

# NMAP SCAN

**Exp No :7**

**Date:08-05-2-23**

**Aim:**

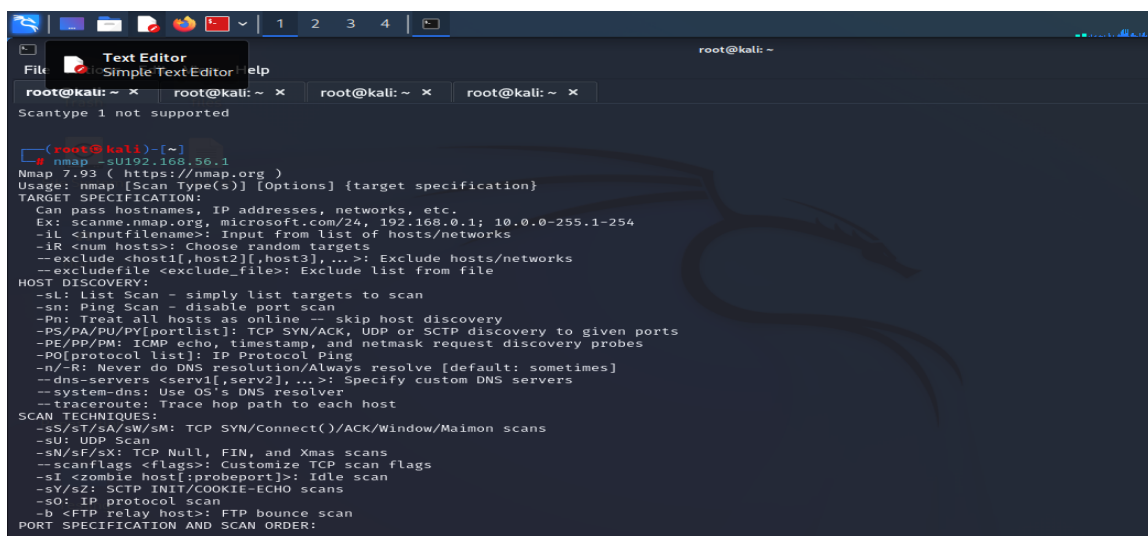
To Perform Nmap Scan Using the Kali Linux.

**Procedure :**

- Perform the Scanning Techniques.
- Scan for the Host Discovery.
- Specify the ports.
- Service and OS Detection.
- Timing and performance.
- Perform all the Nmap Scans.

**Output :**

## Scanning Techniques



```
(root@kali)-[~]
└─$ nmap -sU192.168.56.1
Nmap 7.93 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sV/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
```

```
Scantype 1 not supported

(root@kali)-[~]
# nmap -sT192.168.56.1
Nmap 7.93 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --exclude-file <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
```

```
/home/kali
File Actions Edit View Help
root@kali: ~ x root@kali: ~ x root@kali: ~ x root@kali: ~ x

(root@kali)-[~]
# nmap -sS192.168.56.1
Nmap 7.93 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
```

```
root@kali: ~  
139/tcp open  netbios-ssn  
445/tcp open  microsoft-ds  
6646/tcp open  unknown  
Nmap done: 1 IP address (1 host up) scanned in 2.69 seconds  
  
(root@kali)-[~]  
# nmap -sV 192.168.56.1  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-04 00:57 EDT  
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan  
SYN Stealth Scan Timing: About 0.50% done  
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan  
SYN Stealth Scan Timing: About 64.30% done; ETC: 00:58 (0:00:02 remaining)  
Stats: 0:00:10 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan  
Service scan Timing: About 33.33% done; ETC: 00:58 (0:00:12 remaining)  
Stats: 0:00:15 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan  
Service scan Timing: About 83.33% done; ETC: 00:58 (0:00:02 remaining)  
Stats: 0:01:03 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan  
Service scan Timing: About 83.33% done; ETC: 00:59 (0:00:12 remaining)  
Stats: 0:01:08 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan  
Service scan Timing: About 83.33% done; ETC: 00:59 (0:00:13 remaining)  
Stats: 0:02:26 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan  
Service scan Timing: About 83.33% done; ETC: 01:00 (0:00:28 remaining)  
Nmap scan report for 192.168.56.1  
Host is up (0.0042s latency).  
Not shown: 994 filtered tcp ports (no-response)  
PORT      STATE SERVICE          VERSION  
135/tcp   open  msrpc             Microsoft Windows RPC  
139/tcp   open  netbios-ssn      Microsoft Windows netbios-ssn  
445/tcp   open  microsoft-ds?       
902/tcp   open  ssl/vmware-auth  VMware Authentication Daemon 1.10 (Uses VNC, SOAP)  
912/tcp   open  vmware-auth       VMware Authentication Daemon 1.0 (Uses VNC, SOAP)  
6646/tcp  open  unknown  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

## Host Discovery

