Roll Number:- 2105048
Name:-Manav Jain
Date:- 13/09/2023

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 :- LO4

Theory:-

1. What is port scanning ? What is Nmap?

Port scanning is a crucial technique in the realm of networking and cybersecurity. It involves probing a host or network to discover open ports, which act as gateways for network services or applications. These ports are the entry points through which data flows in and out of a system.

Each port is associated with a specific protocol and service, making them essential for communication within a network. The primary purpose of port scanning is to unveil the network landscape, assess the security posture of a system, and identify potential vulnerabilities or attack vectors. Network administrators use it for troubleshooting and monitoring network health, while security professionals use it to detect and mitigate security threats.

However, malicious actors also leverage port scanning to identify vulnerable targets for cyberattacks.Nmap, short for "Network Mapper," is a versatile and widely used open-source tool for network discovery and security auditing. Developed by Gordon Lyon, also known as Fyodor, Nmap has earned a reputation

as the go-to tool for port scanning due to its comprehensive feature set and cross-platform compatibility. Nmap's capabilities extend beyond basic port scanning.

It can perform a wide range of tasks, including host discovery, service and version detection, operating system fingerprinting, and scripting for automation. Nmap is favored by security professionals, network administrators, and ethical hackers for its flexibility and accuracy

2. Explain in brief different states of port.

Ports are essential components of network communication, and they can exist in various states, each conveying specific information about their accessibility and functionality. Understanding these port states is crucial for network administrators and security professionals. Here are brief explanations of different port states:

1. **Open:** An "open" port is one that is actively listening for incoming connections. It indicates that a network service or application is running and ready to accept data or requests. Open ports are crucial for legitimate network communication.

2. **Closed:** A "closed" port is one that is not actively listening for connections. It means there is no service or application running on that port. Closed ports are safe from unauthorized access, but they still indicate the presence of a host.

3. **Filtered:** A "filtered" port is one that cannot be determined as open or closed with certainty. This state often occurs when a firewall, intrusion detection system (IDS), or other security measure blocks incoming requests to the port. It makes it challenging to discern the actual status of the port.

4. **Unfiltered:** An "unfiltered" port is one that is accessible and can be reached, but its status (open or closed) remains undetermined. Unfiltered ports usually indicate that no significant firewall rules are blocking access to the port.

5. **Open | Filtered:** This state combines characteristics of both open and filtered ports. It suggests that the port is reachable, but the response to a probing request is filtered, possibly by a firewall. It can be challenging to ascertain the exact state of such ports.

6. **Closed | Filtered:** This state also combines characteristics of both closed and filtered ports. It implies that the port is accessible, but the response is filtered, typically indicating that a firewall is blocking probing attempts. This state can be confusing during port scanning.

Write the commands for following type of port scanning techniques using NMAP, Explain in 4 to 5 lines how each of them works.

Port scanning is an integral part of network reconnaissance, allowing us to discover open ports on target hosts and gain insights into their configuration and potential vulnerabilities. Nmap (Network Mapper) is a versatile tool that offers various scanning techniques to achieve this.

1. TCP Connect Scan Command: `nmap -sT target`

Description: This scan emulates a full TCP connection attempt to each target port. If a connection is successfully established, the port is considered open. It's the most straightforward scanning method, but it can be easily detected by intrusion detection systems (IDS) and firewalls because it fully completes the TCP handshake.

2. TCP SYN Scan Command: `nmap -sS target`

Description: The TCP SYN scan, also known as the "half-open" scan, is stealthier than the TCP Connect scan. It sends SYN (Synchronize) packets to target ports and examines their responses. If a port responds with a SYN-ACK (Synchronize-Acknowledgment) packet, it's considered open. If it responds with an RST (Reset) packet, it's considered closed. This scan doesn't complete the full TCP handshake, making it less likely to trigger alarms.

3. FIN Scan Command: `nmap -sF target`

Description: The FIN scan sends FIN (Finish) packets to target ports. If a port is closed, it should respond with an RST packet. If it's open, it should ignore the FIN packet. This scan is effective for identifying systems with non-standard TCP stack implementations.

4. Null Scan Command: `nmap -sN target`

Description: Similar to the FIN scan, the Null scan sends packets with no TCP flags set, making them appear "null." If a port is closed, it should respond with an RST packet. If it's open, it should ignore the packet. This technique is stealthy and can bypass some firewall rules.

5. XMAS Scan Command: `nmap -sX target`

Description: The XMAS scan sets multiple TCP flags in the packet, making it look like a Christmas tree. If a port is closed, it should respond with an RST packet. If it's open, it should ignore the packet. Like the Null scan, this method can bypass firewall rules.

6. ACK Scan Command: `nmap -sA target`

Description: The ACK scan sends ACK (Acknowledgment) packets to target ports. It can be used to determine if a firewall is in place; open ports will typically respond with an RST packet, while filtered ports may not respond at all. This scan can identify packet-filtering firewalls.

7. Ping Sweep Command: `nmap -sn target_range`

Description: Ping sweeping is not a port scanning technique but is often used to identify live hosts before conducting port scans. It sends ICMP echo requests (pings) to a range of IP addresses and identifies responsive hosts, reducing unnecessary scanning on non-responsive Hosts.

8. Service and Version Detection Command: `nmap -sV target`

Description: Nmap can probe open ports to identify the services running on them and their versions. This information is crucial for understanding the potential attack surface and vulnerabilities.

