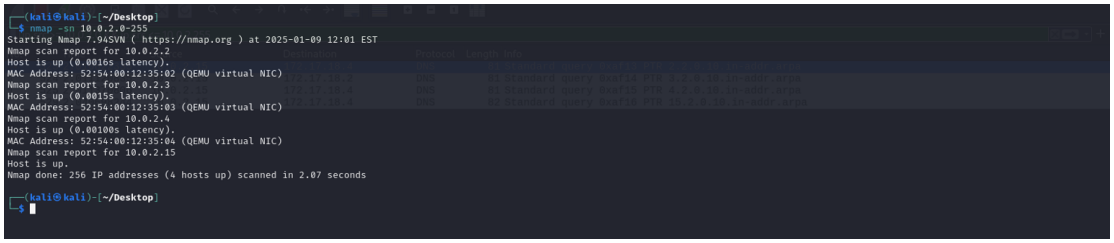
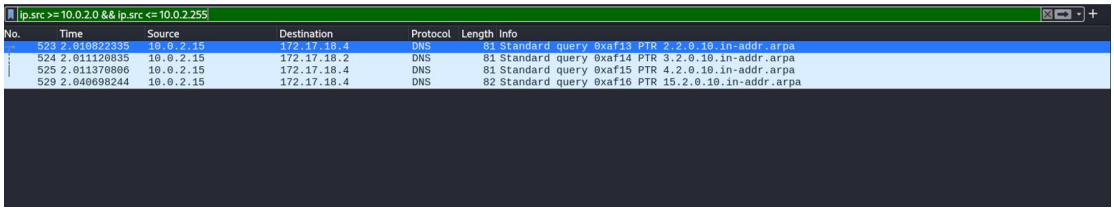
Rangineny sai kiran
CB.SC.P2CYS24011

1. Scenario: You are tasked with verifying whether the victim Metasploit2 VM is active on the network and responding to any type of ping. What Nmap command would you use to check its availability?

nmap -sn <target-ip>

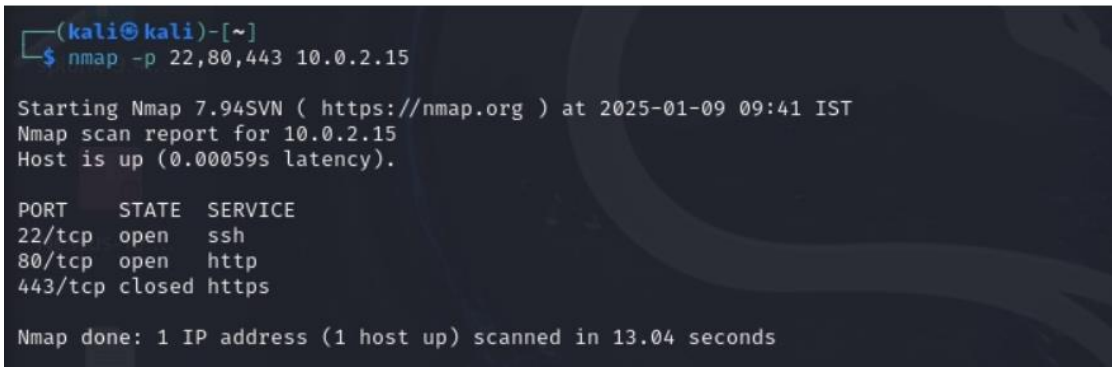




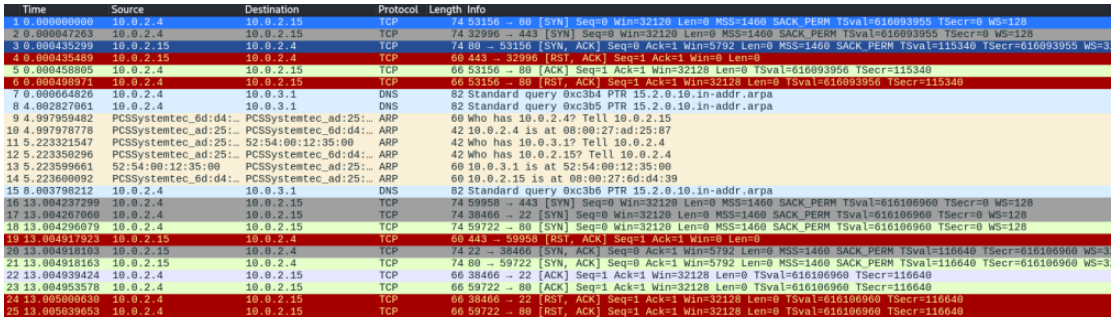
The command nmap -sn 10.0.2.0-255 performs a ping scan to identify active hosts within the specified IP range. In Wireshark, this scan generates ARP requests as it attempts to discover live devices. Additionally, you may observe TCP packets such as SYN, SYN-ACK, ACK, and RST-ACK, which indicate further communication between the detected hosts.

2. Scenario: You want to check if common ports like SSH (22), HTTP (80), and HTTPS (443) are open on the victim Metasploit2 VM. How would you scan these specific ports?

