Experiment No. 4

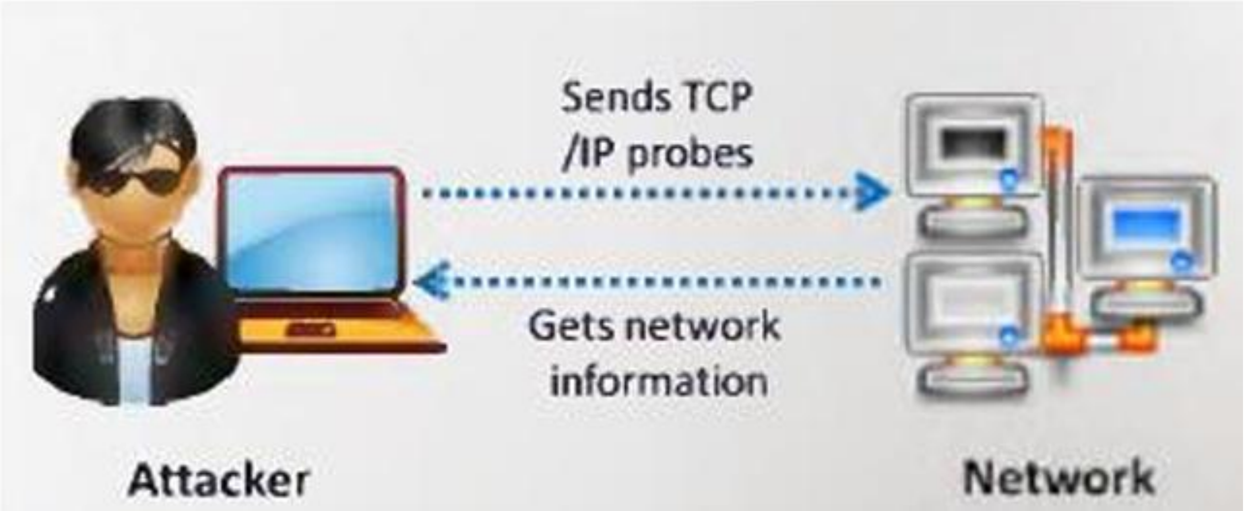
Aim: Perform network discovery using discovery tool (e.g Nmap, mrtg)

Resource required: Nmap, Zenmap, Command Prompt.

- Nmap ("Network Mapper") is an open source tool that is freely available for network discovery and vulnerability scanning.
- Nmap tool helps network administrators in identifying the devices running on the systems, discovering the accessible hosts and their services such as finding open ports and detecting security risks.

SCANNING

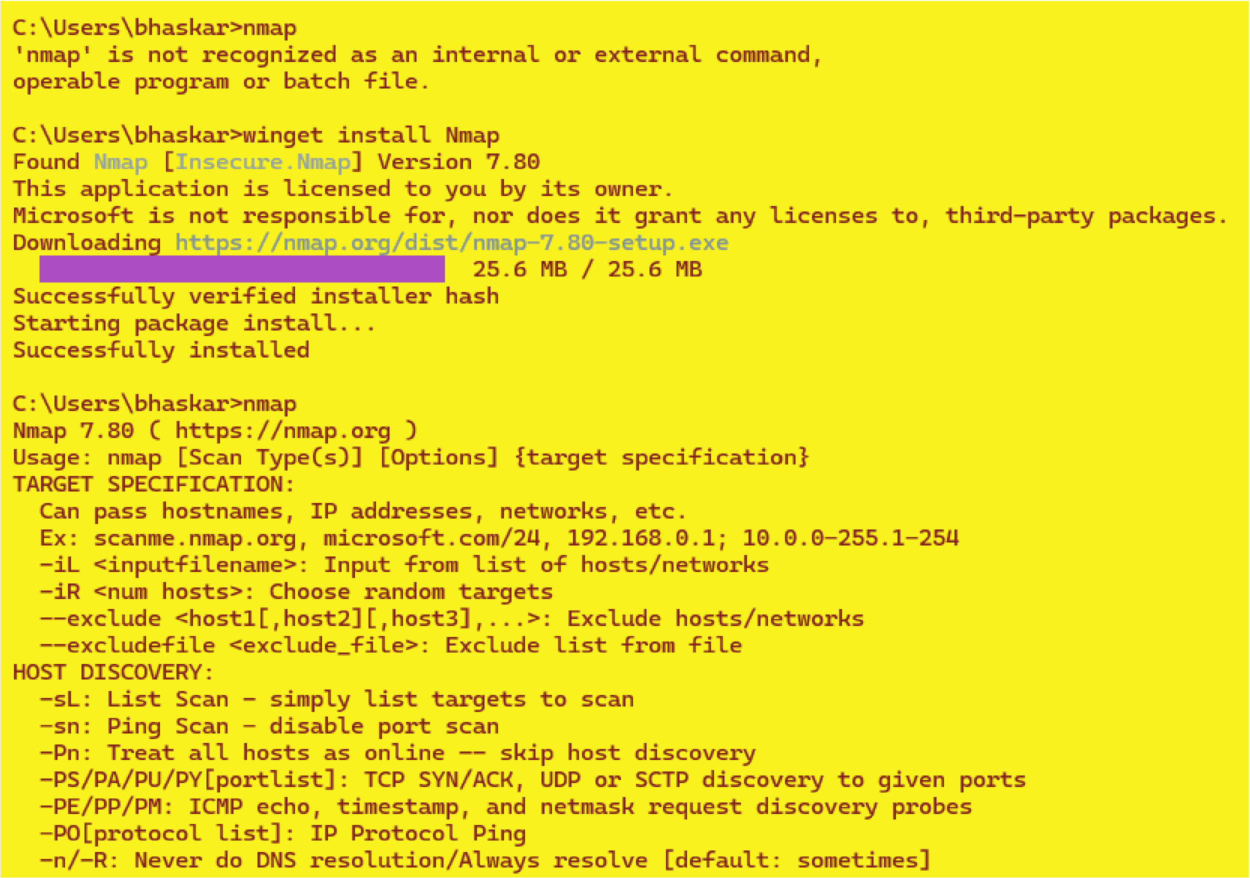
- Scanning is an active mode of information gathering.
- It refers to a set of procedures for identifying machines, open ports, and services running in network.
- The purpose is to find exploitable communication channels by discovering live machines, IP addresses, open ports, and services.
- It also identifies operating system, system architectures, and various vulnerabilities associated with it.



