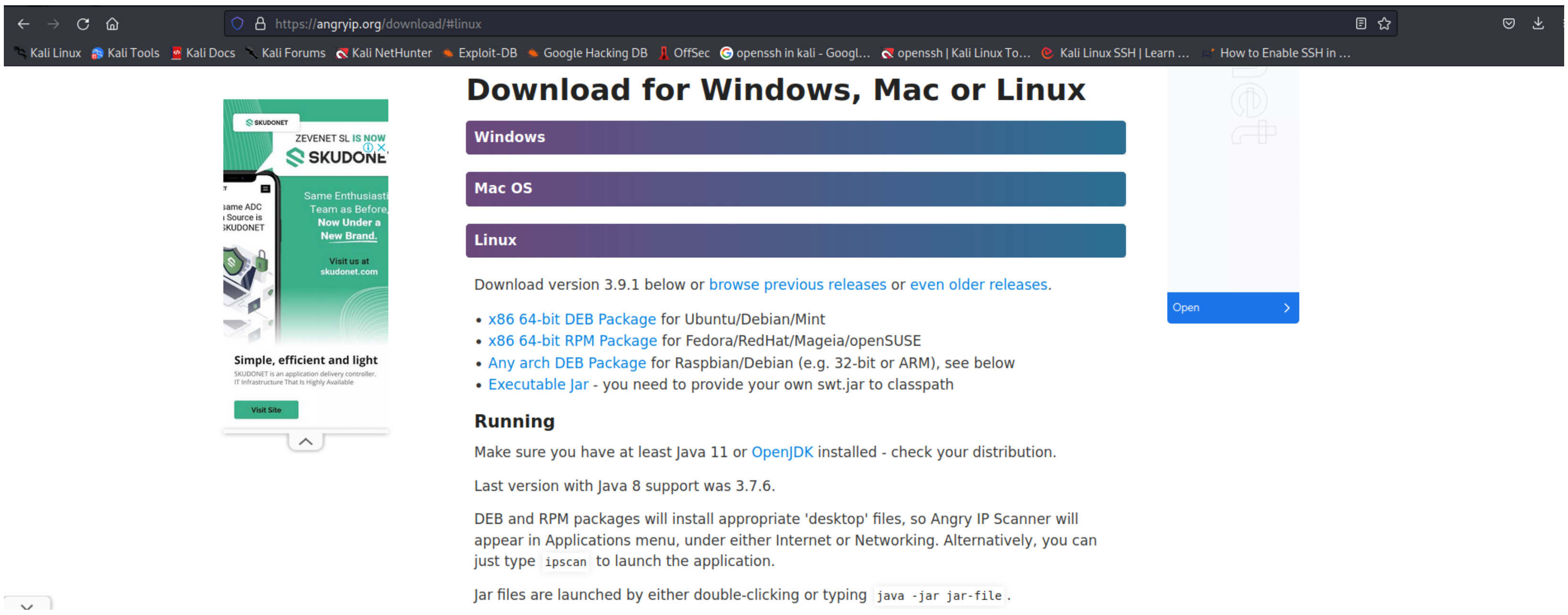
NETWORK SCANNING

Download angry Ip Scanner

https://angryip.org/download/#google_vignette


https://angryip.org/download/#linux
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
openssh in kali - Googl...
openssh | Kali Linux To...
Kali Linux SSH | Learn ...
How to Enable SSH in ...
ZEVENET SL IS NOW SKUDONET
Simple, efficient and light
Visit Site
Open

Download for Windows, Mac or Linux

Windows

Mac OS

Linux

Download version 3.9.1 below or browse previous releases or even older releases.

- x86 64-bit DEB Package for Ubuntu/Debian/Mint
- x86 64-bit RPM Package for Fedora/RedHat/Mageia/openSUSE
- Any arch DEB Package for Raspbian/Debian (e.g. 32-bit or ARM), see below
- Executable Jar - you need to provide your own swt.jar to classpath

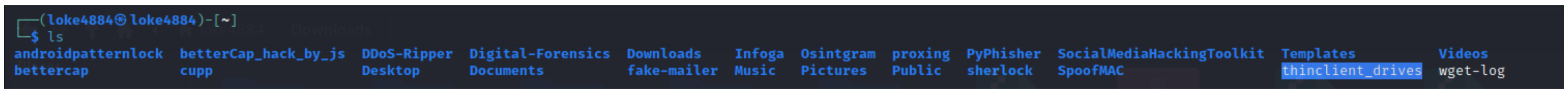
Running

Make sure you have at least Java 11 or OpenJDK installed - check your distribution.

Last version with Java 8 support was 3.7.6.

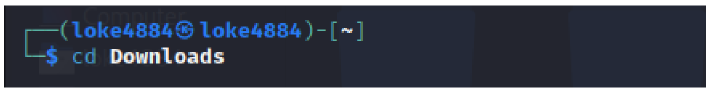
DEB and RPM packages will install appropriate 'desktop' files, so Angry IP Scanner will appear in Applications menu, under either Internet or Networking. Alternatively, you can just type `ipscan` to launch the application.

Jar files are launched by either double-clicking or typing `java -jar jar-file`.

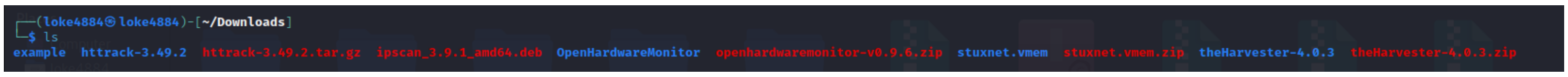


```
┌──(loke4884㉿loke4884)-[~]
└─$ ls
androidpatternlock  betterCap_hack_by_js  DDoS-Ripper  Digital-Forensics  Downloads    Infoga  Osintgram  proxing  PyPhisher  SocialMediaHackingToolkit  Templates          Videos
bettercap           cupp                  Desktop      Documents          fake-mailer  Music   Pictures   Public   sherlock   SpoofMAC                   thinclient_drives  wget-log
```

Go o downloads

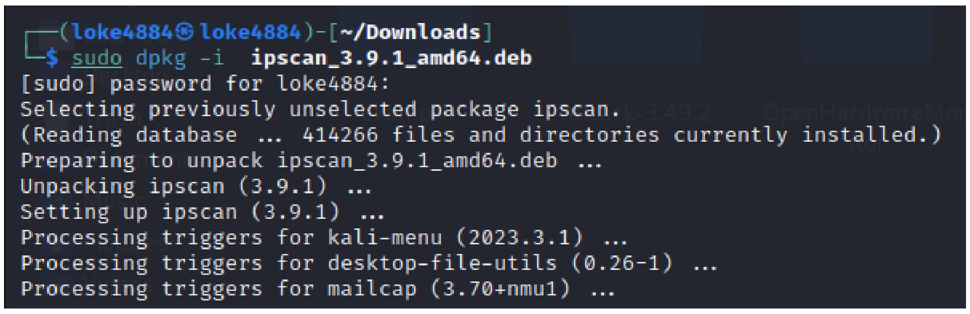


```
┌──(loke4884㉿loke4884)-[~]
└─$ cd Downloads
```



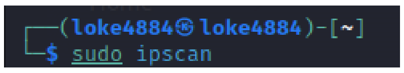
```
┌──(loke4884㉿loke4884)-[~/Downloads]
└─$ ls
example  httrack-3.49.2  httrack-3.49.2.tar.gz  ipscan_3.9.1_amd64.deb  OpenHardwareMonitor  openhardwaremonitor-v0.9.6.zip  stuxnet.vmem  stuxnet.vmem.zip  theHarvester-4.0.3  theHarvester-4.0.3.zip
```

Unpack the deb file you downloaded



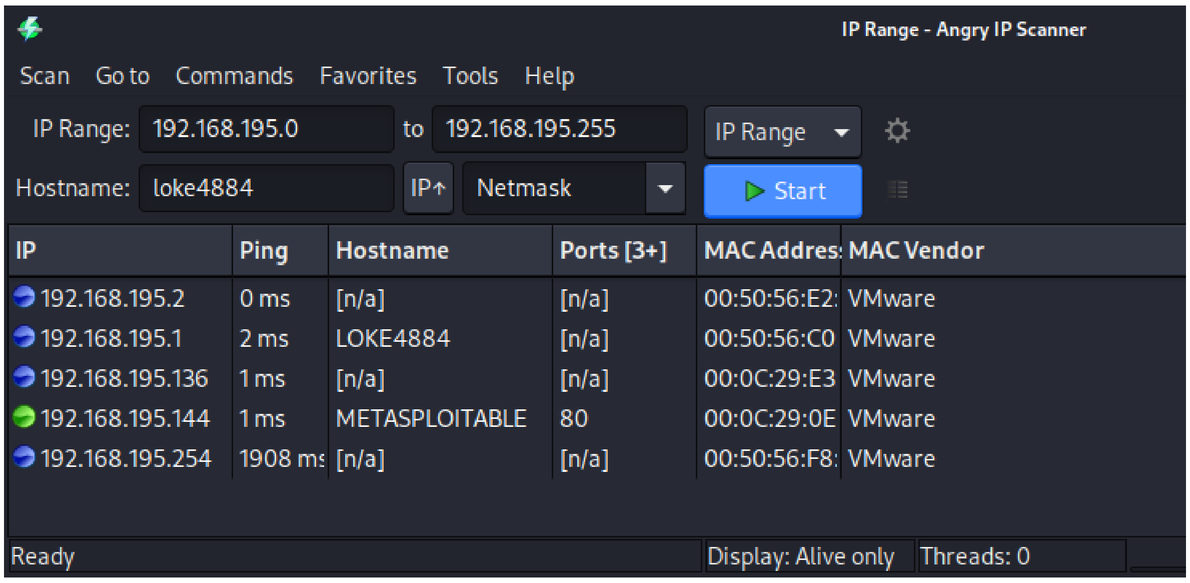
```
┌──(loke4884㉿loke4884)-[~/Downloads]
└─$ sudo dpkg -i  ipscan_3.9.1_amd64.deb
[sudo] password for loke4884:
Selecting previously unselected package ipscan.
(Reading database ... 414266 files and directories currently installed.)
Preparing to unpack ipscan_3.9.1_amd64.deb  ...
Unpacking ipscan (3.9.1) ...
Setting up ipscan (3.9.1)  ...
Processing triggers for kali-menu (2023.3.1) ...
Processing triggers for desktop-file-utils (0.26-1)  ...
Processing triggers for mailcap (3.70+nmu1)  ...
```

Sudo ipscan



```
┌──(loke4884㉿loke4884)-[~]
└─$ sudo ipscan
```

Click on Start

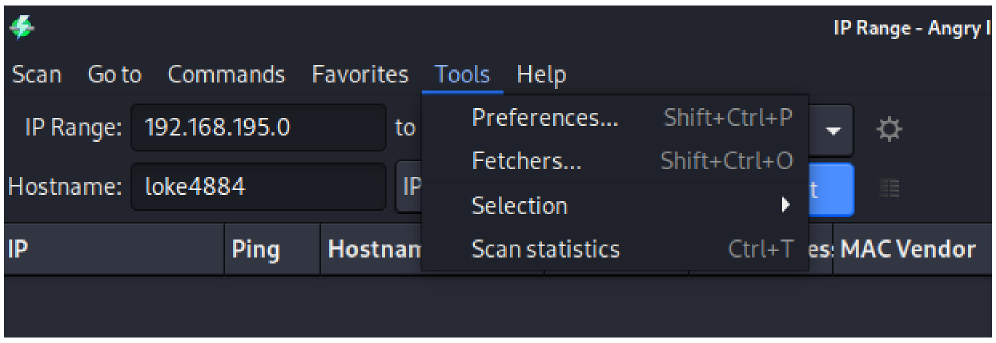


IP Range: 192.168.195.0 to 192.168.195.255 IP Range

Hostname: loke4884 Netmask

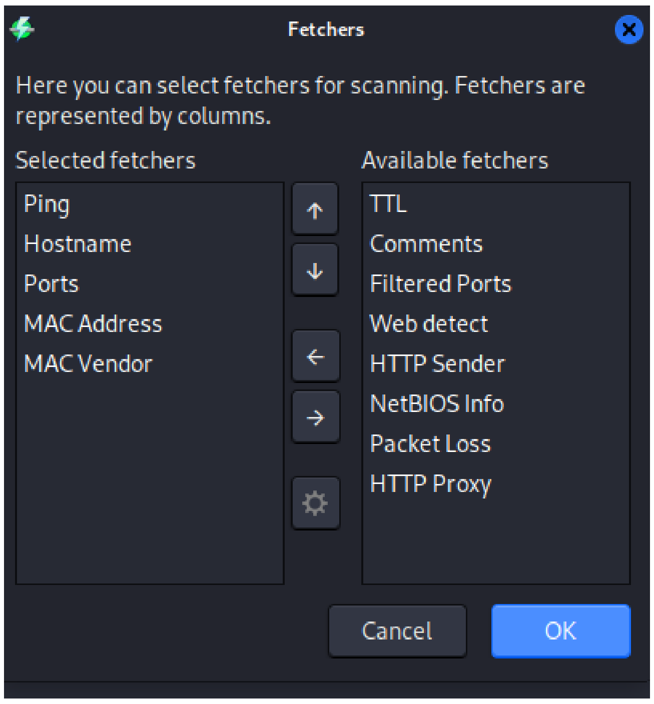
IP	Ping	Hostname	Ports [3+]	MAC Addres:	MAC Vendor
● 192.168.195.2	0 ms	[n/a]	[n/a]	00:50:56:E2:	VMware
● 192.168.195.1	2 ms	LOKE4884	[n/a]	00:50:56:C0	VMware
● 192.168.195.136	1 ms	[n/a]	[n/a]	00:0C:29:E3	VMware
● 192.168.195.144	1 ms	METASPLOITABLE	80	00:0C:29:0E	VMware
● 192.168.195.254	1908 ms	[n/a]	[n/a]	00:50:56:F8:	VMware

Ready | Display: Alive only | Threads: 0



IP Range: 192.168.195.0 to

Hostname: loke4884



Here you can select fetchers for scanning. Fetchers are represented by columns.

