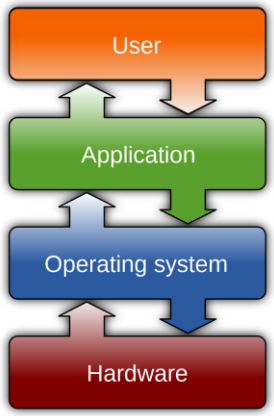


Mobile Operating System Security

Mobile computing devices:

New threat?

- Apps (programs) may be malicious.
- More tightly connected with personal life of the user e.g. personal health and banking apps.





Security mechanisms?

- Isolation of each app.
- Users assess risks of apps.
- Risk communication.

Google Play Protect

https://support.google.com/googleplay/answer/2812853?hl=en

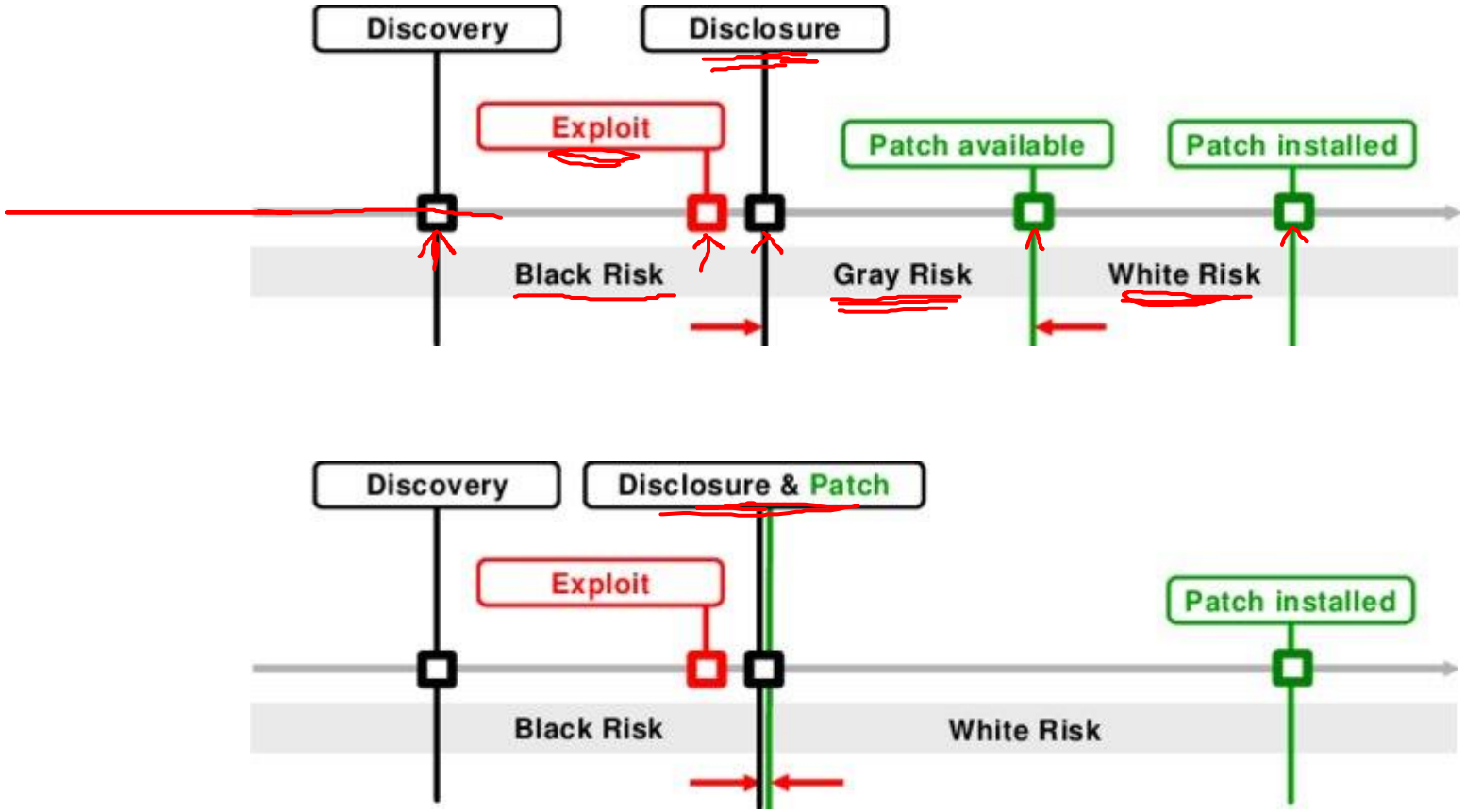
Use Google Play Protect to help keep your apps safe and your data private

Google Play Protect checks your apps and devices for harmful behavior.

- It runs a safety check on apps from the Google Play Store before you download them.
- It checks your device for potentially harmful apps from other sources. These harmful apps are sometimes called malware.
- It warns you about potentially harmful apps.
- It may deactivate or remove harmful apps from your device.
- It warns you about detected apps that violate our Unwanted Software Policy by hiding or misrepresenting important information.
- It sends you privacy alerts about apps that can get user permissions to access your personal information, violating our Developer Policy .
- It may reset app permissions to protect your privacy on certain Android versions.

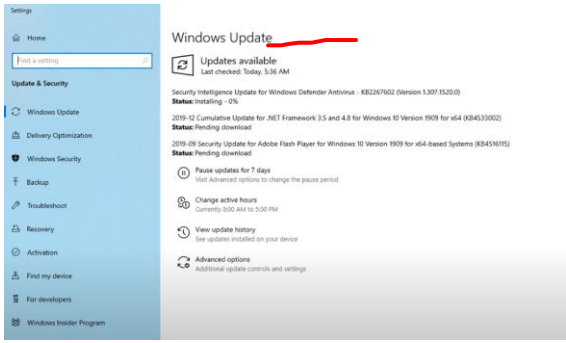
Operating System Hardening

Operating Systems' Risks
Vulnerability, Exploit, Patch…



Operating Systems Hardening

- The idea of OS hardening is to minimize a computer's exposure to current and future threats by fully configuring the operating system and removing unnecessary applications.
  - Updates in Windows
  - Patch Management System in Linux/Unix



- Basic steps
  - Install and patch the operating system
  - Harden and configure the operating system to adequately address the indentified security needs of the system by:
    - Removing unnecessary services, applications, and protocols
    - Configuring users, groups, and permissions
    - Configuring resource controls
  - Install and configure additional security controls, such as anti-virus, host-based firewalls, and intrusion detection system (IDS)
  - Test the security of the basic operating system to ensure that the steps taken adequately address its security needs

Remove Unnecessary Services, Applications, Protocols

- When performing the initial installation the supplied defaults should not be used
  - Default configuration is set to maximize ease of use and functionality rather than security
  - If additional packages are needed later they can be installed when they are required
- If fewer software packages are available to run the risk is reduced
- System planning process should identify what is actually required for a given system



