Task-1-Scan-Your-Local-Network-for-Open-Ports

Network Port Scanning with Nmap

Objective

- The objective of this task is to discover open ports on devices within my local network using Nmap. This helps in understanding network exposure and learning how attackers might identify and exploit vulnerable services.

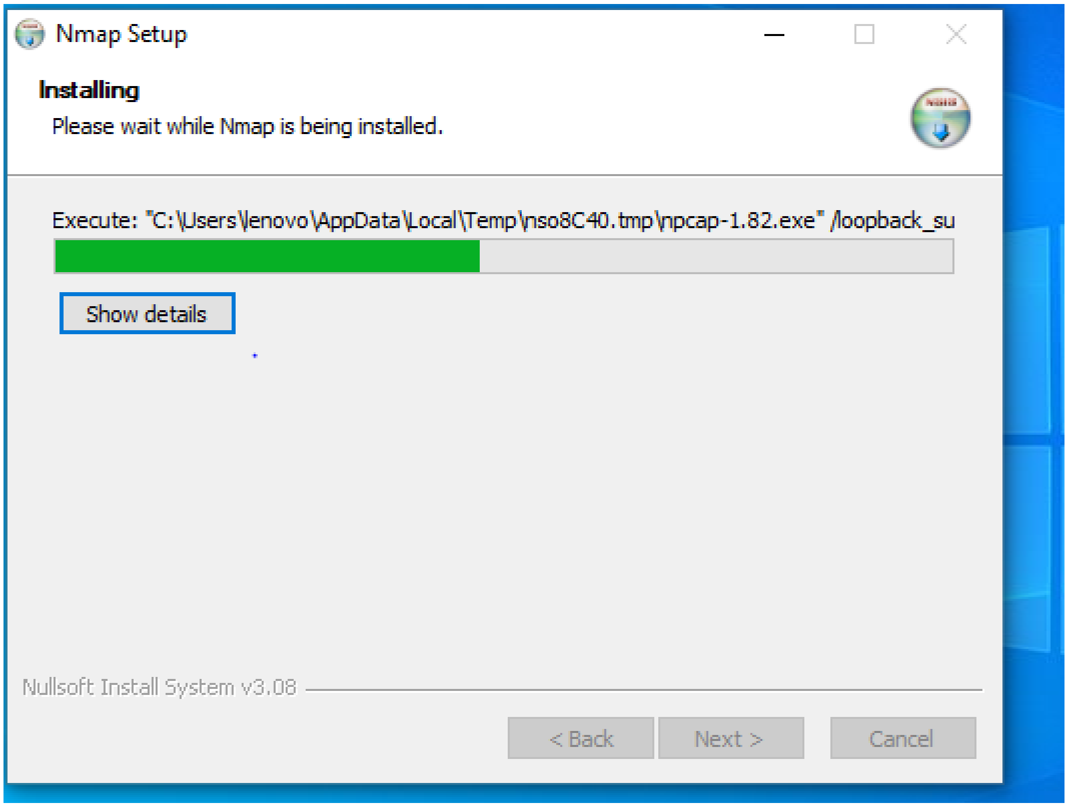
Tools Used

- Nmap - Free and open-source network scanner (for port scanning)
- Windows Command Prompt

Steps Performed

1. Installed Nmap

- Downloaded Nmap from the official site: https://nmap.org -> https://nmap.org/download.html
- Installed it for my operating system (Windows).

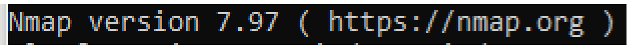


Installing

Please wait while Nmap is being installed.

```
Execute: "C:\Users\lenovo\AppData\Local\Temp\nso8C40.tmp\npcap-1.82.exe" /loopback_su
```

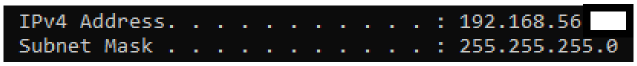
- Verified installation by running:
  - nmap -— version



```
Nmap version 7.97 ( https://nmap.org )
```

2. Identified Local IP Range

- Found My IP using the following command: Windows Command Prompt: ipconfig
- Result: 192.168.56.***/24 (IP is masked for privacy)
- Based on this, my local network range is: 192.168.56.***/24.

