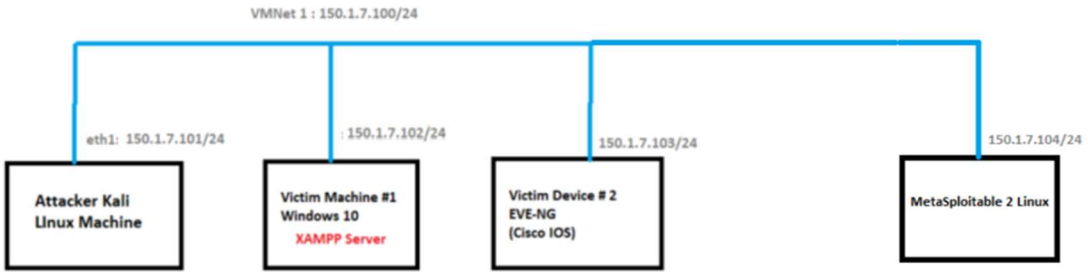
# Cyber Security – Assessment # 3

**Q1.** Network scanning is systematic probing of IP addresses and ports to discover live hosts and exposed services. It includes host discovery, port scanning, service/version fingerprinting, and vulnerability scanning.

- Perform port scanning to determine open ports using Nmap on all live hosts in 150.1.7.0/24 network. Ensure that host discovery is disabled and output should be detailed one
    - TCP Full-Open Scan
    - TCP Half-Open (SYN) Scan - Also known as “Stealth Scan”
    - XMAS Tree Scan
- Perform scan of host 150.1.7.102. Ensure that your scan is not detected by IPS/IDS or by firewall: -
    - Use packet fragmentation (with default MTU of 8 bytes)
    - Specify MTU to 16 bytes
- Carry out decoy scan of host 150.1.7.102 so as to:-
    - Send scan from 10 x Spoofed IPs
    - Specify single IP (171.124.180.173) as decoy address
- Perform idle zombie scan on host 150.1.7.102
- To avoid IDS/IPS or firewall detection, perform source port manipulation
- Use AI and launch IP address decoy technique with following prompt:
    - “To evade an IDS/Firewall, use IP address decoy technique to scan the target IP address 150.1.7.102”




- **Scanning the entire subnet `150.1.7.0/24` with host discovery disabled:**

**1. TCP Full-Open Scan (connect scan)**

nmap -Pn -sT -F -T4 150.1.7.0/24

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -Pn -sT -F -T4 150.1.7.0/24 > nmap_full.txt
```

-F for fast scan, -T4 for fast result, since we are scanning entire network so we are scanning specific ports only, Saved in file because the verbose would go on and on, so for later analysis the file is stored.

```
┌──(root㉿kali)-[/home/kali]
└─# cat nmap_full.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-19 03:01 EDT
Nmap scan report for 150.1.7.0
Host is up (0.42s latency).
All 100 scanned ports on 150.1.7.0 are in ignored states.
Not shown: 64 filtered tcp ports (host-unreach), 36 filtered tcp ports (no-re
sponse)
```

Only the live hosts are captured **104(Metasploit Machine)**

```
Nmap scan report for 150.1.7.104
Host is up (0.0012s latency).
Not shown: 82 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
513/tcp  open  login
514/tcp  open  shell
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
8009/tcp open  ajp13
```

**100(Base/Host Machine)**

```
Nmap scan report for 150.1.7.100
Host is up (0.00049s latency).
Not shown: 95 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5800/tcp open  vnc-http
5900/tcp open  vnc

Nmap scan report for 150.1.7.101
```

**2. TCP Half-Open SYN Scan ("Stealth Scan")**

nmap -Pn -sS -v 150.1.7.0/24

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -Pn -sS -F -T4 150.1.7.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-19 03:13 EDT
Nmap scan report for 150.1.7.100
Host is up (0.00022s latency).
Not shown: 95 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5800/tcp open  vnc-http
5900/tcp open  vnc
MAC Address: 00:50:56:C0:00:01 (VMware)

Nmap scan report for 150.1.7.102
Host is up (0.00018s latency).
Not shown: 96 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
MAC Address: 00:0C:29:9E:3E:35 (VMware)
```

