**Network Scanning**

**Index:**

|  |  |
| --- | --- |
| 1. **Overview of Network Scanning** | 2 |
| 1. **TCP Communication Flags** | 2-3 |
| 1. **TCP/IP communication** | 3 |
| 1. **Scanning Tools:** 2. **Nmap** 3. **Hping3** | 3-5 |
| 1. **Host Discovery Techniques** | 5 |
| 1. **Nmap** | 6-15 |
| 1. **OS discovery** | 16 |
| 1. **OS discovery using NMAP script engine** | 16-17 |
| 1. **IDS and Firewalls** | 17-18 |
| 1. **Packet fragmentation** | 18 |
| 1. **Source Routing** | 19 |
| 1. **Source Port Manipulation** | 19 |
| 1. **IP Address Decoy** | 19 |
| 1. **IP Address Spoofing** | 19 |
| 1. **Proxy Servers** | 19 |
| 1. **Anonymizers** | 20 |
| 1. **Zenmap** | 21-22 |
| 1. **Hping3** | 23 |
| 1. **Scanning a target network using Metasploit** | 23-29 |

**Overview of Network Scanning:**

Here are the four major objectives of network scanning in ethical hacking and cybersecurity:

1. Identifying Live Hosts: Detect active devices within a network to map targets for further investigation or testing.
2. Port Identification: Determine open, closed, or filtered ports to assess potential entry points for unauthorized access.
3. Service and Version Detection: Identify services running on open ports and their software versions to detect vulnerabilities or outdated applications.
4. Discovering Network Vulnerabilities: Scan for weak configurations, known vulnerabilities, or misconfigurations to assess the security posture of systems.

**TCP Communication Flags:**

In TCP (Transmission Control Protocol) communication, flags are control bits in the TCP header that manage the state and flow of connections. Each flag has a specific purpose, helping to initiate, control, and terminate connections. Here’s a summary of the most important TCP flags:

1. SYN (Synchronize)

Initiates a new connection by synchronizing sequence numbers between sender and receiver.

Used during the first step of the threeway handshake.

2. ACK (Acknowledgment)

Confirms the receipt of data or a connection request.

Set in most TCP segments after the handshake begins.

3. FIN (Finish)

Requests graceful termination of the connection.

Both sides exchange FIN flags to close the session.

4. RST (Reset)

Abruptly terminates a connection in case of errors or unexpected conditions.

Used to reject unwanted connections or reset faulty sessions.

5. PSH (Push)

Instructs the receiver to process the data immediately, without buffering.

Useful for sending realtime data, like chat messages.

6. URG (Urgent)

Marks a segment as urgent, giving it priority over other data in the queue.

The Urgent Pointer field specifies the end of the urgent data.

These flags help maintain reliable data transmission and control the state of communication between devices.

**TCP/IP communication:**

The TCP 3way handshake is a process used to establish a reliable connection between a client and server.

1. SYN: The client sends a SYN packet to request a connection, indicating its sequence number.
2. SYNACK: The server responds with a SYNACK packet, acknowledging the client’s request and providing its own sequence number.
3. ACK: The client sends an ACK packet, confirming the connection.

After this exchange, both devices are synchronized and can begin secure data transmission. The handshake ensures proper connection setup before communication.

**Scanning Tools:**

1. **NMAP:**

**What’s Nmap**

Nmap (Network Mapper) is an open-source tool used for network discovery and security auditing. It scans IP addresses, hosts, and ports to identify active devices, services, and potential vulnerabilities on a network.

**Why Use Nmap**

Nmap helps ethical hackers, security professionals, and administrators map network infrastructures, detect unauthorized devices, find open ports, and assess vulnerabilities. It’s essential for penetration testing and maintaining network security.

**Advantages of Nmap**

* Supports multiple scan types (TCP, UDP, SYN, etc.).
* Identifies live hosts, open ports, and running services.
* Detects vulnerabilities by discovering software versions.
* Scalable for small and large networks.

**Disadvantages of Nmap**

* May trigger security alerts (detected as malicious scanning).
* Ineffective against firewalls or IDS that block scans.
* Requires experience for interpreting complex outputs.
* Slow performance when scanning large networks.

**Syntax of Major Nmap Commands**

* **Basic Scan:** nmap <IP>
* **Port Scan:** nmap -p 80,443 <IP>
* **Service Detection:** nmap -sV <IP>
* **Operating System Detection:** nmap -O <IP>
* **Scan a Range:** nmap <IP range>

**How to Protect from Nmap Scanning**

* Implement **firewalls** to block suspicious traffic.
* Use **Intrusion Detection Systems (IDS)** to detect scans.
* Enable **port knocking** for critical ports.
* Regularly close unnecessary or unused ports.
* Monitor network traffic for unusual scanning behavior.

1. **Hping3:**

**What’s Hping3**

Hping3 is a command-line tool used for network scanning, auditing, and packet crafting. It supports sending custom TCP, UDP, and ICMP packets, allowing testers to analyze networks, detect vulnerabilities, and simulate attacks like DoS.

**Why Use Hping3**

Hping3 allows ethical hackers and security professionals to craft custom packets for testing firewalls, network paths, and intrusion detection systems. It is used for advanced port scanning, packet spoofing, and performance analysis.

**Advantages of Hping3**

* Supports customized packet creation for testing purposes.
* Can simulate DoS attacks for stress testing.
* Bypasses some firewalls with stealth packet injections.
* Enables traceroute and time delay measurements.

**Disadvantages of Hping3**

* Requires expertise to properly craft and interpret packets.
* Can be blocked by firewalls or intrusion detection systems.
* Can generate network instability if misused.
* Less user-friendly than automated scanning tools like Nmap.