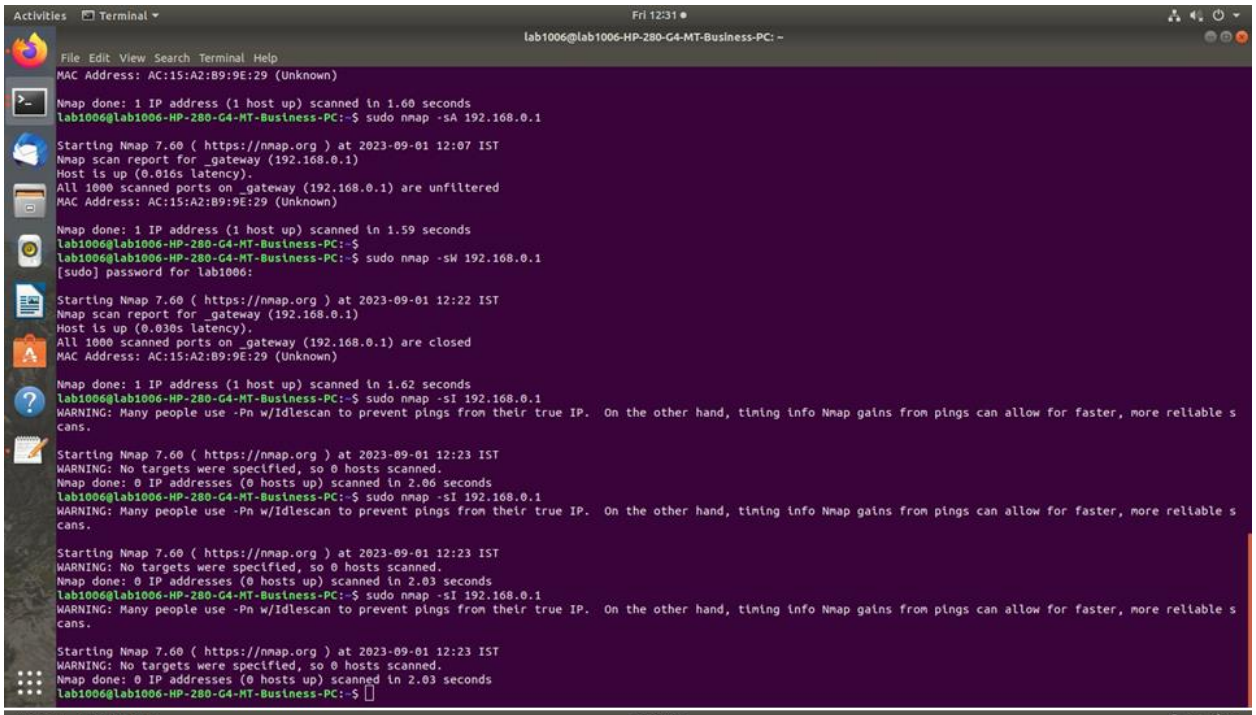
9. Port and Port Range Scanning Command: `nmap -p ports target`

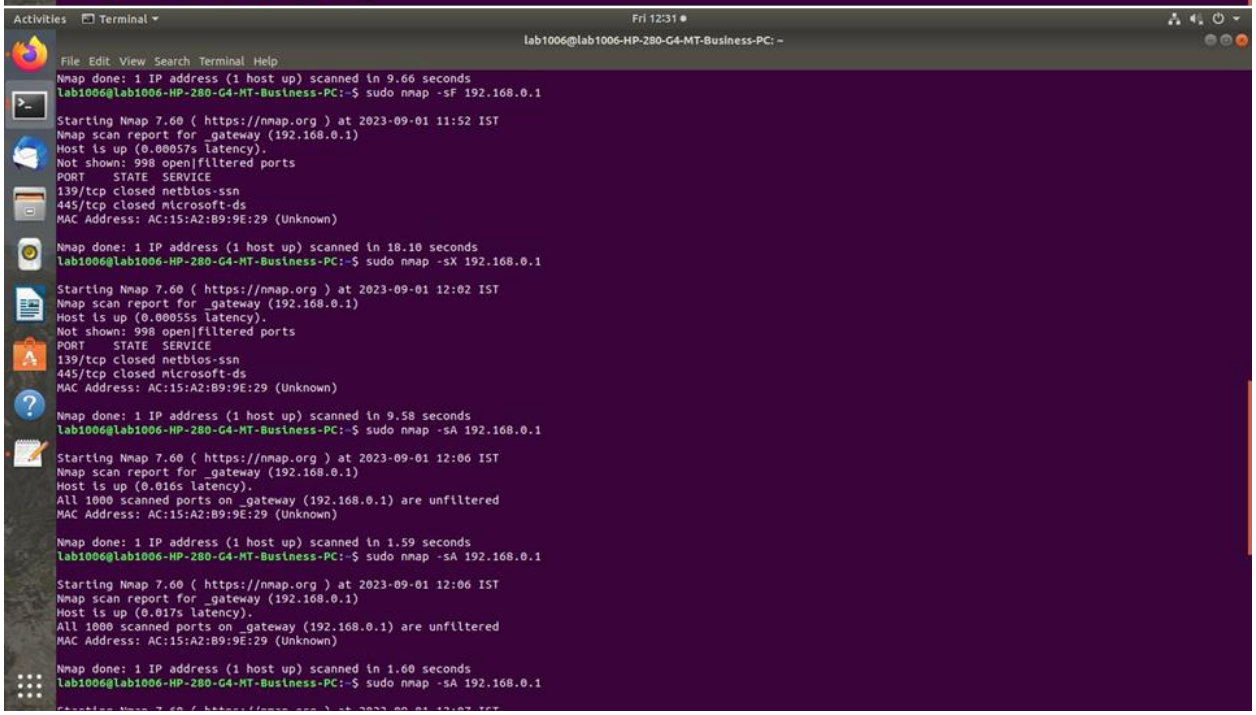
Description: Nmap allows users to specify individual ports or port ranges for scanning, giving flexibility in targeting specific services or performing broad scans of common ports.

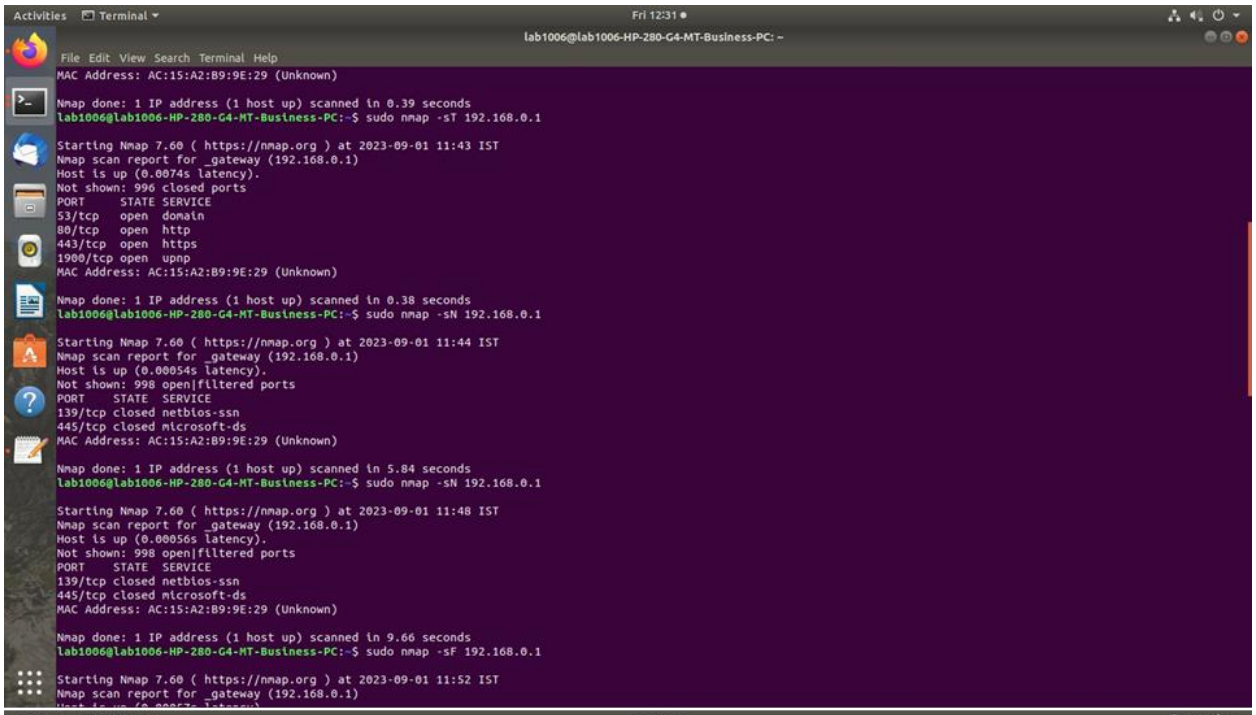
10. OS Fingerprinting Command: `nmap -O target`