-F for fast scan, -T4 for fast result, since we are scanning entire network so we are scanning specific ports only.

```
Nmap scan report for 150.1.7.104
Host is up (0.00020s latency).
Not shown: 82 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
513/tcp  open  login
514/tcp  open  shell
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
8009/tcp open  ajp13
MAC Address: 00:0C:29:A5:C3:BD (VMware)

Nmap scan report for 150.1.7.101
Host is up (0.0000050s latency).
All 100 scanned ports on 150.1.7.101 are in ignored states.
Not shown: 100 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 34.07 seconds
```

**3. XMAS Tree Scan**

nmap -Pn -sX -F -T4 150.1.7.0/24

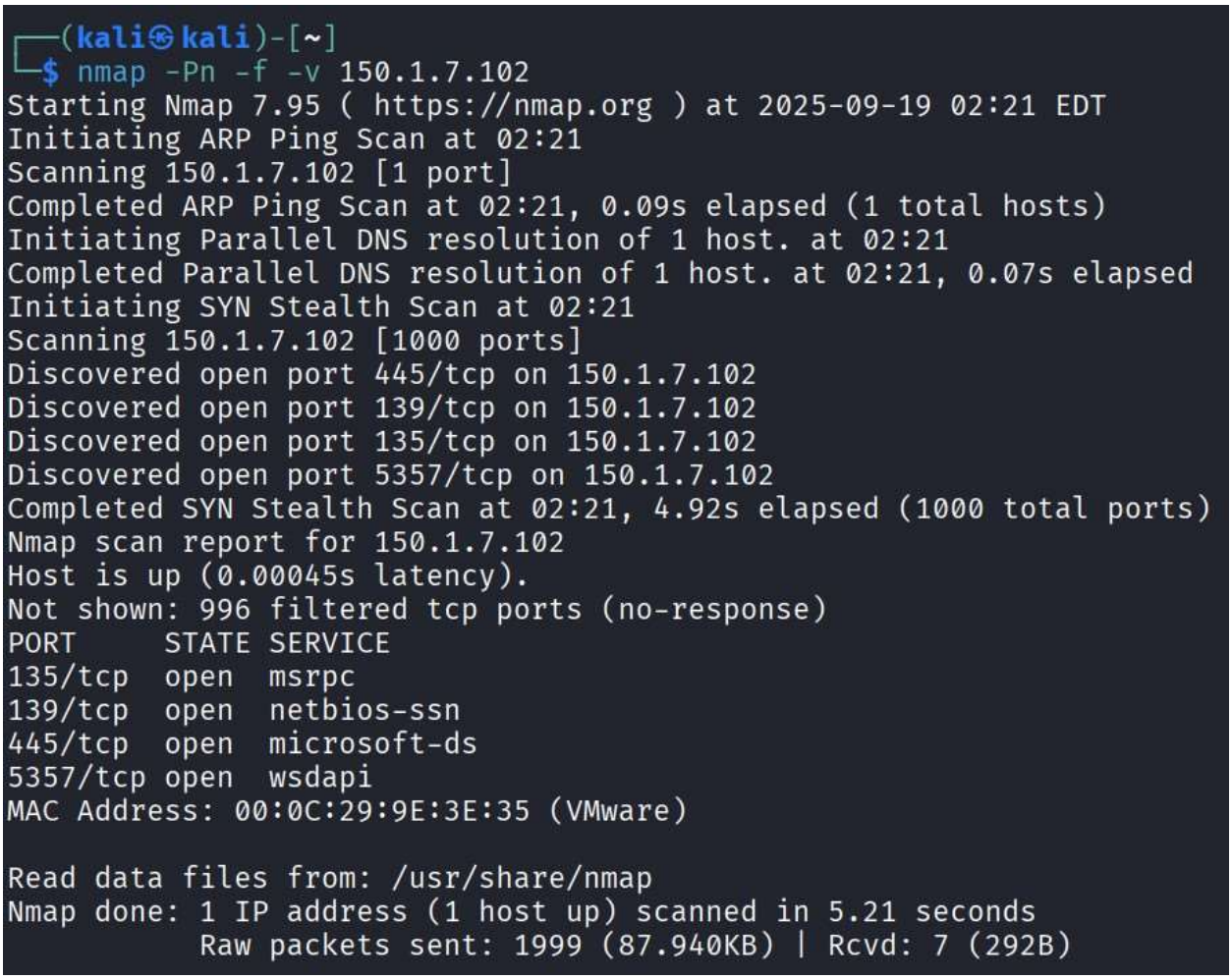
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -Pn -sX -F -T4 150.1.7.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-19 03:16 EDT
Nmap scan report for 150.1.7.100
Host is up (0.000063s latency).
All 100 scanned ports on 150.1.7.100 are in ignored states.
Not shown: 100 open|filtered tcp ports (no-response)
MAC Address: 00:50:56:C0:00:01 (VMware)