**Syntax of Major Commands of Hping3**

* **Ping a Host:** hping3 <IP>
* **TCP Port Scan:** hping3 -S -p 80 <IP>
* **UDP Scan:** hping3 --udp -p 53 <IP>
* **Packet Spoofing:** hping3 -a <spoofed IP> <target IP>
* **Traceroute:** hping3 --traceroute <IP>

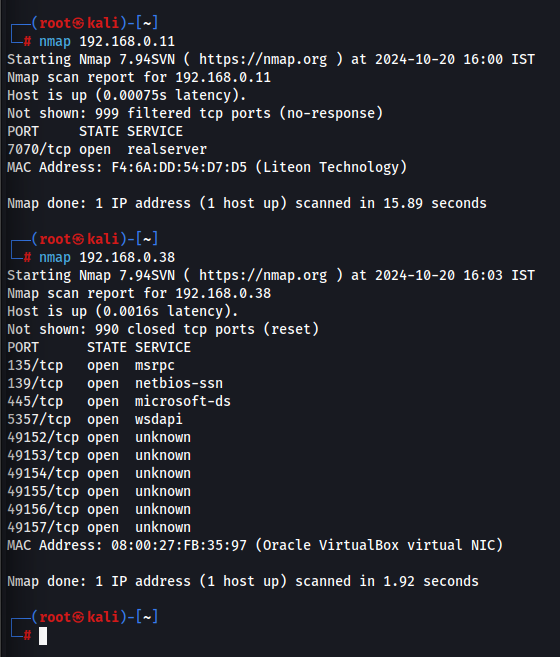
**How to Protect from Hping3 Scanning**

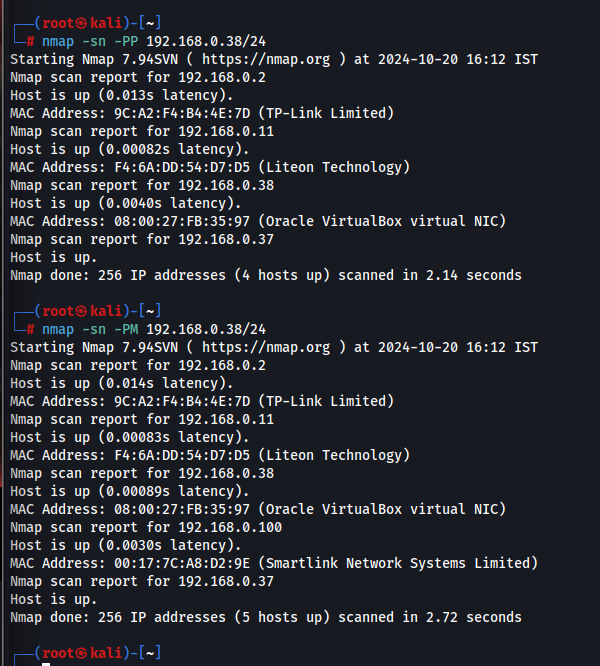
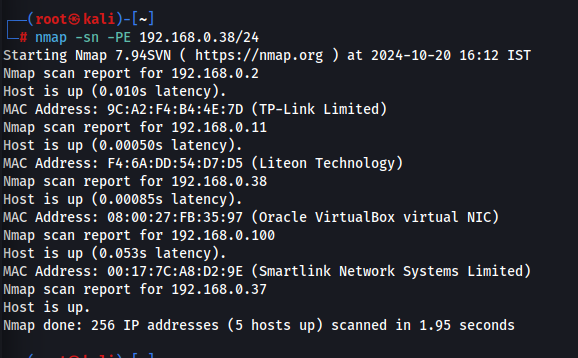
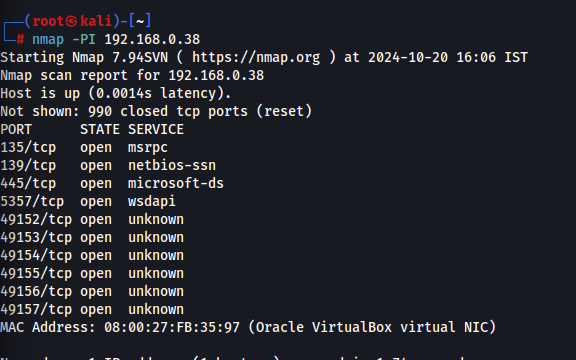
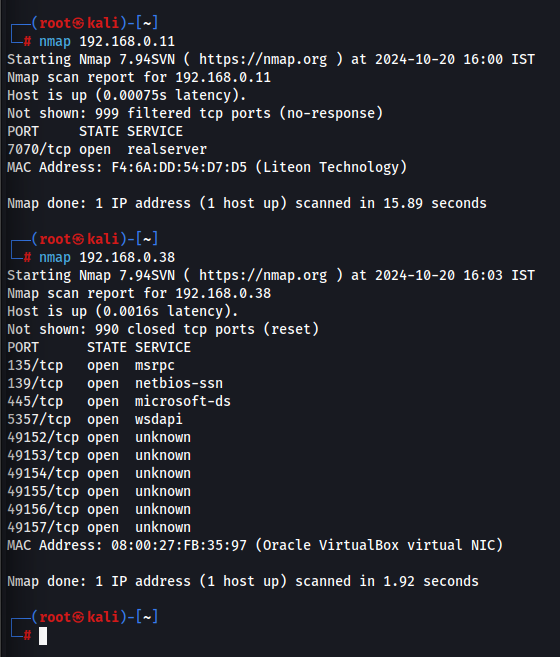
* Use **firewalls** to block malicious packets.
* Implement **rate-limiting** to prevent DoS attempts.
* Monitor for unusual traffic with **IDS/IPS**.
* Disable unnecessary ports and services.
* Use **anti-spoofing rules** to block spoofed packets.