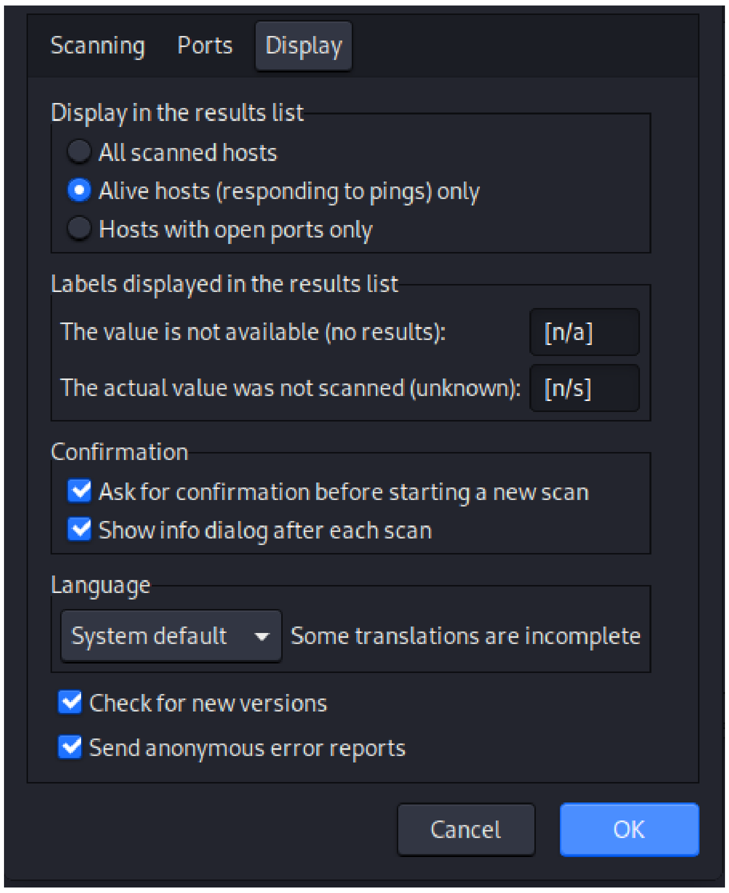
Selected fetchers

Ping
Hostname
Ports
MAC Address
MAC Vendor

Available fetchers

TTL
Comments
Filtered Ports
Web detect
HTTP Sender
NetBIOS Info
Packet Loss
HTTP Proxy

In settings



Display in the results list

○ All scanned hosts
● Alive hosts (responding to pings) only
○ Hosts with open ports only

Labels displayed in the results list

The value is not available (no results): [n/a]
The actual value was not scanned (unknown): [n/s]

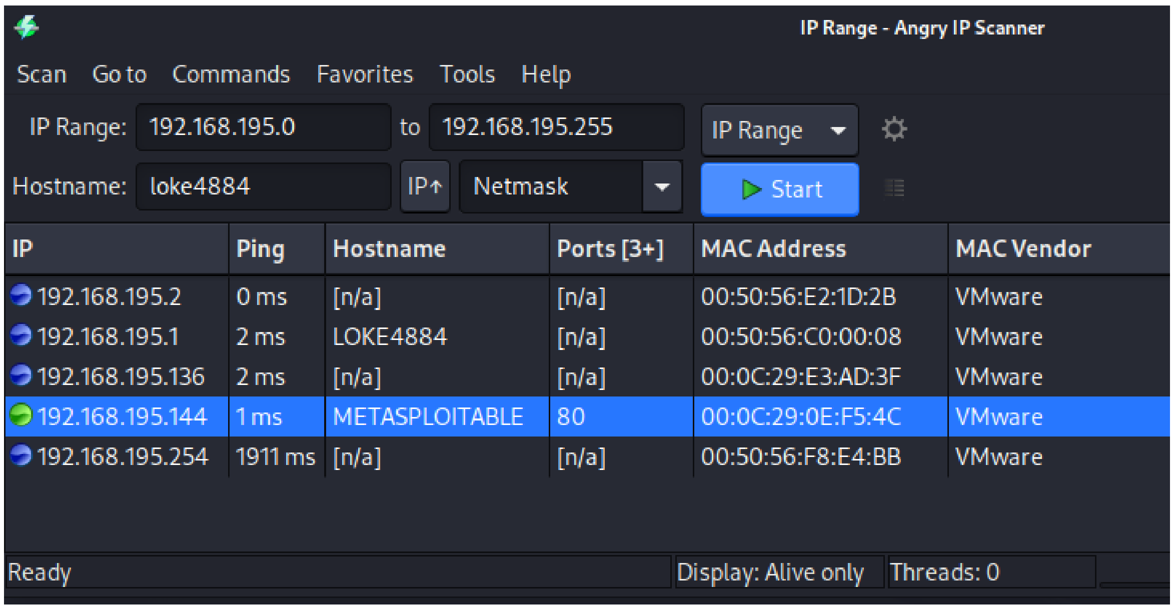
Confirmation

☑ Ask for confirmation before starting a new scan
☑ Show info dialog after each scan

Language

System default Some translations are incomplete

☑ Check for new versions
☑ Send anonymous error reports



IP Range: 192.168.195.0 to 192.168.195.255

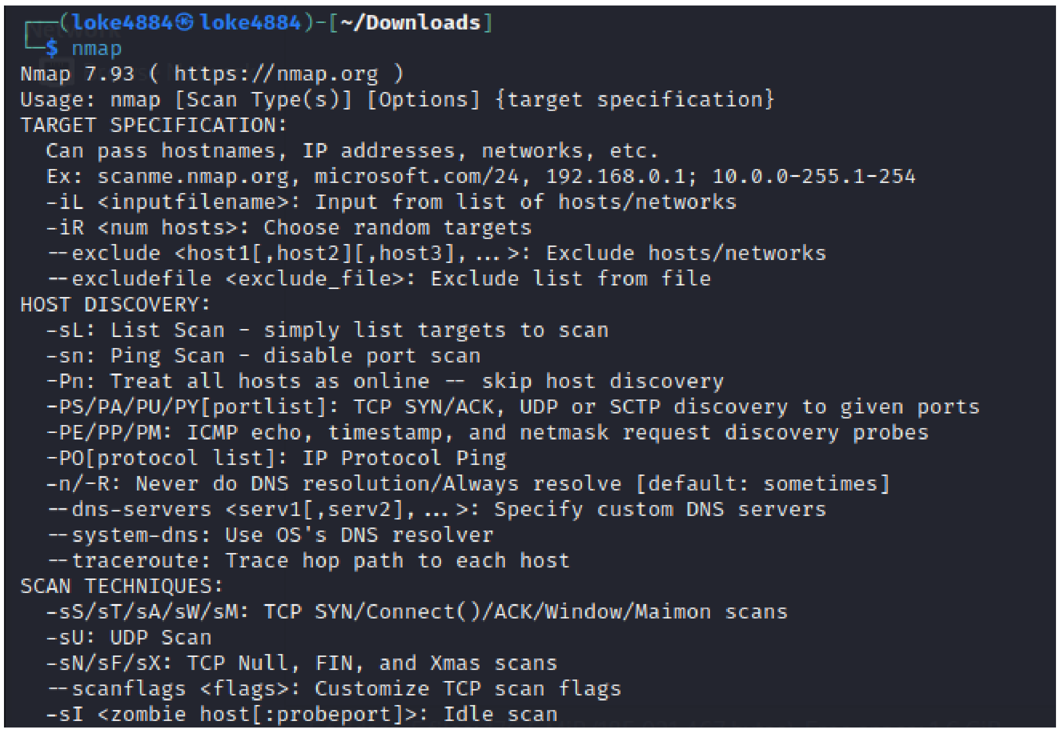
Hostname: loke4884 Netmask

IP	Ping	Hostname	Ports [3+]	MAC Address	MAC Vendor
192.168.195.2	0 ms	[n/a]	[n/a]	00:50:56:E2:1D:2B	VMware
192.168.195.1	2 ms	LOKE4884	[n/a]	00:50:56:C0:00:08	VMware
192.168.195.136	2 ms	[n/a]	[n/a]	00:0C:29:E3:AD:3F	VMware
192.168.195.144	1 ms	METASPLOITABLE	80	00:0C:29:0E:F5:4C	VMware
192.168.195.254	1911 ms	[n/a]	[n/a]	00:50:56:F8:E4:BB	VMware

Ready Display: Alive only Threads: 0

Green color Ip → Ip active and ports are open

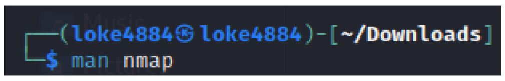
Nmap



```
┌──(loke4884㉿loke4884)-[~/Downloads]
└─$ nmap
Nmap 7.93 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
```

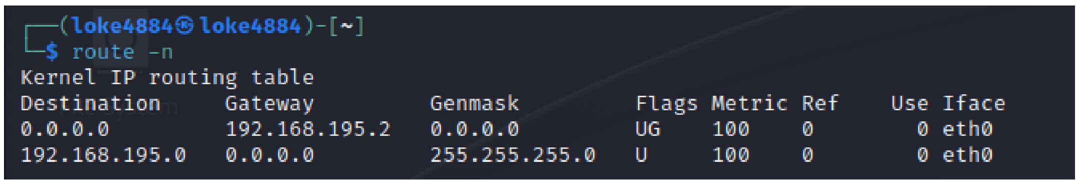
To get to know about nmap

man nmap →manual on nmap



```
┌──(loke4884㉿loke4884)-[~/Downloads]
└─$ man nmap
```

route -n →Here you get Gateway Ip which is router ip



```
┌──(loke4884㉿loke4884)-[~]
└─$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.195.2   0.0.0.0         UG    100    0        0 eth0
192.168.195.0   0.0.0.0         255.255.255.0   U     100    0        0 eth0
```

To check open ports and filter ports

sudo nmap -sT targetMachineIp/24

or

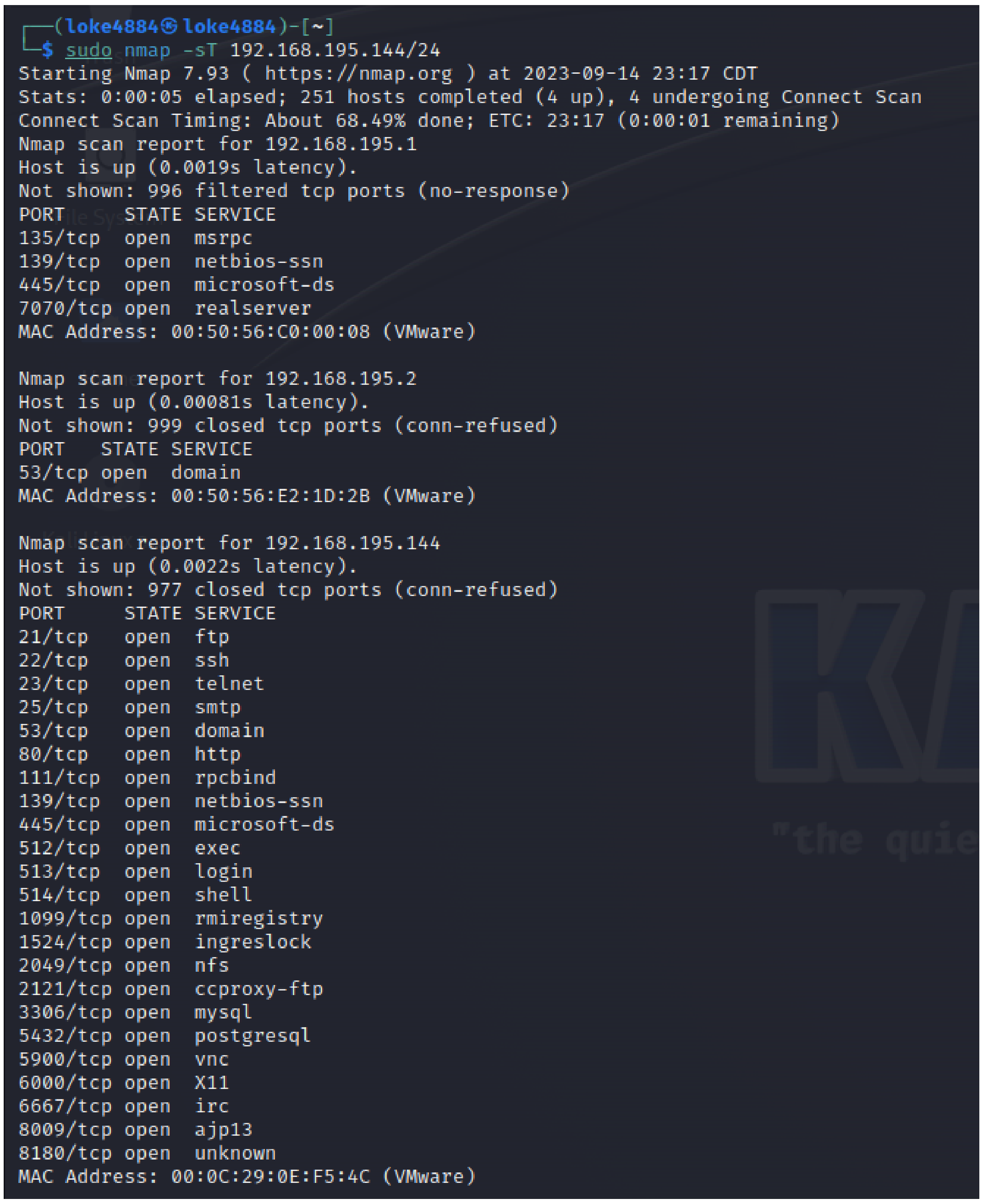
sudo nmap -sT targetMchine

-sT: This is an Nmap option that specifies the scan type. In this case, it's a TCP connect scan. Nmap will attempt to establish a full TCP connection to the specified target machine's IP address to determine whether the port is open or closed. It's a basic and reliable scan type but less stealthy compared to other scan types.

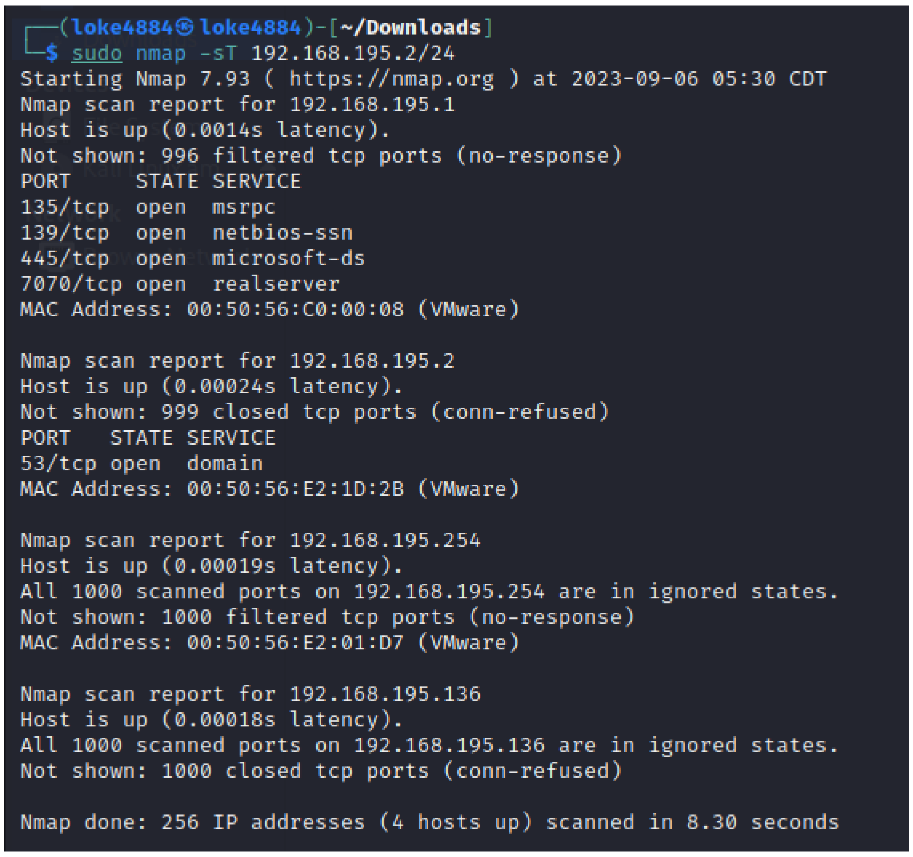
targetMachineIp/24: This is the target IP address or IP address range you want to scan. In this case, you've specified an IP address with the "/24" CIDR notation. This means you're scanning a range of IP addresses within the same subnet. The "/24" signifies a subnet mask of 255.255.255.0, so it will scan all IP addresses in that subnet. For example, if the target IP address is 192.168.1.1, it will scan all IP addresses from 192.168.1.1 to 192.168.1.254.

here targetMachine I gave metasploitable Ip

while running the command to know how much percentage nmap scanned just give enter percentage of scanned value is printed



```
┌──(loke4884㉿loke4884)-[~]
└─$ sudo nmap -sT 192.168.195.144/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-14 23:17 CDT
Stats: 0:00:05 elapsed; 251 hosts completed (4 up), 4 undergoing Connect Scan
Connect Scan Timing: About 68.49% done; ETC: 23:17 (0:00:01 remaining)
Nmap scan report for 192.168.195.1
Host is up (0.0019s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
7070/tcp open  realserver
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.195.2
Host is up (0.00081s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:E2:1D:2B (VMware)

Nmap scan report for 192.168.195.144
Host is up (0.0022s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:0E:F5:4C (VMware)
```



```
┌──(loke4884㉿loke4884)-[~/Downloads]
└─$ sudo nmap -sT 192.168.195.2/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-06 05:30 CDT
Nmap scan report for 192.168.195.1
Host is up (0.0014s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
7070/tcp open  realserver
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.195.2
Host is up (0.00024s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:E2:1D:2B (VMware)

Nmap scan report for 192.168.195.254
Host is up (0.00019s latency).
All 1000 scanned ports on 192.168.195.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:E2:01:D7 (VMware)

Nmap scan report for 192.168.195.136
Host is up (0.00018s latency).
All 1000 scanned ports on 192.168.195.136 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 256 IP addresses (4 hosts up) scanned in 8.30 seconds
```

