Roll No 06

Name – Prasad Sunil Arote

Date - 07/09/2023

Lab 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.

LO4: Use tools like sniffers, port scanners and other related tools for analyzing packets in a network.

THEORY:

Port Scanning:

Port scanning is a network reconnaissance technique used to discover open ports on a target system. It involves sending requests to various ports on a target computer to determine which ports are open, closed, or filtered. This information is valuable for both legitimate network administrators and malicious hackers as it helps identify services running on a system and potential vulnerabilities.

NMAP:

Nmap (Network Mapper) is a widely used open-source tool for network discovery and security auditing. It provides a variety of scanning techniques and options to probe networks and identify open ports, services, and operating systems.

Different States of Ports:

1. Open: The target system actively accepts connections on the specified port. This indicates that a service is running and listening on that port.
2. Closed: The target system actively rejects connections on the specified port. This means there's no service listening on that port.
3. Filtered: The target system actively drops incoming packets, making it difficult to determine whether the port is open or closed. Firewalls or security measures often cause this state.
4. Unfiltered: Nmap cannot determine whether the port is open or closed due to the lack of response from the target system. This state indicates a less common configuration.
5. Open | Filtered: Nmap cannot reliably determine whether the port is open or filtered. This state often occurs when firewalls are in place.
6. Closed | Filtered: Nmap cannot reliably determine whether the port is closed or filtered. This state is also often the result of firewalls.

Port Scanning Techniques using NMAP:

TCP Connect Scan:

Command: nmap -sT target

Explanation: This scan establishes a full TCP connection to each specified port. It actively opens a connection to each target port to check if it's open. This method is reliable but not as stealthy as other scans because it leaves a clear trace in the target's logs.

TCP SYN Scan:

Command: nmap -sS target

Explanation: The SYN scan, also known as a half-open scan, sends SYN packets to target ports. If a port is open, it responds with a SYN-ACK packet, allowing Nmap to determine that the port is open. If the port is closed, it responds with a RST packet. This scan is stealthier than a connect scan.

FIN Scan:

Command: nmap -sF target

Explanation: In a FIN scan, Nmap sends FIN packets to target ports. If a port is closed, it responds with a RST packet, indicating that the port is closed. However, if the port is open, it ignores the packet. This scan is used to identify open ports without triggering alarms.

Null Scan:

Command: nmap -sN target

Explanation: A null scan involves sending TCP packets with no flags set (i.e., all flags set to zero) to target ports. Similar to the FIN scan, if a port is closed, it responds with a RST packet, but if the port is open, it ignores the packet. This scan can help identify open ports while evading detection.

XMAS Scan:

Command: nmap -sX target

Explanation: An XMAS scan sends packets with the FIN, URG, and PSH flags set to target ports. Like the FIN and Null scans, if a port is closed, it responds with a RST packet. If open, it usually doesn't respond. This scan can help identify open ports in stealthy scenarios.

ACK Scan:

Command: nmap -sA target

Explanation: The ACK scan sends ACK packets to target ports. If a port is unfiltered and open, it will respond with an RST packet. However, if the port is filtered or closed, it typically won't respond. This scan is primarily used to identify firewall rules.

Ping Sweep:

Command: nmap -sn target

Explanation: A ping sweep is used to discover live hosts in a network by sending ICMP echo requests (ping) to multiple IP addresses within a specified range. It helps identify which hosts are online and reachable.

Service and Version Detection:

Command: nmap -sV target

Explanation: This scan detects the services running on open ports and attempts to determine their versions by analyzing the responses from those services. It helps in identifying specific software and their versions.