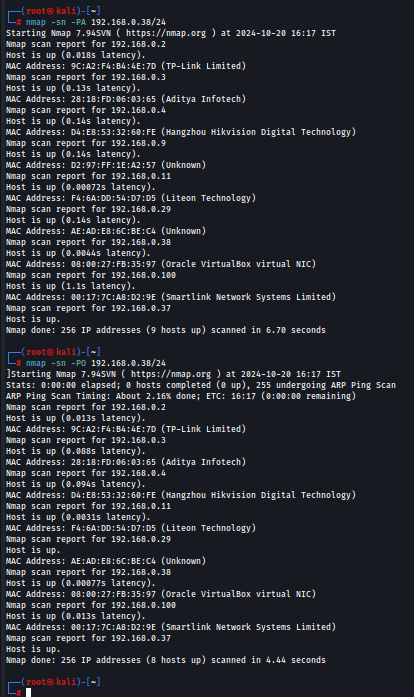
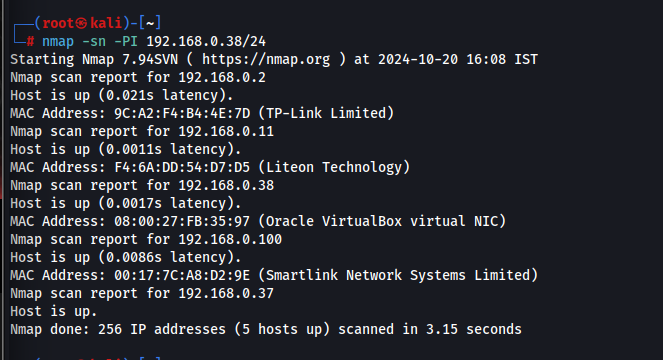
**Host Discovery Techniques:**

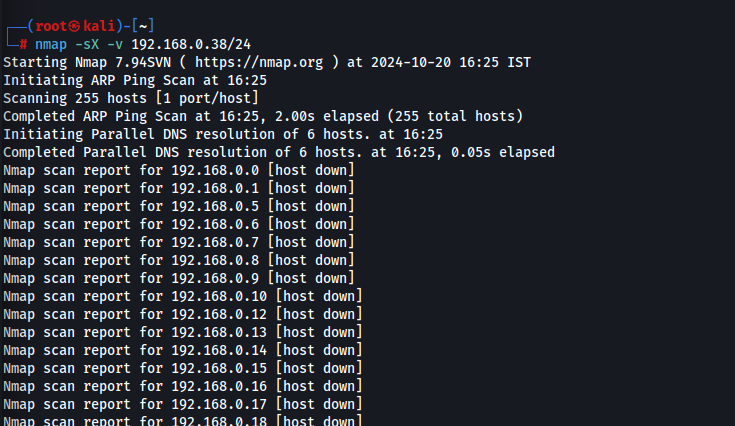
| **Method** | **Protocol/Layer** | **Scope** | **Tools** |
| --- | --- | --- | --- |
| ICMP Ping Sweep | ICMP (Layer 3) | Any Network | Ping, Fping, Nmap |
| ARP Ping | ARP (Layer 2) | Local Network (LAN) | Arp-scan, Netdiscover |
| TCP SYN Scan | TCP (Layer 4) | Any Network | Nmap |
| UDP Ping | UDP (Layer 4) | Any Network | Nmap |
| DNS Discovery | DNS (Layer 7) | External/Internal | Nslookup, Dig |
| SNMP Walk | SNMP (Layer 7) | Internal Network | Snmpwalk |
| Passive Monitoring | - | Local Network | Wireshark, Tcpdump |

