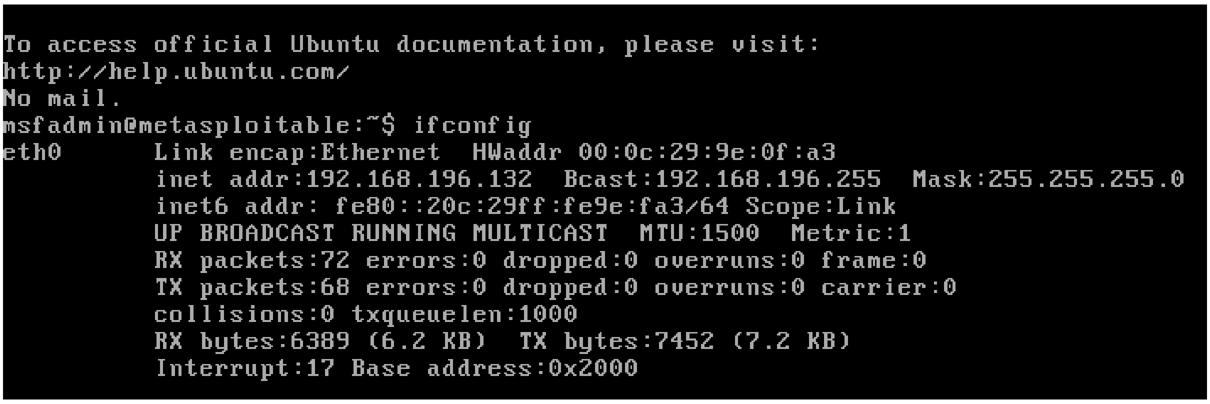
Lab 04

EXPLORING NMAP COMMANDS

Nmap command

The Network Mapper tool used for network discovery and security auditing.

Identify the IP address of the target

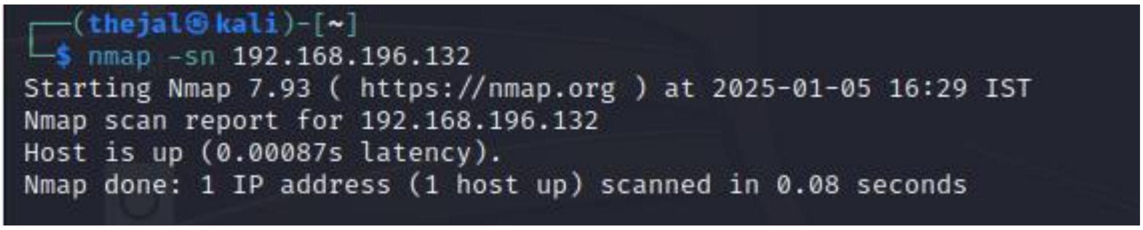


```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:9e:0f:a3
          inet addr:192.168.196.132  Bcast:192.168.196.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe9e:fa3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:72 errors:0 dropped:0 overruns:0 frame:0
          TX packets:68 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6389 (6.2 KB)  TX bytes:7452 (7.2 KB)
          Interrupt:17 Base address:0x2000
```

1.Check if Metasploit is active and responding to ping:

Syntax: nmap -sn <target_ip>

- -sn used to determine availability of a target without scanning ports.
- Nmap sends an 'ICMP echo request' packet to the target.
- If the target responds with 'ICMP echo reply', host is marked as "UP".
- If the request are blocked, nmap may send a 'TCP SYN' packet to common port.
- A 'TCP ACK' packet to check response.



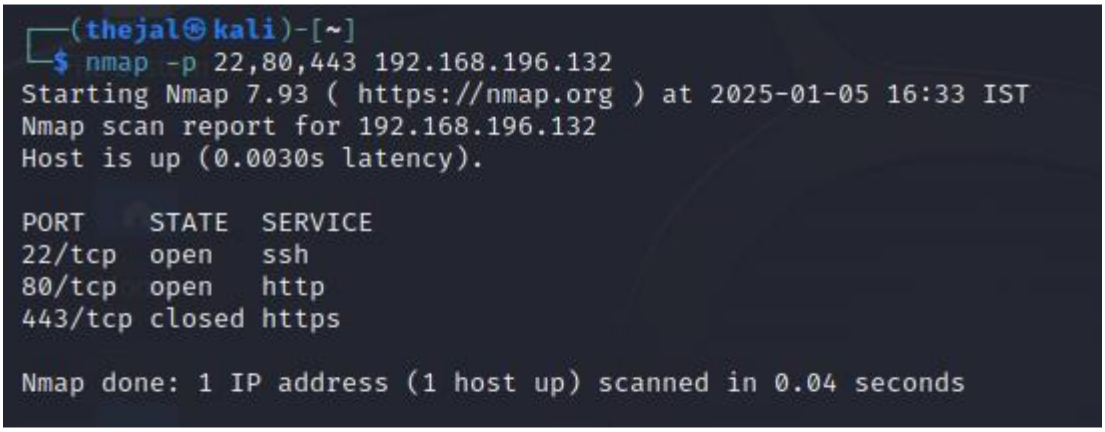
```
┌──(thejal㉿kali)-[~]
└─$ nmap -sn 192.168.196.132
Starting Nmap 7.93 ( https://nmap.org ) at 2025-01-05 16:29 IST
Nmap scan report for 192.168.196.132
Host is up (0.00087s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```

The scan did not include any port scanning or service detection, as the -sn option only performs host discovery.

2.Check for open ports

Syntax: nmap -p 22,80,443 <target_ip>

- Used to perform a targeted port scan for the specified ports 22, 80, and 443 on the target.
- -p specifies the ports to scan.
- 22 is used for SSH, 80 is for HTTP, and 443 is for HTTPS.
- Nmap will determine state of each port
    1. **Open** – A service is actively listening on the port.
    2. **Closed** – The port is accessible but no service is listening.
    3. **Filtered –** A firewall or other security device is blocking access.
- If the command run without privileges, nmap performs a ‘TCP SYN’ scan sending SYN packets to the target ports and waiting for responses.
- If runs without privileges nmap performs TCP connect scan.