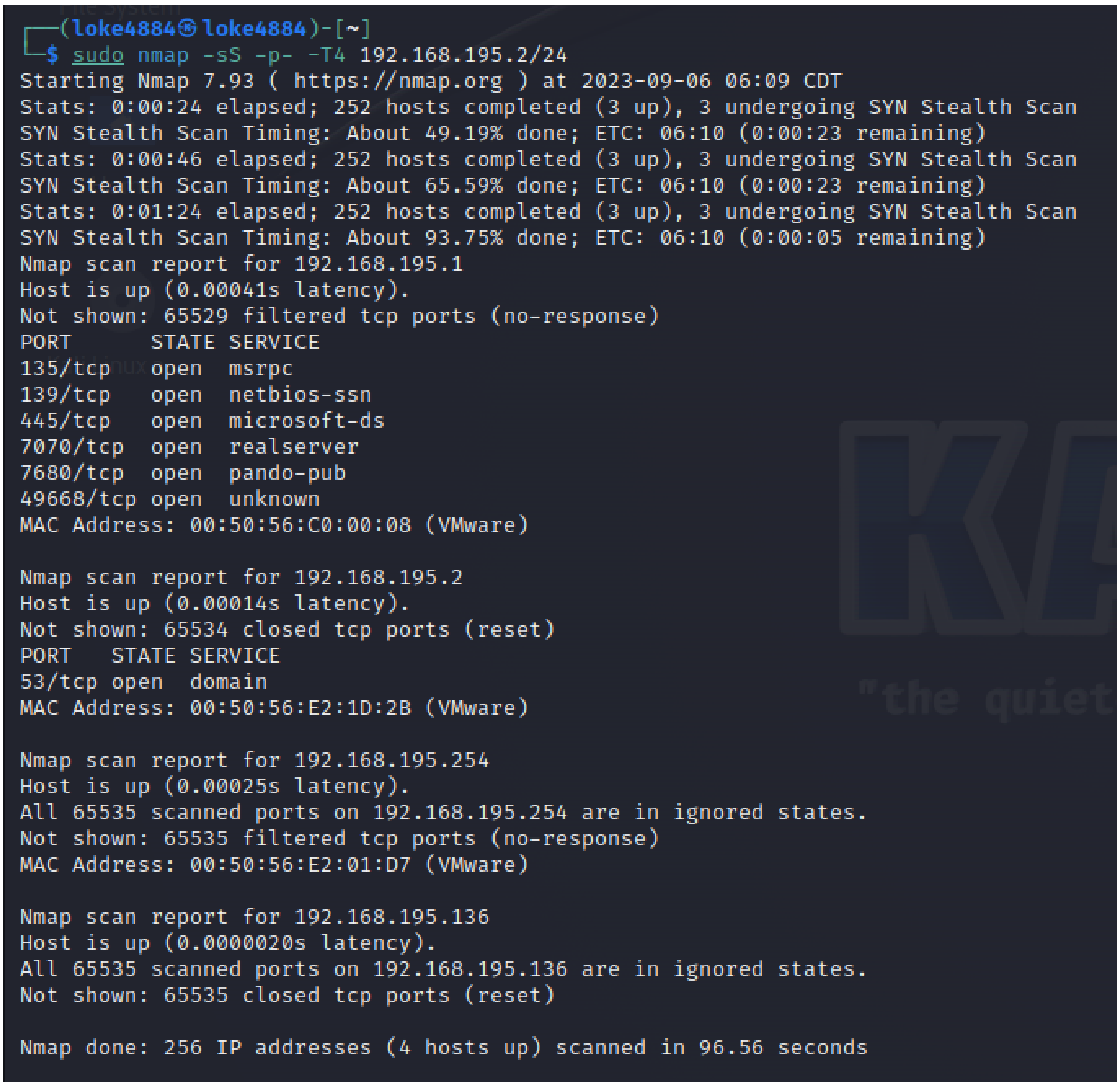
To Scan on all the 64,000 ports → May reveal some services

sudo nmap -sS -p- -T4 192.168.195.2/24

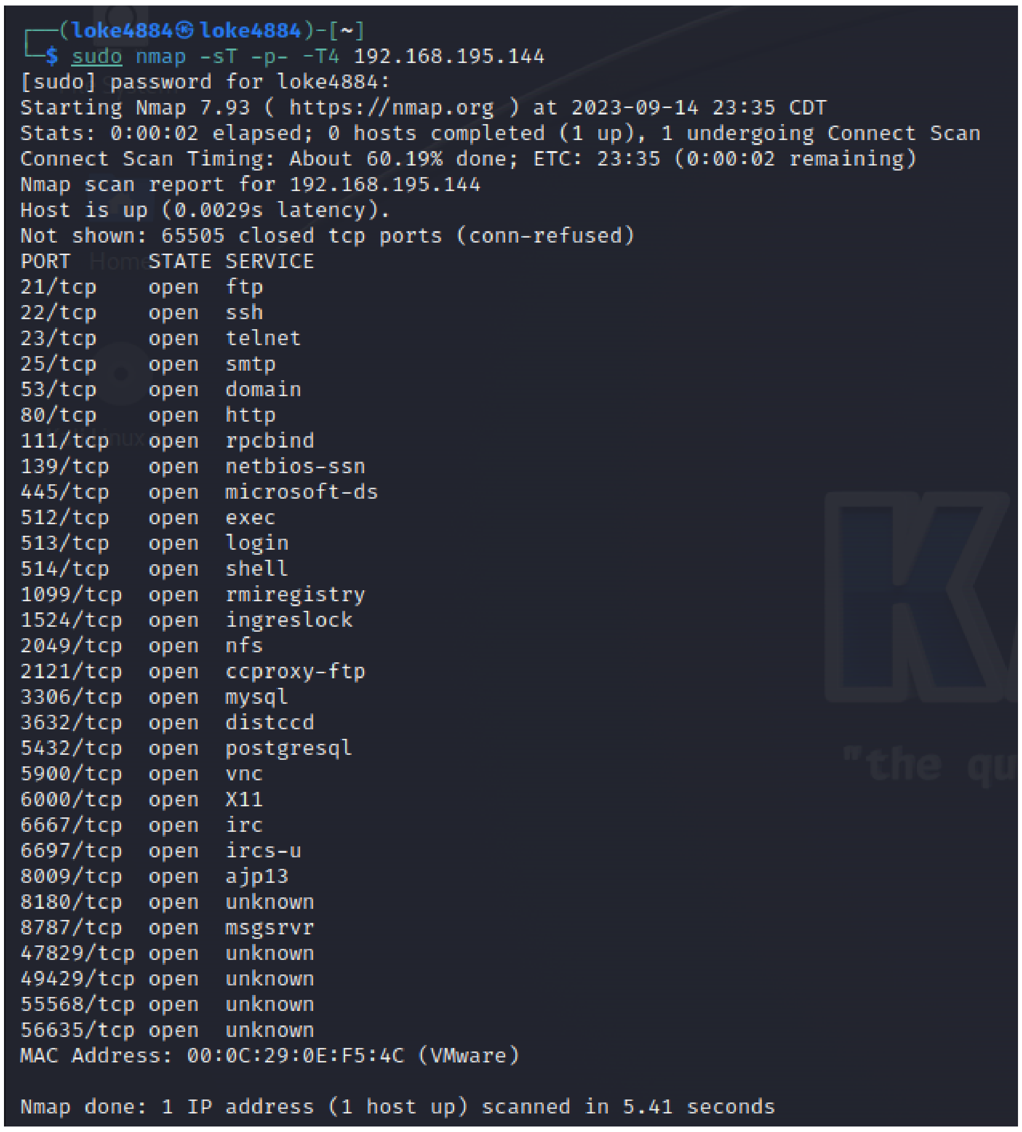
-sS: This is an Nmap option that specifies the scan type. In this case, it's a SYN scan. The SYN scan is a stealthy scan that sends TCP SYN packets to the target ports and analyzes the responses to determine if the ports are open or closed. It's one of the most common and widely used scan types.

-p-: This option tells Nmap to scan all 65,535 TCP ports on the target machine. Scanning all ports is useful for thorough port enumeration, but it can be time-consuming.

-T4: This is an Nmap option that sets the timing template for the scan. The -T4 option sets the scan speed to "aggressive." This means Nmap will send packets more quickly, which can result in faster scan completion but may be noisier on the network.



```
┌──(loke4884㉿loke4884)-[~]
└─$ sudo nmap -sS -p- -T4 192.168.195.2/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-06 06:09 CDT
Stats: 0:00:24 elapsed; 252 hosts completed (3 up), 3 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 49.19% done; ETC: 06:10 (0:00:23 remaining)
Stats: 0:00:46 elapsed; 252 hosts completed (3 up), 3 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 65.59% done; ETC: 06:10 (0:00:23 remaining)
Stats: 0:01:24 elapsed; 252 hosts completed (3 up), 3 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 93.75% done; ETC: 06:10 (0:00:05 remaining)
Nmap scan report for 192.168.195.1
Host is up (0.00041s latency).
Not shown: 65529 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
7070/tcp  open  realserver
7680/tcp  open  pando-pub
49668/tcp open  unknown
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.195.2
Host is up (0.00014s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:E2:1D:2B (VMware)

Nmap scan report for 192.168.195.254
Host is up (0.00025s latency).
All 65535 scanned ports on 192.168.195.254 are in ignored states.
Not shown: 65535 filtered tcp ports (no-response)
MAC Address: 00:50:56:E2:01:D7 (VMware)

Nmap scan report for 192.168.195.136
Host is up (0.0000020s latency).
All 65535 scanned ports on 192.168.195.136 are in ignored states.
Not shown: 65535 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 96.56 seconds
```

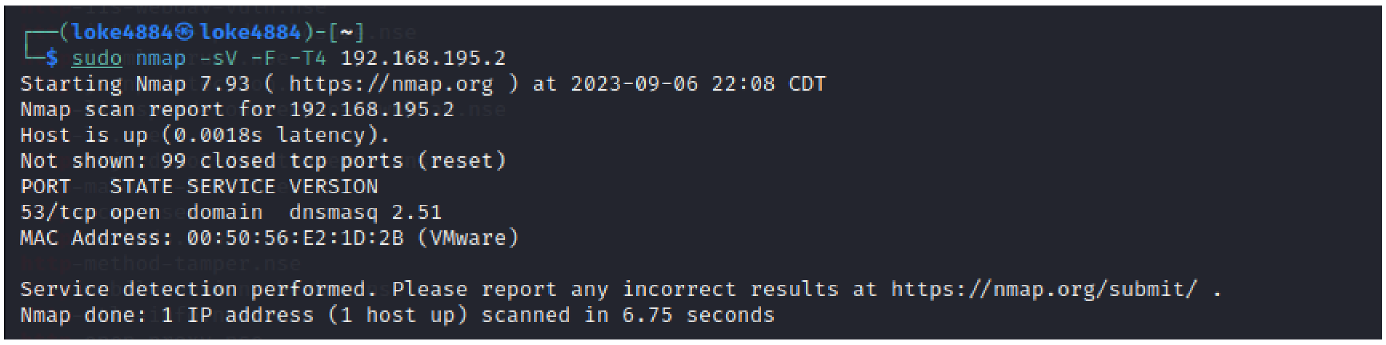


```
┌──(loke4884㉿loke4884)-[~]
└─$ sudo nmap -sT -p- -T4 192.168.195.144
[sudo] password for loke4884:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-14 23:35 CDT
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 60.19% done; ETC: 23:35 (0:00:02 remaining)
Nmap scan report for 192.168.195.144
Host is up (0.0029s latency).
Not shown: 65505 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
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
47829/tcp open  unknown
49429/tcp open  unknown
55568/tcp open  unknown
56635/tcp open  unknown
MAC Address: 00:0C:29:0E:F5:4C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 5.41 seconds
```

Specific with specific ports

-F → common 100 ports scan

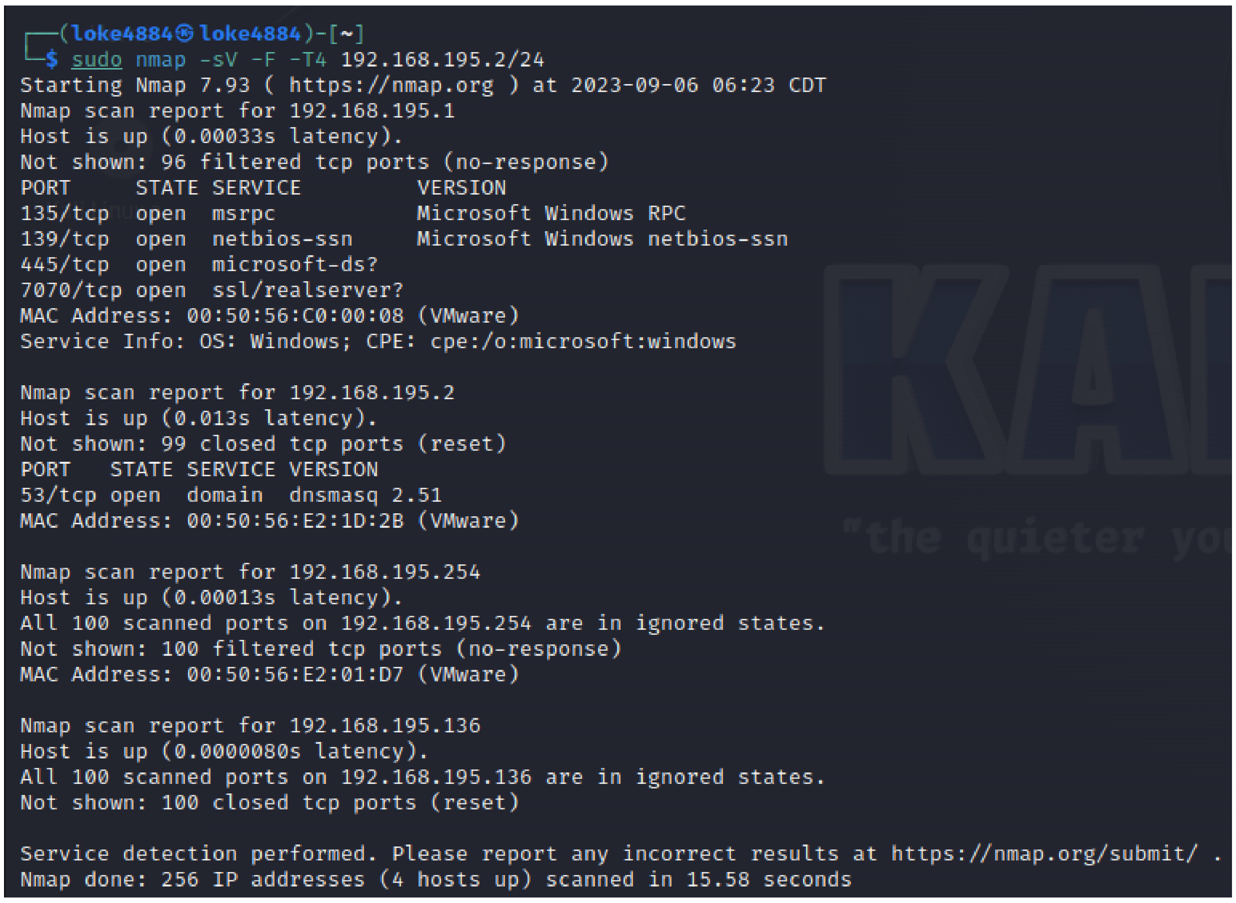
sudo nmap -sV -F -T4 192.168.195.2



```
┌──(loke4884㉿loke4884)-[~]
└─$ sudo nmap -sV -F -T4 192.168.195.2
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-06 22:08 CDT
Nmap scan report for 192.168.195.2
Host is up (0.0018s latency).
Not shown: 99 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
53/tcp open  domain  dnsmasq 2.51
MAC Address: 00:50:56:E2:1D:2B (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.75 seconds
```