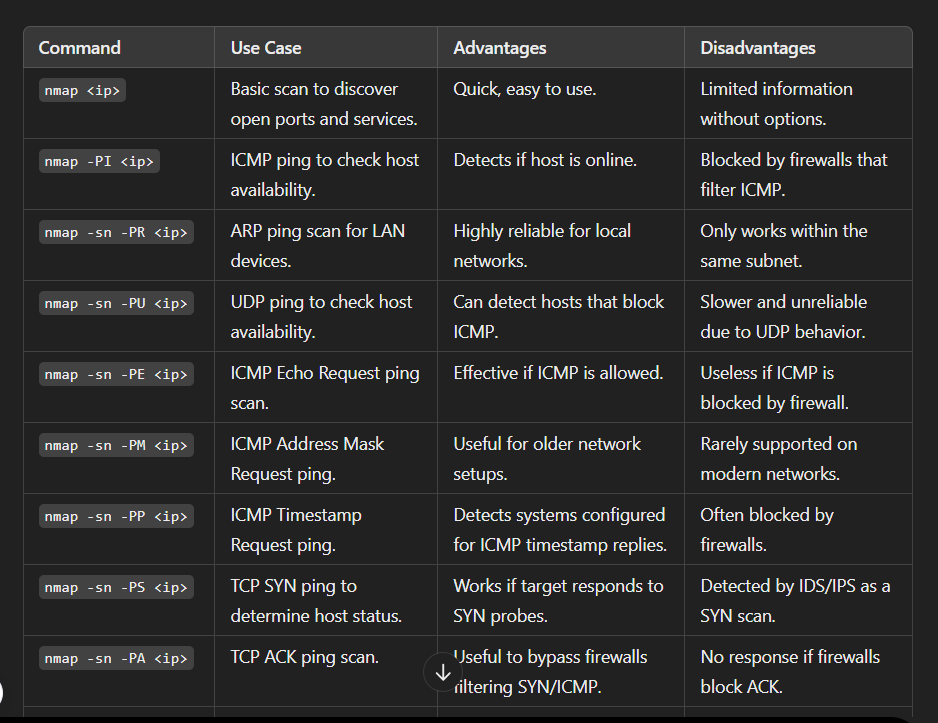
**Nmap:**

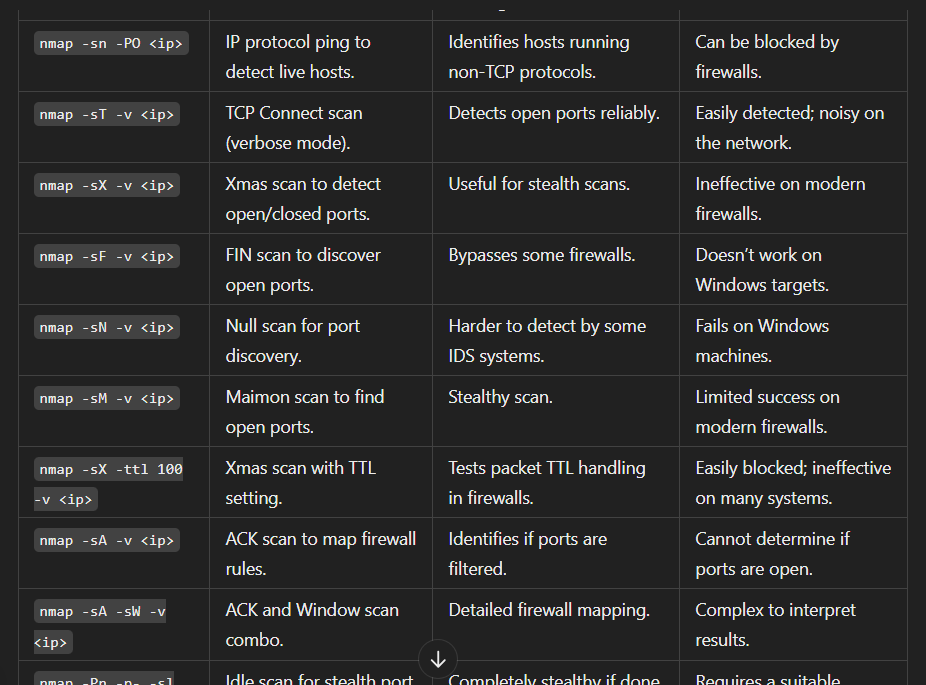
****

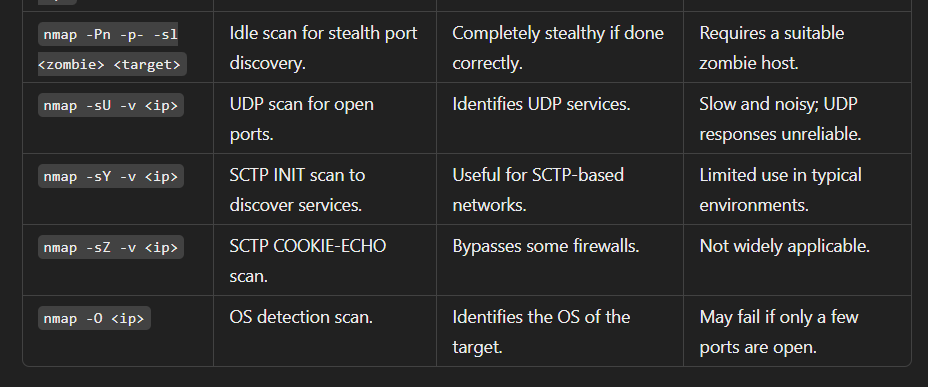
****

****

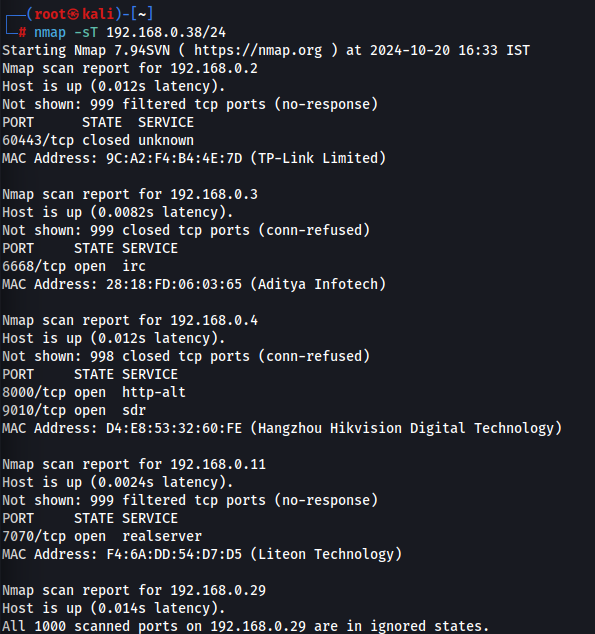
****

****

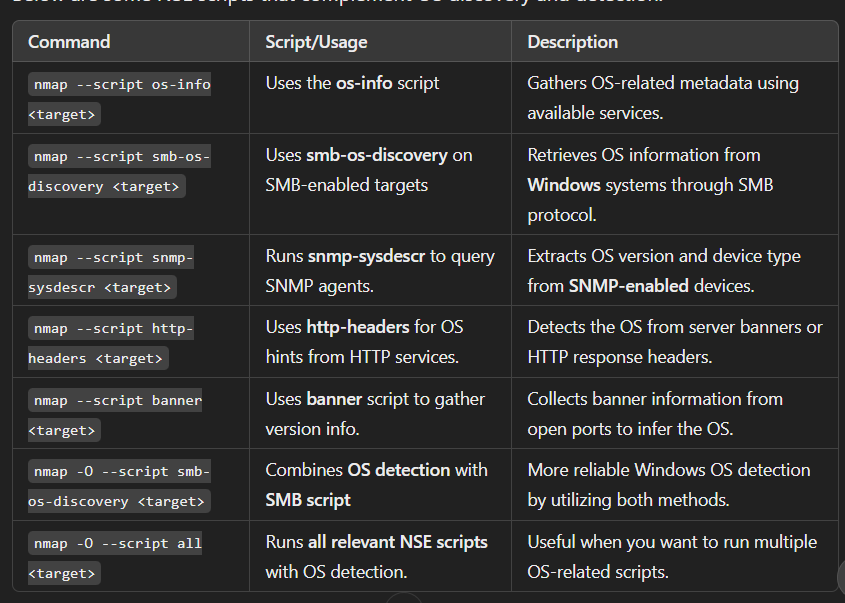
****

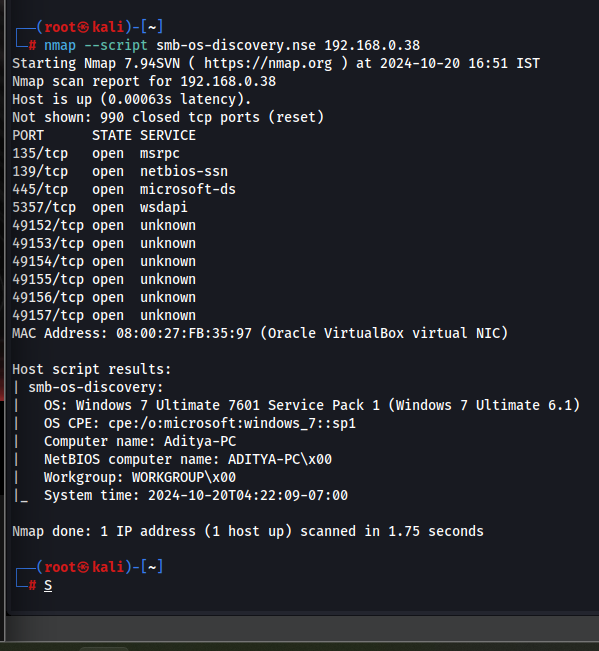
****

**OS discovery:**

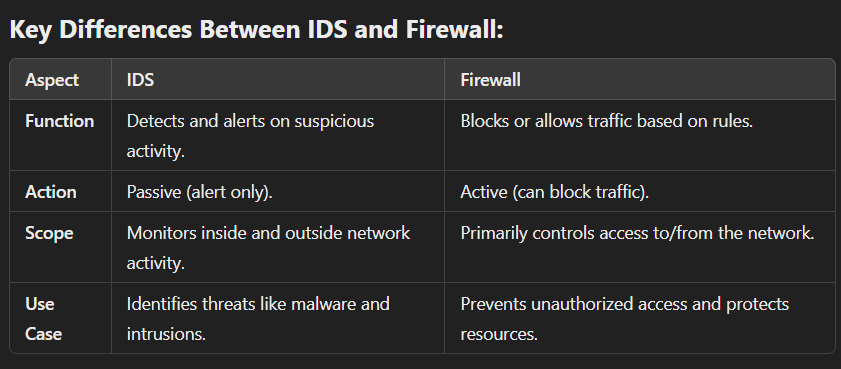
****

**OS discovery using NMAP script engine:**

****

****

**IDS and Firewalls:**

****

**Use of IDS (Intrusion Detection System)**

An IDS monitors network and host activity to detect malicious actions, policy violations, and unusual behavior. It provides real-time threat detection by alerting administrators about attacks such as DoS, brute force attempts, or malware infections. IDS systems analyze traffic patterns to identify deviations from normal baselines and keep logs for forensic investigations. They help detect insider threats by tracking unauthorized internal access. Additionally, IDS tools integrate with systems like SIEM (Security Information and Event Management) to enhance threat intelligence. However, IDS operates passively, only detecting and alerting, without directly blocking attacks.

**Use of Firewalls**

Firewalls control both incoming and outgoing network traffic by acting as a barrier between trusted and untrusted networks, such as the LAN and the Internet. They prevent unauthorized access by blocking or allowing traffic based on predefined security policies, including IP addresses, protocols, and