- System planning process should consider:
  - Categories of users on the system
  - Privileges they have
  - Types of information they can access
  - How and where they are defined and authenticated
- Default accounts included as part of the system installation should be secured
  - Those that are not required should be either removed or disabled
  - Policies that apply to authentication credentials configured

Not all users with access to a system will have the same access to all data and resources on that system

Elevated privileges should be restricted to only those users that require them, and then only when they are needed to perform a task





Once the users and groups are defined, appropriate permissions can be set on data and resources

Many of the security hardening guides provide lists of recommended changes to the default access configuration

- Further security possible by installing and configuring additional security tools:
  - Anti-virus software
  - Host-based firewalls
  - IDS or IPS software
  - Application white-listing



- There are programs specifically designed to:
  - Review a system to ensure that a system meets the basic security requirements
  - Scan for known vulnerabilities and poor configuration practices
- Should be done following the initial hardening of the system
- Repeated periodically as part of the security maintenance process

- Final step in the process of initially securing the base operating system is security testing
- Goal:
  - Ensure the previous security configuration steps are correctly implemented
  - Identify any possible vulnerabilities

Security Maintenance

Security Maintenance

Process of maintaining security is continuous

Security maintenance includes:

- Monitoring and analyzing logging information
- Performing regular backups
- Recovering from security compromises
- Regularly testing system security
- Using appropriate software maintenance processes to patch and update all critical software

Logging

Logging

Can only inform you about bad things that have already happened

In the event of a system breach or failure, system administrators can more quickly identify what happened

Key is to ensure you capture the correct data and then appropriately monitor and analyze this data

Information can be generated by the system, network and applications

Range of data acquired should be determined during the system planning stage

Generates significant volumes of information and it is important that sufficient space is allocated for them

- automatic log rotation

Automated analysis is preferred

Data Backup and Archive

Data Backup and Archive

Performing regular backups of data is a critical control that assists with maintaining the integrity of the system and user data

- May be legal or operational requirements for the retention of data

Backup

- The process of making copies of data at regular intervals

Archive

- The process of retaining copies of data over extended periods of time in order to meet legal and operational requirements to access past data

Needs and policy relating to backup and archive should be determined during the system planning stage

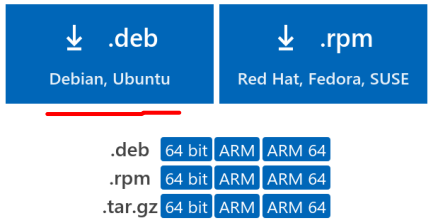
- Kept online or offline
- Stored locally or transported to a remote site
  - Trade-offs include ease of implementation and cost versus greater security and robustness against different threats

Example: Attack on an Australian hosting provider in early 2011

Linux/Unix Security

Linux/Unix Security





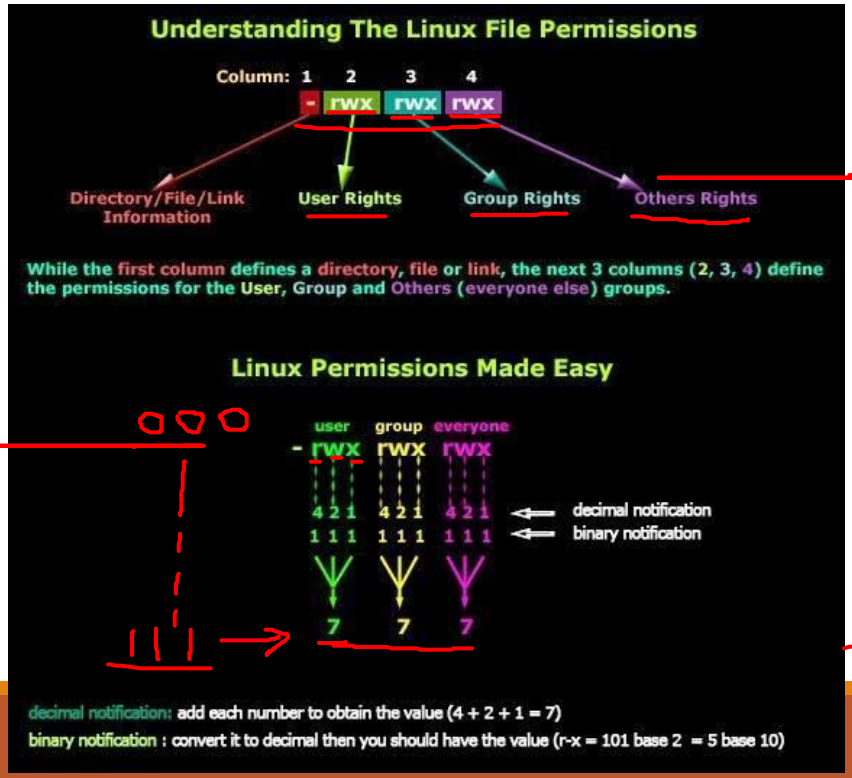
Patch Management

- Keeping security patches up to date is a widely recognized and critical control for maintaining security
  - Debian based distribution e.g. Ubuntu…include apt-get
  - RPM… Redhat based distribution e.g. Fedora…include up2date or yum
- Application and service configuration
  - Most commonly implemented using separate text files for each application and service
  - Generally located either in the /etc directory or in the installation tree for a specific application
- Individual user configurations that can override the system defaults are located in hidden “dot” files in each user’s home directory
- Most important changes needed to improve system security are to disable services and applications that are not required

Linux/Unix Security

Users, groups, and permissions

- Access is specified as granting read, write, and execute permissions to each of owner, group, and others for each resource
  - These are set using the **chmod** command.




```
israr@israr-VirtualBox: ~/Desktop/CS627/Assignment2
israr@israr-VirtualBox:~/Desktop/CS627/Assignment2$ ls
AES  aes-brute-force-master  AES.c
israr@israr-VirtualBox:~/Desktop/CS627/Assignment2$ ls -l
total 32
-rwxrwxr-x 1 israr israr 17784 2021  31 سمبر AES
drwxrwxr-x 4 israr israr  4096 2021  27 سمبر aes-brute-force-master
-rw-rw-r-- 1 israr israr  5661 2021  27 سمبر AES.c
israr@israr-VirtualBox:~/Desktop/CS627/Assignment2$
```

```
israr@israr-VirtualBox:~/Desktop/CS627/Assignment2$ chmod 777 AES.c
israr@israr-VirtualBox:~/Desktop/CS627/Assignment2$ ls -l
total 32
-rwxrwxr-x 1 israr israr 17784 2021  31 سمبر AES
drwxrwxr-x 4 israr israr  4096 2021  27 سمبر aes-brute-force-master
-rwxrwxrwx 1 israr israr  5661 2021  27 سمبر AES.c
```

```
israr@israr-VirtualBox:~/Desktop/CS627/Assignment2$ chmod 700 AES.c
israr@israr-VirtualBox:~/Desktop/CS627/Assignment2$ ls -l
total 32
-rwxrwxr-x 1 israr israr 17784 2021  31 سمبر AES
drwxrwxr-x 4 israr israr  4096 2021  27 سمبر aes-brute-force-master
-rwx------ 1 israr israr  5661 2021  27 سمبر AES.c
israr@israr-VirtualBox:~/Desktop/CS627/Assignment2$
```

