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 :- LO4 mapped

THEORY :- NMAP is a versatile network exploration and security auditing, revealing open ports, services, and vulnerabilities on target system, aiding in network assessment and defence.

TCP SYN: 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.

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

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 15:25 IST
Nmap scan report for flipkart.com (103.243.32.90)
Host is up (0.029s latency).
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 17.83 seconds
```

TCP Connect: 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.

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

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 15:35 IST
Nmap scan report for flipkart.com (103.243.32.90)
Host is up (0.026s latency).
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 4.86 seconds
```

UDP: 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.

```
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# nmap -sU flipkart.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 15:37 IST
Nmap scan report for flipkart.com (103.243.32.90)
Host is up (0.028s latency).
All 1000 scanned ports on flipkart.com (103.243.32.90) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 12.35 seconds
```

TCP Null: 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. Page 65 of 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.” Null scan (`-sN`)
Does not set any bits (TCP flag header is 0)

```
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# nmap -sN flipkart.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 15:38 IST
Nmap scan report for flipkart.com (103.243.32.90)
Host is up (0.024s latency).
All 1000 scanned ports on flipkart.com (103.243.32.90) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 25.70 seconds
```

TCP FIN: 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. Page 65 of 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.”
FIN scan (`-sF`)
Sets just the TCP FIN bit.

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

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 15:39 IST
Nmap scan report for flipkart.com (103.243.32.90)
Host is up (0.024s latency).
All 1000 scanned ports on flipkart.com (103.243.32.90) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 25.25 seconds
```

TCP XMAS: 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. Page 65 of 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.”Xmas scan (`-sX`)
Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.

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

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 15:40 IST
Nmap scan report for flipkart.com (103.243.32.90)
Host is up (0.024s latency).
All 1000 scanned ports on flipkart.com (103.243.32.90) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 25.50 seconds
```

TCP ACK: 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.

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

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 15:43 IST
Nmap scan report for flipkart.com (103.243.32.90)
Host is up (0.026s latency).
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 5.65 seconds
```

IP Protocol: This 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. So it is close enough to a port scan that it belongs here.

```
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# nmap -sO flipkart.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 15:45 IST
Nmap scan report for flipkart.com (103.243.32.90)
Host is up (0.036s latency).
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 7.27 seconds
```

OS Fingerprinting: OS fingerprinting works by sending up to 16 TCP, UDP, and ICMP probes to known open and closed ports of the target machine. These probes are specially designed to exploit various ambiguities in the standard protocol RFCs. Then Nmap listens for responses. Dozens of attributes in those responses are analyzed and combined to generate a fingerprint. Every probe packet is tracked and resent at least once if there is no response. All of the packets are IPv4 with a random IP ID value. Probes to an open TCP port are skipped if no such port has been found. For closed TCP or UDP ports, Nmap will first check if such a port has been found. If not, Nmap will just pick a port at random and hope for the best.

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

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-09 15:51 IST
Nmap scan report for flipkart.com (103.243.32.90)
Host is up (0.029s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Aggressive OS guesses: Crestron XPanel control system (89%), HP P2000 G3 NAS dev
ice (86%), ASUS RT-N56U WAP (Linux 3.4) (86%), Linux 3.1 (86%), Linux 3.16 (86%)
, Linux 3.2 (86%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (86%), Android
 4.1 - 6.0 (Linux 3.4 or 3.10) (85%), Android 5.0 - 5.1 (85%), Android 5.0 - 6.0
 (Linux 3.10) (85%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.17 seconds
```

Ping Sweep: A ping sweep is a network scanning technique to identify active devices on a network by pinging a range of IP addresses. Compared to other methods, ping sweeps can be harder to detect as it is not as aggressive and can skip regular scan stages, making it more of an advantage

```
Nmap scan report for 192.168.0.200
Host is up (-0.100s latency).
MAC Address: A0:8C:FD:CA:58:4A (Hewlett Packard)
Nmap scan report for 192.168.0.206
Host is up (0.00071s latency).
MAC Address: 04:0E:3C:1A:64:38 (Unknown)
Nmap scan report for 192.168.0.209
Host is up (0.00042s latency).
MAC Address: 00:C0:02:12:35:89 (Sercomm)
Nmap scan report for 192.168.0.211
Host is up (0.00059s latency).
MAC Address: A0:8C:FD:D6:EF:86 (Hewlett Packard)
Nmap scan report for 192.168.0.213
Host is up (0.00034s latency).
MAC Address: 04:0E:3C:1B:D1:42 (Unknown)
Nmap scan report for 192.168.0.214
Host is up (0.00040s latency).
MAC Address: 04:0E:3C:19:2D:11 (Unknown)
Nmap scan report for 192.168.0.215
Host is up (-0.087s latency).
MAC Address: 74:F2:FA:90:D2:AF (Unknown)
Nmap scan report for 192.168.0.219
Host is up (-0.10s latency).
MAC Address: 04:0E:3C:19:2B:7B (Unknown)
Nmap scan report for 192.168.0.226
Host is up (-0.10s latency).
MAC Address: 04:0E:3C:19:28:80 (Unknown)
Nmap scan report for 192.168.0.236
Host is up (-0.100s latency).
MAC Address: 04:0E:3C:1A:62:25 (Unknown)
Nmap scan report for 192.168.0.244
Host is up (0.00068s latency).
MAC Address: 04:0E:3C:19:2C:38 (Unknown)
Nmap scan report for 192.168.0.245
Host is up (0.0044s latency).
MAC Address: 04:0E:3C:1A:64:32 (Unknown)
Nmap scan report for 192.168.0.249
Host is up (0.00083s latency).
MAC Address: 04:0E:3C:1A:5F:06 (Unknown)
Nmap scan report for lab1006-HP-280-G4-MT-Business-PC (192.168.0.161)
Host is up.
Nmap done: 256 IP addresses (45 hosts up) scanned in 3.34 seconds
```

Wireshark results:

2001	56.318257002	192.168.0.190	142.250.192.132	TCP	58	52626 → 1037 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2002	56.318266291	192.168.0.190	142.250.192.132	TCP	58	52626 → 8333 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2003	56.318275619	192.168.0.190	142.250.192.132	TCP	58	52626 → 2040 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2004	56.318285439	192.168.0.190	142.250.192.132	TCP	58	52626 → 32778 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2005	56.320642990	192.168.0.190	142.250.192.132	TCP	58	52626 → 11110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2006	56.320668043	192.168.0.190	142.250.192.132	TCP	58	52626 → 1087 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2007	56.320678131	192.168.0.190	142.250.192.132	TCP	58	52626 → 64623 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2008	56.320687593	192.168.0.190	142.250.192.132	TCP	58	52626 → 1272 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2009	56.320696895	192.168.0.190	142.250.192.132	TCP	58	52626 → 19842 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2010	56.320706275	192.168.0.190	142.250.192.132	TCP	58	52626 → 3260 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2011	56.343275717	Cisco_15:44:53	Cisco_77:e4:61	0xa0a0	60	Ethernet II
2012	56.378696036	192.168.0.190	142.250.192.132	TCP	58	52627 → 513 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

CONCLUSION :- In this assignment we succesfully install NMAP and successfully implemented its various options to scan open ports, perform OS fingerprinting, etc.