ports. Firewalls protect against malware and exploit attempts by filtering harmful traffic. They can also limit access to specific applications and services, like databases or web servers. Additionally, firewalls provide network address translation (NAT), which hides internal IPs behind a public IP for enhanced security, and offer VPN support for secure remote connections. Firewalls are crucial in preventing DoS attacks by regulating traffic and avoiding flooding attempts.

**IDS Evasion Techniques**

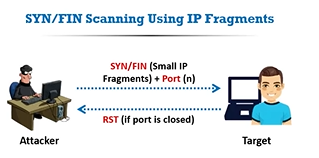
Intrusion Detection Systems (IDS) evasion techniques aim to avoid detection by manipulating traffic patterns. Common methods include fragmentation, where attackers split malicious payloads into smaller packets to bypass detection thresholds, and obfuscation, which alters the attack signatures through encoding or encryption. Additionally, attackers may use protocol tunneling to hide malicious traffic within legitimate protocols, reducing the likelihood of alerts.

**Firewall Evasion Techniques**

Firewall evasion techniques focus on circumventing traffic filtering mechanisms. Techniques include port scanning, where attackers probe for open ports, and using non-standard ports to evade detection. Protocol manipulation, such as using tunneling to encapsulate malicious traffic within allowed protocols, can also bypass firewall rules. Attackers might also employ traffic encryption to obscure content, making it difficult for firewalls to inspect packets.

