

## **LAB ASSIGNMENT NO:08**

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

### **Theory:**

#### 1. What is Port Scanning? What is NMAP?

**Port Scanning:** Port scanning is a technique used in computer networking and cybersecurity to discover open network ports on a target system. A network port is a virtual endpoint for communication, and each port serves a specific purpose (e.g., web traffic on port 80, email on port 25). Port scanning tools and techniques are commonly used by security professionals and hackers to assess the security posture of a network, identify potential vulnerabilities, and gather information about services running on a target system.

**Nmap (Network Mapper):** Nmap is a powerful and open-source network scanning tool that is widely used for network discovery and security auditing. It allows users to discover devices and services running on a network and provides detailed information about open ports, services, and operating systems. Nmap is known for its flexibility and extensive feature set, making it a valuable tool for both network administrators and security experts.

#### 2. Explain in brief different states of port. (open, closed, filtered, unfiltered, open | filtered and closed | filtered)

**Different States of Ports:**

**Open:** An "open" port indicates that a network service or application is actively listening and available to accept incoming connections. This state implies that communication is possible, and a connection can be established if the client and server agree on the protocol.

**Closed:** A "closed" port means that there is no application or service listening on that port. The operating system may respond with a

"Connection Refused" message to indicate that no service is available.

**Filtered:** A "filtered" port indicates that a firewall or filtering mechanism is actively blocking incoming connection attempts to the port. The firewall may be configured to silently drop connection requests or respond with an ICMP "Destination Unreachable" message.

**Unfiltered:** An "unfiltered" port means that the port is accessible, but the scanner couldn't determine whether it is open or closed. This state often occurs when a firewall allows all packets, including those destined for closed ports, to pass through without filtering.

**Open | Filtered:** The "open | filtered" state indicates that the scanner couldn't reliably determine whether the port is open or filtered. This state can occur when a firewall or intrusion detection system (IDS) behaves in a way that obscures the true state of the port.

**Closed | Filtered:** The "closed | filtered" state indicates that the scanner couldn't reliably determine whether the port is closed or filtered. Similar to "open | filtered," this state can occur when a firewall or filtering device generates ambiguous responses.

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

TCP Connect scan:

```
# nmap -sT ipaddress
```

These scans are so called because UNIX sockets programming uses a system call named `connect()` to begin a TCP connection to a remote site. If `connect()` succeeds, a connection was made. If it fails, the connection could not be made (the remote system is offline, the port is closed, or some other error occurred along the way). This allows a basic type of port scan, which attempts to connect to every port in turn, and notes whether or not the connection succeeded. Once the scan is completed, ports to which a connection could be established are listed

as open, the rest are said to be closed.

### TCP SYN scan:

```
#nmap -sS ipaddress
```

SYN or Stealth scanning makes use of this procedure by sending a SYN packet and looking at the response. If SYN/ACK is sent back, the port is open and the remote end is trying to open a TCP connection. The scanner then sends an RST to tear down the connection before it can be established fully; often preventing the connection attempt appearing in application logs. If the port is closed, an RST will be sent.

### FIN Scan:

```
#nmap -sF ipaddress
```

The idea behind these type of scans is that a closed port should respond with an RST upon receiving packets, whereas an open port should just drop them (it's listening for packets with SYN set). This way, you never make even part of a connection, and never send a SYN packet; which is what most IDS' look out for. The FIN scan sends a packet with only the FIN flag set.

### Null Scan:

```
#nmap -sN target
```

The Null Scan is a type of TCP scan that hackers — both ethical and malicious — use to identify listening TCP ports. In the right hands, a Null Scan can help identify potential holes for server hardening, but in the wrong hands, it is a reconnaissance tool. It is a pre-attack probe. A Null Scan is a series of TCP packets that contain a sequence number of 0 and no set flags.

### XMAS Scan:

```
#nmap -sX target
```

The Xmas Tree scan sets the FIN, URG and PUSH flags are set. This scan will work on UNIX and related systems and cause the kernel to drop the packet if the receiving port is open.

