Module 1

Module 1

- Introduction
- Types of Hackers
- CIA Triad
- Computing Hands on
- Some Basic Terminologies
- Setting Up your Hacking environment

Learning Objective

- Understanding hacker classifications and their roles in cybersecurity awareness.
- Grasping the CIA Triad's importance in data security and protection.
- Gaining practical experience in computing through hands-on exercises.
- Acquiring fundamental hacking terminology for effective communication and comprehension.
- Establishing a secure hacking environment for ethical hacking practice sessions.

1

Introduction to Ethical Hacking

Ethical Hacking

- Legally authorized efforts to assess system vulnerabilities for security improvement.
- Conducted by skilled professionals to mimic potential malicious attacks.
- Identifies weaknesses, enhancing defenses, and protecting against real cyber threats.
- A crucial element in safeguarding digital assets and maintaining cybersecurity.

Ethical Hacking: Example

- Like a car mechanic checking for brake issues to prevent accidents.
- ethical hackers examine software vulnerabilities to avert data breaches, underscoring their vital role in safeguarding digital assets.

Ethical Hacking: Example

- Certainly, just as a locksmith tests and reinforces locks to enhance home security.
- Ethical hackers assess digital systems and strengthen cybersecurity measures to protect against potential cyber threats, underscoring their vital role in ensuring a secure online environment.

Need for Ethical Hacking:

- **Proactive Defense**: Identifying vulnerabilities before malicious hackers exploit them.
- **Data Protection**: Safeguarding sensitive information from cyberattacks and data breaches.
- **Compliance Assurance:** Ensuring adherence to legal and industry-specific cybersecurity standards.

Benefits of Ethical Hacking:

Identifying Vulnerabilities

Improving System Security

Safeguarding Reputation

Reducing Security Incidents

Protecting Sensitive Data

Compliance Verification

Enhancing Incident Response

Minimizing Legal and Financial Risks

2

Types of Hacker

Black Hat:
Criminal
Hackers

White Hat:
Authorized
Hackers

Gray Hat:
"Just for Fun"
Hackers

Black Hat Hackers

- Unauthorized cyber intruder with malicious intent and no ethical considerations.
- Engages in illegal activities, including hacking, data theft, and system disruption.
- Operates outside legal boundaries, often for financial or personal gain.
- Contrasts with ethical hackers (white hats) who improve cybersecurity legitimately.

Black Hat Hackers Intention

- Malicious aims involve exploiting vulnerabilities for personal, often illegal, advantages.
- Target financial data, steal sensitive information, or disrupt computer systems.
- Pursue financial gain, power, or chaos, with no ethical constraints.
- Pose significant threats to organizations and individuals' online security.

Example of Black Hat Hacker

- *Alex, a skilled computer programmer, infiltrated a bank's network illegally.*
- *He stole sensitive customer data, including financial records, for financial gain.*
- *His actions led to financial losses for individuals and severe legal consequences.*
- *Alex's intent was purely malicious, driven by personal profit at others' expense.*

White Hat Hackers

- Ethical cybersecurity expert.
- Authorized to test systems.
- Identifies and reports vulnerabilities.
- Enhances security, prevents cyber threats, and abides by legal standards

White Hat Hackers Intention

- Protects systems from malicious attacks.
- Ethical hacking for security improvement.
- Safeguards data, privacy, and network integrity.
- Aims to benefit organizations by enhancing their cybersecurity defenses.

Example of White Hat Hacker

- *John, a certified ethical hacker, tests company systems for vulnerabilities.*
- *Employed by a cybersecurity firm, he uncovers weaknesses and advises improvements.*
- *His actions are legal and aimed at enhancing security, not compromising it.*
- *He collaborates with organizations to strengthen defenses and protect data.*

Grey Hat Hackers

- Operates between ethical white hat and malicious black hat hacking.
- Engages in hacking without explicit authorization but with some moral considerations.
- Typically notifies organizations about vulnerabilities after discovery, balancing legality.
- Often bridges the gap between ethical disclosure and potentially harmful exploitation.

Grey Hat Hackers Intention

- Exploration: Curiosity drives them to seek security weaknesses and vulnerabilities.
- Awareness: Intends to raise awareness by disclosing vulnerabilities to organizations.
- Partial Anonymity: Strives to maintain a degree of anonymity while exposing flaws.
- Ethical Ambiguity: Operates in a gray area, sometimes for recognition or compensation.

Example of Grey Hat Hacker

- *Lisa, a grey hat hacker, discovers a security flaw in a website.*
- *Without authorization, she reports the issue to the website owner.*
- *While well-intentioned, her actions may raise ethical and legal questions.*
- *She operates in a moral gray area, balancing good intent and unauthorized access.*

3

CIA Triads

3 Fundamental Pillars of Cyber Security.

- The CIA Triad, in the context of information security and cybersecurity, is a fundamental framework used to describe and evaluate the core principles of information security

Confidentiality

- Protecting data from unauthorized access, ensuring privacy and secrecy.
- Limits access to authorized individuals, preventing data exposure or leaks.
- Enforced through encryption, access controls, and strict user authentication measures.
- Critical in safeguarding sensitive information, such as personal, financial, or classified data.

Integrity

- Guarantees data accuracy, consistency, and trustworthiness throughout its lifecycle.
- Ensures data remains unaltered, uncorrupted, and reliable for decision-making.
- Achieved through checksums, hashing, version control, and access restrictions.
- Essential to maintain data's reliability and prevent unauthorized tampering or corruption.

Availability

- Ensures data and systems are accessible when needed, minimizing downtime.
- Mitigates disruptions caused by hardware failures, cyberattacks, or natural disasters.
- Achieved through redundancy, backup systems, and disaster recovery plans.
- Crucial for business continuity, uninterrupted services, and user satisfaction.

Purpose of CIA Triad

Confidentiality:

Purpose: Ethical hackers aim to ensure that sensitive data remains confidential.

Role: By assessing and identifying vulnerabilities that could lead to unauthorized access, ethical hackers help organizations strengthen confidentiality controls. They ensure that only authorized individuals can access sensitive information.

Integrity:

Purpose: Ethical hackers work to maintain the integrity of data and systems.

Role: They assess systems to detect vulnerabilities that might allow unauthorized alterations or tampering with data. By identifying these weaknesses, they help organizations implement safeguards to maintain data accuracy and reliability.

Availability:

Purpose: Ethical hackers strive to ensure that systems and data are available when needed.

Role: By identifying vulnerabilities that could lead to system downtime or unavailability, ethical hackers help organizations strengthen their availability controls. This includes measures to prevent and mitigate denial-of-service attacks and other disruptions.

Importance of CIA Triad

- Guides ethical hackers to assess and enhance data protection comprehensively.
- Ensures a balanced focus on confidentiality, integrity, and system availability.
- Forms the foundation for ethical hacking assessments and security audits.
- Helps identify vulnerabilities, reduce risks, and fortify cybersecurity defenses.

CIA Triad:-

Example of Confidentiality

❖ *Imagine an e-commerce company that wants to ensure the security of its online shopping platform, which handles sensitive customer information, including personal details and payment information.*

❑ ***Scenario :-***

The ethical hacker is tasked with assessing the confidentiality of customer data on the e-commerce website. They perform penetration testing and discover a vulnerability in the website's login system.

❑ ***Action :-***

The hacker exploits this vulnerability, gaining unauthorized access to a database containing customer profiles and payment details. This highlights a potential breach of confidentiality.

❑ ***Solution :-***

The ethical hacker immediately reports their findings to the e-commerce company, which promptly fixes the vulnerability by strengthening the login system, implementing encryption, and enhancing access controls. This ensures that customer data remains confidential and accessible only to authorized users.

CIA Triad:-

Example of Integrity

❖ *Imagine an e-commerce company that wants to ensure the security of its online shopping platform, which handles sensitive customer information, including personal details and payment information.*

❑ ***Scenario :-***

During penetration testing, the ethical hacker identifies another vulnerability that allows them to manipulate product prices on the website, potentially causing financial losses and damaging the integrity of the platform.

❑ ***Action :-***

The hacker alters the prices of several products, demonstrating that unauthorized individuals could tamper with the website's data.

❑ ***Solution :-***

The e-commerce company takes immediate action to resolve this issue by implementing data integrity checks and auditing mechanisms. They also introduce additional security layers to prevent unauthorized data alterations, preserving the integrity of product information.

CIA Triad:-

Example of Availability

- *Imagine an e-commerce company that wants to ensure the security of its online shopping platform, which handles sensitive customer information, including personal details and payment information.*

- ***Scenario :-***

  The ethical hacker simulates a Distributed Denial of Service (DDoS) attack against the e-commerce website, overwhelming its servers and making the site inaccessible to legitimate users.

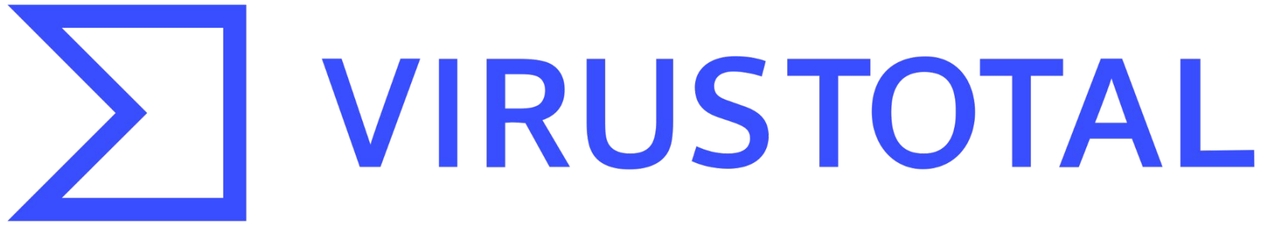
- ***Action :-***

  The hacker conducts a DDoS attack to assess how the website responds under such circumstances, causing temporary unavailability.

- ***Solution :-***

  In response, the e-commerce company strengthens its infrastructure by implementing DDoS mitigation tools and services. This ensures that even during a real attack, the website remains available to customers, enhancing the availability of the platform.

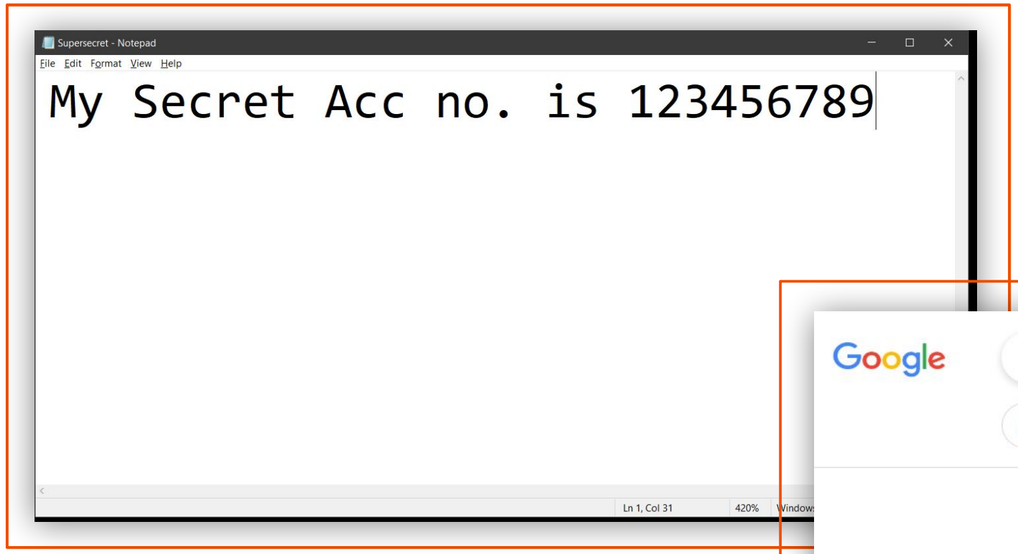
CIA Integrity Practical with Virus Total

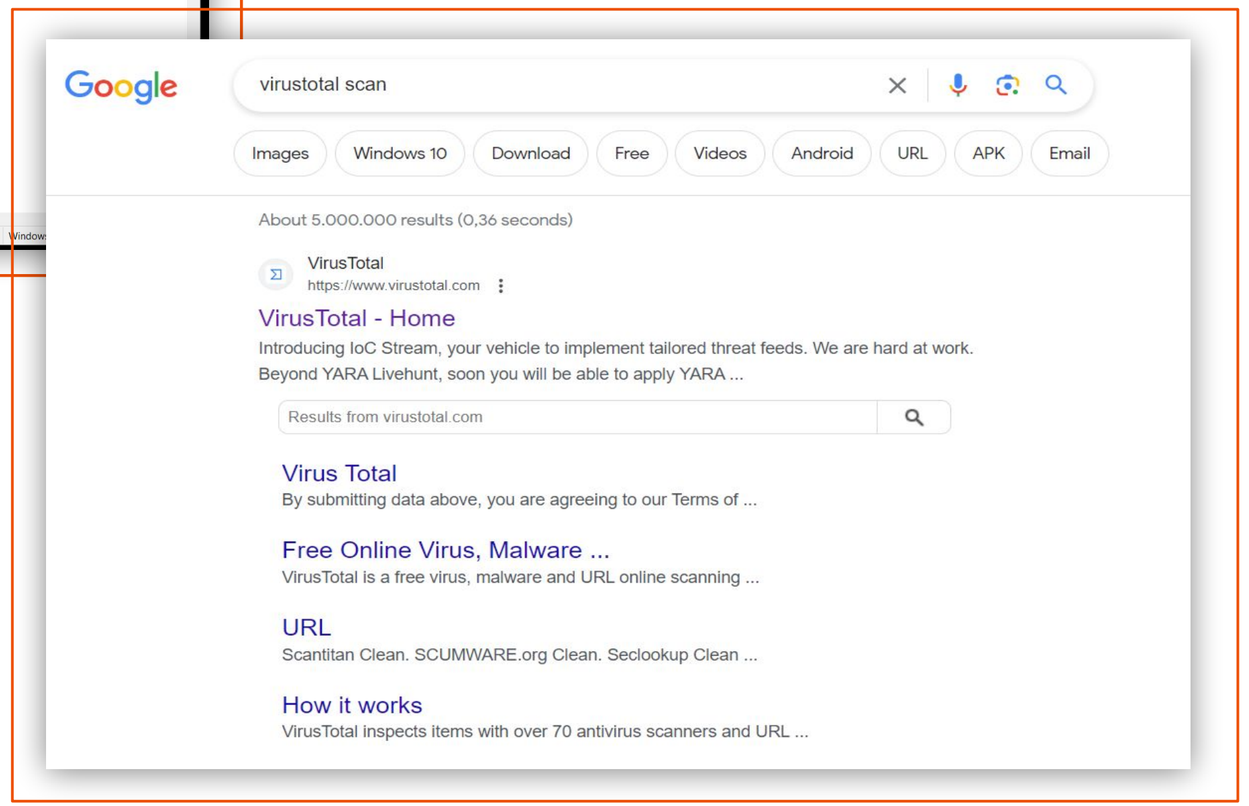


VirusTotal is an online service for scanning files and URLs.

It checks for malware using multiple antivirus engines simultaneously.

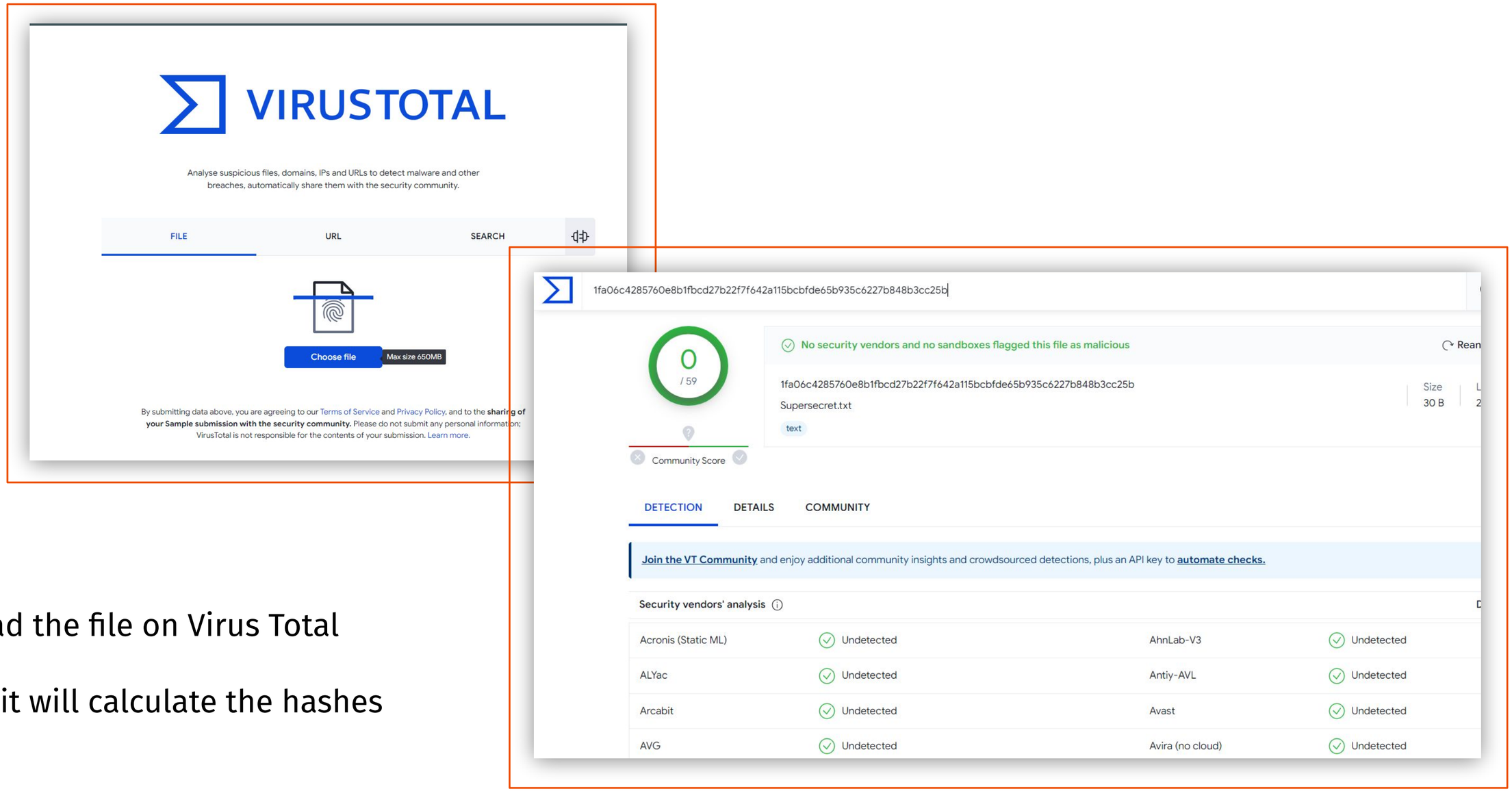
CIA Integrity Practical with Virus Total





- ➔ Firstly Create A file and write your secret code.
- ➔ Then visit Virus Total Website.

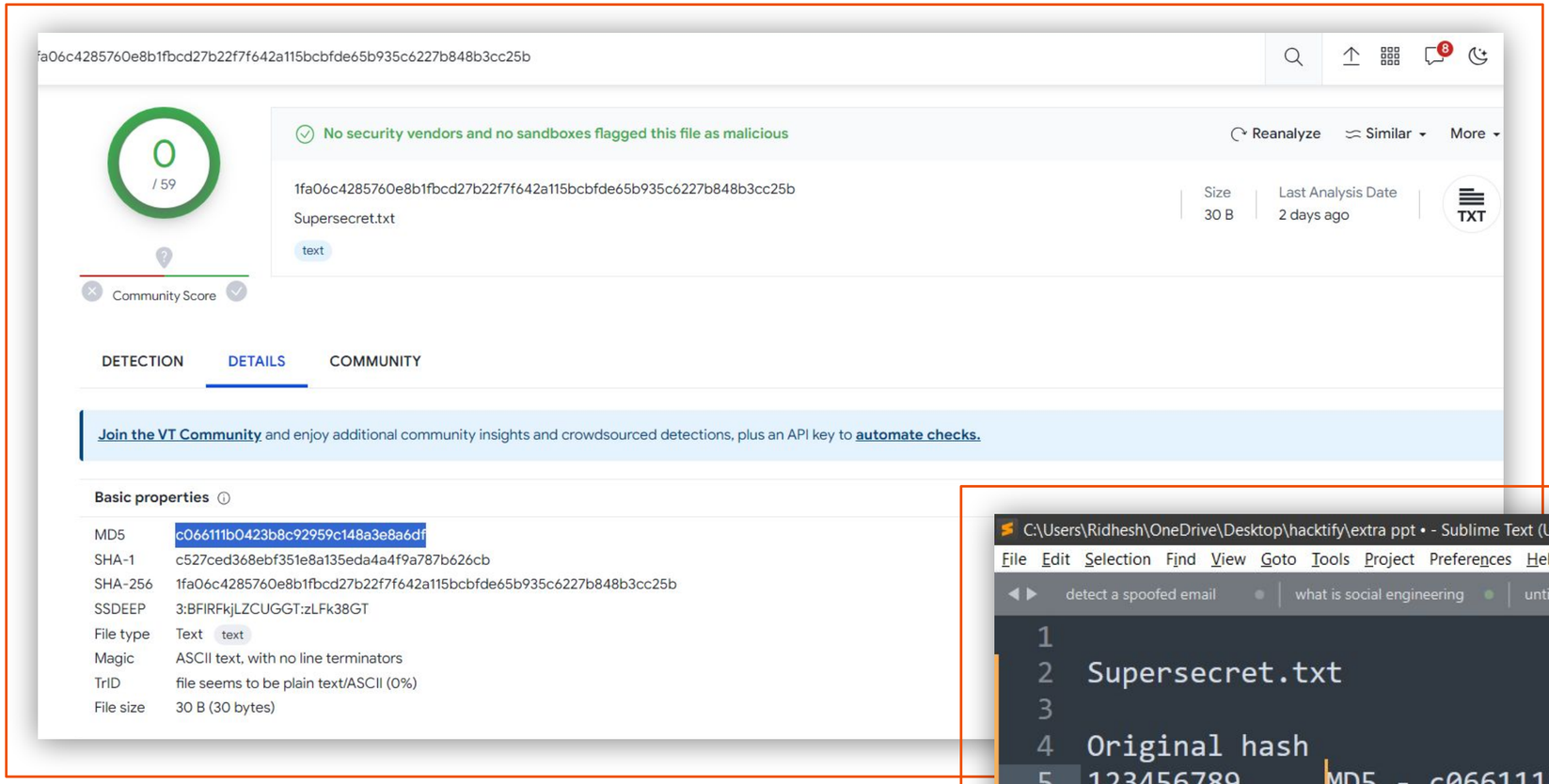
CIA Integrity Practical with Virus Total

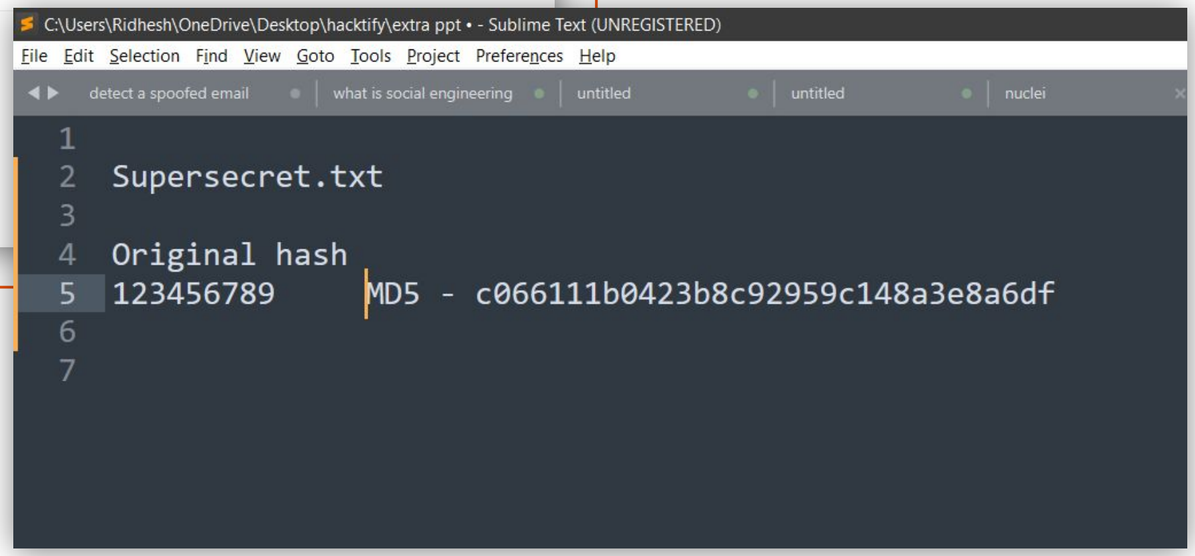


➔ Upload the file on Virus Total

➔ Then it will calculate the hashes

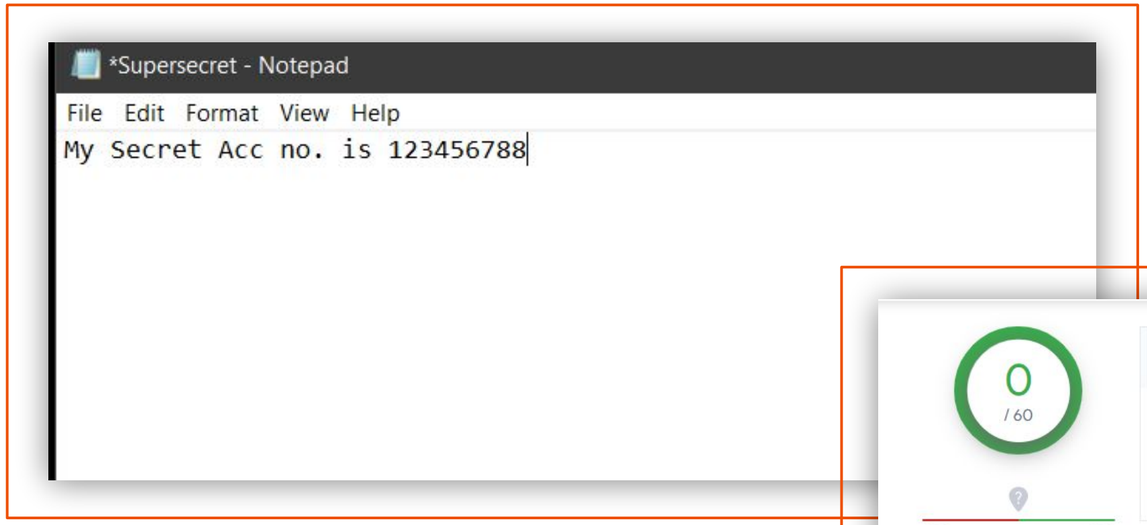
CIA Integrity Practical with Virus Total

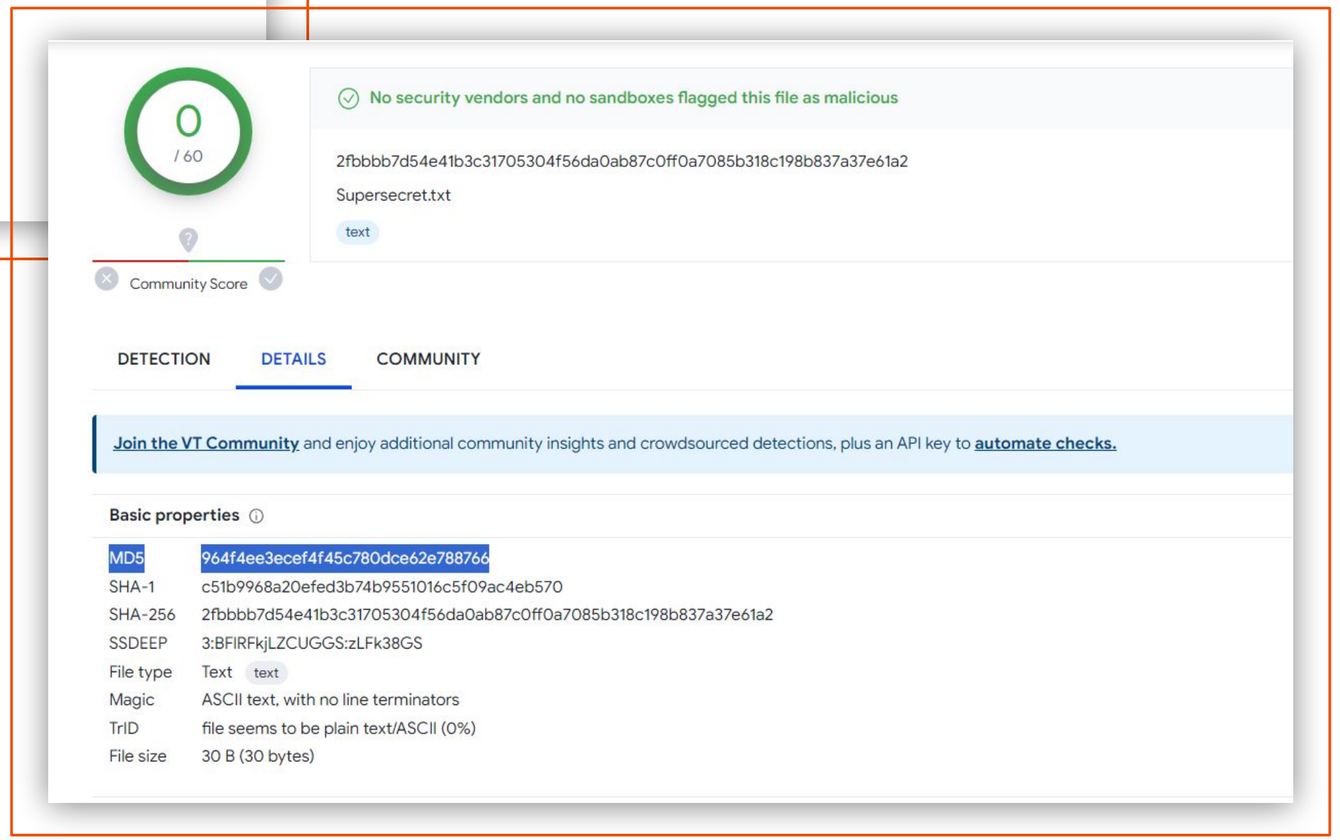




- ➔ Once the Scan is Complete we can see the MD5 Hash
- ➔ We'll copy and paste in sublime