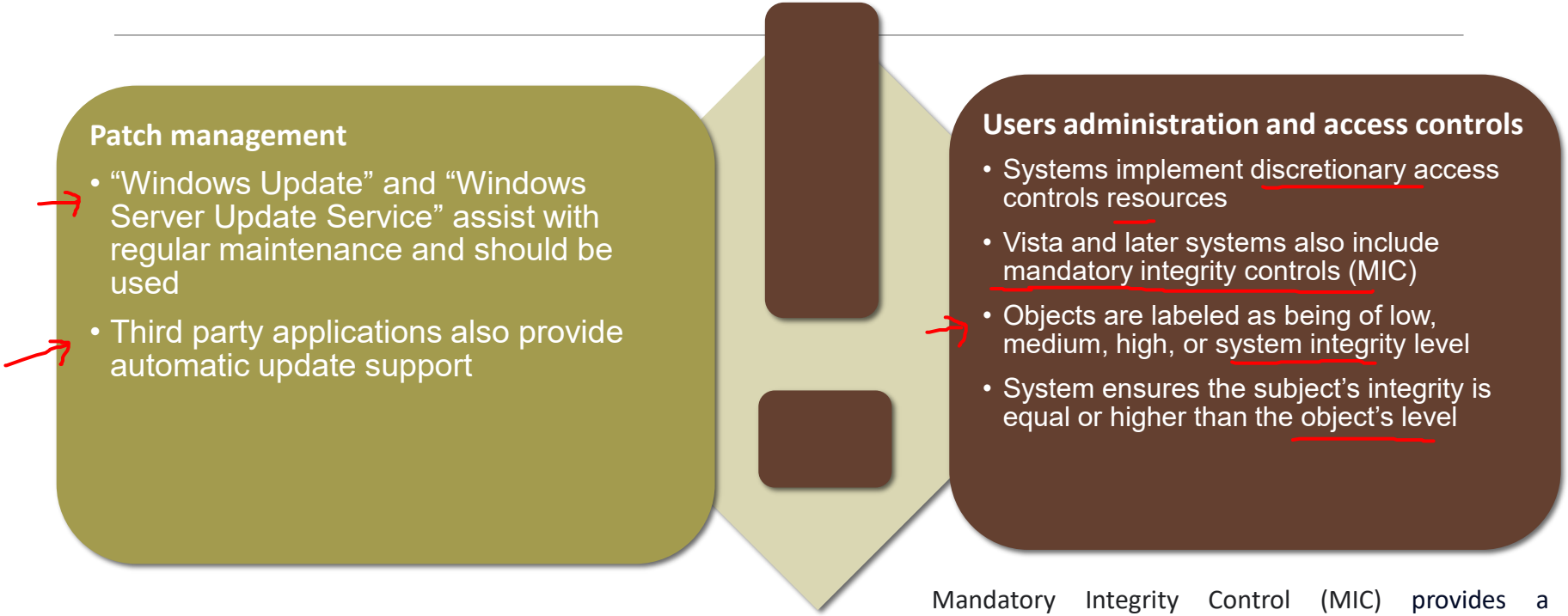
Linux/Unix Security

- Guides recommend changing the access permissions for critical directories and files

- Local exploit
  - Software vulnerability that can be exploited by an attacker to gain elevated privileges
- Remote exploit
  - Software vulnerability in a network server that could be triggered by a remote attacker

Windows Security

Windows Security



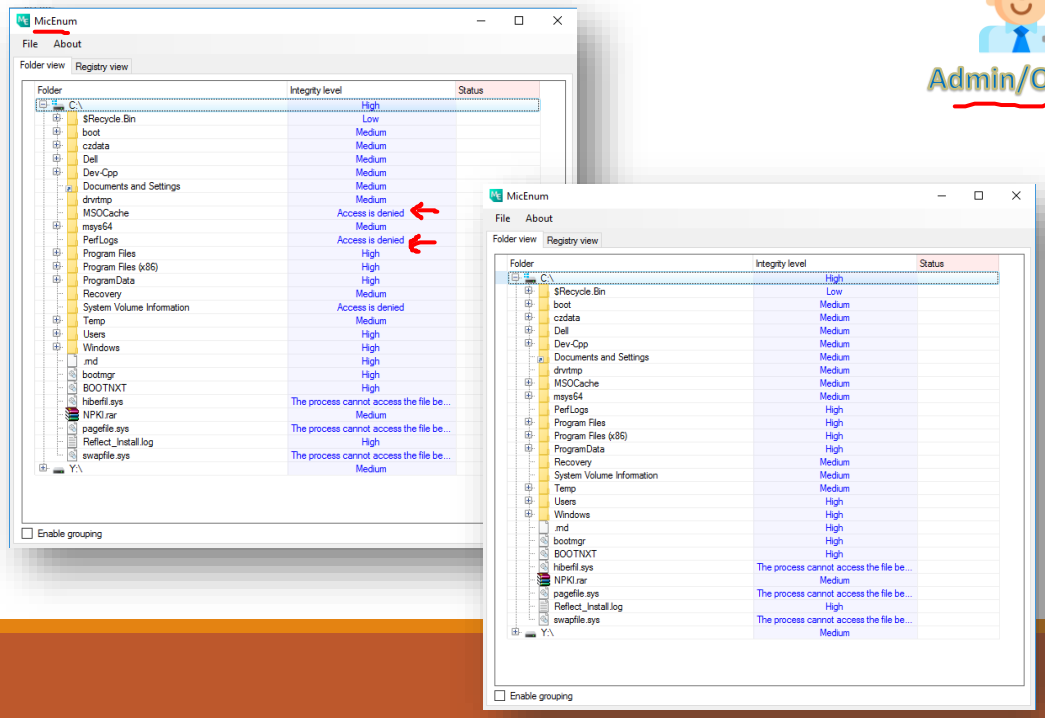
Mandatory Integrity Control (MIC) provides a mechanism for controlling access to securable objects. This mechanism is in addition to discretionary access control and evaluates access before access checks against an object's discretionary access control list (DACL) are evaluated

