

## ASSIGNMENT 8

### AIM:

Installation of NMAP and using it with different options to scan open ports, perform OS fingerprinting, ping scan, TCP port scan, UDP port scan, etc.

### LO MAPPED: LO4

### THEORY:

#### 1. TCP SYN SCAN:

- SYN scan is the default and most popular scan option for good reasons. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by restrictive firewalls.
- It is also relatively unobtrusive and stealthy since it never completes TCP connections.
- SYN scan works against any compliant TCP stack rather than depending on idiosyncrasies of specific platforms as Nmap's FIN/NULL/Xmas, Maimon and idle scans do.

Command: `nmap -sS [DomainName] [IP Address]`

```
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# nmap -sS www.google.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 15:04 IST
Nmap scan report for www.google.com (142.250.192.132)
Host is up (0.0045s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4009:82b::2004
rDNS record for 142.250.192.132: bom12s18-in-f4.1e100.net
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 17.07 seconds
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006#
```

No.	Time	Source	Destination	Protocol	Length	Info
2038	14.270203335	192.168.0.206	142.250.192.132	TCP	58	39628 → 1998 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2039	14.270211852	192.168.0.206	142.250.192.132	TCP	58	39628 → 28201 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2040	14.270219245	192.168.0.206	142.250.192.132	TCP	58	39628 → 2382 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2041	14.270226691	192.168.0.206	142.250.192.132	TCP	58	39628 → 5959 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2042	14.270233972	192.168.0.206	142.250.192.132	TCP	58	39628 → 16016 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2043	14.270241211	192.168.0.206	142.250.192.132	TCP	58	39628 → 5904 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2044	14.270248377	192.168.0.206	142.250.192.132	TCP	58	39628 → 8873 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2045	14.272433666	192.168.0.206	142.250.192.132	TCP	58	39628 → 48080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2046	14.272449555	192.168.0.206	142.250.192.132	TCP	58	39628 → 389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2047	14.272458534	192.168.0.206	142.250.192.132	TCP	58	39628 → 1099 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2048	14.272467927	192.168.0.206	142.250.192.132	TCP	58	39628 → 7443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2049	14.344173319	192.168.0.206	142.250.192.132	TCP	58	39628 → 1063 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2050	14.381009838	192.168.0.206	142.250.192.132	TCP	58	39628 → 3995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Frame 1: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface 0  
Ethernet II, Src: 04:0e:3c:19:2e:35 (04:0e:3c:19:2e:35), Dst: IPv4mcast\_7f:ff:fa (01:00:5e:7f:ff:fa)  
Internet Protocol Version 4, Src: 192.168.0.205, Dst: 239.255.255.250  
User Datagram Protocol, Src Port: 59869, Dst Port: 1900  
Simple Service Discovery Protocol

## 2. TCP CONNECT SCAN:

- TCP connect scan is the default TCP scan type when SYN scan is not an option.
- This is the case when a user does not have raw packet privileges.
- Instead of writing raw packets as most other scan types do, Nmap asks the underlying operating system to establish a connection with the target machine and port by issuing the connect system call.
- This is the same high-level system call that web browsers, P2P clients, and most other network-enabled applications use to establish a connection.
- It is part of a programming interface known as the Berkeley Sockets API. Rather than read raw packet responses off the wire, Nmap uses this API to obtain status information on each connection attempt.

Command: `nmap -sT [DomainName] [IP Address]`

```
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# nmap -sT www.google.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 15:13 IST
Nmap scan report for www.google.com (142.250.192.132)
Host is up (0.0029s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4009:82b::2004
rDNS record for 142.250.192.132: bom12s18-in-f4.1e100.net
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 5.10 seconds
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006#
```

## 3. UDP SCANS:

- While most popular services on the Internet run over the TCP protocol, [UDP](#) services are widely deployed. DNS, SNMP, and DHCP (registered ports 53, 161/162, and 67/68) are three of the most common.
- Because UDP scanning is generally slower and more difficult than TCP, some security auditors ignore these ports.
- This is a mistake, as exploitable UDP services are quite common and attackers certainly don't ignore the whole protocol. Fortunately, Nmap can help inventory UDP ports.
- UDP scan is activated with the -sU option. It can be combined with a TCP scan type such as SYN scan (-sS) to check both protocols during the same run.