Nmap scan report for 150.1.7.102
Host is up (0.0013s latency).
All 100 scanned ports on 150.1.7.102 are in ignored states.
Not shown: 100 closed tcp ports (reset)
MAC Address: 00:0C:29:9E:3E:35 (VMware)

Nmap scan report for 150.1.7.104
Host is up (0.00026s latency).
Not shown: 82 closed tcp ports (reset)
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
23/tcp   open|filtered telnet
25/tcp   open|filtered smtp
53/tcp   open|filtered domain
80/tcp   open|filtered http
111/tcp  open|filtered rpcbind
139/tcp  open|filtered netbios-ssn
445/tcp  open|filtered microsoft-ds
513/tcp  open|filtered login
514/tcp  open|filtered shell
2049/tcp open|filtered nfs
2121/tcp open|filtered ccproxy-ftp
3306/tcp open|filtered mysql
5432/tcp open|filtered postgresql
5900/tcp open|filtered vnc
6000/tcp open|filtered X11
8009/tcp open|filtered ajp13
MAC Address: 00:0C:29:A5:C3:BD (VMware)
```

-F for fast scan, -T4 for fast result, since we are scanning entire network so we are scanning specific ports only.

- **Scanning single host `150.1.7.102` with fragmentation:**

**1. Fragmented packets with default MTU (8 bytes)**

nmap -Pn -f -v 150.1.7.102



**2. Specify custom MTU of 16 bytes**

nmap -Pn --mtu 16 -v 150.1.7.102

```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn --mtu 16 -v 150.1.7.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-19 02:21 EDT
Initiating ARP Ping Scan at 02:21
Scanning 150.1.7.102 [1 port]
Completed ARP Ping Scan at 02:21, 0.10s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:21
Completed Parallel DNS resolution of 1 host. at 02:21, 0.01s elapsed
Initiating SYN Stealth Scan at 02:21
Scanning 150.1.7.102 [1000 ports]
Discovered open port 135/tcp on 150.1.7.102
Discovered open port 445/tcp on 150.1.7.102
Discovered open port 139/tcp on 150.1.7.102
Discovered open port 5357/tcp on 150.1.7.102
Completed SYN Stealth Scan at 02:21, 4.38s elapsed (1000 total ports)
Nmap scan report for 150.1.7.102
Host is up (0.00037s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
MAC Address: 00:0C:29:9E:3E:35 (VMware)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.63 seconds
           Raw packets sent: 1999 (87.940KB) | Rcvd: 7 (292B)
```

- **Decoy scans against `150.1.7.102`:**

**1. Use 10 spoofed IPs as decoys**

nmap -Pn -D RND:10 -v 150.1.7.102

```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn -D RND:10 -v 150.1.7.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-19 02:21 EDT
Initiating ARP Ping Scan at 02:21
Scanning 150.1.7.102 [1 port]
Completed ARP Ping Scan at 02:21, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:21
Completed Parallel DNS resolution of 1 host. at 02:21, 0.05s elapsed
Initiating SYN Stealth Scan at 02:21
Scanning 150.1.7.102 [1000 ports]
Discovered open port 135/tcp on 150.1.7.102
Discovered open port 139/tcp on 150.1.7.102
Discovered open port 445/tcp on 150.1.7.102
Discovered open port 5357/tcp on 150.1.7.102
Completed SYN Stealth Scan at 02:21, 5.58s elapsed (1000 total ports)
Nmap scan report for 150.1.7.102
Host is up (0.00042s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
MAC Address: 00:0C:29:9E:3E:35 (VMware)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 5.82 seconds
           Raw packets sent: 21990 (967.544KB) | Rcvd: 8 (336B)
```

**2. Specify a single decoy IP**

nmap -Pn -D 171.124.180.173 -v 150.1.7.102

