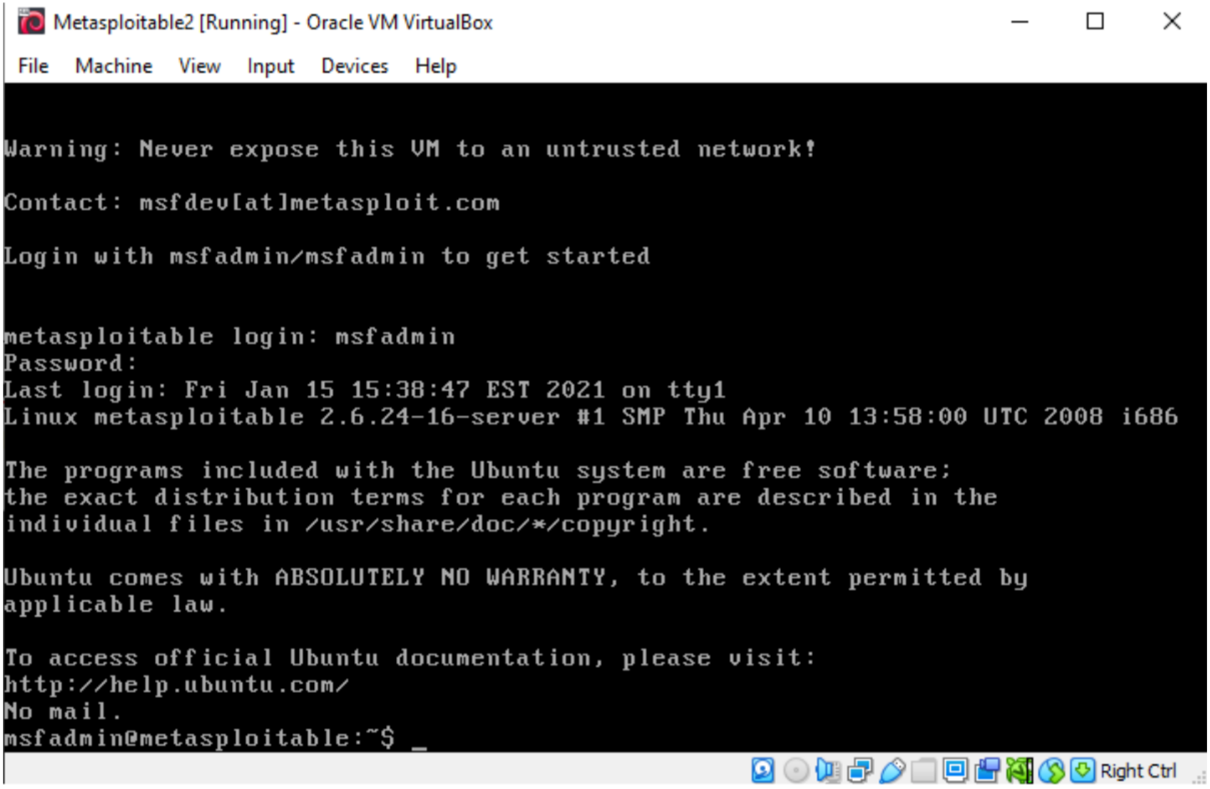