Command: `nmap -sU [DomainName] [IP Address]`

```

Nmap done: 1 IP address (1 host up) scanned in 5.10 seconds
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# nmap -sU www.google.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 15:16 IST
Nmap scan report for www.google.com (142.250.192.132)
Host is up (0.0034s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4009:82b::2004
rDNS record for 142.250.192.132: bom12s18-in-f4.1e100.net
Not shown: 999 open|filtered ports
PORT      STATE SERVICE
33459/udp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 10.93 seconds
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# 

```

#### 4. TCP NULL, FIN, and Xmas scans:

- These three scan types (even more are possible with the --scanflags option described in the next section) exploit a subtle loophole in the TCP RFC to differentiate between open and closed ports.
- RFC 793 says that “if the [destination] port state is CLOSED .... an incoming segment not containing a RST causes a RST to be sent in response.” Then the next page discusses packets sent to open ports without the SYN, RST, or ACK bits set, stating that: “you are unlikely to get here, but if you do, drop the segment, and return.”
- When scanning systems compliant with this RFC text, any packet not containing SYN, RST, or ACK bits will result in a returned RST if the port is closed and no response at all if the port is open. As long as none of those three bits are included, any combination of the other three (FIN, PSH, and URG) are OK. Nmap exploits this with three scan types:
- Null scan (-sN)  
Does not set any bits (TCP flag header is 0)
- FIN scan (-sF)  
Sets just the TCP FIN bit.
- Xmas scan (-sX)

```

Nmap done: 1 IP address (1 host up) scanned in 10.93 seconds
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# nmap -sN www.google.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 15:22 IST
Nmap scan report for www.google.com (142.250.192.132)
Host is up (0.033s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4009:82b::2004
rDNS record for 142.250.192.132: bom12s18-in-f4.1e100.net
All 1000 scanned ports on www.google.com (142.250.192.132) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 13.67 seconds
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# 

```



```

root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# nmap -sF www.google.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 15:25 IST
Nmap scan report for www.google.com (142.250.192.132)
Host is up (0.0029s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4009:82b::2004
rDNS record for 142.250.192.132: bom12s18-in-f4.1e100.net
All 1000 scanned ports on www.google.com (142.250.192.132) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 11.33 seconds
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# 

```

```

root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# nmap -sX www.google.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 15:26 IST
Nmap scan report for www.google.com (142.250.192.132)
Host is up (0.0036s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4009:82b::2004
rDNS record for 142.250.192.132: bom12s18-in-f4.1e100.net
All 1000 scanned ports on www.google.com (142.250.192.132) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 12.38 seconds
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# 

```

## 5. TCP ACK SCAN:

- This scan is different than the others discussed so far in that it never determines open (or even open|filtered) ports.
- It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.
- The ACK scan probe packet has only the ACK flag set (unless you use --scanflags). When scanning unfiltered systems, open and closed ports will both return a RST packet.
- Nmap then labels them as unfiltered, meaning that they are reachable by the ACK packet, but whether they are open or closed is undetermined. Ports that don't respond, or send certain ICMP error messages back (type 3, code 0, 1, 2, 3, 9, 10, or 13), are labeled filtered.

```

root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# nmap -sA www.google.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 15:28 IST
Nmap scan report for www.google.com (142.250.192.132)
Host is up (0.0043s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4009:82b::2004
rDNS record for 142.250.192.132: bom12s18-in-f4.1e100.net
Not shown: 998 filtered ports
PORT      STATE      SERVICE
80/tcp    unfiltered http
443/tcp   unfiltered https

Nmap done: 1 IP address (1 host up) scanned in 17.02 seconds
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# 

```

## 6. IP PROTOCOL SCAN:

- IP protocol scan allows you to determine which IP protocols (TCP, ICMP, IGMP, etc.) are supported by target machines.
- This isn't technically a port scan, since it cycles through IP protocol numbers rather than TCP or UDP port numbers.
- Yet it still uses the -p option to select scanned protocol numbers, reports its results within the normal port table format, and even uses the same underlying scan engine as the true port scanning methods.

```
File Edit View Search Terminal Help
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# nmap -sO www.google.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 15:32 IST
Nmap scan report for www.google.com (142.250.192.132)
Host is up (0.0031s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4009:82b::2004
rDNS record for 142.250.192.132: bom12s18-in-f4.1e100.net
Not shown: 254 open|filtered protocols
PROTOCOL STATE SERVICE
1      open  icmp
6      open  tcp

Nmap done: 1 IP address (1 host up) scanned in 5.72 seconds
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# ifconfig
```