nmap -p 22,80,443 <target-ip>



Rangineny sai kiran
CB.SC.P2CYS24011

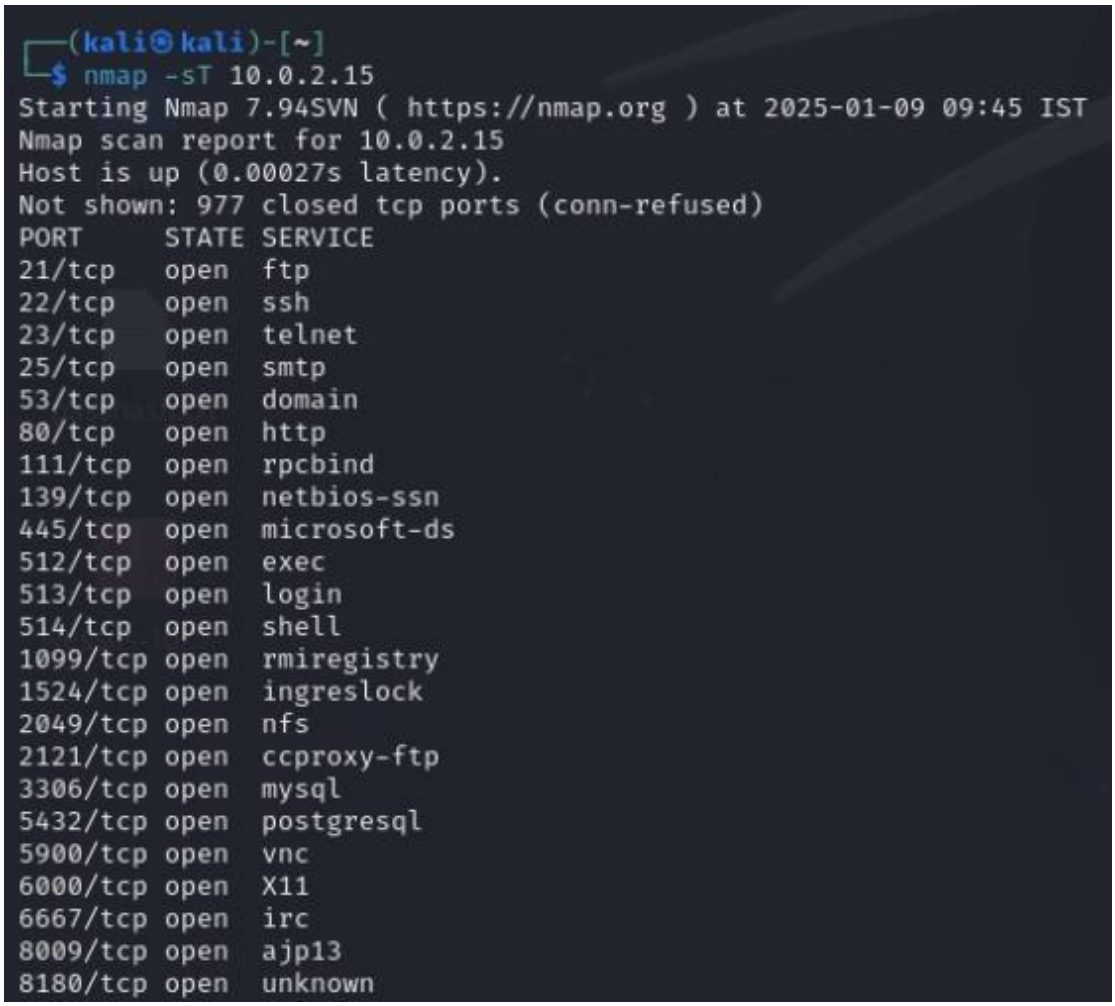


	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.4	10.0.2.15	TCP	74	53156 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=616093955 TSecr=0 WS=128
2	0.000047263	10.0.2.4	10.0.2.15	TCP	74	32996 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=616093955 TSecr=0 WS=128
3	0.000435299	10.0.2.15	10.0.2.4	TCP	74	80 → 53156 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=115340 TSecr=616093955 WS=3
4	0.000435489	10.0.2.15	10.0.2.4	TCP	60	443 → 32996 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
5	0.000458805	10.0.2.4	10.0.2.15	TCP	66	53156 → 80 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=616093956 TSecr=115340
6	0.000498971	10.0.2.4	10.0.2.15	TCP	66	53156 → 80 [RST, ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=616093956 TSecr=115340
7	0.000664826	10.0.2.4	10.0.3.1	DNS	82	Standard query 0xc3b4 PTR 15.2.0.10.in-addr.arpa
8	4.002827061	10.0.2.4	10.0.3.1	DNS	82	Standard query 0xc3b5 PTR 15.2.0.10.in-addr.arpa
9	4.997959482	PCSSystemtec_6d:d4:…	PCSSystemtec_ad:25:…	ARP	60	Who has 10.0.2.4? Tell 10.0.2.15
10	4.997978778	PCSSystemtec_ad:25:…	PCSSystemtec_6d:d4:…	ARP	42	10.0.2.4 is at 08:00:27:ad:25:87
11	5.223321547	PCSSystemtec_ad:25:…	52:54:00:12:35:00	ARP	42	Who has 10.0.3.1? Tell 10.0.2.4
12	5.223350296	PCSSystemtec_ad:25:…	PCSSystemtec_6d:d4:…	ARP	42	Who has 10.0.2.15? Tell 10.0.2.4
13	5.223599661	52:54:00:12:35:00	PCSSystemtec_ad:25:…	ARP	60	10.0.3.1 is at 52:54:00:12:35:00
14	5.223600092	PCSSystemtec_6d:d4:…	PCSSystemtec_ad:25:…	ARP	60	10.0.2.15 is at 08:00:27:6d:d4:39
15	8.003798212	10.0.2.4	10.0.3.1	DNS	82	Standard query 0xc3b6 PTR 15.2.0.10.in-addr.arpa
16	13.004237299	10.0.2.4	10.0.2.15	TCP	74	59958 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=616106960 TSecr=0 WS=128
17	13.004267060	10.0.2.4	10.0.2.15	TCP	74	38466 → 22 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=616106960 TSecr=0 WS=128
18	13.004296079	10.0.2.4	10.0.2.15	TCP	74	59722 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=616106960 TSecr=0 WS=128
19	13.004917923	10.0.2.15	10.0.2.4	TCP	60	443 → 59958 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
20	13.004918103	10.0.2.15	10.0.2.4	TCP	74	22 → 38466 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=116640 TSecr=616106960 WS=3
21	13.004918163	10.0.2.15	10.0.2.4	TCP	74	80 → 59722 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=116640 TSecr=616106960 WS=3
22	13.004939424	10.0.2.4	10.0.2.15	TCP	66	38466 → 22 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=616106960 TSecr=116640
23	13.004953578	10.0.2.4	10.0.2.15	TCP	66	59722 → 80 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=616106960 TSecr=116640
24	13.005000638	10.0.2.4	10.0.2.15	TCP	66	38466 → 22 [RST, ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=616106960 TSecr=116640
25	13.005039653	10.0.2.4	10.0.2.15	TCP	66	59722 → 80 [RST, ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=616106960 TSecr=116640

The command nmap -p 22,80,443 10.0.2.15 conducts a TCP SYN scan to determine the status of these ports on the target system. In the packet capture, ports 22 and 80 reply with SYN-ACK, signifying they are open, whereas port 443 responds with RST-ACK, indicating it is closed.

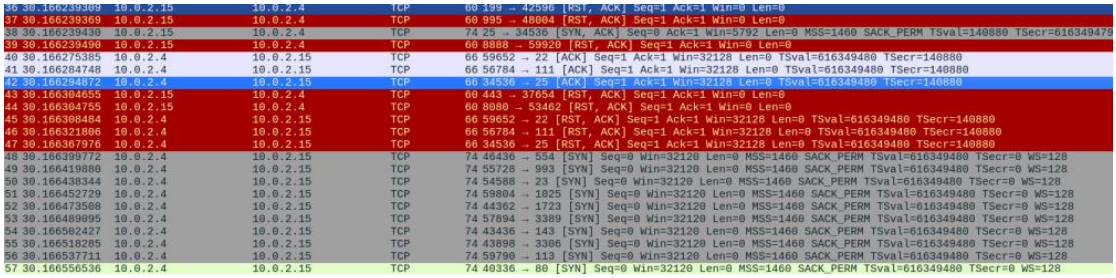
3. Scenario: You need to perform a full TCP connection scan on the victim Metasploit2 VM to see which ports are open. What would be your approach?

```
sudo nmap -sT <target-ip>
```



```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 10.0.2.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-09 09:45 IST
Nmap scan report for 10.0.2.15
Host is up (0.00027s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
```