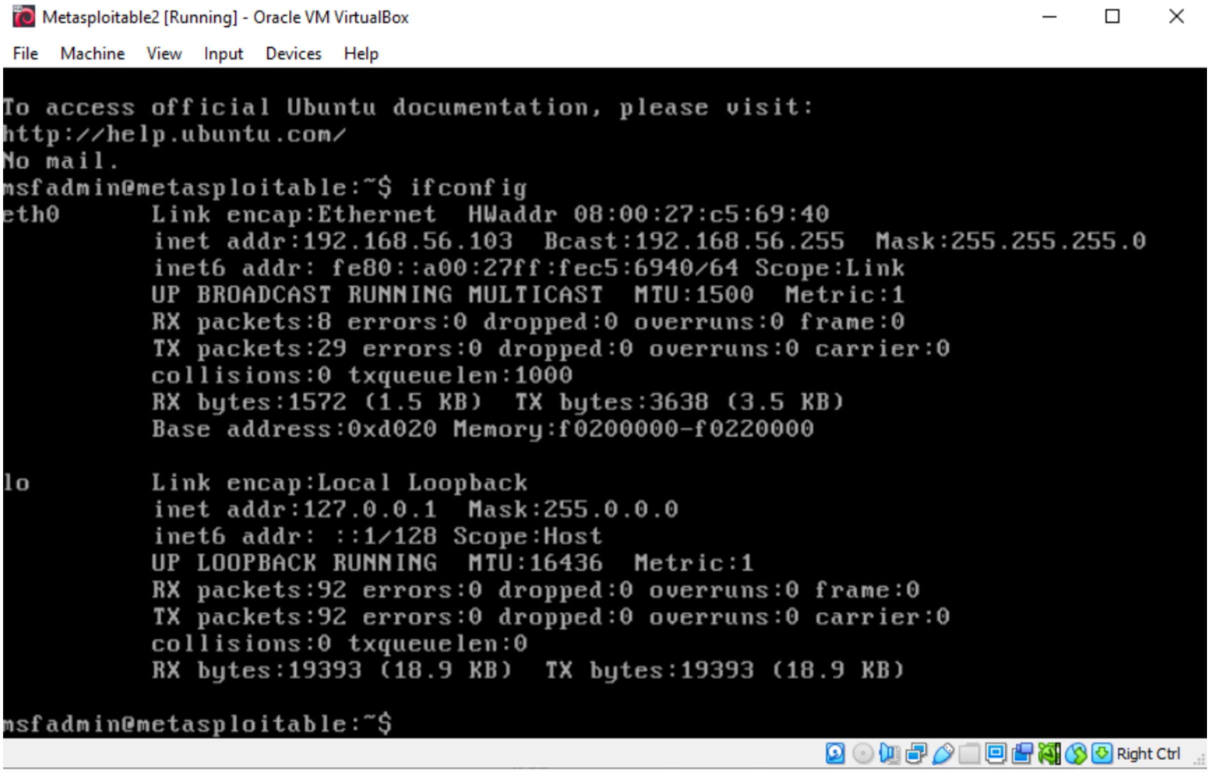
Network Scanning using nmap