Port and Port Range Scanning:

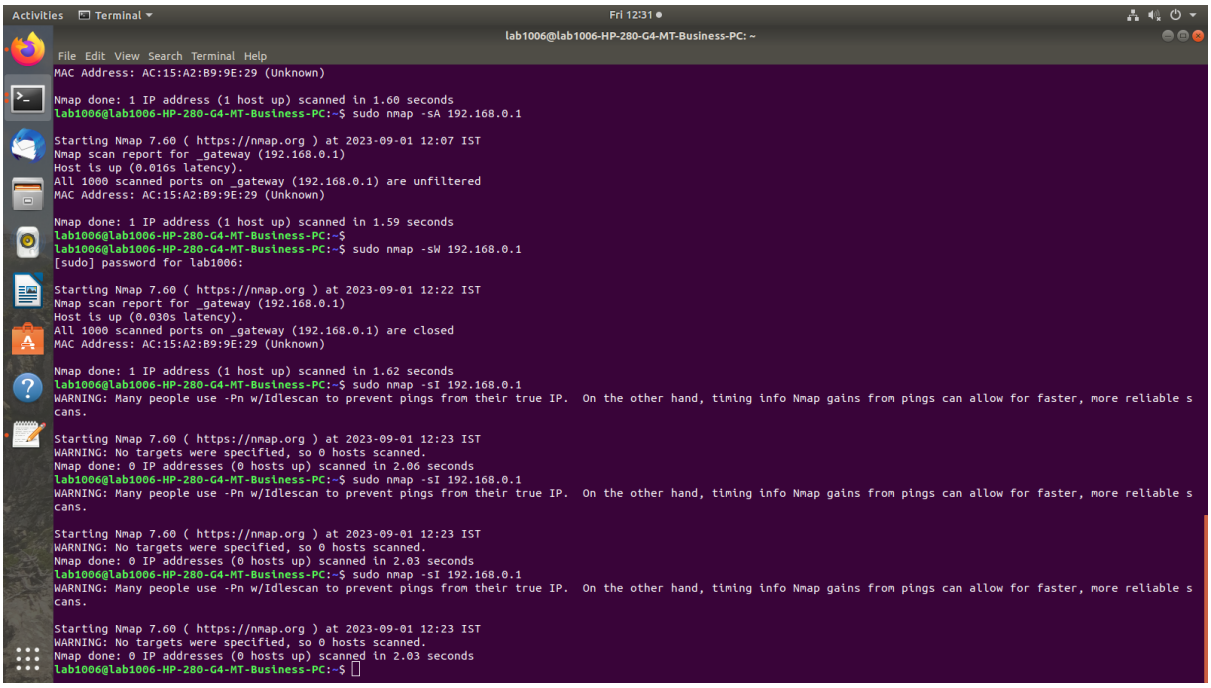
Command: nmap -p port(s) target

Explanation: You can use this command to specify specific ports or a range of ports to scan. For example, nmap -p 80,443 target scans only ports 80 and 443.

OS Fingerprinting:

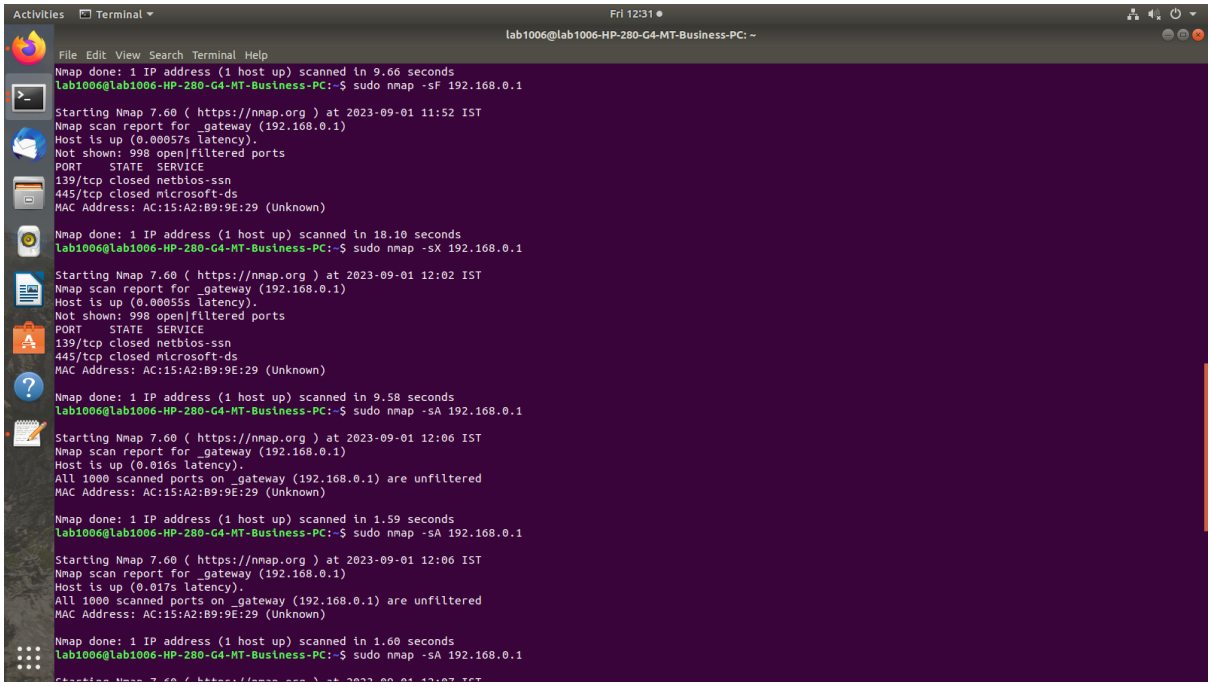
Command: nmap -O target

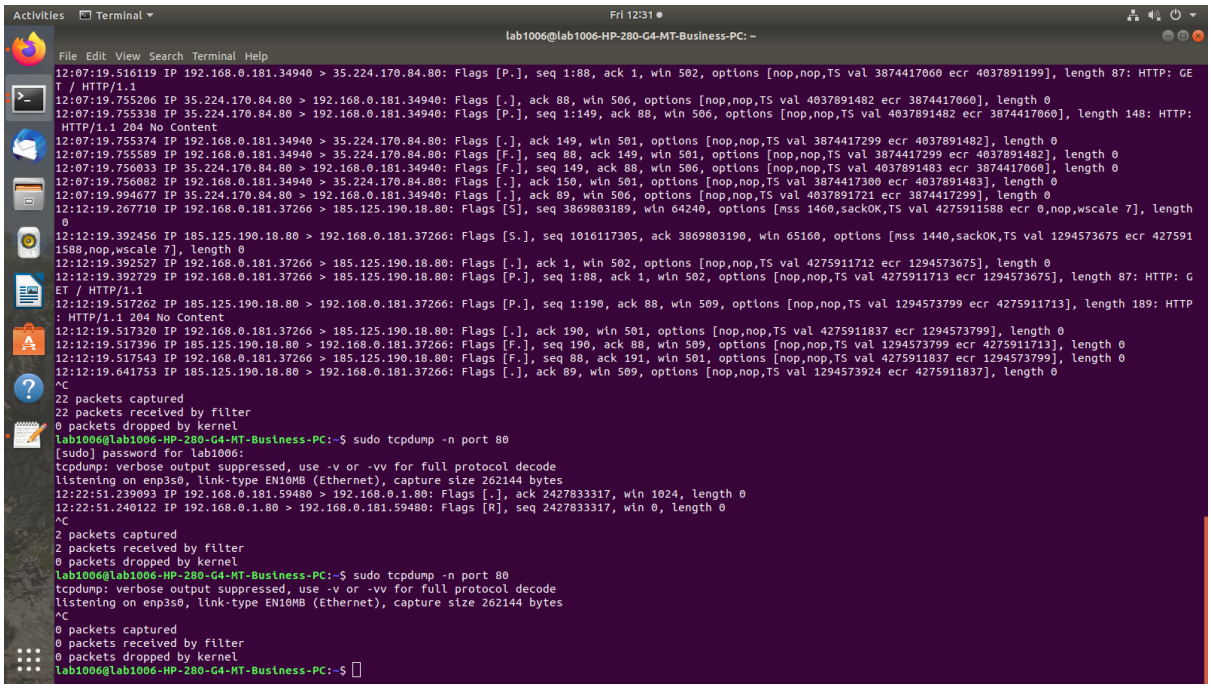
Explanation: This scan attempts to identify the operating system running on the target by analyzing various network responses and characteristics. Nmap compares these patterns to its database to make an educated guess about the OS.



```
MAC Address: AC:15:A2:B9:9E:29 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo nmap -sT 192.168.0.1

Starting Nmap 7.60 ( https://nmap.org ) at 2023-09-01 11:43 IST
Nmap scan report for _gateway (192.168.0.1)
Host is up (0.0074s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
443/tcp  open  https
1900/tcp open  upnp
MAC Address: AC:15:A2:B9:9E:29 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo nmap -sN 192.168.0.1

Starting Nmap 7.60 ( https://nmap.org ) at 2023-09-01 11:44 IST
Nmap scan report for _gateway (192.168.0.1)
Host is up (0.00054s latency).
Not shown: 998 open|filtered ports
PORT    STATE  SERVICE
139/tcp closed netbios-ssn
445/tcp closed microsoft-ds
MAC Address: AC:15:A2:B9:9E:29 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 5.84 seconds
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo nmap -sN 192.168.0.1

Starting Nmap 7.60 ( https://nmap.org ) at 2023-09-01 11:48 IST
Nmap scan report for _gateway (192.168.0.1)
Host is up (0.00056s latency).
Not shown: 998 open|filtered ports
PORT    STATE  SERVICE
139/tcp closed netbios-ssn
445/tcp closed microsoft-ds
MAC Address: AC:15:A2:B9:9E:29 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 9.66 seconds
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo nmap -sF 192.168.0.1

Starting Nmap 7.60 ( https://nmap.org ) at 2023-09-01 11:52 IST
Nmap scan report for _gateway (192.168.0.1)
```

```
0 packets dropped by kernel
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo tcpdump -n port 445
[sudo] password for lab1006:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
12:06:51.203178 IP 192.168.0.181.61140 > 192.168.0.1.445: Flags [.], ack 764217825, win 1024, length 0
12:06:51.204633 IP 192.168.0.1.445 > 192.168.0.181.61140: Flags [R], seq 764217825, win 0, length 0