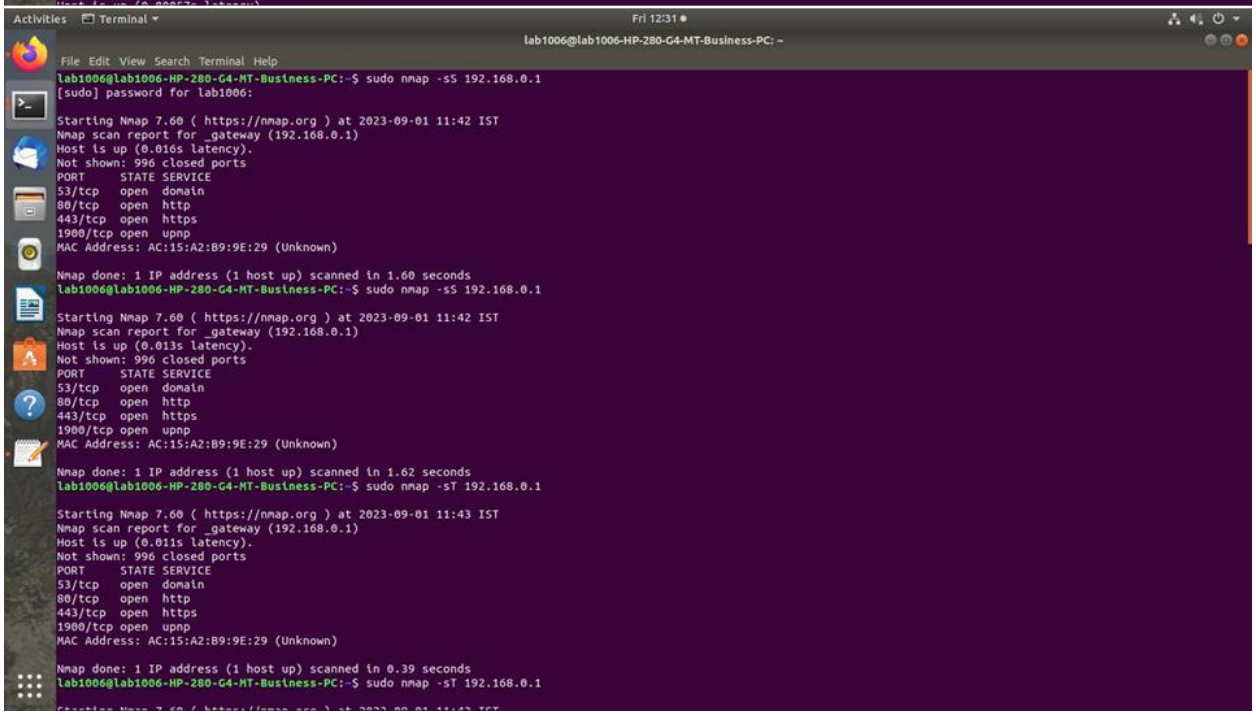
Description: Nmap can attempt to identify the operating system running on the target by analyzing network responses and characteristics. This information aids in understanding the target environment.

