Roll no. : 53
Name: Shreya Kamath
Date: 12th September, 2023.

LAB ASSIGNMENT NO. 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.

LAB OUTCOME ATTAINED:

LO 3: Explore the different network reconnaissance tools to gather information about networks.

THEORY:

While Nmap has grown in functionality over the years, it began as an efficient port scanner, and that remains its core function. The simple command **nmap *<target>*** scans 1,000 TCP ports on the host *<target>*. While many port scanners have traditionally lumped all ports into the open or closed states, Nmap is much more granular. It divides ports into six states: open, closed, filtered, unfiltered, open|filtered, or closed|filtered. These states are not intrinsic properties of the port itself, but describe how Nmap sees them. For example, an Nmap scan from the same network as the target may show port 135/tcp as open, while a scan at the same time with the same options from across the Internet might show that port as filtered.

The six port states recognized by Nmap:

1. Open

An application is actively accepting TCP connections, UDP datagrams or SCTP associations on this port. Finding these is often the primary goal of port scanning. Security-minded people know that each open port is an avenue for attack. Attackers and pen-testers want to exploit the open ports, while administrators try to close or protect them with firewalls without thwarting legitimate users. Open ports are also interesting for non-security scans because they show services available for use on the network.

2. closed

A closed port is accessible (it receives and responds to Nmap probe packets), but there is no application listening on it. They can be helpful in showing that a host is up on an IP address (host discovery, or ping scanning), and as part of OS detection. Because closed ports are reachable, it may be worth scanning later in case some open up. Administrators may want to consider blocking such ports with a firewall. Then they would appear in the filtered state, discussed next.

3. Filtered

Nmap cannot determine whether the port is open because packet filtering prevents its probes from reaching the port. The filtering could be from a dedicated firewall device, router rules, or host-based firewall software. These ports frustrate attackers because they provide so little information. Sometimes they respond with ICMP error messages such as type 3 code 13 (destination unreachable: communication administratively prohibited), but filters that simply drop probes without responding are far more common. This forces Nmap to retry several times just in case the probe was dropped due to network congestion rather than filtering. This slows down the scan dramatically.

4. unfiltered

The unfiltered state means that a port is accessible, but Nmap is unable to determine whether it is open or closed. Only the ACK scan, which is used to map firewall rulesets, classifies ports into this state. Scanning unfiltered ports with other scan types such as Window scan, SYN scan, or FIN scan, may help resolve whether the port is open.

5. open|filtered

Nmap places ports in this state when it is unable to determine whether a port is open or filtered. This occurs for scan types in which open ports give no response. The lack of response could also mean that a packet filter dropped the probe or any response it elicited. So Nmap does not know for sure whether the port is open or being filtered. The UDP, IP protocol, FIN, NULL, and Xmas scans classify ports this way.

6. closed|filtered

This state is used when Nmap is unable to determine whether a port is closed or filtered. It is only used for the IP ID idle scan.

COMMANDS FOR VARIOUS PORT SCANNING TECHNIQUES:

1. TCP Connect Scan:
   - Command: `*nmap -sT target_ip*`
   - Explanation: TCP Connect Scan is a basic port scanning technique. It establishes a full connection to each target port to determine whether it's open or closed. Open ports will complete the connection, while closed ports will result in a refusal.

2. TCP SYN Scan:
   - Command: `*nmap -sS target_ip*`
   - Explanation: TCP SYN Scan sends SYN packets to target ports and analyses the response. If a SYN/ACK is received, the port is open; if a RST is received, it's closed. This scan is stealthy and doesn't complete the full connection.

3. FIN Scan:
   - Command: `*nmap -sF target_ip*`
   - Explanation: FIN Scan sends FIN packets to target ports. If the port is closed, it should respond with a RST. However, if the port is open, it may ignore the packet. This scan can be used to identify firewall filtering.

4. Null Scan:
   - Command: `*nmap -sN target_ip*`
   - Explanation: Null Scan sends packets with no flags set to target ports. If the port is closed, it should respond with a RST. If it's open, it may ignore the packet. Similar to the FIN Scan, it can identify firewall filtering.

5. XMAS Scan:
   - Command: `*nmap -sX target_ip*`
   - Explanation: XMAS Scan sends packets with multiple TCP flags set (FIN, URG, and PSH) to target ports. Similar to Null and FIN Scans, it's used to identify filtering or state of the ports.

6. ACK Scan:

- Command: `*nmap -sA target_ip*`
- Explanation: ACK Scan sends packets with only the ACK flag set to target ports. It's used to detect stateful filtering systems. If it receives an RST, the port is unfiltered.

7. Ping Sweep:
- Command: `*nmap -sn target_subnet*`
- Explanation: Ping Sweep scans a range of IP addresses to identify hosts that are up and responsive. It sends ICMP echo requests to discover active hosts in the specified subnet.

