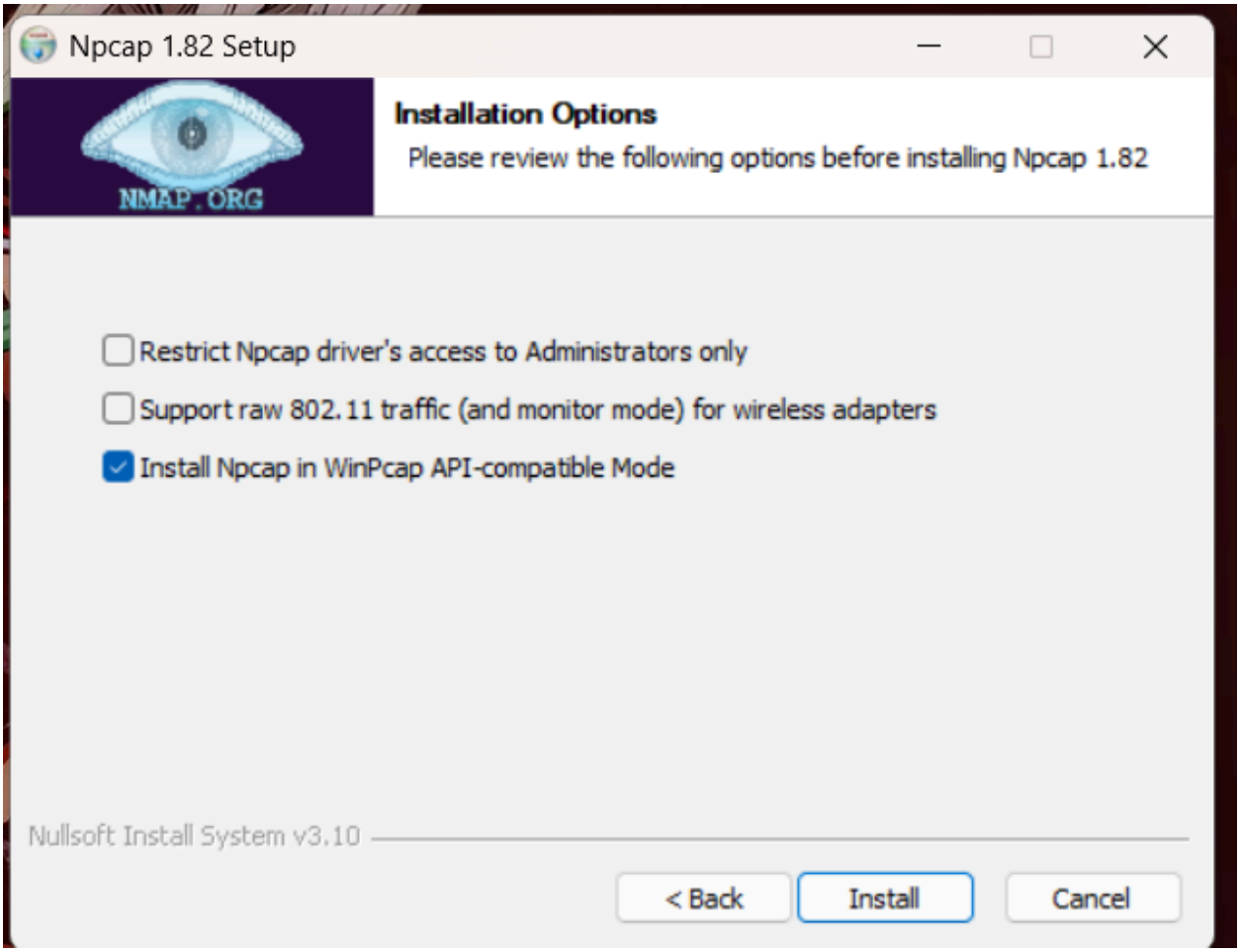
Task 1: Scan Your Local Network for Open Ports

Step 1: Install Nmap

Download and install Nmap from the official website: https://nmap.org/download.html



Nmap (Network Mapper) is a powerful open-source tool used to scan and discover devices on a network. It identifies open **ports**, which are communication endpoints used by services or applications (like HTTP on port 80 or SSH on port 22). By scanning these ports, Nmap helps users understand what services are running on a device and whether they are vulnerable. It's widely used by network administrators for security auditing, troubleshooting, and inventory management. Hackers may also use it for reconnaissance. Nmap supports advanced features like OS detection, version detection, and scriptable interactions.