### ACK Scan:

```
#nmap -sA target
```

This scan type sends ACK packets to a host.

If an RST comes back, the port is classified "unfiltered" (that is, it was allowed to send its RST through whatever firewall was in place). If nothing comes back, the port is said to be "filtered", that is, the firewall prevented the RST coming back from the port.

### Ping Sweep:

```
# nmap -sP IP address of gateway
```

This scan type lists the hosts within the specified range that responded to a ping. It allows you to detect which computers are online, rather than which ports are open.

### Service and version detection:

```
#nmap -sV target
```

Nmap attempts to identify the services running on open ports by analyzing their responses. It sends probes to determine service types and versions, providing valuable information about the target system's software stack.

### Port and Port range scanning:

```
#nmap -p23 ipaddress scans specific port
```

```
#nmap -p23-443 ipaddress scans ports ranging from 23 to 443
```

These commands allow you to specify individual ports or port ranges to scan. For example, -p 80,443 scans ports 80 and 443, while -p- scans all 65,535 ports.

### OS fingerprinting:

```
#nmap -O ipaddress
```

Nmap sends a series of TCP and UDP packets to the remote host and

examines practically every bit in the responses. After performing dozens of tests such as TCP ISN sampling, TCP options support and ordering, IP ID sampling, and the initial window size check, Nmap compares the results to its nmap-os-db database of more than 2,600 known OS fingerprints and prints out the OS details if there is a match.