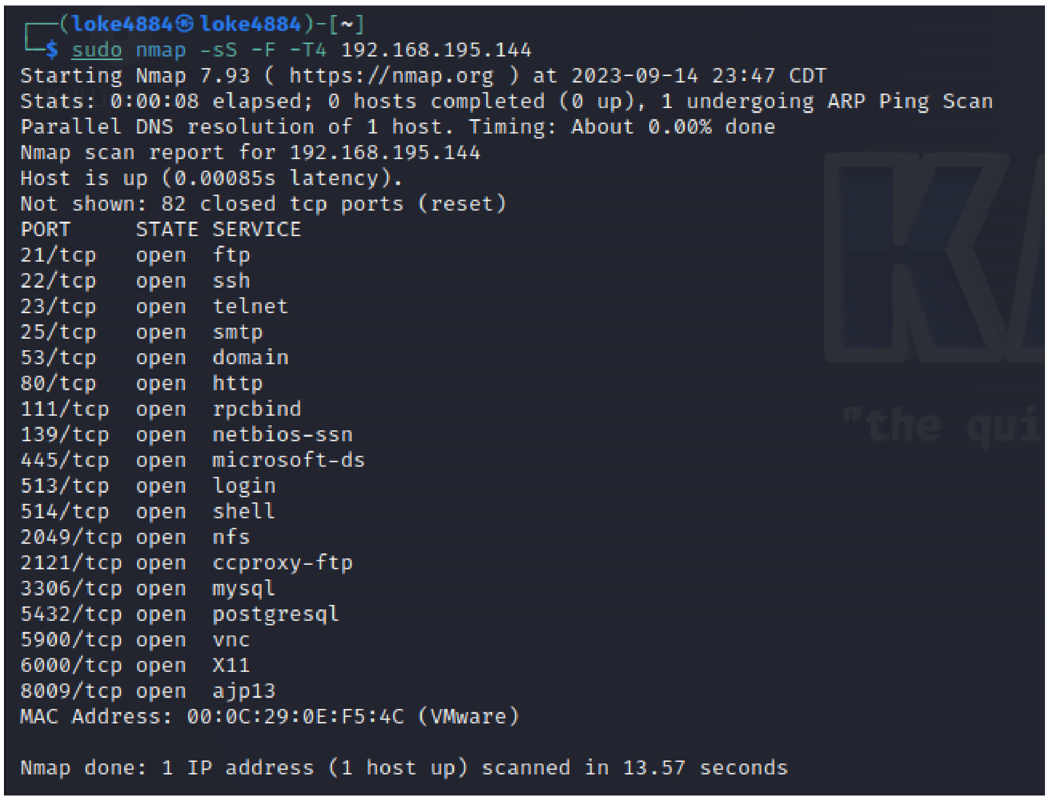
To scan ports by version based → you can able to

sudo nmap -sV -F -T4 192.168.195.2/24



```
┌──(loke4884㉿loke4884)-[~]
└─$ sudo nmap -sV -F -T4 192.168.195.2/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-06 06:23 CDT
Nmap scan report for 192.168.195.1
Host is up (0.00033s latency).
Not shown: 96 filtered tcp ports (no-response)
PORT     STATE SERVICE         VERSION
135/tcp  open  msrpc           Microsoft Windows RPC
139/tcp  open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
7070/tcp open  ssl/realserver?
MAC Address: 00:50:56:C0:00:08 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.195.2
Host is up (0.013s latency).
Not shown: 99 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
53/tcp open  domain  dnsmasq 2.51
MAC Address: 00:50:56:E2:1D:2B (VMware)

Nmap scan report for 192.168.195.254
Host is up (0.00013s latency).
All 100 scanned ports on 192.168.195.254 are in ignored states.
Not shown: 100 filtered tcp ports (no-response)
MAC Address: 00:50:56:E2:01:D7 (VMware)

Nmap scan report for 192.168.195.136
Host is up (0.0000080s latency).
All 100 scanned ports on 192.168.195.136 are in ignored states.
Not shown: 100 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 15.58 seconds
```

sudo nmap -sS -F -T4 192.168.195.144



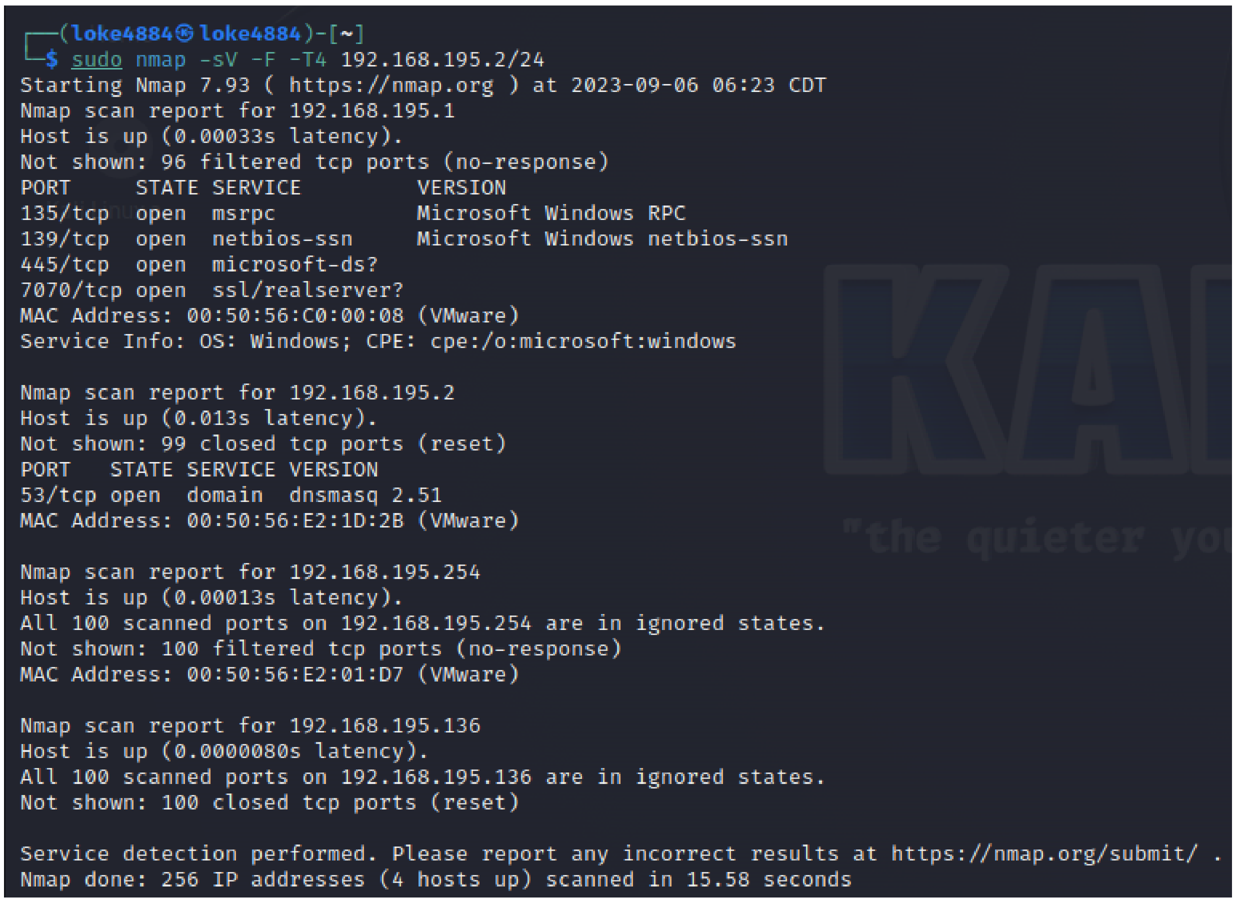
```
┌──(loke4884㉿loke4884)-[~]
└─$ sudo nmap -sS -F -T4 192.168.195.144
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-14 23:47 CDT
Stats: 0:00:08 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.195.144
Host is up (0.00085s latency).
Not shown: 82 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
513/tcp  open  login
514/tcp  open  shell
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
8009/tcp open  ajp13
MAC Address: 00:0C:29:0E:F5:4C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.57 seconds
```

by version based → you can able to

sudo nmap -sV -F -T4 192.168.195.2/24

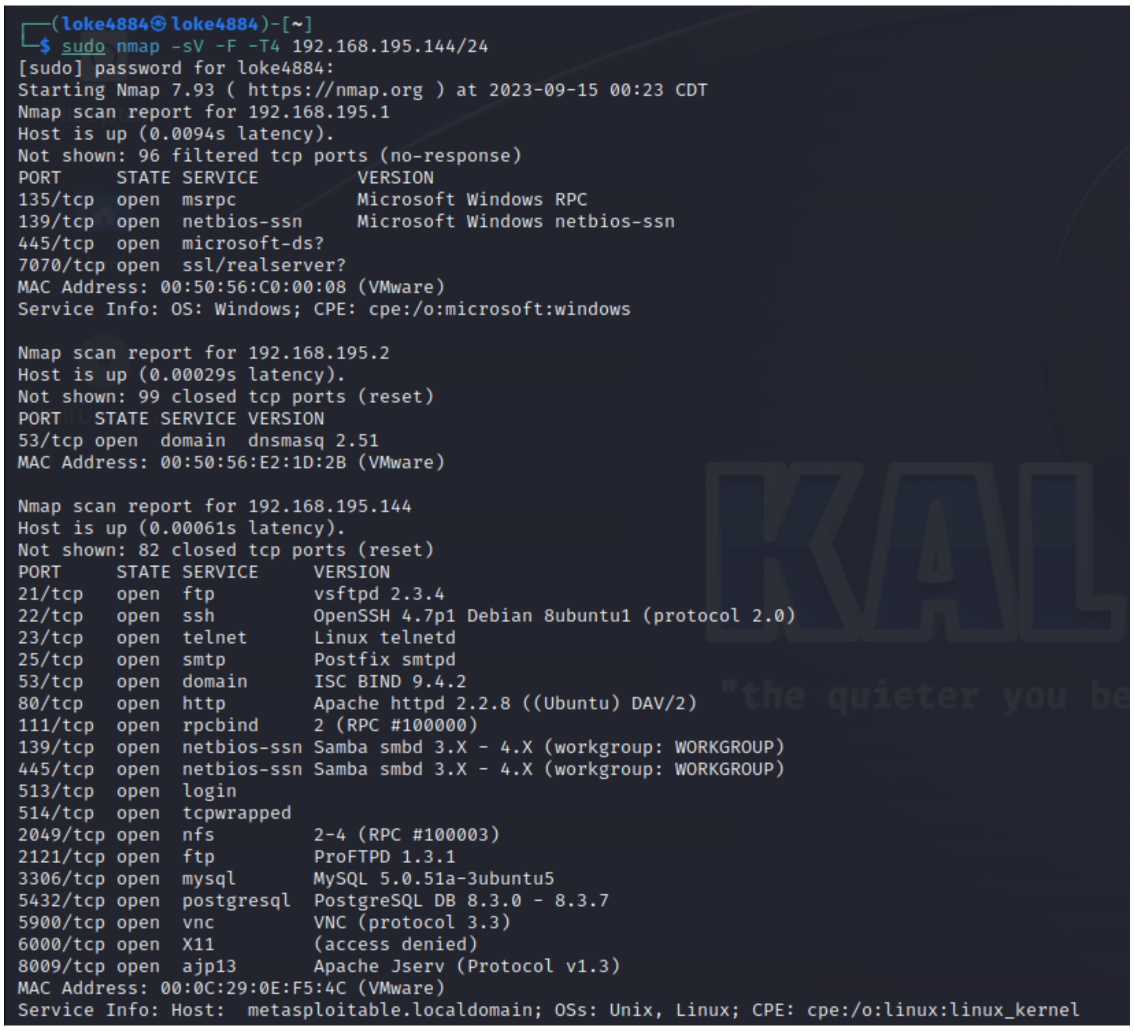
-sV: This is an Nmap option that specifies the version detection scan. Nmap will attempt to determine the version of services running on open ports. This can provide information about the software and potentially its vulnerabilities.

-F: This option tells Nmap to perform a fast scan. The fast scan, also known as a "Fast Mode" scan, is a quick scan that targets the most common 100 ports. It's a faster alternative to scanning all 65,535 ports, which can be time-consuming.



```
┌──(loke4884㉿loke4884)-[~]
└─$ sudo nmap -sV -F -T4 192.168.195.2/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-06 06:23 CDT
Nmap scan report for 192.168.195.1
Host is up (0.00033s latency).
Not shown: 96 filtered tcp ports (no-response)
PORT     STATE SERVICE         VERSION
135/tcp  open  msrpc           Microsoft Windows RPC
139/tcp  open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
7070/tcp open  ssl/realserver?
MAC Address: 00:50:56:C0:00:08 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.195.2
Host is up (0.013s latency).
Not shown: 99 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
53/tcp open  domain  dnsmasq 2.51
MAC Address: 00:50:56:E2:1D:2B (VMware)

Nmap scan report for 192.168.195.254
Host is up (0.00013s latency).
All 100 scanned ports on 192.168.195.254 are in ignored states.
Not shown: 100 filtered tcp ports (no-response)
MAC Address: 00:50:56:E2:01:D7 (VMware)

Nmap scan report for 192.168.195.136
Host is up (0.0000080s latency).
All 100 scanned ports on 192.168.195.136 are in ignored states.
Not shown: 100 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 15.58 seconds
```

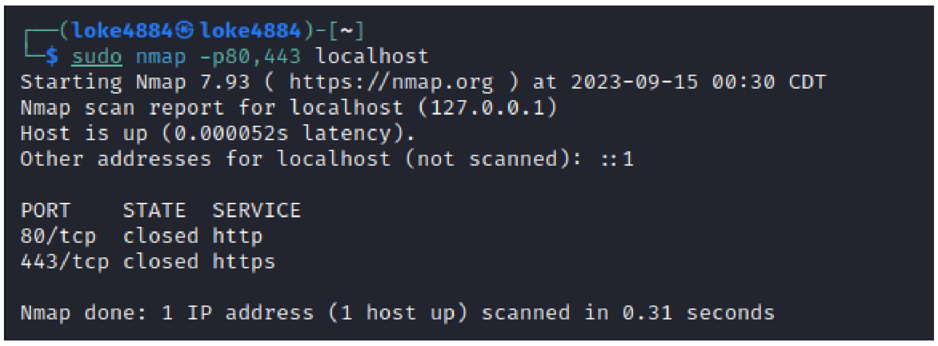
sudo nmap -sV -F -T4 192.168.195.144/24



```
┌──(loke4884㉿loke4884)-[~]
└─$ sudo nmap -sV -F -T4 192.168.195.144/24
[sudo] password for loke4884:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-15 00:23 CDT
Nmap scan report for 192.168.195.1
Host is up (0.0094s latency).
Not shown: 96 filtered tcp ports (no-response)
PORT     STATE SERVICE         VERSION
135/tcp  open  msrpc           Microsoft Windows RPC
139/tcp  open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
7070/tcp open  ssl/realserver?
MAC Address: 00:50:56:C0:00:08 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.195.2
Host is up (0.00029s latency).
Not shown: 99 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
53/tcp open  domain  dnsmasq 2.51
MAC Address: 00:50:56:E2:1D:2B (VMware)

Nmap scan report for 192.168.195.144
Host is up (0.00061s latency).
Not shown: 82 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
513/tcp  open  login
514/tcp  open  tcpwrapped
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)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
MAC Address: 00:0C:29:0E:F5:4C (VMware)
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

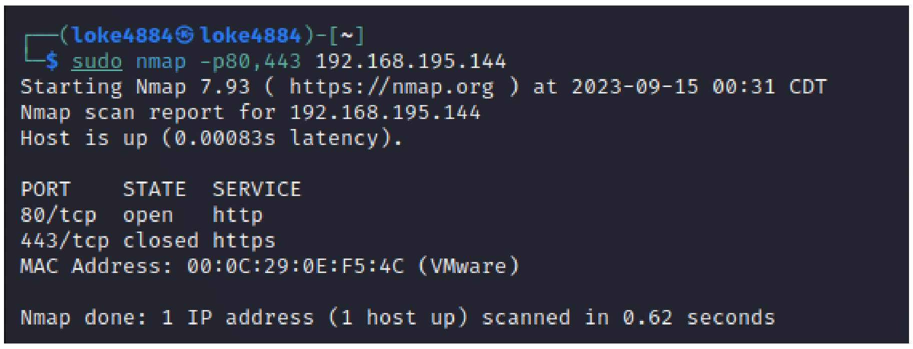
-p →To specify which port you want to scan

sudo nmap -p80,443 localhost



```
┌──(loke4884㉿loke4884)-[~]
└─$ sudo nmap -p80,443 localhost
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-15 00:30 CDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000052s latency).
Other addresses for localhost (not scanned): ::1