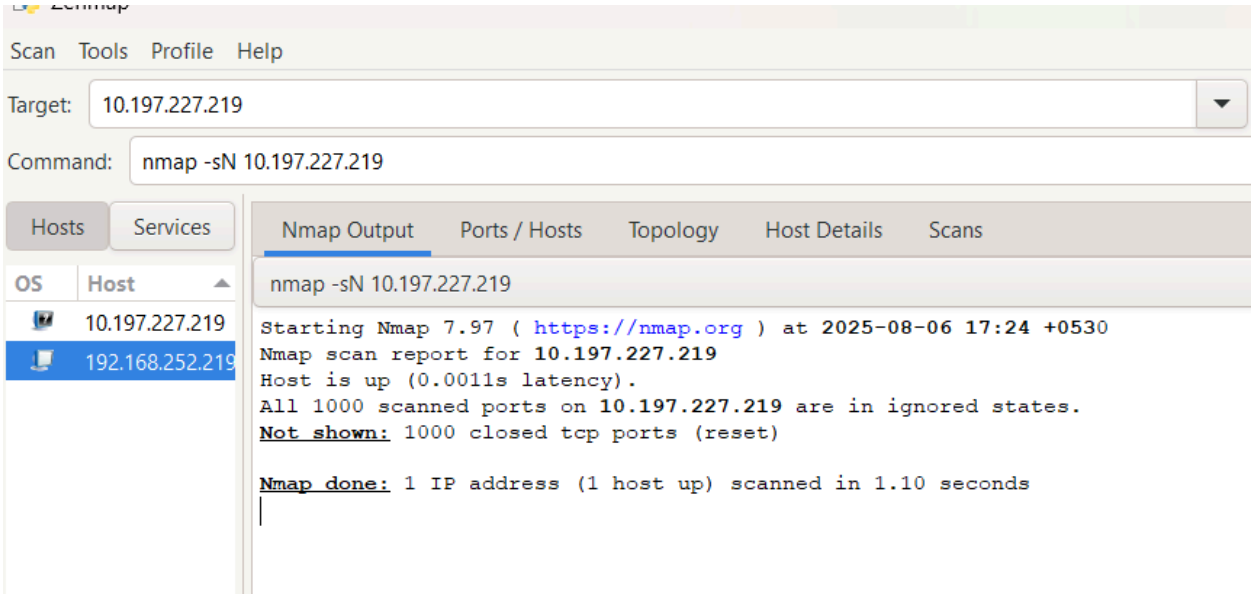
Step 2: Identify Your Local Network Range

Find your local network's IP address range. Typically, it's 192.168.0.x or 192.168.1.x. You can check your router's settings or use the command ipconfig (Windows) or ifconfig (macOS/Linux) to find this information.

```
Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2409:40e2:1007:ae39:a655:a9d7:5bb7:fd2c
   Temporary IPv6 Address. . . . . . : 2409:40e2:1007:ae39:90c9:11ce:8b74:d53c
   Link-local IPv6 Address . . . . . : fe80::3868:c23d:9770:7302%4
   IPv4 Address. . . . . . . . . . . : 10.197.227.219
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::3866:42ff:fec0:a375%4
                                       10.197.227.68
```