Rangineny sai kiran
CB.SC.P2CYS24011



36	30.166200309	10.0.2.15	10.0.2.4	TCP	60 199 → 42596 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
37	30.166239369	10.0.2.15	10.0.2.4	TCP	60 995 → 48004 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
38	30.166239430	10.0.2.15	10.0.2.4	TCP	74 25 → 34536 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=140880 TSecr=616349479
39	30.166239490	10.0.2.15	10.0.2.4	TCP	60 8888 → 59920 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
40	30.166275385	10.0.2.4	10.0.2.15	TCP	66 59652 → 22 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=616349480 TSecr=140880
41	30.166284748	10.0.2.4	10.0.2.15	TCP	66 56784 → 111 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=616349480 TSecr=140880
42	30.166294872	10.0.2.4	10.0.2.15	TCP	66 34536 → 25 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=616349480 TSecr=140880
43	30.166304655	10.0.2.15	10.0.2.4	TCP	60 443 → 37654 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
44	30.166304755	10.0.2.15	10.0.2.4	TCP	60 8080 → 53462 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
45	30.166308484	10.0.2.4	10.0.2.15	TCP	66 59652 → 22 [RST, ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=616349480 TSecr=140880
46	30.166321806	10.0.2.4	10.0.2.15	TCP	66 56784 → 111 [RST, ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=616349480 TSecr=140880
47	30.166367976	10.0.2.4	10.0.2.15	TCP	66 34536 → 25 [RST, ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=616349480 TSecr=140880
48	30.166399772	10.0.2.4	10.0.2.15	TCP	74 46436 → 554 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=616349480 TSecr=0 WS=128
49	30.166419880	10.0.2.4	10.0.2.15	TCP	74 55728 → 993 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=616349480 TSecr=0 WS=128
50	30.166438344	10.0.2.4	10.0.2.15	TCP	74 54588 → 23 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=616349480 TSecr=0 WS=128
51	30.166452729	10.0.2.4	10.0.2.15	TCP	74 59804 → 1025 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=616349480 TSecr=0 WS=128
52	30.166473508	10.0.2.4	10.0.2.15	TCP	74 44362 → 1723 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=616349480 TSecr=0 WS=128
53	30.166489095	10.0.2.4	10.0.2.15	TCP	74 57894 → 3389 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=616349480 TSecr=0 WS=128
54	30.166502427	10.0.2.4	10.0.2.15	TCP	74 43436 → 143 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=616349480 TSecr=0 WS=128
55	30.166518285	10.0.2.4	10.0.2.15	TCP	74 43898 → 3306 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=616349480 TSecr=0 WS=128
56	30.166537711	10.0.2.4	10.0.2.15	TCP	74 59790 → 113 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=616349480 TSecr=0 WS=128
57	30.166556536	10.0.2.4	10.0.2.15	TCP	74 40336 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=616349480 TSecr=0 WS=128

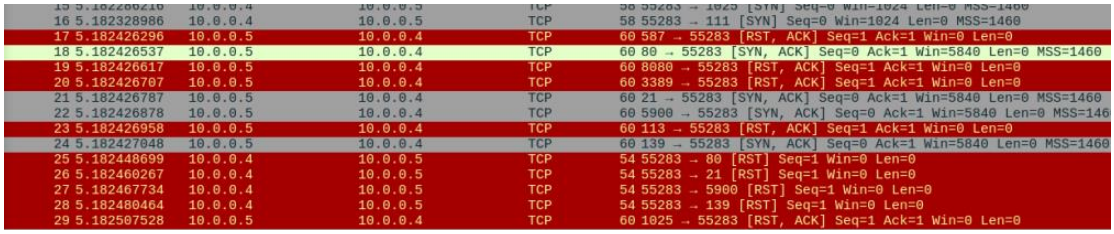
The nmap -sT 10.0.2.15 scan establishes full TCP connections to various ports, such as 25, 80, and 3306, as indicated by the SYN, SYN-ACK, and ACK sequence. In the packet capture, Nmap sends SYN packets, receives SYN-ACK responses for open ports, completes the handshake, and then terminates the connection with an RST. This confirms the presence of multiple active services on the target 10.0.2.15.

4. Scenario: You want to conduct a stealthy scan on the victim Metasploit2 VM, trying to avoid detection by completing only part of the TCP handshake. Which Nmap command should you use for this scan?

```
sudo nmap -sS <target-ip>
```

```
└─$ sudo nmap -sS 10.0.0.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-09 20:44 IST
Nmap scan report for 10.0.0.5
Host is up (0.000093s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:6D:D4:39 (Oracle VirtualBox virtual NIC)
```

Rangineny sai kiran
CB.SC.P2CYS24011



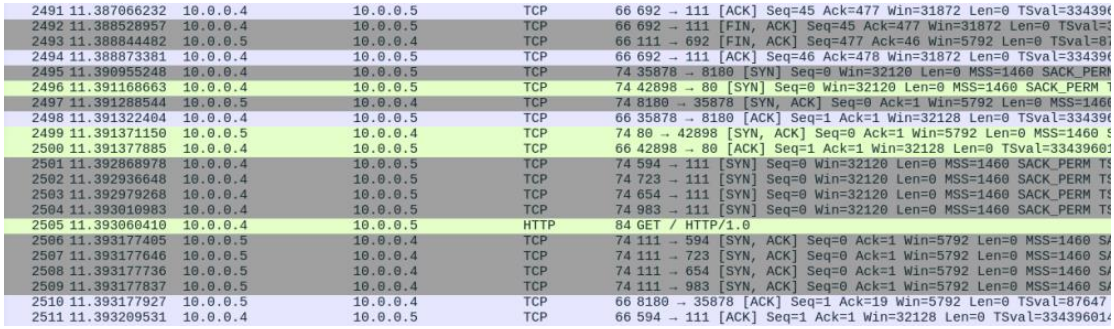
16	5.182328986	10.0.0.4	10.0.0.5	TCP	58 55283 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
17	5.182426296	10.0.0.5	10.0.0.4	TCP	60 587 → 55283 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
18	5.182426537	10.0.0.5	10.0.0.4	TCP	60 80 → 55283 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
19	5.182426617	10.0.0.5	10.0.0.4	TCP	60 8080 → 55283 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
20	5.182426707	10.0.0.5	10.0.0.4	TCP	60 3389 → 55283 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
21	5.182426787	10.0.0.5	10.0.0.4	TCP	60 21 → 55283 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
22	5.182426878	10.0.0.5	10.0.0.4	TCP	60 5900 → 55283 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=146
23	5.182426958	10.0.0.5	10.0.0.4	TCP	60 113 → 55283 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	5.182427048	10.0.0.5	10.0.0.4	TCP	60 139 → 55283 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
25	5.182448699	10.0.0.4	10.0.0.5	TCP	54 55283 → 80 [RST] Seq=1 Win=0 Len=0
26	5.182460267	10.0.0.4	10.0.0.5	TCP	54 55283 → 21 [RST] Seq=1 Win=0 Len=0
27	5.182467734	10.0.0.4	10.0.0.5	TCP	54 55283 → 5900 [RST] Seq=1 Win=0 Len=0
28	5.182480464	10.0.0.4	10.0.0.5	TCP	54 55283 → 139 [RST] Seq=1 Win=0 Len=0
29	5.182507528	10.0.0.5	10.0.0.4	TCP	60 1025 → 55283 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

The command nmap -sS 10.0.0.5 conducts a stealthy SYN scan on the target host 10.0.0.5. This method identifies the status of ports without fully establishing a TCP connection. In a Wireshark capture, you will observe SYN packets sent by Nmap, SYN-ACK responses for open ports, and RST packets used to terminate the connection.

5. Scenario: You want to determine the versions of the services running on the open ports of the victim Metasploit2 VM. How would you do this using Nmap?