- The NMAP tool performs following steps of scanning:
  ¬ Step 1: Find live machines
  ¬ Step 2: Discover open ports
  ¬ Step 3: Scanning beyond IDS
  ¬ Step 4: Identify vulnerabilities

HOW TO OPEN NMAP

- Open the Terminal in windows i.e. cmd and type nmap.

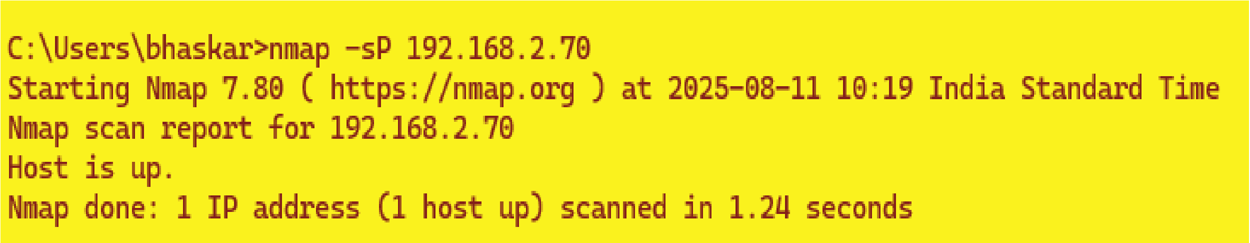


```
C:\Users\bhaskar>nmap
'nmap' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\bhaskar>winget install Nmap
Found Nmap [Insecure.Nmap] Version 7.80
This application is licensed to you by its owner.
Microsoft is not responsible for, nor does it grant any licenses to, third-party packages.
Downloading https://nmap.org/dist/nmap-7.80-setup.exe
  ██████████████████████████████  25.6 MB / 25.6 MB
Successfully verified installer hash
Starting package install...
Successfully installed

C:\Users\bhaskar>nmap
Nmap 7.80 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
```

STEP 1: FIND LIVE MACHINES

Introduction: Ping Sweep/Scan (-sP) is used to find live machines from a range of IP addresses. It sends ICMP echo request to multiple machines. In case of ping request, a single packet (56 bytes data + 08 byte header) is sent. It also determines round trip time.

