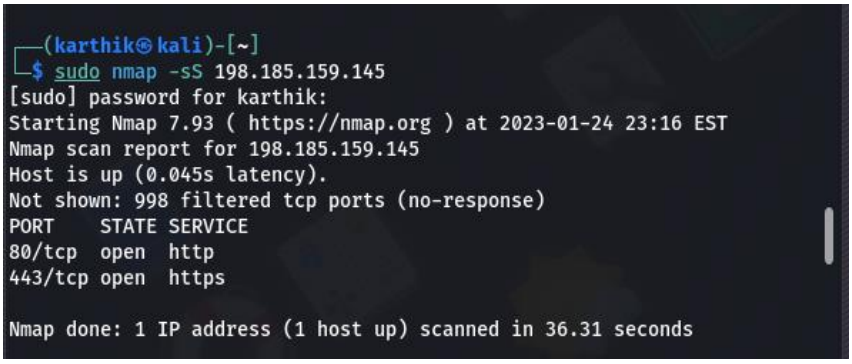
EXERCISE 1: Nmap scan

Scanning Techniques

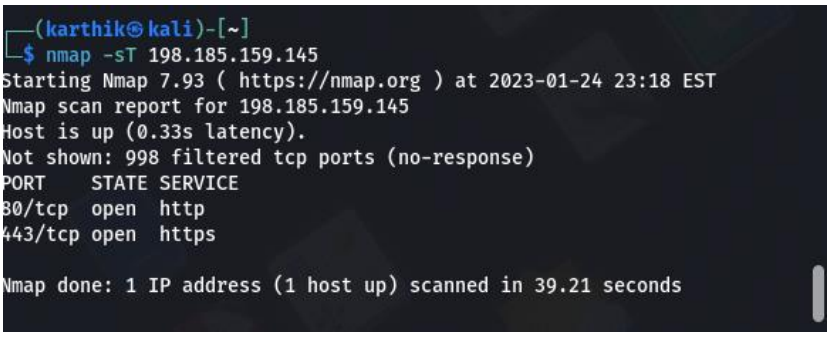
Flag	Use	Example
-sS	**TCP syn port scan**	**Nmap -sS 198.185.159.145**
-sT	**TCP connect port scan**	**Nmap -sT 198.185.159.145**
–sU	**UDP port scan**	**Nmap –sU 198.185.159.145**
–sA	**TCP ack port scan**	**Nmap –sA 198.185.159.145**

❖OUTPUT:

-sS



-sT



-sU

```
┌──(karthik㉿kali)-[~]
└─$ sudo nmap -sU 192.185.159.145
[sudo] password for karthik:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-24 23:48 EST
Nmap scan report for 192.185.159.145
Host is up (0.00043s latency).
Not shown: 999 filtered udp ports (net-unreach)
PORT   STATE         SERVICE
67/udp open|filtered dhcps

Nmap done: 1 IP address (1 host up) scanned in 15.31 seconds
```

-sA

```
┌──(karthik㉿kali)-[~]
└─$ sudo nmap -sA 192.185.159.145
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-24 23:52 EST
Nmap scan report for 192.185.159.145
Host is up (0.00061s latency).
All 1000 scanned ports on 192.185.159.145 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 13.47 seconds
```

- **HOST DISCOVERY:**

-Pn	only port scan	Nmap –Pn 198.185.159.145
-sn	only host discover	Nmap -sn 198.185.159.145
-PR	Arp discovery on a local network	Nmap -PR 198.185.159.145
-n	disable DNS resolution	Nmap -n 198.185.159.145

-Pn:

```
┌──(karthik㉿kali)-[~]
└─$ sudo nmap -Pn 198.185.159.145
[sudo] password for karthik:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-25 00:20 EST
Nmap scan report for 198.185.159.145
Host is up (0.52s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 45.59 seconds
```