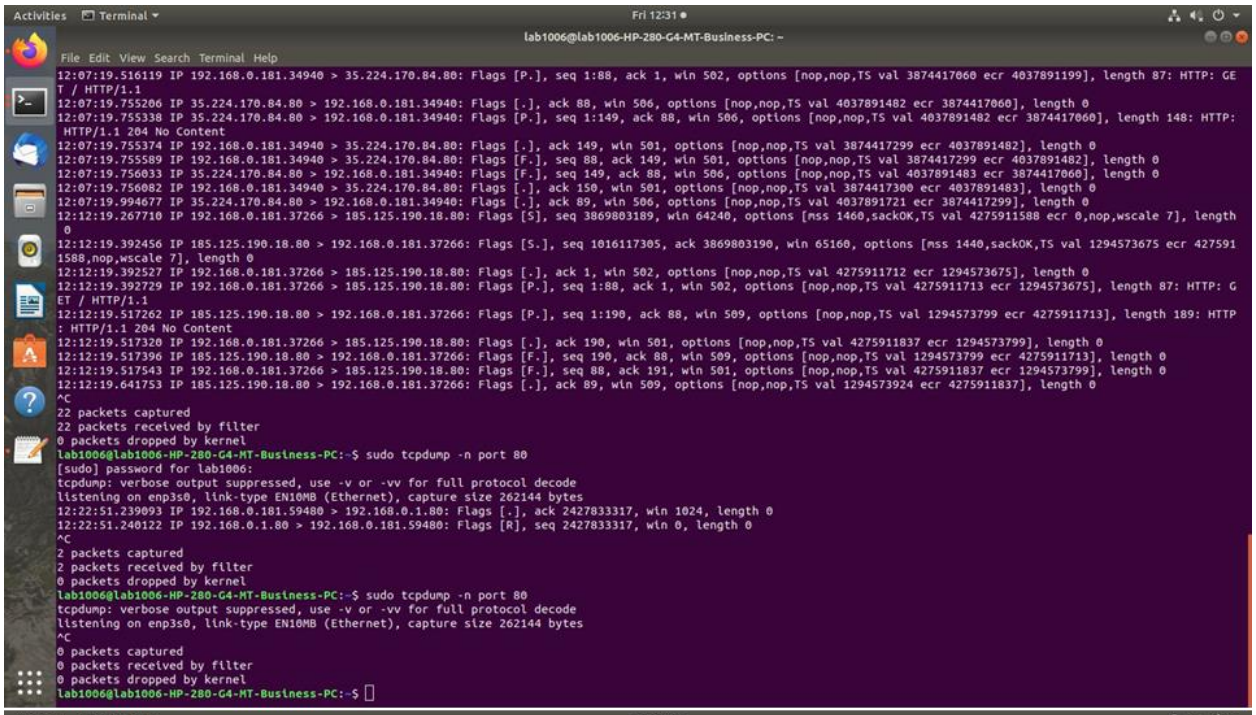
Output Screenshots:-

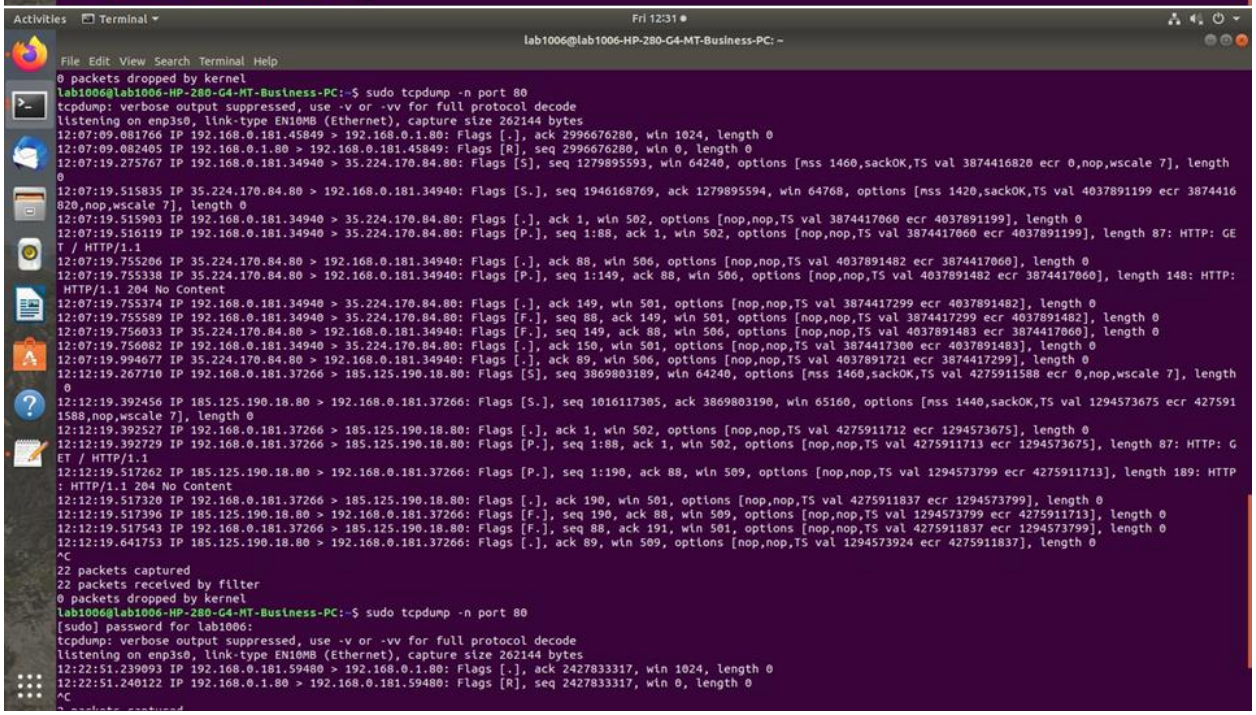

Activities
Terminal
Fri 12:31
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help
MAC Address: AC:15:A2:B9:9E:29 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 1.60 seconds
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo nmap -sA 192.168.0.1
Starting Nmap 7.60 (https://nmap.org) at 2023-09-01 12:07 IST
Nmap scan report for _gateway (192.168.0.1)
Host is up (0.016s latency).
All 1000 scanned ports on _gateway (192.168.0.1) are unfiltered
MAC Address: AC:15:A2:B9:9E:29 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 1.59 seconds
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo nmap -sW 192.168.0.1
[sudo] password for lab1006:
Starting Nmap 7.60 (https://nmap.org) at 2023-09-01 12:22 IST
Nmap scan report for _gateway (192.168.0.1)
Host is up (0.030s latency).
All 1000 scanned ports on _gateway (192.168.0.1) are closed
MAC Address: AC:15:A2:B9:9E:29 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 1.62 seconds
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo nmap -sI 192.168.0.1
WARNING: Many people use -Pn w/Idlescan to prevent pings from their true IP. On the other hand, timing info Nmap gains from pings can allow for faster, more reliable s
cans.
Starting Nmap 7.60 (https://nmap.org) at 2023-09-01 12:23 IST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 2.06 seconds
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo nmap -sI 192.168.0.1
WARNING: Many people use -Pn w/Idlescan to prevent pings from their true IP. On the other hand, timing info Nmap gains from pings can allow for faster, more reliable s
cans.
Starting Nmap 7.60 (https://nmap.org) at 2023-09-01 12:23 IST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 2.03 seconds
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo nmap -sI 192.168.0.1
WARNING: Many people use -Pn w/Idlescan to prevent pings from their true IP. On the other hand, timing info Nmap gains from pings can allow for faster, more reliable s
cans.
Starting Nmap 7.60 (https://nmap.org) at 2023-09-01 12:23 IST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 2.03 seconds
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$

