Reconnaissance Monitoring Lab

Niranjan Meegammana
MSc (Cyber Security)

Tools : Wireshark and nmap

Install Wireshark

```
sudo apt update
```

```
sudo apt install nmap wireshark
```

#Open Terminal

```
sudo su
```

#Find network information

```
ifconfig
```

>>

```
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.240.129  netmask 255.255.255.0  broadcast 192.168.240.255

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
```

#run wireshark

```
wireshark
```

#open another terminal

```
sudo su
which nmap
nmap -h
nmap -sn  <target-IP>
```

#192.168.240.0/24

#Reconnaissance

#Host discovery:

```
nmap -sn 192.168.240.0/24
```

Capture Packets

```
507	1.824110902	VMware_56:53:80	Broadcast	ARP	42	Who has 192.168.240.18? Tell 192.168.240.129

516	1.960640442	192.168.240.129	192.168.240.2	DNS	88	Standard query 0x7498 PTR 254.240.168.192.in-addr.arpa

523	5.331431130	192.168.240.129	91.189.91.157	NTP	90	NTP Version 4, client

592	222.887255298	192.168.240.128	192.168.240.254	DHCP	324	DHCP Request - Transaction ID 0xbd780270

597	223.105152426	192.168.240.128	185.125.190.98	TCP	74	46456 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1087797214 TSecr=0 WS=128

598	223.273971417	185.125.190.98	192.168.240.128	TCP	60	80 → 46456 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460

599	223.274488845	192.168.240.128	185.125.190.98	TCP	60	46456 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0

617	243.241403950	192.168.240.129	185.125.190.48	HTTP	141	GET / HTTP/1.1
```

```
617	243.241403950	192.168.240.129	185.125.190.48	HTTP	141	GET / HTTP/1.1
```

NMAP report

```
nmap -sn 192.168.240.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-12-03 02:47 PST
Nmap scan report for 192.168.240.1
```

```
Host is up (0.00039s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.240.2
Host is up (0.00023s latency).
MAC Address: 00:50:56:FE:42:89 (VMware)

Nmap scan report for 192.168.240.128
Host is up (0.00016s latency).
MAC Address: 00:0C:29:B3:DB:CE (VMware)
Nmap scan report for 192.168.240.254
Host is up (0.00014s latency).
MAC Address: 00:50:56:EA:DE:F0 (VMware)

Nmap scan report for 192.168.240.129
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.13 seconds
```

Wireshark

Apply capture filters to focus on reconnaissance traffic (e.g., ICMP, TCP SYN).

```
icmp || tcp.flags.syn == 1
```

```
124171     562.167761651     192.168.240.129     192.168.1.10   TCP   58     48487 → 26398
[SYN] Seq=0 Win=1024 Len=0 MSS=1460
```

- Timestamp : 124171 — This could be the capture time or packet number.
- Duration : 562.167761651 — Duration associated with the communication or delay between packets.
- Source IP : 192.168.240.129 — The source IP address initiating the communication.
- Destination IP : 192.168.1.10 — The destination IP address of the communication.
- Protocol : TCP — The communication is using the Transmission Control Protocol (TCP).
- Length : 58 bytes — The size of the packet.

- Source Port : 48487 — The source port number on the source machine.
- Destination Port : 26398 — The destination port number on the destination machine.
- Flags : [SYN] — This indicates the initial synchronization request in the TCP handshake.
- Sequence Number : Seq=0 — Sequence number of the packet, 0 for the first packet in the handshake.
- Window Size : Win=1024 — The size of the TCP window used for flow control.
- MSS (Max Segment Size) : 1460 — Specifies the maximum size of the TCP segment can be sent.

This packet is part of a TCP handshake, specifically the initial SYN packet, where the client is attempting to establish a connection with the server (or vice versa).

Port scanning:

```
nmap -p-  <target-IP>
nmap -v -p 1-200 <target-IP>
```

192.168.1.10

192.168.240.129

```
Discovered open port 139/tcp on 192.168.1.10
Discovered open port 135/tcp on 192.168.1.10
Discovered open port 80/tcp on 192.168.1.10
Completed Connect Scan at 04:30, 2.12s elapsed (200 total ports)
Nmap scan report for 192.168.1.10
Host is up (0.0012s latency).
Not shown: 196 filtered ports
PORT    STATE  SERVICE
80/tcp  open   http
135/tcp open   msrpc
137/tcp closed netbios-ns
139/tcp open   netbios-ssn
```

Check port 80 scan in wireshark

```
tcp.port == 80
```

Service detection:

```
nmap -sV <target-IP>
nmap -v -sV -p 1-200 192.168.1.10
```

```
PORT    STATE  SERVICE     VERSION
80/tcp  open   http        Apache httpd 2.4.56 ((Win64) OpenSSL/1.1.1t PHP/8.0.28)
135/tcp open   msrpc       Microsoft Windows RPC
137/tcp closed netbios-ns
139/tcp open   netbios-ssn Microsoft Windows netbios-ssn
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Apache HTTPD 2.4.56 known Vulnerabilities

Check for the latest CVE

OpenSSL 1.1.1t could also have security flaws

PHP 8.0.28 could have security issues,

OS detection:

```
nmap -O <target-IP>
nmap -v -O 192.168.1.10
```

```
PORT STATE SERVICE
80/tcp open http
OS details: Linux 3.2 - 4.9, Linux 5.0, or Linux 5.4
OS fingerprint not ideal because of insufficient responses.
```

Vulnerability scan

```
nmap -v --script=vuln <target-ip>
nmap -v --script=vuln 192.168.1.10
```

Homework

A potential attacker is scanning your network. Use Wireshark to detect the activity and report findings. Identify the scanning technique and the target ports/services.