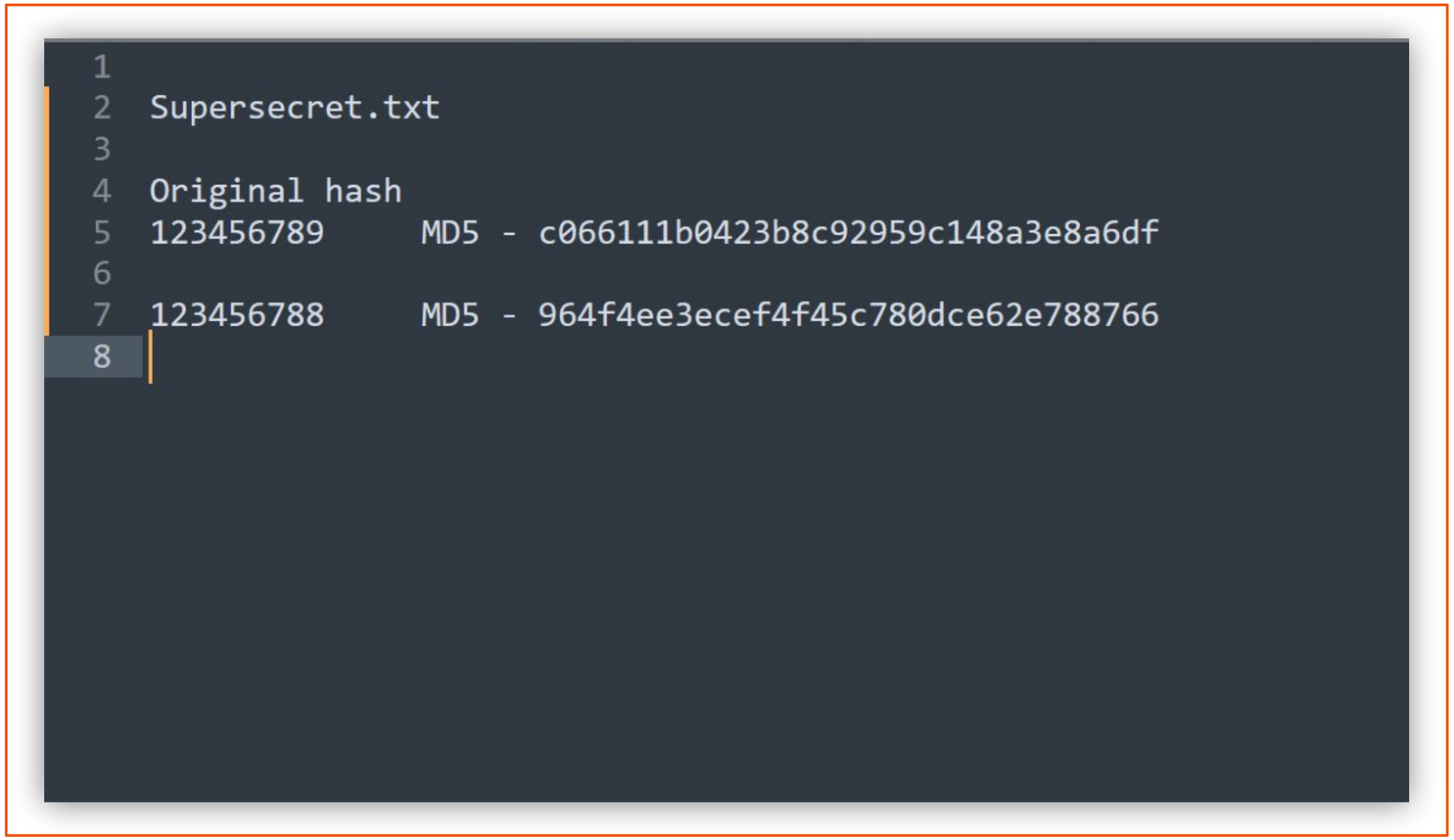
CIA Integrity Practical with Virus Total





- ➔ Now i'll change my Secret Acc no. and upload for scanning.
- ➔ You can see the hash of this file has been changed.

CIA Integrity Practical with Virus Total



➔ You can see in this Image, hash of both the file is Different.

CIA Integrity Practical with Virus Total

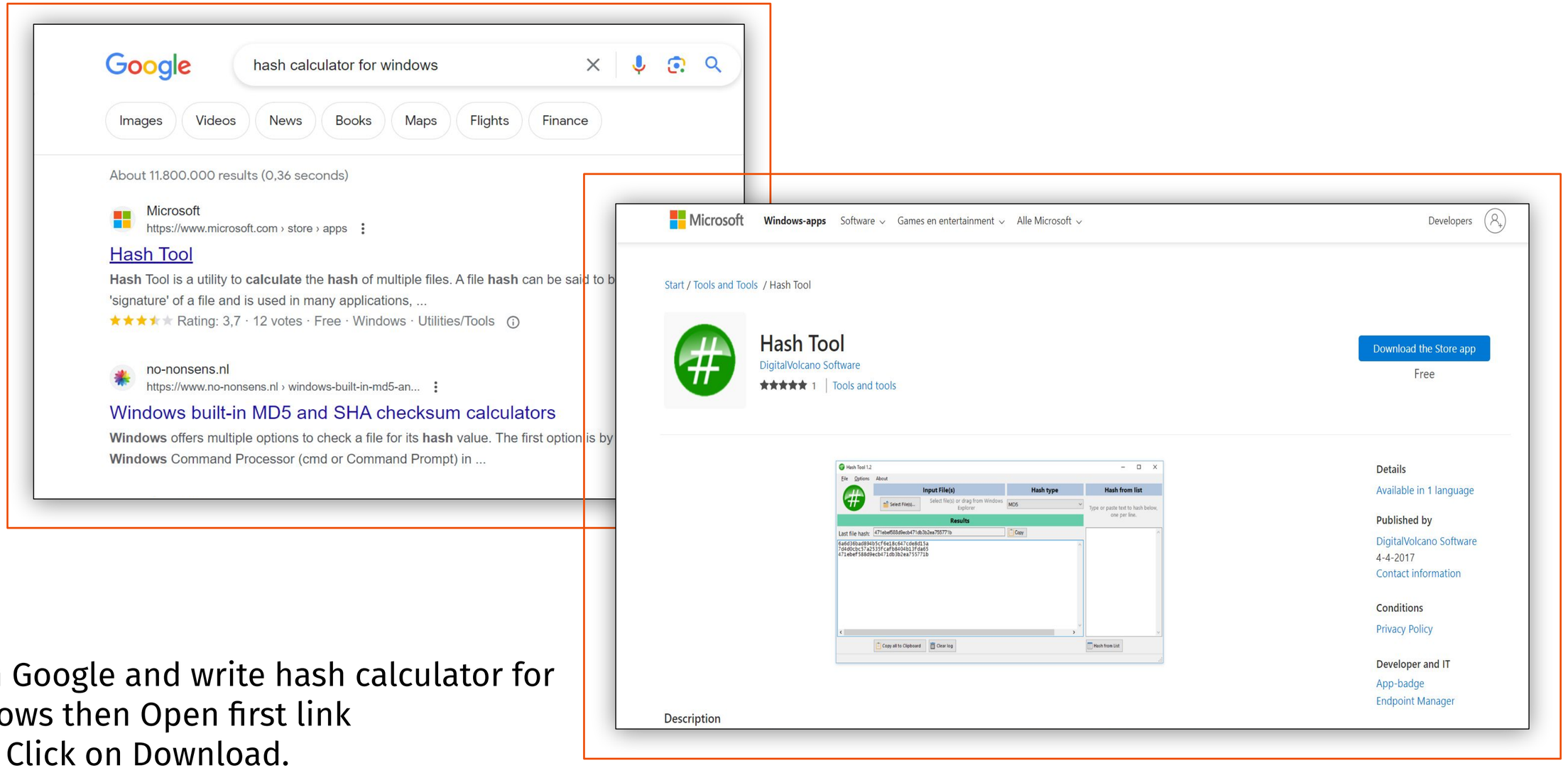
Surprise Test:-

- *Now if I modify the 2 nd file to 123456789 then the hash im going to get will be same as the first Original Hash?*

➔ *The New Hash will Generate.*

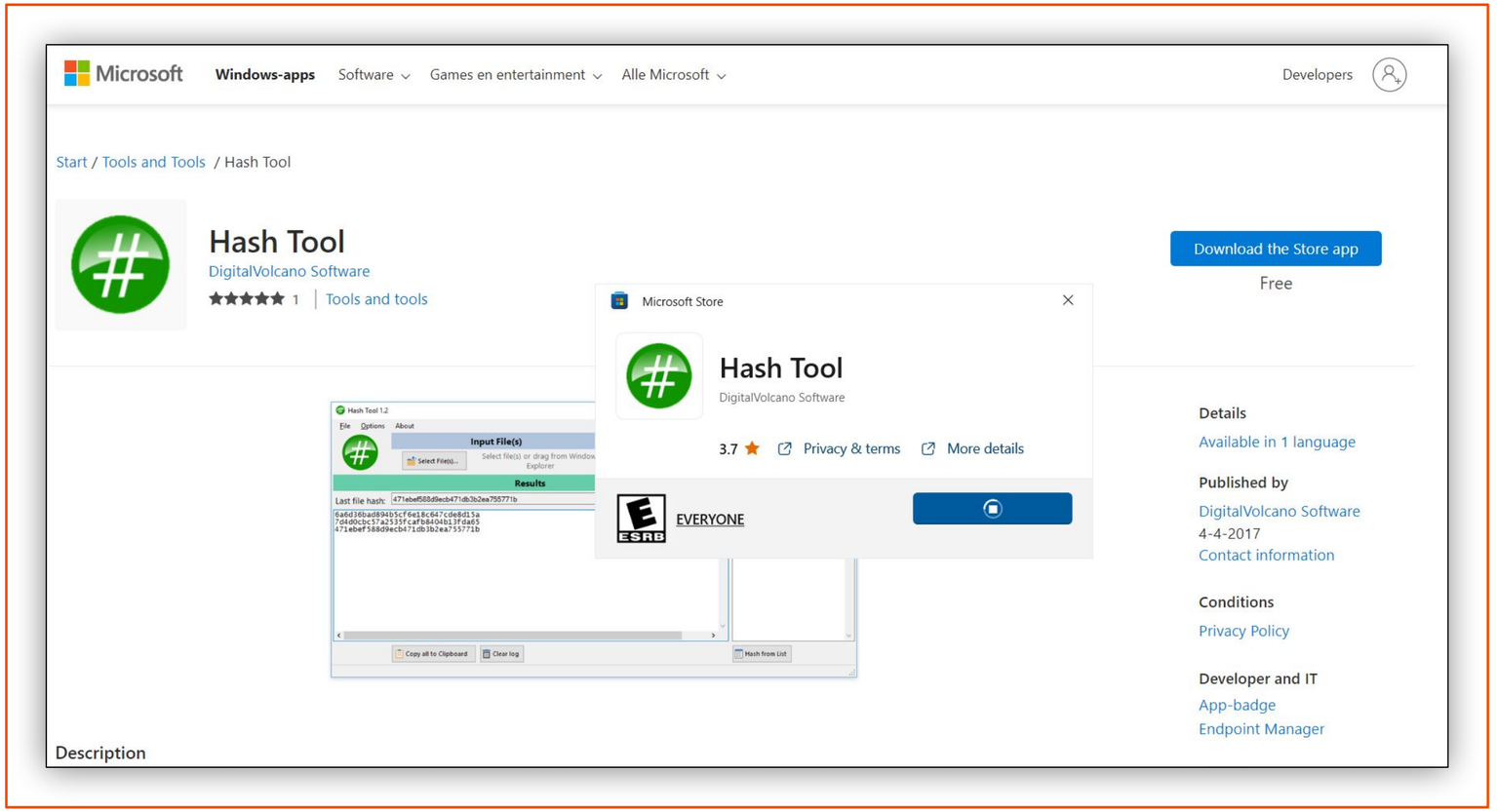
➔ *The Hash will be same as the First Original Hash.*

CIA Integrity Practical with Hash Cal



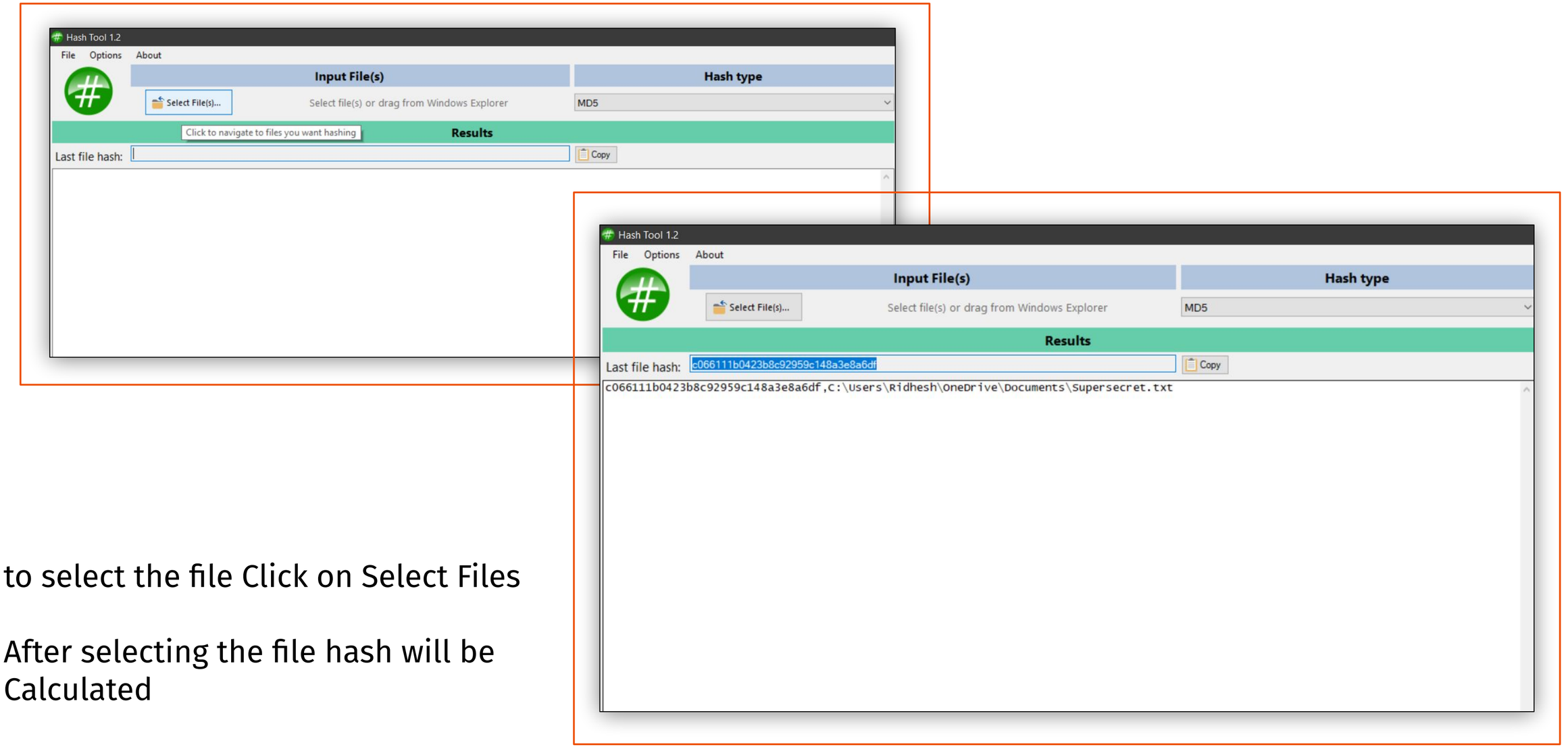
- ➔ Open Google and write hash calculator for windows then Open first link
- ➔ Then Click on Download.

CIA Integrity Practical with Hash Cal



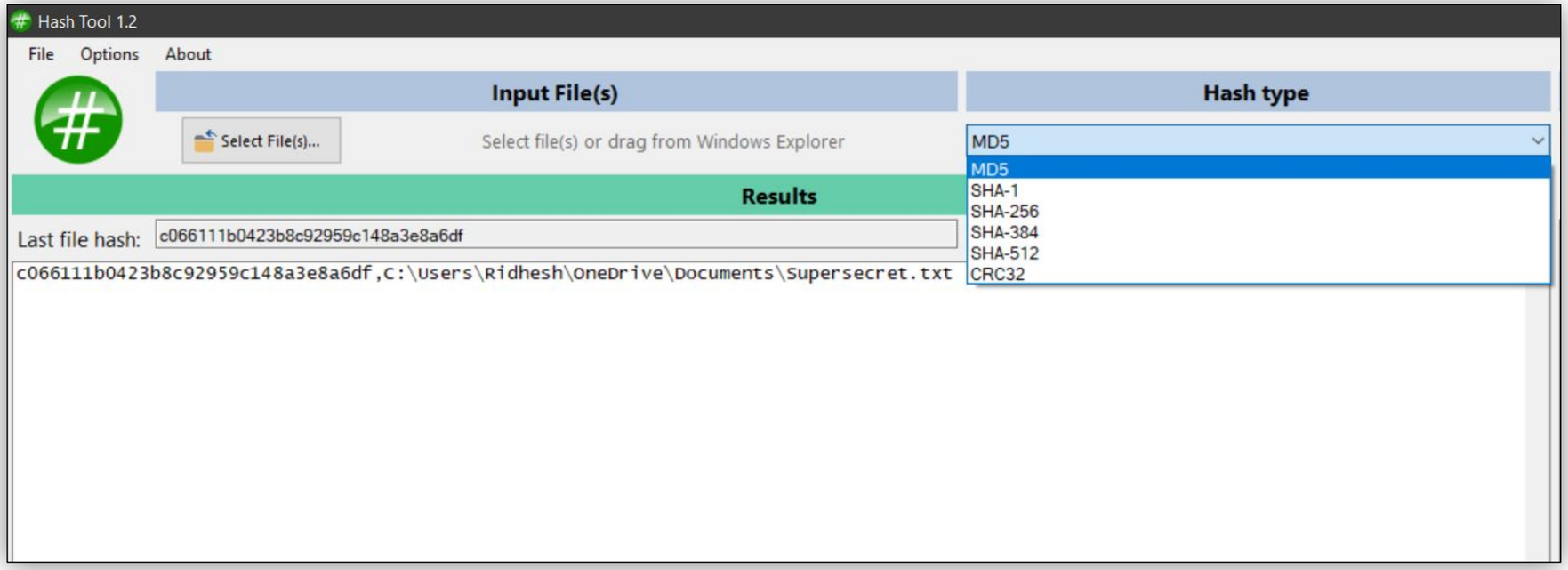
➔ Pop up will Came then Click on Download.

CIA Integrity Practical with Hash Cal



- ➔ to select the file Click on Select Files
- ➔ After selecting the file hash will be Calculated

CIA Integrity Practical with Hash Cal



➔ We can also select the Hash type.

4

Some Basic Terminology

Ethical Hacker (White Hat Hacker)

- *Security professional authorized to test and improve system defenses.*
- *Identifies vulnerabilities before malicious hackers and suggests countermeasures.*
- *Operates within legal and ethical boundaries to enhance cybersecurity.*
- *Helps organizations protect data, systems, and networks from cyber threats.*

Vulnerability

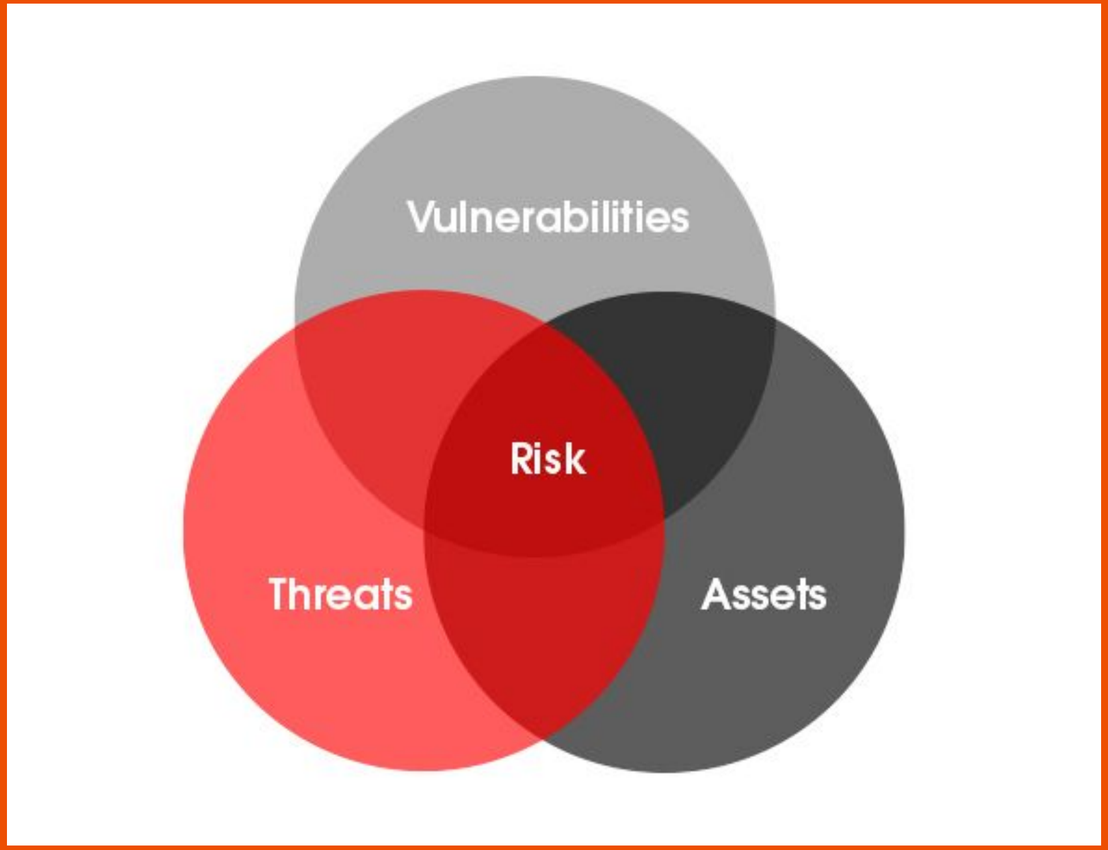
- *Weakness or flaw in a system that can be exploited.*
- *Creates potential entry points for attackers to compromise security.*
- *Ethical hackers find and remediate vulnerabilities to enhance protection.*
- *Vulnerabilities may exist in software, hardware, or human processes.*

Threat

- *Potential danger or harm that may exploit vulnerabilities.*
- *Can be external or internal, intentional or accidental.*
- *Ethical hackers assess threats to identify and mitigate risks.*
- *Threats include malware, hackers, and natural disasters.*

Risk

- *The likelihood of a threat exploiting a vulnerability's impact.*
- *Ethical hackers assess and manage risks to secure organizations effectively.*
- *Balances potential damage with the cost of preventive measures.*
- *Informs decisions on security investments and risk mitigation strategies.*



Penetration Testing

- *Controlled, simulated cyberattacks to assess security weaknesses.*
- *Ethical hackers mimic real-world threats to find and fix vulnerabilities.*
- *Provides insights into system readiness and response to attacks.*
- *Enhances security posture and prepares for potential breaches.*

Vulnerability Assessment

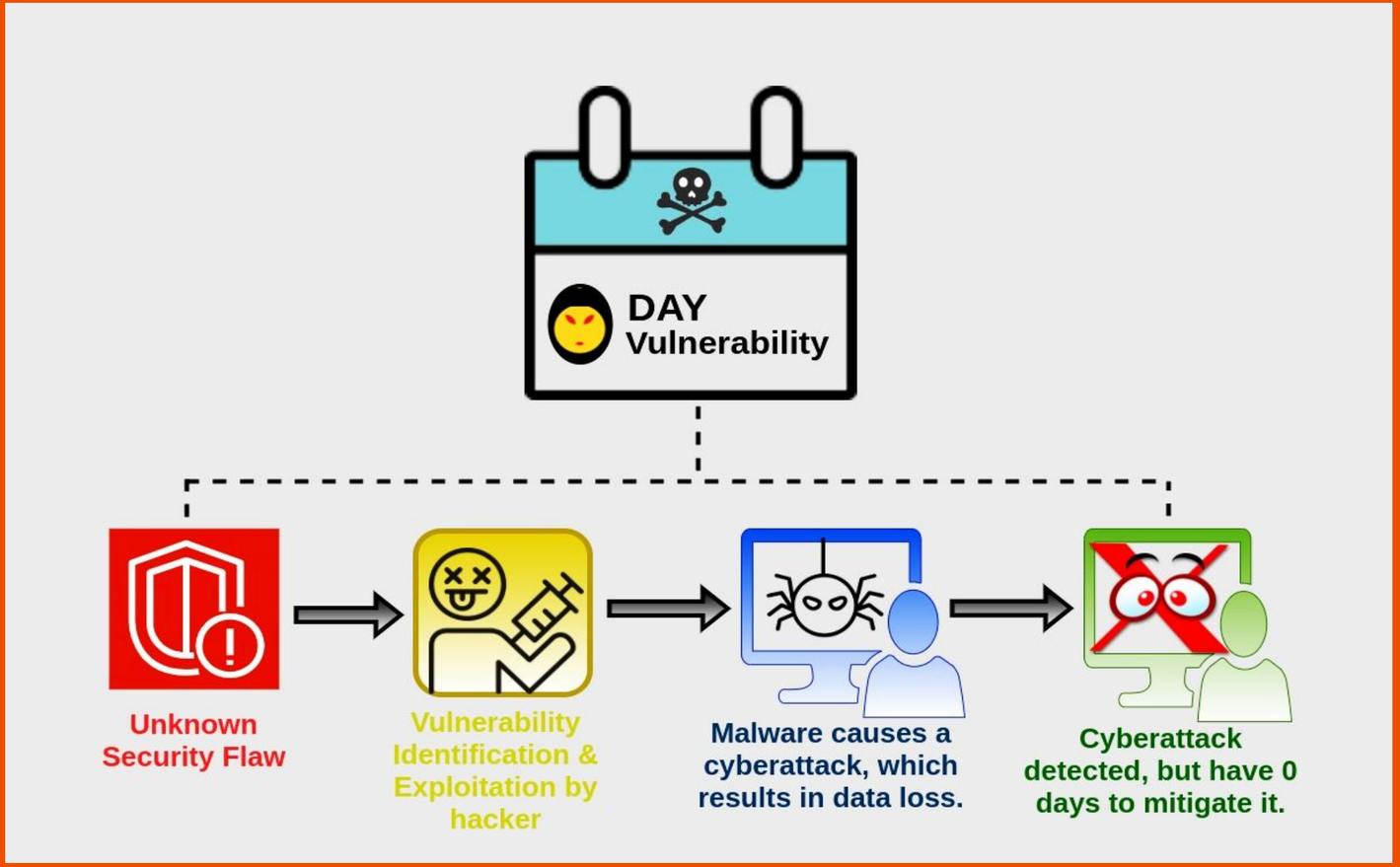
- *Systematic evaluation to identify and prioritize security vulnerabilities.*
- *Ethical hackers use tools and methods to assess weaknesses comprehensively.*
- *Helps organizations understand their risk exposure and plan improvements.*
- *The initial step before implementing security measures.*

Exploit

- *Weakness or flaw in software or system.*
- *Can be exploited, compromising security.*
- *Requires patching or mitigation.*
- *Can lead to breaches or system compromise.*