```
┌──(thejal㉿kali)-[~]
└─$ nmap -p 22,80,443 192.168.196.132
Starting Nmap 7.93 ( https://nmap.org ) at 2025-01-05 16:33 IST
Nmap scan report for 192.168.196.132
Host is up (0.0030s latency).

PORT    STATE  SERVICE
22/tcp  open   ssh
80/tcp  open   http
443/tcp closed https

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
```

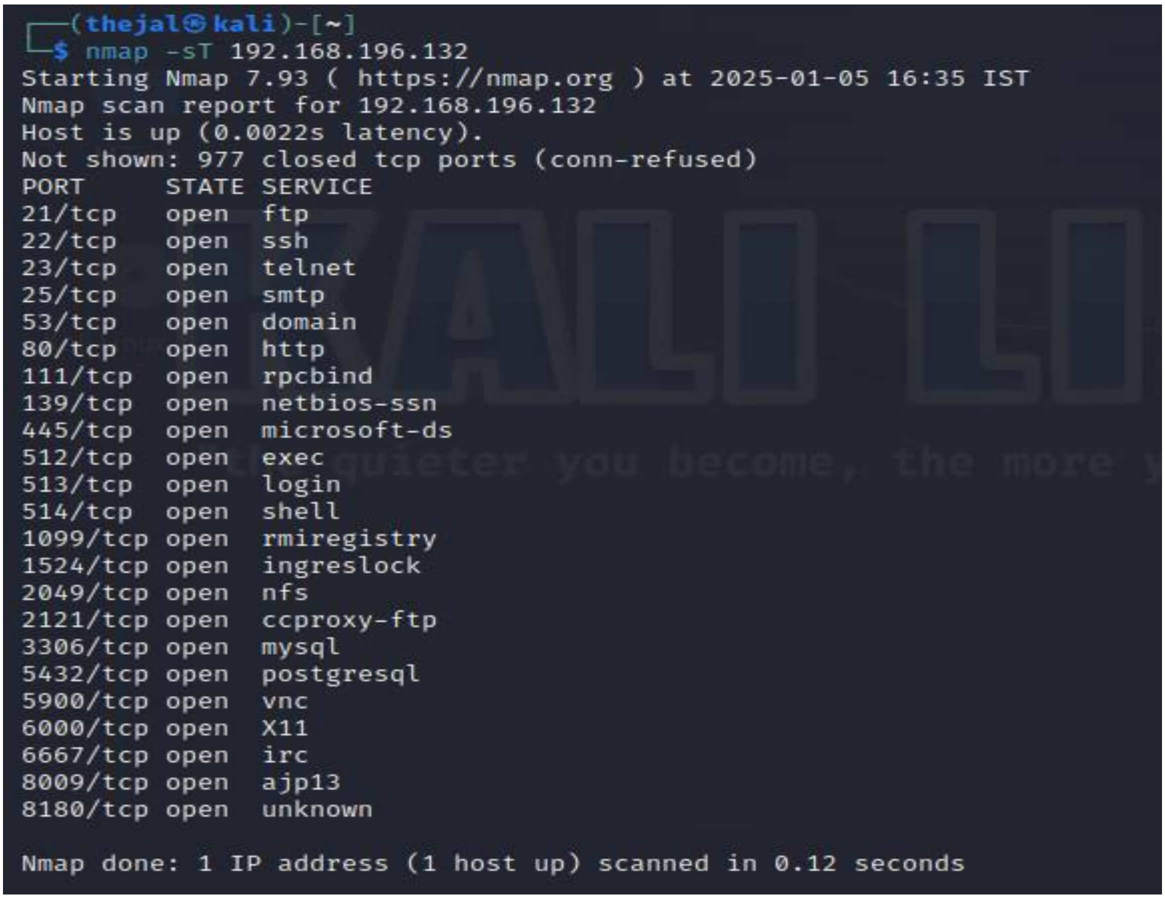
Here, SSH service is running on port 22 and accepting connections, a web server is running on port 80 and accepting HTTP requests and Port 443 is reachable but no service is listening.

3.Full TCP connection scan

Syntax: nmap -sT <target_ip>.

- Performs TCP connection scan on a specific target.
- Establishes a full TCP connection with the target host’s ports to determine their status.
- Nmap performs a full 3 way handshake for each port it scans.
    1. Sends a SYN packet to the target port.
    2. Waits for a SYN-ACK response from the target.
    3. Sends an ACK if the port is open.

- After completing or failing the handshake, nmap classifies each port as open, closed and filtered.
- And sends a RST (reset) packet to close the connection.

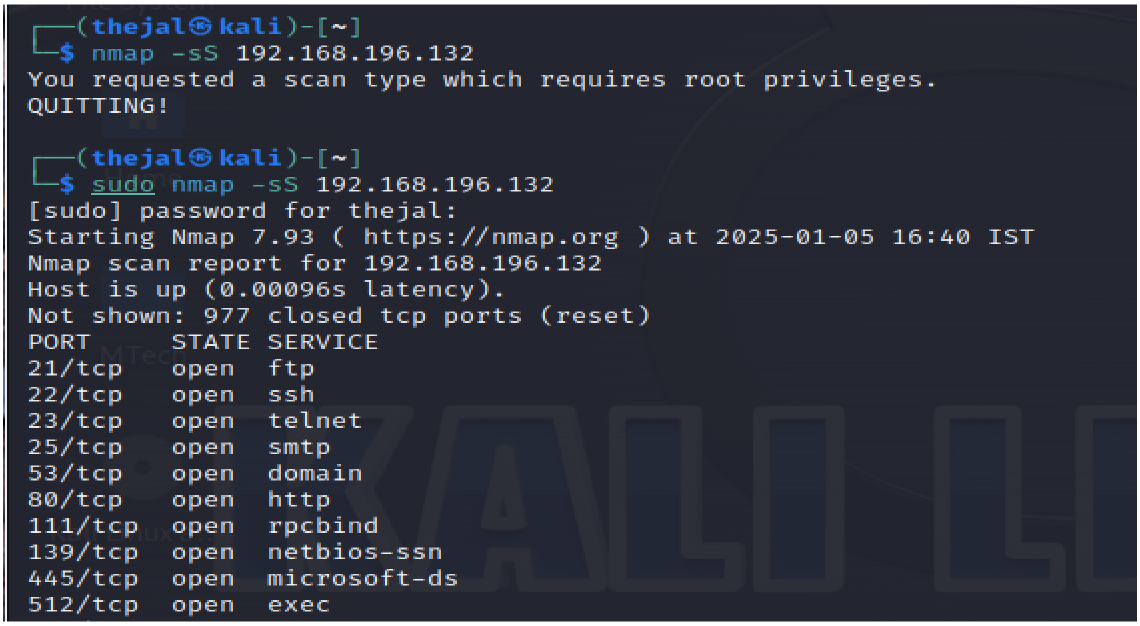