```
root@kali: ~  
Scantype 1 not supported  
  
(root@kali)-[~]  
# nmap -Pn 192.168.56.1  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-04 00:50 EDT  
WARNING: No targets were specified, so 0 hosts scanned.  
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.05 seconds  
  
(root@kali)-[~]  
# nmap -sn 192.168.56.1  
Nmap 7.93 ( https://nmap.org )  
Usage: nmap [Scan Type(s)] [Options] {target specification}  
TARGET SPECIFICATION:  
  Can pass hostnames, IP addresses, networks, etc.  
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254  
  -iL <inputfilename>: Input from list of hosts/networks  
  -iR <num hosts>: Choose random targets  
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks  
  --excludefile <exclude_file>: Exclude list from file  
HOST DISCOVERY:  
  -sl: List Scan - simply list targets to scan  
  -sn: Ping Scan - disable port scan  
  -Pn: Treat all hosts as online -- skip host discovery  
  -PS/PA/PY/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports  
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes  
  -PO[protocol list]: IP Protocol Ping  
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]  
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers  
  --system-dns: Use OS's DNS resolver  
  --traceroute: Trace hop path to each host  
SCAN TECHNIQUES:  
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans  
  -sU: UDP Scan  
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
```

```
root@kali: ~  
--privileged: Assume that the user is fully privileged  
--unprivileged: Assume the user lacks raw socket privileges  
-V: Print version number  
-h: Print this help summary page.  
EXAMPLES:  
nmap -v -A scanme.nmap.org  
nmap -v -sn 192.168.0.0/16 10.0.0.0/8  
nmap -v -iR 10000 -Pn -p 80  
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES  
Scantype 1 not supported  
  
root@kali:~# nmap -PR192.168.56.1  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-04 00:50 EDT  
WARNING: No targets were specified, so 0 hosts scanned.  
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.04 seconds  
  
root@kali:~# nmap -n 192.168.56.1  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-04 00:50 EDT  
Stats: 0:00:04 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan  
SYN Stealth Scan Timing: About 94.15% done; ETC: 00:50 (0:00:00 remaining)  
Nmap scan report for 192.168.56.1  
Host is up (0.0032s latency).  
Not shown: 994 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
902/tcp   open  iss-realsure  
912/tcp   open  apex-mesh  
6646/tcp  open  unknown  
  
Nmap done: 1 IP address (1 host up) scanned in 4.66 seconds
```

## Port Specification

```
root@kali: ~  
root@kali:~# nmap -p 1-30 192.168.56.1  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-04 00:51 EDT  
Nmap scan report for 192.168.56.1  
Host is up (0.0022s latency).  
All 30 scanned ports on 192.168.56.1 are in ignored states.  
Not shown: 30 filtered tcp ports (no-response)  
  
Nmap done: 1 IP address (1 host up) scanned in 2.60 seconds  
  
root@kali:~# nmap -p- 192.168.56.1  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-04 00:51 EDT  
Stats: 0:00:07 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan  
SYN Stealth Scan Timing: About 2.71% done; ETC: 00:55 (0:04:11 remaining)  
Stats: 0:01:55 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan  
SYN Stealth Scan Timing: About 52.78% done; ETC: 00:54 (0:01:44 remaining)  
Stats: 0:03:02 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan  
SYN Stealth Scan Timing: About 53.08% done; ETC: 00:56 (0:02:41 remaining)  
Stats: 0:03:41 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan  
SYN Stealth Scan Timing: About 53.26% done; ETC: 00:58 (0:03:14 remaining)  
Stats: 0:03:44 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan  
SYN Stealth Scan Timing: About 53.27% done; ETC: 00:58 (0:03:16 remaining)  
Stats: 0:04:36 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan  
SYN Stealth Scan Timing: About 53.51% done; ETC: 00:59 (0:04:00 remaining)  
Stats: 0:05:38 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan  
SYN Stealth Scan Timing: About 53.79% done; ETC: 01:01 (0:04:51 remaining)  
Stats: 0:06:30 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan  
SYN Stealth Scan Timing: About 54.02% done; ETC: 01:03 (0:05:32 remaining)  
Stats: 0:07:55 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan  
SYN Stealth Scan Timing: About 54.41% done; ETC: 01:05 (0:06:38 remaining)  
Stats: 0:09:17 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan  
SYN Stealth Scan Timing: About 54.76% done; ETC: 01:08 (0:07:40 remaining)  
Stats: 0:09:44 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan  
SYN Stealth Scan Timing: About 54.81% done; ETC: 01:08 (0:08:02 remaining)
```