## Output Screenshots:

```
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~  
Nmap done: 1 IP address (1 host up) scanned in 1.62 seconds  
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ nmap -sT 192.168.0.1  
  
Starting Nmap 7.60 ( https://nmap.org ) at 2023-09-01 11:34 IST  
Nmap scan report for _gateway (192.168.0.1)  
Host is up (0.0094s 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  
  
Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds  
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ nmap -sU 192.168.0.1  
You requested a scan type which requires root privileges.  
QUITTING!  
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo nmap -sU 192.168.0.1  
[sudo] password for lab1006:  
  
Starting Nmap 7.60 ( https://nmap.org ) at 2023-09-01 11:37 IST  
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 11:42 IST  
Nmap scan report for _gateway (192.168.0.1)  
Host is up (0.00060s 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 16.45 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 11:44 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 0.05 seconds
```

```
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~  
11:09:27.564033 IP 192.168.0.198.51434 > 192.168.0.1.1091: Flags [S], seq 2548987152, win 1024, options [mss 1460], length 0  
11:09:27.564062 IP 192.168.0.198.51434 > 192.168.0.1.5198: Flags [S], seq 2548987152, win 1024, options [mss 1460], length 0  
11:09:27.564080 IP 192.168.0.198.51434 > 192.168.0.1.3077: Flags [S], seq 2548987152, win 1024, options [mss 1460], length 0  
11:09:27.564094 IP 192.168.0.198.51434 > 192.168.0.1.50003: Flags [S], seq 2548987152, win 1024, options [mss 1460], length 0  
11:09:27.564117 IP 192.168.0.198.51434 > 192.168.0.1.648: Flags [S], seq 2548987152, win 1024, options [mss 1460], length 0  
11:09:27.564138 IP 192.168.0.198.51434 > 192.168.0.1.50500: Flags [S], seq 2548987152, win 1024, options [mss 1460], length 0  
11:09:27.564149 IP 192.168.0.198.51434 > 192.168.0.1.5108: Flags [S], seq 2548987152, win 1024, options [mss 1460], length 0  
11:09:27.564171 IP 192.168.0.198.51434 > 192.168.0.1.24: Flags [S], seq 2548987152, win 1024, options [mss 1460], length 0  
11:09:27.564182 IP 192.168.0.198.51434 > 192.168.0.1.1106: Flags [S], seq 2548987152, win 1024, options [mss 1460], length 0  
11:09:27.564216 IP 192.168.0.198.51434 > 192.168.0.1.1099: Flags [S], seq 2548987152, win 1024, options [mss 1460], length 0  
11:09:27.564242 IP 192.168.0.198.51434 > 192.168.0.1.1186: Flags [S], seq 2548987152, win 1024, options [mss 1460], length 0  
11:09:27.564253 IP 192.168.0.198.51434 > 192.168.0.1.19801: Flags [S], seq 2548987152, win 1024, options [mss 1460], length 0  
11:09:27.564287 IP 192.168.0.198.51434 > 192.168.0.1.8031: Flags [S], seq 2548987152, win 1024, options [mss 1460], length 0  
11:09:27.564300 IP 192.168.0.198.51434 > 192.168.0.1.5269: Flags [S], seq 2548987152, win 1024, options [mss 1460], length 0  
11:09:27.564322 IP 192.168.0.198.51434 > 192.168.0.1.2251: Flags [S], seq 2548987152, win 1024, options [mss 1460], length 0  
11:09:27.564333 IP 192.168.0.198.51434 > 192.168.0.1.16992: Flags [S], seq 2548987152, win 1024, options [mss 1460], length 0  
11:09:27.564344 IP 192.168.0.198.51434 > 192.168.0.1.9103: Flags [S], seq 2548987152, win 1024, options [mss 1460], length 0  