sudo nmap -sV <target-ip>

```
└─$ sudo nmap -sV 10.0.0.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-09 20:48 IST
Nmap scan report for 10.0.0.5
Host is up (0.00038s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:6D:D4:39 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```



2491	11.387066232	10.0.0.4	10.0.0.5	TCP	66 692 → 111 [ACK] Seq=45 Ack=477 Win=31872 Len=0 TSval=33439
2492	11.388528957	10.0.0.4	10.0.0.5	TCP	66 692 → 111 [FIN, ACK] Seq=45 Ack=477 Win=31872 Len=0 TSval=
2493	11.388844482	10.0.0.5	10.0.0.4	TCP	66 111 → 692 [FIN, ACK] Seq=477 Ack=46 Win=5792 Len=0 TSval=8
2494	11.388873381	10.0.0.4	10.0.0.5	TCP	66 692 → 111 [ACK] Seq=46 Ack=478 Win=31872 Len=0 TSval=33439
2495	11.390955248	10.0.0.4	10.0.0.5	TCP	74 35878 → 8180 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM
2496	11.391168663	10.0.0.4	10.0.0.5	TCP	74 42898 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM T
2497	11.391288544	10.0.0.5	10.0.0.4	TCP	74 8180 → 35878 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=146
2498	11.391322404	10.0.0.4	10.0.0.5	TCP	66 35878 → 8180 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=33439
2499	11.391371150	10.0.0.5	10.0.0.4	TCP	74 80 → 42898 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 S
2500	11.391377885	10.0.0.4	10.0.0.5	TCP	66 42898 → 80 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=33439601
2501	11.392868978	10.0.0.4	10.0.0.5	TCP	74 594 → 111 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS
2502	11.392936648	10.0.0.4	10.0.0.5	TCP	74 723 → 111 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS
2503	11.392979268	10.0.0.4	10.0.0.5	TCP	74 654 → 111 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS
2504	11.393010983	10.0.0.4	10.0.0.5	TCP	74 983 → 111 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TS
2505	11.393060410	10.0.0.4	10.0.0.5	HTTP	84 GET / HTTP/1.0
2506	11.393177405	10.0.0.5	10.0.0.4	TCP	74 111 → 594 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SA
2507	11.393177646	10.0.0.5	10.0.0.4	TCP	74 111 → 723 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SA
2508	11.393177736	10.0.0.5	10.0.0.4	TCP	74 111 → 654 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SA
2509	11.393177837	10.0.0.5	10.0.0.4	TCP	74 111 → 983 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SA
2510	11.393177927	10.0.0.5	10.0.0.4	TCP	66 8180 → 35878 [ACK] Seq=1 Ack=19 Win=5792 Len=0 TSval=87647
2511	11.393209531	10.0.0.4	10.0.0.5	TCP	66 594 → 111 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=33439601

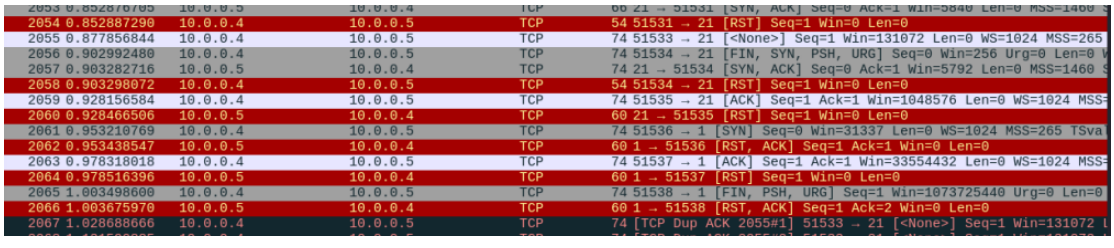
The nmap -sV command probes open ports to determine the running services and their versions. In a Wireshark capture, you will observe communication between 10.0.0.5 and 10.0.0.4, where the target

responds with software and version details. Nmap then matches these responses against its signature database to identify known services.

6. Scenario: You need to find out the operating system running on the victim Metasploit2 VM. What Nmap command will help you gather this information?

sudo nmap -O <target-ip>

```
└─$ sudo nmap -O 10.0.0.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-09 20:54 IST
Nmap scan report for 10.0.0.5
Host is up (0.00025s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:6D:D4:39 (Oracle VirtualBox virtual NIC)
```

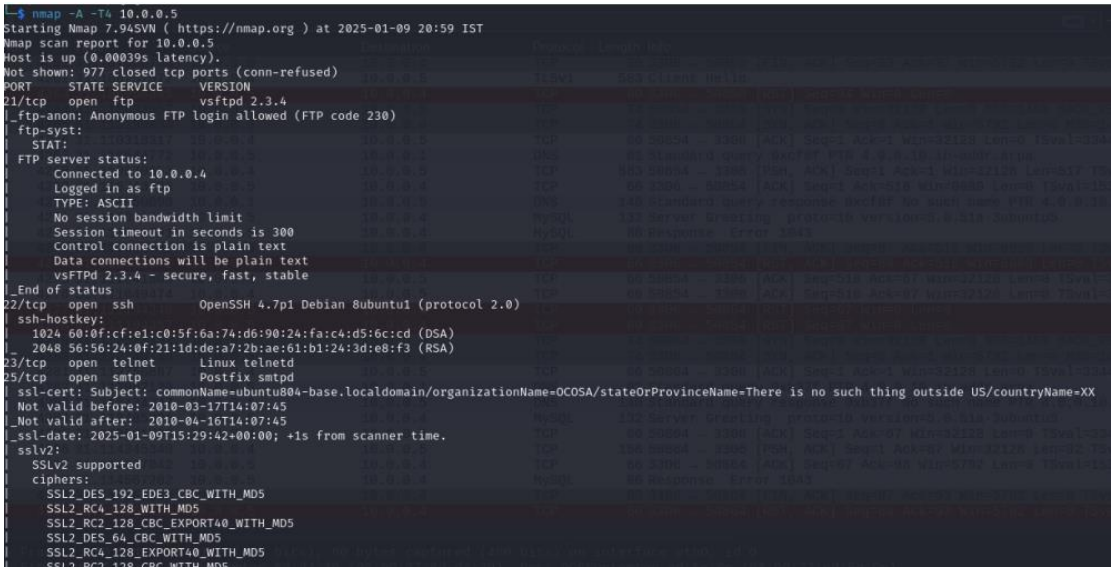


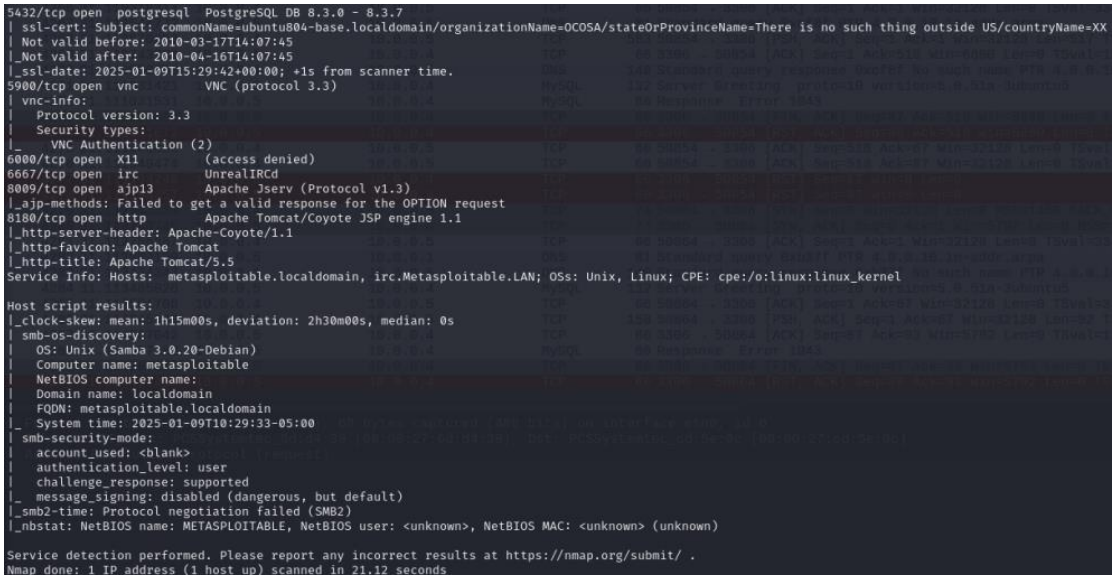
The nmap -O 10.0.0.5 command performs OS detection by sending various TCP and ICMP probes to analyze the target's response patterns. In a Wireshark capture, you will observe details such as TTL values, TCP window sizes, and specific ICMP responses, which help Nmap infer the operating system. These interactions, including SYN, ACK, RST, and ICMP packets, provide key indicators of the target's OS characteristics.

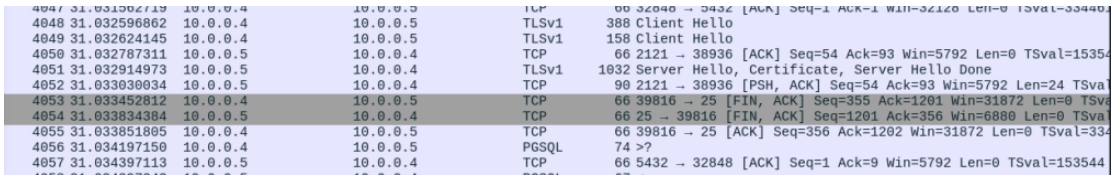
Rangineny sai kiran
CB.SC.P2CYS24011

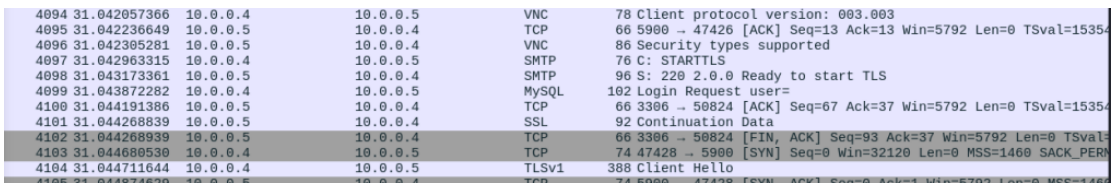
7. Scenario: You're performing a comprehensive scan of the victim Metasploit2 VM to gather information about open ports, services, operating system, and possible vulnerabilities. What Nmap command should you use?