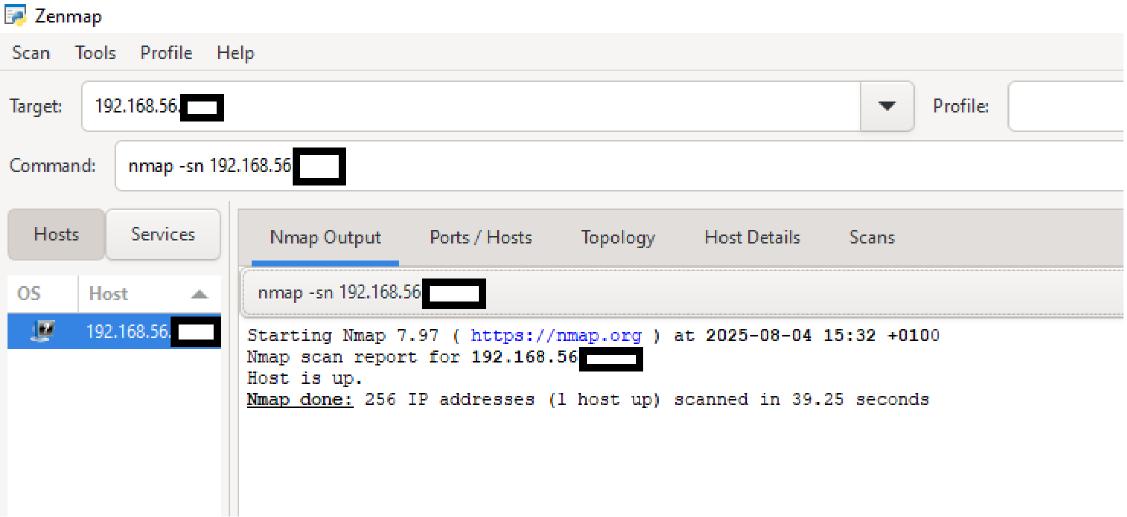


```
IPv4 Address. . . . . . . . . . . : 192.168.56 [redacted]
Subnet Mask . . . . . . . . . . . : 255.255.255.0
```

3. Performed Different Scans

Basic Ping Scan (Discover live hosts)

- Helps us to find hosts that are up without scanning ports.
- ***Command***: nmap -sn 192.168.56.***/24
- Output of this scan is saved in a text file using: Basic Ping Scan.txt



Target: 192.168.56.[redacted]

Command: nmap -sn 192.168.56[redacted]