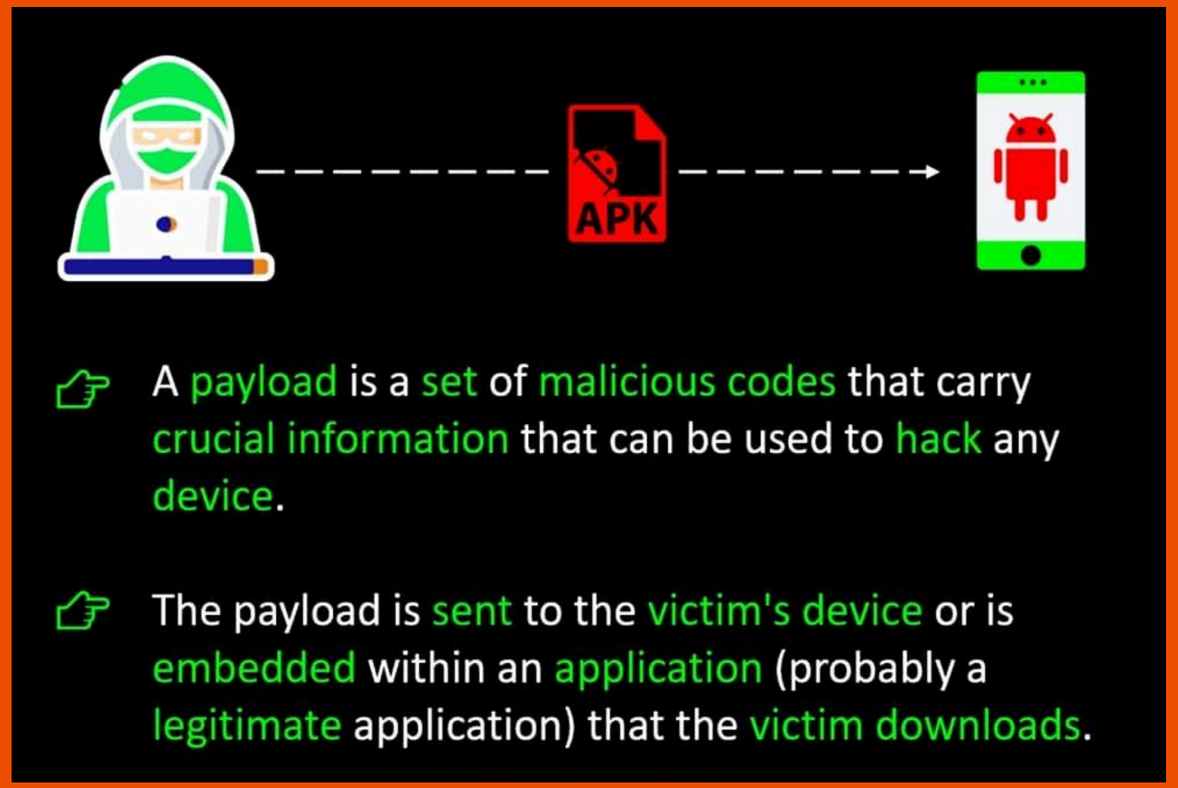
Zero-Day Vulnerability

- *Newly discovered, undisclosed software weakness.*
- *No patch or defense available.*
- *Attractive target for hackers.*
- *Can cause significant damage if exploited.*



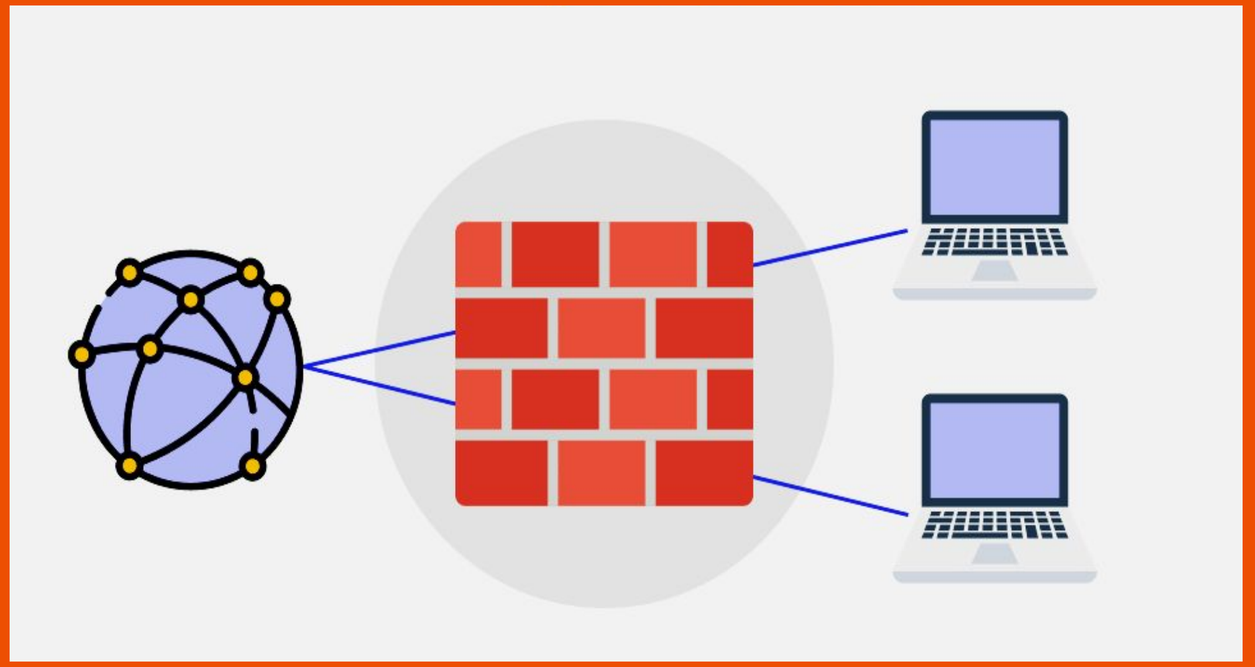
Payload

- *Malicious code or data delivered by an attacker's exploit.*
- *Carries out the intended attack, such as malware installation or data theft.*
- *Ethical hackers analyze payloads to understand attack techniques.*
- *Developing countermeasures often involves studying payload behavior.*



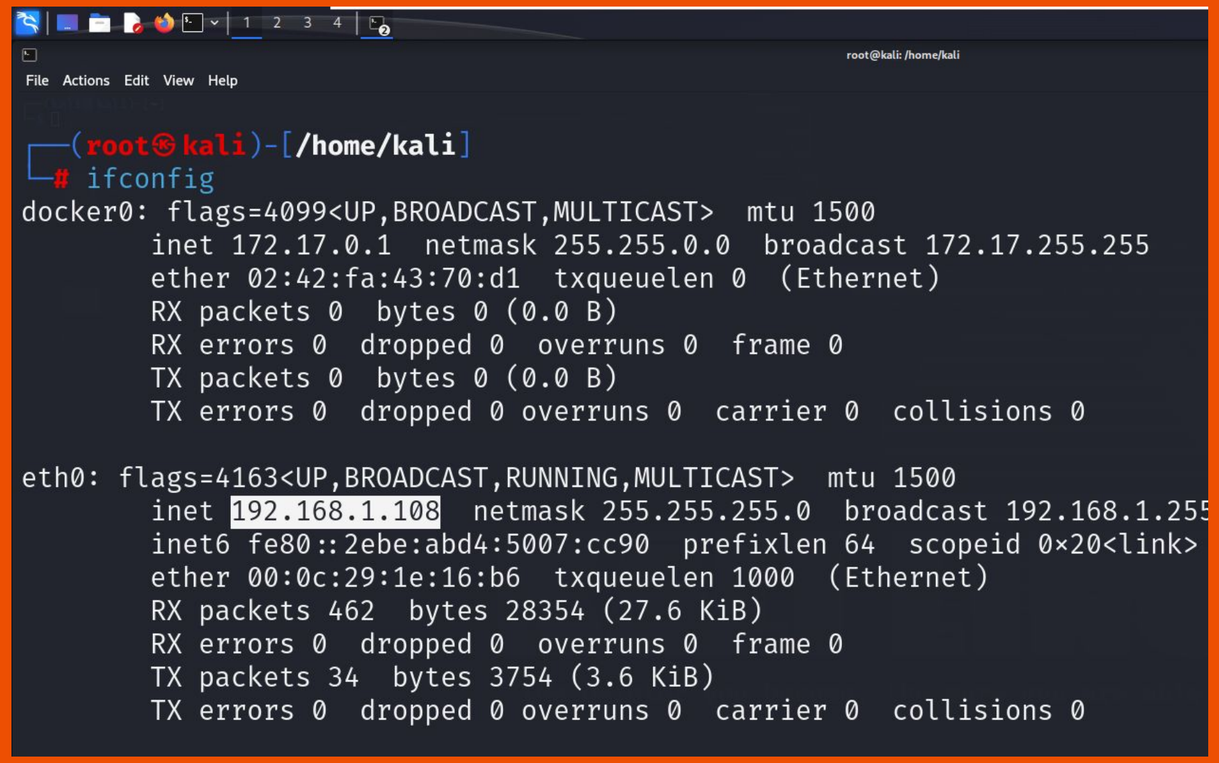
Firewall

- *Network security device that filters incoming and outgoing traffic.*
- *Sets rules to allow or block data based on predefined criteria.*
- *Ethical hackers test firewalls to ensure proper configuration and effectiveness.*
- *Firewalls protect against unauthorized access and threats.*



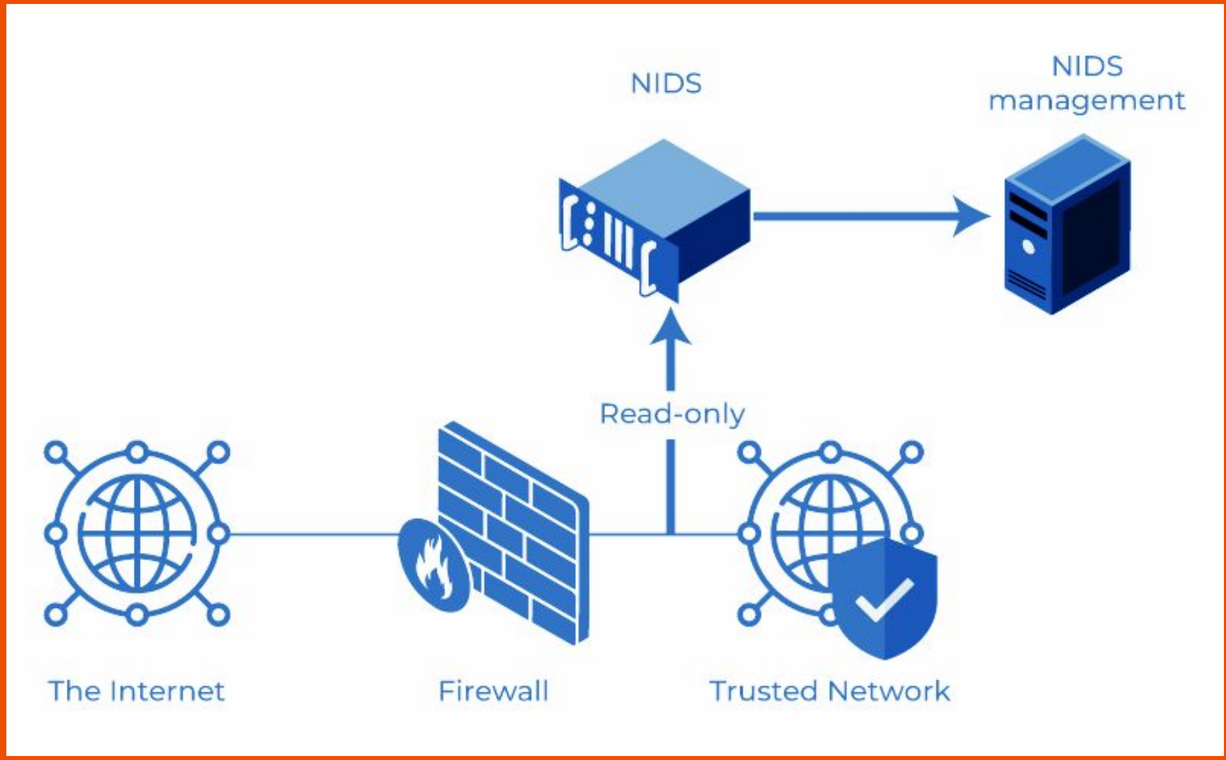
IP Address

- *Unique numerical label for devices in computer networks.*
- *Identifies sender/receiver.*
- *IPv4 (32-bit) and IPv6 (128-bit) versions exist.*
- *Essential for routing data packets on the internet.*
- *Command:- ipconfig (Windows), ifconfig (linux)*



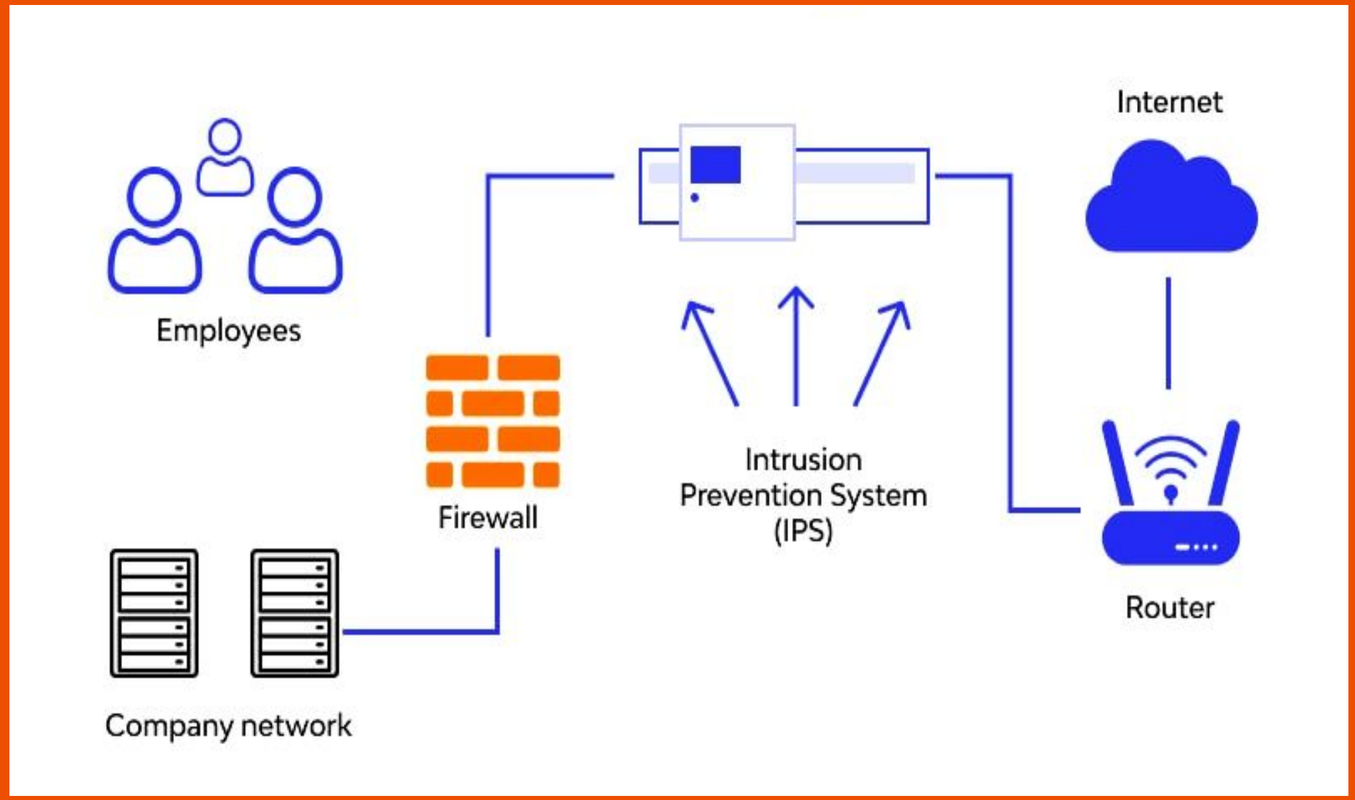
Intrusion Detection System (IDS)

- *Monitors network or system activities for suspicious or malicious behavior.*
- *Alerts security teams to potential threats in real-time.*
- *Ethical hackers assess IDS to enhance detection and response capabilities.*
- *An essential component of proactive security measures.*



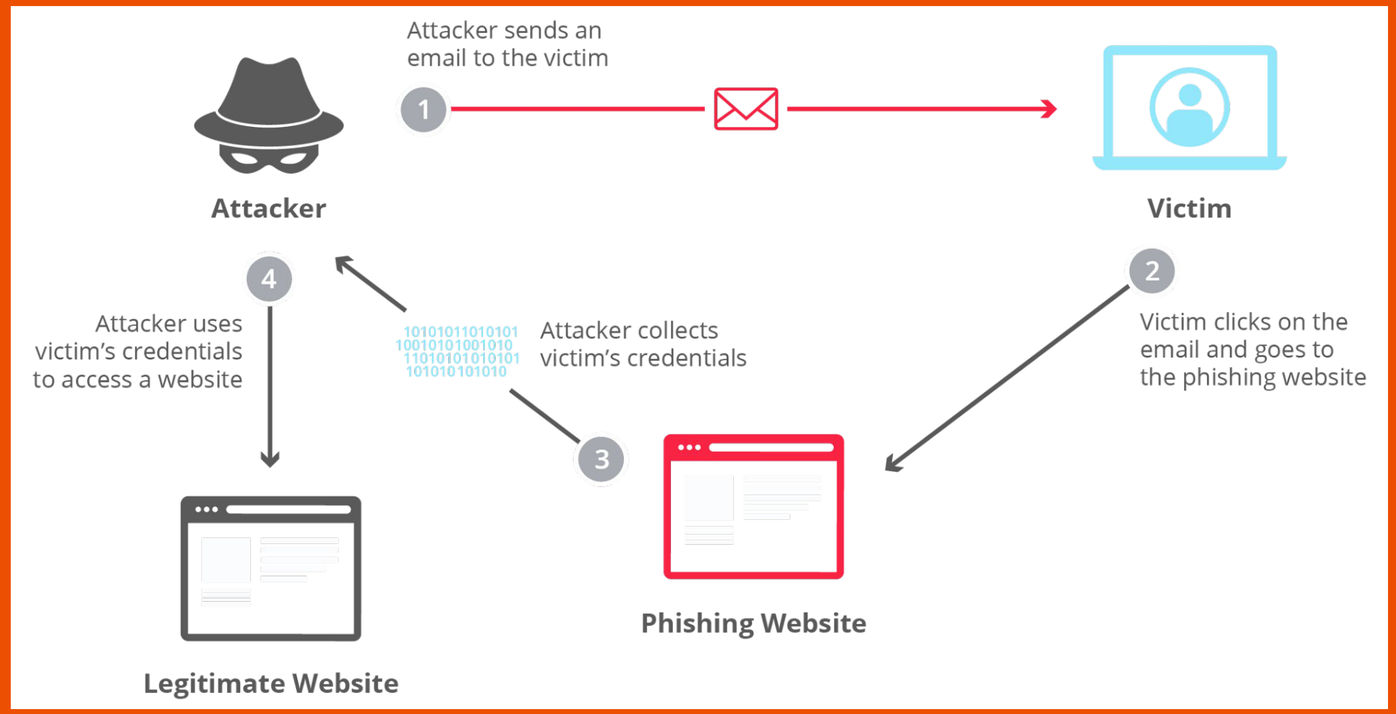
Intrusion Prevention System (IPS)

- *Security system that detects and blocks network threats.*
- *Monitors and responds to suspicious network activities.*
- *Prevents unauthorized access and cyberattacks.*
- *Enhances network security and mitigates risks.*



Phishing

- *Deceptive tactics to trick individuals into revealing sensitive information*
- *Often involves fraudulent emails, websites, or messages impersonating trusted entities.*
- *Ethical hackers simulate phishing attacks to educate and improve defenses.*
- *Awareness and training help users recognize and avoid phishing attempts.*

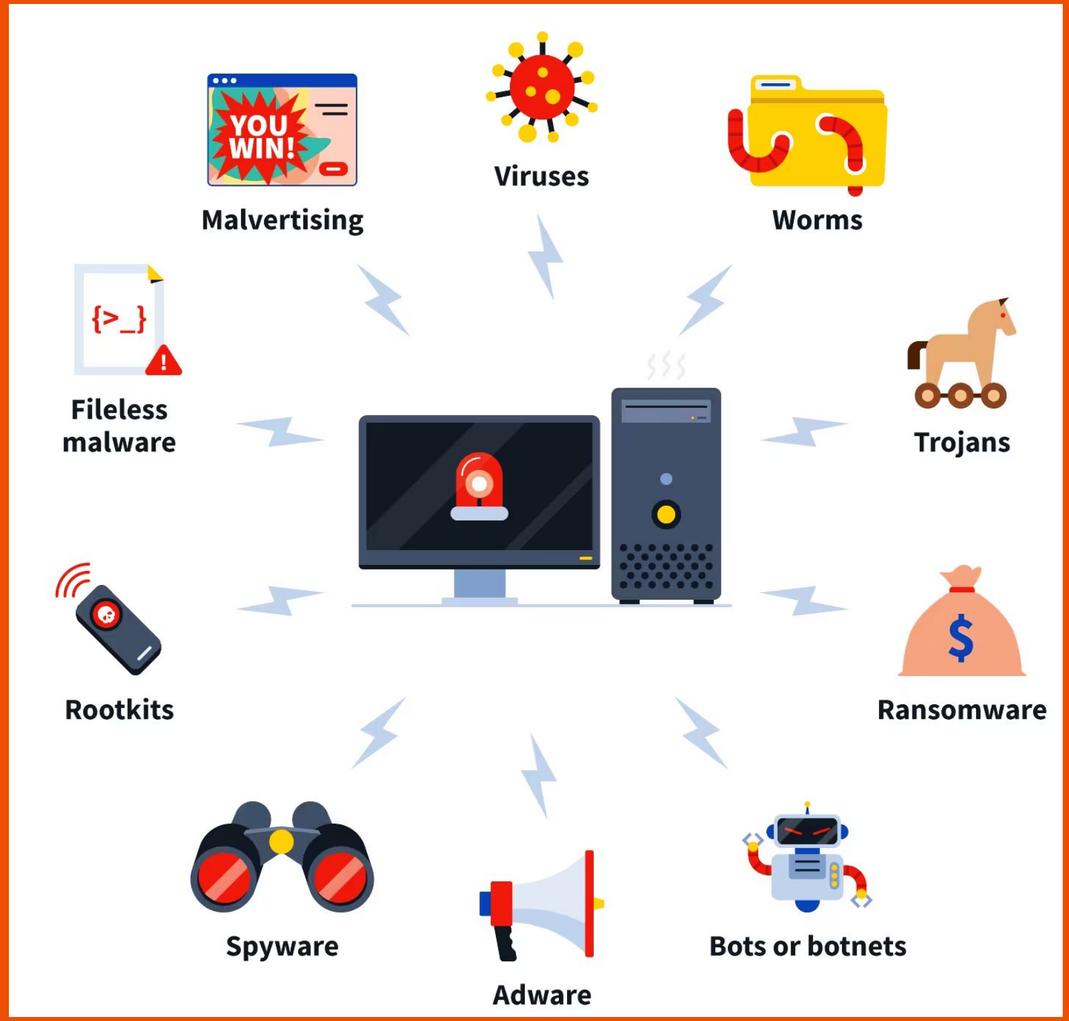


Social Engineering

- *Manipulative techniques used to deceive individuals into divulging confidential information.*
- *Exploits human psychology rather than technical vulnerabilities.*
- *Ethical hackers assess and educate against social engineering threats.*
- *Effective defense includes user awareness and security policies.*

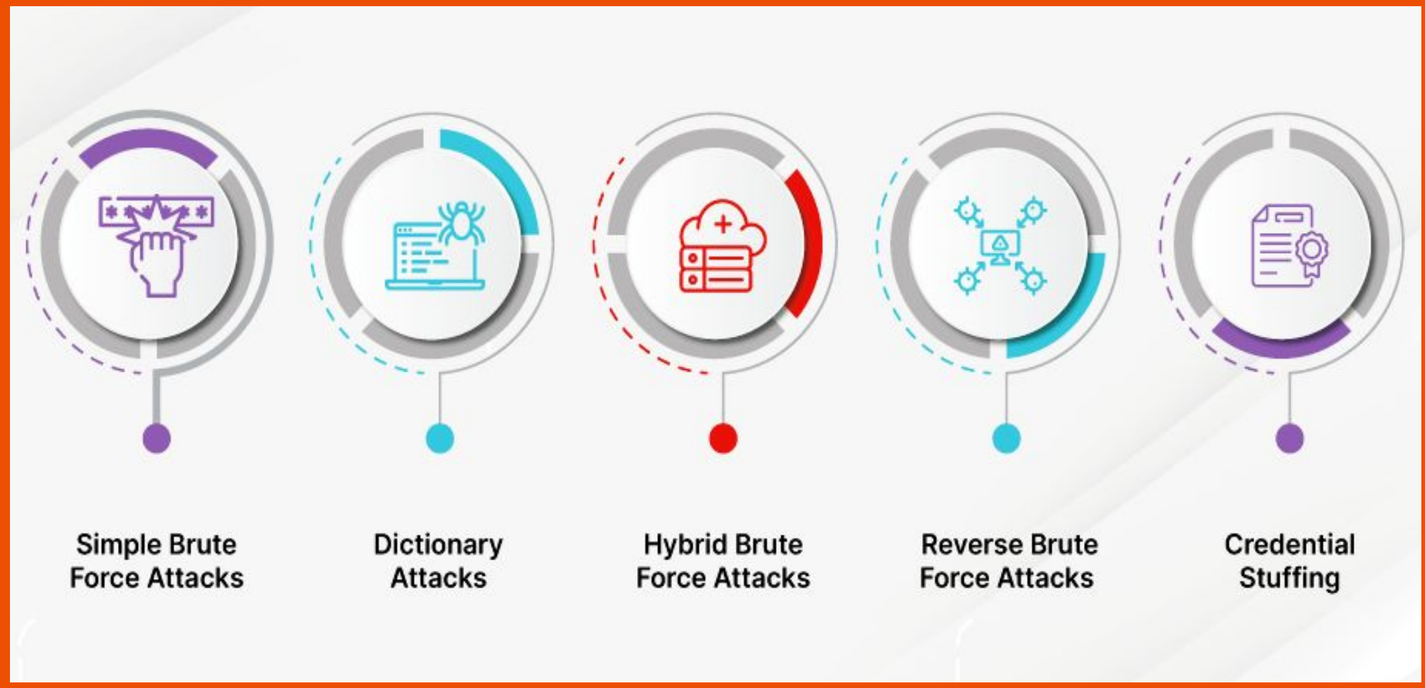
Malware

- *Malicious software designed to harm or compromise systems.*
- *Includes viruses, worms, Trojans, ransomware, and spyware.*
- *Ethical hackers analyze and combat malware to protect systems.*
- *Combating malware involves detection, removal, and prevention strategies.*



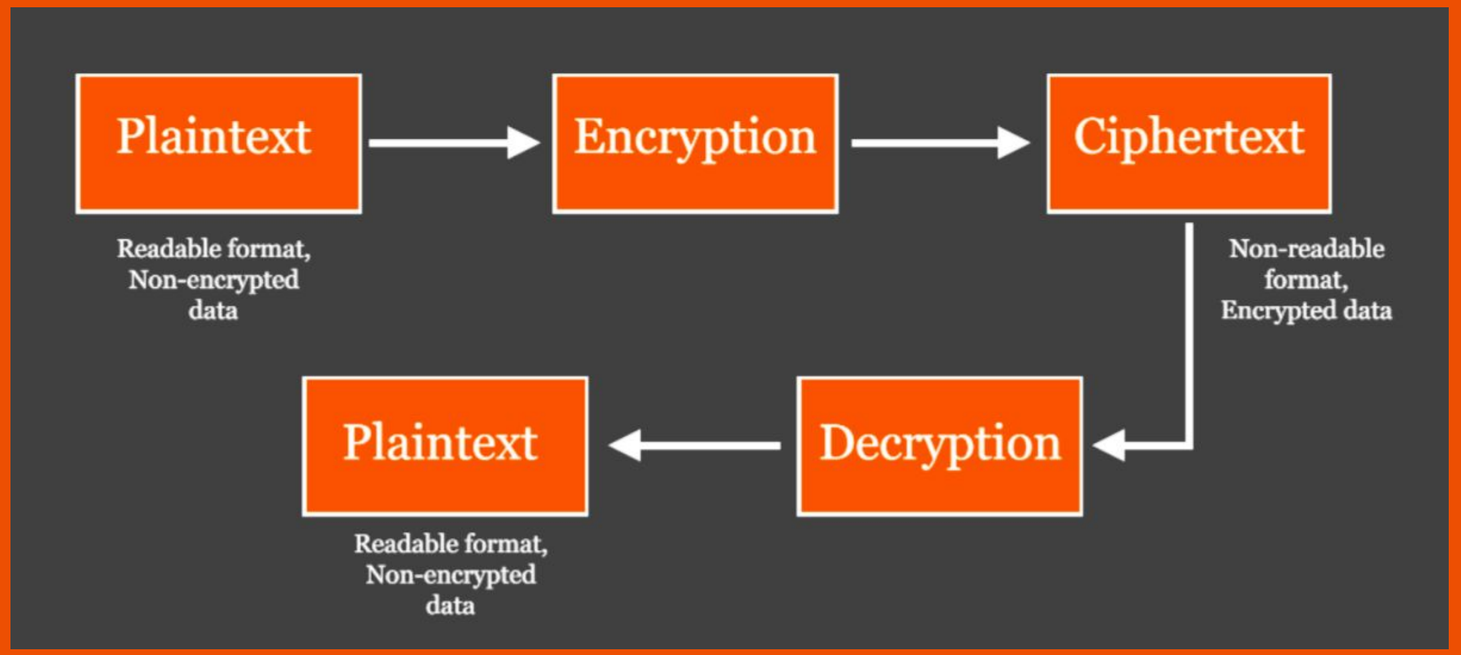
Brute Force Attack

- *Repeated, automated attempts to guess passwords or encryption keys.*
- *Ethical hackers test for weak access controls and recommend improvements.*
- *Targets login pages, encryption, or authentication systems.*
- *Effective security measures include strong passwords and account lockouts.*