11:09:27.564418 IP 192.168.0.1.587 > 192.168.0.198.51434: Flags [R.], seq 0, ack 2548987153, win 0, length 0  
11:09:27.564421 IP 192.168.0.1.250 > 192.168.0.198.51434: Flags [R.], seq 0, ack 2548987153, win 0, length 0  
11:09:27.564455 IP 192.168.0.1.110 > 192.168.0.198.51434: Flags [R.], seq 0, ack 2548987153, win 0, length 0  
11:09:27.564679 IP 192.168.0.1.1723 > 192.168.0.198.51434: Flags [R.], seq 0, ack 2548987153, win 0, length 0  
11:09:27.564699 IP 192.168.0.198.51434 > 192.168.0.1.443: Flags [R.], seq 2548987153, win 0, length 0  
11:09:27.564867 IP 192.168.0.1.3306 > 192.168.0.198.51434: Flags [R.], seq 0, ack 2548987153, win 0, length 0  
11:09:27.564873 IP 192.168.0.1.135 > 192.168.0.198.51434: Flags [R.], seq 0, ack 2548987153, win 0, length 0  
11:09:27.564953 IP 192.168.0.1.1726 > 192.168.0.198.51434: Flags [R.], seq 0, ack 2548987153, win 0, length 0  
11:09:27.564955 IP 192.168.0.1.110 > 192.168.0.198.51434: Flags [R.], seq 0, ack 2548987153, win 0, length 0  
11:09:27.565097 IP 192.168.0.1.23 > 192.168.0.198.51434: Flags [R.], seq 0, ack 2548987153, win 0, length 0  
11:09:27.565111 IP 192.168.0.1.8888 > 192.168.0.198.51434: Flags [R.], seq 0, ack 2548987153, win 0, length 0  
11:09:27.565197 IP 192.168.0.1.25 > 192.168.0.198.51434: Flags [R.], seq 0, ack 2548987153, win 0, length 0  
11:09:27.565204 IP 192.168.0.1.80 > 192.168.0.198.51434: Flags [S.], seq 1690757563, ack 2548987153, win 14600, options [mss 1460], length 0  
11:09:27.565219 IP 192.168.0.198.51434 > 192.168.0.1.80: Flags [R.], seq 0, ack 2548987153, win 0, length 0  
11:09:27.565335 IP 192.168.0.1.199 > 192.168.0.198.51434: Flags [R.], seq 0, ack 2548987153, win 0, length 0  
11:09:27.565339 IP 192.168.0.1.111 > 192.168.0.198.51434: Flags [R.], seq 0, ack 2548987153, win 0, length 0  
11:09:27.565369 IP 192.168.0.1.22 > 192.168.0.198.51434: Flags [R.], seq 0, ack 2548987153, win 0, length 0  
11:09:27.565478 IP 192.168.0.1.993 > 192.168.0.198.51434: Flags [R.], seq 0, ack 2548987153, win 0, length 0  
11:09:27.565485 IP 192.168.0.1.8192 > 192.168.0.198.51434: Flags [R.], seq 0, ack 2548987153, win 0, length 0  
11:09:27.565572 IP 192.168.0.1.5900 > 192.168.0.198.51434: Flags [R.], seq 0, ack 2548987153, win 0, length 0  
11:09:27.565575 IP 192.168.0.1.3324 > 192.168.0.198.51434: Flags [R.], seq 0, ack 2548987153, win 0, length 0  
11:09:27.565735 IP 192.168.0.1.1091 > 192.168.0.198.51434: Flags [R.], seq 0, ack 2548987153, win 0, length 0  
11:09:27.565740 IP 192.168.0.1.2006 > 192.168.0.198.51434: Flags [R.], seq 0, ack 2548987153, win 0, length 0  
11:09:27.565790 IP 192.168.0.1.8009 > 192.168.0.198.51434: Flags [R.], seq 0, ack 2548987153, win 0, length 0  
11:09:27.565793 IP 192.168.0.1.5198 > 192.168.0.198.51434: Flags [R.], seq 0, ack 2548987153, win 0, length 0  
11:09:27.565910 IP 192.168.0.1.2045 > 192.168.0.198.51434: Flags [R.], seq 0, ack 2548987153, win 0, length 0  
11:09:27.565980 IP 192.168.0.1.3077 > 192.168.0.198.51434: Flags [R.], seq 0, ack 2548987153, win 0, length 0  
11:09:27.566008 IP 192.168.0.1.50003 > 192.168.0.198.51434: Flags [R.], seq 0, ack 2548987153, win 0, length 0  
11:09:27.566011 IP 192.168.0.1.2381 > 192.168.0.198.51434: Flags [R.], seq 0, ack 2548987153, win 0, length 0
```