-sn:

```
┌──(karthik㉿kali)-[~]
└─$ sudo nmap -sn 198.185.159.145
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-25 00:22 EST
Nmap scan report for 198.185.159.145
Host is up (0.00060s latency).
Nmap done: 1 IP address (1 host up) scanned in 13.17 seconds
```

-PR:

```
┌──(karthik㉿kali)-[~]
└─$ sudo nmap -PR 198.185.159.145
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-25 00:24 EST
Nmap scan report for 198.185.159.145
Host is up (0.033s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
```

-n:

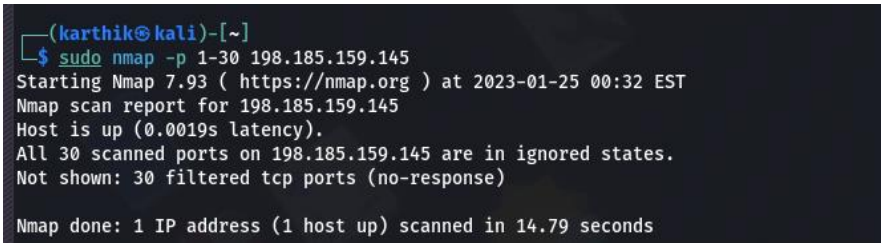
```
┌──(karthik㉿kali)-[~]
└─$ sudo nmap -n 198.185.159.145
[sudo] password for karthik:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-25 00:27 EST
Nmap scan report for 198.185.159.145
Host is up (0.036s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 28.15 seconds
```

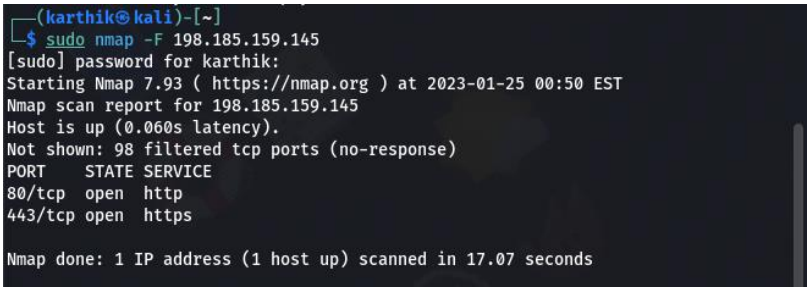
Port Specification

Flag	Use	Example
-p	specify a port or port range	Nmap -p 1-30 198.185.159.145
-p-	scan all ports	Nmap -p- 198.185.159.145
F	fast port scan	Nmap -F 198.185.159.145

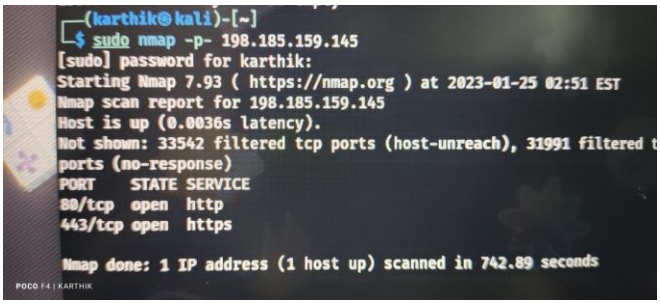
-p 1-30:



-F:



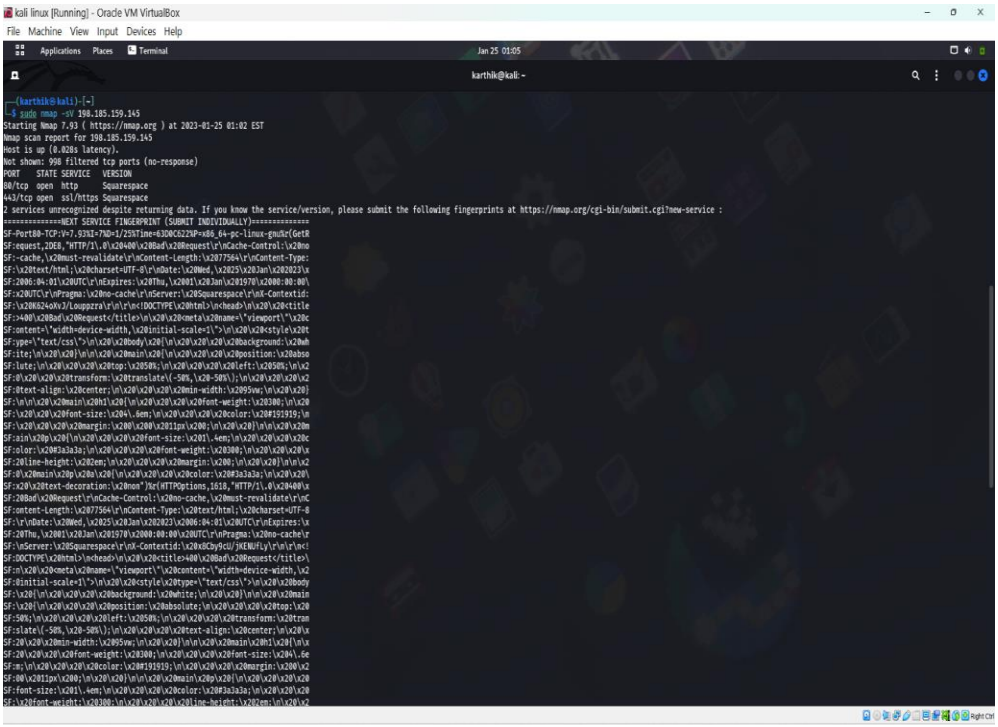
-p-



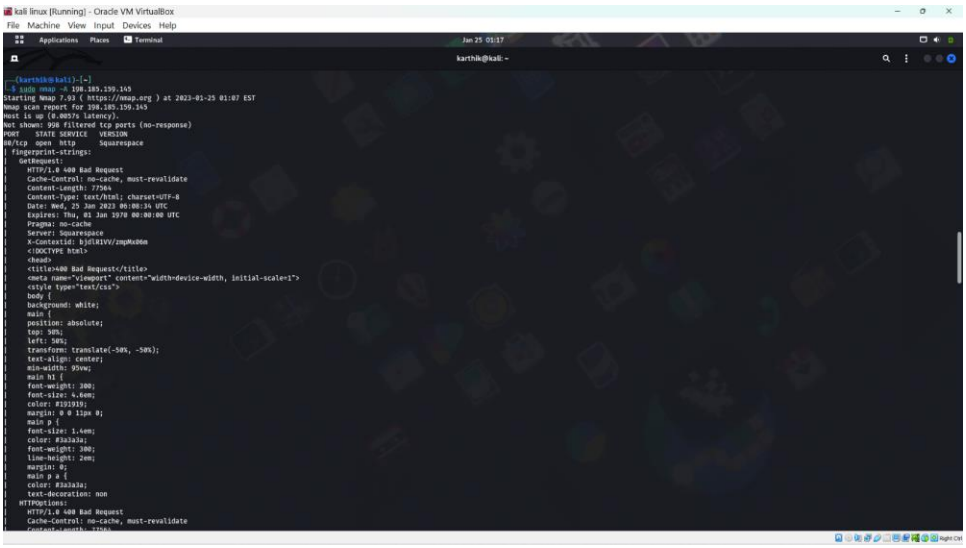
Service Version and OS Detection

Flag	Use	Example
-sV	detect the version of services running	Nmap -sV 198.185.159.145
-A	aggressive scan	Nmap -A 198.185.159.145
-O	detect operating system of the target	Nmap -O 198.185.159.145