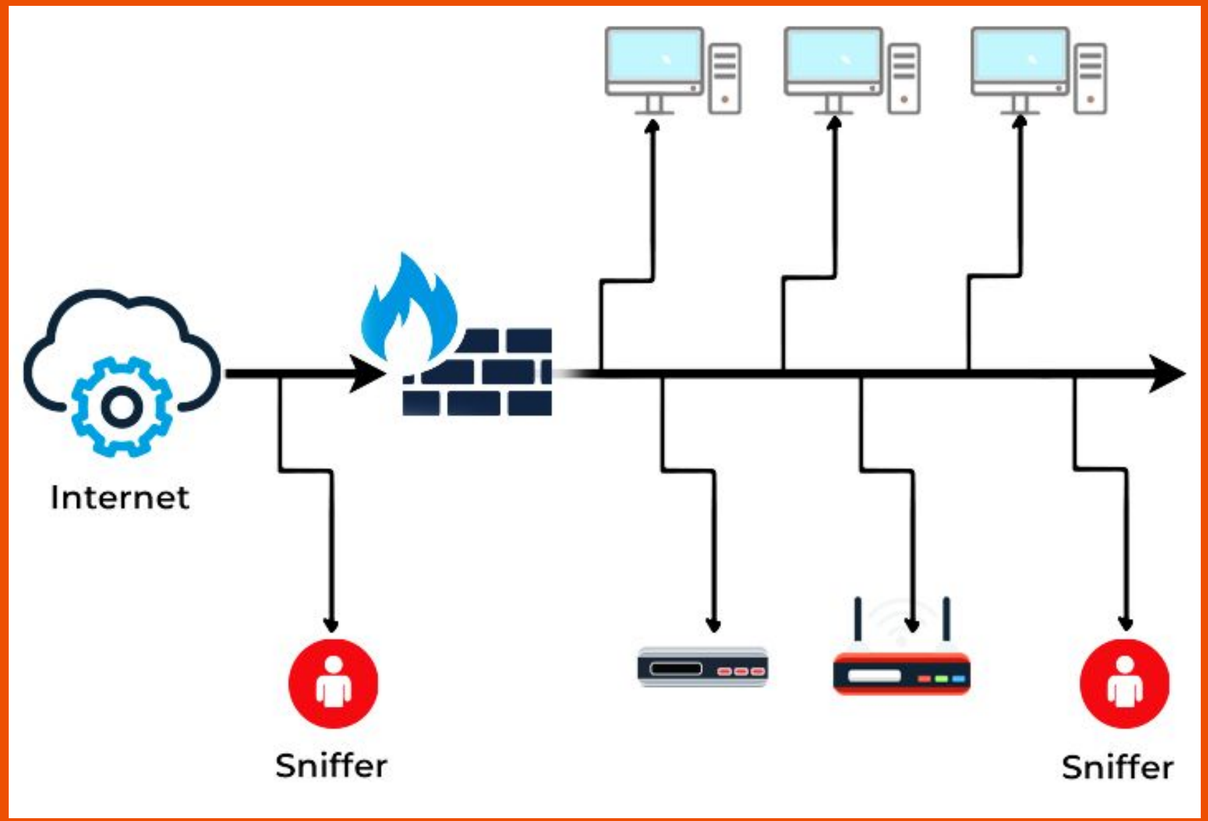
Cryptography

- *Techniques for secure communication and data protection using encryption.*
- *Ethical hackers assess encryption methods for vulnerabilities and weaknesses.*
- *Protects data confidentiality and integrity from unauthorized access.*
- *Essential for secure data transmission and storage.*



Packet Sniffing

- *Intercepting and analyzing data packets in transit on a network.*
- *Ethical hackers use packet sniffing for network troubleshooting and security.*
- *Detects unauthorized data access and potential threats.*
- *Requires proper authorization and ethical use to avoid privacy violations.*



Patch

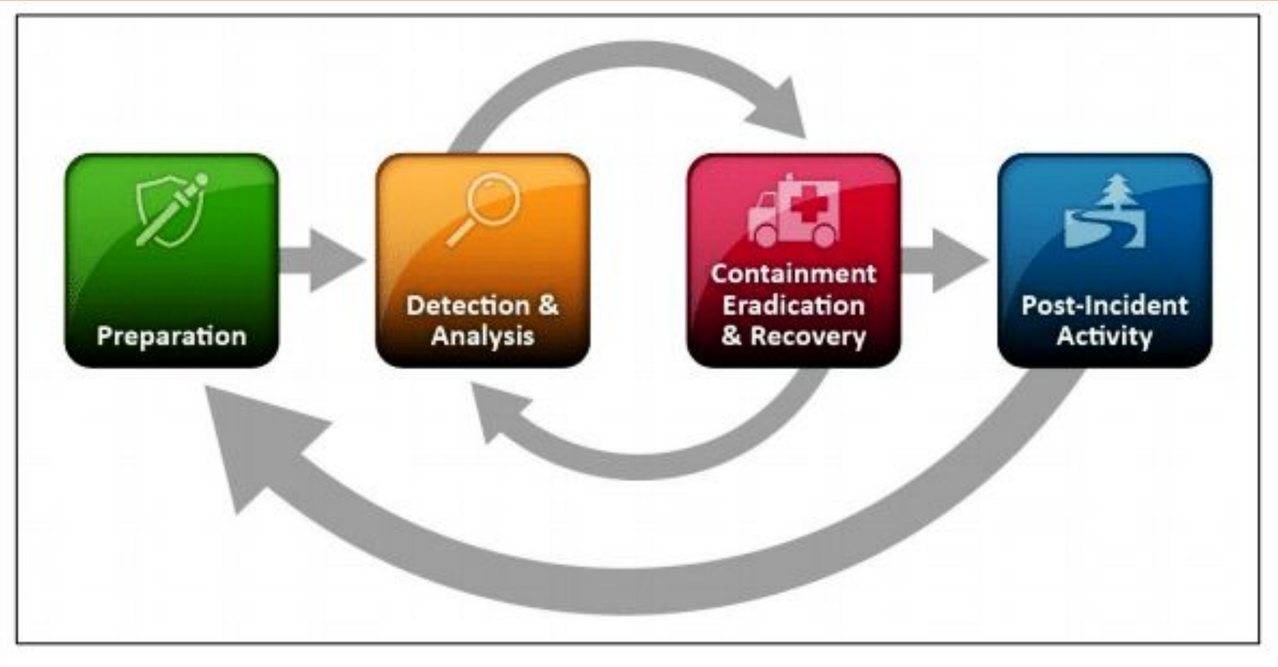
- *Software update or fix designed to address vulnerabilities and bugs.*
- *Ethical hackers recommend prompt patching to close security holes.*
- *Critical for maintaining system integrity and protection.*
- *Neglecting patches exposes systems to exploitation.*

Cyber Security Policy

- *Documented guidelines and procedures to protect an organization's digital assets.*
- *Defines roles, responsibilities, and security measures to mitigate risks.*
- *Ethical hackers align practices with policies to ensure compliance and security.*
- *Establishes a framework for security governance and risk management.*

Incident Response

- *Organized process for handling security incidents and breaches.*
- *Ethical hackers assist in incident response by investigating, containing, and mitigating.*
- *Minimizes damage, restores normal operations, and prevents future incidents.*
- *Rapid response is crucial to limit potential harm and data loss.*

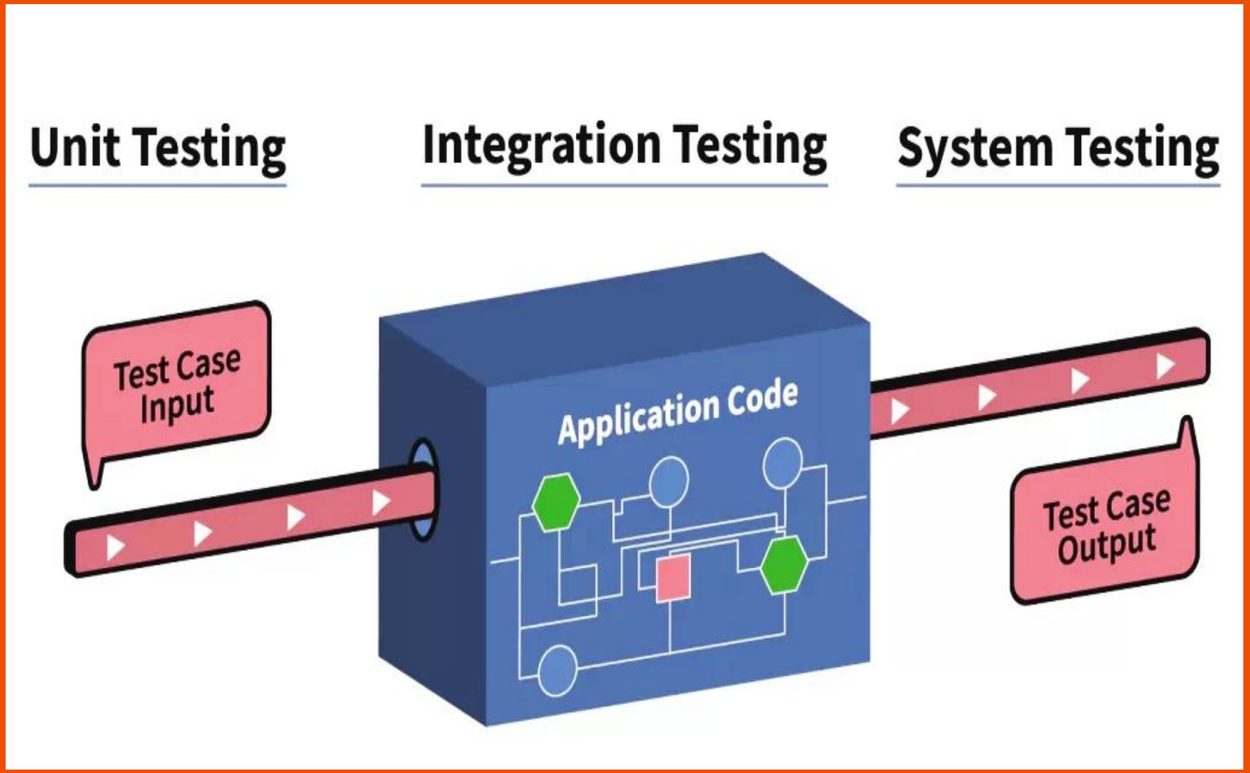


Black Box Testing

- *Assessment of a system without prior knowledge of its internal workings.*
- *Ethical hackers simulate external attacks to uncover vulnerabilities and weaknesses.*
- *Mimics the perspective of an external hacker.*
- *Evaluates the effectiveness of external defenses and security measures.*

White Box Testing

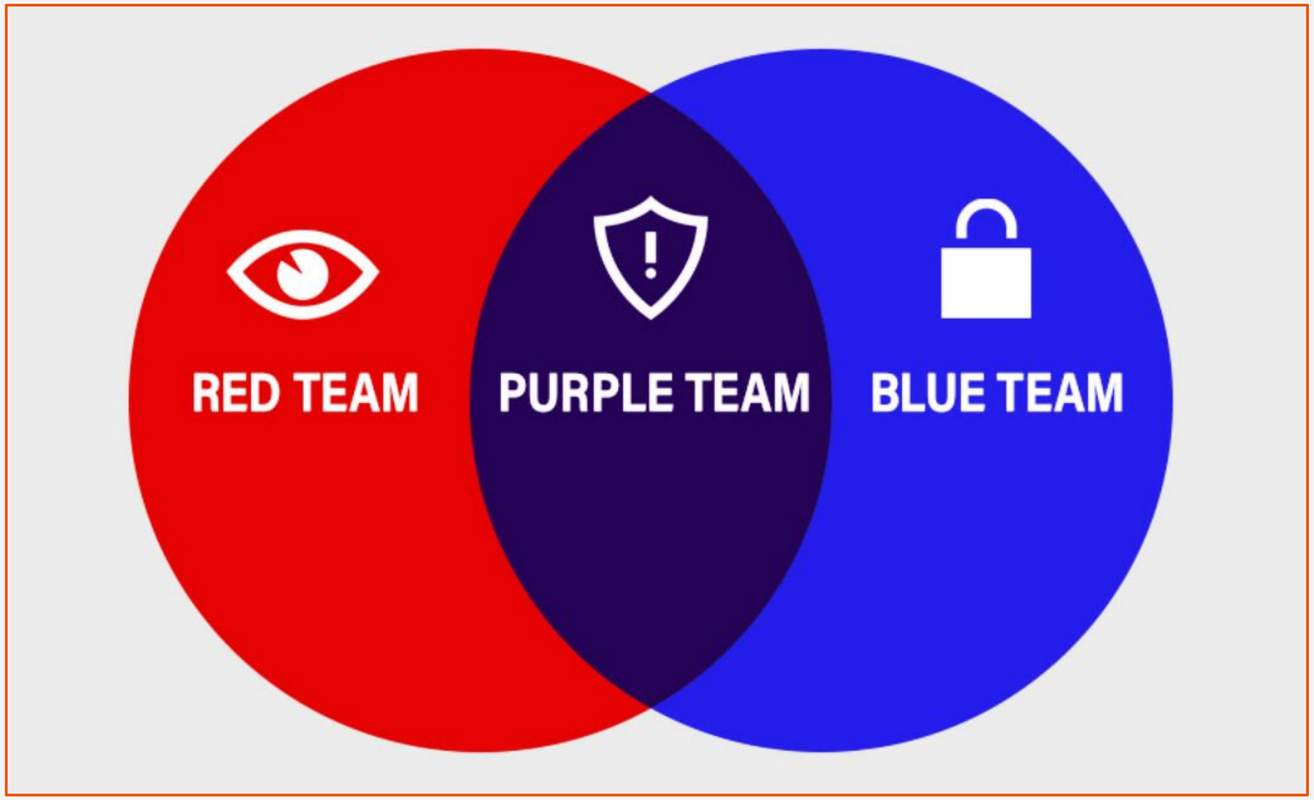
- *Evaluation of a system with full knowledge of its internal structure.*
- *Ethical hackers assess the system's architecture, code, and design.*
- *Provides an in-depth analysis to identify vulnerabilities and recommend fixes.*
- *Helps improve software security from within the development process.*



5

Teams in Cyber Security.

Why teams are essential in Ethical Hacking ?



Teams are crucial in ethical hacking as they bring together diverse expertise, fostering creative problem-solving and comprehensive security assessments. Collaboration ensures thorough testing and better protection against cyber threats.

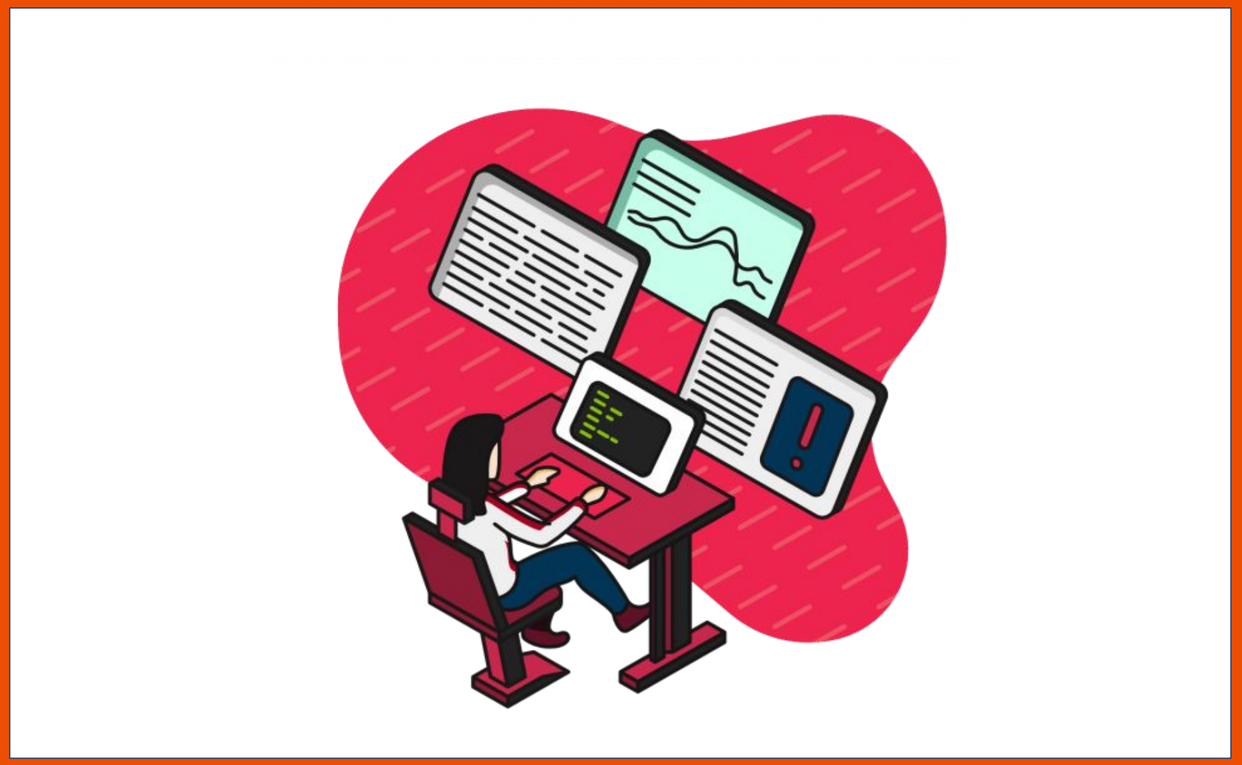
Red Teaming

- Simulates real-world cyberattacks to test an organization's defenses.
- Uncover vulnerabilities and weaknesses through offensive techniques and strategies.
- Identifies gaps in security controls, helping improve overall cybersecurity posture.
- Enhances preparedness for potential threats and improves incident response capabilities.

Role of Red Teaming

- Mimics adversarial attackers, attempting to breach systems and networks.
- Explores weaknesses, vulnerabilities, and potential entry points in the target.
- Provides actionable insights to strengthen security measures and policies.
- Aims to identify and prioritize security risks and vulnerabilities effectively.

Responsibilities of Red Teaming



- Conduct ethical hacking assessments to identify vulnerabilities.
- Report findings, including potential attack paths and compromised data.
- Suggest countermeasures and security enhancements.
- Collaborate with the Blue Team to improve defense strategies.

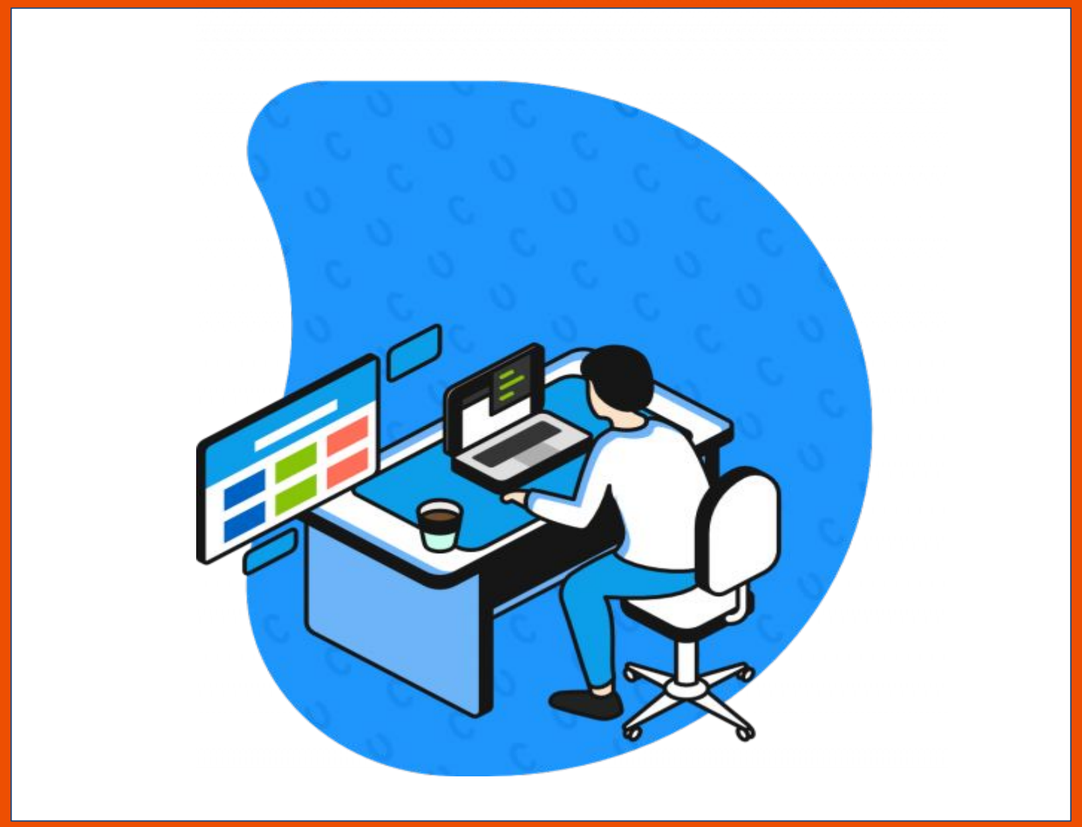
Blue Teaming

- Focuses on defending against cyber threats and securing systems.
- Monitors, detects, and responds to security incidents and breaches.
- Implements security controls and evaluates their effectiveness.
- Enhances network and system security through proactive defense measures.

Role of Blue Teaming

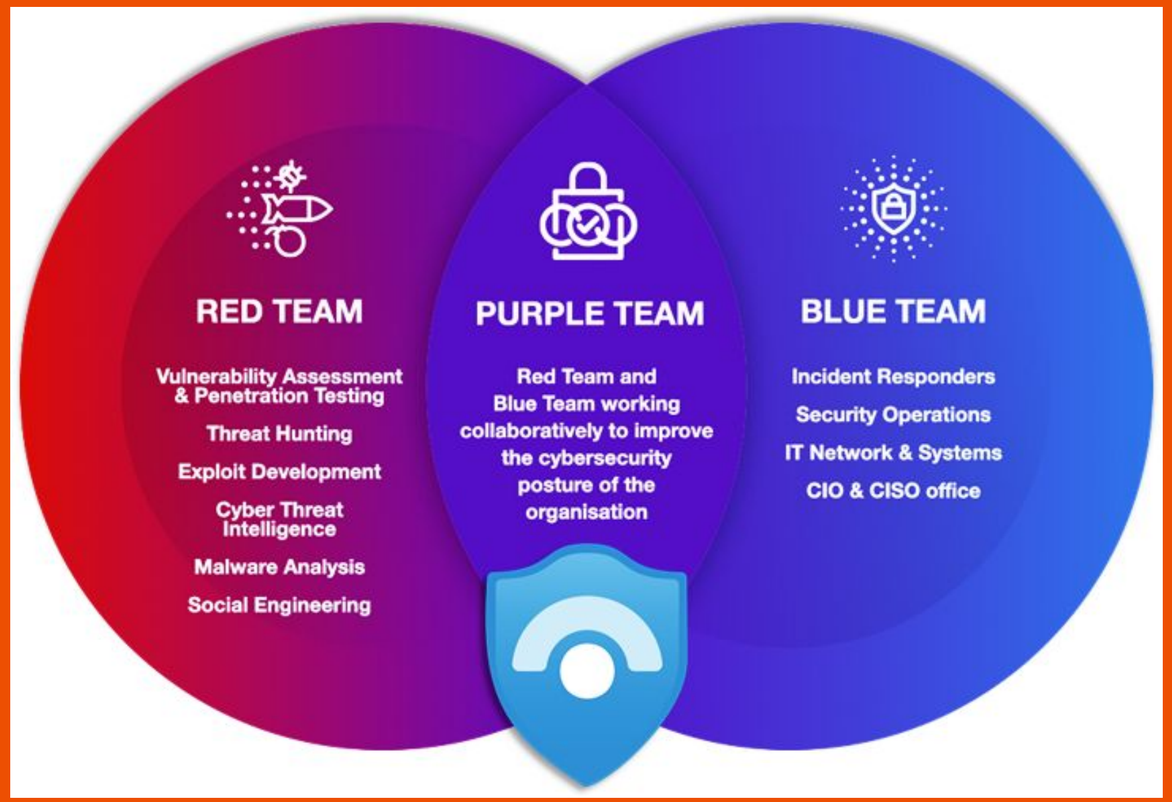
- Guards against Red Team attacks, actively defending systems and data.
- Monitors for suspicious activities, investigates incidents, and mitigates threats.
- Ensures the proper functioning of security tools and mechanisms.
- Works to maintain a resilient security posture and minimize vulnerabilities.

Responsibilities of Blue Teaming



- Continuously monitor networks, systems, and security alerts.
- Investigate and respond to security incidents and breaches promptly.
- Collaborate with the Red Team to understand attack tactics and techniques.
- Implement and improve security policies and measures based on insights.

Purple Teaming



- Combines Red and Blue Teams to collaboratively assess and optimize security.
- Validates defense strategies, tests incident response, and enhances cybersecurity.
- Encourages knowledge sharing and strengthens teamwork between Red and Blue.
- Ensures a comprehensive approach to security assessment and improvement.

Role of Purple Teaming

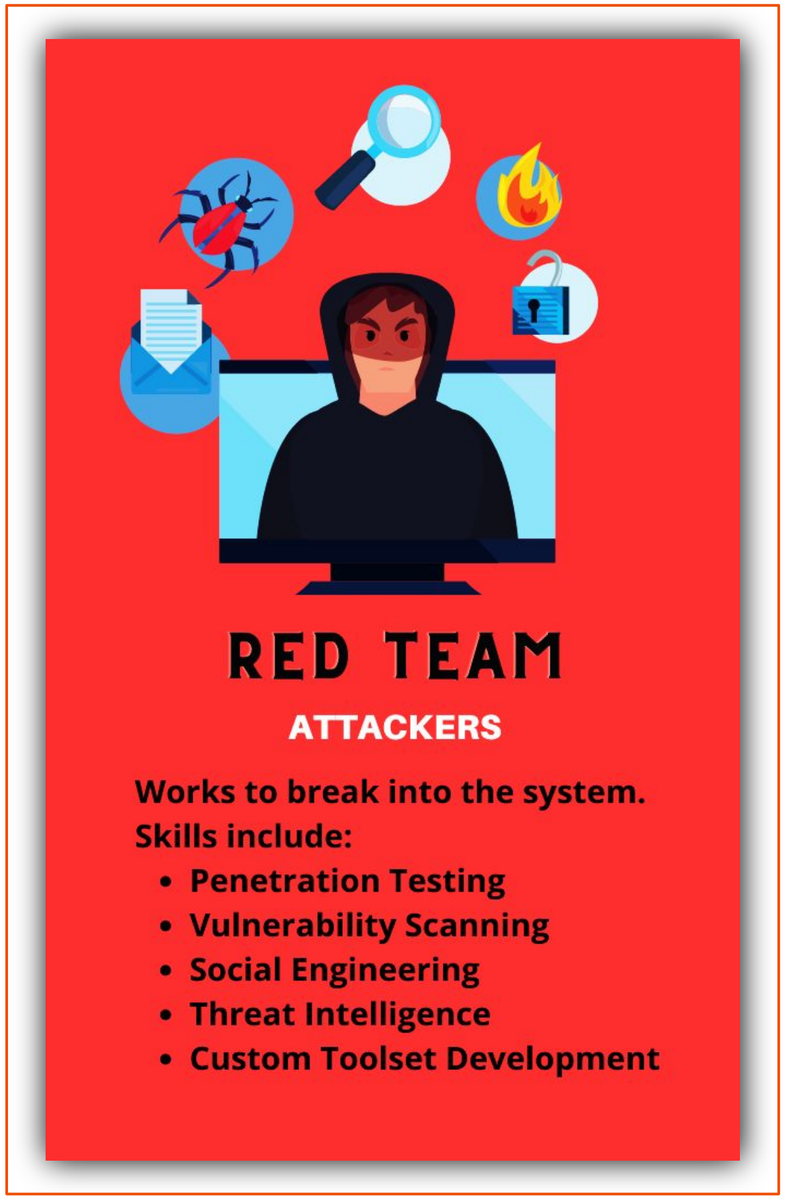
- Aligns offensive and defensive strategies for a holistic security assessment.
- Validates security controls and measures through controlled testing scenarios.
- Promotes effective communication between Red and Blue Teams.
- Focuses on improving security effectiveness based on lessons learned.

Responsibilities of Blue Teaming

- Conduct joint assessments to identify security strengths and weaknesses.
- Share insights, tactics, and findings between Red and Blue Teams.
- Collaboratively develop and refine security policies and incident response plans.
- Facilitate ongoing security improvement through coordinated efforts.

Objective of Red Teaming.

- **Identify Vulnerabilities:** Uncover weaknesses and vulnerabilities within the security infrastructure.
- **Assess Defensive Measures:** Evaluate the effectiveness of existing security controls.
- I**mprove Incident Response:** Test incident response procedures and readiness thoroughly.
- **Enhance Security Awareness:** Educate teams on threats and promote proactive defense.



Objective of Blue Teaming.

- **Detection and Analysis:** Identify vulnerabilities, threats, and breaches for proactive defense.
- **Incident Response Enhancement:** Strengthen incident handling procedures and minimize recovery time.
- **Security Posture Assessment:** Evaluate defenses to enhance resilience and protect critical assets.
- **Team Skill Development:** Train and improve cybersecurity skills through real-world simulations.