```
┌──(thejal㉿kali)-[~]
└─$ nmap -sT 192.168.196.132
Starting Nmap 7.93 ( https://nmap.org ) at 2025-01-05 16:35 IST
Nmap scan report for 192.168.196.132
Host is up (0.0022s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   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

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

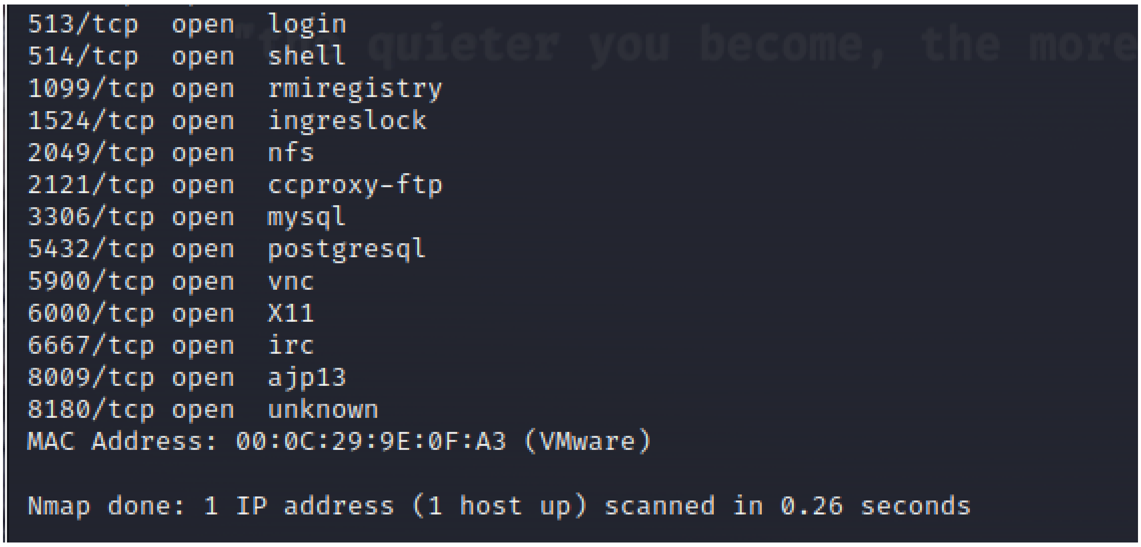
4.Stealthy scan by completing only part of the TCP handshake

Syntax: nmap-sS <target_ip>

- Instead of completing the full TCP handshake, Nmap only sends a SYN packet and evaluates the response to determine the port's state.
- Nmap sends a TCP SYN packet to the target's ports.
- The target responds with one of the following:
  1. SYN-ACK: Indicates the port is open.
  2. RST: Indicates the port is closed.
  3. No response or ICMP error: Indicates the port is filtered.
- If the target responds with a SYN-ACK (indicating the port is open), Nmap sends an RST packet instead of completing the handshake.



```
┌──(thejal㉿kali)-[~]
└─$ nmap -sS 192.168.196.132
You requested a scan type which requires root privileges.
QUITTING!

┌──(thejal㉿kali)-[~]
└─$ sudo nmap -sS 192.168.196.132
[sudo] password for thejal:
Starting Nmap 7.93 ( https://nmap.org ) at 2025-01-05 16:40 IST
Nmap scan report for 192.168.196.132
Host is up (0.00096s 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
```