## 7. OS DETECTION:

- One of Nmap's best-known features is remote OS detection using TCP/IP stack fingerprinting.
- Nmap sends a series of TCP and UDP packets to the remote host and examines practically every bit in the responses.
- After performing dozens of tests such as TCP ISN sampling, TCP options support and ordering, IP ID sampling, and the initial window size check, Nmap compares the results to its nmap-os-db database of more than 2,600 known OS fingerprints and prints out the OS details if there is a match.

```
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# nmap -O 192.168.0.226

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 15:36 IST
Nmap scan report for 192.168.0.226
Host is up (0.00054s latency).
All 1000 scanned ports on 192.168.0.226 are closed
MAC Address: 04:0E:3C:19:28:80 (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.69 seconds
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006#
```

## 8. PING SCAN:

- This scan type lists the hosts within the specified range that responded to a ping.
- It allows you to detect which computers are online, rather than which ports are open. Four methods exist within Nmap for ping sweeping.
- The first method sends an ICMP ECHO REQUEST (ping request) packet to the destination system.
- If an ICMP ECHO REPLY is received, the system is up, and ICMP packets are not blocked. If there is no response to the ICMP ping, Nmap will try a "TCP Ping", to determine whether ICMP is blocked, or if the host is really not online.
- A TCP Ping sends either a SYN or an ACK packet to any port (80 is the default) on the remote system. If RST, or a SYN/ACK, is returned, then the remote system is online. If the remote system does not respond, either it is offline, or the chosen port is filtered, and thus not responding to anything.

```
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# nmap -sP 192.168.0.*

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 15:39 IST
Nmap scan report for _gateway (192.168.0.1)
Host is up (0.00076s latency).
MAC Address: AC:15:A2:B9:9E:29 (Unknown)
Nmap scan report for 192.168.0.105
Host is up (-0.099s latency).
MAC Address: A4:AE:12:84:7F:CF (Unknown)
Nmap scan report for 192.168.0.114
Host is up (-0.100s latency).
MAC Address: 04:0E:3C:19:2E:0F (Unknown)
Nmap scan report for 192.168.0.115
Host is up (-0.099s latency).
MAC Address: 04:0E:3C:1A:5C:AD (Unknown)
Nmap scan report for 192.168.0.116
Host is up (0.00039s latency).
MAC Address: 04:0E:3C:1A:60:A0 (Unknown)
Nmap scan report for 192.168.0.117
Host is up (0.00039s latency).
MAC Address: 04:0E:3C:19:2D:1C (Unknown)
Nmap scan report for 192.168.0.118
Host is up (0.00055s latency).
MAC Address: E4:54:E8:C6:37:76 (Unknown)
Nmap scan report for 192.168.0.119
Host is up (0.00040s latency).
MAC Address: 04:0E:3C:1A:5F:16 (Unknown)
Nmap scan report for 192.168.0.121
Host is up (0.00075s latency).
MAC Address: 90:8D:78:7E:5A:B3 (D-Link International)
Nmap scan report for 192.168.0.123
Host is up (-0.099s latency).
MAC Address: F4:39:09:49:0A:33 (Unknown)
Nmap scan report for 192.168.0.126
Host is up (-0.10s latency).
MAC Address: 04:0E:3C:1A:61:7F (Unknown)
Nmap scan report for 192.168.0.133
Host is up (-0.10s latency).
MAC Address: A0:8C:FD:C5:AD:A1 (Hewlett Packard)
Nmap scan report for 192.168.0.135
Host is up (-0.10s latency).
MAC Address: A0:8C:FD:DD:8C:AE (Hewlett Packard)
Nmap scan report for 192.168.0.141
Host is up (-0.100s latency).
```

**CONCLUSION:** In this experiment we learnt about installation of NMAP and using it with different options to scan open ports, perform OS fingerprinting, ping scan, TCP port scan, UDP port scan, etc.