Roll No: 09  
Name: Shreya Bagade  
Date: 01/09/2023

```
Activities Terminal Fri 12:28 lab1006@lab1006-HP-280-G4-MT-Business-PC: ~  
File Edit View Search Terminal Help  
11:09:32.904195 IP 192.168.0.132.5353 > 224.0.0.251.5353: 0 PTR (QM)? _googlecast._tcp.local. (40)  
11:09:32.904215 IP6 Fe80::98b4:47fb:4996:5056.5353 > ff02::fb.5353: 0 PTR (QM)? _googlecast._tcp.local. (40)  
11:09:32.904238 IP 192.168.0.132.5353 > 224.0.0.251.5353: 0+ [0q] 0/0/0 (12)  
11:09:32.904301 IP6 Fe80::98b4:47fb:4996:5056.5353 > ff02::fb.5353: 0+ [0q] 0/0/0 (12)  
11:09:33.129204 ARP, Request who-has 192.168.0.146 tell 192.168.0.1, length 46  
11:09:34.129160 ARP, Request who-has 192.168.0.146 tell 192.168.0.1, length 46  
AC  
1570 packets captured  
2083 packets received by filter  
513 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  
AC  
0 packets captured  
0 packets received by filter  
0 packets dropped by kernel  
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo tcpdump -n port 80  
tcpdump: listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes  
^C^C  
0 packets captured  
0 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  
11:32:37.990803 IP 192.168.0.198.53402 > 91.189.91.48.80: Flags [S], seq 1340570033, win 64240, options [mss 1460,sackOK,TS val 1978664477 ecr 0,nop,wscale 7], length 0  
11:32:38.189093 IP 91.189.91.48.80 > 192.168.0.198.53402: Flags [S.], seq 2212074944, ack 1340570034, win 65160, options [mss 1440,sackOK,TS val 2738221173 ecr 1978664477,nop,wscale 7], length 0  
11:32:38.189761 IP 192.168.0.198.53402 > 91.189.91.48.80: Flags [.] ack 1, win 502, options [nop,nop,TS val 1978664670 ecr 2738221173], length 0  
11:32:38.189952 IP 192.168.0.198.53402 > 91.189.91.48.80: Flags [P.], seq 1:88, ack 1, win 502, options [nop,nop,TS val 1978664670 ecr 2738221173], length 87: HTTP: GET / HTTP/1.1  
11:32:38.382288 IP 91.189.91.48.80 > 192.168.0.198.53402: Flags [P.], seq 1:190, ack 88, win 506, options [nop,nop,TS val 2738221427 ecr 1978664670], length 189: HTTP: HTTP/1.1 204 No Content  
11:32:38.382346 IP 192.168.0.198.53402 > 91.189.91.48.80: Flags [.] ack 190, win 501, options [nop,nop,TS val 1978664862 ecr 2738221427], length 0  
11:32:38.382564 IP 192.168.0.198.53402 > 91.189.91.48.80: Flags [F.], seq 88, ack 190, win 501, options [nop,nop,TS val 1978664863 ecr 2738221427], length 0  
11:32:38.383689 IP 91.189.91.48.80 > 192.168.0.198.53402: Flags [F.], seq 190, ack 88, win 506, options [nop,nop,TS val 2738221428 ecr 1978664670], length 0  
11:32:38.383735 IP 192.168.0.198.53402 > 91.189.91.48.80: Flags [.] ack 191, win 501, options [nop,nop,TS val 1978664864 ecr 2738221428], length 0  
11:32:38.575109 IP 91.189.91.48.80 > 192.168.0.198.53402: Flags [.] ack 89, win 506, options [nop,nop,TS val 2738221619 ecr 1978664863], length 0  
AC  
10 packets captured  
10 packets received by filter  
0 packets dropped by kernel  
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
```

```
Activities Terminal Fri 12:27 lab1006@lab1006-HP-280-G4-MT-Business-PC: ~  
File Edit View Search Terminal Help  
11:05:13.326842 IP 192.168.0.192.137 > 192.168.0.255.137: UDP, length 50  
11:05:13.476267 IP 192.168.0.194.137 > 192.168.0.255.137: UDP, length 50  
11:05:13.559765 IP 192.168.0.249.64834 > 224.0.0.252.5355: UDP, length 25  
11:05:13.559785 IP 192.168.0.249.61240 > 224.0.0.252.5355: UDP, length 25  