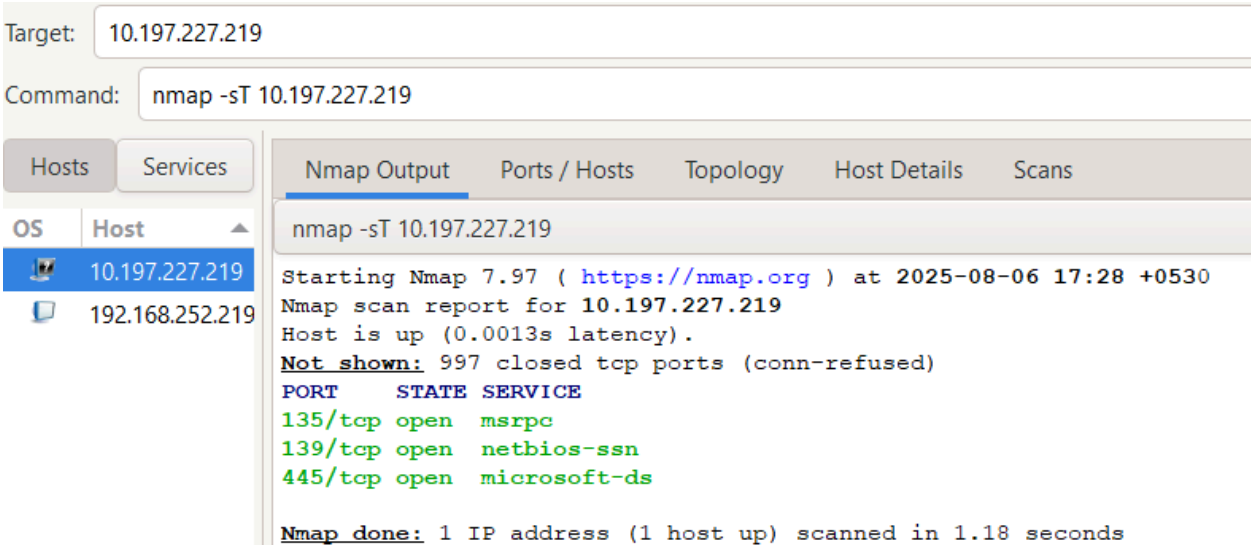
Step 3: Scan Your Network with Nmap

Open a terminal or command prompt and run the following command to scan your local network:nmap -sn 192.168.252.219



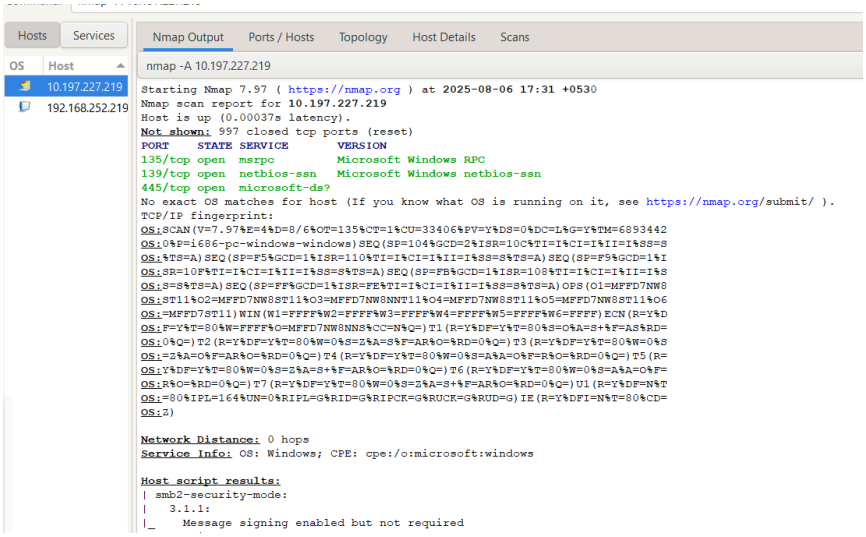
Step 4: Scan for Open Ports on a Specific Device

Choose a device from the previous scan and run the following command to scan for open ports:nmap -sT -p 1-65535 192.168.252.219



Aggressive Scan

The -A flag enables an aggressive scan, which performs the following additional tests:
OS Detection: Attempts to identify the operating system running on the target device.
Version Detection: Tries to determine the version of services running on open ports.
Script Scanning: Runs Nmap's built-in scripts to gather more information about the target device.
The nmap -A command is equivalent to combining the following flags:
-O (OS detection)
-sV (version detection)
--script=default (script scanning)



SYN Scan (Stealthy Scan)