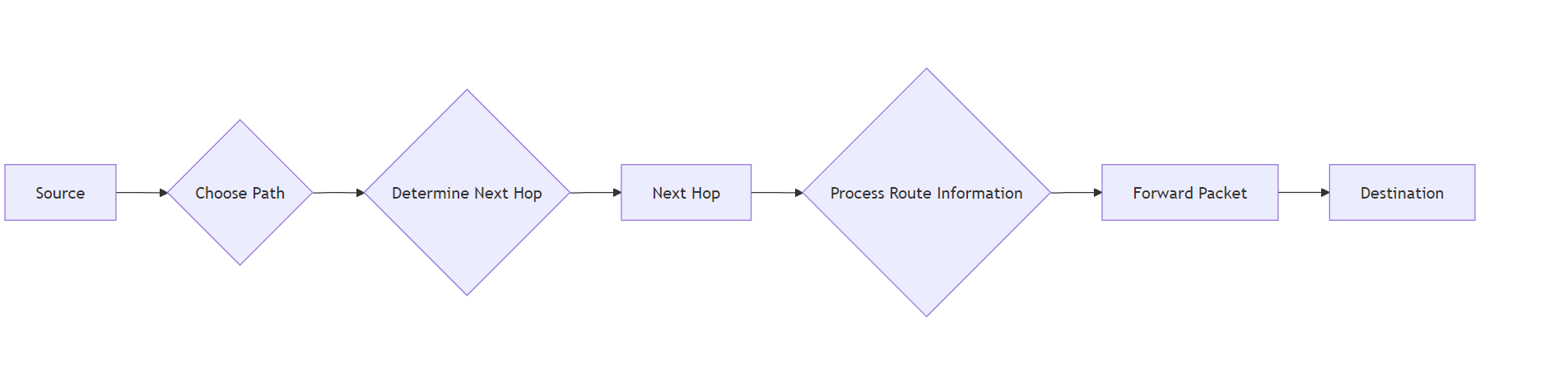
**Packet fragmentation:**

Packet fragmentation is the process of dividing large data packets into smaller fragments to fit network protocols' size limits, ensuring efficient transmission and reassembly at the destination.



**Source Routing:**

Source routing allows the sender to specify the entire route a packet takes through the network. This can improve routing efficiency but may complicate security and network management.



**Source Port Manipulation:**

Source port manipulation involves altering the source port number in network packets. This technique can enhance security, bypass firewalls, or establish multiple connections, but it may lead to potential vulnerabilities.

**IP Address Decoy:**

An IP address decoy is a technique used to mask the true source of internet traffic by routing it through various intermediary servers. This approach can enhance online privacy and anonymity, making it difficult for observers to trace activities back to the original user.

**IP Address Spoofing:**

IP address spoofing is a malicious practice where an attacker sends IP packets from a false source address to disguise their identity. This can be used for various cyberattacks, including Denial of Service (DoS) attacks, as it allows the attacker to bypass security measures and evade detection.

**Proxy Servers:**

A proxy server acts as an intermediary between a user and the internet. It forwards requests from clients to web servers and retrieves the requested data, providing anonymity and security. Proxy servers can filter content, improve load times, and bypass geographical restrictions, enhancing privacy and access to information online.

Attackers use proxy servers for several reasons:

* 1. Anonymity: Proxies mask the attacker's real IP address, making it difficult for security systems to trace the origin of malicious activities.
  2. Bypassing Restrictions: Proxies can help attackers circumvent firewalls, content filters, and geo-blocks, allowing access to restricted networks or systems.
  3. Traffic Redirection: Attackers can route traffic through multiple proxies to disguise their intent, making it harder to detect patterns of malicious behavior.
  4. Distributed Attacks: Using multiple proxy servers allows attackers to launch distributed attacks (like DDoS) more effectively, as the traffic appears to come from various sources.
  5. Access Control Evasion: Proxies can help bypass security measures and access restricted resources, enabling unauthorized data access or exploitation of vulnerabilities.

By leveraging these advantages, attackers can execute their strategies with greater stealth and effectiveness.

**Anonymizers:**

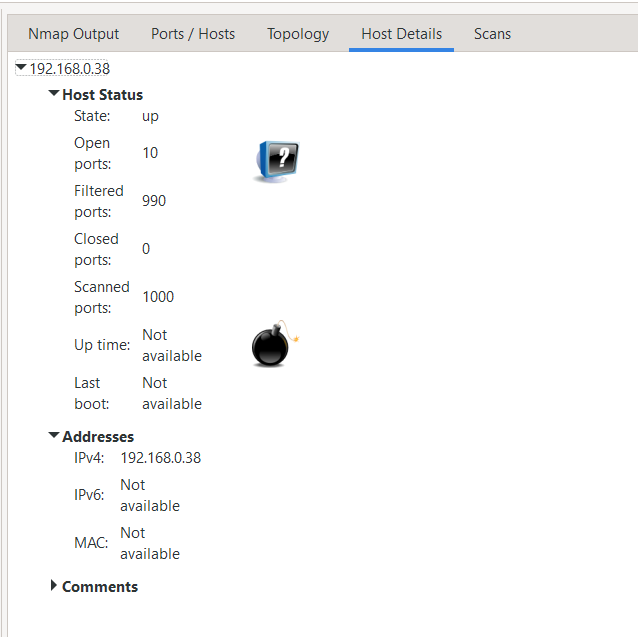
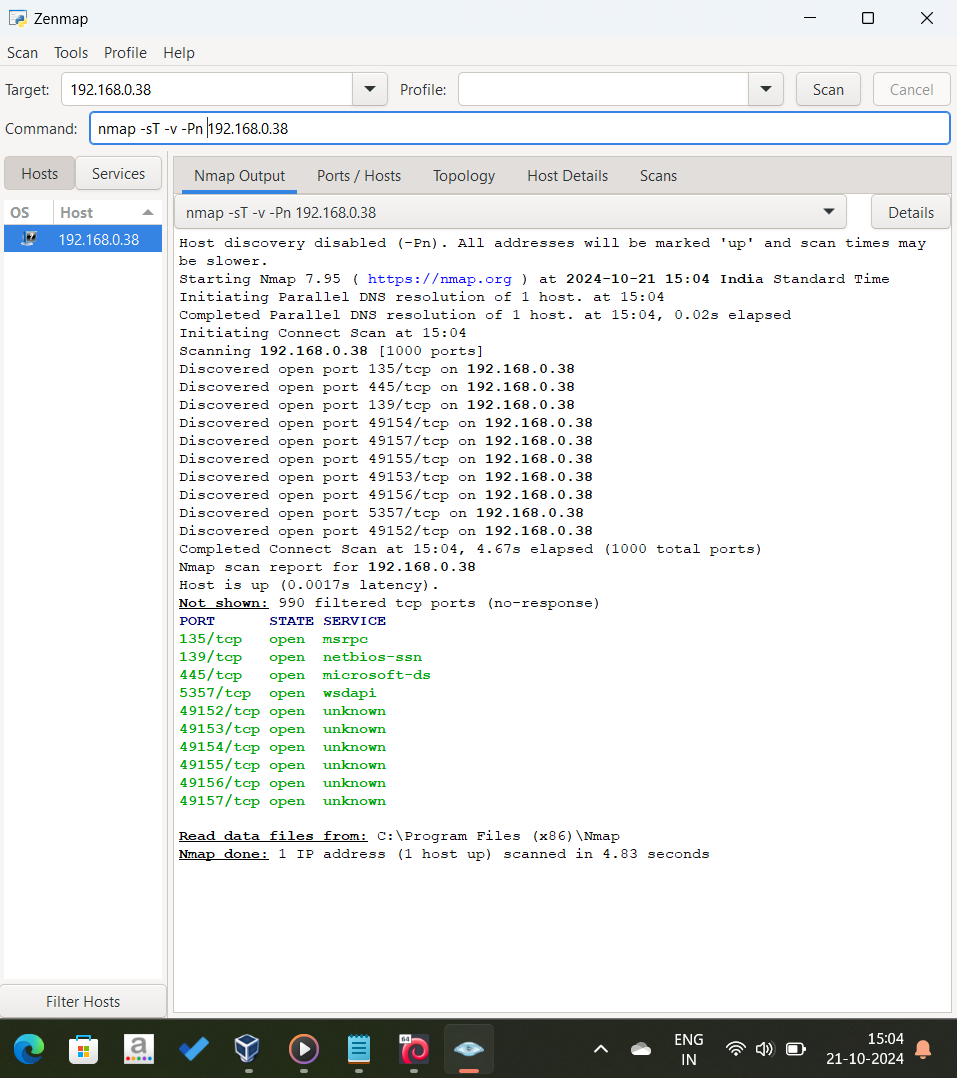
A proxy server acts as an intermediary between a user and the internet. It forwards requests from clients to web servers and retrieves the requested data, providing anonymity and security. Proxy servers can filter content, improve load times, and bypass geographical restrictions, enhancing privacy and access to information online.