Objective of Purple Teaming.

- **Enhance Defense**: Strengthen security measures through constructive, collaborative assessments.
- **Validation of Controls**: Confirm the effectiveness of existing security controls.
- **Knowledge Transfer**: Promote knowledge sharing between Red and Blue Teams.
- **Continuous Improvement**: Identify and rectify vulnerabilities for ongoing security enhancement.

Red Teaming Tactics

01 Email and Phone Based Social Engineering

02 Network Service Exploitation

03 Physical Facility Exploitation

04 Application Layer Exploitation

Blue Teaming Tactics

01 Penetration Testing and Vulnerability Assessment

02 Incident Response Planning and Drills

03 Threat Intelligence Analysis

04 Continuous Monitoring and Security Information and Event Management (SIEM)

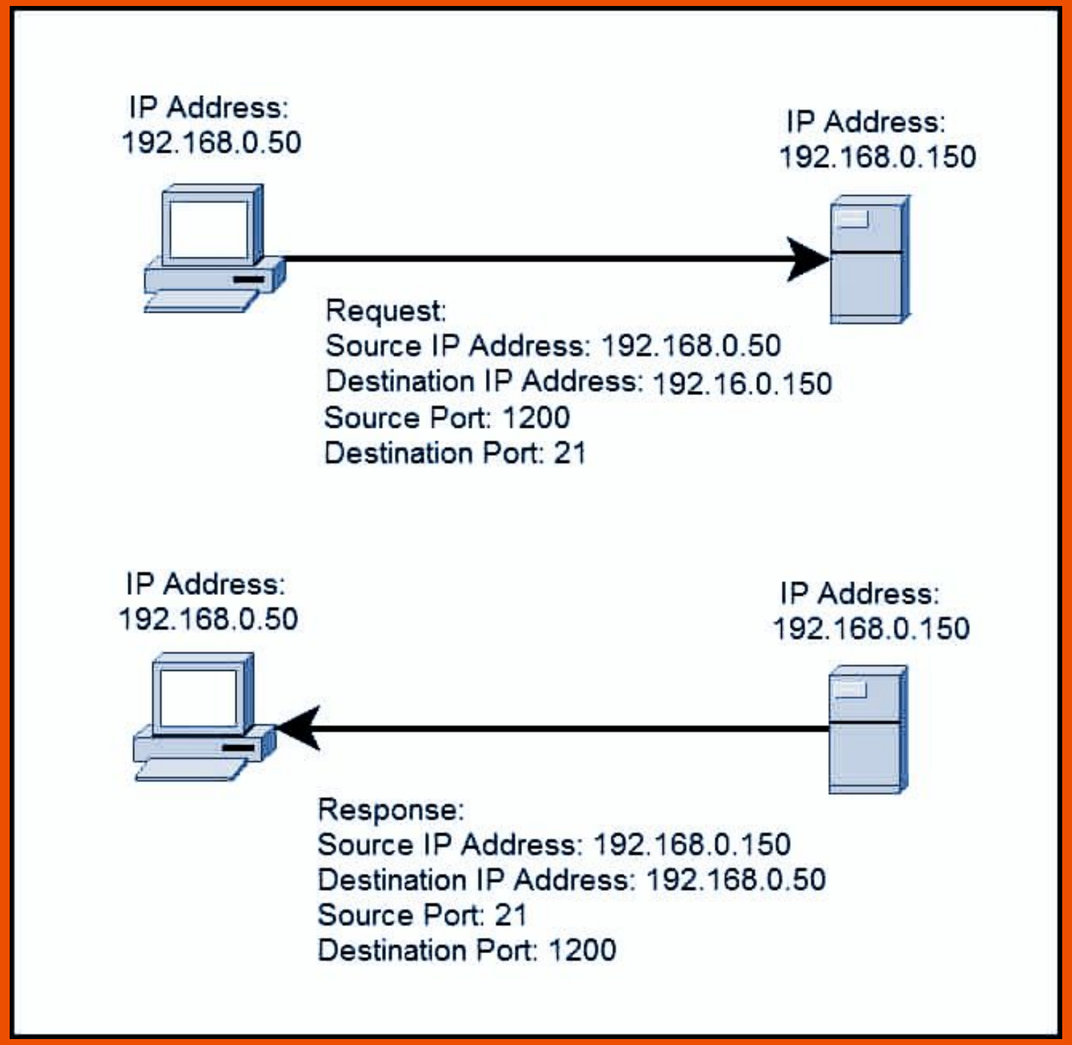
6

Ports & Protocols

Importance of Understanding Ports and Protocol

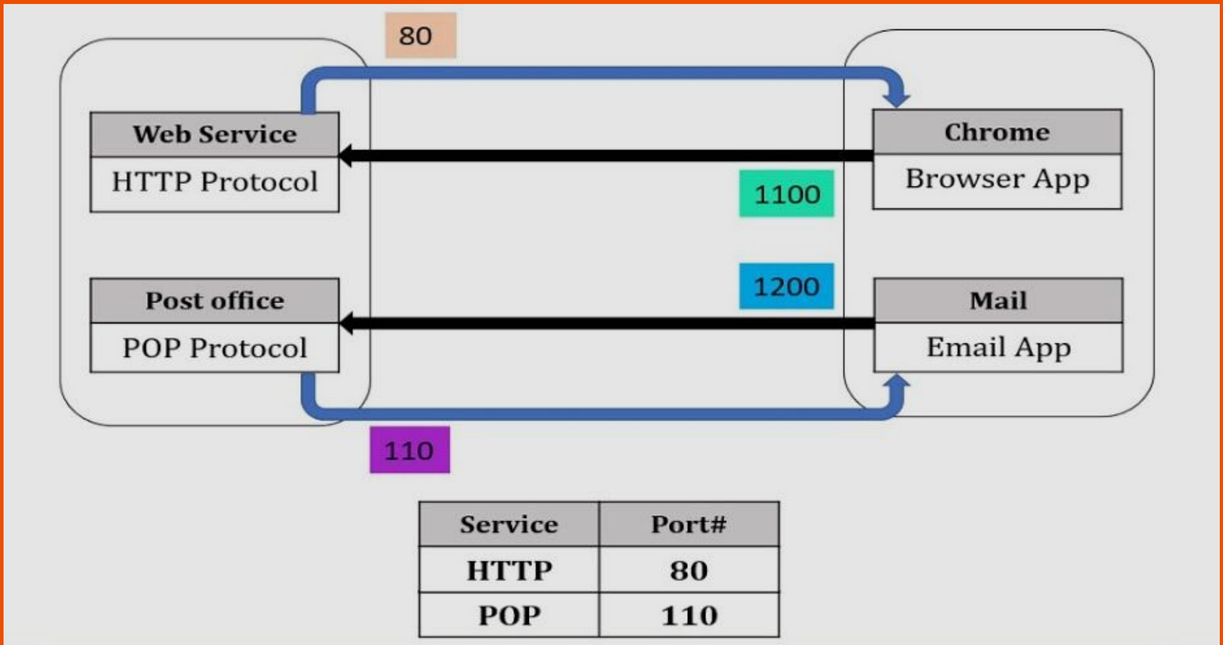
- Network Management: Essential for configuring and troubleshooting network devices effectively.
- Security: Identifies open ports susceptible to unauthorized access and attacks.
- Application Compatibility: Ensures applications communicate correctly by using the right protocols.
- Traffic Control: Helps optimize data routing, reducing congestion and improving performance.

Introduction to Ports in Networking



- Logical endpoints for communication in computer networks.
- Enable data to reach specific applications or services on a device.
- Identified by numbers and facilitate data exchange between devices.
- Crucial for networking protocols like TCP and UDP.

Concept of Port Number



Service	Port#
HTTP	80
POP	110

- Numeric labels assigned to network endpoints for data routing.
- Range from 0 to 65535 (16 bits), categorized as well-known, registered, dynamic.
- TCP and UDP protocols use port numbers to direct traffic.
- Ensure data packets reach the correct destination service/application.

Well-known Ports (0-1023)

Port 80: HTTP (web servers)

Port 443: HTTPS (secure web servers)

Port 21: FTP (file transfer)

Port 22: SSH (secure shell)

Port 23: Telnet (remote terminal access)

Port 25: SMTP (email)

Port 110: POP3 (email)

Port 143: IMAP (email)

Registered Ports (1024-49151)

- Span a range of port numbers between 1024 and 49151.
- Typically linked to specific applications or services on computer systems.
- Ethical hackers explore these ports for potential vulnerabilities or misconfigurations.
- Relevance depends on the objectives and scope of security assessments.

Dynamic/Private Ports:49152 to 65535.

- Range from 49152 to 65535.
- Temporary connections in networking.
- Not tied to specific services, vary with applications.
- Relevant based on diverse testing requirements and use cases.

Commonly used Ports and their associated service

1. **Port 80: HTTP (web servers)**

- ➔ Common for web traffic.
- ➔ Transmits web pages and content.
- ➔ Unencrypted communication.
- ➔ Basis for the World Wide Web.

Commonly used Ports and their associated service

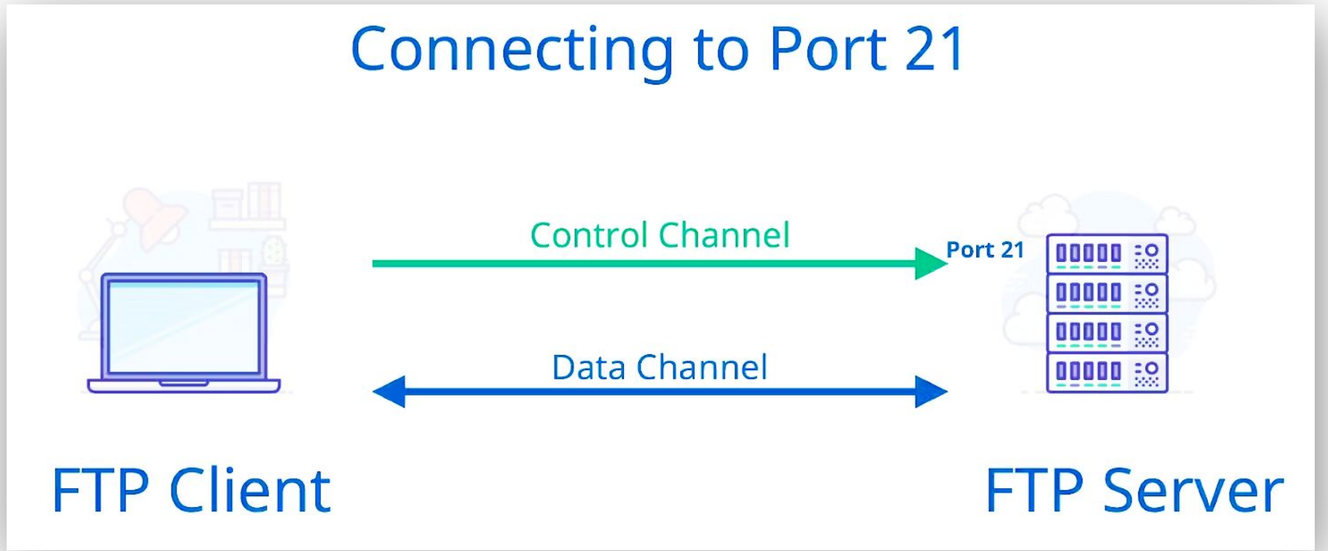
2. Port 443: HTTPS (secure web servers)

- ➔ Secure web traffic.
- ➔ Encrypts data transmission.
- ➔ Protects sensitive information.
- ➔ Used for online banking, shopping, and secure logins.

Commonly used Ports and their associated service

3. Port 21: FTP (file transfer)

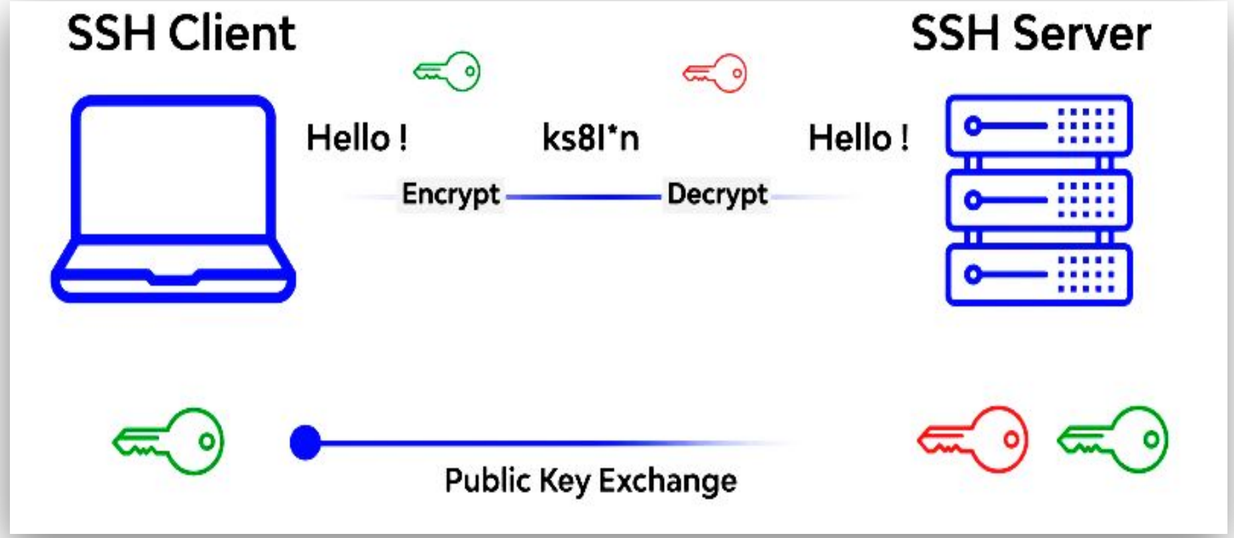
- ➔ File transfer protocol.
- ➔ Transfers files between client and server.
- ➔ Supports upload and download.
- ➔ Often used for website maintenance



Commonly used Ports and their associated service

4. Port 22: SSH (secure shell)

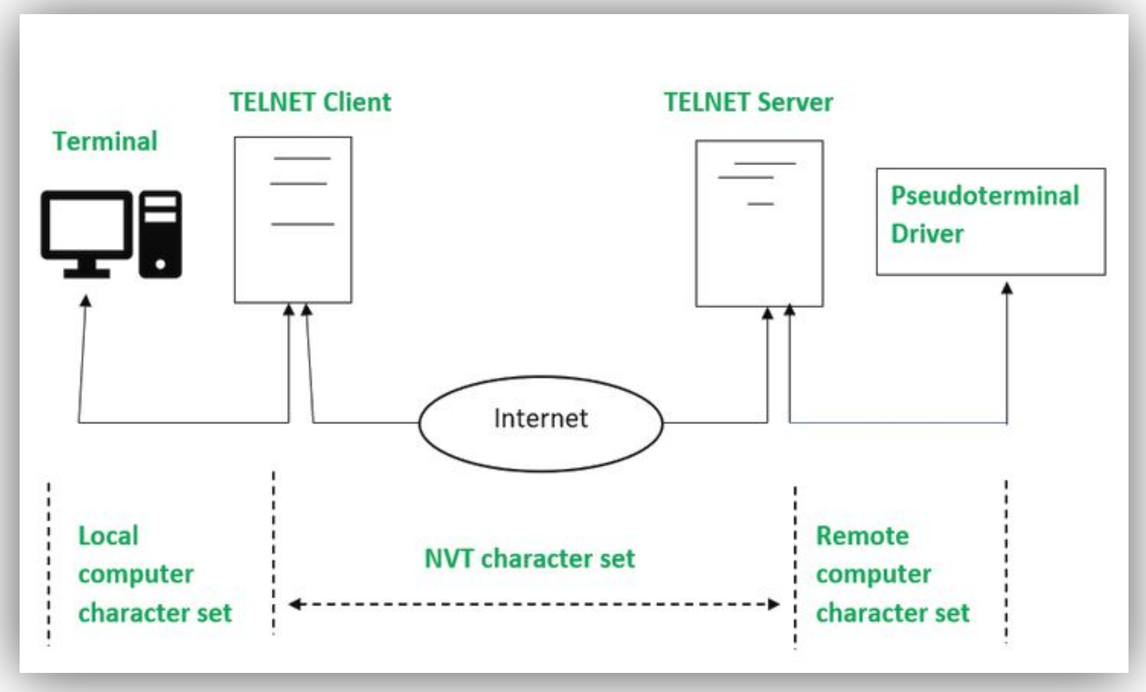
- ➔ Secure remote access.
- ➔ Encrypted terminal connections.
- ➔ Authentication and secure file transfers.
- ➔ Used for remote server management.



Commonly used Ports and their associated service

5. Port 23: Telnet (remote terminal access).

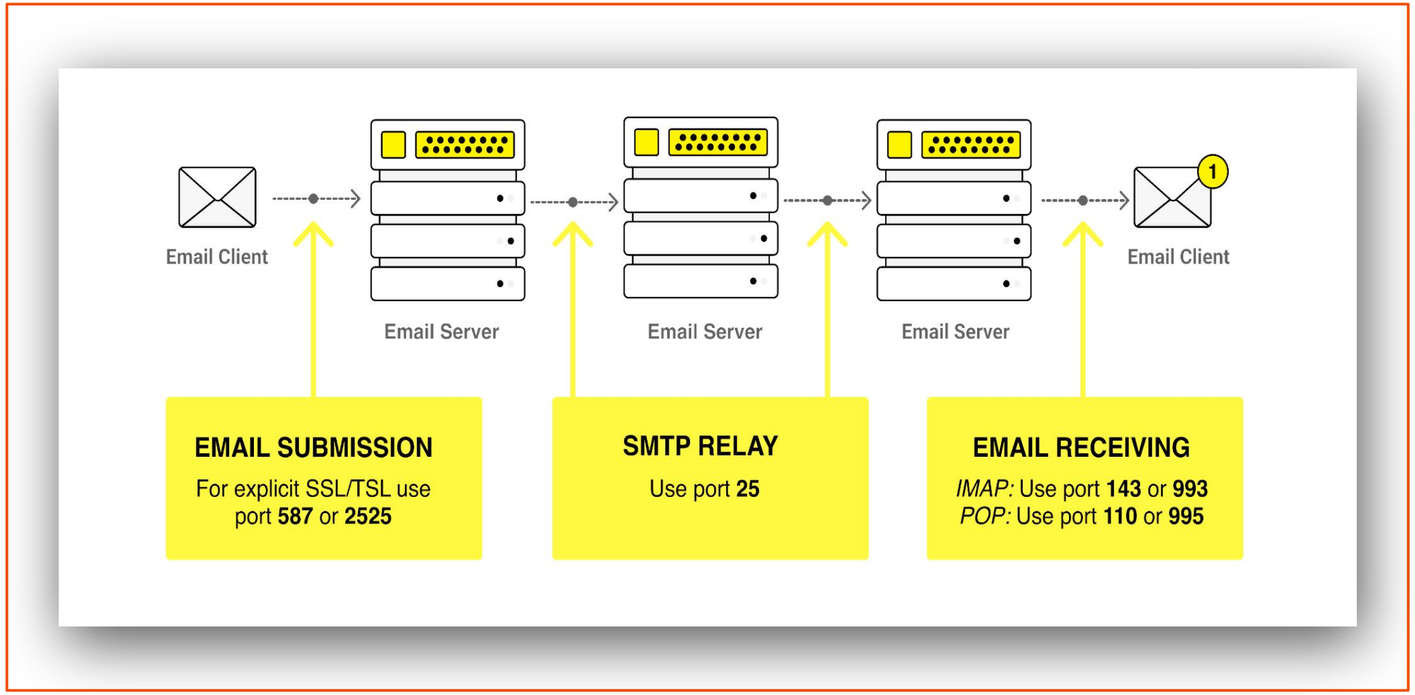
- ➔ Unsecured remote terminal access.
- ➔ Sends text-based commands.
- ➔ Lacks encryption, vulnerable to eavesdropping.
- ➔ Less secure, mostly replaced by SSH.



Commonly used Ports and their associated service

6. Port 25: SMTP (email)

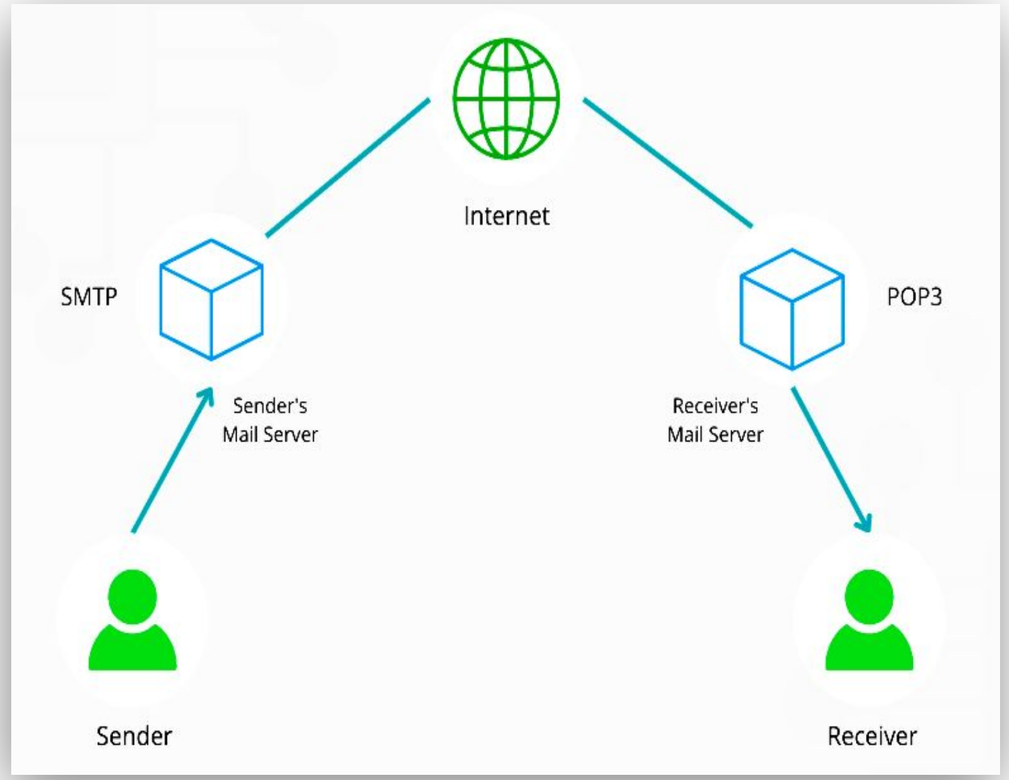
- ➔ Simple Mail Transfer Protocol.
- ➔ Sends email messages.
- ➔ Used for outgoing mail.
- ➔ Essential for email communication.



Commonly used Ports and their associated service

7. Port 110: POP3 (email)

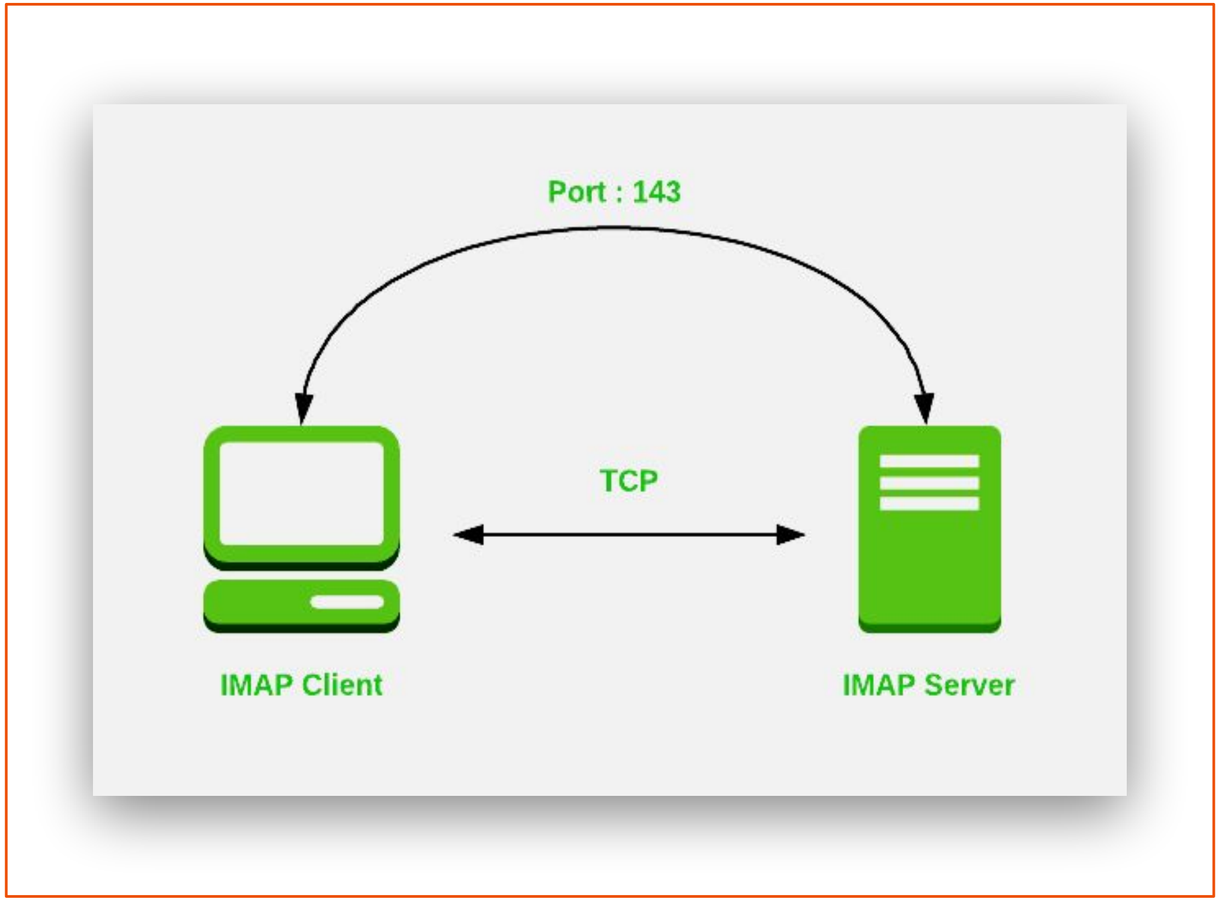
- ➔ Post Office Protocol version 3.
- ➔ Retrieves email from a server.
- ➔ Downloads messages to the client.
- ➔ Often used for email storage and retrieval.



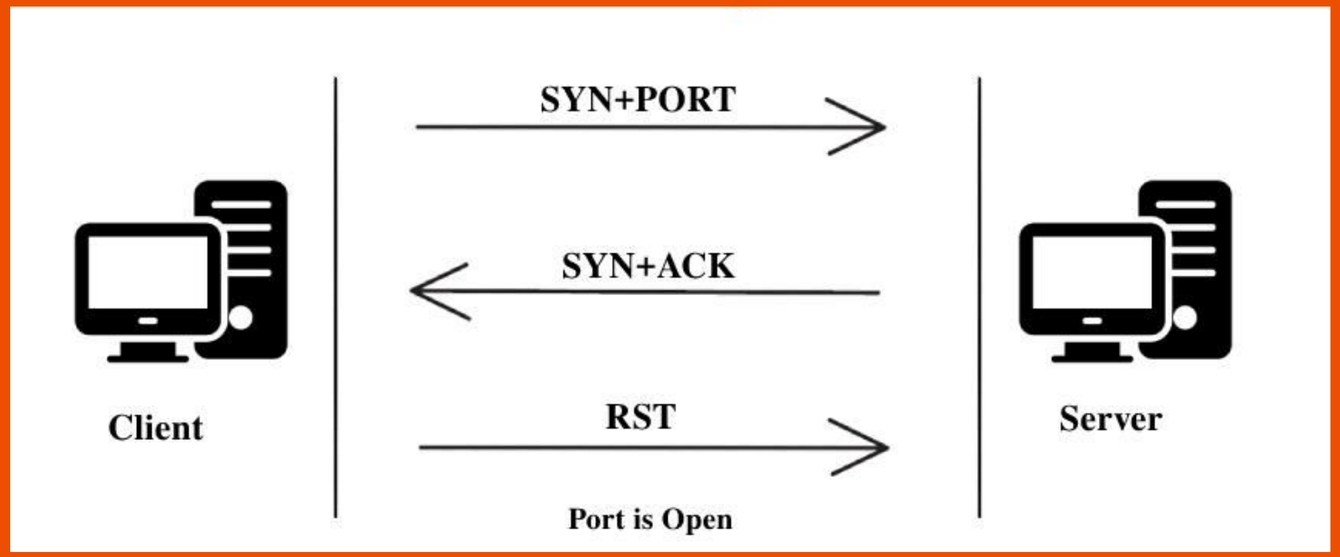
Commonly used Ports and their associated service

8. Port 143: IMAP (email)

- ➔ Internet Message Access Protocol.
- ➔ Manages email on the server.
- ➔ Supports multiple devices synchronization.
- ➔ Ideal for accessing emails from different locations.