Windows Security

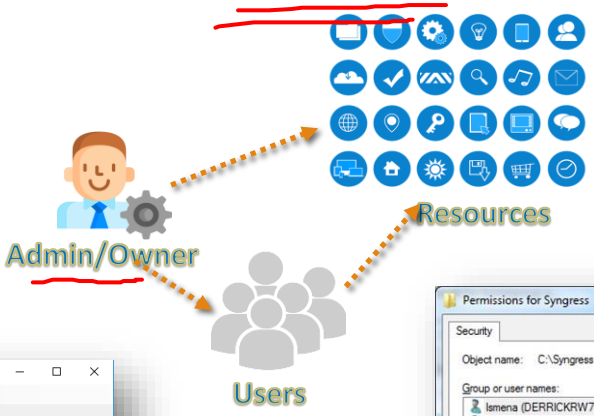
Mandatory Integrity Control (MIC) provides a mechanism for controlling access to securable objects. This mechanism is in addition to discretionary access control and evaluates access before access checks against an object's discretionary access control list (DACL) are evaluated

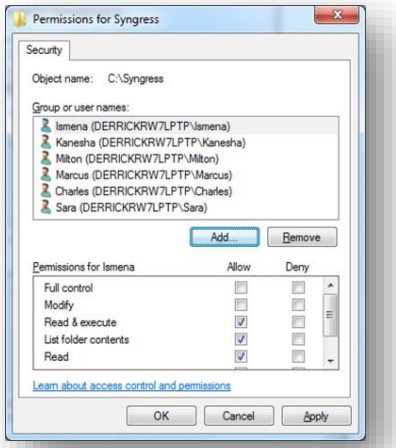
MANDATORY INTEGRITY CONTROL (MIC)

MicEnum Tool, Mandatory Integrity Control Enumerator



DISCRETIONARY ACCESS CONTROL LIST (DACL)

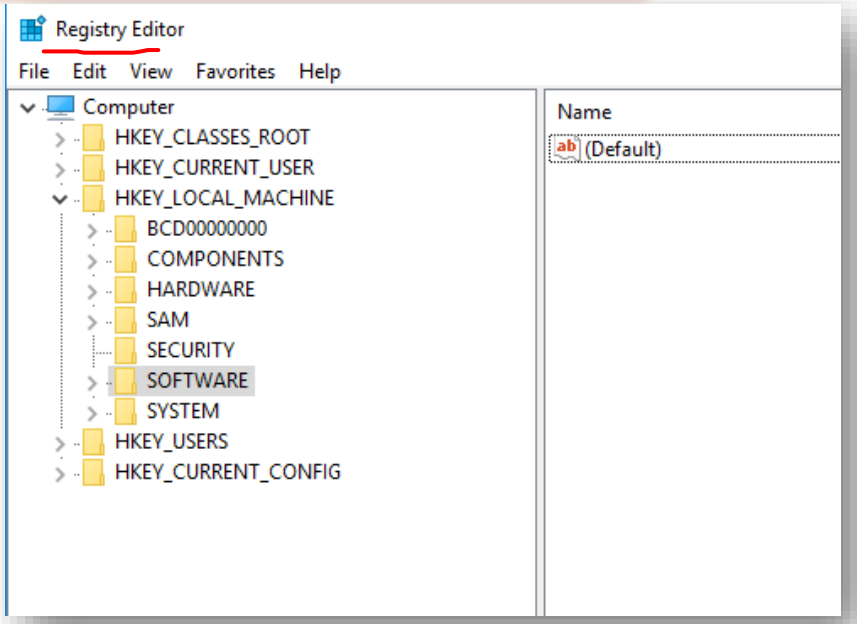




Windows Security

Application and service configuration

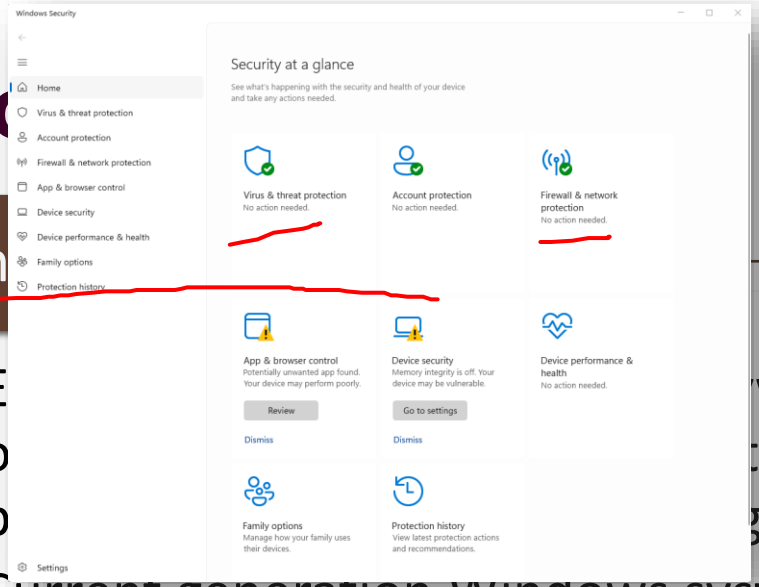
- Much of the configuration information is centralized in the Registry
  - Forms a database of keys and values that may be queried and interpreted by applications
- Registry keys can be directly modified using the “Registry Editor”
  - More useful for making bulk changes