PORT    STATE  SERVICE
80/tcp  closed http
443/tcp closed https

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
```

sudo nmap -p80,433 metasploitableIp

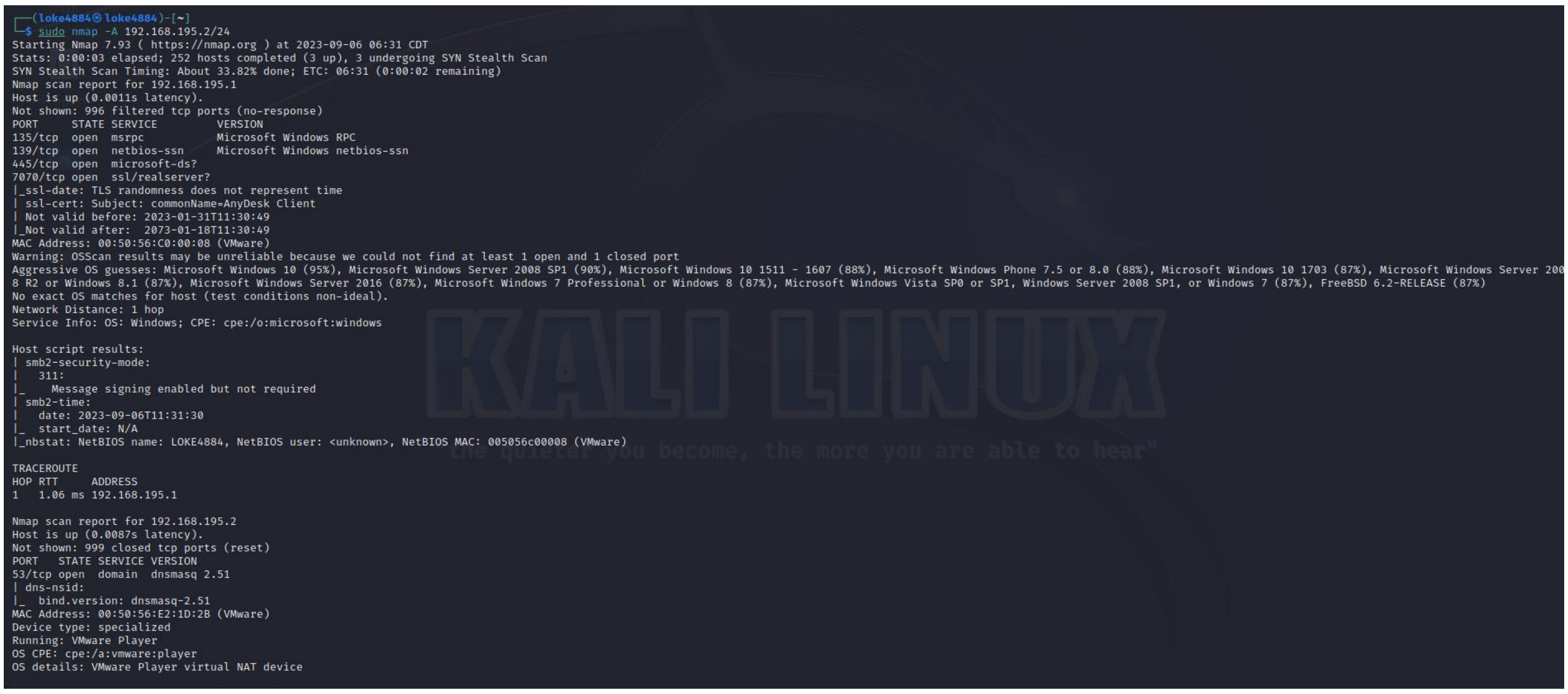


```
┌──(loke4884㉿loke4884)-[~]
└─$ sudo nmap -p80,443 192.168.195.144
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-15 00:31 CDT
Nmap scan report for 192.168.195.144
Host is up (0.00083s latency).

PORT    STATE  SERVICE
80/tcp  open   http
443/tcp closed https
MAC Address: 00:0C:29:0E:F5:4C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.62 seconds
```

-A → All scan

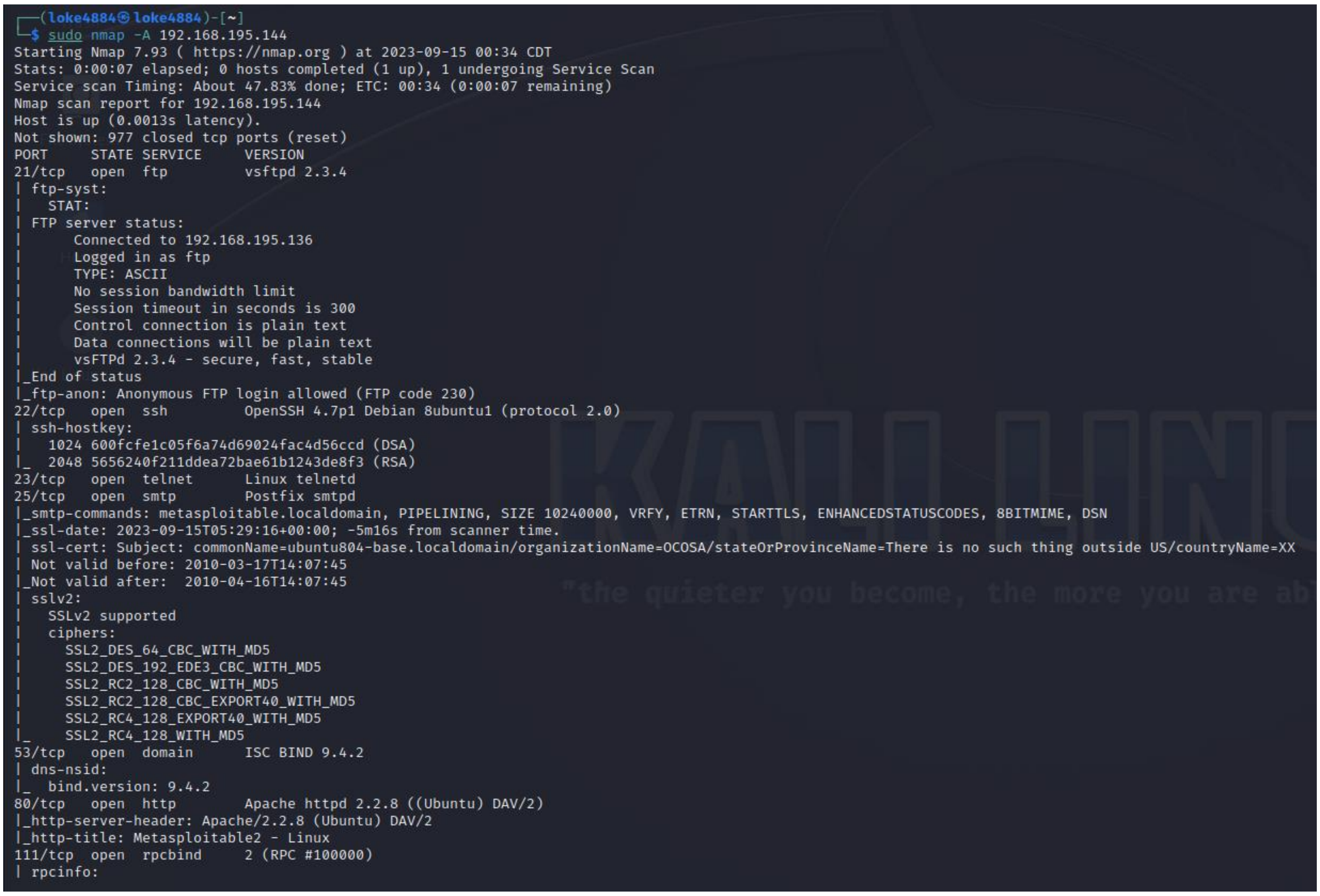
For router

sudo nmap -A 192.168.195.2/24

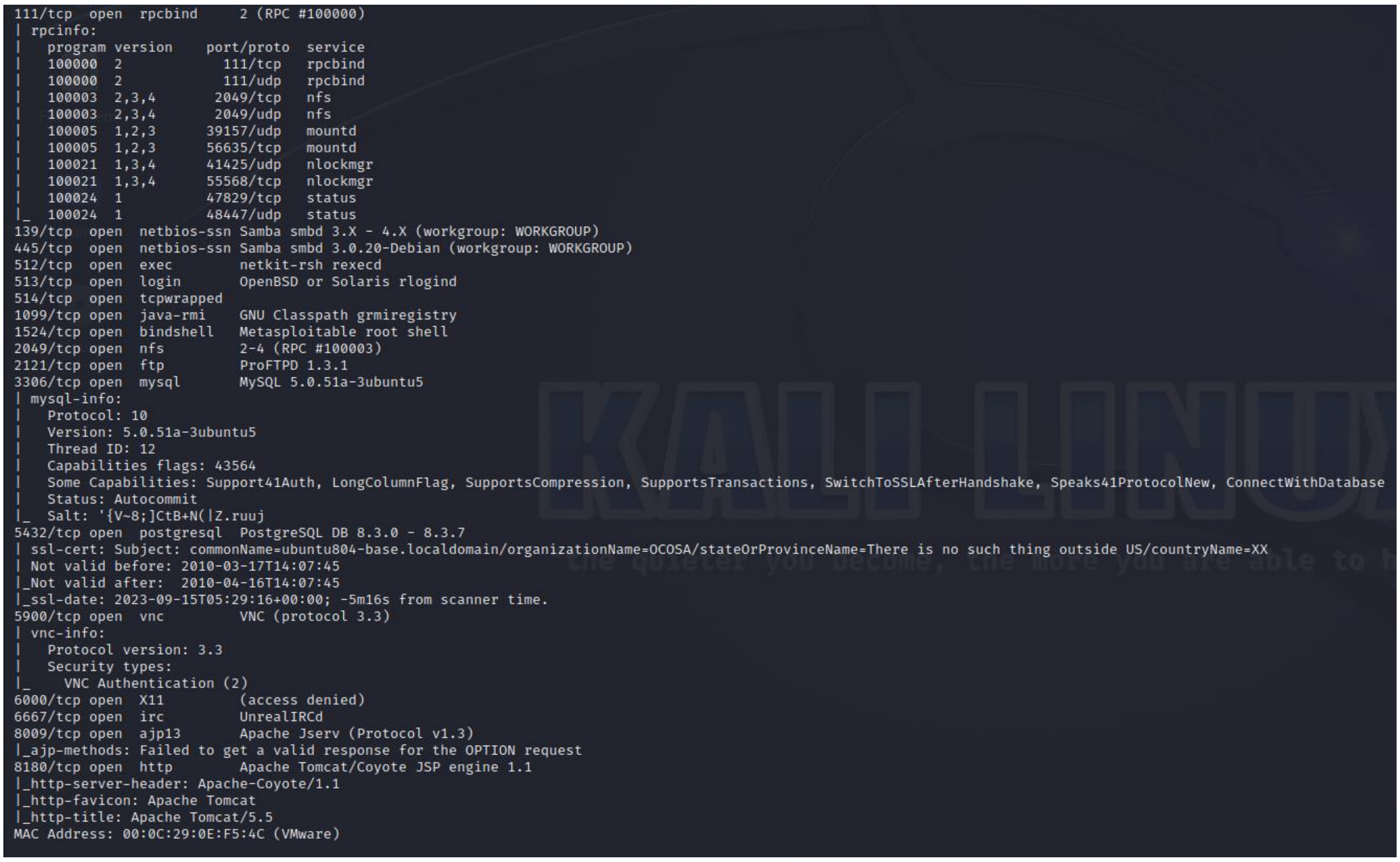


```
┌──(loke4884㉿loke4884)-[~]
└─$ sudo nmap -A 192.168.195.2/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-06 06:31 CDT
Stats: 0:00:03 elapsed; 252 hosts completed (3 up), 3 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 33.82% done; ETC: 06:31 (0:00:02 remaining)
Nmap scan report for 192.168.195.1
Host is up (0.0011s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE          VERSION
135/tcp  open  msrpc            Microsoft Windows RPC
139/tcp  open  netbios-ssn      Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
7070/tcp open  ssl/realserver?
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=AnyDesk Client
| Not valid before: 2023-01-31T11:30:49
|_Not valid after:  2073-01-18T11:30:49
MAC Address: 00:50:56:C0:00:08 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows 10 (95%), Microsoft Windows Server 2008 SP1 (90%), Microsoft Windows 10 1511 - 1607 (88%), Microsoft Windows Phone 7.5 or 8.0 (88%), Microsoft Windows 10 1703 (87%), Microsoft Windows Server 200
8 R2 or Windows 8.1 (87%), Microsoft Windows Server 2016 (87%), Microsoft Windows 7 Professional or Windows 8 (87%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (87%), FreeBSD 6.2-RELEASE (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2023-09-06T11:31:30
|_  start_date: N/A
|_nbstat: NetBIOS name: LOKE4884, NetBIOS user: <unknown>, NetBIOS MAC: 005056c00008 (VMware)

TRACEROUTE
HOP RTT     ADDRESS
1   1.06 ms 192.168.195.1

Nmap scan report for 192.168.195.2
Host is up (0.0087s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
53/tcp open  domain  dnsmasq 2.51
| dns-nsid:
|_  bind.version: dnsmasq-2.51
MAC Address: 00:50:56:E2:1D:2B (VMware)
Device type: specialized
Running: VMware Player
OS CPE: cpe:/a:vmware:player
OS details: VMware Player virtual NAT device
```

For Metasploitable

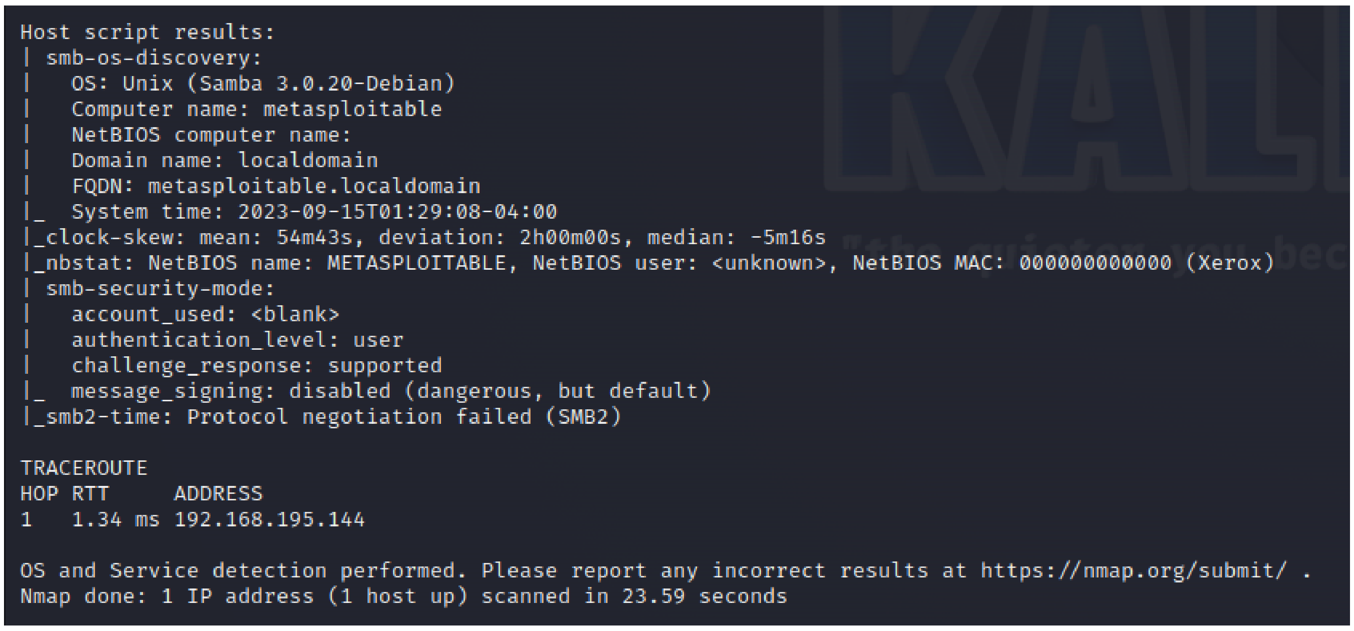


```
┌──(loke4884㉿loke4884)-[~]
└─$ sudo nmap -A 192.168.195.144
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-15 00:34 CDT
Stats: 0:00:07 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 47.83% done; ETC: 00:34 (0:00:07 remaining)
Nmap scan report for 192.168.195.144
Host is up (0.0013s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.195.136
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_  2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-date: 2023-09-15T05:29:16+00:00; -5m16s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|_    SSL2_RC4_128_WITH_MD5
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
```