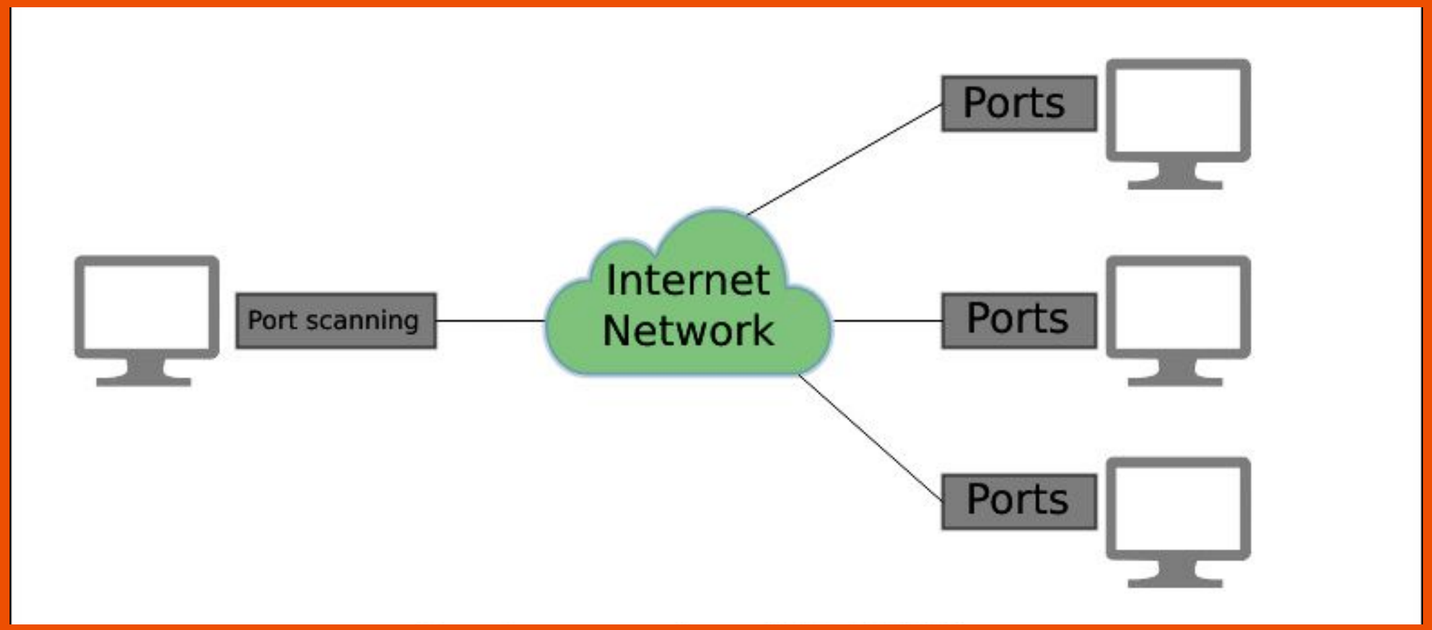


Port Scanning in Ethical Hacking



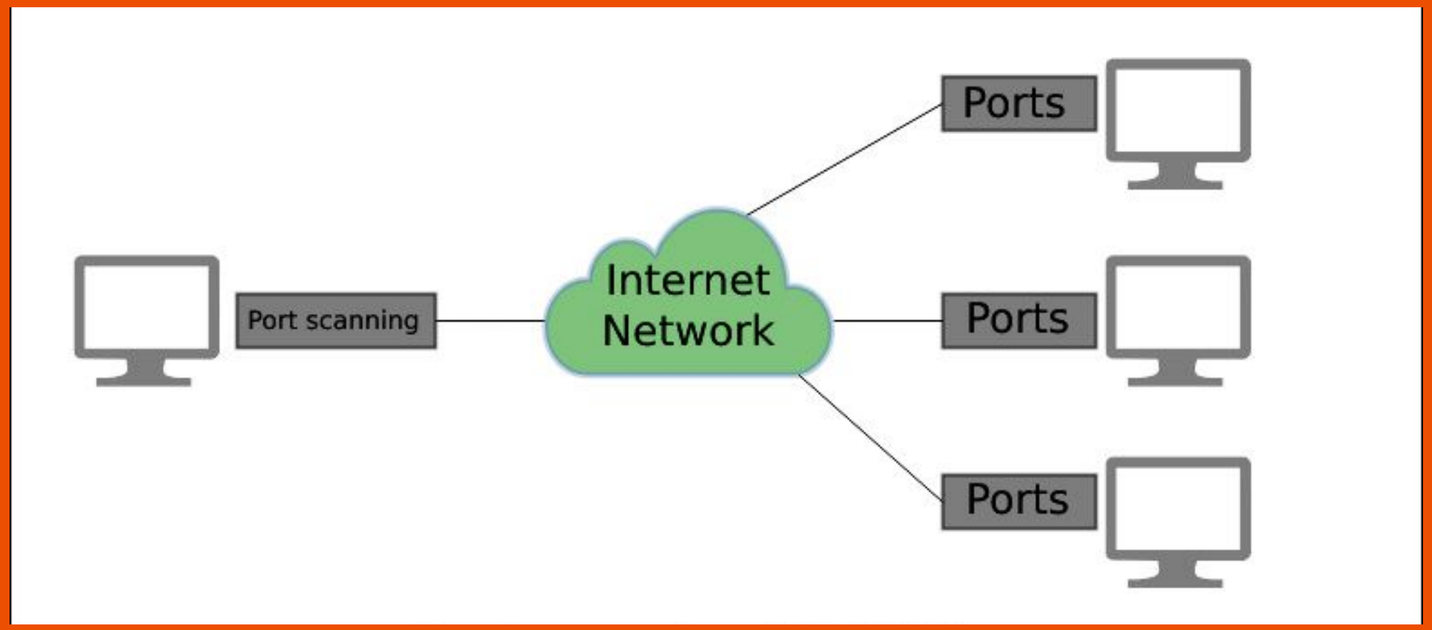
- Definition: The systematic process of probing network ports for vulnerabilities.
- Role: Identifies open ports and services on target systems.
- Method: Conducted using tools to assess network security and weaknesses.
- Objective: Gather information for security assessments and potential exploitation.

Purpose of Port Scanning



- Network Mapping: Reveal live hosts and active services on a network.
- Vulnerability Assessment: Identify potential entry points for security testing.
- Security Auditing: Evaluate firewall rules and security configurations.
- Intrusion Detection: Detect and respond to unauthorized access or anomalies.

Purpose of Port Scanning



- Network Mapping: Reveal live hosts and active services on a network.
- Vulnerability Assessment: Identify potential entry points for security testing.
- Security Auditing: Evaluate firewall rules and security configurations.
- Intrusion Detection: Detect and respond to unauthorized access or anomalies.

Port Scanning Tool:- Nmap

- Nmap is a popular network scanner commonly known as a network mapper.

It can be used with any supported script on an individual machine or a server.

It can work with speed and efficiency over any network.

Syntax: nmap [Scan Type(s)] [Option(s)] <target>

Understanding Nmap-
A network mapper.

- *Nmap is a powerful tool for exploring networks, revealing connected devices.*
- *Scan networks efficiently to discover open ports, aiding cybersecurity assessments.*
- *Nmap provides insights into network vulnerabilities.*
- *With simple commands, Nmap is an indispensable tool for cybersecurity enthusiasts.*

Nmap Features and Capabilities

- *Host Discovery: Nmap locates active hosts, assessing network scope and potential weaknesses using ICMP, TCP, and ARP.*
- *Service and Version Detection: Nmap delivers service specifics, including versions, aiding vulnerability assessment and security audits on network hosts.*
- *Scriptable Interaction: Nmap's scripting engine automates networking tasks, improving efficiency and flexibility in network exploration.*

Installation of Nmap

```
┌──(root㉿kali)-[/home/kali]
└─# apt install nmap
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
nmap is already the newest version (7.94+dfsg1-1kali1).
The following packages were automatically installed and are no longer requi
red:
  golang-1.19-go golang-1.19-src libarmadillo11 libblockdev-crypto2
  libblockdev-fs2 libblockdev-loop2 libblockdev-part-err2
  libblockdev-part2 libblockdev-swap2 libblockdev-utils2 libblockdev2
  libgdal32 libgeos3.11.1 libgupnp-igd-1.0-4 libjim0.81 libmongocrypt0
  libmujs2 libncurses5 libnfs13 libobjc-12-dev libspatialite7 libsuperlu5
  libtinfo5 libwebsockets17 libyara9 python3-cryptography37
  python3-flask-security python3-jaraco.classes python3-jdcal
  python3-promise python3-py python3-pytz-deprecation-shim python3-rx
  python3-texttable
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 13 not upgraded.
```

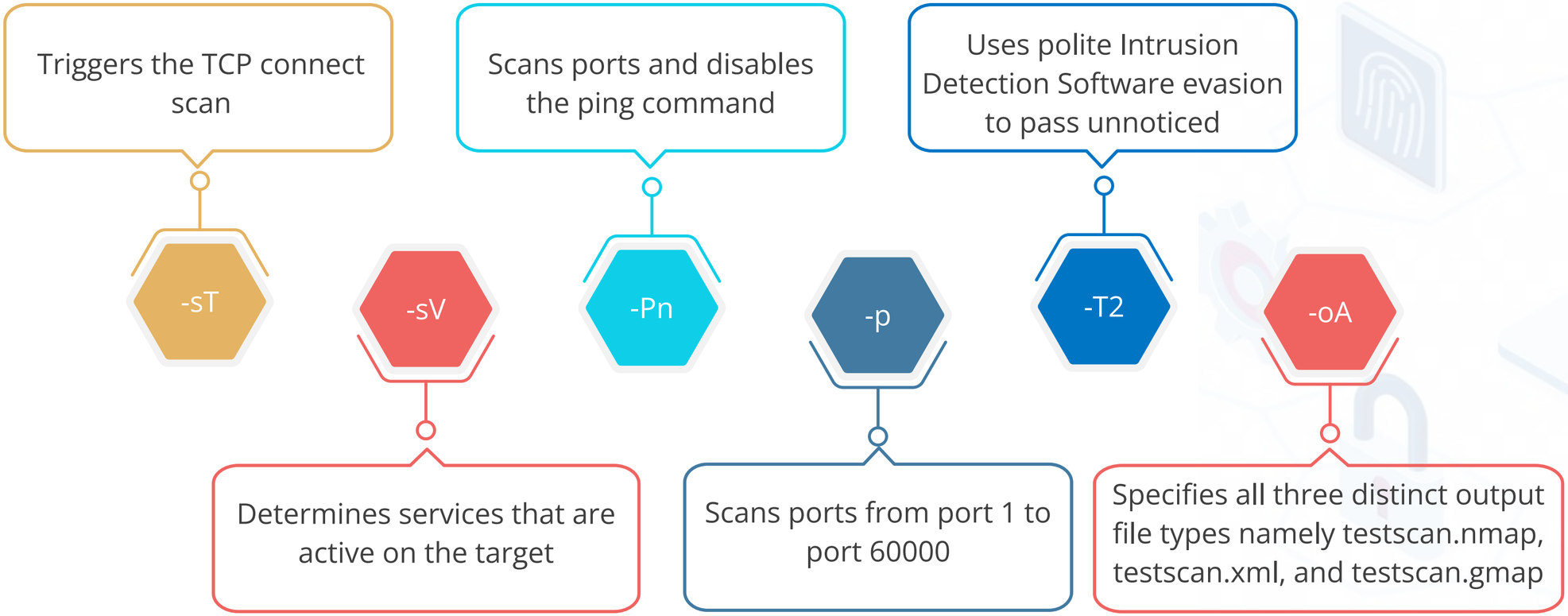
❑ **Command** :- apt install nmap or sudo apt install nmap

To Update Nmap

```
┌──(root㉿kali)-[/home/kali]
└─# apt upgrade nmap
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
nmap is already the newest version (7.94+dfsg1-1kali1).
Calculating upgrade ... Done
The following packages were automatically installed and are no longer requi
red:
  golang-1.19-go golang-1.19-src libarmadillo11 libblockdev-crypto2
  libblockdev-fs2 libblockdev-loop2 libblockdev-part-err2
  libblockdev-part2 libblockdev-swap2 libblockdev-utils2 libblockdev2
  libgdal32 libgeos3.11.1 libgupnp-igd-1.0-4 libjim0.81 libmongocrypt0
  libmujs2 libncurses5 libnfs13 libobjc-12-dev libspatialite7 libsuperlu5
  libtinfo5 libwebsockets17 libyara9 python3-cryptography37
  python3-flask-security python3-jaraco.classes python3-jdcal
  python3-promise python3-py python3-pytz-deprecation-shim python3-rx
  python3-texttable
Use 'sudo apt autoremove' to remove them.
The following packages have been kept back:
  freerdp2-x11 gstreamer1.0-libav libasound2-plugins libchromaprint1
  libfreerdp-client2-2 libfreerdp2-2 libncurses-dev libncurses6
  libncursesw6 libswresample4 libtinfo6 libwinpr2-2 ncurses-bin
0 upgraded, 0 newly installed, 0 to remove and 13 not upgraded.
```

❑ **Command** :- apt upgrade nmap or sudo apt upgrade nmap

Nmap Flags



❑ The Nmap command creates flags that are hyphenated parameters, and each one serves a unique function.

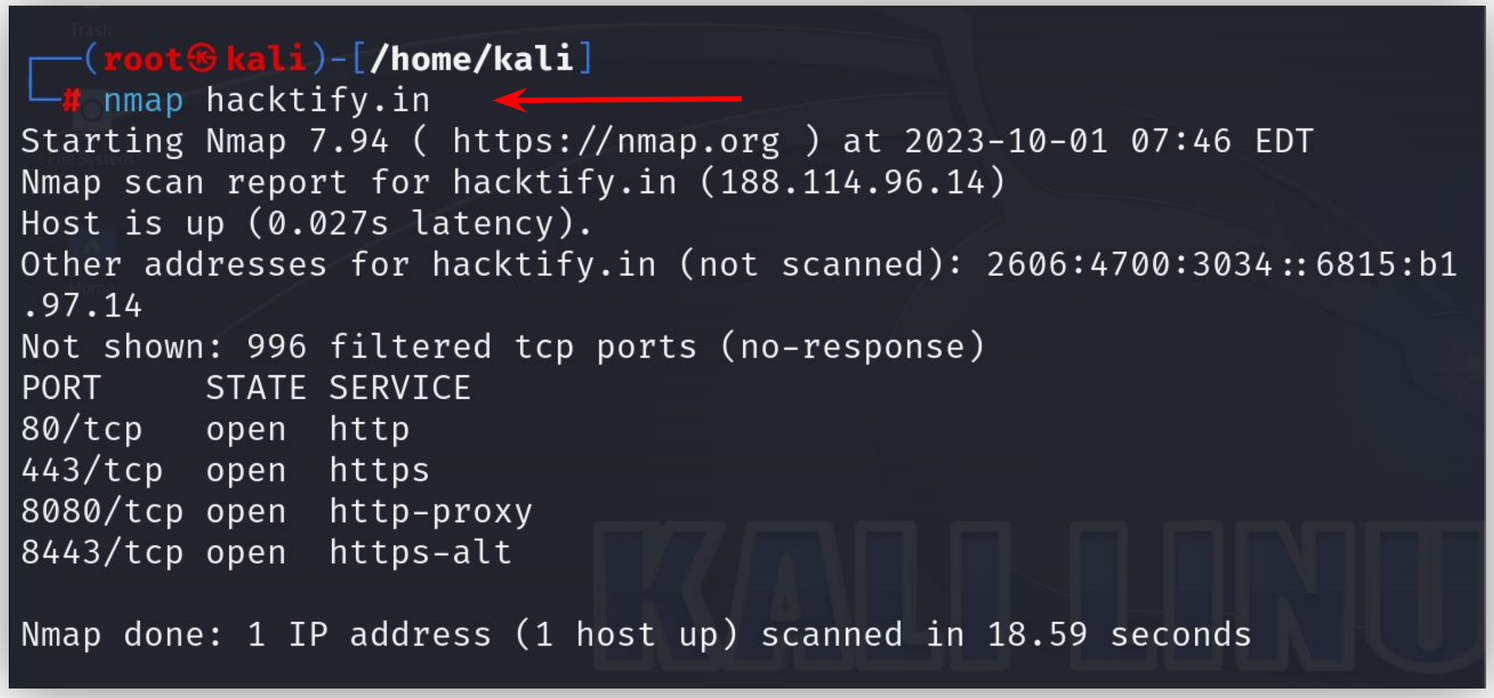
Nmap Target Methods

Examples of Nmap target methods can be seen below:

Command	Description
nmap 192.168.1.40	Used to scan the IP
nmap scname.host.tld	Used to scan the host by a given name
nmap 192.168.1.0/24	Used to scan the complete subnet
nmap scname.host.tld/24	Used to scan the complete subnet for the host
nmap 192.168.1.45-110	Used to scan the range of IPs

- The Nmap command creates flags that are hyphenated parameters, and each one serves a unique function.

Nmap Target Methods



Description:-

This Method is used to scan the host by a given name.

Nmap Target Methods

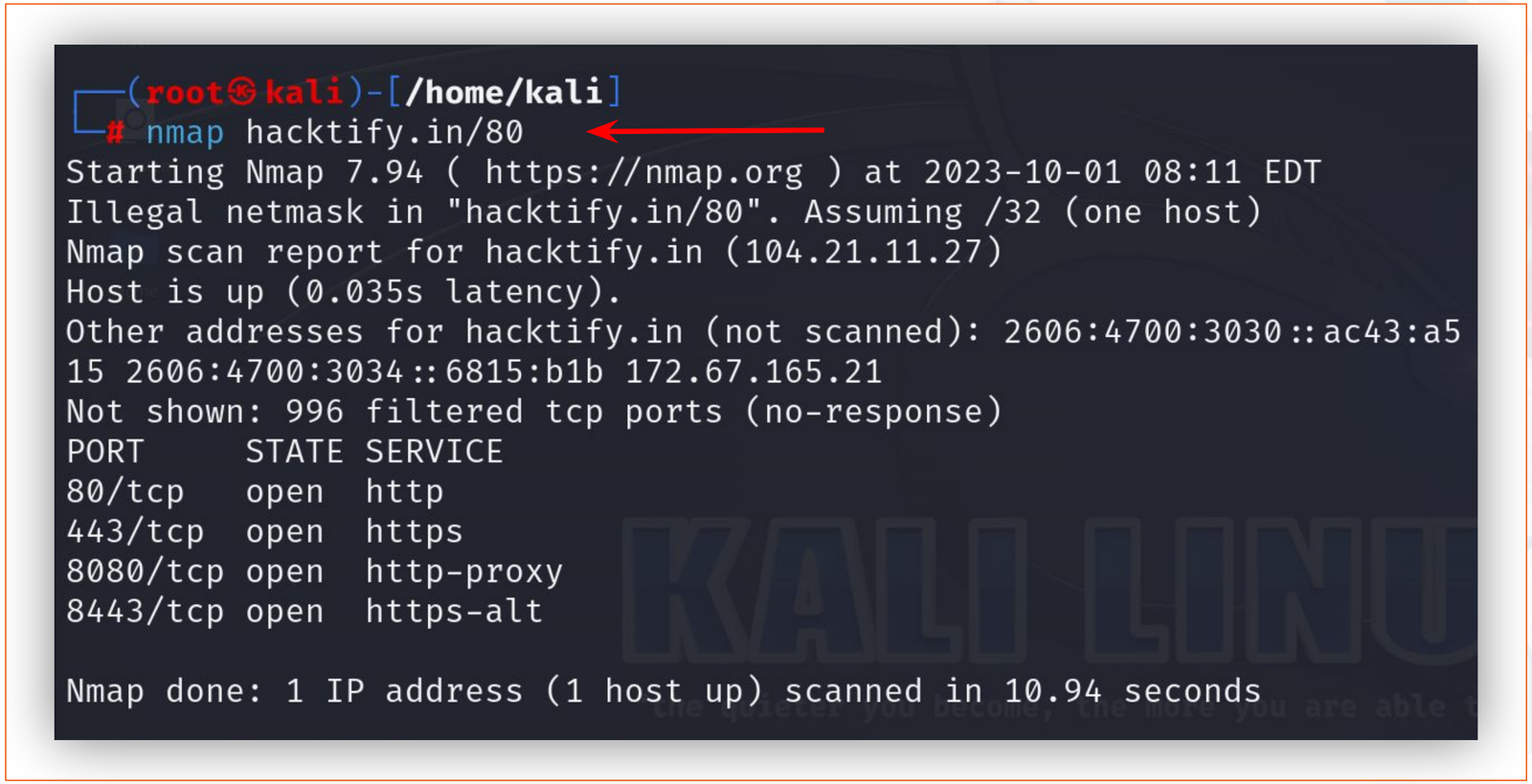
```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.1.7/24
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-01 07:55 EDT
Nmap scan report for dsldevice.lan (192.168.1.1)
Host is up (0.0031s latency).
Not shown: 996 closed tcp ports (reset)
PORT    STATE    SERVICE
22/tcp  filtered ssh
23/tcp  filtered telnet
80/tcp  open     http
443/tcp open     https
MAC Address: 60:BD:2C:37:41:80 (Unknown)

Nmap scan report for 192.168.1.6
Host is up (0.0093s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
49152/tcp open  unknown
62078/tcp open  iphone-sync
MAC Address: CA:F1:55:91:AE:05 (Unknown)
```

```
Nmap scan report for 192.168.1.7
Host is up (0.013s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
5357/tcp open  wsdapi
7070/tcp open  realserver
MAC Address: F8:28:19:D5:81:7F (Liteon Technology)

Nmap scan report for 192.168.1.103
Host is up (0.000026s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 58.08 seconds
```

Description:-

This method is used to scan the Complete Subnet.

Nmap Target Methods



Description:-

This method is used to scan the Complete Subnet for the Host .

Nmap Target Methods

```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.1.7-110
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-01 08:13 EDT
Nmap scan report for 192.168.1.7
Host is up (0.00029s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
5357/tcp open  wsdapi
7070/tcp open  realserver
MAC Address: F8:28:19:D5:81:7F (Liteon Technology)

Nmap scan report for 192.168.1.103
Host is up (0.000017s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh

Nmap done: 104 IP addresses (2 hosts up) scanned in 8.54 seconds
```

Description:-

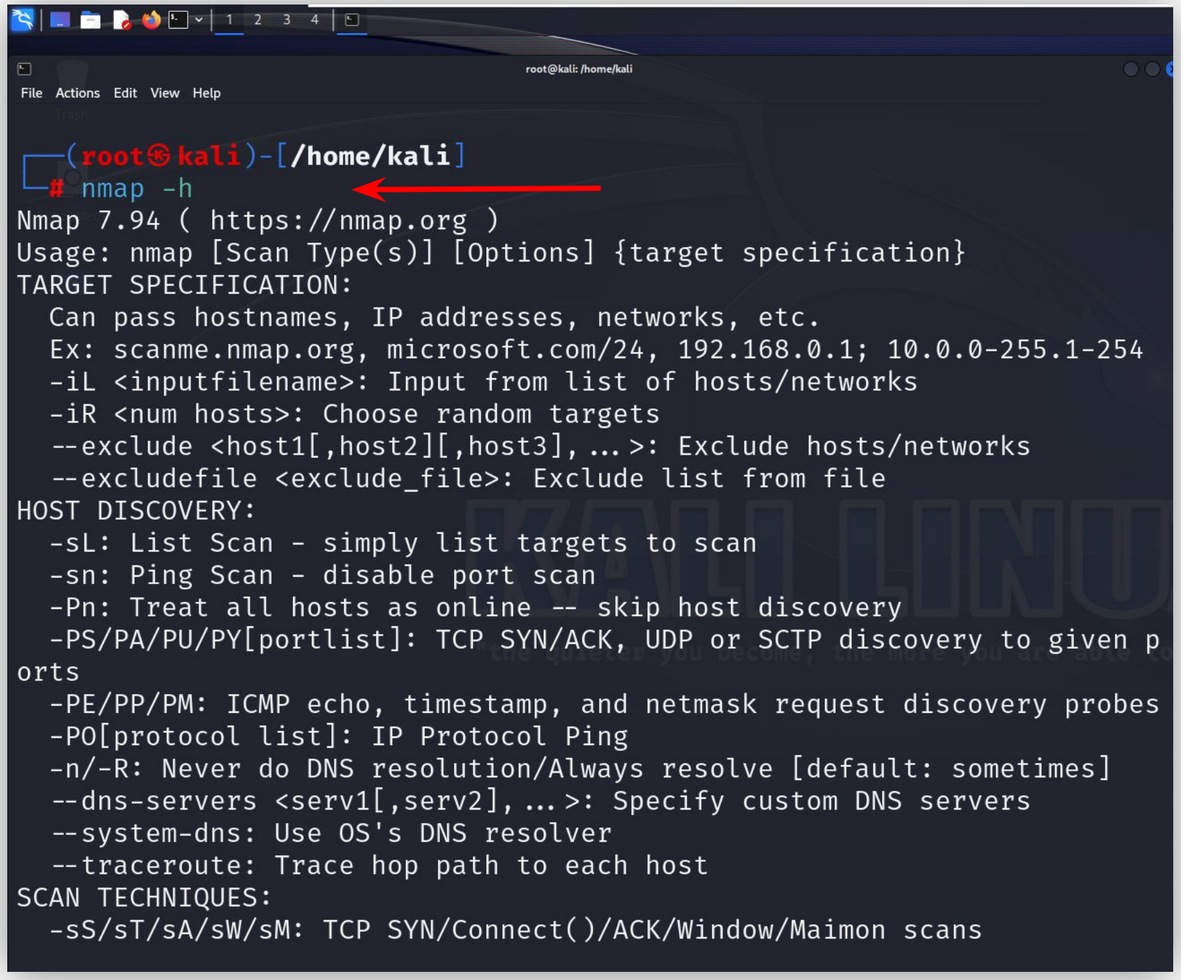
This method is used to scan the range of IP’s

Nmap Scan Methods

Examples of Nmap scan commands can be seen below:

Scan command	Description
Nmap –h	Provides help
Nmap –V	Shows the Nmap version
Nmap –d 192.168.100.251	Enables debugging for the given IP
Nmap –sS 192.168.1.22	Scans a TCP SYN to check the target port with SY ACK or RST
Nmap –sT 192.168.1.25	Checks the complete TCP three-way handshake
Nmap –sU 192.168.1.25	Scans the UDP port
Nmap –sL 192.168.1.25	Lists the targets to scan

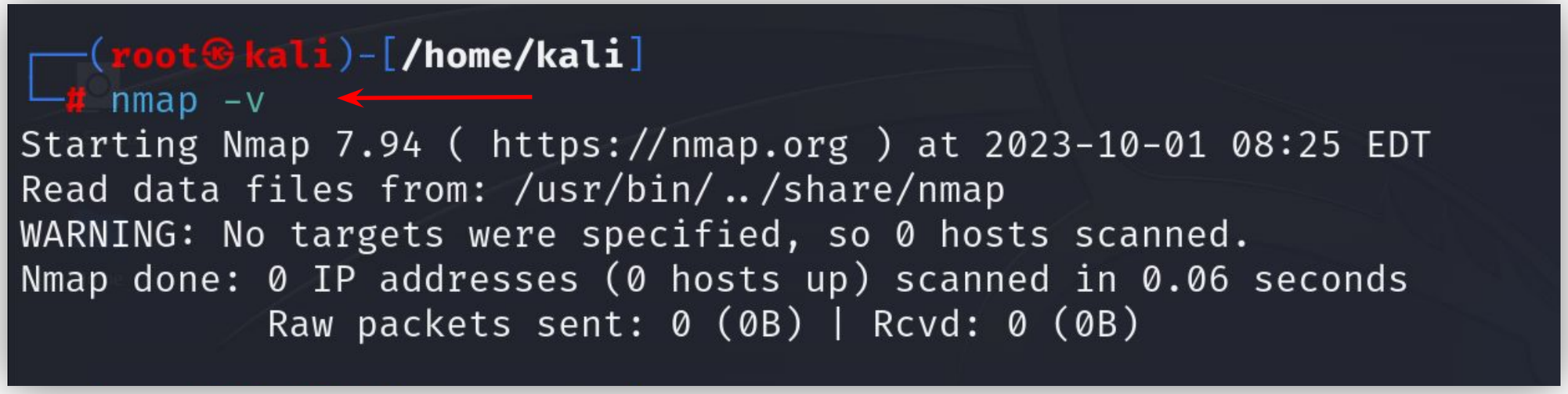
Nmap Scan Methods



Description:-

Provides help.

Nmap Scan Methods



Description:-

Shows the Nmap Version.