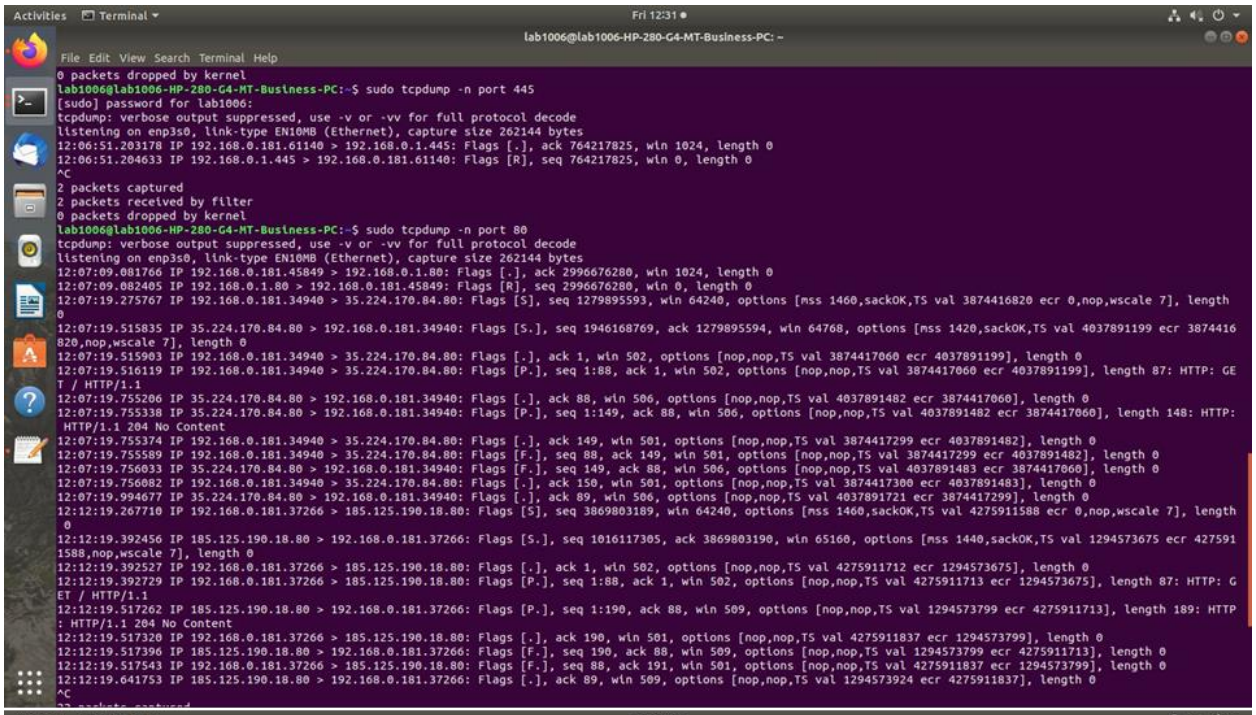

Activities
Terminal
Fri 12:31
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help
Nmap done: 1 IP address (1 host up) scanned in 9.66 seconds
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo nmap -sF 192.168.0.1
Starting Nmap 7.60 (https://nmap.org) at 2023-09-01 11:52 IST
Nmap scan report for _gateway (192.168.0.1)
Host is up (0.00057s 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 18.10 seconds
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo nmap -sX 192.168.0.1
Starting Nmap 7.60 (https://nmap.org) at 2023-09-01 12:02 IST
Nmap scan report for _gateway (192.168.0.1)
Host is up (0.00055s 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 9.58 seconds
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo nmap -sA 192.168.0.1
Starting Nmap 7.60 (https://nmap.org) at 2023-09-01 12:06 IST
Nmap scan report for _gateway (192.168.0.1)
Host is up (0.016s latency).
All 1000 scanned ports on _gateway (192.168.0.1) are unfiltered
MAC Address: AC:15:A2:B9:9E:29 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 1.59 seconds
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo nmap -sA 192.168.0.1
Starting Nmap 7.60 (https://nmap.org) at 2023-09-01 12:06 IST
Nmap scan report for _gateway (192.168.0.1)
Host is up (0.017s latency).
All 1000 scanned ports on _gateway (192.168.0.1) are unfiltered
MAC Address: AC:15:A2:B9:9E:29 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 1.60 seconds
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo nmap -sA 192.168.0.1

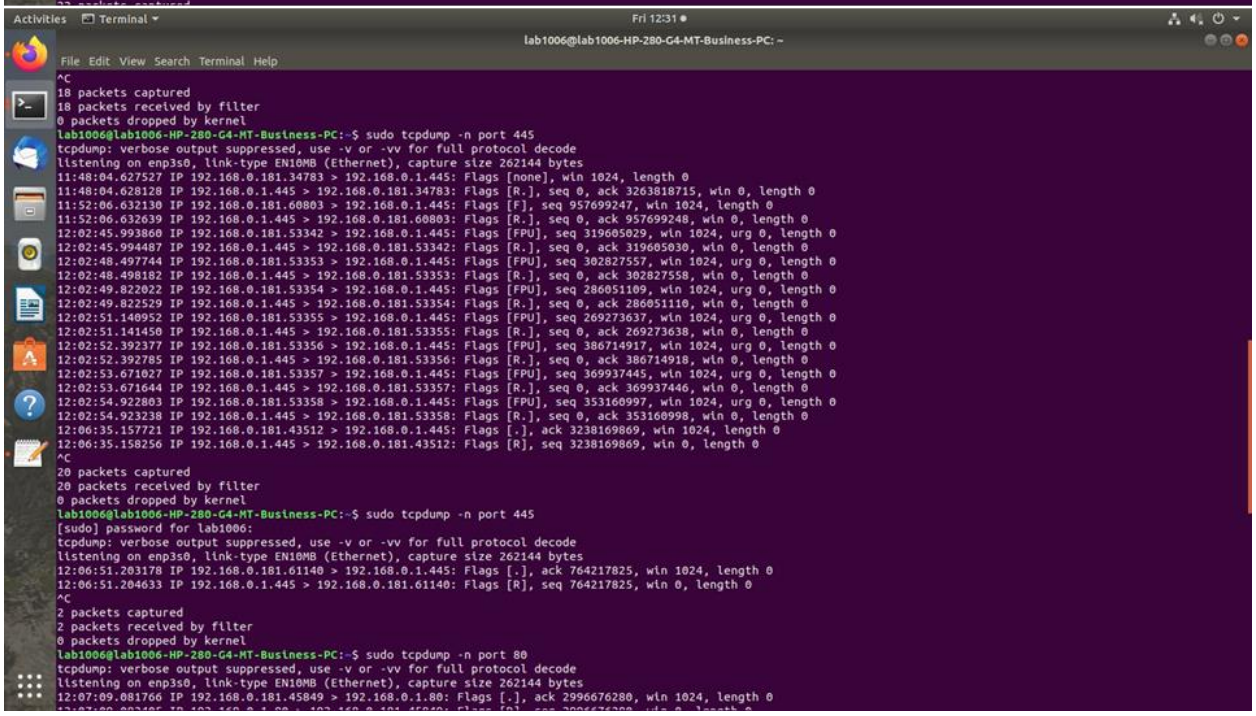

Activities
Terminal
Fri 12:31
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help
MAC Address: AC:15:A2:B9:9E:29 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo nmap -sT 192.168.0.1
Starting Nmap 7.60 (https://nmap.org) 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)