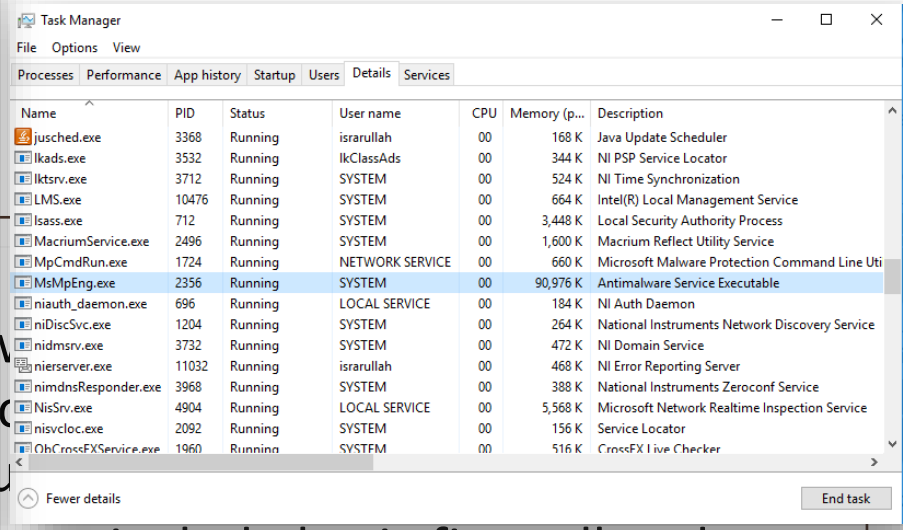


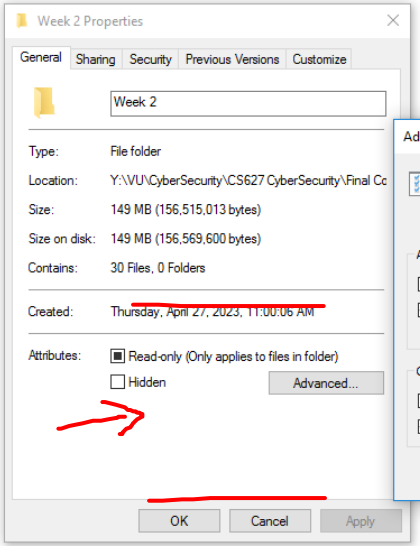
Windo

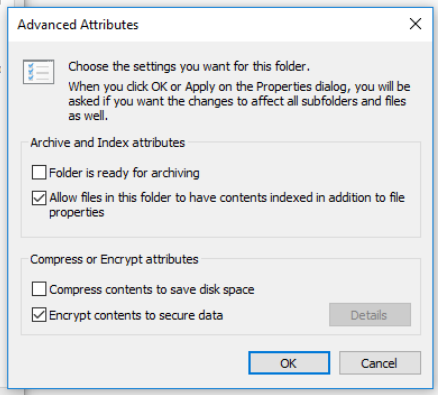
Oth

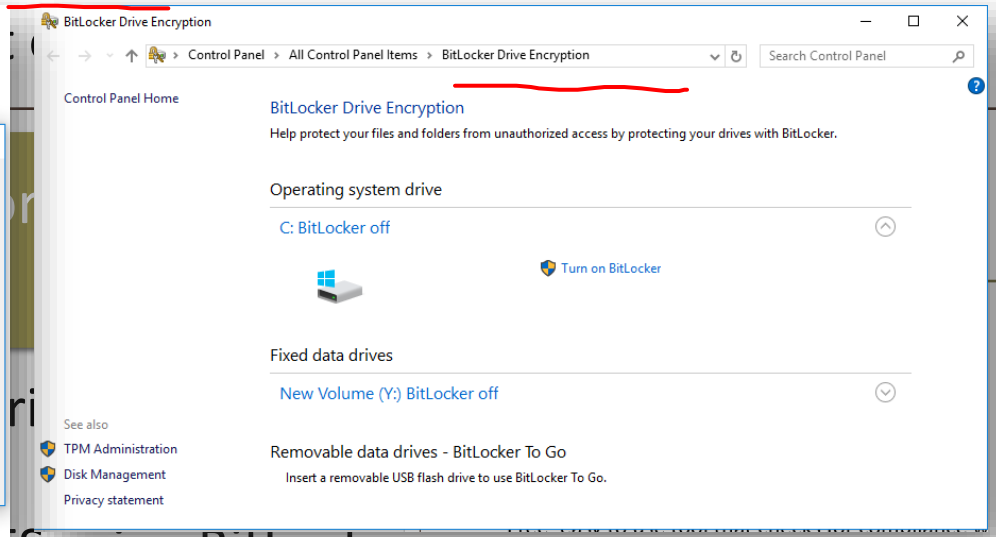
- E
- Current generation Windows systems include basic firewall and malware countermeasure capabilities
- Full-disk encryption with AES using BitLocker











Cyber Crime

Cyber Crime

- Cybercrime is a type of crime involving a computer or a computer network.
- The computer may have been used in committing the crime, or it may be the target.
- Cybercrime may harm someone, someone's security or finances.

Actors and Stakeholders

- Internationally, both state and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes.
- Cybercrimes crossing international borders and involving the actions of at least one nation-state are sometimes referred to as cyberwarfare.
- Warren Buffett describes cybercrime as the "number one problem with mankind" and said that it "poses real risks to humanity".

- A 2014 report sponsored by McAfee estimated that cybercrime had resulted in $445 billion USD in annual damage to the global economy.
- Approximately $1.5 billion was lost in 2012 to online credit and debit card fraud in the US.
- In 2018, a study by the Center for Strategic and International Studies (CSIS), in partnership with McAfee, concluded that nearly 1 percent of global gross domestic product (GDP), close to $600 billion, is lost to cybercrime each year.
- The World Economic Forum 2020 Global Risk Report confirmed that organized cybercrime groups are joining forces to commit criminal activities online, while estimating the likelihood of their detection and prosecution to be less than 1 percent in the US.

Privacy

- There are also many privacy concerns surrounding cybercrime when confidential information is intercepted or disclosed, legally or otherwise.

Cyber Crime Categories

- Computer Fraud
- Cyberterrorism
  - Ransomware
- Cybersex Trafficking
- Cyberwarfare
- Obscene / Offensive Content
- Ad-Fraud
- Online Harassment
  - Cyberbullying
  - Online predator
  - Cyberstalking
  - Cyber Racism
  - Internet troll
- Drug Trafficking
- Identity Theft
- Phishing

Computer Fraud

- Computer fraud is the act of using a computer to take or alter electronic data, or to gain unlawful use of a computer or system.
- If computer fraud involves the use of the internet, it can be considered Internet fraud.
- The legal definition of computer fraud varies by jurisdiction, but typically involves accessing a computer without permission or authorization.
- Forms of computer fraud include hacking into computers to alter information, distributing malicious code such as computer worms or viruses, installing malware or spyware to steal data, phishing, and advance-fee scams.
- Other forms of fraud may be committed using computer systems, including bank fraud, carding, identity theft, extortion, and theft of classified information.
- These types of crimes often result in the loss of personal or financial information.

Cyberterrorism

- Cyberterrorism are acts of terrorism committed through the use of cyberspace or computer resources.
- Acts of disruption of computer networks and personal computers through viruses, worms, phishing, malicious software, hardware, or programming scripts can all be forms of cyberterrorism.
- Government officials and information technology (IT) security specialists have documented a significant increase in network problems and server scams since early 2001.
- Within the United States, there is an increasing concern from agencies such as the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA).
- Such incidents are part of an organized effort by cyberterrorist foreign intelligence services or other groups to map potential security flaws in critical systems.

Cyberextortion (Ransomware)

- Ransomware is a type of malware used in cyberextortion to restrict access to files, sometimes threatening permanent data erasure unless a ransom is paid.
- The threat of ransomware is a global issue, with more than 300 million attacks worldwide in 2021.
- According to the 2022 Unit 42 Ransomware Threat Report, the average ransom demand in cases handled by Norton climbed 144 percent to $2.2 million.
- This report included an 85 percent increase in the number of victims who had their personal information shown on dark web information dumps.
- A loss of nearly $400 million in 2021 and 2022 is just one of the statistics showing the impact of ransomware attacks on everyday people.