- After installing the metasploitable 2 virtual machine, logged into the machine using metasploitable username/password as msfadmin/msfadmin

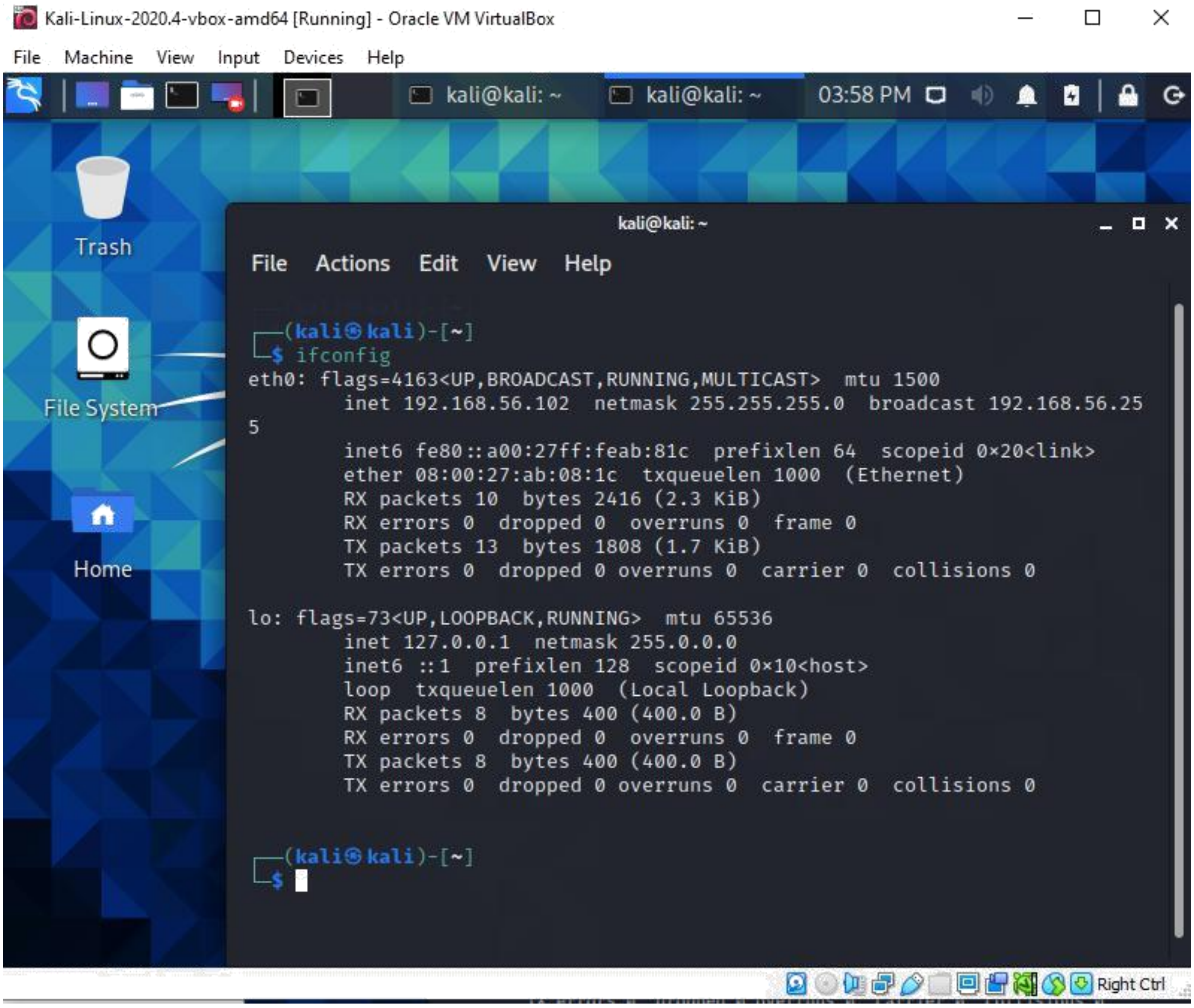


```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Fri Jan 15 15:38:47 EST 2021 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ _
```



```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:c5:69:40
          inet addr:192.168.56.103  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fec5:6940/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:29 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1572 (1.5 KB)  TX bytes:3638 (3.5 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)

msfadmin@metasploitable:~$
```

- Also installed another virtual machine i.e kali linux on virtual box.