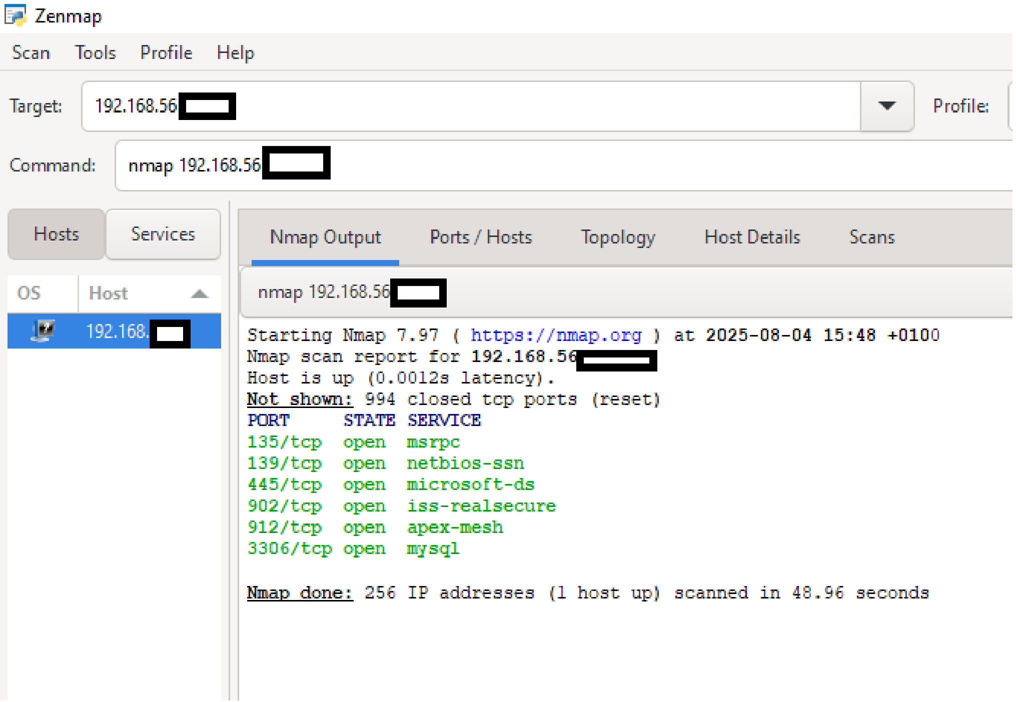
Host: 192.168.56.[redacted]

```
nmap -sn 192.168.56[redacted]
```

```
Starting Nmap 7.97 ( https://nmap.org ) at 2025-08-04 15:32 +0100
Nmap scan report for 192.168.56[redacted]
Host is up.
Nmap done: 256 IP addresses (1 host up) scanned in 39.25 seconds
```

Simple Port Scan (Check common ports)

- Checks the most common ports on live hosts.
- ***Command***: nmap 192.168.56.***/24
- Output of this scan is saved in a text file using: Simple Port Scan.txt



Target: 192.168.56[redacted]

Command: nmap 192.168.56[redacted]

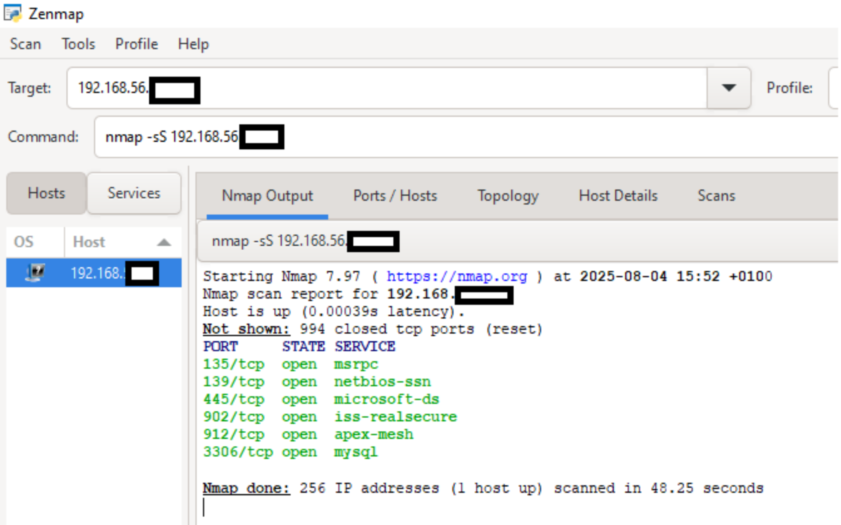
192.168.[redacted]

```
nmap 192.168.56[redacted]
Starting Nmap 7.97 ( https://nmap.org ) at 2025-08-04 15:48 +0100
Nmap scan report for 192.168.56[redacted]
Host is up (0.0012s latency).
Not shown: 994 closed tcp ports (reset)
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
3306/tcp open  mysql

Nmap done: 256 IP addresses (1 host up) scanned in 48.96 seconds
```

Stealth SYN Scan (More detailed)

- Stealthily discovers all open TCP ports. This performs a stealthy TCP SYN scan on all devices in the subnet.
- ***Command***: nmap -sS 192.168.56.***/24
- Output of this scan is saved in a text file using: Stealth Scan.txt