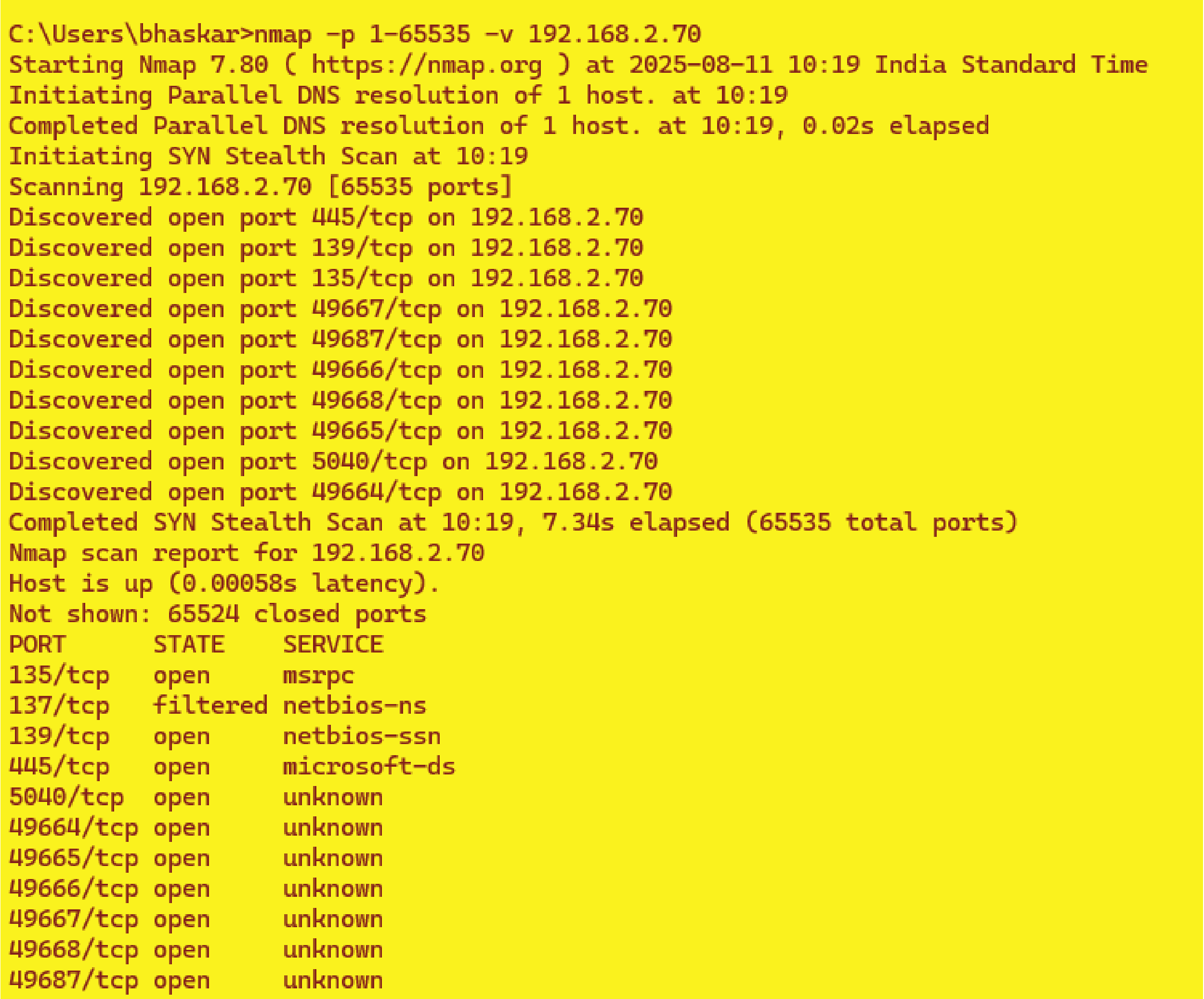
Command: nmap –sP <target>



```
C:\Users\bhaskar>nmap -sP 192.168.2.70
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-11 10:19 India Standard Time
Nmap scan report for 192.168.2.70
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 1.24 seconds
```