^C
2 packets captured
2 packets received by filter
0 packets dropped by kernel
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo tcpdump -n port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
12:07:09.081766 IP 192.168.0.181.45849 > 192.168.0.1.80: Flags [.], ack 2996676280, win 1024, length 0
12:07:09.082405 IP 192.168.0.1.80 > 192.168.0.181.45849: Flags [R], seq 2996676280, win 0, length 0
12:07:19.275767 IP 192.168.0.181.34940 > 35.224.170.84.80: Flags [S], seq 1279895593, win 64240, options [mss 1460,sackOK,TS val 3874416820 ecr 0,nop,wscale 7], length
0
12:07:19.515835 IP 35.224.170.84.80 > 192.168.0.181.34940: Flags [S.], seq 1946168769, ack 1279895594, win 64768, options [mss 1420,sackOK,TS val 4037891199 ecr 3874416
820,nop,wscale 7], length 0
12:07:19.515903 IP 192.168.0.181.34940 > 35.224.170.84.80: Flags [.], ack 1, win 502, options [nop,nop,TS val 3874417060 ecr 4037891199], length 0
12:07:19.516119 IP 192.168.0.181.34940 > 35.224.170.84.80: Flags [P.], seq 1:88, ack 1, win 502, options [nop,nop,TS val 3874417060 ecr 4037891199], length 87: HTTP: GE
T / HTTP/1.1
12:07:19.755206 IP 35.224.170.84.80 > 192.168.0.181.34940: Flags [.], ack 88, win 506, options [nop,nop,TS val 4037891482 ecr 3874417060], length 0
12:07:19.755338 IP 35.224.170.84.80 > 192.168.0.181.34940: Flags [P.], seq 1:149, ack 88, win 506, options [nop,nop,TS val 4037891482 ecr 3874417060], length 148: HTTP:
 HTTP/1.1 204 No Content
12:07:19.755374 IP 192.168.0.181.34940 > 35.224.170.84.80: Flags [.], ack 149, win 501, options [nop,nop,TS val 3874417299 ecr 4037891482], length 0
12:07:19.755589 IP 192.168.0.181.34940 > 35.224.170.84.80: Flags [F.], seq 88, ack 149, win 501, options [nop,nop,TS val 3874417299 ecr 4037891482], length 0
12:07:19.756033 IP 35.224.170.84.80 > 192.168.0.181.34940: Flags [F.], seq 149, ack 88, win 506, options [nop,nop,TS val 4037891483 ecr 3874417060], length 0
12:07:19.756082 IP 192.168.0.181.34940 > 35.224.170.84.80: Flags [.], ack 150, win 501, options [nop,nop,TS val 3874417300 ecr 4037891483], length 0