Target: 192.168.56.[redacted]

Command: nmap -sS 192.168.56[redacted]

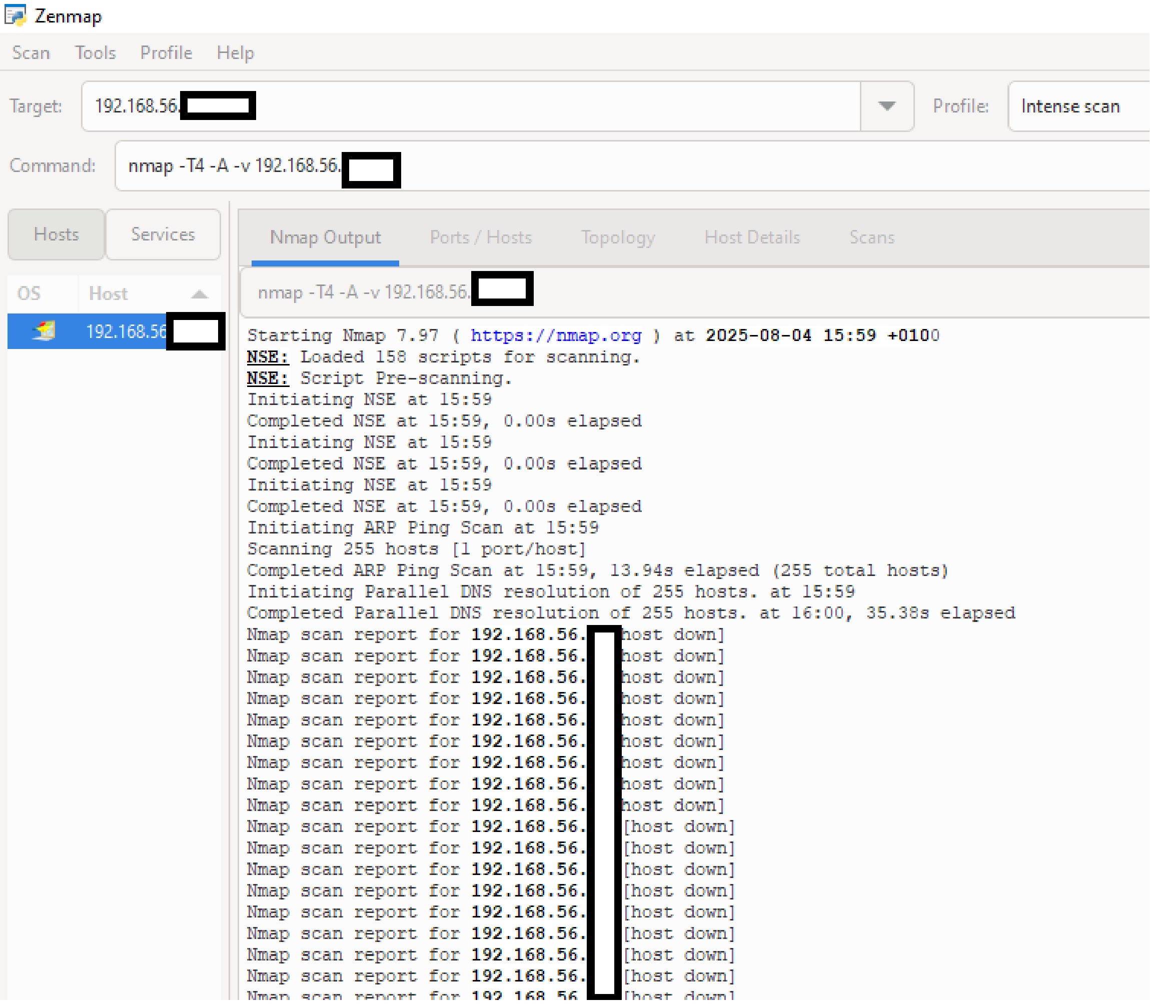
192.168.[redacted]

```
nmap -sS 192.168.56[redacted]
Starting Nmap 7.97 ( https://nmap.org ) at 2025-08-04 15:52 +0100
Nmap scan report for 192.168.[redacted]
Host is up (0.00039s latency).
Not shown: 994 closed tcp ports (reset)
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
3306/tcp open  mysql

Nmap done: 256 IP addresses (1 host up) scanned in 48.25 seconds
```