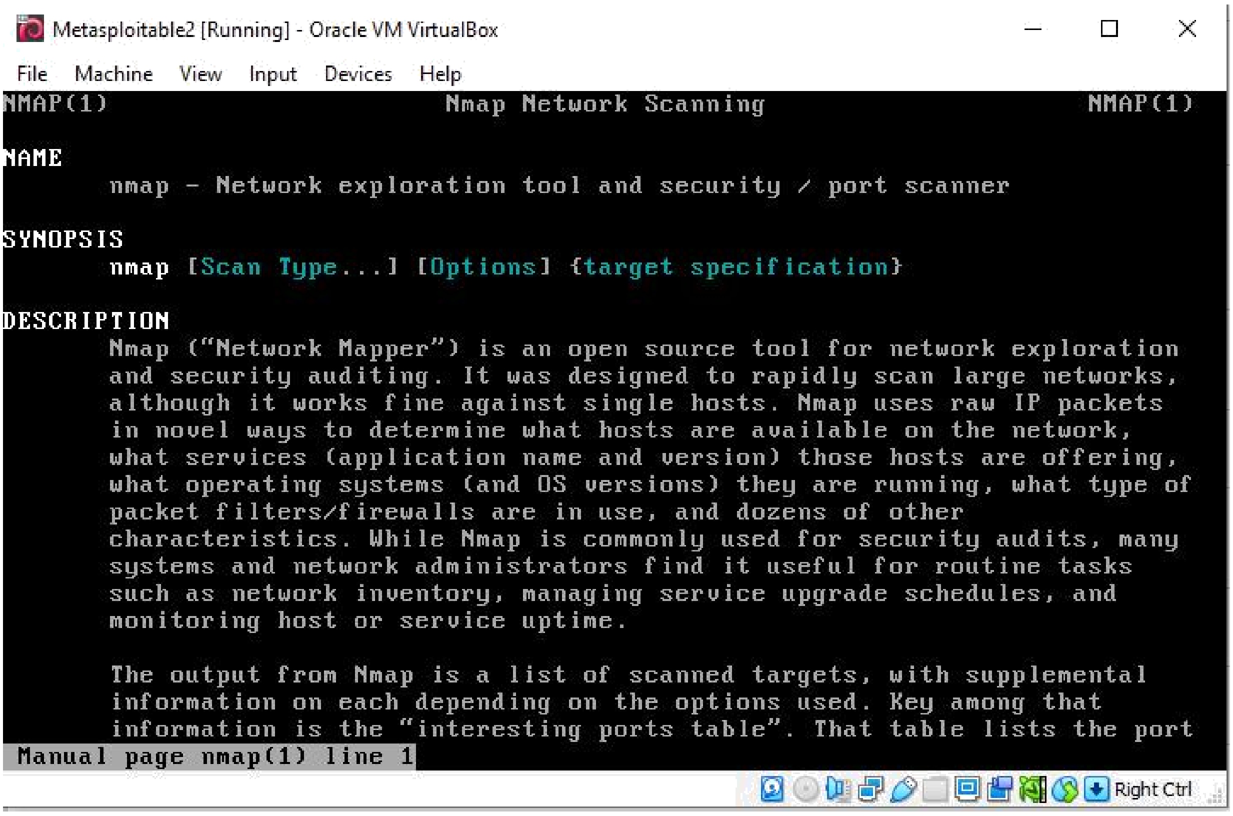
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.102  netmask 255.255.255.0  broadcast 192.168.56.25
5
        inet6 fe80::a00:27ff:feab:81c  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:ab:08:1c  txqueuelen 1000  (Ethernet)
        RX packets 10  bytes 2416 (2.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 13  bytes 1808 (1.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 400 (400.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 400 (400.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ 
```

IP address of both machines:

- Kali linux: 192.168.56.102
- Metasploitable2: 192.168.56.103

Task 1: Getting started with nmap

1) **man nmap**


Metasploitable2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
NMAP(1)                      Nmap Network Scanning                      NMAP(1)

NAME
       nmap - Network exploration tool and security / port scanner

SYNOPSIS
       nmap [Scan Type...] [Options] {target specification}

DESCRIPTION
       Nmap ("Network Mapper") is an open source tool for network exploration
       and security auditing. It was designed to rapidly scan large networks,
       although it works fine against single hosts. Nmap uses raw IP packets
       in novel ways to determine what hosts are available on the network,
       what services (application name and version) those hosts are offering,
       what operating systems (and OS versions) they are running, what type of
       packet filters/firewalls are in use, and dozens of other
       characteristics. While Nmap is commonly used for security audits, many
       systems and network administrators find it useful for routine tasks
       such as network inventory, managing service upgrade schedules, and
       monitoring host or service uptime.

       The output from Nmap is a list of scanned targets, with supplemental
       information on each depending on the options used. Key among that
       information is the "interesting ports table". That table lists the port
 Manual page nmap(1) line 1
```

2) What do the following switches do?

- **-sn:** No port scan.
  This option tells Nmap not to do a port scan after host discovery, and only print out the available hosts that responded to the scan.

- **-PO:** IP Protocol Ping.
  This option sends IP packets with the specified protocol number set in their IP header.

- **-PS:** TCP SYN Ping.
  This option sends an empty TCP packet with the SYN flag set.

- **-PU:** UDP Ping.
  This option sends a UDP packet to the given ports.