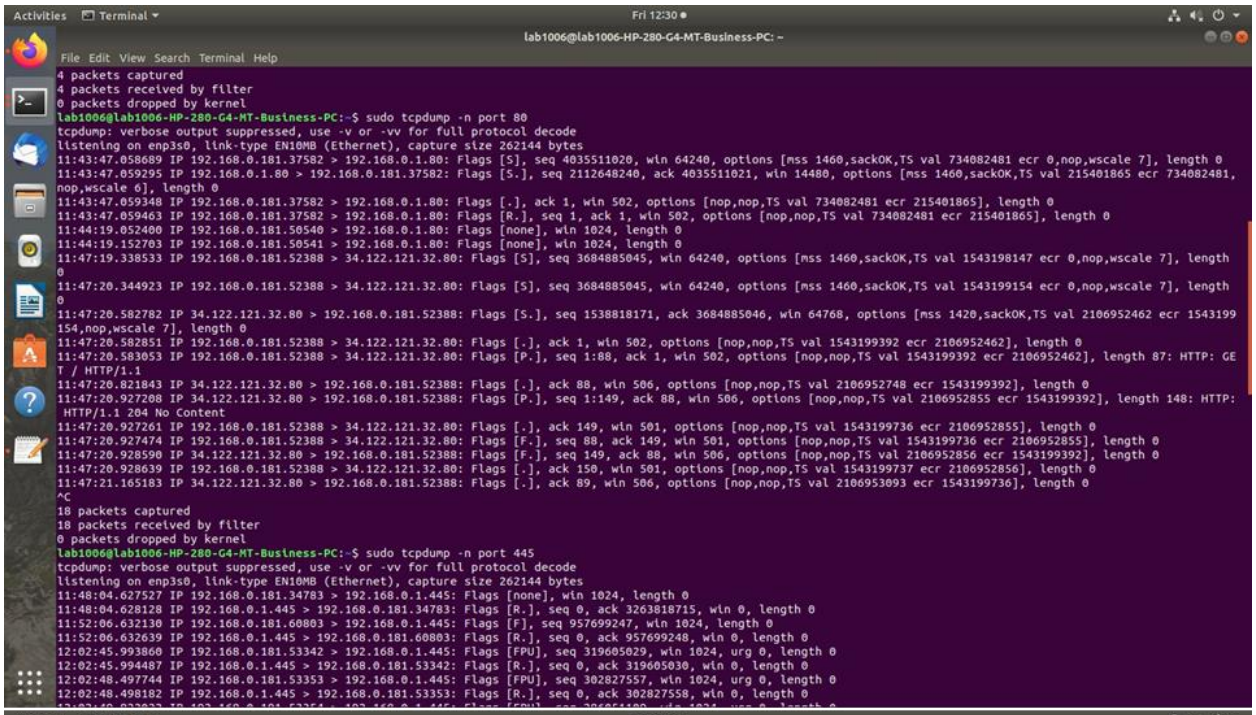

Activities
Terminal
Fri 12:31
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo nmap -sS 192.168.0.1
[sudo] password for lab1006:
Starting Nmap 7.60 (https://nmap.org) at 2023-09-01 11:42 IST
Nmap scan report for _gateway (192.168.0.1)
Host is up (0.016s 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 1.60 seconds
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo nmap -sS 192.168.0.1
Starting Nmap 7.60 (https://nmap.org) at 2023-09-01 11:42 IST
Nmap scan report for _gateway (192.168.0.1)
Host is up (0.013s 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 1.62 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 (0.011s 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 0.39 seconds
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo nmap -sT 192.168.0.1

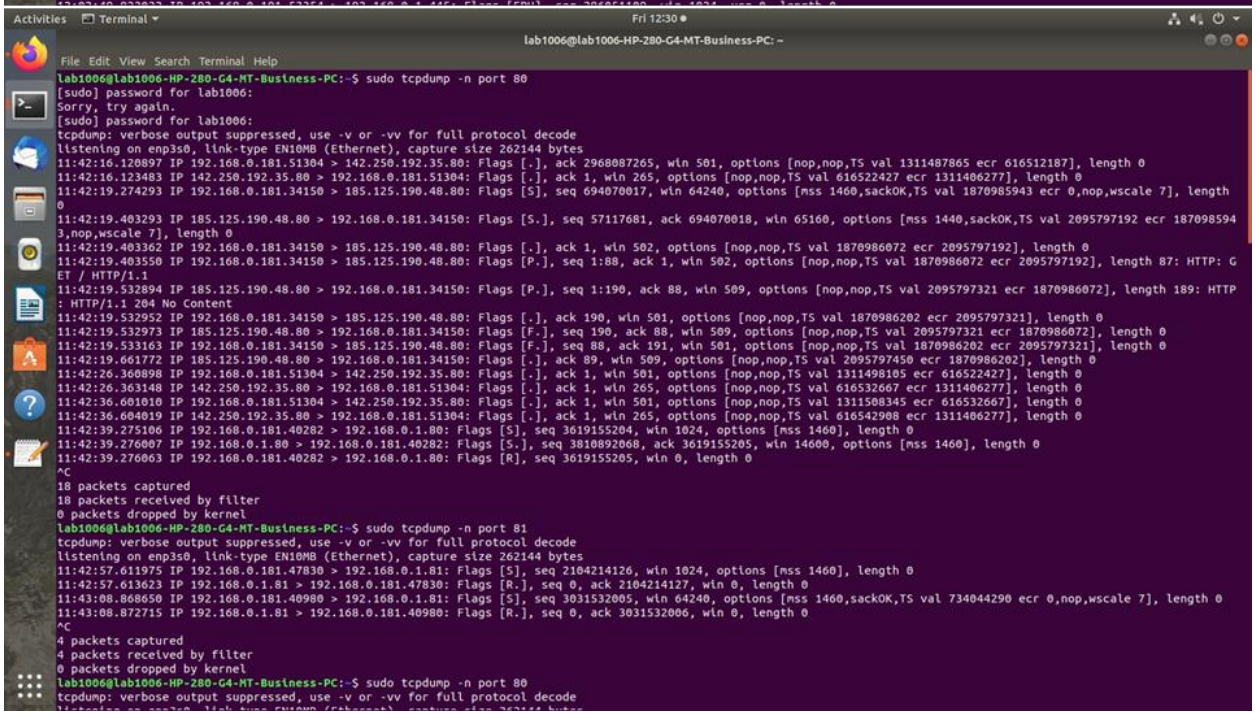

Activities
Terminal
Fri 12:31
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help
12:07:19.516119 IP 192.168.0.181.34940 > 35.224.170.84.80: Flags [P.], seq 1:88, ack 1, win 502, options [nop,nop,TS val 3874417060 ecr 4037891199], length 87: HTTP: GE
T / HTTP/1.1
12:07:19.755206 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
22 packets captured
22 packets received by filter
0 packets dropped by kernel
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo tcpdump -n port 80
[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
12:22:51.239093 IP 192.168.0.181.59480 > 192.168.0.1.80: Flags [.], ack 2427833317, win 1024, length 0
12:22:51.240122 IP 192.168.0.1.80 > 192.168.0.181.59480: Flags [R], seq 2427833317, 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
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$


Activities
Terminal
Fri 12:31
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help
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
22 packets captured
22 packets received by filter
0 packets dropped by kernel
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo tcpdump -n port 80
[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
12:22:51.239093 IP 192.168.0.181.59480 > 192.168.0.1.80: Flags [.], ack 2427833317, win 1024, length 0
12:22:51.240122 IP 192.168.0.1.80 > 192.168.0.181.59480: Flags [R], seq 2427833317, win 0, length 0
^C


Activities
Terminal
Fri 12:31
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help
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 3874416820,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: GET / 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 4275911588,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: GET / 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