Cybersex Trafficking

- Cybersex trafficking is the transportation of victims and then the live streaming of coerced sexual acts or rape on webcam.
- Victims are abducted, threatened, or deceived and transferred to "cybersex dens".
- The dens can be in any location where the cybersex traffickers have a computer, tablet, or phone with an internet connection.
- Perpetrators use social media networks, video conferences, dating pages, online chat rooms, apps, dark web sites, and other platforms.
- They use online payment systems and cryptocurrencies to hide their identities.
- Millions of reports of its occurrence are sent to authorities annually.
- New legislation and police procedures are needed to combat this type of cybercrime.
- There are an estimated 6.3 million victims of cybersex trafficking, according to a recent report by the International Labour Organization and IOM.
- This number includes about 1.7 million child victims.
- An example of cybersex trafficking is the 2018–2020 Nth room case in South Korea.

Cyberwarfare

- The U.S. Department of Defense notes that cyberspace has emerged as a national-level concern through several recent events of geostrategic importance, including the attack on Estonia's infrastructure in 2007, allegedly by Russian hackers.
- In August 2008, Russia again allegedly conducted cyberattacks, this time in a coordinated and synchronized kinetic and non-kinetic campaign against the country of Georgia.
- Fearing that such attacks may become normalized in future warfare among nation-states, the military commanders intend to adapt the concept of cyberspace operations impact in the future.

Obscene or offensive content

- The content of websites and other electronic communications may be distasteful, obscene, or offensive for a variety of reasons. In some instances, these communications may be illegal.

- The extent to which these communications are unlawful varies greatly between countries, and even within nations. It is a sensitive area in which the courts can become involved in arbitrating between groups with strong beliefs.

- One area of internet pornography that has been the target of the strongest efforts at curtailment is child pornography, which is illegal in most jurisdictions in the world.

Computer as a tool

- When the individual is the main target of cybercrime, the computer can be considered as the tool rather than the target.
- These crimes generally involve less technical expertise.
- Human weaknesses are generally exploited.
- The damage dealt is largely psychological and intangible, making legal action against the variants more difficult.
- These are the crimes which have existed for centuries in the offline world.
- Scams, theft, and the like existed before the development of computers and the internet.
- The same criminal has simply been given a tool which increases their potential pool of victims and makes them all the harder to trace and apprehend.

Computer as a tool

- Crimes that use computer networks or devices to advance other ends include:
  - Fraud and identity theft (although this increasingly uses malware, hacking or phishing, making it an example of both "computer as target" and "computer as tool" crime)
  - Information warfare
  - Phishing scams
  - Spam
  - Propagation of illegal obscene or offensive content, including harassment and threats
- The unsolicited sending of bulk email for commercial purposes (spam) is unlawful in some jurisdictions.
- Phishing is mostly propagated via email.
- Phishing emails may contain links to other websites that are affected by malware.
- Or they may contain links to fake online banking or other websites used to steal private account information.

Ad-fraud

- Ad-frauds are particularly popular among cybercriminals, as such frauds are lucrative and less likely to be prosecuted.
- Jean-Loup Richet, a professor at the Sorbonne Business School, classified the large variety of ad-fraud committed by cybercriminals into three categories:
  - identity fraud, attribution fraud, and ad-fraud services.

Ad-fraud

- Identity fraud aims to impersonate real users and inflate audience numbers.

- Several ad-fraud techniques relate to this category and include
  - traffic from bots (coming from a hosting company or a data center, or from compromised devices);
  - cookie stuffing;
  - falsifying user characteristics, such as location and browser type;
  - fake social traffic (misleading users on social networks into visiting the advertised website);
  - the creation of fake social media accounts to make the bot appear legitimate.

Ad-fraud

- Attribution fraud impersonates the activities of real users, such as clicks and conversations.
- Multiple ad-fraud techniques belong to this category:
  - hijacked devices and the use of infected users (through malware) as part of a botnet to participate in ad fraud campaigns;
  - click farms (companies where low-wage employees are paid to click or engage in conversations and affiliates' offers);
  - incentivized browsing;
  - video placement abuse (delivered in display banner slots);
  - hidden ads (which will never be viewed by real users);
  - domain spoofing (ads served on a website other than the advertised real-time bidding website);
  - clickjacking, in which the user is forced to click on an ad.

Ad-fraud

- Ad fraud services are related to all online infrastructure and hosting services that might be needed to undertake identity or attribution fraud.
- Services can involve
  - the creation of spam websites (fake networks of websites created to provide artificial backlinks);
  - link building services;
  - hosting services;
  - creation of fake and scam pages impersonating a famous brand and used as part of an ad fraud campaign.

Online harassment

- Cyberbullying
- Online predator
- Cyberstalking
- Cyber Racism
- Internet troll

- Whereas content may be offensive in a non-specific way, harassment directs obscenities and derogatory comments at specific individuals focusing, for example, on gender, race, religion, nationality, or sexual orientation.
- There are instances when committing a crime using a computer can lead to an enhanced sentence.
  - For example, in the case of United States v. Neil Scott Kramer, the defendant was given an enhanced sentence according to the U.S. Sentencing Guidelines Manual §2G1.3(b)(3) for his use of a cell phone to "persuade, induce, entice, coerce, or facilitate the travel of, the minor to engage in prohibited sexual conduct."
  - Kramer appealed the sentence on the grounds that there was insufficient evidence to convict him under this statute because his charge included persuading through a computer device and his cellular phone technically is not a computer.
  - Although Kramer tried to argue this point, the U.S. Sentencing Guidelines Manual states that the term "computer" means "an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

- In the United States, over 41 states have passed laws and regulations that regard extreme online harassment as a criminal act.
- These acts can be punished on a federal scale, such as US Code 18 Section 2261A, which states that using computers to threaten or harass can lead to a sentence of up to 20 years, depending on the action taken.
- Several countries outside the United States have also created laws to combat online harassment.
- In China, a country that supports over 20 percent of the world's internet users, the Legislative Affairs Office of the State Council passed a strict law against the bullying of young people through a bill in response to the Human Flesh Search Engine.
- The United Kingdom passed the Malicious Communications Act, among other acts from 1997 to 2013, which stated that sending messages or letters electronically that the government deemed "indecent or grossly offensive" and/or language intended to cause "distress and anxiety" can lead to a prison sentence of six months and a potentially large fine.
- Australia, while not directly addressing the issue of harassment, has grouped the majority of online harassment under the Criminal Code Act of 1995.
- Using telecommunication to send threats or harass and cause offense was a direct violation of this act.

- Freedom of Speech:
  - Although freedom of speech is protected by law in most democratic societies (in the US this is done by the First Amendment), it does not include all types of speech.
  - In fact, spoken or written "true threat" speech or text is criminalized because of "intent to harm or intimidate".
  - That also applies to online or network-related threats in written text or speech.