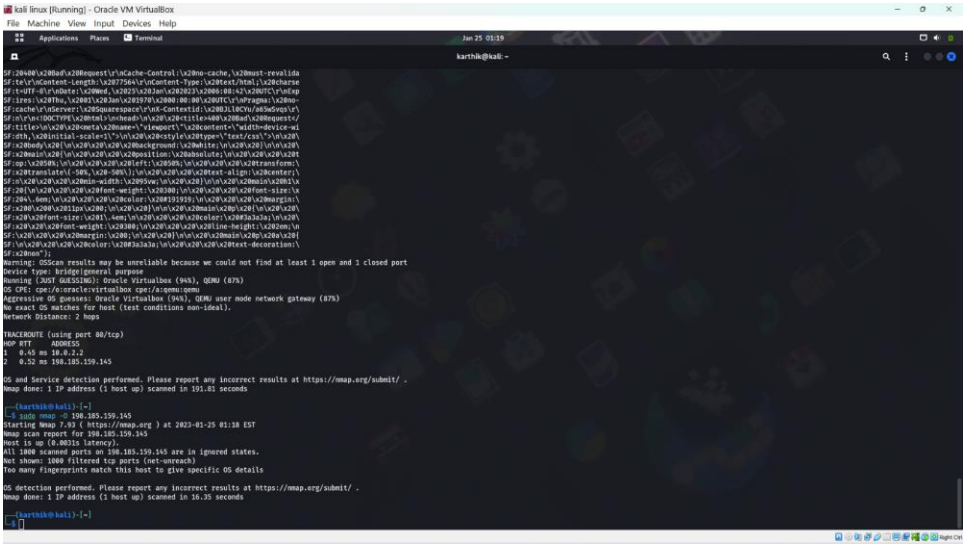
-sV:



-A:


kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
Jan 25 01:17
karthik@kali: ~
┌──(karthik㉿kali)-[~]
└─$ sudo nmap -O 198.185.159.145
Starting Nmap 7.93 (https://nmap.org) at 2023-01-25 01:07 EST
Nmap scan report for 198.185.159.145
Host is up (0.0057s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
80/tcp open http Squarespace
| fingerprint-strings:
| GetRequest:
| HTTP/1.0 400 Bad Request
| Cache-Control: no-cache, must-revalidate
| Content-Length: 7754
| Content-Type: text/html; charset=UTF-8
| Date: Wed, 25 Jan 2023 06:08:34 UTC
| Expires: Thu, 01 Jan 1970 00:00:00 UTC
| Pragma: no-cache
| Server: Squarespace
| X-Contextid: bjdl4IVV/zmpMx0bm
| <!DOCTYPE html>
| <head>
| <title>400 Bad Request</title>
| <meta name="viewport" content="width=device-width, initial-scale=1">
| <style type="text/css">
| body {
| background: white;
| main {
| position: absolute;
| top: 50%;
| left: 50%;
| transform: translate(-50%, -50%);
| text-align: center;
| min-width: 95vw;
| main h1 {
| font-weight: 300;
| font-size: 4.6em;
| color: #191919;
| margin: 0 0 11px 0;
| main p {
| font-size: 1.4em;
| color: #3a3a3a;
| font-weight: 300;
| line-height: 2em;
| margin: 0;
| main p a {
| color: #3a3a3a;
| text-decoration: non
| HTTPOptions:
| HTTP/1.0 400 Bad Request
| Cache-Control: no-cache, must-revalidate

-0:


kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
Jan 25 01:19
karthik@kali: ~
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 (94%), QEMU (87%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (94%), QEMU user mode network gateway (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 0.45 ms 10.0.2.2
2 0.52 ms 198.185.159.145
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 191.81 seconds
┌──(karthik㉿kali)-[~]
└─$ sudo nmap -O 198.185.159.145
Starting Nmap 7.93 (https://nmap.org) at 2023-01-25 01:18 EST
Nmap scan report for 198.185.159.145
Host is up (0.00315 latency).
All 1000 scanned ports on 198.185.159.145 are in ignored states.
Not shown: 1000 filtered tcp ports (net-unreach)
Too many fingerprints match this host to give specific OS details
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.35 seconds
┌──(karthik㉿kali)-[~]
└─$