STEP 2: DISCOVER OPEN PORTS

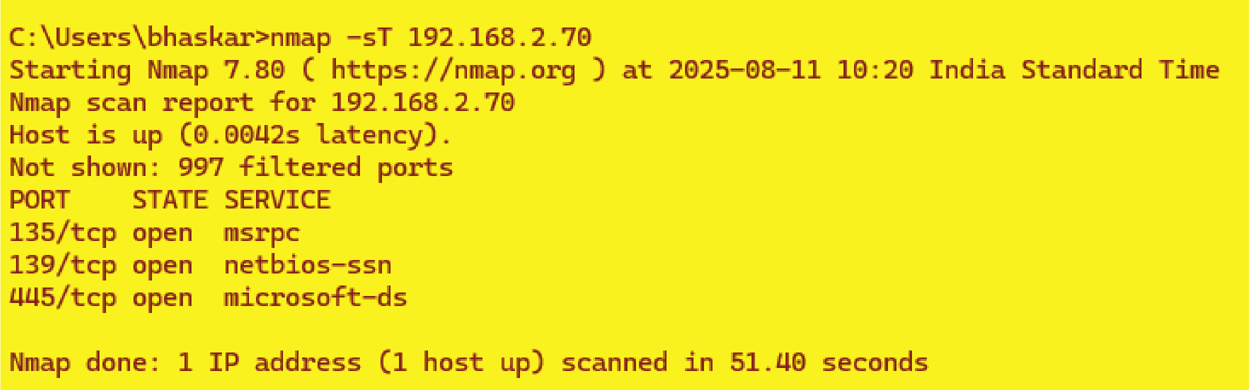
Introduction: In computer networking, a port is a communication endpoint. For example, Server Message Block (SMB) is a network file sharing protocol used by Windows machine for file and printer sharing. It operates on TCP port number 138 and 445. Attackers can exploit the vulnerabilities associated with SMB protocol if these ports are open. Microsoft released a patch for SMB v1 vulnerability but most of the users installed pirated version of operating system which will never be updated.
Command: nmap –p <port number> -v <target>



```
C:\Users\bhaskar>nmap -p 1-65535 -v 192.168.2.70
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-11 10:19 India Standard Time
Initiating Parallel DNS resolution of 1 host. at 10:19
Completed Parallel DNS resolution of 1 host. at 10:19, 0.02s elapsed
Initiating SYN Stealth Scan at 10:19
Scanning 192.168.2.70 [65535 ports]
Discovered open port 445/tcp on 192.168.2.70
Discovered open port 139/tcp on 192.168.2.70
Discovered open port 135/tcp on 192.168.2.70
Discovered open port 49667/tcp on 192.168.2.70
Discovered open port 49687/tcp on 192.168.2.70
Discovered open port 49666/tcp on 192.168.2.70
Discovered open port 49668/tcp on 192.168.2.70
Discovered open port 49665/tcp on 192.168.2.70
Discovered open port 5040/tcp on 192.168.2.70
Discovered open port 49664/tcp on 192.168.2.70
Completed SYN Stealth Scan at 10:19, 7.34s elapsed (65535 total ports)
Nmap scan report for 192.168.2.70
Host is up (0.00058s latency).
Not shown: 65524 closed ports
PORT      STATE    SERVICE
135/tcp   open     msrpc
137/tcp   filtered netbios-ns
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
5040/tcp  open     unknown
49664/tcp open     unknown
49665/tcp open     unknown
49666/tcp open     unknown
49667/tcp open     unknown
49668/tcp open     unknown
49687/tcp open     unknown
```

a) TCP Connect Scan [-sT]

Introduction: TCP Connect scan detects open ports by three way handshake. It is also referred as FULL OPEN Scan. Command: nmap –sT <target>

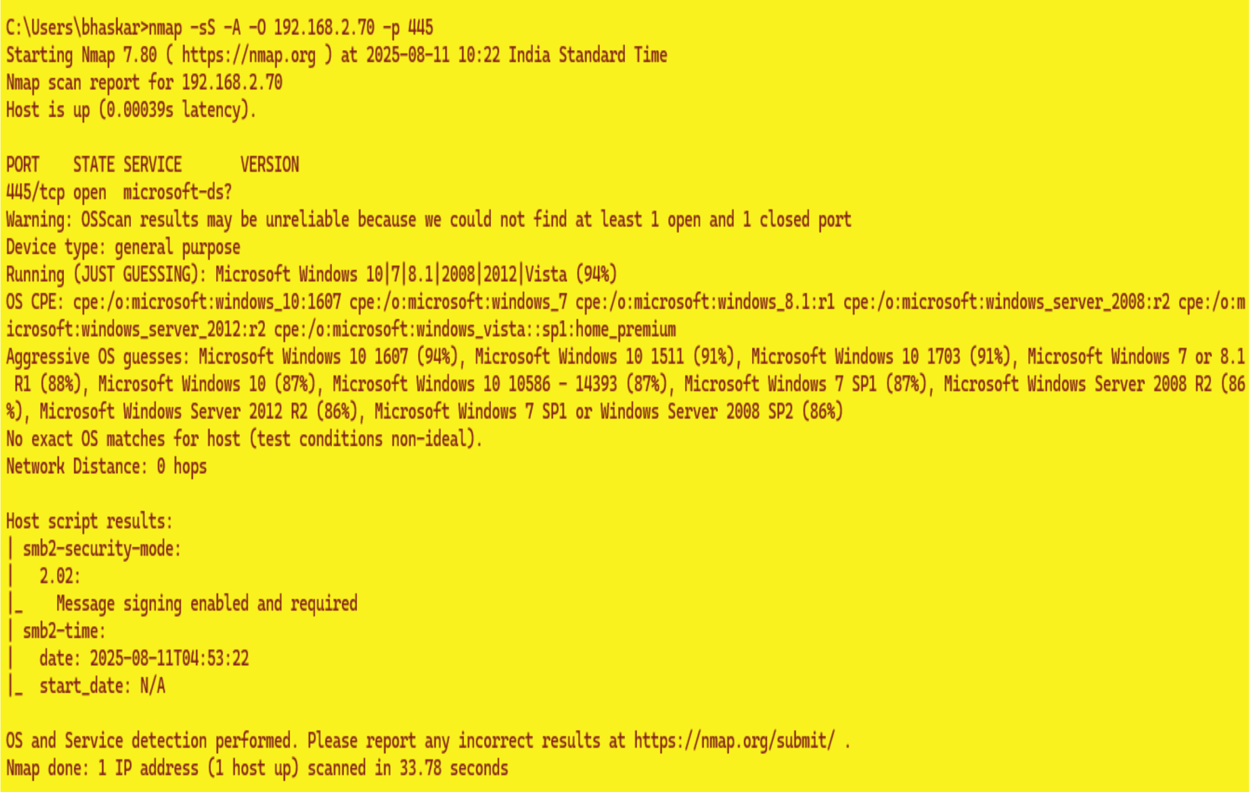


```
C:\Users\bhaskar>nmap -sT 192.168.2.70
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-11 10:20 India Standard Time
Nmap scan report for 192.168.2.70
Host is up (0.0042s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 51.40 seconds
```