8. Service and Version Detection:
- Command: *`nmap -sV target_ip`*
- Explanation: Service and Version Detection is used to identify the services and versions running on open ports. Nmap sends probes to the open ports and matches responses to a database of known services and versions.

9. Port and Port Range Scanning:
- Command: `*nmap -p port(s) target_ip*`
- Explanation: Port and Port Range Scanning allows you to specify single ports or ranges to scan, helping you focus on specific services or areas of interest.

10. OS Fingerprinting:
- Command: `*nmap -O target_ip*`
- Explanation: OS Fingerprinting is used to identify the operating system of the target host. Nmap analyses responses to specific probes and matches them to known OS signatures to make an educated guess about the OS.

These Nmap scanning techniques provide various ways to identify open ports, services, and even the target's operating system, depending on the level of detail and stealth required.

OUTPUT:

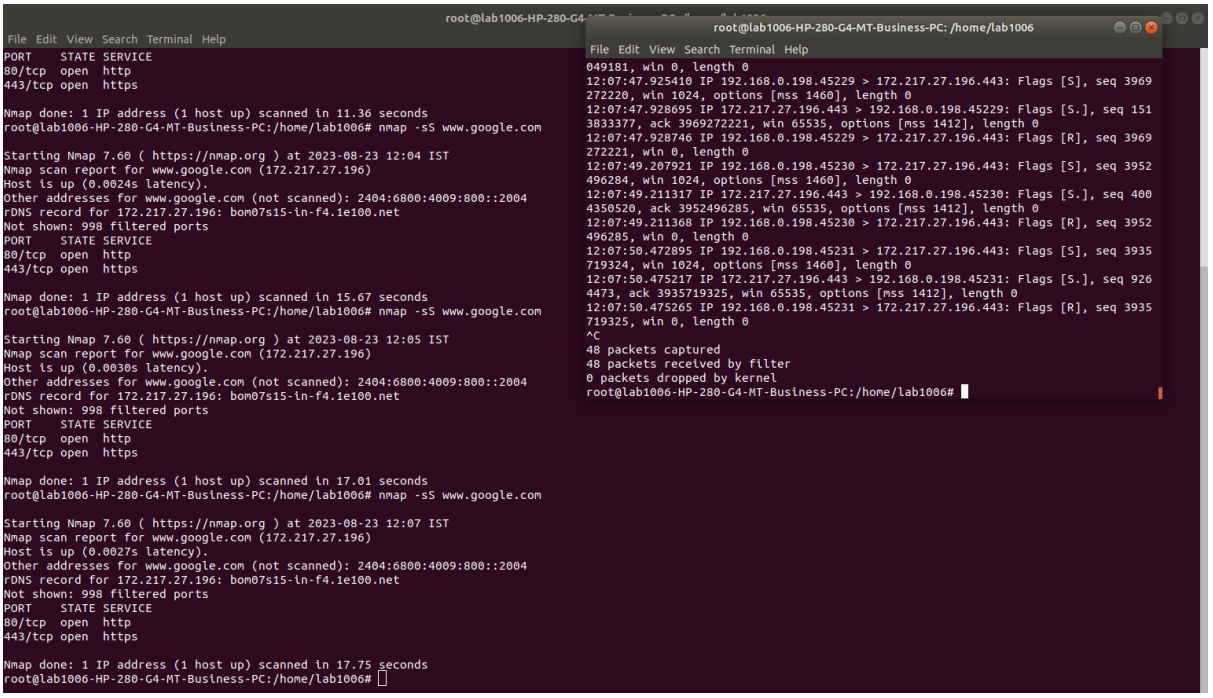
Roll no. : 53
Name: Shreya Kamath
Date: 12th September, 2023.