Activities
Terminal
Fri 12:31
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help
^C
18 packets captured
18 packets received by filter
0 packets dropped by kernel
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo tcpdump -n port 445
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
11:48:04.627527 IP 192.168.0.181.34783 > 192.168.0.1.445: Flags [none], win 1024, length 0
11:48:04.628128 IP 192.168.0.1.445 > 192.168.0.181.34783: Flags [R.], seq 0, ack 3263818715, win 0, length 0
11:52:06.632130 IP 192.168.0.181.60803 > 192.168.0.1.445: Flags [F], seq 957699247, win 1024, length 0
11:52:06.632639 IP 192.168.0.1.445 > 192.168.0.181.60803: Flags [R.], seq 0, ack 957699248, win 0, length 0
12:02:45.993860 IP 192.168.0.181.53342 > 192.168.0.1.445: Flags [FPU], seq 319605029, win 1024, urg 0, length 0
12:02:45.994487 IP 192.168.0.1.445 > 192.168.0.181.53342: Flags [R.], seq 0, ack 319605030, win 0, length 0
12:02:48.497744 IP 192.168.0.181.53353 > 192.168.0.1.445: Flags [FPU], seq 302827557, win 1024, urg 0, length 0
12:02:48.498182 IP 192.168.0.1.445 > 192.168.0.181.53353: Flags [R.], seq 0, ack 302827558, win 0, length 0
12:02:49.822022 IP 192.168.0.181.53354 > 192.168.0.1.445: Flags [FPU], seq 286051109, win 1024, urg 0, length 0
12:02:49.822529 IP 192.168.0.1.445 > 192.168.0.181.53354: Flags [R.], seq 0, ack 286051110, win 0, length 0
12:02:51.140952 IP 192.168.0.181.53355 > 192.168.0.1.445: Flags [FPU], seq 269273637, win 1024, urg 0, length 0
12:02:51.141450 IP 192.168.0.1.445 > 192.168.0.181.53355: Flags [R.], seq 0, ack 269273638, win 0, length 0
12:02:52.392377 IP 192.168.0.181.53356 > 192.168.0.1.445: Flags [FPU], seq 386714917, win 1024, urg 0, length 0
12:02:52.392785 IP 192.168.0.1.445 > 192.168.0.181.53356: Flags [R.], seq 0, ack 386714918, win 0, length 0
12:02:53.671027 IP 192.168.0.181.53357 > 192.168.0.1.445: Flags [FPU], seq 369937445, win 1024, urg 0, length 0
12:02:53.671644 IP 192.168.0.1.445 > 192.168.0.181.53357: Flags [R.], seq 0, ack 369937446, win 0, length 0
12:02:54.922803 IP 192.168.0.181.53358 > 192.168.0.1.445: Flags [FPU], seq 353160997, win 1024, urg 0, length 0
12:02:54.923238 IP 192.168.0.1.445 > 192.168.0.181.53358: Flags [R.], seq 0, ack 353160998, win 0, length 0
12:06:35.157721 IP 192.168.0.181.43512 > 192.168.0.1.445: Flags [.], ack 3238169869, win 1024, length 0
12:06:35.158256 IP 192.168.0.1.445 > 192.168.0.181.43512: Flags [R], seq 3238169869, win 0, length 0
^C
20 packets captured
20 packets received by filter
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


Activities
Terminal
Fri 12:30
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help
4 packets captured
4 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
11:43:47.058689 IP 192.168.0.181.37582 > 192.168.0.1.80: Flags [S], seq 4035511020, win 64240, options [mss 1460,sackOK,TS val 734082481 ecr 0,nop,wscale 7], length 0
11:43:47.059295 IP 192.168.0.1.80 > 192.168.0.181.37582: Flags [S.], seq 2112648240, ack 4035511021, win 14480, options [mss 1460,sackOK,TS val 215401865 ecr 734082481,
nop,wscale 6], length 0
11:43:47.059348 IP 192.168.0.181.37582 > 192.168.0.1.80: Flags [.], ack 1, win 502, options [nop,nop,TS val 734082481 ecr 215401865], length 0
11:43:47.059463 IP 192.168.0.181.37582 > 192.168.0.1.80: Flags [R.], seq 1, ack 1, win 502, options [nop,nop,TS val 734082481 ecr 215401865], length 0
11:44:19.052400 IP 192.168.0.181.50540 > 192.168.0.1.80: Flags [none], win 1024, length 0
11:44:19.152703 IP 192.168.0.181.50541 > 192.168.0.1.80: Flags [none], win 1024, length 0
11:47:19.338533 IP 192.168.0.181.52388 > 34.122.121.32.80: Flags [S], seq 3684885045, win 64240, options [mss 1460,sackOK,TS val 1543198147 ecr 0,nop,wscale 7], length
0
11:47:20.344923 IP 192.168.0.181.52388 > 34.122.121.32.80: Flags [S], seq 3684885045, win 64240, options [mss 1460,sackOK,TS val 1543199154 ecr 0,nop,wscale 7], length
0
11:47:20.582782 IP 34.122.121.32.80 > 192.168.0.181.52388: Flags [S.], seq 1538818171, ack 3684885046, win 64768, options [mss 1420,sackOK,TS val 2106952462 ecr 1543199
154,nop,wscale 7], length 0
11:47:20.582851 IP 192.168.0.181.52388 > 34.122.121.32.80: Flags [.], ack 1, win 502, options [nop,nop,TS val 1543199392 ecr 2106952462], length 0
11:47:20.583053 IP 192.168.0.181.52388 > 34.122.121.32.80: Flags [P.], seq 1:88, ack 1, win 502, options [nop,nop,TS val 1543199392 ecr 2106952462], length 87: HTTP: GE
T / HTTP/1.1
11:47:20.821843 IP 34.122.121.32.80 > 192.168.0.181.52388: Flags [.], ack 88, win 506, options [nop,nop,TS val 2106952748 ecr 1543199392], length 0
11:47:20.927208 IP 34.122.121.32.80 > 192.168.0.181.52388: Flags [P.], seq 1:149, ack 88, win 506, options [nop,nop,TS val 2106952855 ecr 1543199392], length 148: HTTP:
 HTTP/1.1 204 No Content
11:47:20.927261 IP 192.168.0.181.52388 > 34.122.121.32.80: Flags [.], ack 149, win 501, options [nop,nop,TS val 1543199736 ecr 2106952855], length 0
11:47:20.927474 IP 192.168.0.181.52388 > 34.122.121.32.80: Flags [F.], seq 88, ack 149, win 501, options [nop,nop,TS val 1543199736 ecr 2106952855], length 0
11:47:20.928590 IP 34.122.121.32.80 > 192.168.0.181.52388: Flags [F.], seq 149, ack 88, win 506, options [nop,nop,TS val 2106952856 ecr 1543199392], length 0
11:47:20.928639 IP 192.168.0.181.52388 > 34.122.121.32.80: Flags [.], ack 150, win 501, options [nop,nop,TS val 1543199737 ecr 2106952856], length 0
11:47:21.165183 IP 34.122.121.32.80 > 192.168.0.181.52388: Flags [.], ack 89, win 506, options [nop,nop,TS val 2106953093 ecr 1543199736], length 0
^C
18 packets captured
18 packets received by filter
0 packets dropped by kernel
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo tcpdump -n port 445
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
11:48:04.627527 IP 192.168.0.181.34783 > 192.168.0.1.445: Flags [none], win 1024, length 0
11:48:04.628128 IP 192.168.0.1.445 > 192.168.0.181.34783: Flags [R.], seq 0, ack 3263818715, win 0, length 0
11:52:06.632130 IP 192.168.0.181.60803 > 192.168.0.1.445: Flags [F], seq 957699247, win 1024, length 0
11:52:06.632639 IP 192.168.0.1.445 > 192.168.0.181.60803: Flags [R.], seq 0, ack 957699248, win 0, length 0
12:02:45.993860 IP 192.168.0.181.53342 > 192.168.0.1.445: Flags [FPU], seq 319605029, win 1024, urg 0, length 0
12:02:45.994487 IP 192.168.0.1.445 > 192.168.0.181.53342: Flags [R.], seq 0, ack 319605030, win 0, length 0
12:02:48.497744 IP 192.168.0.181.53353 > 192.168.0.1.445: Flags [FPU], seq 302827557, win 1024, urg 0, length 0
12:02:48.498182 IP 192.168.0.1.445 > 192.168.0.181.53353: Flags [R.], seq 0, ack 302827558, win 0, length 0