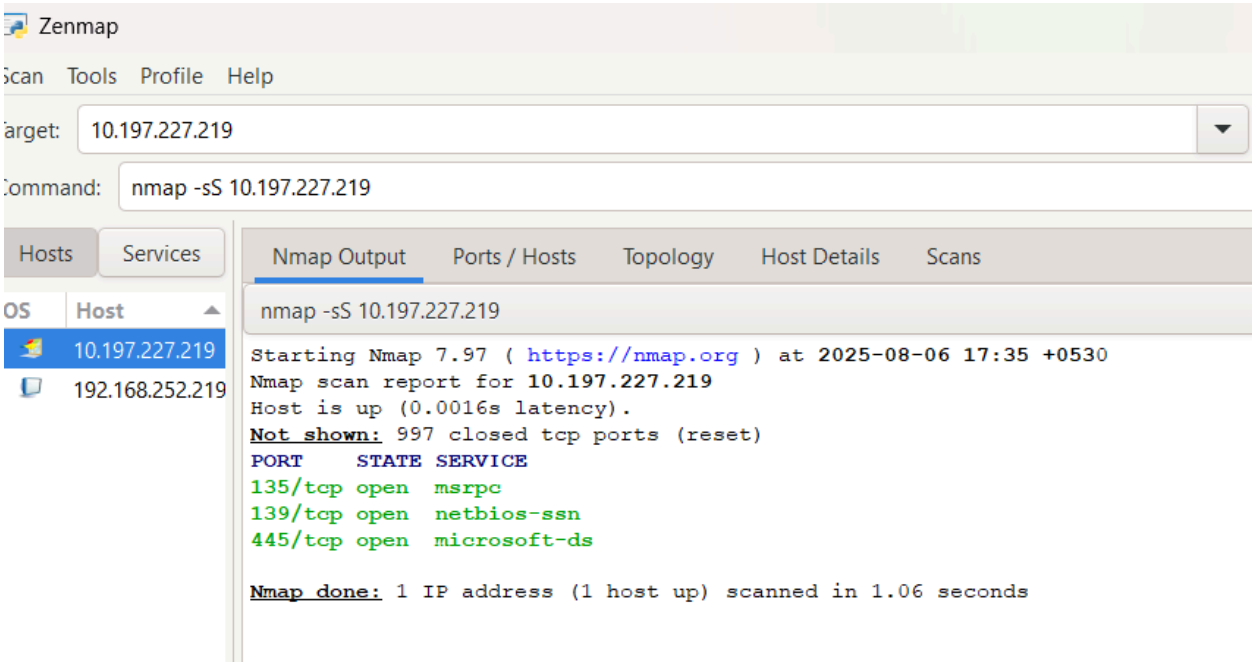
The -sS flag performs a SYN scan, also known as a "half-open" scan. This type of scan is considered stealthy because it doesn't complete the TCP handshake.

Here's how it works:

1. Nmap sends a SYN (synchronize) packet to the target device.
2. If the port is open, the target device responds with a SYN-ACK (synchronize-acknowledgment) packet.
3. Nmap sends a RST (reset) packet to terminate the connection, rather than completing the handshake with an ACK packet.

The -sS flag is useful for:

1. Evading firewalls and intrusion detection systems (IDS)
2. Reducing the likelihood of being detected
3. Scanning for open ports quickly and quietly



Open ports can pose significant security risks to your network and systems. Here are some potential risks to consider:

1. Unauthorized Access: Open ports can provide an entry point for hackers to access your systems and data, allowing them to launch attacks, steal sensitive information, or disrupt your services [1].
2. Malware and Ransomware: Open ports can be exploited by malware and ransomware attacks, which can compromise your systems, encrypt your data, and demand ransom payments.

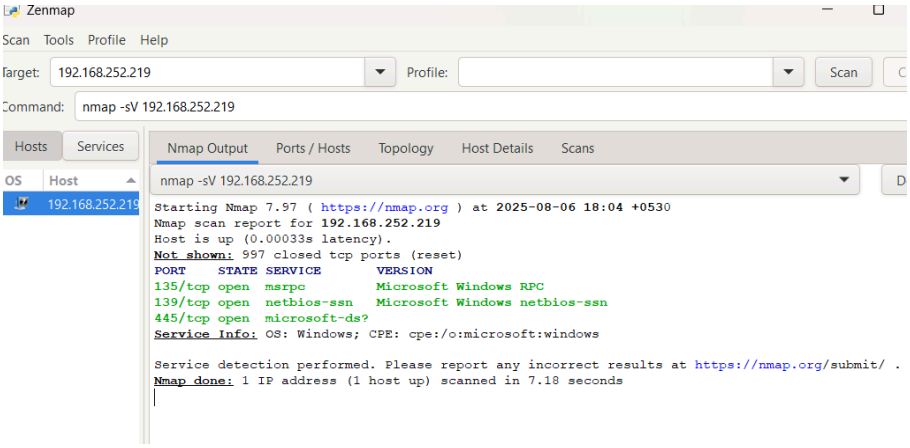
3. Denial of Service (DoS) Attacks: Open ports can be targeted by DoS attacks, which can overwhelm your systems with traffic, causing them to become unresponsive or even crash.
4. Man-in-the-Middle (MitM) Attacks: Open ports can be exploited by MitM attacks, which can intercept and manipulate sensitive data, such as login credentials or financial information.
5. SQL Injection and Cross-Site Scripting (XSS): Open ports can expose your web applications to SQL injection and XSS attacks, which can compromise your databases and steal sensitive data.