```
Root Terminal Emulator
Opens a terminal as the root user, using sudo to ask for the password

root@kali: ~ x root@kali: ~ x root@kali: ~ x root@kali: ~ x

(root@kali)-[~]
# nmap -F 192.168.56.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-04 00:56 EDT
Nmap scan report for 192.168.56.1
Host is up (0.0013s latency).
Not shown: 96 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
6646/tcp   open  unknown

Nmap done: 1 IP address (1 host up) scanned in 2.69 seconds

(root@kali)-[~]
# nmap -sV 192.168.56.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-04 00:57 EDT
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.50% done
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 64.30% done; ETC: 00:58 (0:00:02 remaining)
Stats: 0:00:10 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 33.33% done; ETC: 00:58 (0:00:12 remaining)
Stats: 0:00:15 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 83.33% done; ETC: 00:58 (0:00:02 remaining)
Stats: 0:01:03 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 83.33% done; ETC: 00:59 (0:00:12 remaining)
Stats: 0:01:08 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 83.33% done; ETC: 00:59 (0:00:13 remaining)
Stats: 0:02:26 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 83.33% done; ETC: 01:00 (0:00:28 remaining)
Nmap scan report for 192.168.56.1
Host is up (0.0042s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc         Microsoft Windows RPC
139/tcp    open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
902/tcp    open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp    open  vmware-auth    VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
6646/tcp   open  unknown
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