12:07:19.994677 IP 35.224.170.84.80 > 192.168.0.181.34940: Flags [.], ack 89, win 506, options [nop,nop,TS val 4037891721 ecr 3874417299], length 0
12:12:19.267710 IP 192.168.0.181.37266 > 185.125.190.18.80: Flags [S], seq 3869803189, win 64240, options [mss 1460,sackOK,TS val 4275911588 ecr 0,nop,wscale 7], length
 0
12:12:19.392456 IP 185.125.190.18.80 > 192.168.0.181.37266: Flags [S.], seq 1016117305, ack 3869803190, win 65160, options [mss 1440,sackOK,TS val 1294573675 ecr 427591
1588,nop,wscale 7], length 0
12:12:19.392527 IP 192.168.0.181.37266 > 185.125.190.18.80: Flags [.], ack 1, win 502, options [nop,nop,TS val 4275911712 ecr 1294573675], length 0
12:12:19.392729 IP 192.168.0.181.37266 > 185.125.190.18.80: Flags [P.], seq 1:88, ack 1, win 502, options [nop,nop,TS val 4275911713 ecr 1294573675], length 87: HTTP: G
ET / HTTP/1.1
12:12:19.517262 IP 185.125.190.18.80 > 192.168.0.181.37266: Flags [P.], seq 1:190, ack 88, win 509, options [nop,nop,TS val 1294573799 ecr 4275911713], length 189: HTTP
: HTTP/1.1 204 No Content
12:12:19.517320 IP 192.168.0.181.37266 > 185.125.190.18.80: Flags [.], ack 190, win 501, options [nop,nop,TS val 4275911837 ecr 1294573799], length 0
12:12:19.517396 IP 185.125.190.18.80 > 192.168.0.181.37266: Flags [F.], seq 190, ack 88, win 509, options [nop,nop,TS val 1294573799 ecr 4275911713], length 0
12:12:19.517543 IP 192.168.0.181.37266 > 185.125.190.18.80: Flags [F.], seq 88, ack 191, win 501, options [nop,nop,TS val 4275911837 ecr 1294573799], length 0
12:12:19.641753 IP 185.125.190.18.80 > 192.168.0.181.37266: Flags [.], ack 89, win 509, options [nop,nop,TS val 1294573924 ecr 4275911837], length 0
^C
```





Conclusion:

Port scanning is a crucial technique for network reconnaissance, helping administrators identify security weaknesses and ensuring proper configuration. Nmap provides a comprehensive set of scanning options for various scenarios, from identifying open ports to determining service versions and even fingerprinting the target's operating system. However, it's important to use these tools and techniques responsibly and with proper authorization, as unauthorized scanning can be considered malicious and illegal.