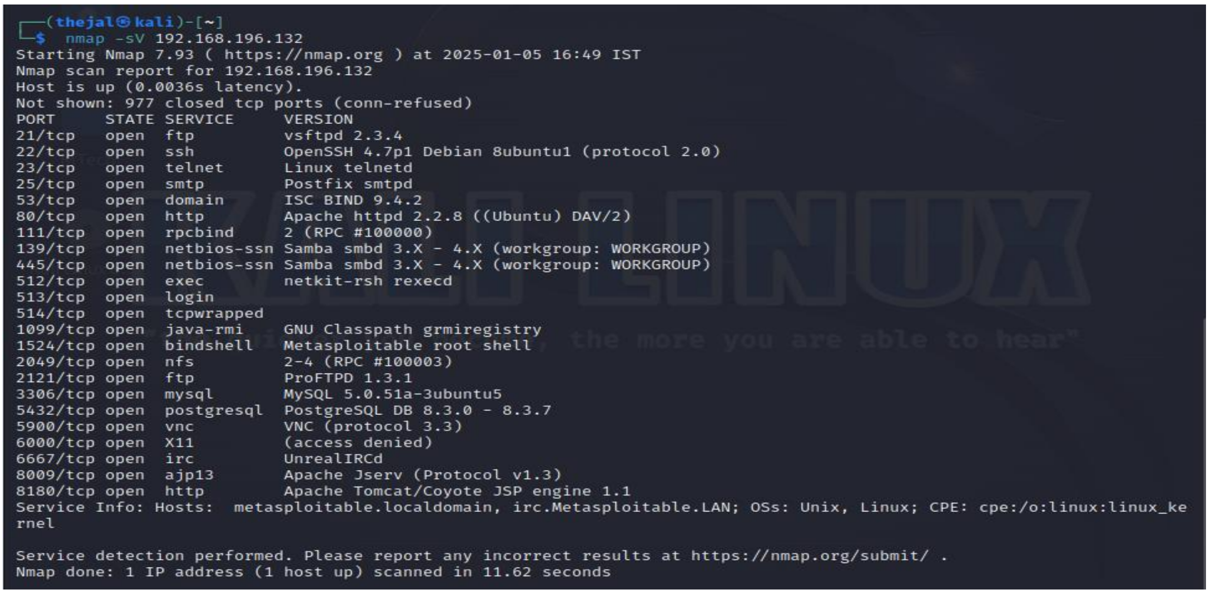


```
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:9E:0F:A3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
```

5.Determine the version of services running on the open ports

Syntax: nmap -sV <target_ip>

- -sV enables services version detection, which probes open ports to determine the specific service running and the version of the software providing the service.
- Nmap first identifies open ports using a basic port scan.
- For each open port, Nmap sends specially crafted probes to interact with the service and extract information.
- These probes analyze responses to understand the details.

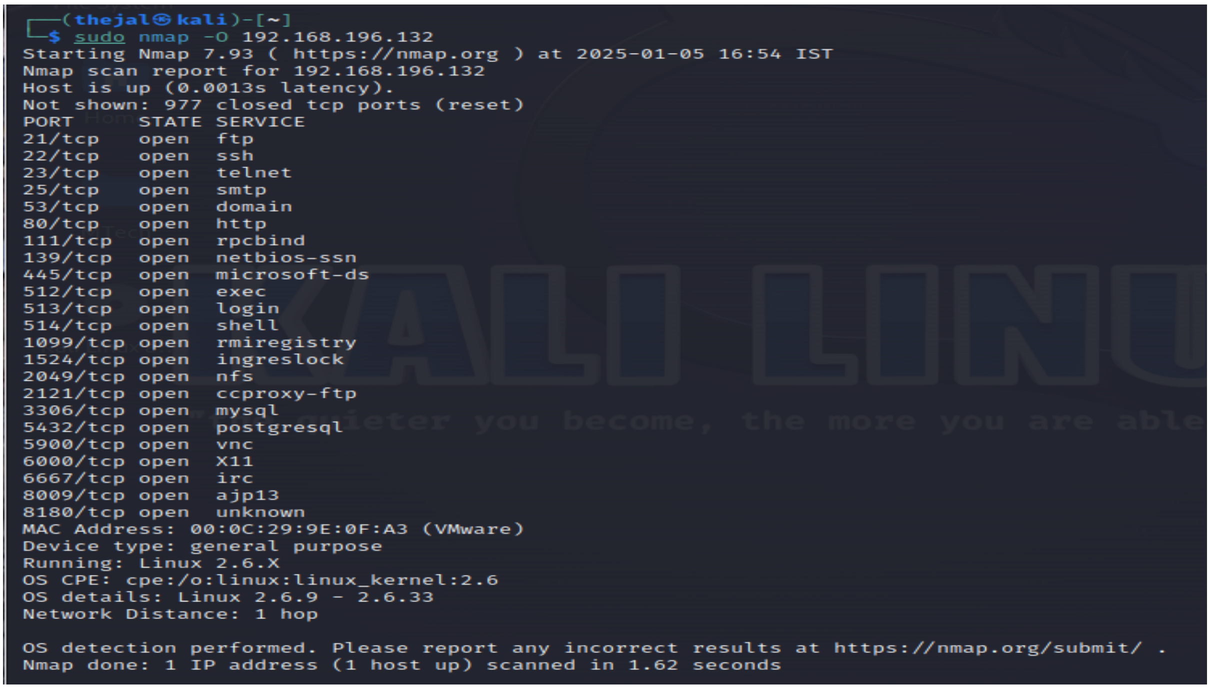


```
┌──(thejal㉿kali)-[~]
└─$ nmap -sV 192.168.196.132
Starting Nmap 7.93 ( https://nmap.org ) at 2025-01-05 16:49 IST
Nmap scan report for 192.168.196.132
Host is up (0.0036s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 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
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
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_ke
rnel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.62 seconds
```