b) SYN Stealth Scan [-sS]

Introduction: It is based upon TCP handshake. It is also referred as HALF OPEN Scan. In this type of scan, Nmap sends SYN packet: ¬ If port is open - it responds with ACK. ¬ If port is closed - it responds with RST. ¬ If port is filtered - it simply drops SYN packet.

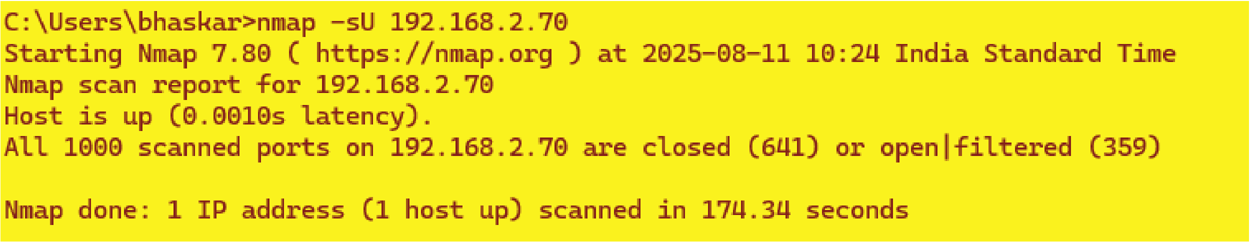
Command: nmap –sS –A –O <target> –p <port> (where –A is Aggressive scan, -O is operating system)



```
C:\Users\bhaskar>nmap -sS -A -O 192.168.2.70 -p 445
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-11 10:22 India Standard Time
Nmap scan report for 192.168.2.70
Host is up (0.00039s latency).

PORT    STATE SERVICE      VERSION
445/tcp open  microsoft-ds?
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 10|7|8.1|2008|2012|Vista (94%)
OS CPE: cpe:/o:microsoft:windows_10:1607 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_8.1:r1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:m
icrosoft:windows_server_2012:r2 cpe:/o:microsoft:windows_vista::sp1:home_premium
Aggressive OS guesses: Microsoft Windows 10 1607 (94%), Microsoft Windows 10 1511 (91%), Microsoft Windows 10 1703 (91%), Microsoft Windows 7 or 8.1
 R1 (88%), Microsoft Windows 10 (87%), Microsoft Windows 10 10586 - 14393 (87%), Microsoft Windows 7 SP1 (87%), Microsoft Windows Server 2008 R2 (86
%), Microsoft Windows Server 2012 R2 (86%), Microsoft Windows 7 SP1 or Windows Server 2008 SP2 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 0 hops

Host script results:
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2025-08-11T04:53:22
|_  start_date: N/A

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.78 seconds
```

c) UDP Scan [-sU]

Introduction: This type of scan is used to scan UDP ports. Nmap sends the 0 byte UDP packets. If source receives an ICMP Port Unreachable message, then the Port is closed. Command: nmap –sU <target>