Some specific ports that are commonly targeted by attackers include:

1. Port 21 (FTP): Vulnerable to brute-force attacks, anonymous authentication, and cross-site scripting.
2. Port 22 (SSH): Vulnerable to brute-force attacks and leaked SSH keys.
3. Port 23 (Telnet): Vulnerable to credential brute-forcing and spoofing.
4. Port 25 (SMTP): Vulnerable to spamming, email spoofing, and man-in-the-middle attacks.
5. Port 445 (SMB): Vulnerable to EternalBlue exploits and ransomware attacks.

To identify potential security risks from open ports, follow these steps:

1. Scan the network using Nmap to list all open ports on each device (e.g., nmap -sV 192.168.1.0/24).
2. Check which services are running on the open ports (like FTP, SSH, HTTP) and their versions.
3. Look for unnecessary open ports that aren't required—these can be closed to reduce attack surface.
4. Identify outdated or vulnerable services using vulnerability databases (e.g., CVE, Exploit-DB).
5. Check for misconfigurations, such as services running without authentication (like open Telnet or SMB).
6. Use Nmap scripts (--script vuln) to detect known vulnerabilities automatically.



CONCLUSION:

By completing this task, you gain essential network reconnaissance skills using tools like Nmap, enabling you to scan and analyze devices on a local network. You learn how to identify open ports and recognize which services are running on them. This knowledge helps you assess how exposed your network is and what potential security risks exist. Understanding which services are needed and which are unnecessarily exposed helps improve security posture. These foundational skills are critical for network troubleshooting, penetration testing, and cybersecurity auditing.

INTERVIEW QUESTIONS

1. What is an open port?

   An open port is a network port that is actively listening for incoming connections and is accepting data from external sources. Open ports can provide services such as HTTP, FTP, SSH, or SMTP, but they can also pose security risks if not properly secured.

2. How does Nmap perform a TCP SYN scan?

   Nmap performs a TCP SYN scan by sending a SYN (synchronize) packet to a target port. If the port is open, the target responds with a SYN-ACK (synchronize-acknowledgment) packet. Nmap then sends a RST (reset) packet to terminate the connection, without completing the full TCP handshake. This scan is also known as a "half-open" scan.

3. What risks are associated with open ports?

   - Open ports can pose significant security risks, including:
   - Unauthorized access to sensitive data or systems
   - Malware and ransomware attacks
   - Denial of Service (DoS) attacks
   - Man-in-the-Middle (MitM) attacks
   - SQL injection and cross-site scripting (XSS) attacks

4. Explain the difference between TCP and UDP scanning.

   TCP (Transmission Control Protocol) scanning involves sending a SYN packet to a target port and waiting for a response. UDP (User Datagram Protocol) scanning, on the other hand, involves sending a UDP packet to a target port and waiting for an ICMP (Internet

Control Message Protocol) "port unreachable" error message. UDP scanning is often used to detect open UDP ports, as UDP does not establish a connection like TCP does.

5. How can open ports be secured?

Open ports can be secured by:

- Closing unnecessary ports
- Implementing firewalls to restrict incoming traffic
- Configuring access controls, such as authentication and authorization
- Regularly updating software and applying security patches
- Using encryption to protect data transmitted over open ports

6. What is a firewall's role regarding ports?

- A firewall's role is to control incoming and outgoing network traffic based on predetermined security rules. Firewalls can:
- Block traffic to specific ports
- Allow traffic to specific ports
- Hide internal IP addresses and network structures
- Provide Network Address Translation (NAT)

7. What is a port scan and why do attackers perform it?

- A port scan is a technique used to identify open ports on a target system. Attackers perform port scans to:
- Identify potential entry points for exploitation
- Gather information about the target system's services and vulnerabilities
- Plan and execute targeted attacks

8. How does Wireshark complement port scanning?

- Wireshark is a network protocol analyzer that can capture and analyze network traffic. Wireshark complements port scanning by:
- Providing detailed information about network traffic and protocols
- Helping to identify suspicious traffic patterns and potential security threats
- Allowing for the analysis of captured packets to understand communication flows and identify vulnerabilities.