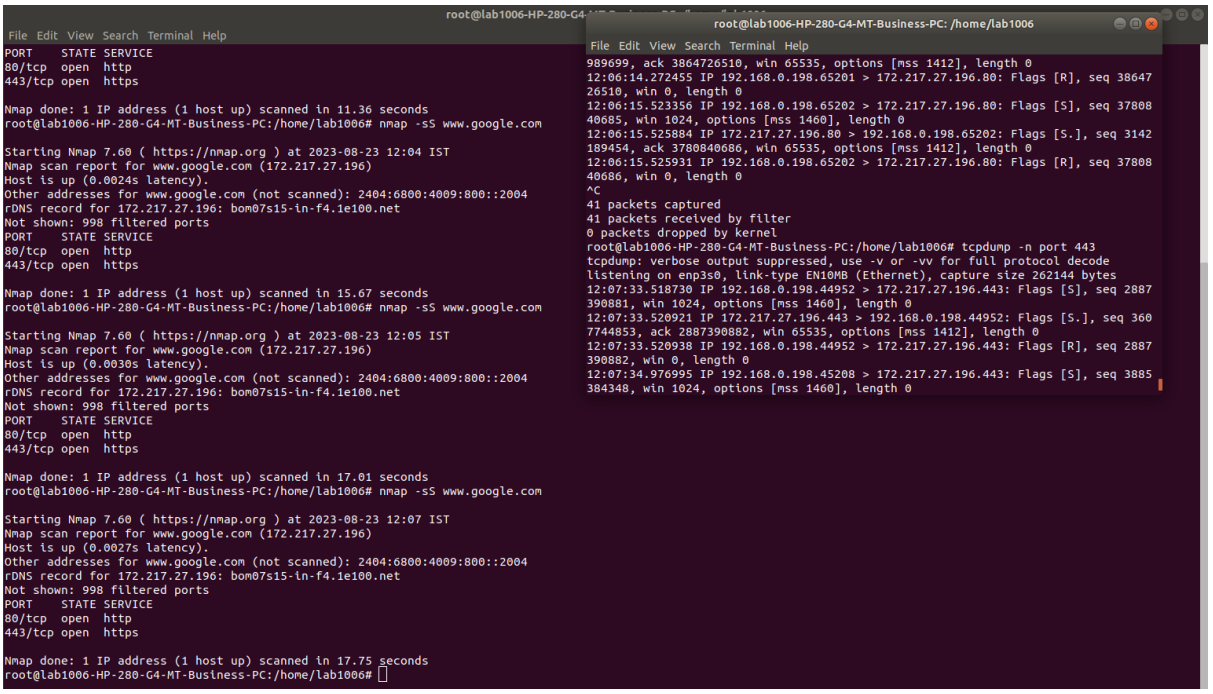
```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ man nmap
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ nmap -sS
You requested a scan type which requires root privileges.
QUITTING!
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo su
[sudo] password for lab1006:
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# nmap -sS

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-23 11:59 IST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.07 seconds
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# nmap -sS www.wikipedia.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-23 12:00 IST

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

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-23 12:02 IST
Nmap scan report for www.google.com (172.217.27.196)
Host is up (0.0025s 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: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 11.36 seconds
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006#
```

```
File  Edit  View  Search  Terminal  Help
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 11.36 seconds
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# nmap -sS www.google.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-23 12:04 IST
Nmap scan report for www.google.com (172.217.27.196)
Host is up (0.0024s 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: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 15.67 seconds
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# nmap -sS www.google.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-23 12:05 IST
Nmap scan report for www.google.com (172.217.27.196)
Host is up (0.0030s 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: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 17.01 seconds
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006# nmap -sS www.google.com

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-23 12:07 IST
Nmap scan report for www.google.com (172.217.27.196)
Host is up (0.0027s 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: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 17.75 seconds
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006#
```

```
root@lab1006-HP-280-G4-MT-Business-PC: /home/lab1006
File  Edit  View  Search  Terminal  Help
049181, win 0, length 0
12:07:47.925410 IP 192.168.0.198.45229 > 172.217.27.196.443: Flags [S], seq 3969
272220, win 1024, options [mss 1460], length 0
12:07:47.928695 IP 172.217.27.196.443 > 192.168.0.198.45229: Flags [S.], seq 151
3833377, ack 3969272221, win 65535, options [mss 1412], length 0
12:07:47.928746 IP 192.168.0.198.45229 > 172.217.27.196.443: Flags [R], seq 3969
272221, win 0, length 0
12:07:49.207921 IP 192.168.0.198.45230 > 172.217.27.196.443: Flags [S], seq 3952
496284, win 1024, options [mss 1460], length 0
12:07:49.211317 IP 172.217.27.196.443 > 192.168.0.198.45230: Flags [S.], seq 400
4350520, ack 3952496285, win 65535, options [mss 1412], length 0
12:07:49.211368 IP 192.168.0.198.45230 > 172.217.27.196.443: Flags [R], seq 3952
496285, win 0, length 0
12:07:50.472895 IP 192.168.0.198.45231 > 172.217.27.196.443: Flags [S], seq 3935
719324, win 1024, options [mss 1460], length 0
12:07:50.475217 IP 172.217.27.196.443 > 192.168.0.198.45231: Flags [S.], seq 926
4473, ack 3935719325, win 65535, options [mss 1412], length 0
12:07:50.475265 IP 192.168.0.198.45231 > 172.217.27.196.443: Flags [R], seq 3935
719325, win 0, length 0
^C
48 packets captured
48 packets received by filter
0 packets dropped by kernel
root@lab1006-HP-280-G4-MT-Business-PC:/home/lab1006#
```

Roll no. : 53
Name: Shreya Kamath
Date: 12th September, 2023.





CONCLUSION:

Hence, I have understood the fundamental concepts and carried out installation of NMAP and used it with different options to scan open ports, perform OS fingerprinting, ping scan, TCP port scan, UDP port scan.