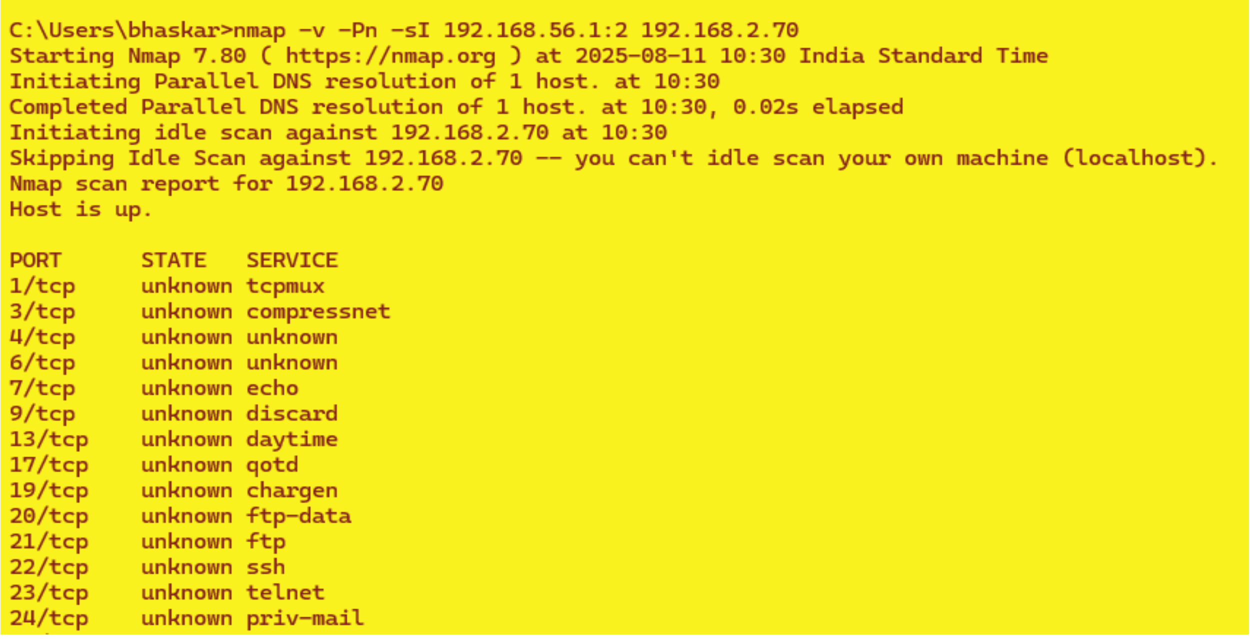


```
C:\Users\bhaskar>nmap -sU 192.168.2.70
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-11 10:24 India Standard Time
Nmap scan report for 192.168.2.70
Host is up (0.0010s latency).
All 1000 scanned ports on 192.168.2.70 are closed (641) or open|filtered (359)

Nmap done: 1 IP address (1 host up) scanned in 174.34 seconds
```

d) Idle Scan [-sI]

Introduction: An idle scan contains three steps that are repeatedly followed for each of the port: ¬ Step 1: Probe the zombie's IP ID and record it. ¬ Step 2: Forge a SYN packet from the zombie and send it to the desired port on the target. Depending on the port state, the target's reaction may or may not cause the zombie's IP ID to be incremented. ¬ Step 3: Probe the zombie's IP ID again. The target port state is then determined by comparing this new IP ID with the previous recorded step.

Command: nmap -V -Pn –sI : (By default port no. is 80)