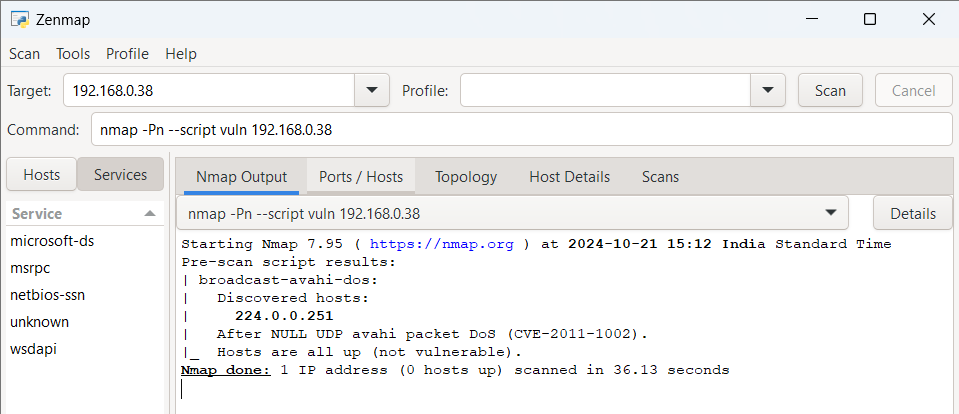
Here are some popular anonymizers:

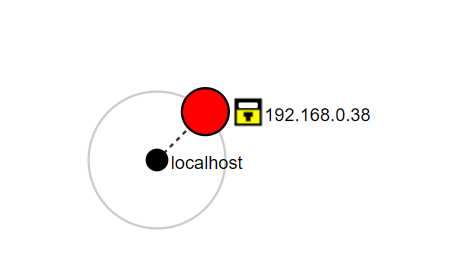
* 1. VPNs (Virtual Private Networks): Services like NordVPN, ExpressVPN, and CyberGhost encrypt internet traffic and hide IP addresses.
  2. Tor: A free, open-source software that routes traffic through a network of volunteer-operated servers for anonymity.
  3. Proxy Servers: Services like Smartproxy and Luminati that act as intermediaries, hiding the user's IP address.
  4. Anonymizing Browsers: Browsers like Brave and the Tor Browser prioritize user privacy and offer built-in anonymization features.
  5. Web-Based Anonymizers: Services like HideMyAss and Anonymouse.org that allow users to browse websites without revealing their identity.
  6. Onion Routing Services: These utilize the Tor network to provide additional layers of anonymity while browsing.

