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

LO MAPPED: LO4

Theory:

Port Scanning Techniques

TCP connect scan

Command: nmap -sT www.google.com

The TCP connect scan is a network reconnaissance technique that establishes full TCP connections to target ports. It determines port states by analyzing the success of failure of these connections. This method is reliable but can be easily detected by intrusion detection systems due to the complete connection setup.

```
shubham@shubham-VirtualBox:/$ nmap -sT www.google.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-26 21:47 IST
Nmap scan report for www.google.com (172.217.166.36)
Host is up (0.032s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4009:80c::2004
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
```

TCP ACK Scan

Command: nmap -sA www.flipkart.com

The TCP ACK scan sends TCP ACK packets to target ports, aiming to distinguish between open, closed, and filtered ports. This scan doesn't determine port status directly but observes the response behavior to infer whether a firewall or filtering device is present. It doesn't work well against hosts with stateful firewalls.

```
shubham@shubham-VirtualBox:/$ sudo nmap -sA www.flipkart.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-26 21:50 IST
Nmap scan report for www.flipkart.com (163.53.76.86)
Host is up (0.00048s latency).
All 1000 scanned ports on www.flipkart.com (163.53.76.86) are unfiltered

Nmap done: 1 IP address (1 host up) scanned in 6.20 seconds
```

Null scan

Command: nmap -sN www.yahoo.com

The Null scan sends TCP packets with no flags (all flags set to 0) to target ports. It relies on analyzing reponses to determine port states. If a port is open, it may ignore the packet, whereas closed ports could respond with a TCP RST packet. Firewalls or some systems may react unpredictably to null packets.

```
root@shubham-VirtualBox:~# nmap -sN www.yahoo.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-26 21:53 IST
Nmap scan report for www.yahoo.com (202.165.107.49)
Host is up (0.00075s latency).
Other addresses for www.yahoo.com (not scanned): 202.165.107.50 2406:2000:e4:1605::9000 2406:2000:e
rDNS record for 202.165.107.49: media-router-fp73.prod.media.vip.sg3.yahoo.com
All 1000 scanned ports on www.yahoo.com (202.165.107.49) are closed

Nmap done: 1 IP address (1 host up) scanned in 3.50 seconds
```

fin scan

Command: nmap -sF www.tsec.edu

The FIN scan sends TCP packets with only the FIN (Finish) flag set to target ports. This method checks for open ports by observing how the target host reacts. If the port is closed, a RST packet might be sent. If the port is open, it could simply ignore the packet. It's stealthy but night not work against all systems.

```
root@shubham-VirtualBox:~# nmap -sF www.tsec.edu

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-26 21:54 IST
Nmap scan report for www.tsec.edu (162.241.70.62)
Host is up (0.00096s latency).
All 1000 scanned ports on www.tsec.edu (162.241.70.62) are closed
```

xmas scan

Command: nmap -sX www.google.com

The Xmas scan sends TCP packets with multiple flags set (FIN, PSH, and URG) to target ports. Similar to FIN and Null scans, it relies on analyzing responses to infer port states. Its name derives from the "lights" created by the flags. However, it's less reliable due to varying responses across different systems.

```
root@shubham-VirtualBox:~# nmap -sX www.google.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-26 21:56 IST
Nmap scan report for www.google.com (172.217.166.36)
Host is up (0.00076s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4009:80c::2004
All 1000 scanned ports on www.google.com (172.217.166.36) are closed

Nmap done: 1 IP address (1 host up) scanned in 5.51 seconds
```

Ip protocol scan

Command: nmap -s0 www.google.com

The IP protocol scan explores which IP protocols are supported by a target. It sends packets with different IP protocol numbers and observes any responses. This can help identify the services running on non-standard protocols. Common protocols have specific numbers (e.g., ICMP is 1, TCP is 6).

```
Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-22 12:08 IST
Nmap scan report for www.google.com (172.217.27.196)
Host is up (0.0036s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4009:800
::2004
rDNS record for 172.217.27.196: bom07s15-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 26.38 seconds
```

os detection scan

Command: nmap -O

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.

```
Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-22 12:07 IST
Nmap scan report for 192.168.0.172
Host is up (0.00034s latency).
All 1000 scanned ports on 192.168.0.172 are closed
MAC Address: 04:0E:3C:1A:5C:4F (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 3.63 seconds
```

ping scan

Command: nmap -sP 192.168.0.172

The ping scan (also called a “ping sweep”) determines the online status of multiple hosts in a range by sending ICMP Echo Requests. It doesn’t provide detailed information about open ports but helps identify active hosts quickly. It’s a basic form of network reconnaissance.

```
Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-22 12:17 IST
Nmap scan report for 192.168.0.172
Host is up (0.00026s latency).
MAC Address: 04:0E:3C:1A:5C:4F (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
```

udp scan

Command: nmap -sU 192.168.0.172

The UDP scan identifies open UDP ports on a target by sending UDP packets and analyzing the responses. Unlike TCP, UDP is connectionless, making it harder to detect open ports. However, it’s slower and less reliable due to UDP’s stateless nature and the potential for packet loss.

```
root@shubham-VirtualBox:~# nmap -sU www.google.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-26 22:25 IST
Nmap scan report for www.google.com (172.217.166.36)
Host is up (0.00031s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4009:80c::2004
All 1000 scanned ports on www.google.com (172.217.166.36) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 9.79 seconds
```

Conclusion: In this assignment implementation of all commands nmap network scanning commands and used wireshark are understood.