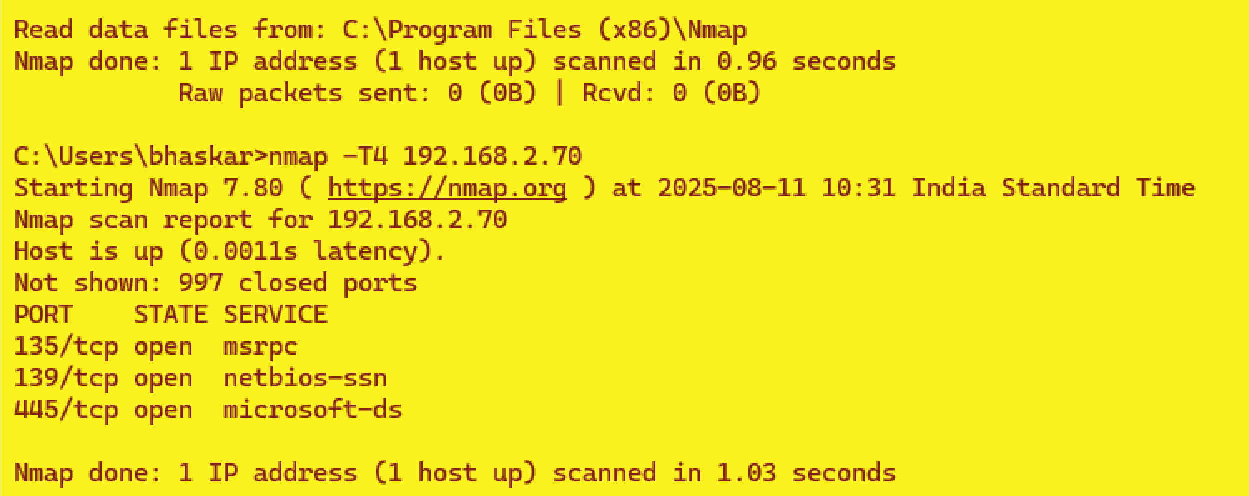
```
C:\Users\bhaskar>nmap -v -Pn -sI 192.168.56.1:2 192.168.2.70
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-11 10:30 India Standard Time
Initiating Parallel DNS resolution of 1 host. at 10:30
Completed Parallel DNS resolution of 1 host. at 10:30, 0.02s elapsed
Initiating idle scan against 192.168.2.70 at 10:30
Skipping Idle Scan against 192.168.2.70 -- you can't idle scan your own machine (localhost).
Nmap scan report for 192.168.2.70
Host is up.

PORT     STATE   SERVICE
1/tcp    unknown tcpmux
3/tcp    unknown compressnet
4/tcp    unknown unknown
6/tcp    unknown unknown
7/tcp    unknown echo
9/tcp    unknown discard
13/tcp   unknown daytime
17/tcp   unknown qotd
19/tcp   unknown chargen
20/tcp   unknown ftp-data
21/tcp   unknown ftp
22/tcp   unknown ssh
23/tcp   unknown telnet
24/tcp   unknown priv-mail
```

STEP 3: SCANNING BEYOND FIREWALL

Introduction: Nmap provides feature to control time options– [-T].

The timings are: Paranoid [-T0], Sneaky [-T1], Polite [-T2], Normal [-T3], Aggressive [-T4], and Insane [-T5]. Where –T0 implies 5 minutes wait between each packet to send that make it almost impossible for firewall to detect. Similarly, –T1 implies 4 minutes wait between each packet to send. –T2 implies 3 minutes wait between each packet to send. –T3 implies 2 minutes wait between each packet to send. –T4 implies 1 minutes wait between each packet to send. –T5 implies no wait between each packet to send.

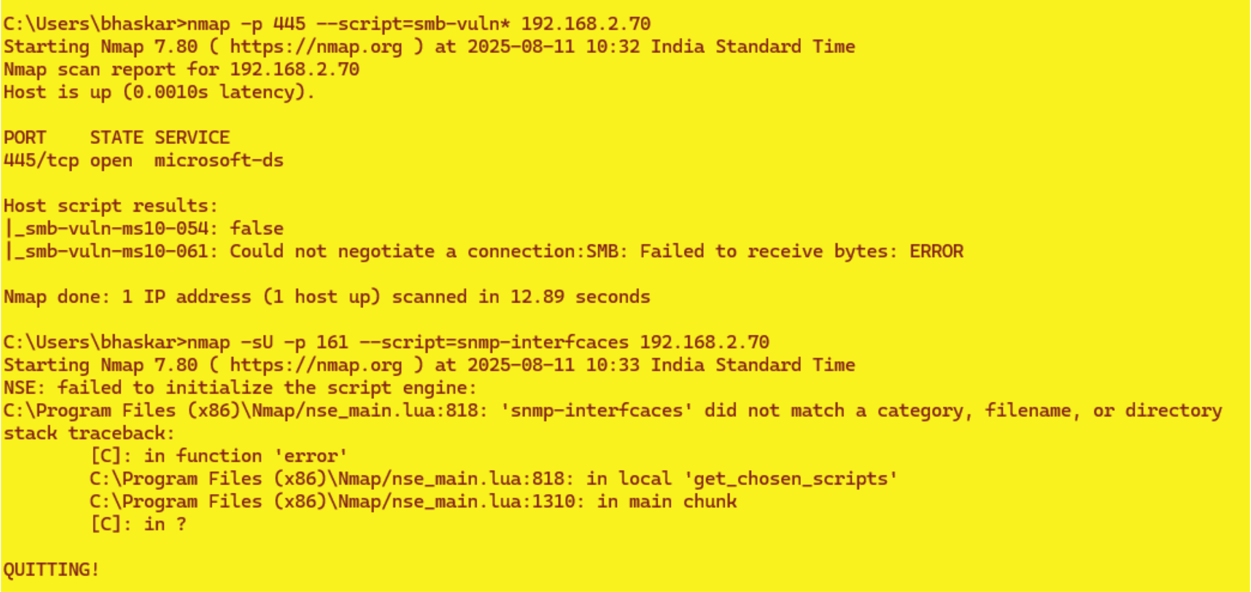
Command: nmap -T[0-5] [target]



```
Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 0.96 seconds
           Raw packets sent: 0 (0B) | Rcvd: 0 (0B)

C:\Users\bhaskar>nmap -T4 192.168.2.70
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-11 10:31 India Standard Time
Nmap scan report for 192.168.2.70
Host is up (0.0011s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 1.03 seconds
```