11:05:13.902045 IP 192.168.0.249.137 > 192.168.0.255.137: UDP, length 50  
11:05:13.908949 0609:1e15:44:53 > 3d:db:ff:77:e4:d1, ethernet type Unknown (0xa0a0), length 60:  
0x0000: 0003 0101 0101 0101 0101 0101 0101 0101 .....  
0x0010: 0101 0101 0101 0101 0101 0101 0101 0101 .....  
0x0020: 0101 0101 0101 0101 0101 0101 0101 0101 .....  
11:05:14.092118 IP 192.168.0.192.137 > 192.168.0.255.137: UDP, length 50  
11:05:14.152024 IP 192.168.0.249.5353 > 224.0.0.251.5353: 0 AAAA (QM)? nta-064.local. (31)  
11:05:14.152175 IP 192.168.0.249.5353 > 224.0.0.251.5353: 0 A (QM)? nta-064.local. (31)  
11:05:14.152864 IP 192.168.0.132.5353 > 224.0.0.251.5353: 0+ [0q] 0/0/0 (12)  
11:05:14.152980 IP 192.168.0.132.5353 > 224.0.0.251.5353: 0+ [0q] 0/0/0 (12)  
11:05:14.229268 IP 192.168.0.194.137 > 192.168.0.255.137: UDP, length 50  
11:05:14.630862 ARP, Request who-has 192.168.0.176 tell 192.168.0.128, length 46  
11:05:14.653921 IP 192.168.0.249.137 > 192.168.0.255.137: UDP, length 50  
11:05:14.776304 ARP, Request who-has 192.168.0.237 tell 192.168.0.123, length 46  
11:05:14.791681 ARP, Request who-has 192.168.0.117 tell 192.168.0.123, length 46  
11:05:14.979438 IP 192.168.0.194.137 > 192.168.0.255.137: UDP, length 50  
11:05:15.168552 ARP, Request who-has 192.168.0.155 tell 192.168.0.168, length 46  
11:05:15.191912 IP 192.168.0.227.138 > 192.168.0.255.138: UDP, length 176  
11:05:15.400927 ARP, Request who-has 192.168.0.237 tell 192.168.0.123, length 46  
11:05:15.400947 ARP, Request who-has 192.168.0.117 tell 192.168.0.123, length 46  
11:05:15.892962 IP6 Fe80::192e:4c94:cfda:5894.5353 > ff02::fb.5353: 0 [2q] PTR (QM)? _lpps._tcp.local. PTR (QM)? _lpp._tcp.local. (45)  
11:05:15.892981 IP6 Fe80::192e:4c94:cfda:5894.5353 > ff02::fb.5353: 0 [2q] PTR (QM)? _lpps._tcp.local. PTR (QM)? _lpp._tcp.local. (45)  
11:05:15.893375 IP6 Fe80::98b4:47fb:4996:5056.5353 > ff02::fb.5353: 0+ [0q] 0/0/0 (12)  
11:05:15.893635 IP 192.168.0.132.5353 > 224.0.0.251.5353: 0+ [0q] 0/0/0 (12)  
11:05:16.087161 ARP, Request who-has 192.168.0.155 tell 192.168.0.168, length 46  
11:05:16.133528 IP 192.168.0.192.137 > 192.168.0.255.137: UDP, length 50  
11:05:16.167945 IP 192.168.0.167.59199 > 239.255.255.250.1900: UDP, length 175  
11:05:16.172643 ARP, Request who-has 192.168.0.155 tell 192.168.0.168, length 46  
11:05:16.401105 ARP, Request who-has 192.168.0.237 tell 192.168.0.123, length 46  
11:05:16.401125 ARP, Request who-has 192.168.0.117 tell 192.168.0.123, length 46  
11:05:16.873394 IP 192.168.0.192.137 > 192.168.0.255.137: UDP, length 50  
11:05:16.885533 ARP, Request who-has 192.168.0.155 tell 192.168.0.168, length 46  
11:05:17.081881 ARP, Request who-has 192.168.0.155 tell 192.168.0.168, length 46  
11:05:17.179186 IP 192.168.0.167.59199 > 239.255.255.250.1900: UDP, length 175  
11:05:17.191111 IP 192.168.0.194.137 > 192.168.0.255.137: UDP, length 50  
11:05:17.590848 IP 192.168.0.217.51299 > 239.255.255.250.1900: UDP, length 175  
11:05:17.590889 ARP, Request who-has 192.168.0.176 tell 192.168.0.128, length 46  
11:05:17.623591 IP 192.168.0.192.137 > 192.168.0.255.137: UDP, length 50  
11:05:17.885092 ARP, Request who-has 192.168.0.155 tell 192.168.0.168, length 46  
11:05:17.930849 ARP, Request who-has 192.168.0.218 tell 192.168.0.102, length 46  
11:05:17.947219 IP 192.168.0.194.137 > 192.168.0.255.137: UDP, length 50  
11:05:18.129041 ARP, Request who-has 192.168.0.176 tell 192.168.0.128, length 46
```