Intense Scan

- This scan combines several scanning techniques:
  - -sS: SYN scan as in Stealth Scan
  - -T4: Faster scan timing
  - -A: Enables OS detection, version detection, script scanning, and traceroute
  - -v: Verbose output for detailed progress feedback
- This scan delivers detailed information about the devices, open ports, services running, operating systems, and network topology.
- ***Command***: nmap -T4 -A -v 192.168.56.***/24
- Output of this scan is saved in a text file using: Intense Scan.txt



Target: 192.168.56.[redacted]

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.56.[redacted]

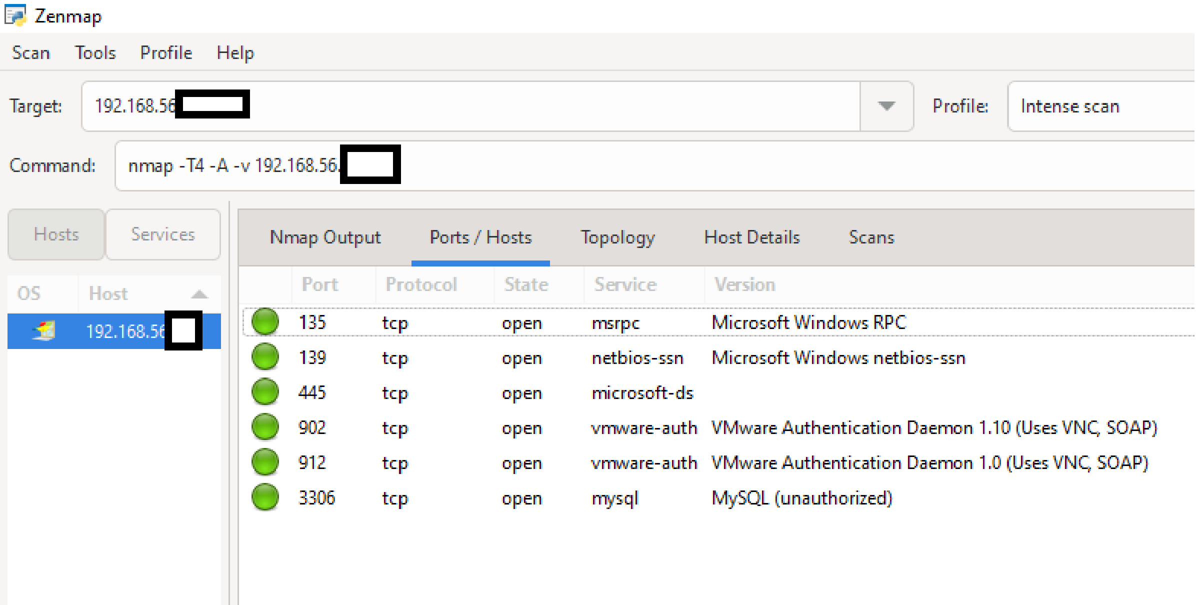
192.168.56[redacted]