```
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      39157/udp   mountd
|   100005  1,2,3      56635/tcp   mountd
|   100021  1,3,4      41425/udp   nlockmgr
|   100021  1,3,4      55568/tcp   nlockmgr
|   100024  1          47829/tcp   status
|_  100024  1          48447/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 12
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, LongColumnFlag, SupportsCompression, SupportsTransactions, SwitchToSSLAfterHandshake, Speaks41ProtocolNew, ConnectWithDatabase
|   Status: Autocommit
|_  Salt: '{V~8;]CtB+N(|Z.ruuj
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2023-09-15T05:29:16+00:00; -5m16s from scanner time.
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
MAC Address: 00:0C:29:0E:F5:4C (VMware)
```

Scroll down you can see os details by doing scan on IP



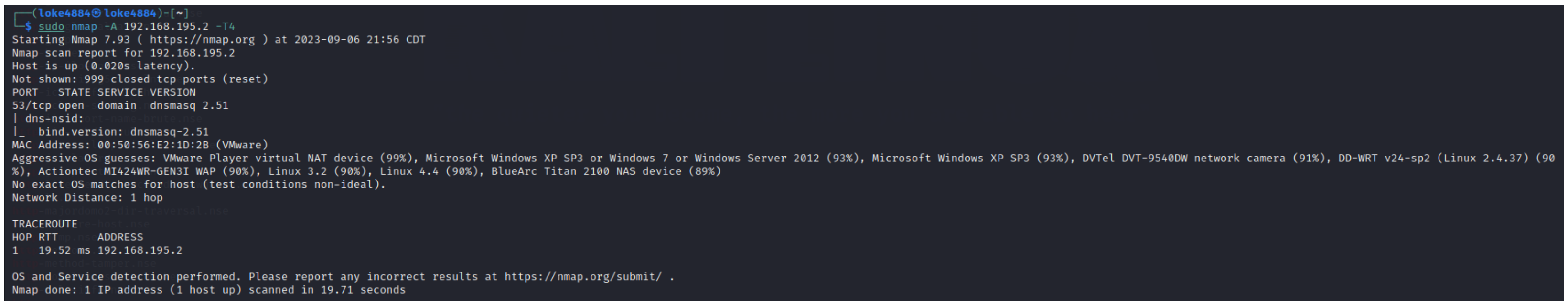
```
Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-09-15T01:29:08-04:00
|_clock-skew: mean: 54m43s, deviation: 2h00m00s, median: -5m16s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT     ADDRESS
1   1.34 ms 192.168.195.144

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 23.59 seconds
```

sudo nmap -A 192.168.195.2 -T4

T4 → used to speed up

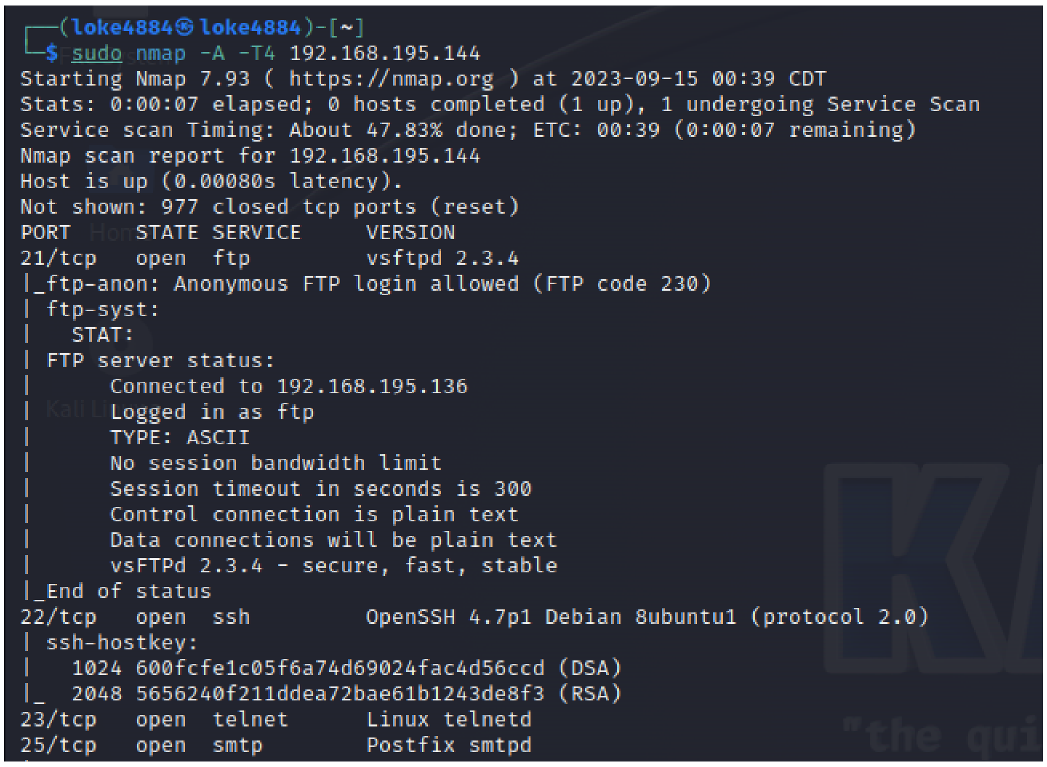
There are T1 to T5 → where T1 is lowest time means less speed to execute , where T5 is heighest time means more speed to execute

Where as T4 is the average time to execute



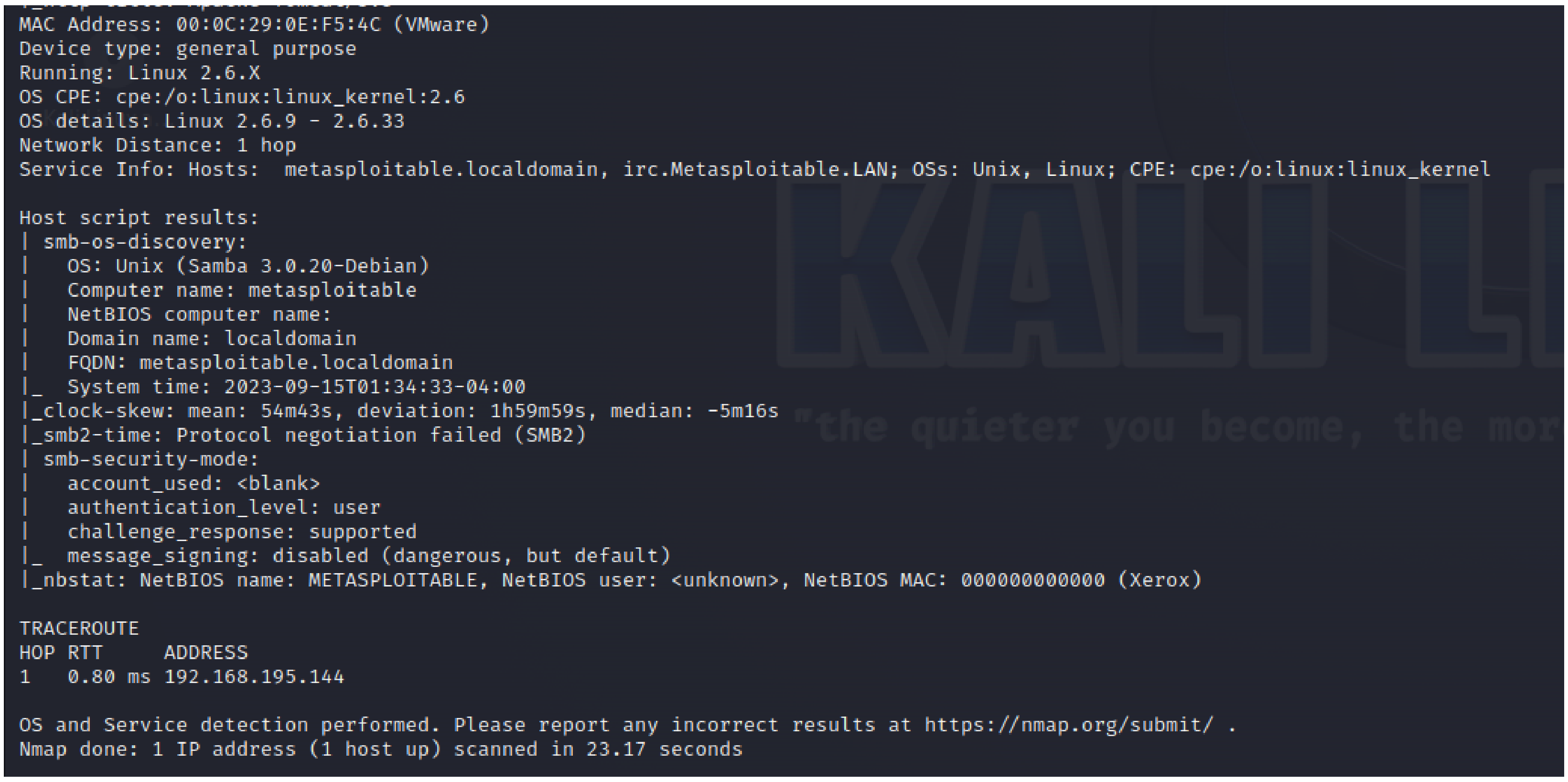
```
┌──(loke4884㉿loke4884)-[~]
└─$ sudo nmap -A 192.168.195.2 -T4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-06 21:56 CDT
Nmap scan report for 192.168.195.2
Host is up (0.020s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
53/tcp open  domain  dnsmasq 2.51
| dns-nsid:
|_  bind.version: dnsmasq-2.51
MAC Address: 00:50:56:E2:1D:2B (VMware)
Aggressive OS guesses: VMware Player virtual NAT device (99%), Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012 (93%), Microsoft Windows XP SP3 (93%), DVTel DVT-9540DW network camera (91%), DD-WRT v24-sp2 (Linux 2.4.37) (90
%), Actiontec MI424WR-GEN3I WAP (90%), Linux 3.2 (90%), Linux 4.4 (90%), BlueArc Titan 2100 NAS device (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   19.52 ms 192.168.195.2

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 19.71 seconds
```

sudo nmap -A -T4 192.168.195.144



```
┌──(loke4884㉿loke4884)-[~]
└─$ sudo nmap -A -T4 192.168.195.144
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-15 00:39 CDT
Stats: 0:00:07 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 47.83% done; ETC: 00:39 (0:00:07 remaining)
Nmap scan report for 192.168.195.144
Host is up (0.00080s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.195.136
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_  2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
```

Scroll down you can see os details by doing scan on IP

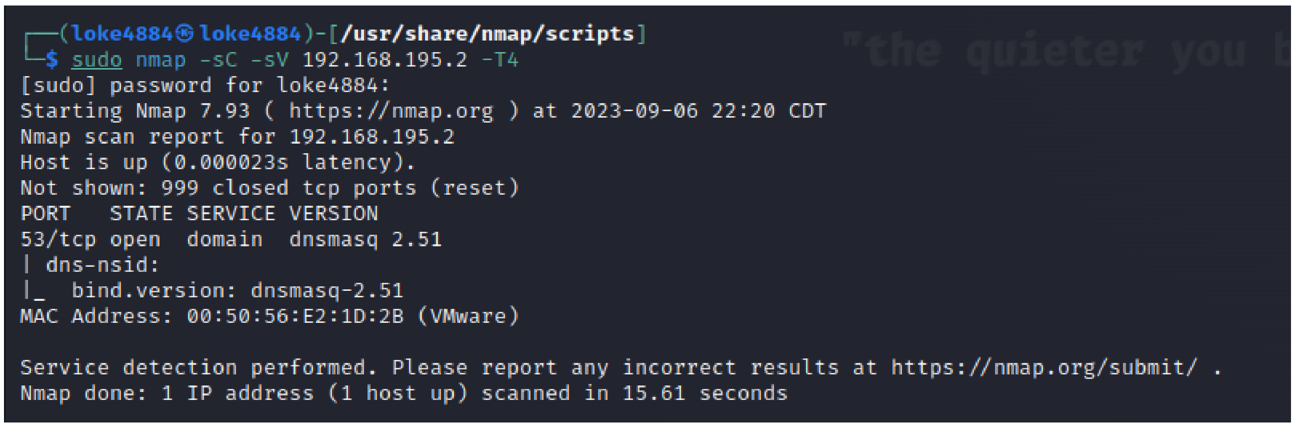


```
MAC Address: 00:0C:29:0E:F5:4C (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-09-15T01:34:33-04:00
|_clock-skew: mean: 54m43s, deviation: 1h59m59s, median: -5m16s
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)