6.OS running on the victim

Syntax: nmap -O <target_ip>

- Enables OS detection on the specified target.
- Nmap sends a variety of TCP, UDP, and ICMP packets to the target host.
- It analyze responses like TTL, window size and flags.
- Nmap compares the collected data with its built-in database of operating system fingerprints to find the best match.
- Nmap assigns a confidence score to the detected OS, indicating how likely the identified OS is correct.

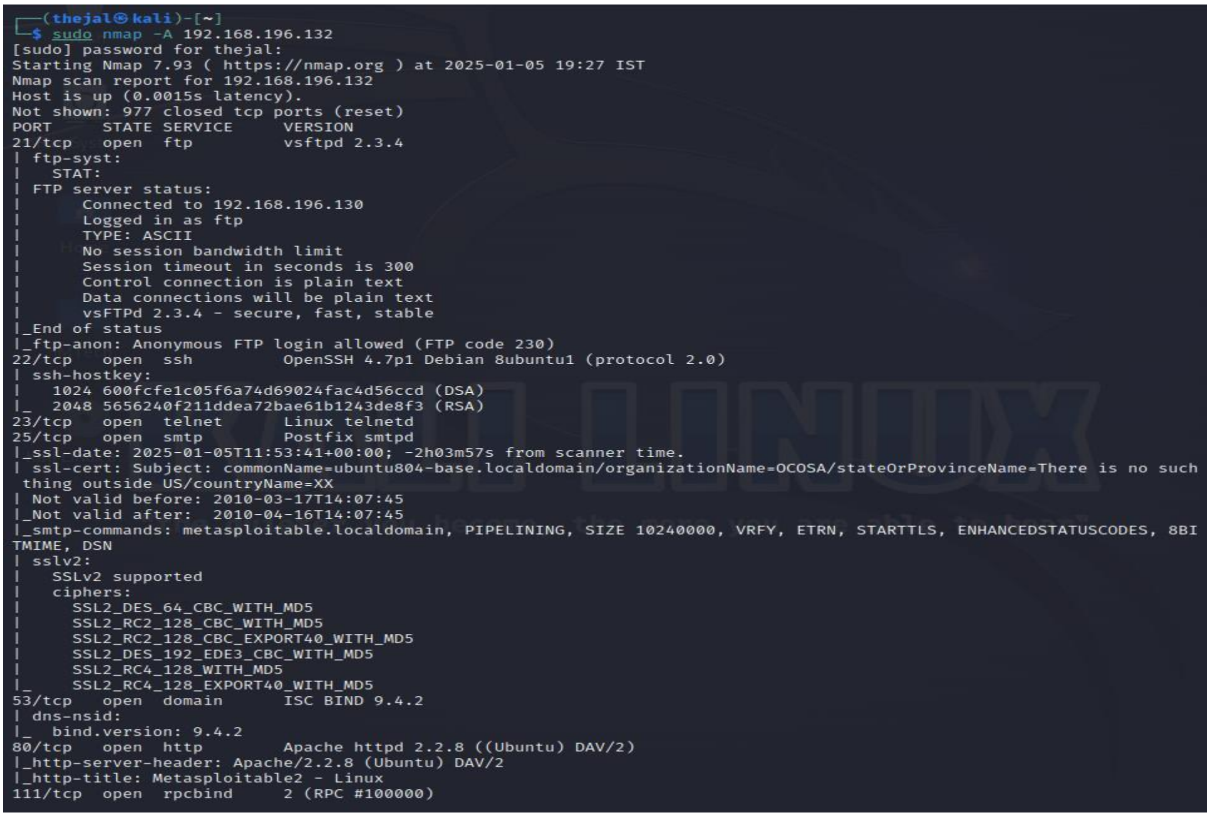


```
┌──(thejal㉿kali)-[~]
└─$ sudo nmap -O 192.168.196.132
Starting Nmap 7.93 ( https://nmap.org ) at 2025-01-05 16:54 IST
Nmap scan report for 192.168.196.132
Host is up (0.0013s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  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: 00:0C:29:9E:0F:A3 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.62 seconds
```