```
sudo nmap -A -T4 <target-ip>
```







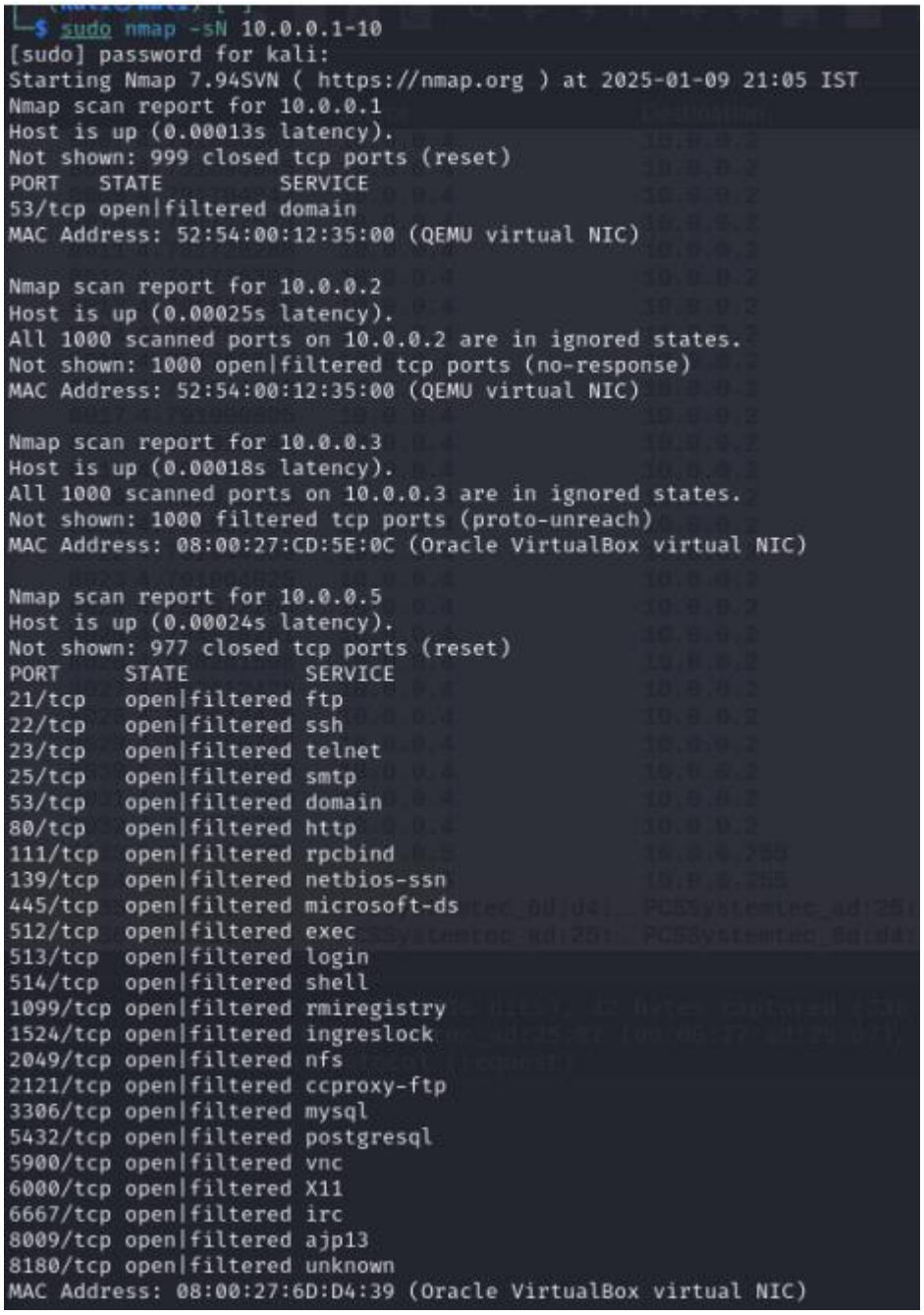


Rangineny sai kiran
CB.SC.P2CYS24011

Nmap dispatches multiple probes, including SYN, ACK, and ICMP packets, to assess the target host. It analyzes responses such as SYN-ACK for open ports and ICMP replies for OS detection. These responses are then compared against a signature database to identify running services and the operating system. The -T4 option enhances scan speed, generating detailed network traffic visible in Wireshark.

8. Scenario: You are assigned to scan a range of victim VMs within a network, specifically from the first to the tenth IP address in the subnet. Which Nmap command will help you scan this IP range to see which machines are alive or have open ports?