Nmap Scan Methods

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -d 192.168.1.7
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-01 08:25 EDT
PORTS: Using ports open on 0% or more average hosts (TCP:1000, UDP:0, S
CTP:0)
------------------ Timing report ------------------
  hostgroups: min 1, max 100000
  rtt-timeouts: init 1000, min 100, max 10000
  max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
  parallelism: min 0, max 0
  max-retries: 10, host-timeout: 0
  min-rate: 0, max-rate: 0
---------------------------------------------------
Initiating ARP Ping Scan at 08:25
Scanning 192.168.1.7 [1 port]
Packet capture filter (device eth0): arp and arp[18:4] = 0×000C291E and
 arp[22:2] = 0×16B6
Completed ARP Ping Scan at 08:25, 0.09s elapsed (1 total hosts)
Overall sending rates: 11.23 packets / s, 471.76 bytes / s.
mass_rdns: Using DNS server 192.168.1.1
mass_rdns: Using DNS server fe80::1%eth0
Initiating Parallel DNS resolution of 1 host. at 08:25
Stats: 0:00:02 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping
 Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
```

```
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 u
lth Scan
SYN Stealth Scan Timing: About 0.50% done
Current sending rates: 447.47 packets / s, 3590.87 by
Discovered open port 139/tcp on 192.168.1.7
Discovered open port 135/tcp on 192.168.1.7
Discovered open port 445/tcp on 192.168.1.7
Discovered open port 5357/tcp on 192.168.1.7
Discovered open port 912/tcp on 192.168.1.7
Discovered open port 7070/tcp on 192.168.1.7
Discovered open port 902/tcp on 192.168.1.7
Completed SYN Stealth Scan at 08:25, 4.11s elapsed (1000 total ports)
Overall sending rates: 484.80 packets / s, 21331.22 bytes / s.
Nmap scan report for 192.168.1.7
Host is up, received arp-response (0.00047s latency).
Scanned at 2023-10-01 08:25:40 EDT for 4s
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE SERVICE        REASON
135/tcp  open  msrpc          syn-ack ttl 128
139/tcp  open  netbios-ssn    syn-ack ttl 128
445/tcp  open  microsoft-ds   syn-ack ttl 128
902/tcp  open  iss-realsecure syn-ack ttl 128
912/tcp  open  apex-mesh      syn-ack ttl 128
5357/tcp open  wsdapi         syn-ack ttl 128
7070/tcp open  realserver     syn-ack ttl 128
MAC Address: F8:28:19:D5:81:7F (Liteon Technology)
```

Description:-

Shows the Nmap Version.

Nmap Scan Methods

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.1.7
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-01 08:26 EDT
Nmap scan report for 192.168.1.7
Host is up (0.00038s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
5357/tcp open  wsdapi
7070/tcp open  realserver
MAC Address: F8:28:19:D5:81:7F (Liteon Technology)

Nmap done: 1 IP address (1 host up) scanned in 4.61 seconds
```

Description:-

Scans a TCP SYN to check the target port with SY ACK or RST

Nmap Scan Methods

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.1.7
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-01 08:27 EDT
Nmap scan report for 192.168.1.7
Host is up (0.00092s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
5357/tcp open  wsdapi
7070/tcp open  realserver
MAC Address: F8:28:19:D5:81:7F (Liteon Technology)

Nmap done: 1 IP address (1 host up) scanned in 4.42 seconds
```

Description:-

Checks the complete TCP three-way handshake

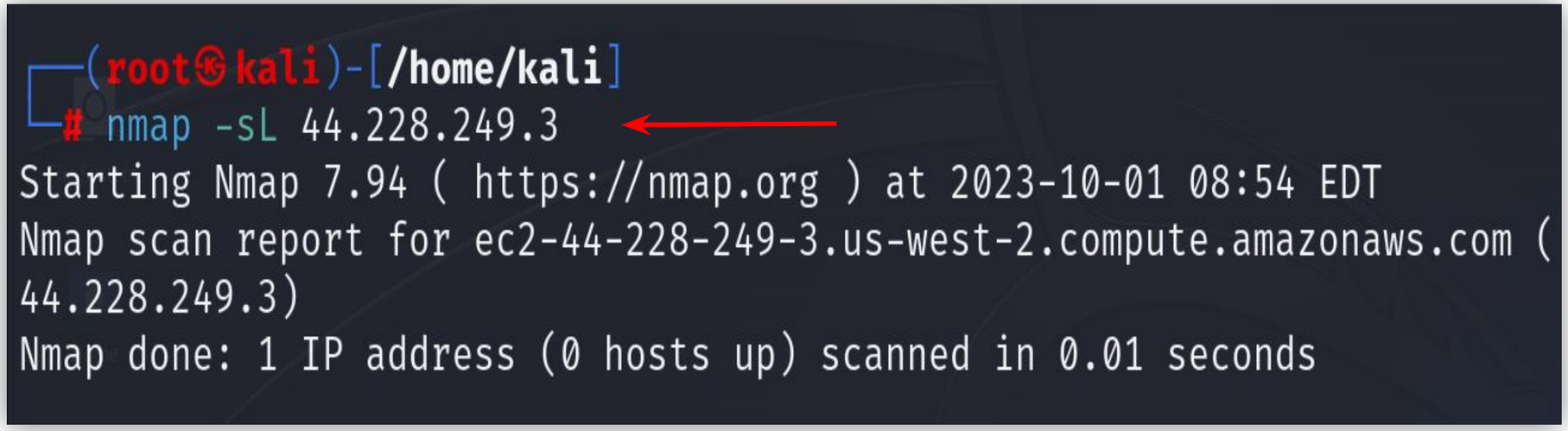
Nmap Scan Methods

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sU 192.168.1.7
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-01 08:27 EDT
Nmap scan report for 192.168.1.7
Host is up (0.00037s latency).
Not shown: 999 open|filtered udp ports (no-response)
PORT    STATE SERVICE
137/udp open  netbios-ns
MAC Address: F8:28:19:D5:81:7F (Liteon Technology)

Nmap done: 1 IP address (1 host up) scanned in 9.02 seconds
```

Description:-

Scans the UDP ports

Nmap Scan Methods



Description:-

Lists the Targets to scan.

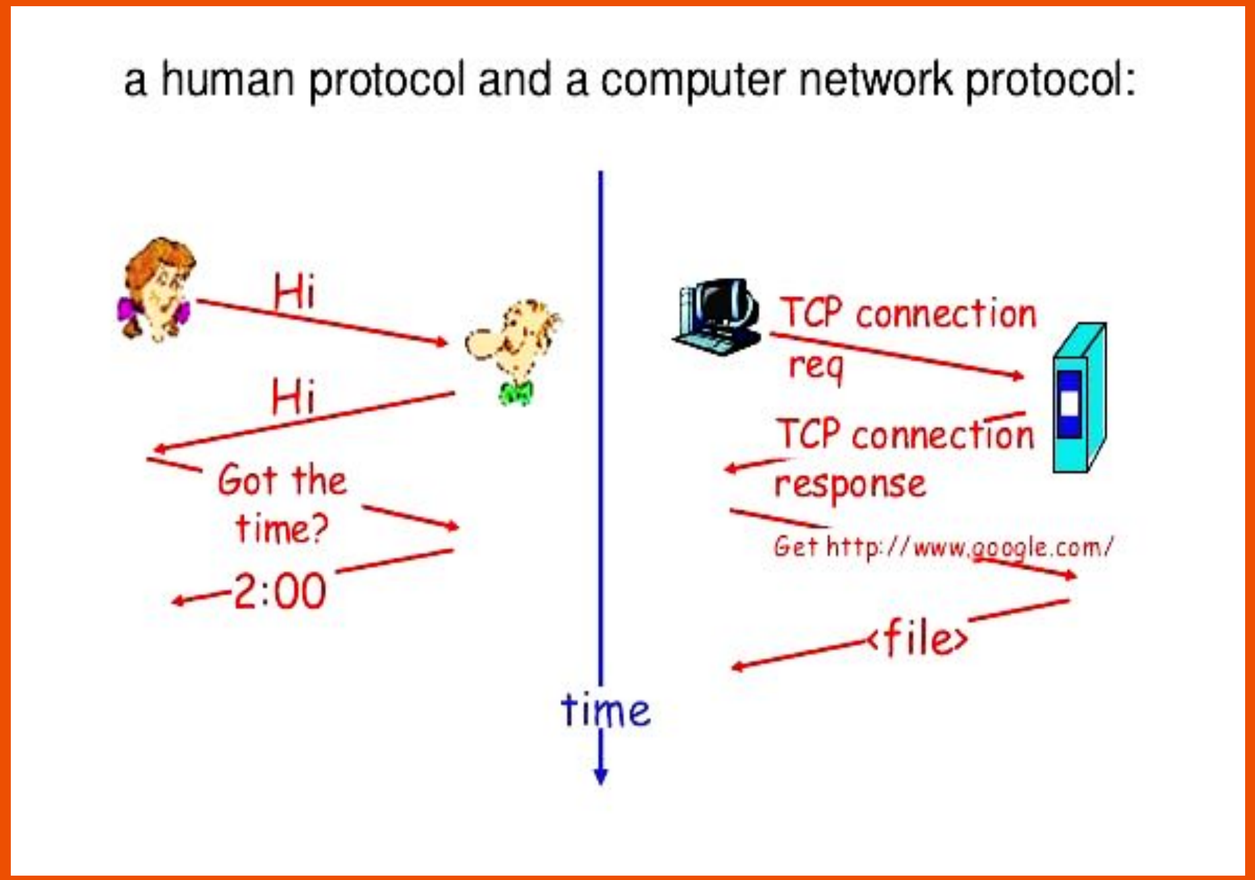
Nmap Scan Methods

Description:-

Lists the Targets to scan.

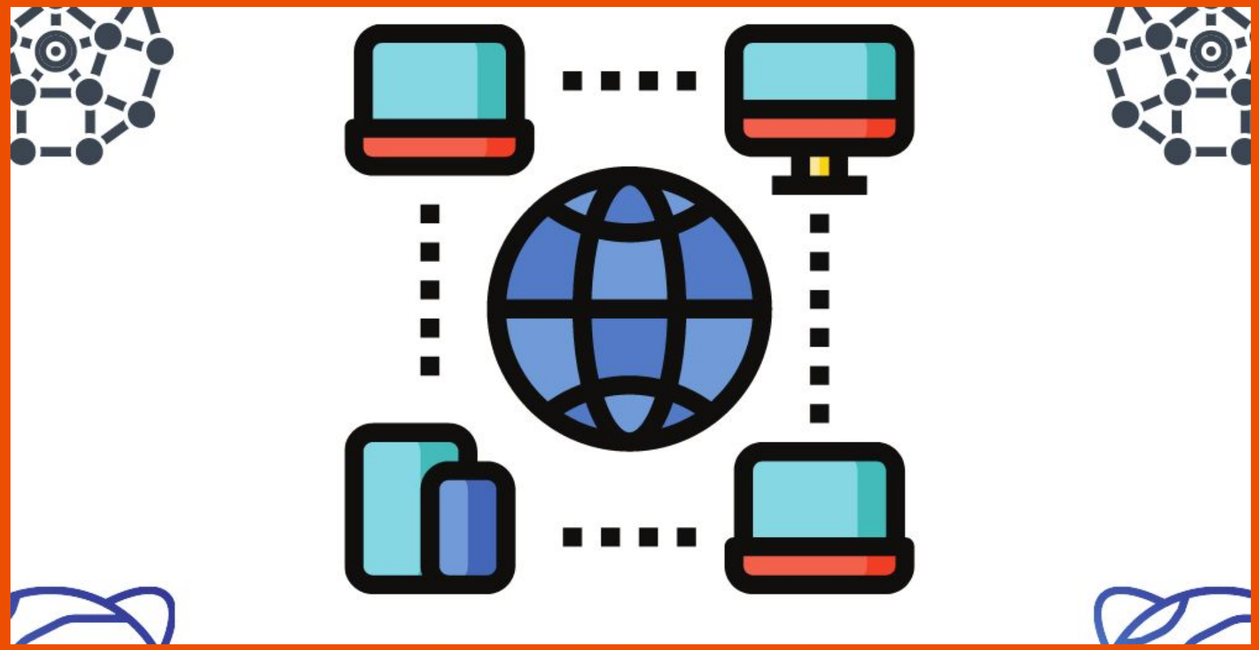
Introduction to Protocol

- *Rules and standards governing data exchange between networked devices.*
- *Ensure consistent and reliable communication over computer networks.*
- *Define the format, timing, sequencing, and error handling of data.*



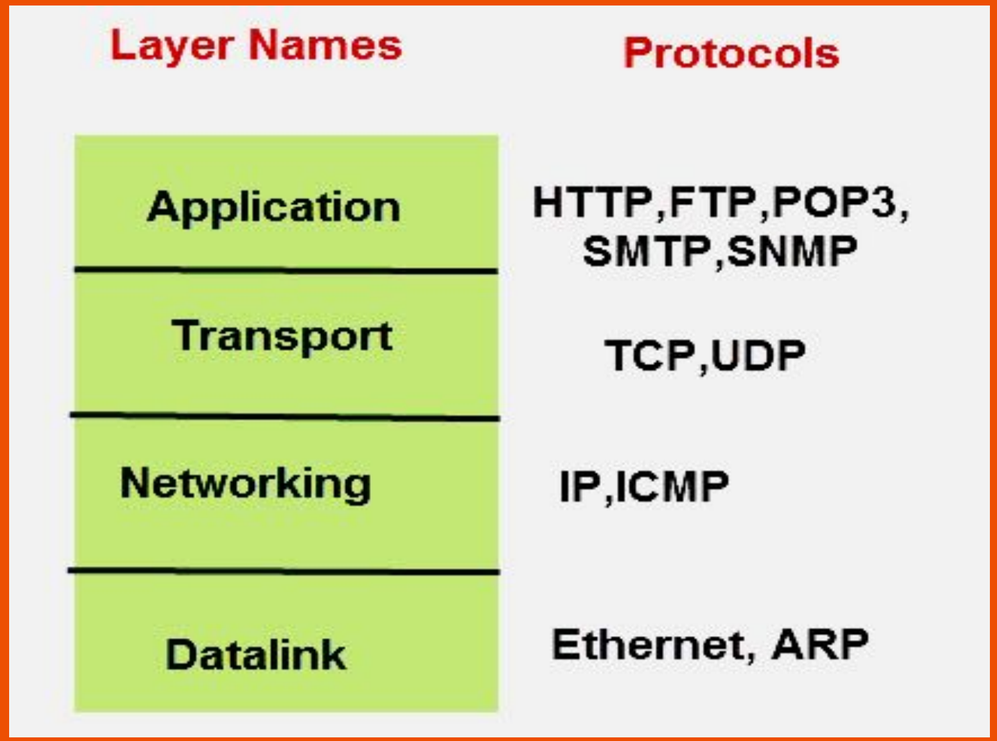
Role of Protocol in Communication

- *Establish communication rules for devices to understand and interpret data.*
- *Enable data transmission, addressing, routing, and error detection and correction.*
- *Facilitate compatibility and interoperability among diverse networked systems.*
- *Govern network operations, ensuring efficient and secure data exchange.*



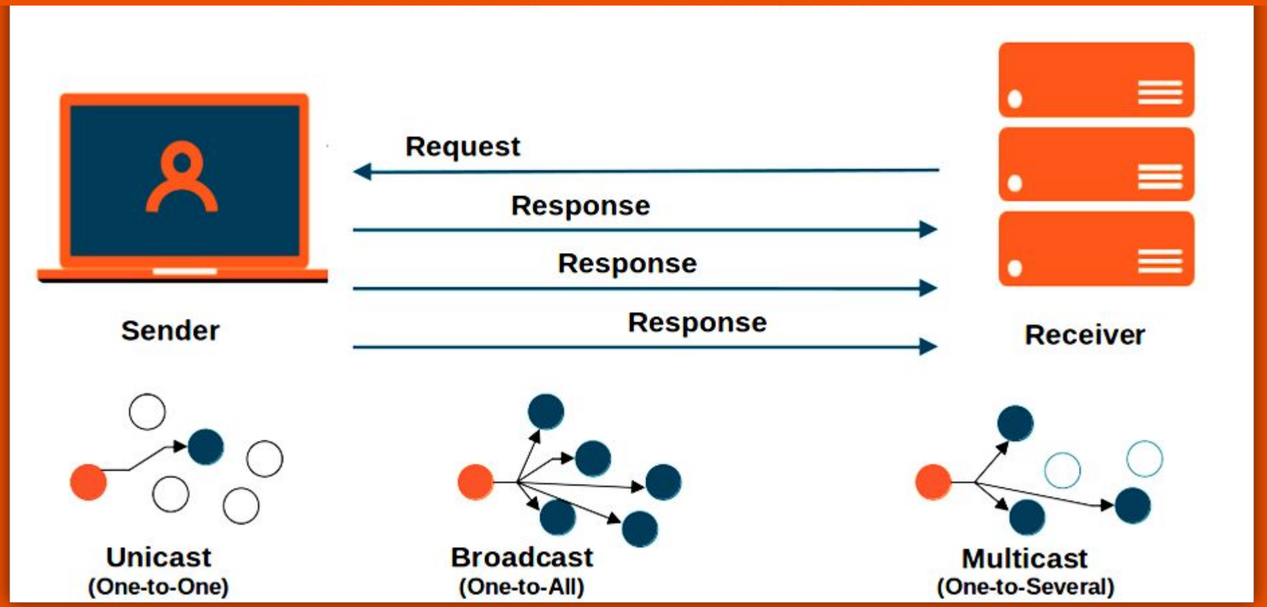
Some Common Protocols:- TCP/IP

- *Internet backbone protocol suite for reliable data transmission and routing.*
- *Includes HTTP (web), SMTP (email), FTP (file transfer).*
- *Ensures data integrity and order with connection-oriented communication.*
- *Powers most internet services.*



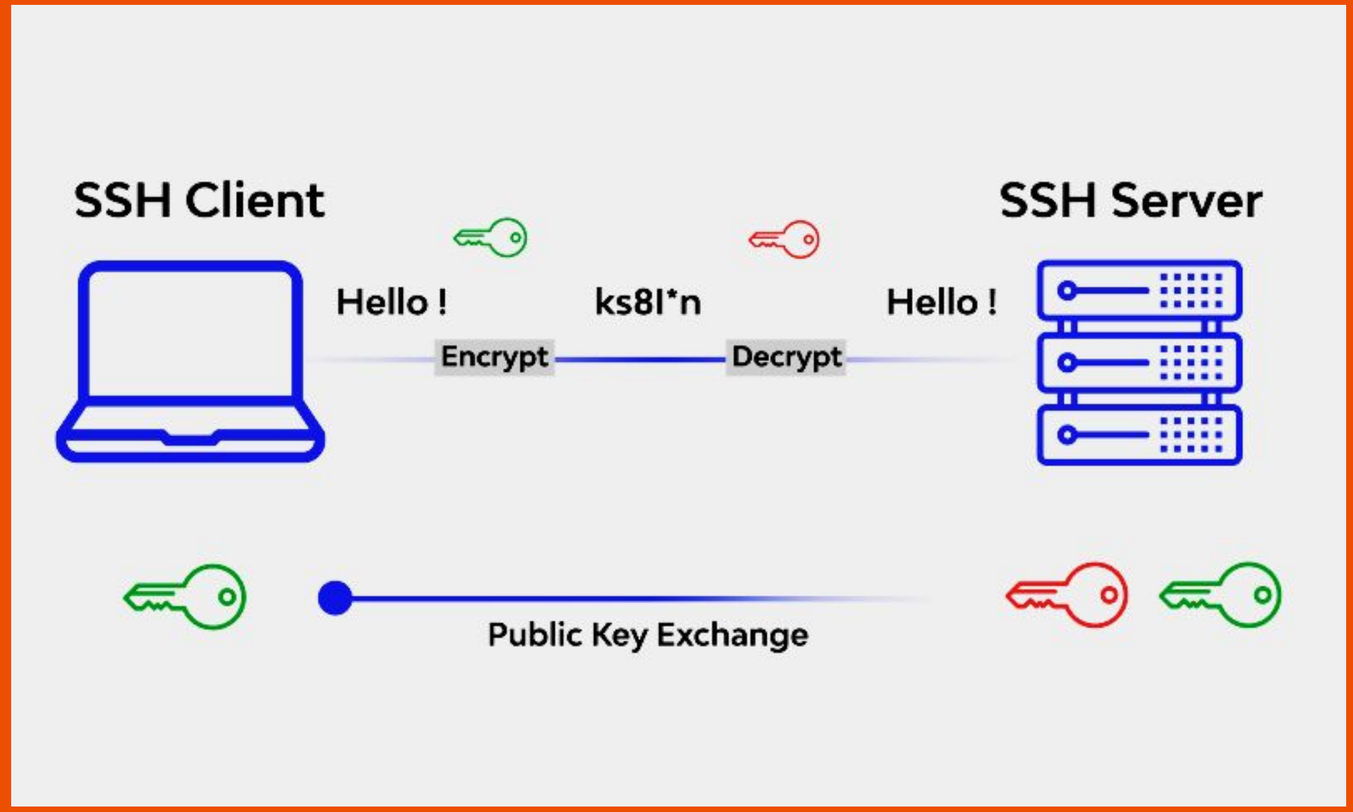
Some Common Protocols:- UDP

- *Lightweight, connectionless protocol for fast data transmission, ideal for real-time.*
- *Used in VoIP, video streaming, online gaming, and DNS.*
- *No handshaking, which can lead to faster, but less reliable, data transfer.*
- *Efficient for time-sensitive applications.*



Some Common Protocols:- SSH

- *Secure Shell protocol provides encrypted remote access and secure file transfers.*
- *Replaces insecure protocols like Telnet and FTP.*
- *Strong authentication and encryption for secure communication over networks.*
- *Commonly used for server administration.*

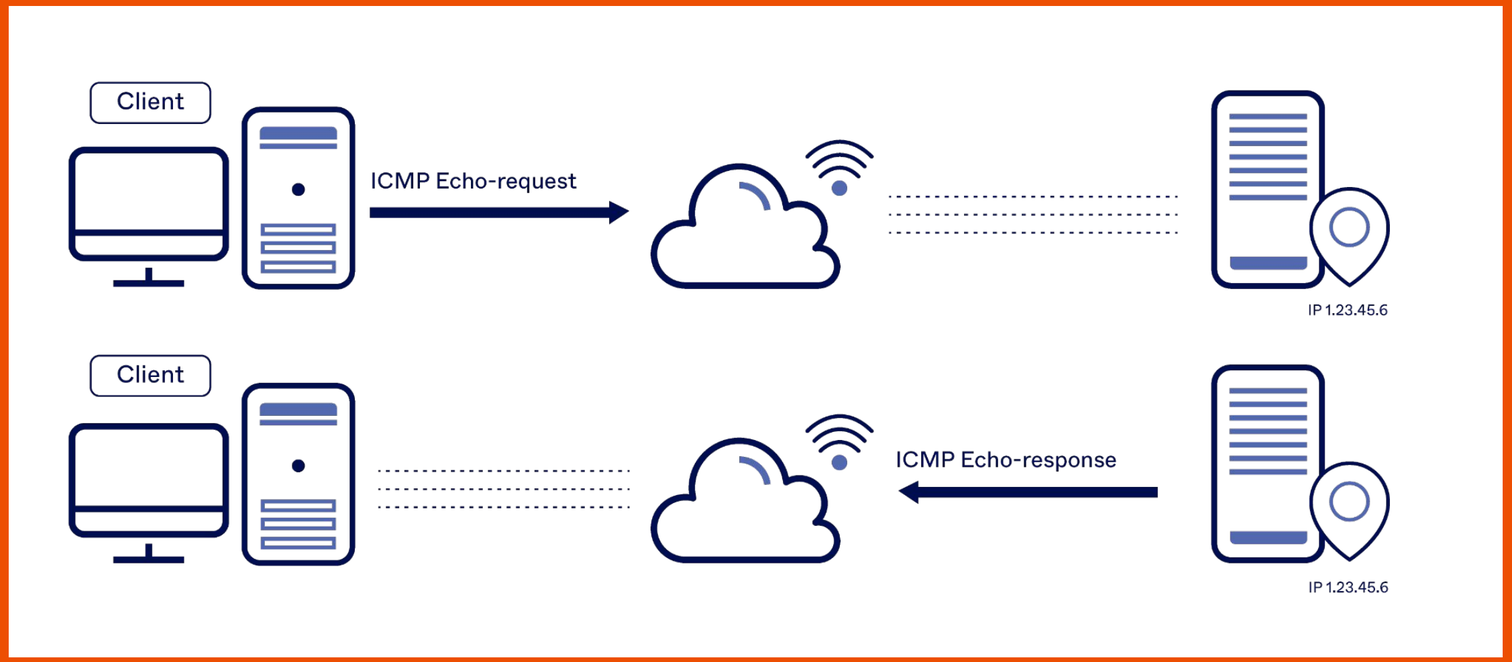


Some Common Protocols:- SSL/TLS

- *Secure Sockets Layer and Transport Layer Security protocols encrypt internet data.*
- *Essential for HTTPS, securing web transactions and user privacy.*
- *Provides authentication, data integrity, and confidentiality for online communication.*
- *Safeguards against eavesdropping and data tampering.*

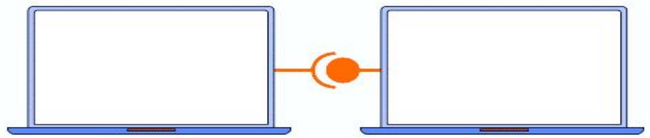
Some Common Protocols:- ICMP

- *Internet Control Message Protocol used for network error messages and diagnostics.*
- *Supports tools like Ping and Traceroute.*
- *Not typically used for data transfer but aids network troubleshooting.*
- *Essential for network health monitoring and error reporting.*

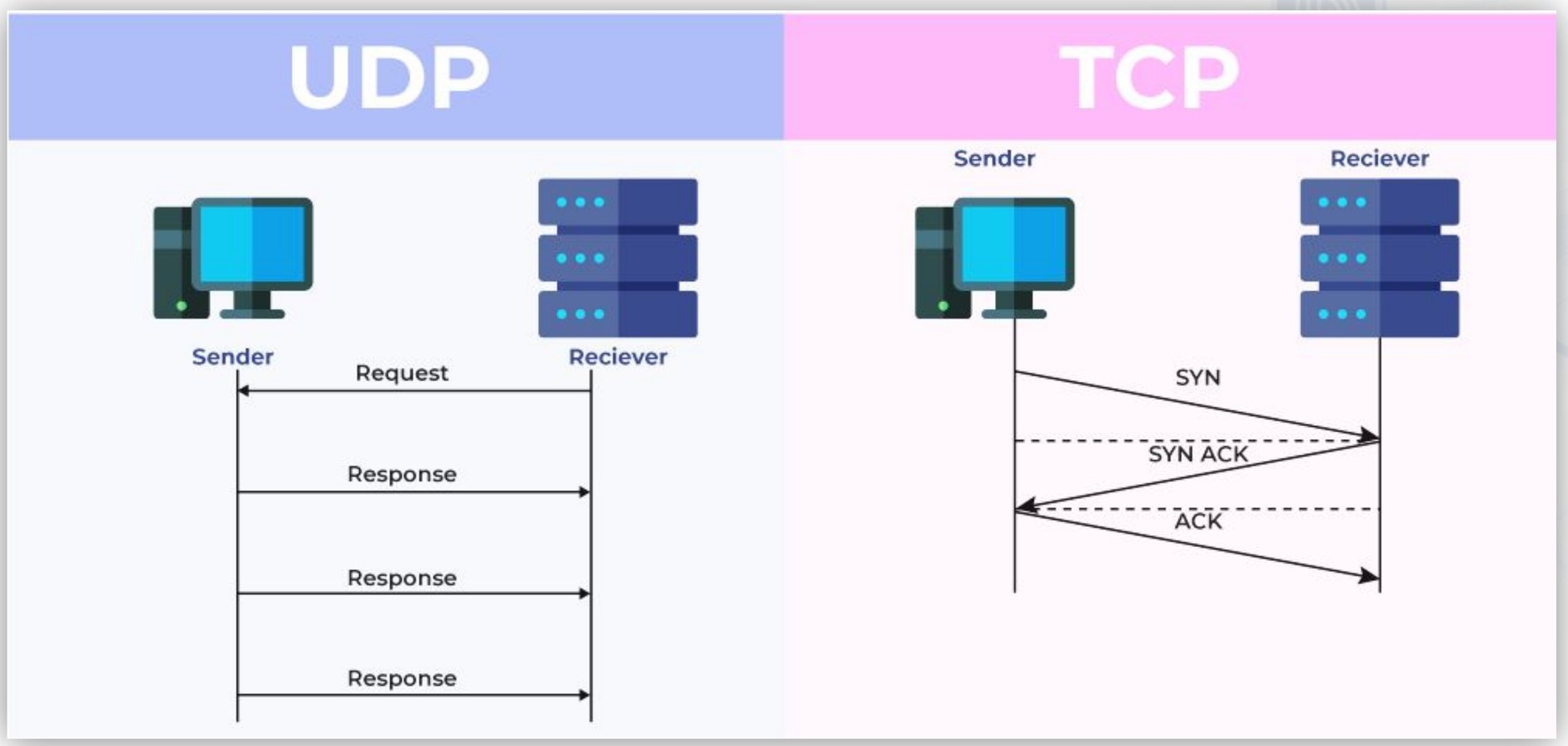


TCP VS UDP

TCP	UDP
Creates a connection between two devices	Sends data without a connection
Breaks data into packets with sequence numbers	Doesn't assign sequence numbers
Sends packets and waits for acknowledgments	Sends packets without waiting for acknowledgment
Re-sends lost packets to make sure all data is received	Doesn't re-sent lost packets
Gets data packets in the correct order	Delivers packets as they arrive, which may be out-of-order



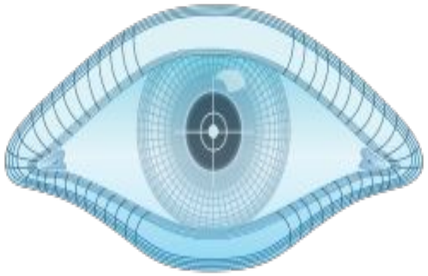
TCP VS UDP


UDP
TCP
Sender
Reciever
Request
Response
Response
Response
Sender
Reciever
SYN
SYN ACK
ACK

Port Scanning Tool:- Zenmap

- Zenmap is a network scanning tool that is used for Network Discovery & Vulnerability Assessment.