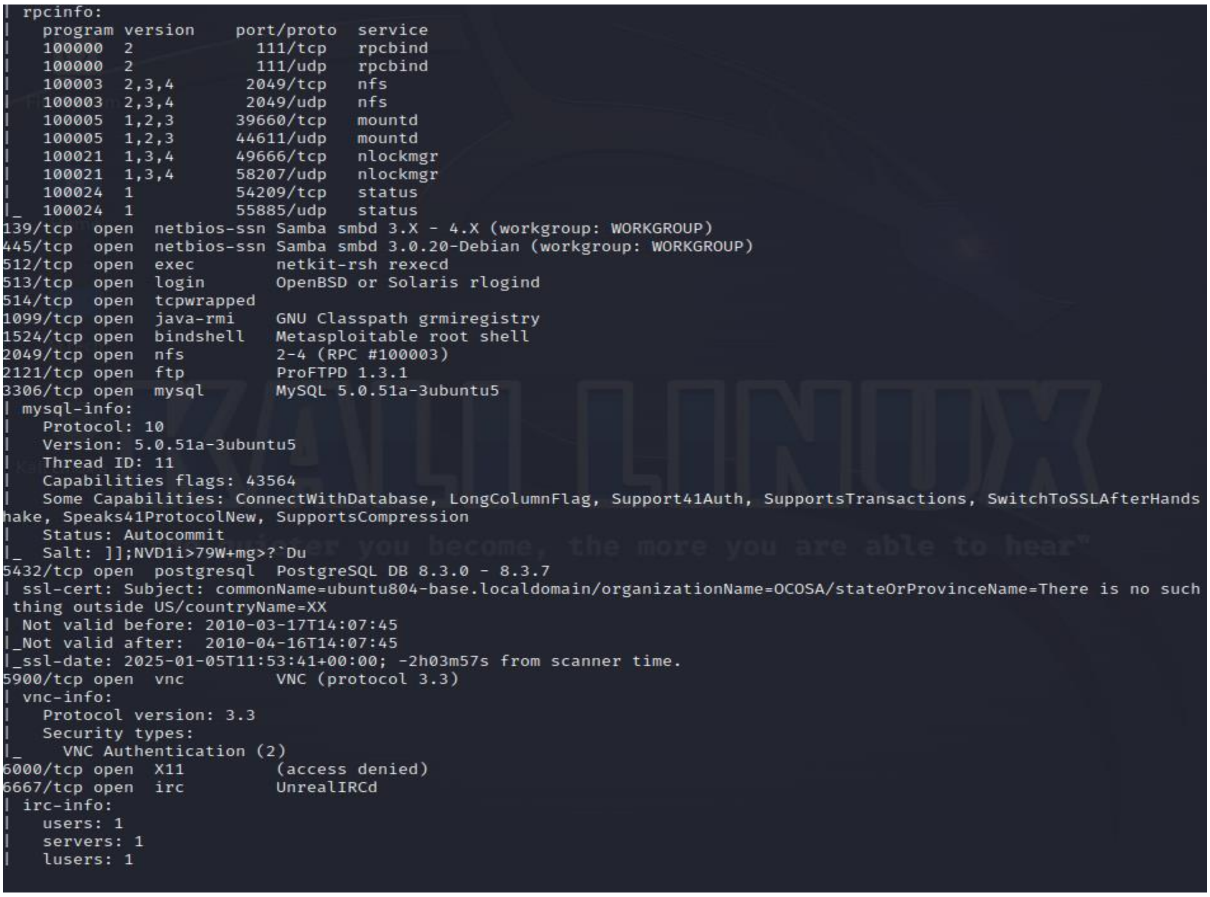
7.Gain information about open ports, services, OS and vulnerabilities