```
sudo nmap -sN 10.0.0.1-10
```



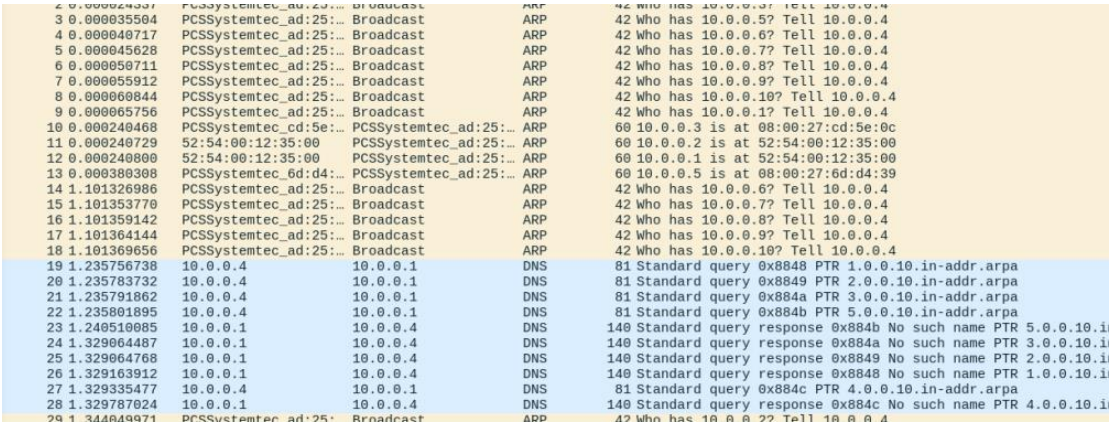
```
└─$ sudo nmap -sN 10.0.0.1-10
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-09 21:05 IST
Nmap scan report for 10.0.0.1
Host is up (0.00013s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE         SERVICE
53/tcp open|filtered domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.0.2
Host is up (0.00025s latency).
All 1000 scanned ports on 10.0.0.2 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.0.3
Host is up (0.00018s latency).
All 1000 scanned ports on 10.0.0.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:CD:5E:0C (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.0.5
Host is up (0.00024s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
23/tcp   open|filtered telnet
25/tcp   open|filtered smtp
53/tcp   open|filtered domain
80/tcp   open|filtered http
111/tcp  open|filtered rpcbind
139/tcp  open|filtered netbios-ssn
445/tcp  open|filtered microsoft-ds
512/tcp  open|filtered exec
513/tcp  open|filtered login
514/tcp  open|filtered shell
1099/tcp open|filtered rmiregistry
1524/tcp open|filtered ingreslock
2049/tcp open|filtered nfs
2121/tcp open|filtered ccproxy-ftp
3306/tcp open|filtered mysql
5432/tcp open|filtered postgresql
5900/tcp open|filtered vnc
6000/tcp open|filtered X11
6667/tcp open|filtered irc
8009/tcp open|filtered ajp13
8180/tcp open|filtered unknown
MAC Address: 08:00:27:6D:D4:39 (Oracle VirtualBox virtual NIC)
```

Rangineny sai kiran
CB.SC.P2CYS24011

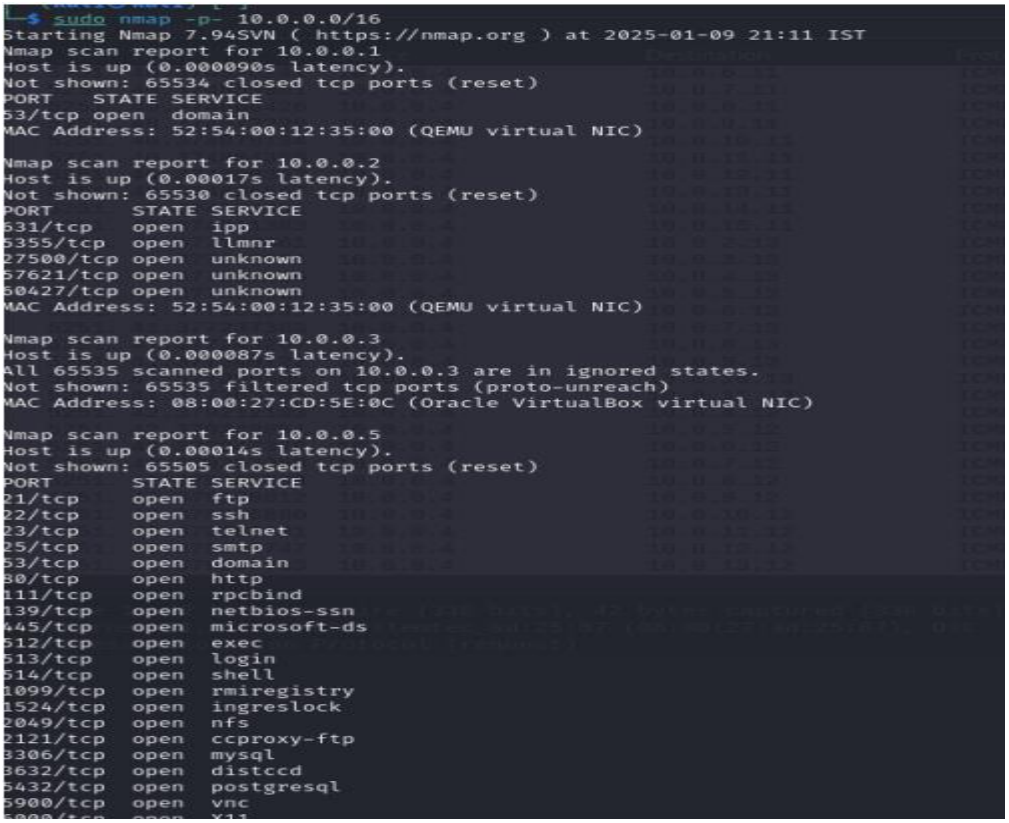


3	0.000035504	PCSSystemtec_ad:25:…	Broadcast	ARP	42 Who has 10.0.0.5? Tell 10.0.0.4
4	0.000040717	PCSSystemtec_ad:25:…	Broadcast	ARP	42 Who has 10.0.0.6? Tell 10.0.0.4
5	0.000045628	PCSSystemtec_ad:25:…	Broadcast	ARP	42 Who has 10.0.0.7? Tell 10.0.0.4
6	0.000050711	PCSSystemtec_ad:25:…	Broadcast	ARP	42 Who has 10.0.0.8? Tell 10.0.0.4
7	0.000055912	PCSSystemtec_ad:25:…	Broadcast	ARP	42 Who has 10.0.0.9? Tell 10.0.0.4
8	0.000060844	PCSSystemtec_ad:25:…	Broadcast	ARP	42 Who has 10.0.0.10? Tell 10.0.0.4
9	0.000065756	PCSSystemtec_ad:25:…	Broadcast	ARP	42 Who has 10.0.0.1? Tell 10.0.0.4
10	0.000240468	PCSSystemtec_cd:5e:…	PCSSystemtec_ad:25:…	ARP	60 10.0.0.3 is at 08:00:27:cd:5e:0c
11	0.000240729	52:54:00:12:35:00	PCSSystemtec_ad:25:…	ARP	60 10.0.0.2 is at 52:54:00:12:35:00
12	0.000240800	52:54:00:12:35:00	PCSSystemtec_ad:25:…	ARP	60 10.0.0.1 is at 52:54:00:12:35:00
13	0.000380308	PCSSystemtec_6d:d4:…	PCSSystemtec_ad:25:…	ARP	60 10.0.0.5 is at 08:00:27:6d:d4:39
14	1.101326986	PCSSystemtec_ad:25:…	Broadcast	ARP	42 Who has 10.0.0.6? Tell 10.0.0.4
15	1.101353770	PCSSystemtec_ad:25:…	Broadcast	ARP	42 Who has 10.0.0.7? Tell 10.0.0.4
16	1.101359142	PCSSystemtec_ad:25:…	Broadcast	ARP	42 Who has 10.0.0.8? Tell 10.0.0.4
17	1.101364144	PCSSystemtec_ad:25:…	Broadcast	ARP	42 Who has 10.0.0.9? Tell 10.0.0.4
18	1.101369656	PCSSystemtec_ad:25:…	Broadcast	ARP	42 Who has 10.0.0.10? Tell 10.0.0.4
19	1.235756738	10.0.0.4	10.0.0.1	DNS	81 Standard query 0x8848 PTR 1.0.0.10.in-addr.arpa
20	1.235783732	10.0.0.4	10.0.0.1	DNS	81 Standard query 0x8849 PTR 2.0.0.10.in-addr.arpa
21	1.235791862	10.0.0.4	10.0.0.1	DNS	81 Standard query 0x884a PTR 3.0.0.10.in-addr.arpa
22	1.235801895	10.0.0.4	10.0.0.1	DNS	81 Standard query 0x884b PTR 5.0.0.10.in-addr.arpa
23	1.240510085	10.0.0.1	10.0.0.4	DNS	140 Standard query response 0x884b No such name PTR 5.0.0.10.i
24	1.329064487	10.0.0.1	10.0.0.4	DNS	140 Standard query response 0x884a No such name PTR 3.0.0.10.i
25	1.329064768	10.0.0.1	10.0.0.4	DNS	140 Standard query response 0x8849 No such name PTR 2.0.0.10.i
26	1.329163912	10.0.0.1	10.0.0.4	DNS	140 Standard query response 0x8848 No such name PTR 1.0.0.10.i
27	1.329335477	10.0.0.4	10.0.0.1	DNS	81 Standard query 0x884c PTR 4.0.0.10.in-addr.arpa
28	1.329787024	10.0.0.1	10.0.0.4	DNS	140 Standard query response 0x884c No such name PTR 4.0.0.10.i

The command nmap -sN 10.0.0.1-10 performs a NULL scan by sending TCP packets with no flags set to the specified IP range. Ports that do not respond are classified as open or filtered, while those returning RST packets are considered closed. In a Wireshark capture, these packets can be observed along with their responses, but they will lack the usual SYN/ACK flags seen in standard TCP connections.