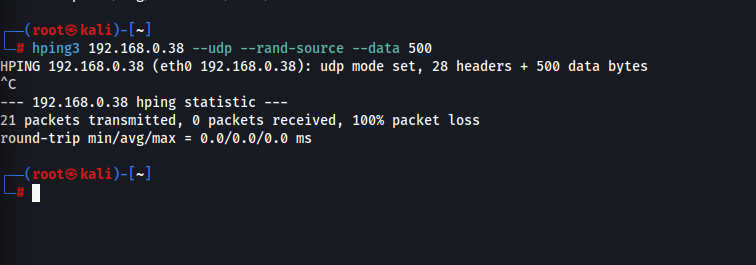
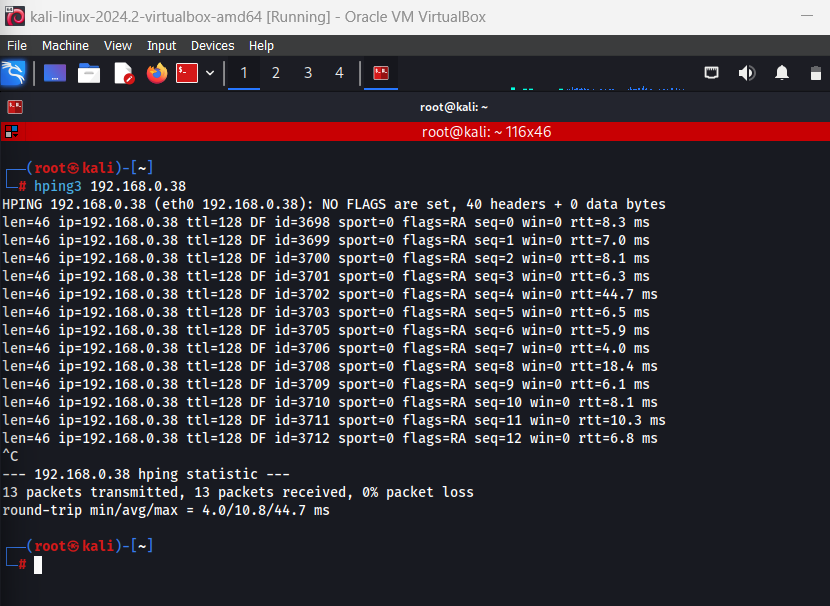
Using these tools helps protect user privacy and maintain anonymity online.

**Zenmap:**

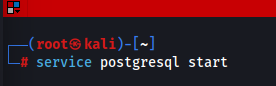


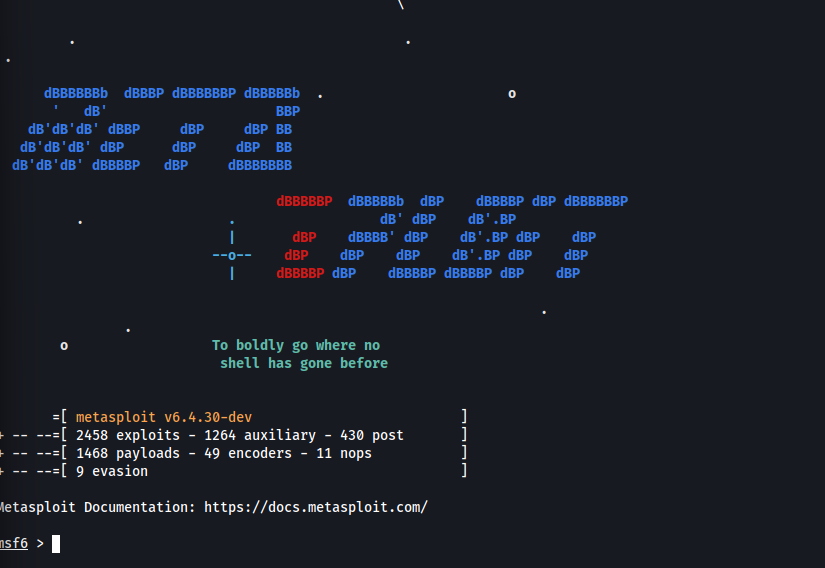


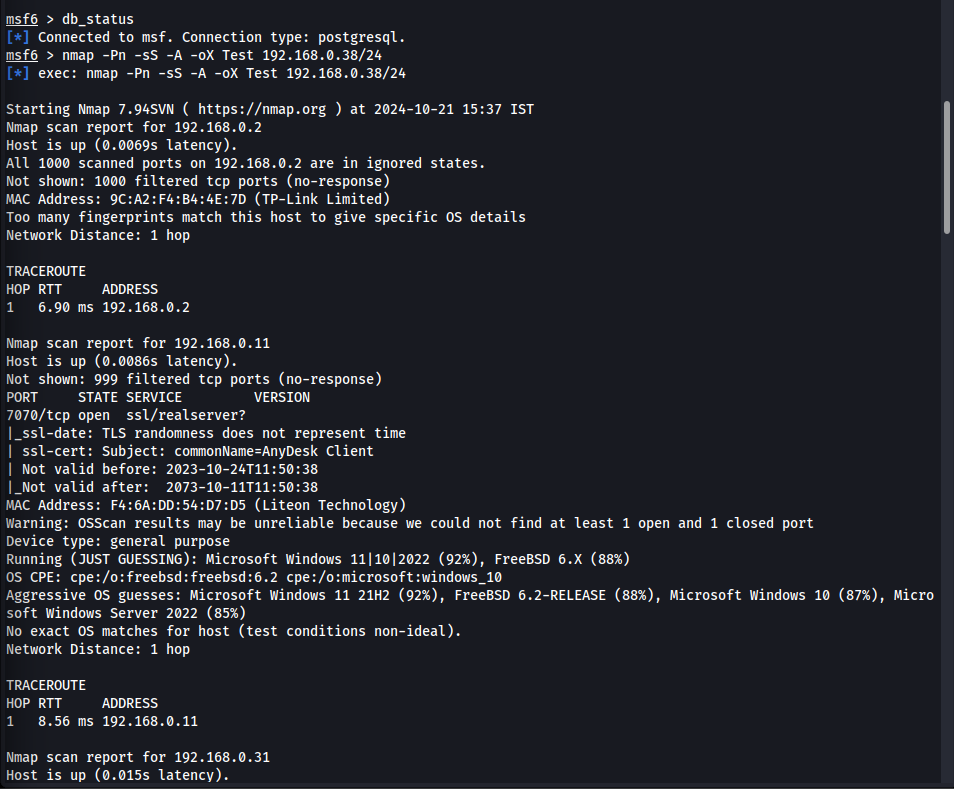


**Hping3:  
**

**Scanning a target network using Metasploit:**

****

****

**\**