Syntax: nmap -A <target_ip>

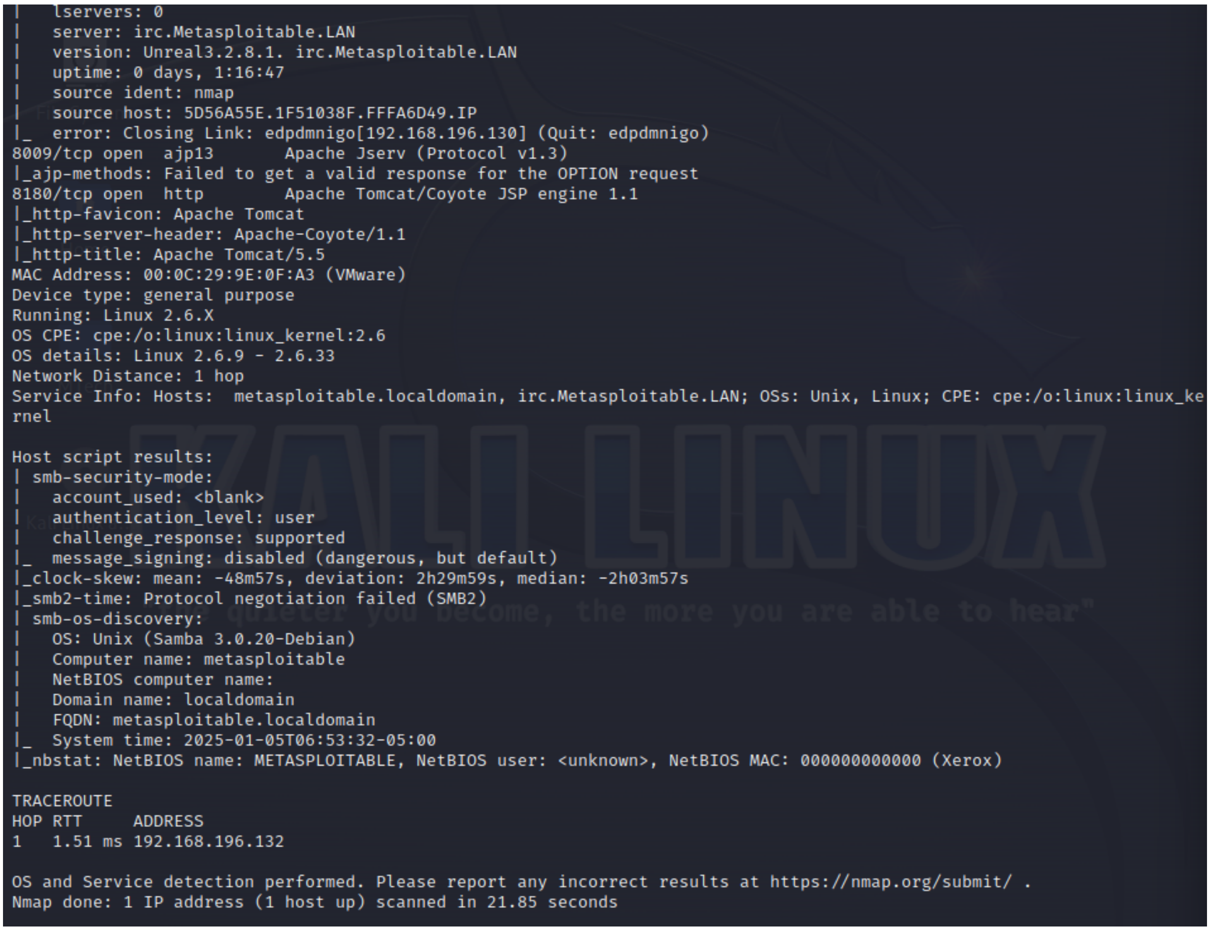
- -A enable aggressive mode that includes,
    1. OS detection – Analyzes responses to determine the OS and version.
    2. Service version detection – Probes open ports to identify services and their software versions.
    3. Script scanning.
    4. Traceroute - Maps the network path between host and the target.



```
┌──(thejal㉿kali)-[~]
└─$ sudo nmap -A 192.168.196.132
[sudo] password for thejal:
Starting Nmap 7.93 ( https://nmap.org ) at 2025-01-05 19:27 IST
Nmap scan report for 192.168.196.132
Host is up (0.0015s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.196.130
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_  2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_ssl-date: 2025-01-05T11:53:41+00:00; -2h03m57s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such
 thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BI
TMIME, DSN
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|_    SSL2_RC4_128_EXPORT40_WITH_MD5
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
```



```
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      39660/tcp   mountd
|   100005  1,2,3      44611/udp   mountd
|   100021  1,3,4      49666/tcp   nlockmgr
|   100021  1,3,4      58207/udp   nlockmgr
|   100024  1          54209/tcp   status
|_  100024  1          55885/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (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
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 11
|   Capabilities flags: 43564
|   Some Capabilities: ConnectWithDatabase, LongColumnFlag, Support41Auth, SupportsTransactions, SwitchToSSLAfterHands
hake, Speaks41ProtocolNew, SupportsCompression
|   Status: Autocommit
|_  Salt: ]];NVD1i>79W+mg>?`Du
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such
 thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2025-01-05T11:53:41+00:00; -2h03m57s from scanner time.
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
```

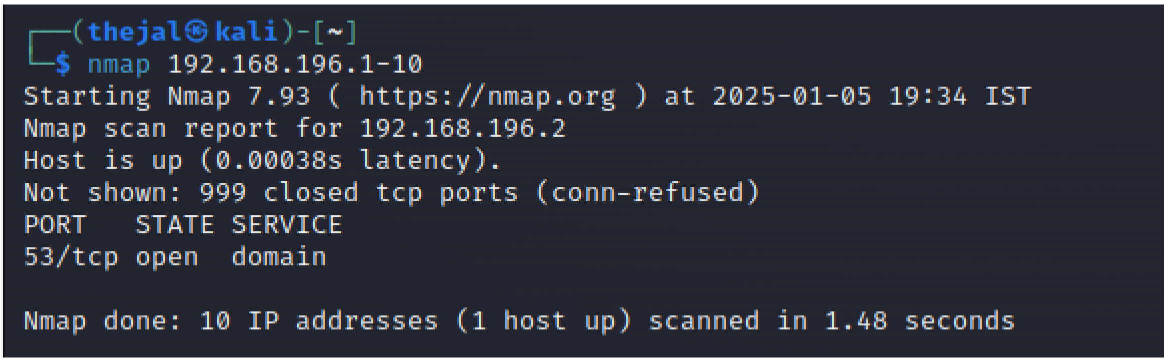


```
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 1:16:47
|   source ident: nmap
|   source host: 5D56A55E.1F51038F.FFFA6D49.IP
|_  error: Closing Link: edpdmnigo[192.168.196.130] (Quit: edpdmnigo)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
MAC Address: 00:0C:29:9E:0F:A3 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_ke
rnel

Host script results:
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: -48m57s, deviation: 2h29m59s, median: -2h03m57s
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-01-05T06:53:32-05:00
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)

TRACEROUTE
HOP RTT     ADDRESS
1   1.51 ms 192.168.196.132

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.85 seconds
```

8.Scan a range of victim VMs from the 1st to the 10th IP address in the subnet

Syntax: nmap <subnet_ip>.1-10

- Scans a range of IP addresses within the subnet, specifically from <subnet_ip>.1 to <subnet_ip>.10
- By default, Nmap performs a TCP SYN scan and scans the 1,000 most common ports on each target IP.
- Nmap first checks if each target is alive by sending ICMP Echo Requests, TCP SYN packets to port 443, or ARP requests (on local networks).
- For each reachable host, Nmap scans the specified ports or the default top 1,000 ports.
- Nmap reports details for each IP in the range.
- Lists open ports and their corresponding services