TRACEROUTE
HOP RTT     ADDRESS
1   0.80 ms 192.168.195.144

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 23.17 seconds
```

sudo nmap -sC -sV 192.168.195.2 -T4

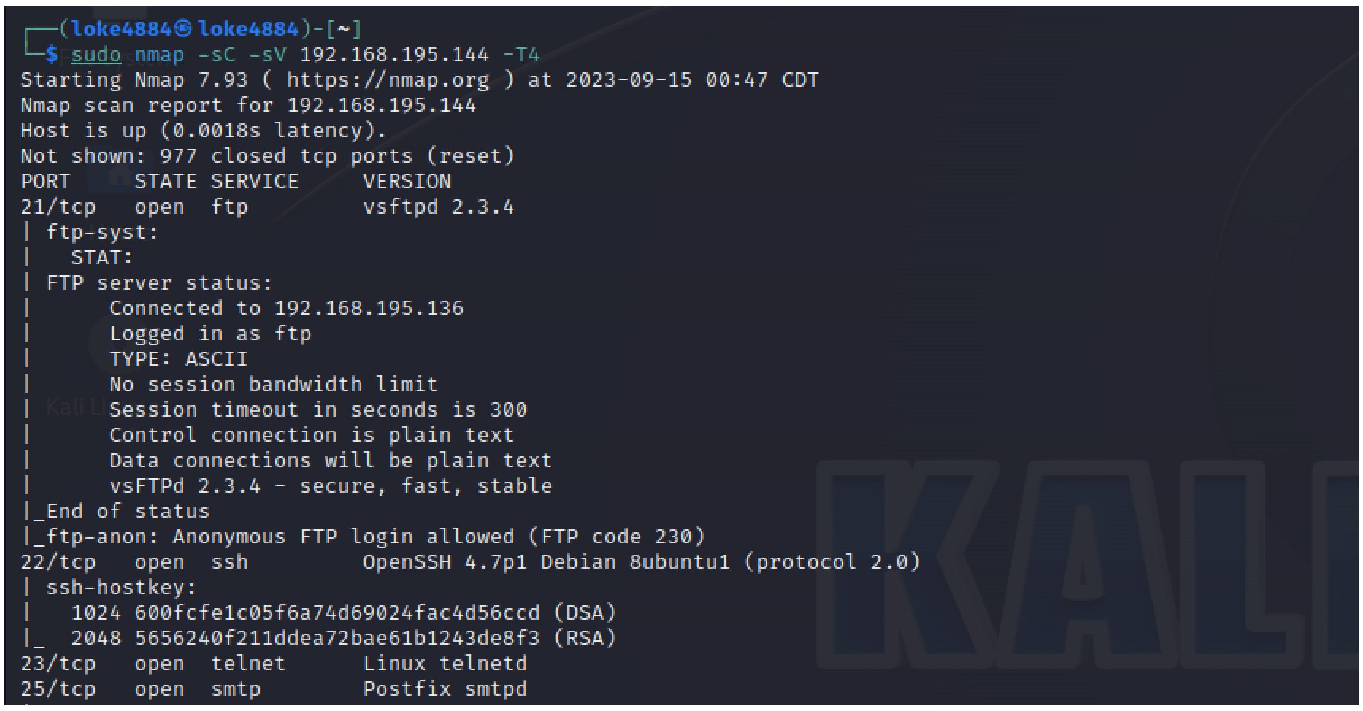
-sC → Script scan

-sV → version detection



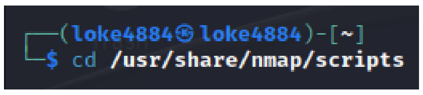
```
┌──(loke4884㉿loke4884)-[/usr/share/nmap/scripts]
└─$ sudo nmap -sC -sV 192.168.195.2 -T4
[sudo] password for loke4884:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-06 22:20 CDT
Nmap scan report for 192.168.195.2
Host is up (0.000023s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
53/tcp open  domain  dnsmasq 2.51
| dns-nsid:
|_  bind.version: dnsmasq-2.51
MAC Address: 00:50:56:E2:1D:2B (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.61 seconds
```

sudo nmap -sC -sV 192.168.195.2 -T4



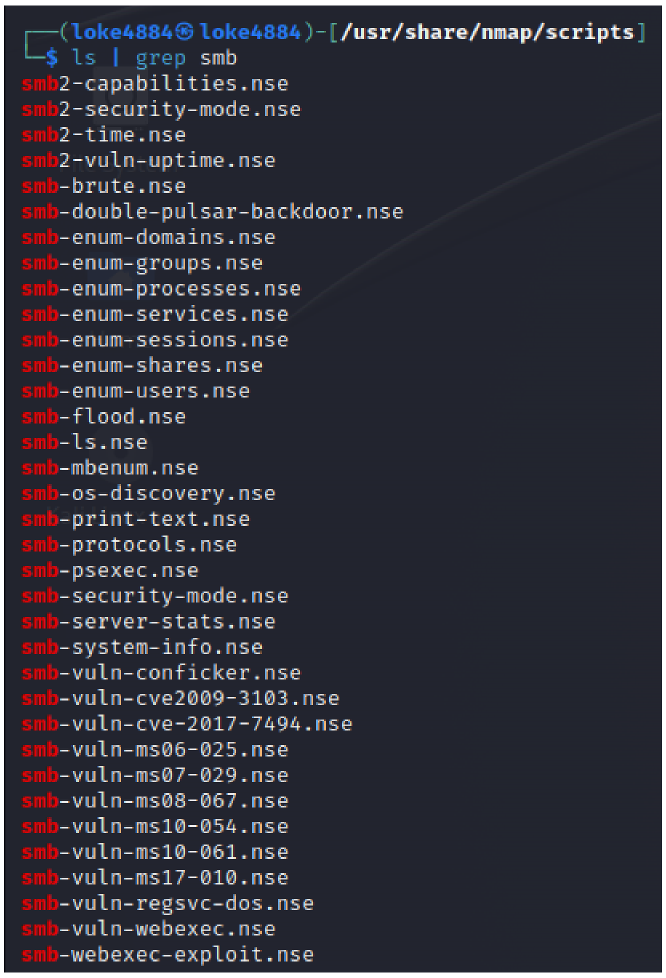
```
┌──(loke4884㉿loke4884)-[~]
└─$ sudo nmap -sC -sV 192.168.195.144 -T4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-15 00:47 CDT
Nmap scan report for 192.168.195.144
Host is up (0.0018s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.195.136
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_  2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
```

cd /usr/share/nmap/scripts



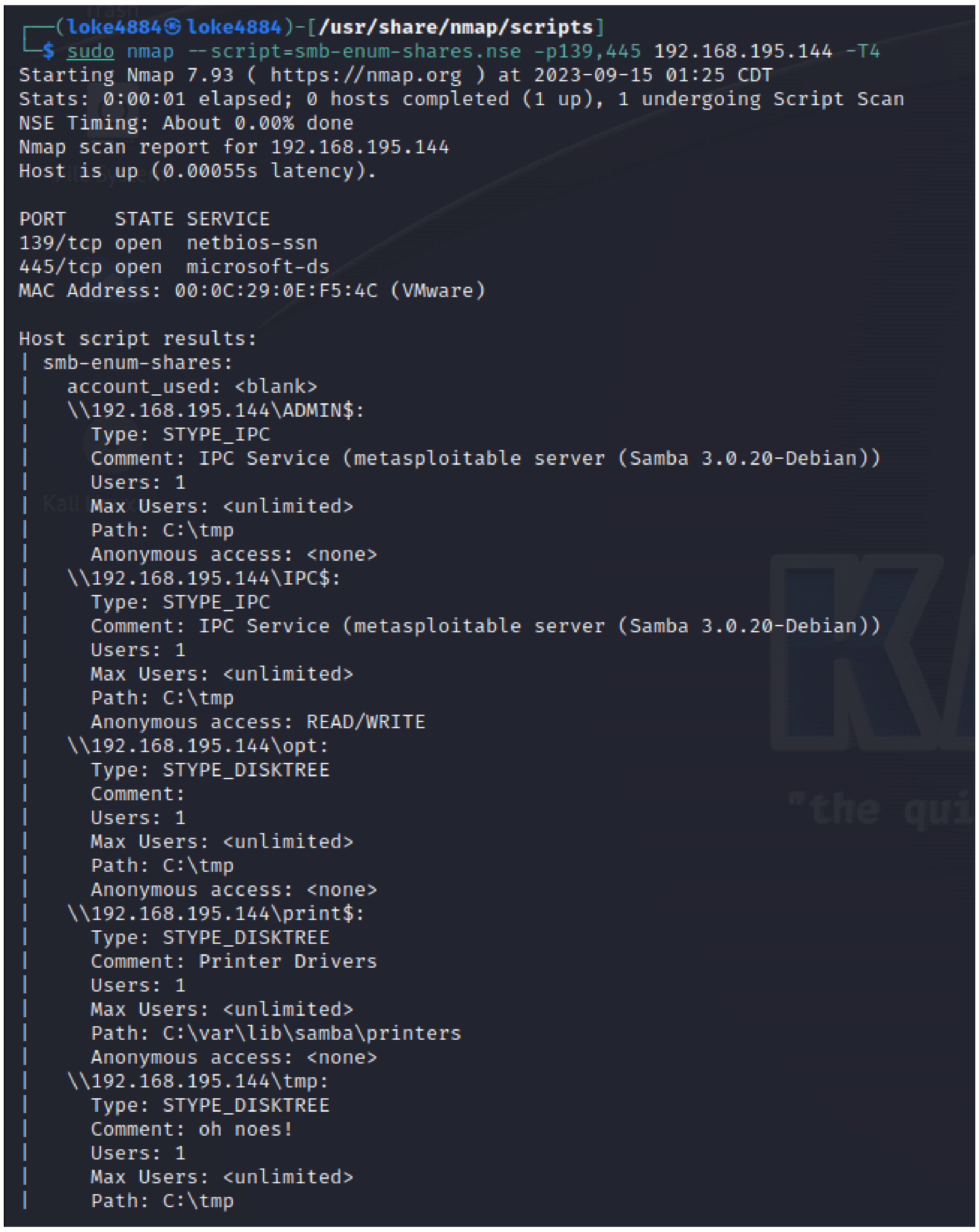
```
┌──(loke4884㉿loke4884)-[~]
└─$ cd /usr/share/nmap/scripts
```

ls | grep smb



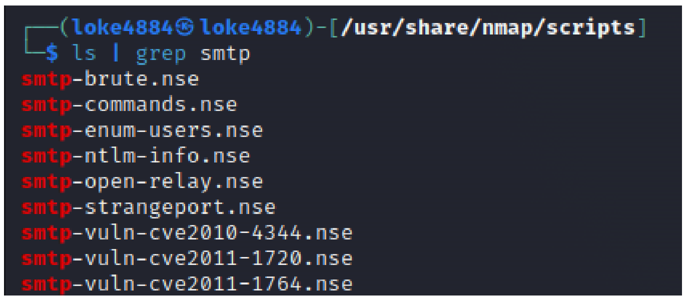
```
┌──(loke4884㉿loke4884)-[/usr/share/nmap/scripts]
└─$ ls | grep smb
smb2-capabilities.nse
smb2-security-mode.nse
smb2-time.nse
smb2-vuln-uptime.nse
smb-brute.nse
smb-double-pulsar-backdoor.nse
smb-enum-domains.nse
smb-enum-groups.nse
smb-enum-processes.nse
smb-enum-services.nse
smb-enum-sessions.nse
smb-enum-shares.nse
smb-enum-users.nse
smb-flood.nse
smb-ls.nse
smb-mbenum.nse
smb-os-discovery.nse
smb-print-text.nse
smb-protocols.nse
smb-psexec.nse
smb-security-mode.nse
smb-server-stats.nse
smb-system-info.nse
smb-vuln-conficker.nse
smb-vuln-cve2009-3103.nse
smb-vuln-cve-2017-7494.nse
smb-vuln-ms06-025.nse
smb-vuln-ms07-029.nse
smb-vuln-ms08-067.nse
smb-vuln-ms10-054.nse
smb-vuln-ms10-061.nse
smb-vuln-ms17-010.nse
smb-vuln-regsvc-dos.nse
smb-vuln-webexec.nse
smb-webexec-exploit.nse
```

sudo nmap --script=smb-enum-shares.nse -p139,445 192.168.195.144 -T4



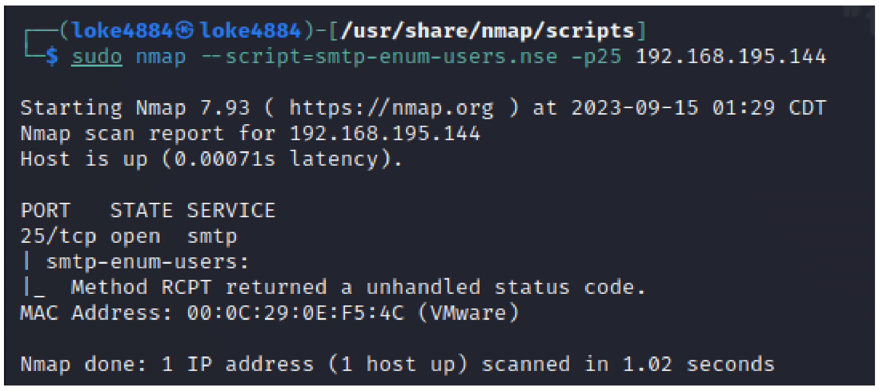
```
┌──(loke4884㉿loke4884)-[/usr/share/nmap/scripts]
└─$ sudo nmap --script=smb-enum-shares.nse -p139,445 192.168.195.144 -T4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-15 01:25 CDT
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 0.00% done
Nmap scan report for 192.168.195.144
Host is up (0.00055s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:0E:F5:4C (VMware)

Host script results:
| smb-enum-shares:
|   account_used: <blank>
|   \\192.168.195.144\ADMIN$:
|     Type: STYPE_IPC
|     Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: <none>
|   \\192.168.195.144\IPC$:
|     Type: STYPE_IPC
|     Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|   \\192.168.195.144\opt:
|     Type: STYPE_DISKTREE
|     Comment:
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: <none>
|   \\192.168.195.144\print$:
|     Type: STYPE_DISKTREE
|     Comment: Printer Drivers
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\var\lib\samba\printers
|     Anonymous access: <none>
|   \\192.168.195.144\tmp:
|     Type: STYPE_DISKTREE
|     Comment: oh noes!
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
```

ls | grep smtp



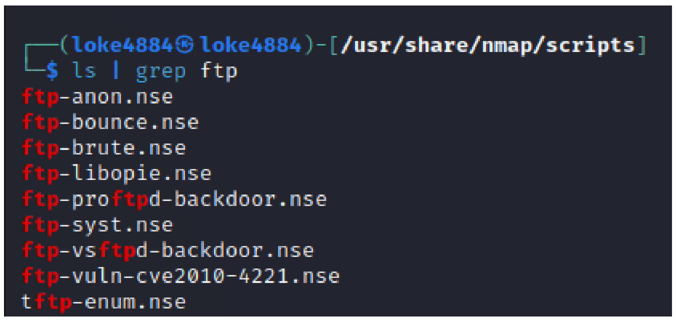
```
┌──(loke4884㉿loke4884)-[/usr/share/nmap/scripts]
└─$ ls | grep smtp
smtp-brute.nse
smtp-commands.nse
smtp-enum-users.nse
smtp-ntlm-info.nse
smtp-open-relay.nse
smtp-strangeport.nse
smtp-vuln-cve2010-4344.nse
smtp-vuln-cve2011-1720.nse
smtp-vuln-cve2011-1764.nse
```

sudo nmap --script=smtp-enum-users.nse -p25 192.168.195.144



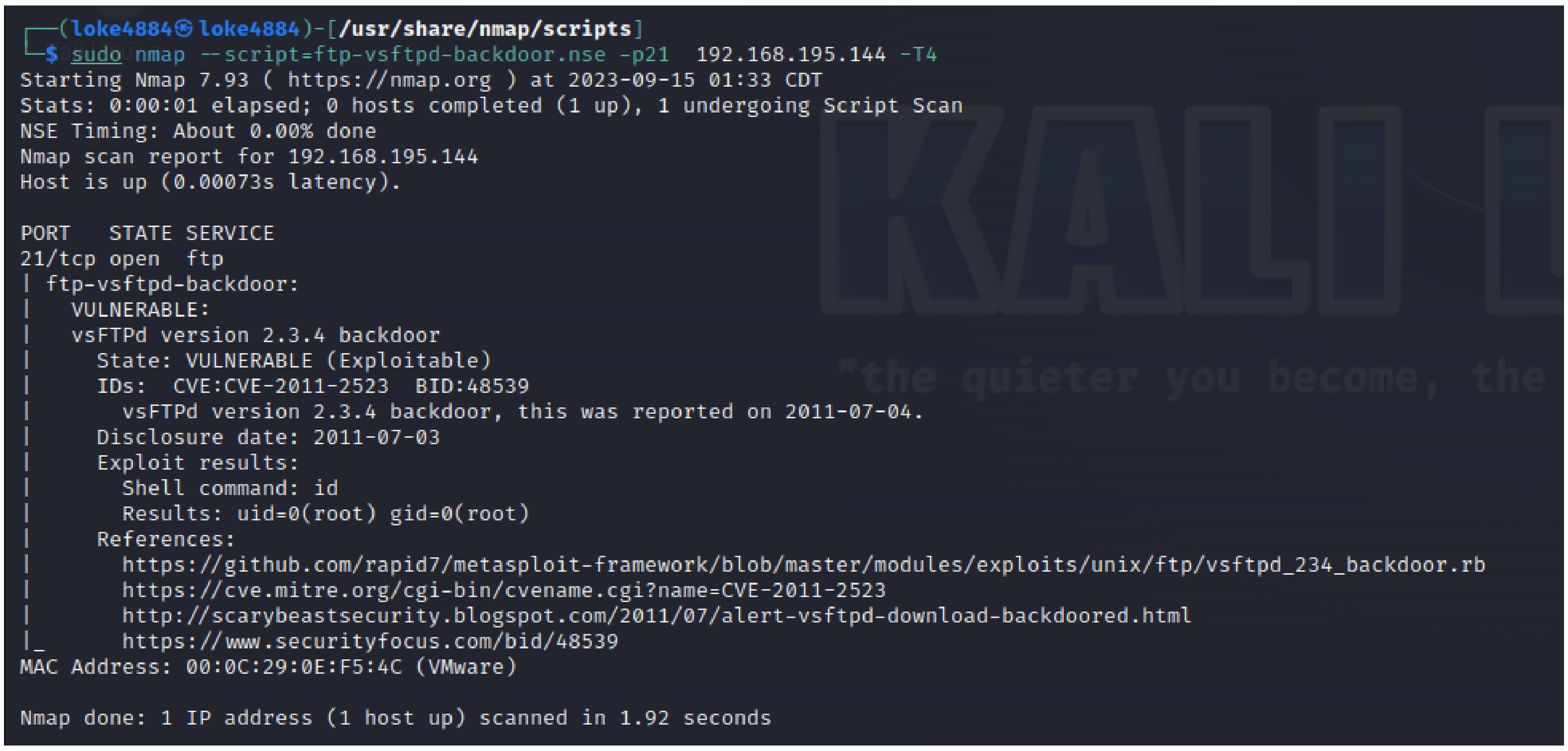
```
┌──(loke4884㉿loke4884)-[/usr/share/nmap/scripts]
└─$ sudo nmap --script=smtp-enum-users.nse -p25 192.168.195.144

Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-15 01:29 CDT
Nmap scan report for 192.168.195.144
Host is up (0.00071s latency).