## Service Version And

```
Firefox ESR
File Edit View Bookmarks History Tools Help
Browse the World Wide Web

root@kali: ~ x root@kali: ~ x root@kali: ~ x root@kali: ~ x

139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
6646/tcp   open  unknown

Nmap done: 1 IP address (1 host up) scanned in 2.69 seconds

(root@kali)-[~]
# nmap -sV 192.168.56.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-04 00:57 EDT
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.50% done
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 64.30% done; ETC: 00:58 (0:00:02 remaining)
Stats: 0:00:10 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 33.33% done; ETC: 00:58 (0:00:12 remaining)
Stats: 0:00:15 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 83.33% done; ETC: 00:58 (0:00:02 remaining)
Stats: 0:01:03 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 83.33% done; ETC: 00:59 (0:00:12 remaining)
Stats: 0:01:08 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 83.33% done; ETC: 00:59 (0:00:13 remaining)
Stats: 0:02:26 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 83.33% done; ETC: 01:00 (0:00:28 remaining)
Nmap scan report for 192.168.56.1
Host is up (0.0042s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc         Microsoft Windows RPC
139/tcp    open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
902/tcp    open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp    open  vmware-auth    VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
6646/tcp   open  unknown
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

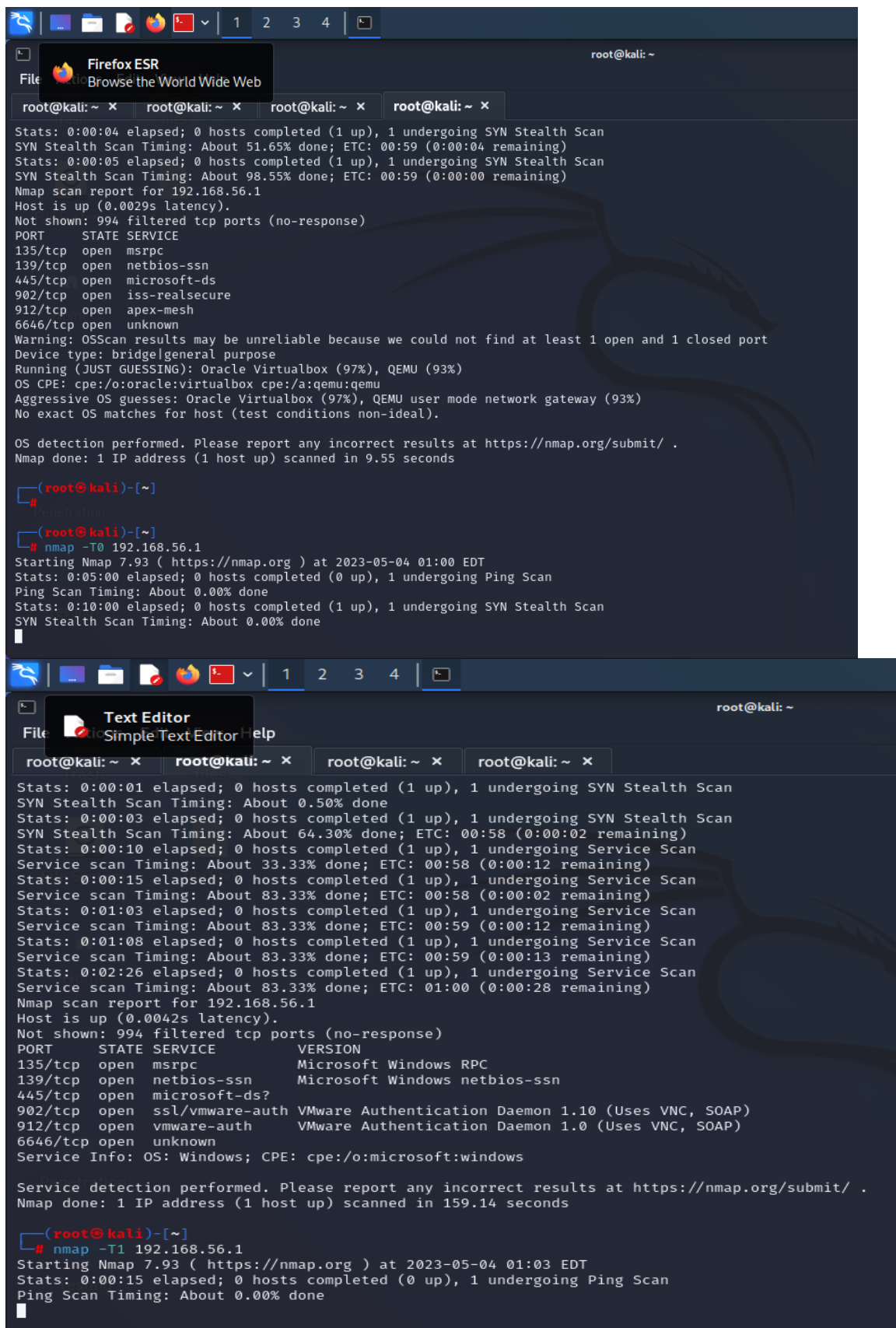


## Os Detection

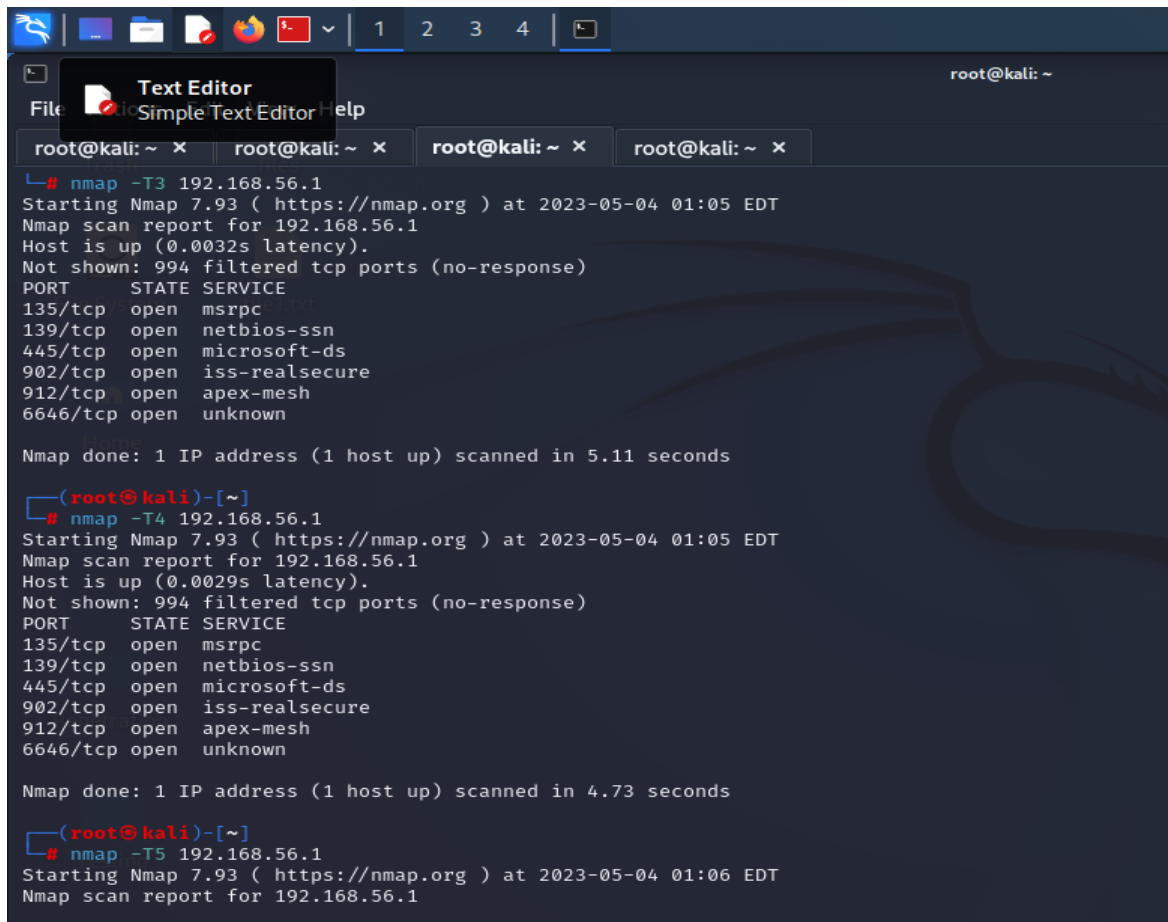
```
root@kali: ~  
# nmap -O 192.168.56.1  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-04 00:59 EDT  
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan  
SYN Stealth Scan Timing: About 0.65% done  
Stats: 0:00:04 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan  
SYN Stealth Scan Timing: About 51.65% done; ETC: 00:59 (0:00:04 remaining)  
Stats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan  
SYN Stealth Scan Timing: About 98.55% done; ETC: 00:59 (0:00:00 remaining)  
Nmap scan report for 192.168.56.1  
Host is up (0.0029s latency).  
Not shown: 994 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
902/tcp   open  iss-realsure  
912/tcp   open  apex-mesh  
6646/tcp  open  unknown  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Device type: bridge|general purpose  
Running (JUST GUESSING): Oracle Virtualbox (97%), QEMU (93%)  
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu  
Aggressive OS guesses: Oracle Virtualbox (97%), QEMU user mode network gateway (93%)  
No exact OS matches for host (test conditions non-ideal).  
  