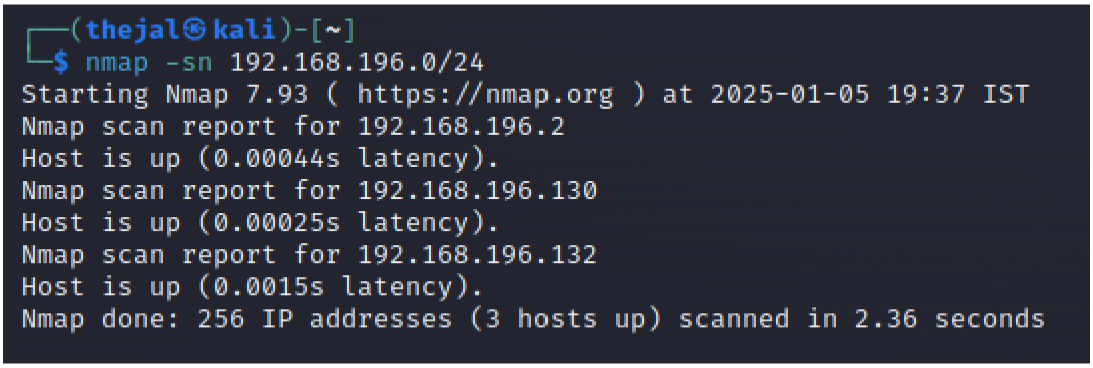


```
┌──(thejal㉿kali)-[~]
└─$ nmap 192.168.196.1-10
Starting Nmap 7.93 ( https://nmap.org ) at 2025-01-05 19:34 IST
Nmap scan report for 192.168.196.2
Host is up (0.00038s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
53/tcp open  domain

Nmap done: 10 IP addresses (1 host up) scanned in 1.48 seconds
```

9.Scan all target machines in the subnet and find which are live and open ports

Syntax: nmap -sn 192.168.0.0/24

- -sn disables port scanning and checks if hosts in the range are active by sending ICMP echo requests.

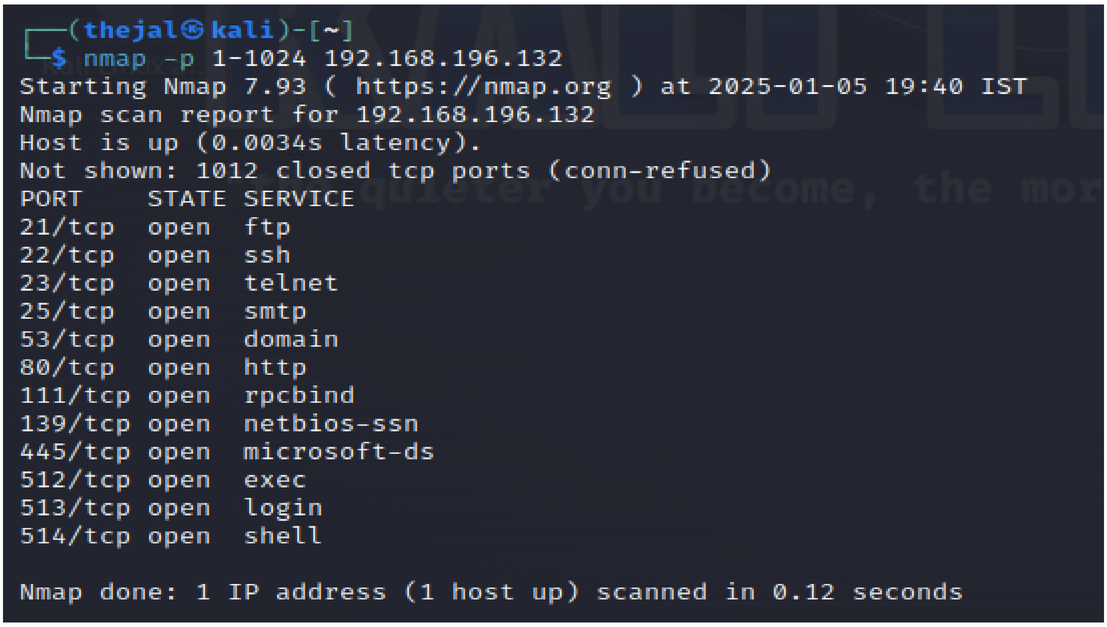


```
┌──(thejal㉿kali)-[~]
└─$ nmap -sn 192.168.196.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2025-01-05 19:37 IST
Nmap scan report for 192.168.196.2
Host is up (0.00044s latency).
Nmap scan report for 192.168.196.130
Host is up (0.00025s latency).
Nmap scan report for 192.168.196.132
Host is up (0.0015s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.36 seconds
```

10.Scan common ports 1 to 1024:

Syntax: nmap -p 1-1024 <target_ip>

- Scans all the ports in the range 1 to 1024 on the specified target ip.
- Nmap first checks if the target host is reachable using ICMP Echo Requests or TCP/ARP probes.
- Nmap probes each of the 1024 specified ports on the target to check
    - Whether the port is open, closed, or filtered.
    - The service associated with the port, if open.
- By default, Nmap performs a TCP SYN scan to check the state of each port. If not permitted, it falls back to a TCP Connect scan.



```
┌──(thejal㉿kali)-[~]
└─$ nmap -p 1-1024 192.168.196.132
Starting Nmap 7.93 ( https://nmap.org ) at 2025-01-05 19:40 IST
Nmap scan report for 192.168.196.132
Host is up (0.0034s latency).
Not shown: 1012 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

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```