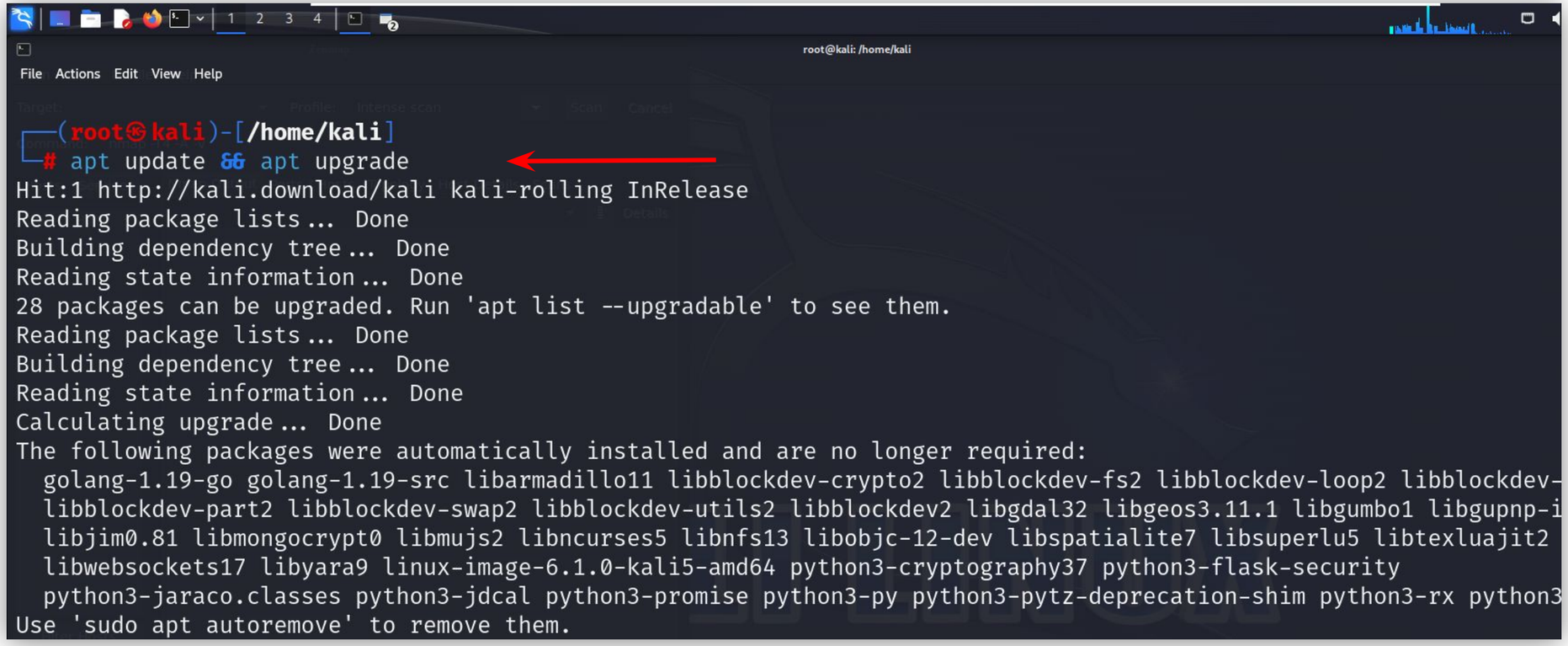
Network scanning tool for discovering vulnerabilities and network topology.



ZENMAP

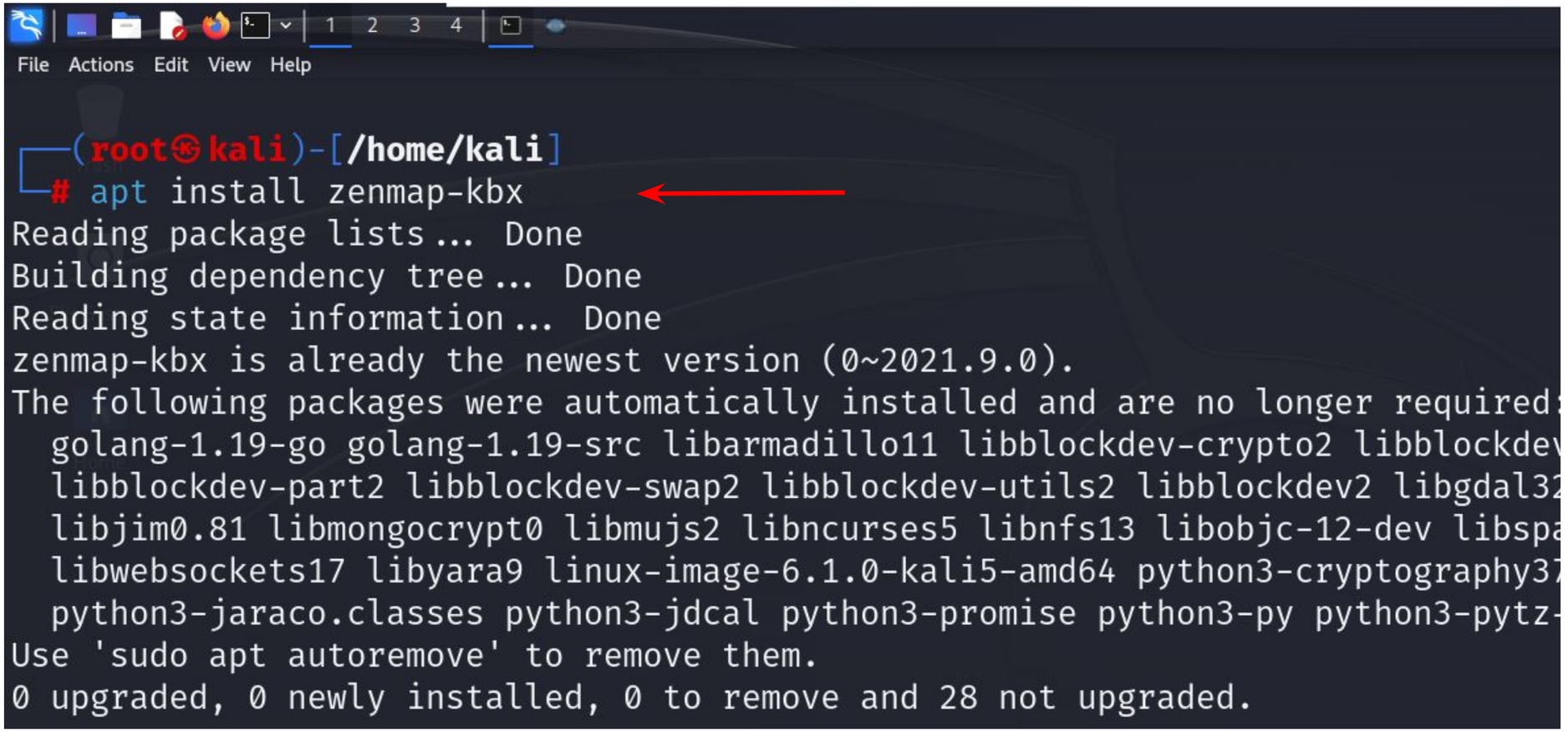
Provides GUI interface to Nmap, offering ease of use and analysis.

Installation of Zenmap



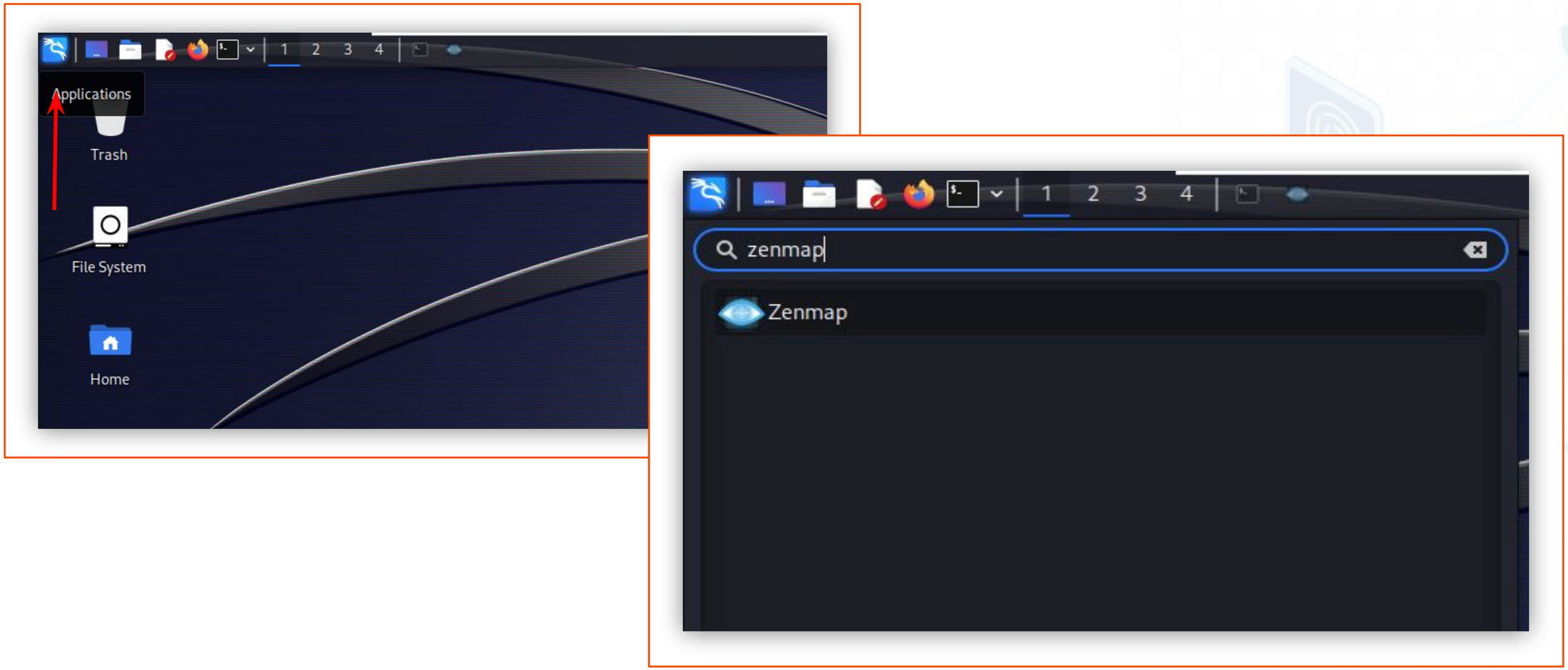
- Firstly we have to update our system to install the Zenmap

Installation of Zenmap



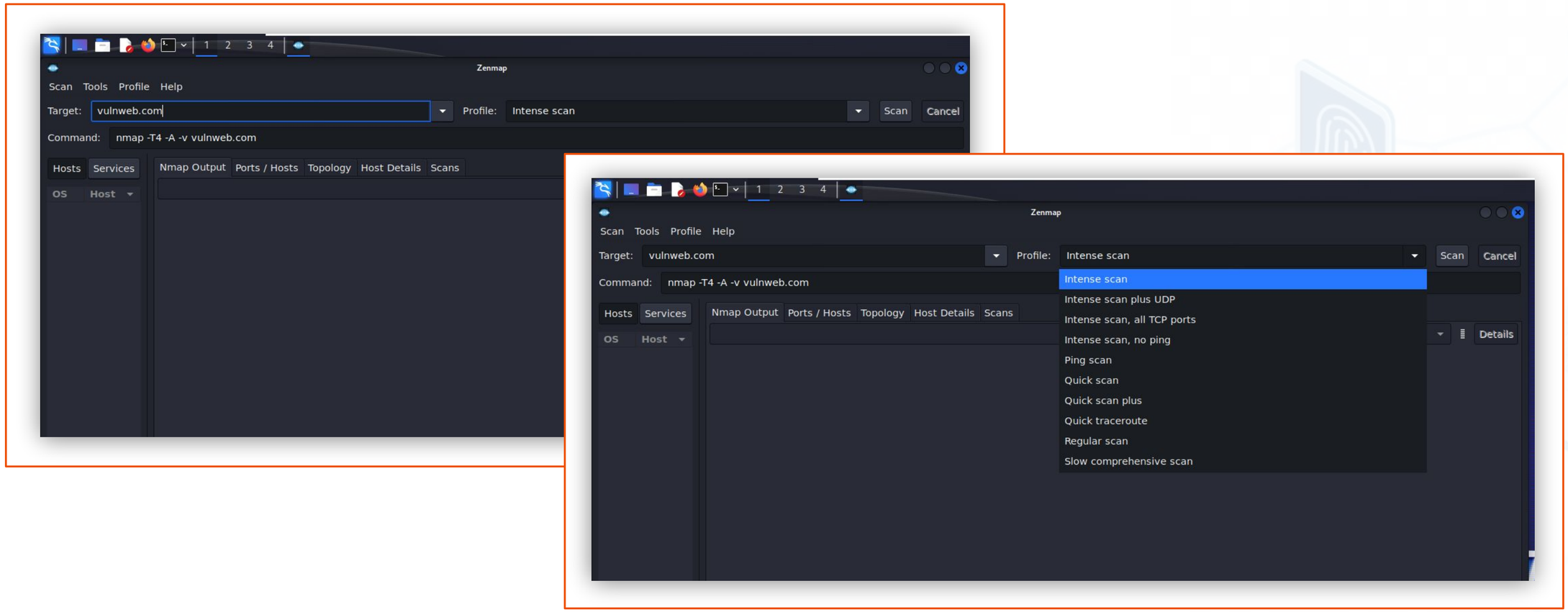
- Then we have to install Zenmap using this command (*apt install zenmap-kbx)*

How to use Zenmap



- After Completing the installation part you have to click on Kali linux image on top left corner then search for zenmap.

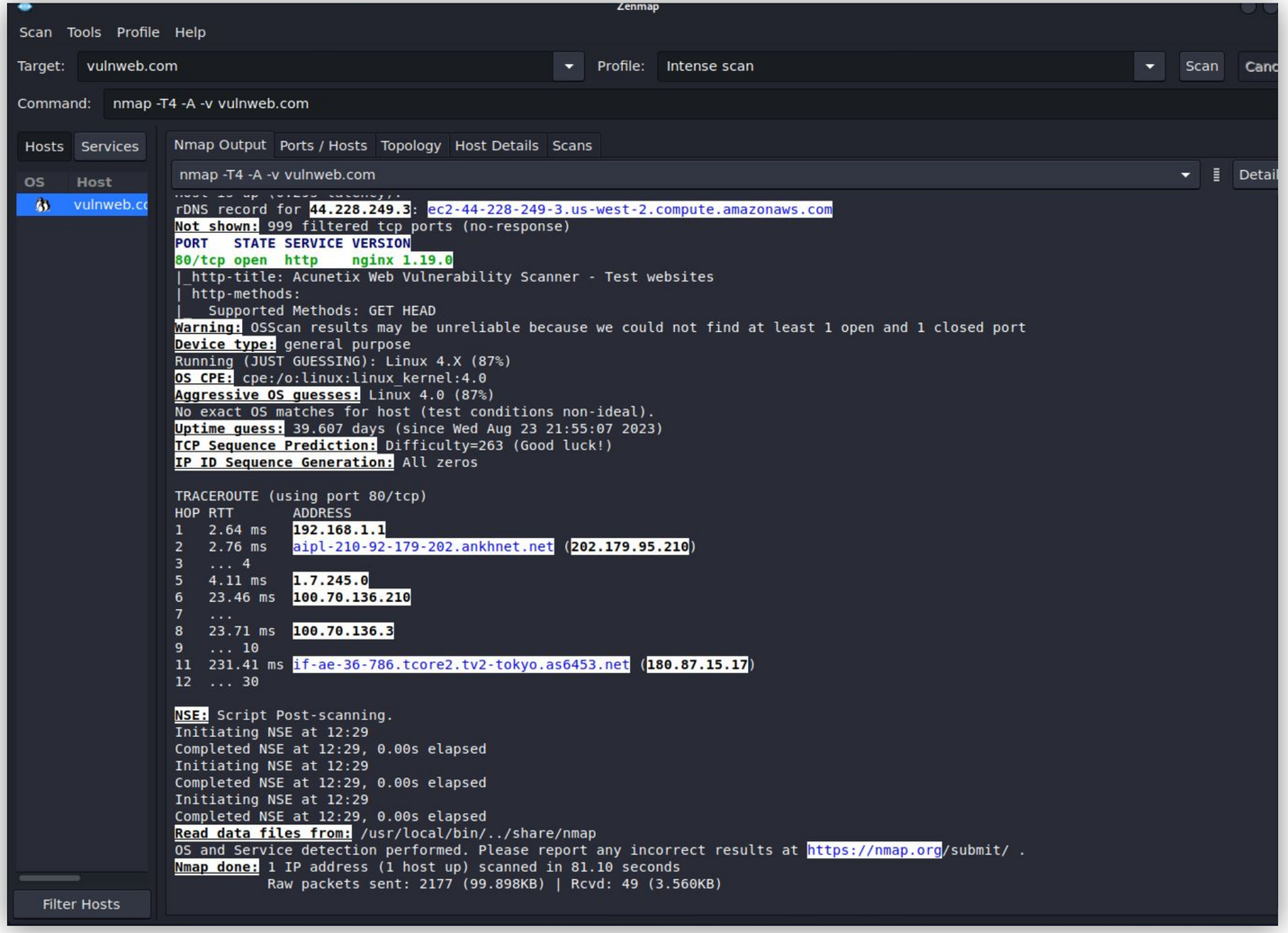
How to use Zenmap



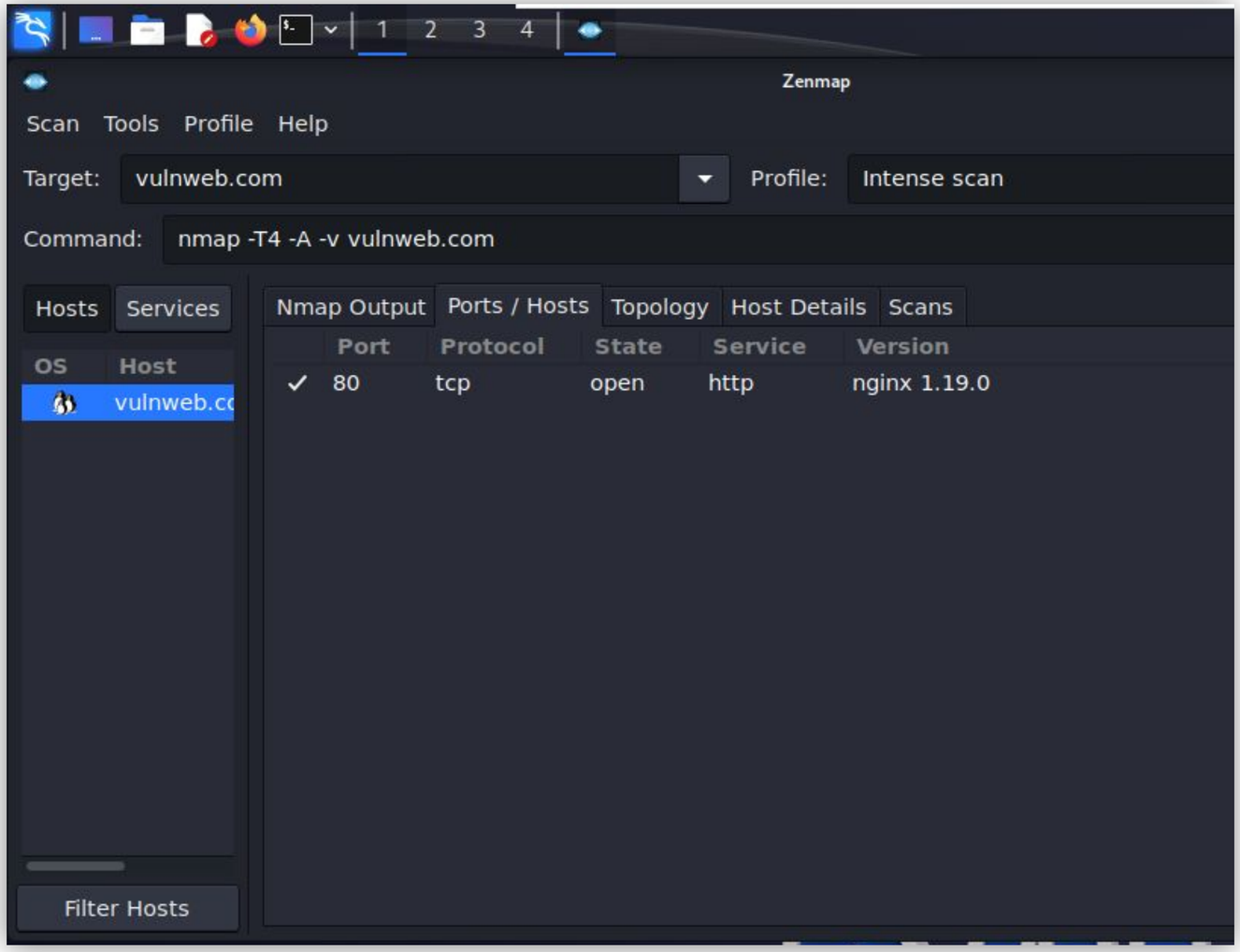
- Here you have to give target and select which type of scan you wanna do.
- In Command section you can change the command as you want then click on scan.

How to use Zenmap

- The "Nmap Output" section displays detailed results of network scans, including open ports, service information, and potential vulnerabilities.

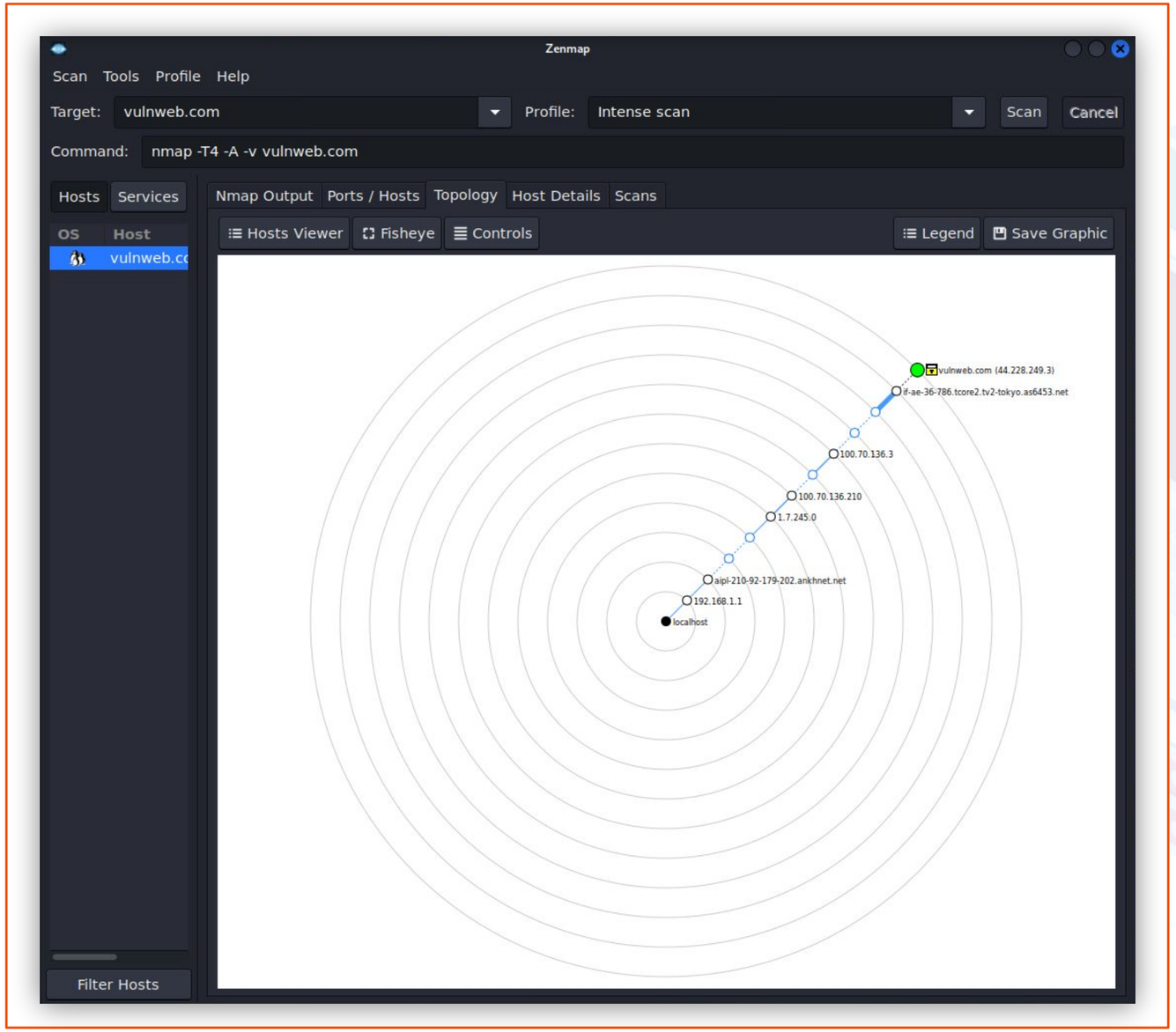


How to use Zenmap



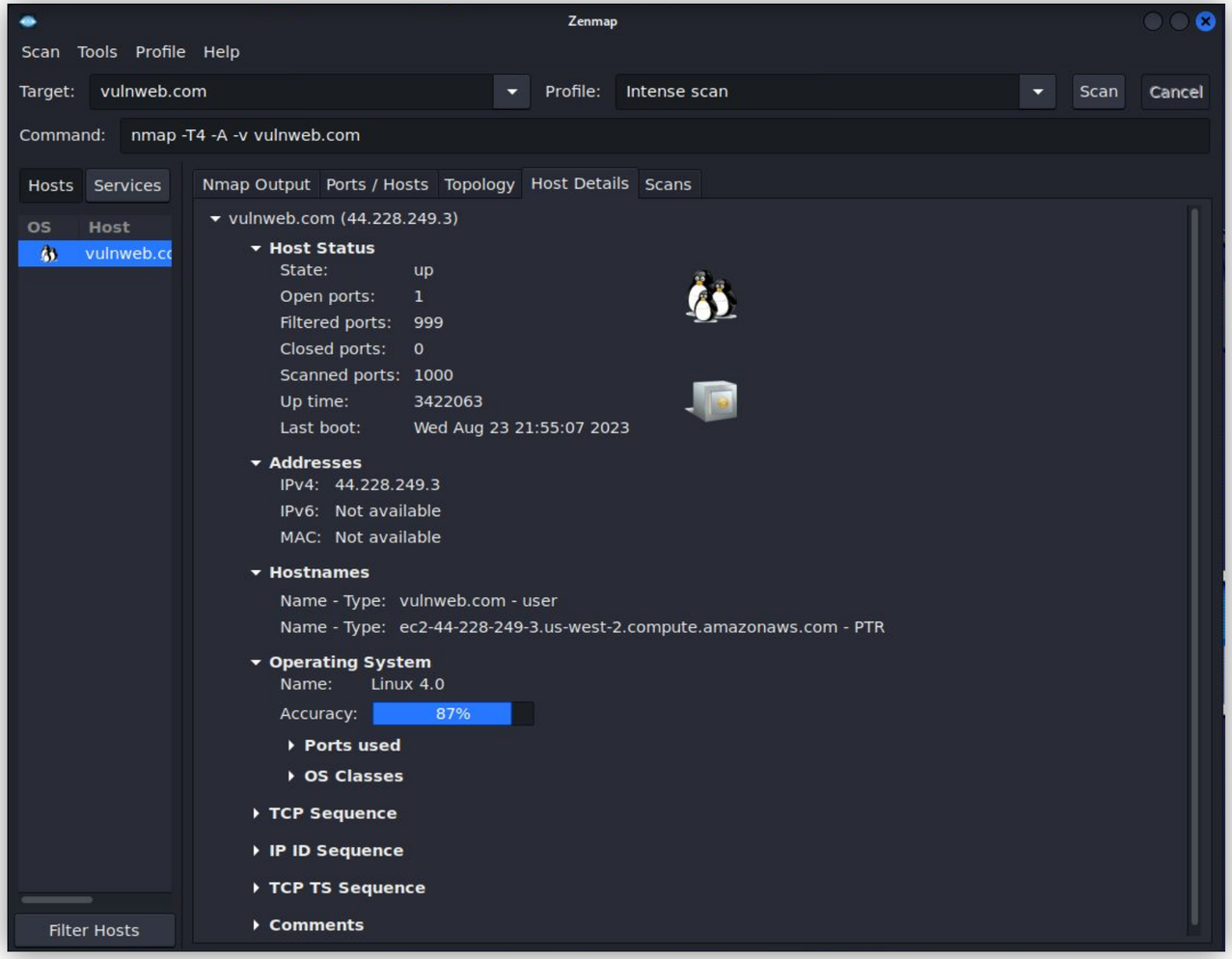
- The "Ports/Hosts" section displays discovered network hosts and open ports, revealing the structure and accessibility of the network.

How to use Zenmap



- Topology section provides a visual representation of network device connections and relationships.

How to use Zenmap



- The Host Details section displays comprehensive information about a scanned network host, including open ports, services, and operating system details.

6

Assessment

1. Perform Nmap on hacktify.in and find total open ports

2. Create a file and Change Filename and check integrity remains same or not?

Thank you