nmap -T4 -A -v 192.168.56.[redacted]

```
Starting Nmap 7.97 ( https://nmap.org ) at 2025-08-04 15:59 +0100
NSE: Loaded 158 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:59
Completed NSE at 15:59, 0.00s elapsed
Initiating NSE at 15:59
Completed NSE at 15:59, 0.00s elapsed
Initiating NSE at 15:59
Completed NSE at 15:59, 0.00s elapsed
Initiating ARP Ping Scan at 15:59
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 15:59, 13.94s elapsed (255 total hosts)
Initiating Parallel DNS resolution of 255 hosts. at 15:59
Completed Parallel DNS resolution of 255 hosts. at 16:00, 35.38s elapsed
Nmap scan report for 192.168.56.[redacted]host down]
Nmap scan report for 192.168.56.host down]
Nmap scan report for 192.168.56.host down]
Nmap scan report for 192.168.56.host down]
Nmap scan report for 192.168.56.host down]
Nmap scan report for 192.168.56.host down]
Nmap scan report for 192.168.56.host down]
Nmap scan report for 192.168.56.host down]
Nmap scan report for 192.168.56.host down]
Nmap scan report for 192.168.56.[host down]
Nmap scan report for 192.168.56.[host down]
Nmap scan report for 192.168.56.[host down]
Nmap scan report for 192.168.56.[host down]
Nmap scan report for 192.168.56.[host down]
Nmap scan report for 192.168.56.[host down]
Nmap scan report for 192.168.56.[host down]
Nmap scan report for 192.168.56.[host down]
Nmap scan report for 192.168.56.[host down]
```

4. ***Potential Security Risks from Open Ports***

- The scan revealed the following open ports and associated services on the target device:



Target: 192.168.56[redacted]

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.56.[redacted]

192.168.5[redacted]

	Port	Protocol	State	Service	Version
●	135	tcp	open	msrpc	Microsoft Windows RPC
●	139	tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
●	445	tcp	open	microsoft-ds	
●	902	tcp	open	vmware-auth	VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
●	912	tcp	open	vmware-auth	VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
●	3306	tcp	open	mysql	MySQL (unauthorized)

  - Port: 135 | Protocol: TCP | Service: msrpc | Description: Microsoft Windows Remote Procedure Call
    - Potential Security Risks: This port can be exploited for remote code execution if vulnerable. It is a known target for malware and worms.
  - Port: 139 | Protocol: TCP | Service: netbios-ssn | Description: Microsoft Windows NetBIOS Session Service
    - Potential Security Risks: Exposes file sharing and may allow unauthorised access if not properly secured. Vulnerable to certain attacks like SMB relay.
  - Port: 445 | Protocol: TCP | Service: microsoft-ds | Description: Microsoft Directory Services (SMB)
    - Potential Security Risks: Frequently targeted by ransomware and exploits such as EternalBlue if unpatched. Critical to secure or restrict.
  - Port: 902 | Protocol: TCP | Service: vmware-auth | Description: VMware Authentication Daemon using VNC/ SOAP
    - Potential Security Risks: Open VMware ports may expose the host to unauthorised remote management if not properly secured.
  - Port: 912 | Protocol: TCP | Service: vmware-auth | Description: VMware Authentication Daemon (VNC/SOAP)

        - Potential Security Risks: Similar risks to port 902 could provide access to VM management interfaces.
    - Port: 3306 | Protocol: TCP | Service: mysql | Description: MySQL Database (unauthorised access possible)
        - Potential Security Risks: Unauthorised access risk if not properly secured with strong credentials. Can lead to data breaches.

Summary of Risks:

- Ports associated with Windows RPC and SMB (135, 139, 445) are common attack vectors for malware and ransomware. Ensuring these services are patched, firewalled, or disabled if unused is crucial.
- VMware-related ports (902, 912) could permit unauthorised remote control of virtual machines if exposed without proper authentication.
- The MySQL port (3306) being open and unauthenticated is risky, as attackers can access or manipulate databases, potentially leading to data theft or corruption.

Recommended Actions:

- Close or restrict access to unnecessary ports.
- Apply all security patches and updates.
- Use firewalls to control external access to these services.
- Enforce strong passwords and authentication on all exposed services.

Concepts Learned

- Port scanning
- TCP SYN scanning
- Local network reconnaissance
- Identifying IP ranges
- Basic risk analysis based on open ports

Final Outcome

- By completing this task, I developed basic network reconnaissance skills, gained familiarity with Nmap, and understood how open ports may expose services to attackers. This activity emphasised the importance of regular network audits and port management in cybersecurity.