Roll No: 09  
Name: Shreya Bagade  
Date: 01/09/2023

```

Fri 12:06
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help
SF:><BODY><H1>Not<x20Implemented</H1>The<x20HTTP<x20Method<x20is<x20not<x2
SF:Implemented<x20by<x20this<x20server<.</BODY><HTML>\r\n)<(HTTPOption
SF:is_12C,"HTTP/1.0)<x20501<x20Not<x20Implemented<\r\nContent-Type:<x20text/
SF:html\r\n\r\nConnection:<x20close\r\nContent-Length:<x20149\r\nServer:<x20TP
SF:-Link/TP-Link<x20UPnP/1.1<x20MlnUPnPd/1.0\r\nExt:<.\r\n\r\nHTML><HEAD
SF:><TITLE>501<x20Not<x20Implemented</TITLE><./HEAD><BODY><H1>Not<x20Imple
SF:mented</H1>The<x20HTTP<x20Method<x20is<x20not<x20Implemented<x20by<x20th
SF:is<x20server<.</BODY><HTML>\r\n)<(RTSPRequest_12c,"RTSP/1.0)<x20501
SF:>Not<x20Implemented<\r\nContent-Type:<x20text/html\r\n\r\nConnection:<x20c
SF:lose\r\nContent-Length:<x20149\r\nServer:<x20TP-Link/TP-Link<x20UPnP/1
SF:.1<x20MlnUPnPd/1.0\r\nExt:<.\r\n\r\nHTML><HEAD><TITLE>501<x20Not<x20Im
SF:plemented</TITLE><./HEAD><BODY><H1>Not<x20Implemented</H1>The<x20HTTP<x2
SF:Method<x20is<x20not<x20Implemented<x20by<x20this<x20server<.</BODY><H
SF:TML>\r\n)<(FourFourFourRequest_117,"HTTP/1.0)<x20404<x20Not<x20Found<\r
SF:nContent-Type:<x20text/html\r\n\r\nConnection:<x20close\r\nContent-Length:
SF:>20134\r\nServer:<x20TP-Link/TP-Link<x20UPnP/1.1<x20MlnUPnPd/1.0\r\n
SF:Ext:<.\r\n\r\nHTML><HEAD><TITLE>404<x20Not<x20Found</TITLE><./HEAD><BODY>
SF:<H1>Not<x20Found</H1>The<x20Requested<x20URL<x20was<x20not<x20found<x20
SF:on<x20this<x20server<.</BODY><HTML>\r\n)<(SIPOptions_12b,"SIP/2.0)<x
SF:20501<x20Not<x20Implemented<\r\nContent-Type:<x20text/html\r\n\r\nConne
SF:>tion:<x20close\r\nContent-Length:<x20149\r\nServer:<x20TP-Link/TP-Link<x20
SF:UPnP/1.1<x20MlnUPnPd/1.0\r\nExt:<.\r\n\r\nHTML><HEAD><TITLE>501<x20Not
SF:>Implemented</TITLE><./HEAD><BODY><H1>Not<x20Implemented</H1>The<x20H
SF:>TTP<x20Method<x20is<x20not<x20Implemented<x20by<x20this<x20server<.</BO
SF:DY><HTML>\r\n)";
MAC Address: AC:15:A2:B9:9E:29 (Unknown)
Service Info: OS: Linux; CPE: o:/linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.58 seconds
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo nmap --allports 192.168.0.1

Starting Nmap 7.60 ( https://nmap.org ) at 2023-09-01 11:53 IST
Nmap scan report for gateway (192.168.0.1)
Host is up (0.036s 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 1.59 seconds
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$