9. Scenario: You want to scan all victim machines in the 192.168.x.x subnet, including the Metasploit2 VM, to find which ones are alive and open ports. What is the best approach for scanning an entire subnet?

sudo nmap -p- 10.0.0.0/16



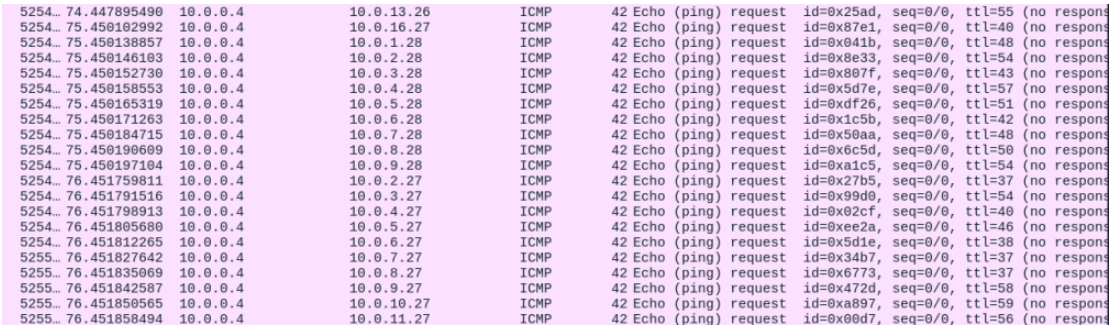
```
└─$ sudo nmap -p- 10.0.0.0/16
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-09 21:11 IST
Nmap scan report for 10.0.0.1
Host is up (0.000090s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.0.2
Host is up (0.00017s latency).
Not shown: 65530 closed tcp ports (reset)
PORT      STATE SERVICE
631/tcp   open  ipp
5355/tcp  open  llmnr
27500/tcp open  unknown
57621/tcp open  unknown
60427/tcp open  unknown
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.0.3
Host is up (0.000087s latency).
All 65535 scanned ports on 10.0.0.3 are in ignored states.
Not shown: 65535 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:CD:5E:0C (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.0.5
Host is up (0.00014s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
```

Rangineny sai kiran
CB.SC.P2CYS24011

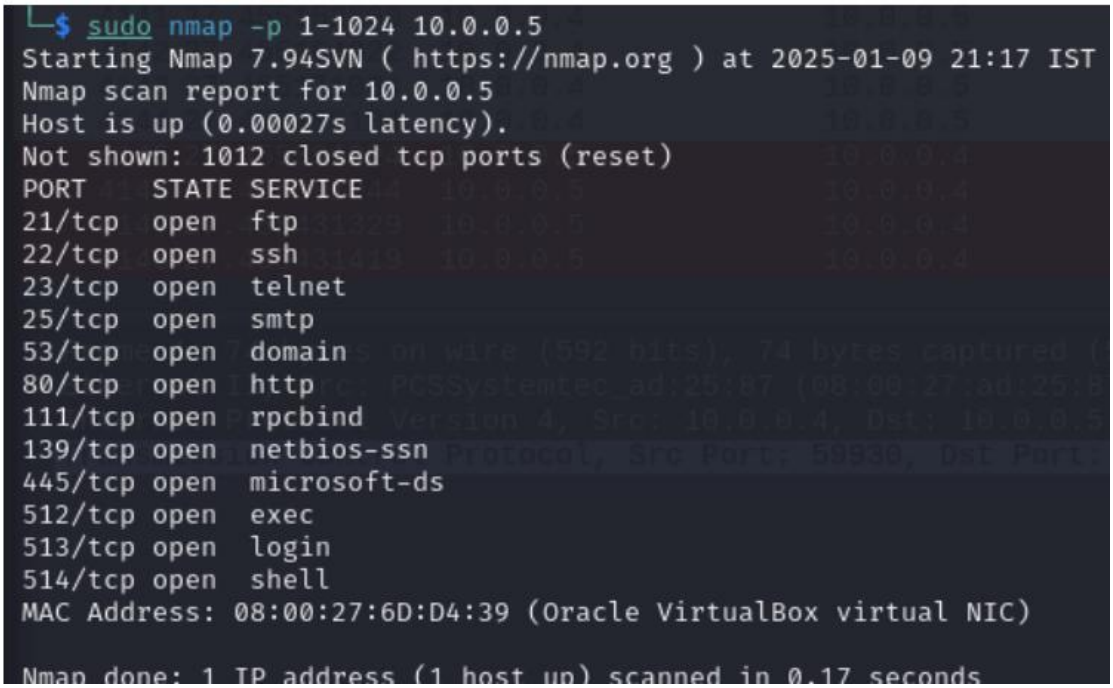


5254…	74.447895490	10.0.0.4	10.0.13.26	ICMP	42	Echo (ping) request id=0x25ad, seq=0/0, ttl=55 (no respons
5254…	75.450102992	10.0.0.4	10.0.16.27	ICMP	42	Echo (ping) request id=0x87e1, seq=0/0, ttl=40 (no respons
5254…	75.450138857	10.0.0.4	10.0.1.28	ICMP	42	Echo (ping) request id=0x041b, seq=0/0, ttl=48 (no respons
5254…	75.450146103	10.0.0.4	10.0.2.28	ICMP	42	Echo (ping) request id=0x8e33, seq=0/0, ttl=54 (no respons
5254…	75.450152730	10.0.0.4	10.0.3.28	ICMP	42	Echo (ping) request id=0x807f, seq=0/0, ttl=43 (no respons
5254…	75.450158553	10.0.0.4	10.0.4.28	ICMP	42	Echo (ping) request id=0x5d7e, seq=0/0, ttl=57 (no respons
5254…	75.450165319	10.0.0.4	10.0.5.28	ICMP	42	Echo (ping) request id=0xdf26, seq=0/0, ttl=51 (no respons
5254…	75.450171263	10.0.0.4	10.0.6.28	ICMP	42	Echo (ping) request id=0x1c5b, seq=0/0, ttl=42 (no respons
5254…	75.450184715	10.0.0.4	10.0.7.28	ICMP	42	Echo (ping) request id=0x50aa, seq=0/0, ttl=48 (no respons
5254…	75.450190609	10.0.0.4	10.0.8.28	ICMP	42	Echo (ping) request id=0x6c5d, seq=0/0, ttl=50 (no respons
5254…	75.450197104	10.0.0.4	10.0.9.28	ICMP	42	Echo (ping) request id=0xa1c5, seq=0/0, ttl=54 (no respons
5254…	76.451759811	10.0.0.4	10.0.2.27	ICMP	42	Echo (ping) request id=0x27b5, seq=0/0, ttl=37 (no respons
5254…	76.451791516	10.0.0.4	10.0.3.27	ICMP	42	Echo (ping) request id=0x99d0, seq=0/0, ttl=54 (no respons
5254…	76.451798913	10.0.0.4	10.0.4.27	ICMP	42	Echo (ping) request id=0x02cf, seq=0/0, ttl=40 (no respons
5254…	76.451805680	10.0.0.4	10.0.5.27	ICMP	42	Echo (ping) request id=0xee2a, seq=0/0, ttl=46 (no respons
5254…	76.451812265	10.0.0.4	10.0.6.27	ICMP	42	Echo (ping) request id=0x5d1e, seq=0/0, ttl=38 (no respons
5255…	76.451827642	10.0.0.4	10.0.7.27	ICMP	42	Echo (ping) request id=0x34b7, seq=0/0, ttl=37 (no respons
5255…	76.451835069	10.0.0.4	10.0.8.27	ICMP	42	Echo (ping) request id=0x6773, seq=0/0, ttl=37 (no respons
5255…	76.451842587	10.0.0.4	10.0.9.27	ICMP	42	Echo (ping) request id=0x472d, seq=0/0, ttl=58 (no respons
5255…	76.451850565	10.0.0.4	10.0.10.27	ICMP	42	Echo (ping) request id=0xa897, seq=0/0, ttl=59 (no respons
5255…	76.451858494	10.0.0.4	10.0.11.27	ICMP	42	Echo (ping) request id=0x00d7, seq=0/0, ttl=56 (no respons

The command nmap -p- 10.0.0.0/16 performs a comprehensive scan of all 65,535 ports on hosts within the 10.0.0.0/16 subnet. It detects open ports and active services by sending probes to each port on every IP address in the range. In a Wireshark capture, you will observe a high volume of ICMP echo requests, SYN packets, and corresponding SYN-ACK or RST responses, providing detailed insights into the network's active services.

10. Scenario: You want to focus your scan on checking common ports (from 1 to 1024) on the victim Metasploit2 VM to detect popular services like FTP, SSH, HTTP, etc. What Nmap command would you use to scan this range of ports?

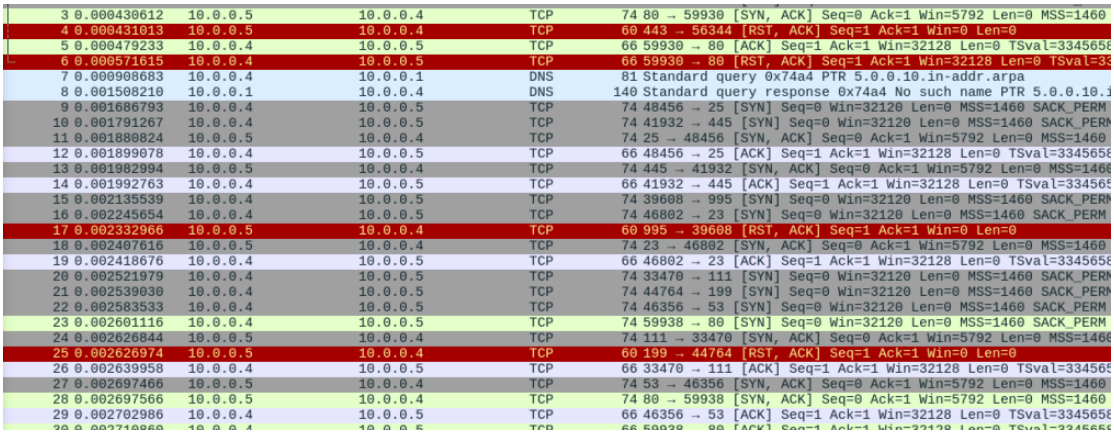
sudo nmap -p 1-1024 <target-ip>