- Cyberbullying:
  - Cyberbullying has increased drastically with the growing popularity of online social networking.
  - As of January 2020, 44 percent of adult internet users in the United States have "personally experienced online harassment".
  - Children who experience online harassment deal with negative and sometimes life-threatening side effects.
  - In 2021, reports displayed 41 percent of children developing social anxiety, 37 percent of children developing depression, and 26 percent of children having suicidal thoughts.

- Spying:
  - The United Arab Emirates was named in a spying scandal where the Gulf nation along with other repressive governments purchased NSO Group's mobile spyware Pegasus for mass surveillance.
  - Prominent activists and journalists were targeted as part of the campaign, including Ahmed Mansoor, Princess Latifa, Princess Haya, and more.
  - Ghada Oueiss was one of the many high-profile female journalists and activists who became the target of online harassment.
  - Oueiss filed a lawsuit against UAE ruler Mohamed bin Zayed Al Nahyan along with other defendants, accusing them of sharing her photos online.
  - The defendants, including the UAE ruler, filed motions to dismiss the case of the hack-and-leak attack.

Drug trafficking

- Darknet markets are used to buy and sell recreational drugs online.
- Some drug traffickers use encrypted messaging tools to communicate with drug mules or potential customers.
- The dark web site Silk Road was the first major online marketplace for drugs, starting operation in 2011.
- It was permanently shut down in 2014 by the FBI and Europol.
- After Silk Road 2.0 went down, Silk Road 3 Reloaded emerged.
- However, it was just an older marketplace named Diabolus Market, that used the name for more exposure from the brand's previous success.

- Darknet markets have had a rise in traffic in recent years for many reasons, one of the biggest contributors being the anonymity offered in purchases, and often a seller-review system.
- There are many ways in which darknet markets can financially drain individuals.
- Vendors and customers alike go to great lengths to keep their identities a secret while online.
- Commonly used tools are virtual private networks (VPN), Tails, and the Tor Browser to help hide their online presence.

- Darknet markets entice customers by making them feel comfortable.
- People can easily gain access to a Tor browser with DuckDuckGo browser that allows a user to explore much deeper than other browsers such as Google Chrome.
- However, actually gaining access to an illicit market is not as simple as typing it in on a search engine like one would with Google.
- Darknet markets have special links that change frequently, ending in .onion as opposed to the typical .com, .net, and .org domain extensions.

- Digital/Virtual Currency:
  - To add to privacy, the most prevalent currency on these markets is Bitcoin.
  - Bitcoin allows transactions to be anonymous, with the only information available to the public being the record that a transaction occurred between two parties.

- An issue marketplace users face is when vendors or the market itself are exit scamming.
- This is when a vendor with a high rating will act as if they are selling on the market and have users pay for products they will not receive.
- The vendor will then close off their account after receiving money from multiple buyers and never send what was purchased.
- The vendors all being involved in illegal activities have a low chance of not exiting scamming when they no longer want to be a vendor.
- In 2019, an entire market known as Wall Street Market had allegedly exit scammed, stealing $30 million dollars from the vendors' and buyers' wallets in bitcoin.

- FBI has cracked down on these markets.
- In July 2017, FBI seized one of the biggest markets, commonly called Alphabay, which later re-opened in August 2021 under the control of DeSnake, one of the original administrators.
- Investigators will pose as a buyer and order products from darknet vendors in the hopes that vendors leave a trail the investigators can follow.
- One investigation had an investigator pose as a firearms seller and for six months people purchased from them and provided home addresses.
- The FBI was able to make over a dozen arrests during this six-month investigation.

- Another one of law enforcement's crackdowns was on vendors selling fentanyl and opiates.
- With thousands of people dying each year due to drug overdose, investigators have made it a priority.
- Many vendors do not realize the extra criminal charges that go along with selling drugs online.
- Commonly they get charged with money laundering and charges for when the drugs are shipped in the mail on top of being a drug distributor.
- In 2019, a vendor was sentenced to 10 years in prison after selling cocaine and methamphetamine under the name JetSetLife.
- Although investigators spend large amounts of time tracking down people, in 2018, only 65 suspects who bought and sold illegal goods on some of the biggest markets were identified.
- This is compared to the thousands of transactions taking place daily on these markets.

Famous Incidents:

- Data Leaks
- Celebrity Leaks
- Blackmailing
- Web Defacements
- Hacking / Spying
- Data Stealing
- Impersonation
- Superimposing / Fake Media
- ATM Fraud/Hacking
- Car Hacking
- Cryptocurrency / Forex

Identity Theft

- Identity theft occurs when someone uses another person's personal identifying information, like their name, identifying number, or credit card number, without their permission, to commit fraud or other crimes.
- The term identity theft was coined in 1964.
- Since that time, the definition of identity theft has been statutorily defined throughout both the U.K. and the U.S. as the theft of personally identifiable information [PII].
- Identity theft deliberately uses someone else's identity as a method to gain financial advantages or obtain credit and other benefits, and perhaps to cause other person's disadvantages or loss.
- The person whose identity has been stolen may suffer adverse consequences, especially if they are falsely held responsible for the perpetrator's actions.
- Personally identifiable information generally includes a person's name, date of birth, social security number, driver's license number, bank account or credit card numbers, PINs, electronic signatures, fingerprints, passwords, or any other information that can be used to access a person's financial resources.

Phishing

- Phishing is a form of social engineering where attackers deceive people into revealing sensitive information or installing malware such as ransomware.
- Phishing attacks have become increasingly sophisticated and often transparently mirror the site being targeted, allowing the attacker to observe everything while the victim is navigating the site, and transverse any additional security boundaries with the victim.
- As of 2020, it is the most common type of cybercrime, with the FBI's Internet Crime Complaint Centre reporting more incidents of phishing than any other type of computer crime.
- The term "phishing" was first recorded in 1995 in the cracking toolkit AOHell, but may have been used earlier in the hacker magazine 2600.
- It is a variation of fishing and refers to the use of lures to "fish" for sensitive information.
- Measures to prevent or reduce the impact of phishing attacks include legislation, user education, public awareness, and technical security measures.
- The importance of phishing awareness has increased in both personal and professional settings, with phishing attacks among businesses rising from 72% to 86% from 2017 to 2020.

Phishing Types

- Email phishing
- Spear phishing
- Whaling and CEO fraud
- Clone phishing
- Voice phishing
- SMS phishing
- Page hijacking
- Calendar phishing

Phishing Types

- Email phishing
  - Phishing attacks, often delivered via email spam, attempt to trick individuals into giving away sensitive information or login credentials.
  - Most attacks are "bulk attacks" that are not targeted and are instead sent in bulk to a wide audience.
  - The goal of the attacker can vary, with common targets including financial institutions, email and cloud productivity providers, and streaming services.
  - The stolen information or access may be used to steal money, install malware, or spear phish others within the target organization.
  - Compromised streaming service accounts may also be sold on darknet markets.
  - This method of social engineering attack involve sending fraud email or messages that appear to be from a trusted source, such as bank, amazon, or government agency.
  - These messages will typically contain a link or attachment that, when you click, will install malware automatically on the targeted device or redirect them to fake login page of any trusted website where they will be promoted to enter their login credential.