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 9.55 seconds  
  
#  
  
# nmap -T0 192.168.56.1  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-04 01:00 EDT
```

```
root@kali: ~  
# nmap -A 192.168.56.1  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-04 00:58 EDT  
Stats: 0:00:22 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan  
Service scan Timing: About 83.33% done; ETC: 00:58 (0:00:03 remaining)  
Stats: 0:00:37 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan  
Service scan Timing: About 83.33% done; ETC: 00:59 (0:00:06 remaining)  
Stats: 0:01:47 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan  
Service scan Timing: About 83.33% done; ETC: 01:00 (0:00:20 remaining)  
Stats: 0:02:36 elapsed; 0 hosts completed (1 up), 1 undergoing Traceroute  
Traceroute Timing: About 32.26% done; ETC: 01:01 (0:00:00 remaining)  
Nmap scan report for 192.168.56.1  
Host is up (0.0019s latency).  
Not shown: 994 filtered tcp ports (no-response)  
PORT      STATE SERVICE      VERSION  
135/tcp   open  msrpc        Microsoft Windows RPC  
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn  
445/tcp   open  microsoft-ds?   
902/tcp   open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)  
912/tcp   open  vmware-auth  VMware Authentication Daemon 1.0 (Uses VNC, SOAP)  
6646/tcp  open  unknown  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Device type: bridge|general purpose  
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (92%)  
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu  
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network gateway (92%)  
No exact OS matches for host (test conditions non-ideal).  
Network Distance: 2 hops  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Host script results:  
|_ smb2-time:  
|   date: 2023-05-04T05:01:12  
|_ start_date: N/A  
|_ smb2-security-mode:
```

## Timing And Performance