```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn -D 171.124.180.173 -v 150.1.7.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-19 02:21 EDT
Initiating ARP Ping Scan at 02:21
Scanning 150.1.7.102 [1 port]
Completed ARP Ping Scan at 02:21, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:21
Completed Parallel DNS resolution of 1 host. at 02:21, 0.02s elapsed
Initiating SYN Stealth Scan at 02:21
Scanning 150.1.7.102 [1000 ports]
Discovered open port 135/tcp on 150.1.7.102
Discovered open port 445/tcp on 150.1.7.102
Discovered open port 139/tcp on 150.1.7.102
Discovered open port 5357/tcp on 150.1.7.102
Completed SYN Stealth Scan at 02:21, 4.77s elapsed (1000 total ports)
Nmap scan report for 150.1.7.102
Host is up (0.00036s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
MAC Address: 00:0C:29:9E:3E:35 (VMware)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 5.03 seconds
           Raw packets sent: 3997 (175.852KB) | Rcvd: 7 (292B)
```

- **Idle (Zombie) Scan against `150.1.7.102`**

nmap -Pn -sI ZOMBIE_IP 150.1.7.102

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -Pn -sI 150.1.7.100 150.1.7.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-19 02:26 EDT
Idle scan using zombie 150.1.7.100 (150.1.7.100:80); Class: Incremental
Even though your Zombie (150.1.7.100; 150.1.7.100) appears to be vulnerable to IP ID sequence prediction (class: Inc
remental), our attempts have failed.  This generally means that either the Zombie uses a separate IP ID base for eac
h host (like Solaris), or because you cannot spoof IP packets (perhaps your ISP has enabled egress filtering to prev
ent IP spoofing), or maybe the target network recognizes the packet source as bogus and drops them
QUITTING!
```

- **Source Port Manipulation (pretend packets are from trusted service like DNS/HTTP):**

For example, source port 53 (DNS):

nmap -Pn --source-port 53 -v 150.1.7.102

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -Pn --source-port 53 -v 150.1.7.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-19 02:34 EDT
Initiating ARP Ping Scan at 02:34
Scanning 150.1.7.102 [1 port]
Completed ARP Ping Scan at 02:34, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:34
Completed Parallel DNS resolution of 1 host. at 02:35, 13.00s elapsed
Initiating SYN Stealth Scan at 02:35
Scanning 150.1.7.102 [1000 ports]
Discovered open port 139/tcp on 150.1.7.102
Discovered open port 445/tcp on 150.1.7.102
Discovered open port 135/tcp on 150.1.7.102
Increasing send delay for 150.1.7.102 from 0 to 5 due to 24 out of 79 dropped probes since last increase.
Increasing send delay for 150.1.7.102 from 5 to 10 due to 12 out of 38 dropped probes since last increase.
Discovered open port 5357/tcp on 150.1.7.102
Completed SYN Stealth Scan at 02:35, 10.36s elapsed (1000 total ports)
Nmap scan report for 150.1.7.102
Host is up (0.00040s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
MAC Address: 00:0C:29:9E:3E:35 (VMware)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 23.57 seconds
           Raw packets sent: 1066 (46.888KB) | Rcvd: 1001 (40.044KB)
```

- **Using AI and launch IP address decoy technique:**

```
┌──(root㉿kali)-[/home/kali]
└─# sgpt --shell "To evade an IDS/Firewall, use IP address decoy technique to scan the target IP address 150.1.7.102"
nmap -D RND:10 150.1.7.102
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-19 02:34 EDT
Nmap scan report for 150.1.7.102
Host is up (0.00059s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
MAC Address: 00:0C:29:9E:3E:35 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 35.35 seconds
```