Phishing Types

- Spear phishing
  - Spear phishing is a targeted phishing attack that uses personalized emails to trick a specific individual or organization into believing they are legitimate.
  - It often utilizes personal information about the target to increase the chances of success.
  - These attacks often target executives or those in financial departments with access to sensitive financial data and services.
  - Accountancy and audit firms are particularly vulnerable to spear phishing due to the value of the information their employees have access to.
  - Threat Group-4127 (Fancy Bear) targeted Hillary Clinton's 2016 presidential campaign with spear phishing attacks on over 1,800 Google accounts, using the accounts-google.com domain to threaten targeted users.
  - A study on spear phishing susceptibility among different age groups found that 43% of 100 young and 58 older users clicked on simulated phishing links in daily emails over 21 days.
  - Older women had the highest susceptibility, while susceptibility in young users declined over the study, but remained stable in older users.

Phishing Types

- Whaling and CEO fraud
  - Whaling attacks use spear phishing techniques to target senior executives and other high-profile individuals[with customized content, often related to a subpoena or customer complaint.
  - CEO fraud involves sending fake emails from senior executives to trick employees into sending money to an offshore account.
  - It has a low success rate, but can result in organizations losing large sums of money.

Phishing Types

- Clone phishing
  - Clone phishing is a type of attack where a legitimate email with an attachment or link is copied and modified to contain malicious content.
  - The modified email is then sent from a fake address made to look like it's from the original sender.
  - The attack may appear to be a resend or update of the original email.
  - It often relies on the sender or recipient being previously hacked so the attacker can access the legitimate email.

Phishing Types

- Voice phishing
  - Voice over IP (VoIP) is used in vishing or voice phishing attacks, where attackers make automated phone calls to large numbers of people, often using text-to-speech synthesizers, claiming fraudulent activity on their accounts.
  - The attackers spoof the calling phone number to appear as if it is coming from a legitimate bank or institution.
  - The victim is then prompted to enter sensitive information or connected to a live person who uses social engineering tactics to obtain information.
  - Vishing takes advantage of the public's lower awareness and trust in voice telephony compared to email phishing.

Phishing Types

- SMS phishing (Smishing)
  - SMS phishing or smishing is a type of phishing attack that uses text messages from a cell phone or smartphone to deliver a bait message.
  - The victim is usually asked to click a link, call a phone number, or contact an email address provided by the attacker.
  - They may then be asked to provide private information, such as login credentials for other websites.
  - The difficulty in identifying illegitimate links can be compounded on mobile devices due to the limited display of URLs in mobile browsers.
  - Smishing can be just as effective as email phishing, as many smartphones have fast internet connectivity. Smishing messages may also come from unusual phone numbers.

Phishing Types

- Page hijacking
  - Page hijacking involves redirecting users to malicious websites or exploit kits through the compromise of legitimate web pages, often using cross site scripting.
  - Hackers may insert exploit kits such as MPack into compromised websites to exploit legitimate users visiting the server.
  - Page hijacking can also involve the insertion of malicious inline frames, allowing exploit kits to load.
  - This tactic is often used in conjunction with watering hole attacks on corporate targets.

Phishing Types

- Calendar phishing
  - Calendar phishing involves sending fake calendar invitations with phishing links.
  - These invitations often mimic common event requests and can easily be added to calendars automatically.
  - To protect against this form of fraud, former Google click fraud czar Shuman Ghosemajumder recommends changing calendar settings to not automatically add new invitations.

Phishing Techniques

- Link manipulation
- Filter evasion
- Social engineering

Phishing Techniques

- Link manipulation
  - Phishing attacks often involve creating fake links that appear to be from a legitimate organization.
  - These links may use misspelled URLs or subdomains to deceive the user.

  - Another tactic is to make the displayed text for a link appear trustworthy, while the actual link goes to the phisher's site.
  - To check the destination of a link, many email clients and web browsers will show the URL in the status bar when the mouse is hovering over it.
  - However, some phishers may be able to bypass this security measure.

Phishing Techniques

- Filter evasion
  - Phishers have sometimes used images instead of text to make it harder for anti-phishing filters to detect the text commonly used in phishing emails.
  - In response, more sophisticated anti-phishing filters are able to recover hidden text in images using optical character recognition (OCR).

Phishing Techniques

- Social engineering
  - Phishing often uses social engineering techniques to trick users into performing actions such as clicking a link or opening an attachment, or revealing sensitive information.
  - It often involves pretending to be a trusted entity and creating a sense of urgency, like threatening to close or seize a victim's bank or insurance account.
  - An alternative technique to impersonation-based phishing is the use of fake news articles to trick victims into clicking on a malicious link.
  - These links often lead to fake websites that appear legitimate, but are actually run by attackers who may try to install malware or present fake "virus" notifications to the victim.

Anti-phishing

Combating computer crime

- It is difficult to find and combat cybercrime perpetrators due to their use of the internet in support of cross-border attacks.
- Not only does the internet allow people to be targeted from various locations, but the scale of the harm done can be magnified.
- Cybercriminals can target more than one person at a time.
- The availability of virtual spaces to public and private sectors has allowed cybercrime to become an everyday occurrence.
- In 2018, The Internet Crime Complaint Center received 351,937 complaints of cybercrime, which lead to $2.7 billion lost.

Combating computer crime

- Investigation
- Prevention
- Legislation
- Penalties
- Awareness
- Intelligence

Cyber Crime Jobs

- Government, Military, Law Enforcement Agencies
- Private sector companies
- Designations:
  - Cyber Crime Analyst / Forensic Examiner / Scientist / Specialist / Investigator
- Relevant Degree, Certifications and Experience



Cyber Crime Agencies and Organizations

- FIA – CCW
- Military
- Government Sector
- Private Companies
- CERTs

Cyber Crime Law in Pakistan

- PECA (2016)
  - Prevention of Electronic Crimes Act

- PPC (Pakistan Penal Code)
- CrPC (Criminal Procedure Code)
- FERA (Foreign Exchange Regulation Act, 1947)
- AMLA (Anti-Money Laundering Act, 2010)
- The Anti-Terrorism Act,1997

Cyber Crime Reporting in Pakistan

- Modes:
  - Phone
  - Online
  - In-Person
- Required Documents
  - Application / Matter
  - CNIC
  - Proofs
- Process:
  - Application submission
  - Verification
  - Enquiry
  - FIR