```

```
activities Terminal
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
Nmap done: 1 IP address (1 host up) scanned in 9.53 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 11:45 IST
Nmap scan report for _gateway (192.168.0.1)
Host is up (0.00060s 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 11.37 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 11:47 IST
Nmap scan report for _gateway (192.168.0.1)
Host is up (0.0059s 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 1.63 seconds
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo nmap -sV 192.168.0.1

Starting Nmap 7.60 ( https://nmap.org ) at 2023-09-01 11:50 IST
WARNING: Service 192.168.0.1:1900 had already soft-matched rtsp, but now soft-matched sip; ignoring second value
Nmap scan report for _gateway (192.168.0.1)
Host is up (0.012s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE VERSION
53/tcp    open  domain
60/tcp    open  http    BusyBox http 1.19.4
443/tcp   open  ssl/http BusyBox http 1.19.4
1900/tcp  open  rtsp
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-servic
SF:Port1900-TCP:V=7.60X=7MD=9/1KLine=64F1B2C6XP=x86_64-pc-linux-gnuusr(GET
SF:Header=HTTP/1.1X=2044X=20FoundM\r\nContent-Type:\x20text/
SF:chtml\r\nconnection:\x20close\r\ncontent-Length:\x20134\r\n\r\nserver:\x20TP
SF:Link/TP-Link\x20UPnP/1.1\x20MiniUPnPd/1.1.8\r\nExt:\r\n\r\n<HTML><HEAD
SF:Title=404\x20Not\x20Found/>TITLE=</HEAD><BODY><H1>Not\x20Found</H1>Th
SF:e\x20requested\x20URL\x20was\x20not\x20found\x20on\x20this\x20server.\<
SF:/BODY></HTML>\r\n"3xr(GenercLLines, 124, "\x20501\x20not\x20implemented\r
SF:Content-Type:\x20text/html\r\nconnection:\x20close\r\ncontent-Length:
SF:\x20149\r\n\r\nserver:\x20TP-Link/TP-Link\x20UPnP/1.1\x20MiniUPnPd/1.1.8\r
SF:Content-Length:\x20134\r\n\r\n</HTML>
SF:Content-Length:\x20134\r\n\r\n</HTML>
```

```
Activities Terminal Fri 12:06 lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ ifconfig
enp3s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.198 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::fe04:484c:fba7:922c prefixlen 64 scopeid 0x20<link>
    ether 04:0e:3c:1a:64:30 txqueuelen 1000 (Ethernet)
    RX packets 63605 bytes 78293252 (78.2 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 17094 bytes 1457853 (1.4 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 837 bytes 90251 (90.2 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 837 bytes 90251 (90.2 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ nmap -sS 192.168.0.208
You requested a scan type which requires root privileges.
QUITTING!
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo nmap -sS 192.168.0.208
[sudo] password for lab1006:

Starting Nmap 7.60 ( https://nmap.org ) at 2023-09-01 11:07 IST
Nmap scan report for 192.168.0.208
Host is up (0.00017s latency).
All 1000 scanned ports on 192.168.0.208 are closed
MAC Address: 04:0E:3C:1A:5C:72 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.61 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 11:09 IST
Nmap scan report for _gateway (192.168.0.1)
Host is up (0.028s 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
```

```
Activities Terminal Fri 12:06 lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
Nmap done: 1 IP address (1 host up) scanned in 1.62 seconds
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ nmap -sT 192.168.0.1

Starting Nmap 7.60 ( https://nmap.org ) at 2023-09-01 11:34 IST
Nmap scan report for _gateway (192.168.0.1)
Host is up (0.0094s 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 0.09 seconds
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ nmap -sU 192.168.0.1
You requested a scan type which requires root privileges.
QUITTING!
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ sudo nmap -sU 192.168.0.1
[sudo] password for lab1006:

Starting Nmap 7.60 ( https://nmap.org ) at 2023-09-01 11:37 IST
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 11:42 IST
Nmap scan report for _gateway (192.168.0.1)
Host is up (0.0000s 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 16.45 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 11:44 IST
Nmap scan report for _gateway (192.168.0.1)
Host is up (0.00007s 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 0.03 seconds
```

**Conclusion:** This experiment focused on the installation and practical usage of Nmap, a versatile network scanning tool. By exploring various options and techniques, such as scanning for open ports, conducting OS fingerprinting, ping scans, TCP and UDP port scans, we gained valuable insights into network reconnaissance and vulnerability assessment. Nmap's capabilities in mapping network landscapes and identifying potential security risks make it an indispensable tool for cybersecurity professionals and network administrators.