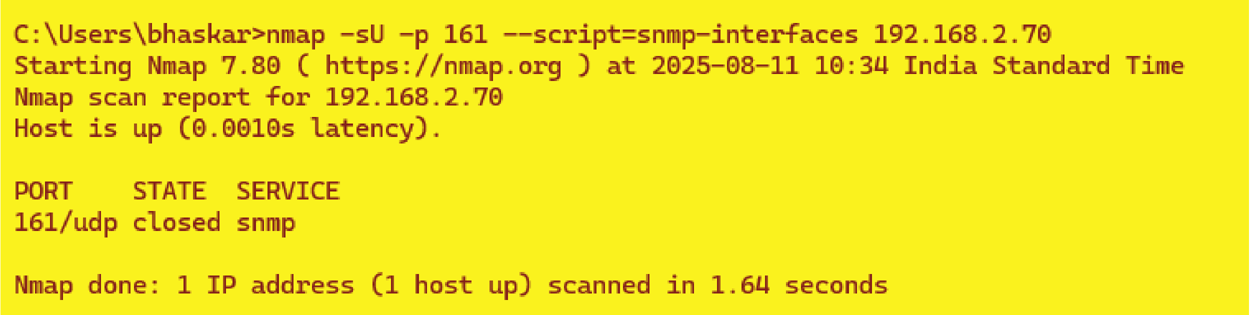
STEP 4: IDENTIFY VULNERABILITIES

Introduction: After finding the open ports and services running on it, this step identifies the vulnerabilities associated with the open ports. For example, vulnerabilities associated with the open ports of Simple Network Management Protocol (SNMP) and Server Message Block (SMB) protocols. Simple Network Management Protocol (SNMP) is built in to virtually every network device. Network management programs (such as HP OpenView and LANDesk) use SNMP for remote network host management. Unfortunately, SNMP also presents security vulnerabilities. If SNMP is compromised, an attacker can collect information of network such as ARP tables, usernames, and TCP connections to perform various attacks. If SNMP shows up in port scans, then a hacker will try to hack the system.
Command: nmap -p 445 --script=smb-vuln* 21



```
C:\Users\bhaskar>nmap -p 445 --script=smb-vuln* 192.168.2.70
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-11 10:32 India Standard Time
Nmap scan report for 192.168.2.70
Host is up (0.0010s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR

Nmap done: 1 IP address (1 host up) scanned in 12.89 seconds

C:\Users\bhaskar>nmap -sU -p 161 --script=snmp-interfcaces 192.168.2.70
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-11 10:33 India Standard Time
NSE: failed to initialize the script engine:
C:\Program Files (x86)\Nmap/nse_main.lua:818: 'snmp-interfcaces' did not match a category, filename, or directory
stack traceback:
        [C]: in function 'error'
        C:\Program Files (x86)\Nmap/nse_main.lua:818: in local 'get_chosen_scripts'
        C:\Program Files (x86)\Nmap/nse_main.lua:1310: in main chunk
        [C]: in ?

QUITTING!
```

Command: nmap -sU -p 161 --script=snmp-interfaces



```
C:\Users\bhaskar>nmap -sU -p 161 --script=snmp-interfaces 192.168.2.70
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-11 10:34 India Standard Time
Nmap scan report for 192.168.2.70
Host is up (0.0010s latency).

PORT    STATE  SERVICE
161/udp closed snmp

Nmap done: 1 IP address (1 host up) scanned in 1.64 seconds
```

Conclusion: In this practical, network discovery was performed using tools such as Nmap. The main goal was to identify active hosts, open ports, services, and traffic statistics within the network.

Using Nmap, we successfully scanned the network and discovered:

- Live hosts (IP addresses of active devices)
- Open ports and the services running on them (e.g., SSH, HTTP, FTP)
- Operating system information and device types (when possible)