```
root@kali: ~  
Firefox ESR  
File Edit View History Bookmarks Tools Help  
Browse the World Wide Web  
root@kali: ~ x root@kali: ~ x root@kali: ~ x root@kali: ~ x  
Stats: 0:00:04 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan  
SYN Stealth Scan Timing: About 51.65% done; ETC: 00:59 (0:00:04 remaining)  
Stats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan  
SYN Stealth Scan Timing: About 98.55% done; ETC: 00:59 (0:00:00 remaining)  
Nmap scan report for 192.168.56.1  
Host is up (0.0029s latency).  
Not shown: 994 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
902/tcp   open  iss-realsure  
912/tcp   open  apex-mesh  
6646/tcp  open  unknown  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Device type: bridge/general purpose  
Running (JUST GUESSING): Oracle Virtualbox (97%), QEMU (93%)  
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu  
Aggressive OS guesses: Oracle Virtualbox (97%), QEMU user mode network gateway (93%)  
No exact OS matches for host (test conditions non-ideal).  
  
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 9.55 seconds  
  
(root@kali)-[~]  
#  
  
(root@kali)-[~]  
# nmap -T0 192.168.56.1  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-04 01:00 EDT  
Stats: 0:05:00 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan  
Ping Scan Timing: About 0.00% done  
Stats: 0:10:00 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan  
SYN Stealth Scan Timing: About 0.00% done  
#  
  
root@kali: ~  
Text Editor  
File Edit View Help  
Simple Text Editor  
root@kali: ~ x root@kali: ~ x root@kali: ~ x root@kali: ~ x  
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan  
SYN Stealth Scan Timing: About 0.50% done  
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan  
SYN Stealth Scan Timing: About 64.30% done; ETC: 00:58 (0:00:02 remaining)  
Stats: 0:00:10 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan  
Service scan Timing: About 33.33% done; ETC: 00:58 (0:00:12 remaining)  
Stats: 0:00:15 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan  
Service scan Timing: About 83.33% done; ETC: 00:58 (0:00:02 remaining)  
Stats: 0:01:03 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan  
Service scan Timing: About 83.33% done; ETC: 00:59 (0:00:12 remaining)  
Stats: 0:01:08 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan  
Service scan Timing: About 83.33% done; ETC: 00:59 (0:00:13 remaining)  
Stats: 0:02:26 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan  
Service scan Timing: About 83.33% done; ETC: 01:00 (0:00:28 remaining)  
Nmap scan report for 192.168.56.1  
Host is up (0.0042s latency).  
Not shown: 994 filtered tcp ports (no-response)  
PORT      STATE SERVICE      VERSION  
135/tcp   open  msrpc        Microsoft Windows RPC  
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn  
445/tcp   open  microsoft-ds?   
902/tcp   open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)  
912/tcp   open  vmware-auth  VMware Authentication Daemon 1.0 (Uses VNC, SOAP)  
6646/tcp  open  unknown  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 159.14 seconds  
  
(root@kali)-[~]  
# nmap -T1 192.168.56.1  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-04 01:03 EDT  
Stats: 0:00:15 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan  
Ping Scan Timing: About 0.00% done  
#
```



```
(root@kali)~  
# nmap -T3 192.168.56.1  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-04 01:05 EDT  
Nmap scan report for 192.168.56.1  
Host is up (0.0032s latency).  
Not shown: 994 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
902/tcp   open  iss-realsure  
912/tcp   open  apex-mesh  
6646/tcp  open  unknown  
  
Nmap done: 1 IP address (1 host up) scanned in 5.11 seconds  
  
(root@kali)~  
# nmap -T4 192.168.56.1  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-04 01:05 EDT  
Nmap scan report for 192.168.56.1  
Host is up (0.0029s latency).  
Not shown: 994 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
902/tcp   open  iss-realsure  
912/tcp   open  apex-mesh  
6646/tcp  open  unknown  
  
Nmap done: 1 IP address (1 host up) scanned in 4.73 seconds  
  
(root@kali)~  
# nmap -T5 192.168.56.1  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-04 01:06 EDT  
Nmap scan report for 192.168.56.1
```

## Result :

Hence the Nmap Scan using the KaliLinux is Performed.