PORT   STATE SERVICE
25/tcp open  smtp
| smtp-enum-users:
|_  Method RCPT returned a unhandled status code.
MAC Address: 00:0C:29:0E:F5:4C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.02 seconds
```

ls | grep ftp



```
┌──(loke4884㉿loke4884)-[/usr/share/nmap/scripts]
└─$ ls | grep ftp
ftp-anon.nse
ftp-bounce.nse
ftp-brute.nse
ftp-libopie.nse
ftp-proftpd-backdoor.nse
ftp-syst.nse
ftp-vsftpd-backdoor.nse
ftp-vuln-cve2010-4221.nse
tftp-enum.nse
```

sudo nmap --script=ftp-vsftpd-backdoor.nse -p21 192.168.195.144 -T4



```
┌──(loke4884㉿loke4884)-[/usr/share/nmap/scripts]
└─$ sudo nmap --script=ftp-vsftpd-backdoor.nse -p21  192.168.195.144 -T4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-15 01:33 CDT
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 0.00% done
Nmap scan report for 192.168.195.144
Host is up (0.00073s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  BID:48539
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|_      https://www.securityfocus.com/bid/48539
MAC Address: 00:0C:29:0E:F5:4C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.92 seconds
```

Inverse Scan

When normal scan is failed then Inverse scan is used , there is a chance to bypass firewall to hit Open port

If normal scan shows all as Filtered ,Closed there is chance that Firewall is blocking then you can go for Inverse to find Open port which cant be triggered by firewall there is a chance to bypass firewall also

3 type of scans those are Fin , Null ,Xmas

For Fin → Fin = 1 ,Remaining All = 0

For Null → All =0

For Xmas → Fin =1 ,Push =1 , Urg =1 remaining All =0

If port is closed → has response

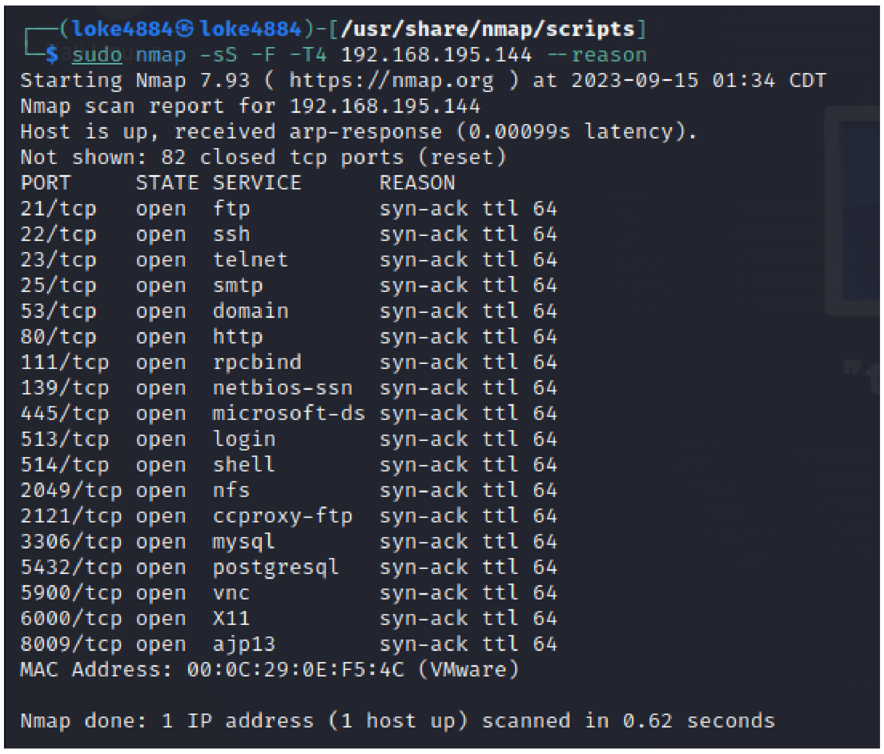
If port is open → No response

-sF → Fin

-sN → Null

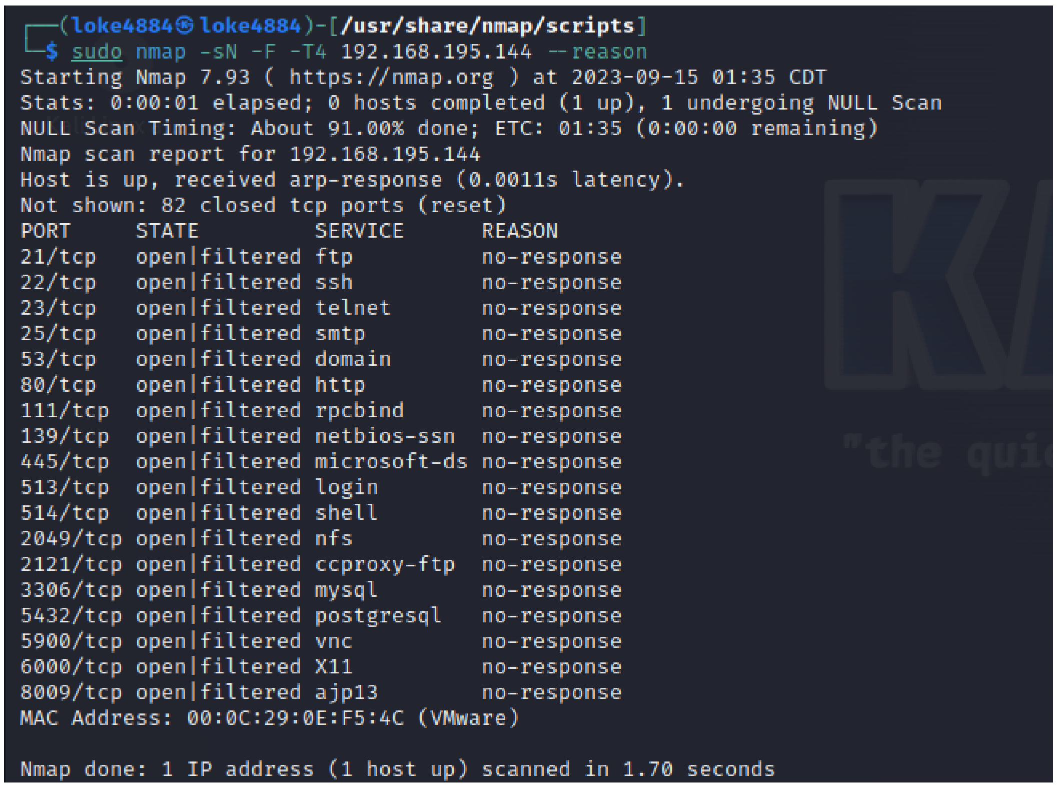
-sX → Xmus

sudo nmap -sS -F -T4 192.168.195.144 -- reason



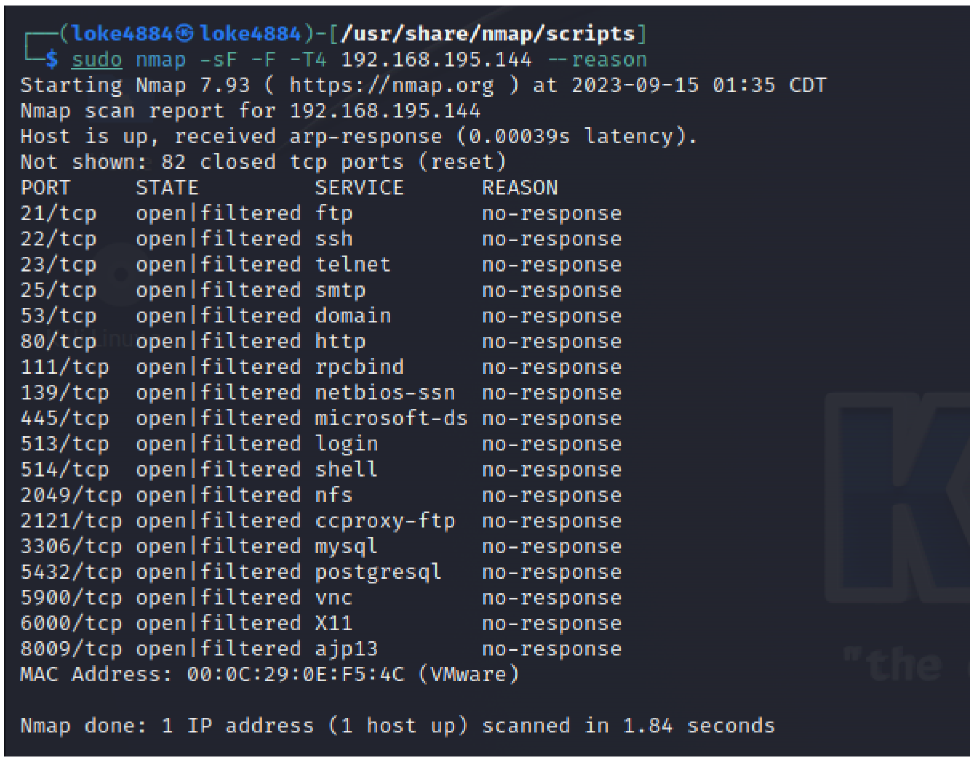
```
┌──(loke4884㉿loke4884)-[/usr/share/nmap/scripts]
└─$ sudo nmap -sS -F -T4 192.168.195.144 --reason
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-15 01:34 CDT
Nmap scan report for 192.168.195.144
Host is up, received arp-response (0.00099s latency).
Not shown: 82 closed tcp ports (reset)
PORT     STATE SERVICE      REASON
21/tcp   open  ftp          syn-ack ttl 64
22/tcp   open  ssh          syn-ack ttl 64
23/tcp   open  telnet       syn-ack ttl 64
25/tcp   open  smtp         syn-ack ttl 64
53/tcp   open  domain       syn-ack ttl 64
80/tcp   open  http         syn-ack ttl 64
111/tcp  open  rpcbind      syn-ack ttl 64
139/tcp  open  netbios-ssn  syn-ack ttl 64
445/tcp  open  microsoft-ds syn-ack ttl 64
513/tcp  open  login        syn-ack ttl 64
514/tcp  open  shell        syn-ack ttl 64
2049/tcp open  nfs          syn-ack ttl 64
2121/tcp open  ccproxy-ftp  syn-ack ttl 64
3306/tcp open  mysql        syn-ack ttl 64
5432/tcp open  postgresql   syn-ack ttl 64
5900/tcp open  vnc          syn-ack ttl 64
6000/tcp open  X11          syn-ack ttl 64
8009/tcp open  ajp13        syn-ack ttl 64
MAC Address: 00:0C:29:0E:F5:4C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.62 seconds
```

sudo nmap -sN -F -T4 192.168.195.144 --reason



```
┌──(loke4884㉿loke4884)-[/usr/share/nmap/scripts]
└─$ sudo nmap -sN -F -T4 192.168.195.144 --reason
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-15 01:35 CDT
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing NULL Scan
NULL Scan Timing: About 91.00% done; ETC: 01:35 (0:00:00 remaining)
Nmap scan report for 192.168.195.144
Host is up, received arp-response (0.0011s latency).
Not shown: 82 closed tcp ports (reset)
PORT     STATE         SERVICE      REASON
21/tcp   open|filtered ftp          no-response
22/tcp   open|filtered ssh          no-response
23/tcp   open|filtered telnet       no-response
25/tcp   open|filtered smtp         no-response
53/tcp   open|filtered domain       no-response
80/tcp   open|filtered http         no-response
111/tcp  open|filtered rpcbind      no-response
139/tcp  open|filtered netbios-ssn  no-response
445/tcp  open|filtered microsoft-ds no-response
513/tcp  open|filtered login        no-response
514/tcp  open|filtered shell        no-response
2049/tcp open|filtered nfs          no-response
2121/tcp open|filtered ccproxy-ftp  no-response
3306/tcp open|filtered mysql        no-response
5432/tcp open|filtered postgresql   no-response
5900/tcp open|filtered vnc          no-response
6000/tcp open|filtered X11          no-response
8009/tcp open|filtered ajp13        no-response
MAC Address: 00:0C:29:0E:F5:4C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.70 seconds
```

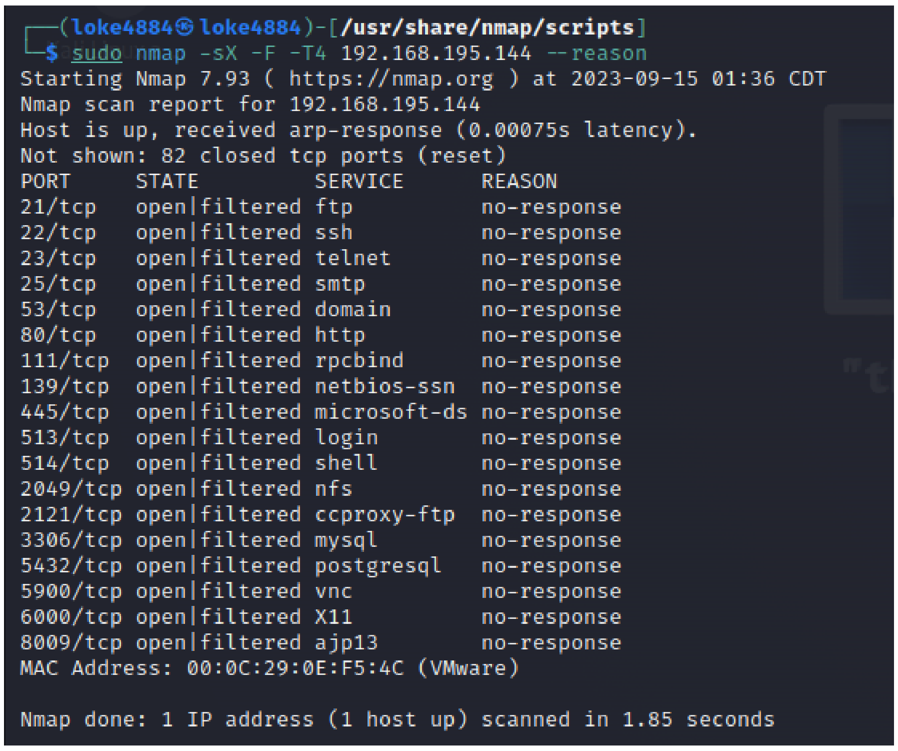
sudo nmap -sF -F -T4 192.168.195.144 -- reason



```
┌──(loke4884㉿loke4884)-[/usr/share/nmap/scripts]
└─$ sudo nmap -sF -F -T4 192.168.195.144 --reason
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-15 01:35 CDT
Nmap scan report for 192.168.195.144
Host is up, received arp-response (0.00039s latency).
Not shown: 82 closed tcp ports (reset)
PORT     STATE         SERVICE      REASON
21/tcp   open|filtered ftp          no-response
22/tcp   open|filtered ssh          no-response
23/tcp   open|filtered telnet       no-response
25/tcp   open|filtered smtp         no-response
53/tcp   open|filtered domain       no-response
80/tcp   open|filtered http         no-response
111/tcp  open|filtered rpcbind      no-response
139/tcp  open|filtered netbios-ssn  no-response
445/tcp  open|filtered microsoft-ds no-response
513/tcp  open|filtered login        no-response
514/tcp  open|filtered shell        no-response
2049/tcp open|filtered nfs          no-response
2121/tcp open|filtered ccproxy-ftp  no-response
3306/tcp open|filtered mysql        no-response
5432/tcp open|filtered postgresql   no-response
5900/tcp open|filtered vnc          no-response
6000/tcp open|filtered X11          no-response
8009/tcp open|filtered ajp13        no-response
MAC Address: 00:0C:29:0E:F5:4C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.84 seconds
```

sudo nmap -sX -F -T4 192.168.195.144 –reason

-sX → Xmus



```
┌──(loke4884㉿loke4884)-[/usr/share/nmap/scripts]
└─$ sudo nmap -sX -F -T4 192.168.195.144 --reason
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-15 01:36 CDT
Nmap scan report for 192.168.195.144
Host is up, received arp-response (0.00075s latency).
Not shown: 82 closed tcp ports (reset)
PORT     STATE         SERVICE      REASON
21/tcp   open|filtered ftp          no-response
22/tcp   open|filtered ssh          no-response
23/tcp   open|filtered telnet       no-response
25/tcp   open|filtered smtp         no-response
53/tcp   open|filtered domain       no-response
80/tcp   open|filtered http         no-response
111/tcp  open|filtered rpcbind      no-response
139/tcp  open|filtered netbios-ssn  no-response
445/tcp  open|filtered microsoft-ds no-response
513/tcp  open|filtered login        no-response
514/tcp  open|filtered shell        no-response
2049/tcp open|filtered nfs          no-response
2121/tcp open|filtered ccproxy-ftp  no-response
3306/tcp open|filtered mysql        no-response
5432/tcp open|filtered postgresql   no-response
5900/tcp open|filtered vnc          no-response
6000/tcp open|filtered X11          no-response
8009/tcp open|filtered ajp13        no-response
MAC Address: 00:0C:29:0E:F5:4C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.85 seconds
```

Refer 20 network scanning tools : https://intellipaat.com/blog/network-scanning-tools/