```
└─$ sudo nmap -p 1-1024 10.0.0.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-09 21:17 IST
Nmap scan report for 10.0.0.5
Host is up (0.00027s latency).
Not shown: 1012 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  open  telnet
25/tcp  open  smtp
53/tcp  open  domain
80/tcp  open  http
111/tcp open  rpcbind
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
512/tcp open  exec
513/tcp open  login
514/tcp open  shell
MAC Address: 08:00:27:6D:D4:39 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```

Rangineny sai kiran
CB.SC.P2CYS24011



3	0.000430612	10.0.0.5	10.0.0.4	TCP	74	80 → 59930 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460
4	0.000431013	10.0.0.5	10.0.0.4	TCP	60	443 → 56344 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
5	0.000479233	10.0.0.4	10.0.0.5	TCP	66	59930 → 80 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=3345658
6	0.000571615	10.0.0.4	10.0.0.5	TCP	66	59930 → 80 [RST, ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=33
7	0.000908683	10.0.0.4	10.0.0.1	DNS	81	Standard query 0x74a4 PTR 5.0.0.10.in-addr.arpa
8	0.001508210	10.0.0.1	10.0.0.4	DNS	140	Standard query response 0x74a4 No such name PTR 5.0.0.10.i
9	0.001686793	10.0.0.4	10.0.0.5	TCP	74	48456 → 25 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM
10	0.001791267	10.0.0.4	10.0.0.5	TCP	74	41932 → 445 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM
11	0.001880824	10.0.0.5	10.0.0.4	TCP	74	25 → 48456 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460
12	0.001899078	10.0.0.4	10.0.0.5	TCP	66	48456 → 25 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=3345658
13	0.001982994	10.0.0.5	10.0.0.4	TCP	74	445 → 41932 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460
14	0.001992763	10.0.0.4	10.0.0.5	TCP	66	41932 → 445 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=334565
15	0.002135539	10.0.0.4	10.0.0.5	TCP	74	39608 → 995 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM
16	0.002245654	10.0.0.4	10.0.0.5	TCP	74	46802 → 23 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM
17	0.002332966	10.0.0.5	10.0.0.4	TCP	60	995 → 39608 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
18	0.002407616	10.0.0.5	10.0.0.4	TCP	74	23 → 46802 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460
19	0.002418676	10.0.0.4	10.0.0.5	TCP	66	46802 → 23 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=3345658
20	0.002521979	10.0.0.4	10.0.0.5	TCP	74	33470 → 111 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM
21	0.002539030	10.0.0.4	10.0.0.5	TCP	74	44764 → 199 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM
22	0.002583533	10.0.0.4	10.0.0.5	TCP	74	46356 → 53 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM
23	0.002601116	10.0.0.4	10.0.0.5	TCP	74	59938 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM
24	0.002626844	10.0.0.5	10.0.0.4	TCP	74	111 → 33470 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460
25	0.002626974	10.0.0.5	10.0.0.4	TCP	60	199 → 44764 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
26	0.002639958	10.0.0.4	10.0.0.5	TCP	66	33470 → 111 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=334565
27	0.002697466	10.0.0.5	10.0.0.4	TCP	74	53 → 46356 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460
28	0.002697566	10.0.0.5	10.0.0.4	TCP	74	80 → 59938 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460
29	0.002702986	10.0.0.4	10.0.0.5	TCP	66	46356 → 53 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=3345658

The command sudo nmap -p 1-1024 10.0.0.5 scans the first 1,024 ports on the host 10.0.0.5 to detect open services. Since these are privileged ports, sudo is required for access. In a Wireshark capture, you will observe SYN packets being sent, followed by SYN-ACK responses for open ports and RST responses for closed ones.