Activities
Terminal
Fri 12:30
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo tcpdump -n port 80
[sudo] password for lab1006:
Sorry, try again.
[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
11:42:16.120897 IP 192.168.0.181.51304 > 142.250.192.35.80: Flags [.], ack 2968087265, win 501, options [nop,nop,TS val 1311487865 ecr 616512187], length 0
11:42:16.123483 IP 142.250.192.35.80 > 192.168.0.181.51304: Flags [.], ack 1, win 265, options [nop,nop,TS val 616522427 ecr 1311406277], length 0
11:42:19.274293 IP 192.168.0.181.34150 > 185.125.190.48.80: Flags [S], seq 694070017, win 64240, options [mss 1460,sackOK,TS val 1870985943 ecr 0,nop,wscale 7], length
0
11:42:19.403293 IP 185.125.190.48.80 > 192.168.0.181.34150: Flags [S.], seq 57117681, ack 694070018, win 65160, options [mss 1440,sackOK,TS val 2095797192 ecr 187098594
3,nop,wscale 7], length 0
11:42:19.403362 IP 192.168.0.181.34150 > 185.125.190.48.80: Flags [.], ack 1, win 502, options [nop,nop,TS val 1870986072 ecr 2095797192], length 0
11:42:19.403550 IP 192.168.0.181.34150 > 185.125.190.48.80: Flags [P.], seq 1:88, ack 1, win 502, options [nop,nop,TS val 1870986072 ecr 2095797192], length 87: HTTP: G
ET / HTTP/1.1
11:42:19.532894 IP 185.125.190.48.80 > 192.168.0.181.34150: Flags [P.], seq 1:190, ack 88, win 509, options [nop,nop,TS val 2095797321 ecr 1870986072], length 189: HTTP
: HTTP/1.1 204 No Content
11:42:19.532952 IP 192.168.0.181.34150 > 185.125.190.48.80: Flags [.], ack 190, win 501, options [nop,nop,TS val 1870986202 ecr 2095797321], length 0
11:42:19.532973 IP 185.125.190.48.80 > 192.168.0.181.34150: Flags [F.], seq 190, ack 88, win 509, options [nop,nop,TS val 2095797321 ecr 1870986072], length 0
11:42:19.533163 IP 192.168.0.181.34150 > 185.125.190.48.80: Flags [F.], seq 88, ack 191, win 501, options [nop,nop,TS val 1870986202 ecr 2095797321], length 0
11:42:19.661772 IP 185.125.190.48.80 > 192.168.0.181.34150: Flags [.], ack 89, win 509, options [nop,nop,TS val 2095797450 ecr 1870986202], length 0
11:42:26.360898 IP 192.168.0.181.51304 > 142.250.192.35.80: Flags [.], ack 1, win 501, options [nop,nop,TS val 1311498105 ecr 616522427], length 0
11:42:26.363148 IP 142.250.192.35.80 > 192.168.0.181.51304: Flags [.], ack 1, win 265, options [nop,nop,TS val 616532667 ecr 1311406277], length 0
11:42:36.601010 IP 192.168.0.181.51304 > 142.250.192.35.80: Flags [.], ack 1, win 501, options [nop,nop,TS val 1311508345 ecr 616532667], length 0
11:42:36.604019 IP 142.250.192.35.80 > 192.168.0.181.51304: Flags [.], ack 1, win 265, options [nop,nop,TS val 616542908 ecr 1311406277], length 0
11:42:39.275106 IP 192.168.0.181.40282 > 192.168.0.1.80: Flags [S], seq 3619155204, win 1024, options [mss 1460], length 0
11:42:39.276007 IP 192.168.0.1.80 > 192.168.0.181.40282: Flags [S.], seq 3810892068, ack 3619155205, win 14600, options [mss 1460], length 0
11:42:39.276063 IP 192.168.0.181.40282 > 192.168.0.1.80: Flags [R], seq 3619155205, win 0, length 0
^C
18 packets captured
18 packets received by filter
0 packets dropped by kernel
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo tcpdump -n port 81
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
11:42:57.611975 IP 192.168.0.181.47830 > 192.168.0.1.81: Flags [S], seq 2104214126, win 1024, options [mss 1460], length 0
11:42:57.613623 IP 192.168.0.1.81 > 192.168.0.181.47830: Flags [R.], seq 0, ack 2104214127, win 0, length 0
11:43:08.868650 IP 192.168.0.181.40980 > 192.168.0.1.81: Flags [S], seq 3031532005, win 64240, options [mss 1460,sackOK,TS val 734044290 ecr 0,nop,wscale 7], length 0
11:43:08.872715 IP 192.168.0.1.81 > 192.168.0.181.40980: Flags [R.], seq 0, ack 3031532006, win 0, length 0
^C
4 packets captured
4 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

Conclusion:-

Nmap offers a diverse set of scanning techniques to suit various network reconnaissance needs. The choice of scan depends on factors like stealth, speed, and the specific information you seek. Understanding these techniques is vital for network administrators and security professionals to safeguard their networks and systems from potential threats