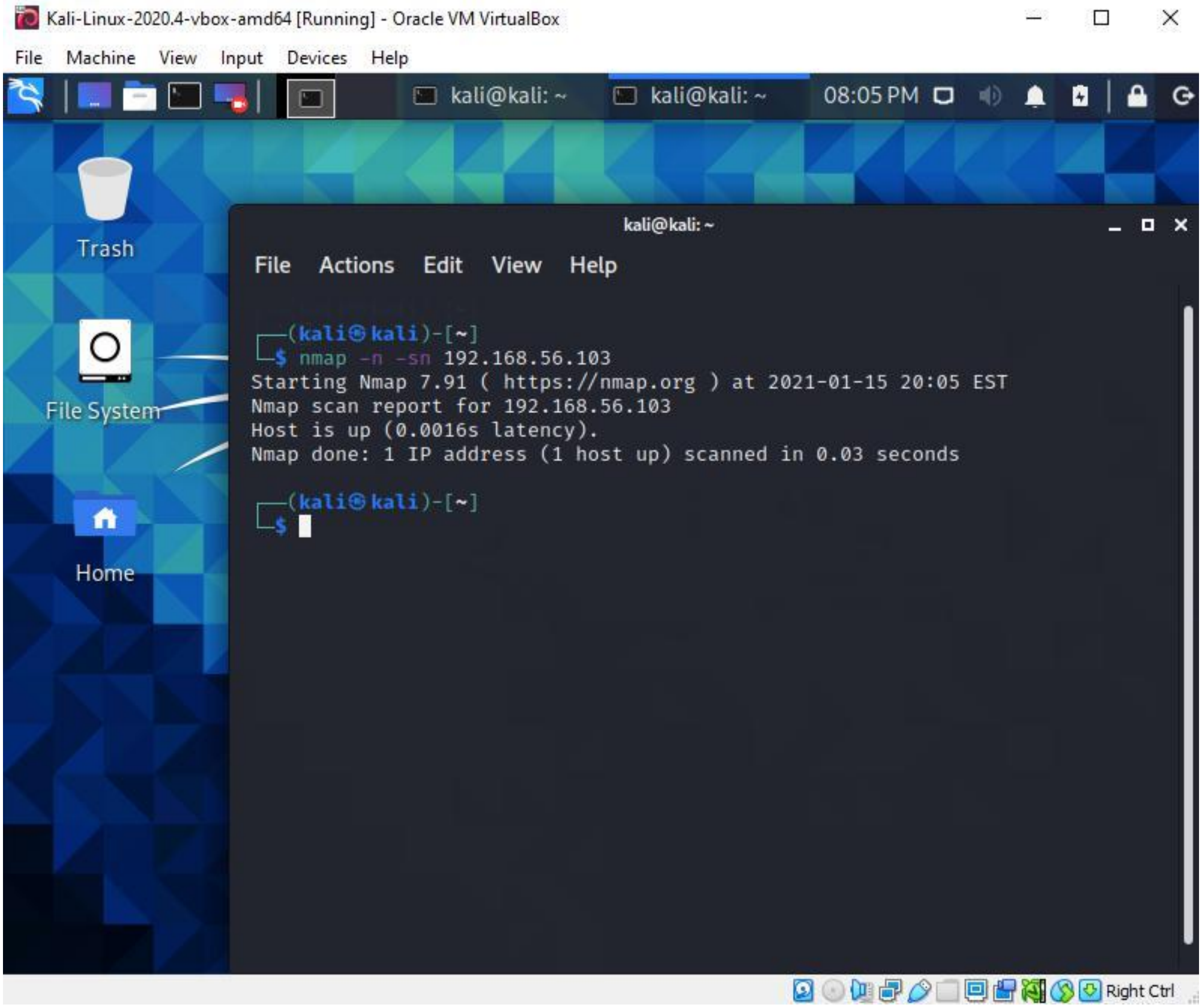
- **-sO:** IP Protocol Scan.
  IP protocol scan allows you to determine which IP protocols (TCP, ICMP, IGMP, etc.) are supported by target machines.

- **-sV:** Service/Version detection**.**
  Probe open ports to determine service/version info.

- **-O:** Enable OS detection.

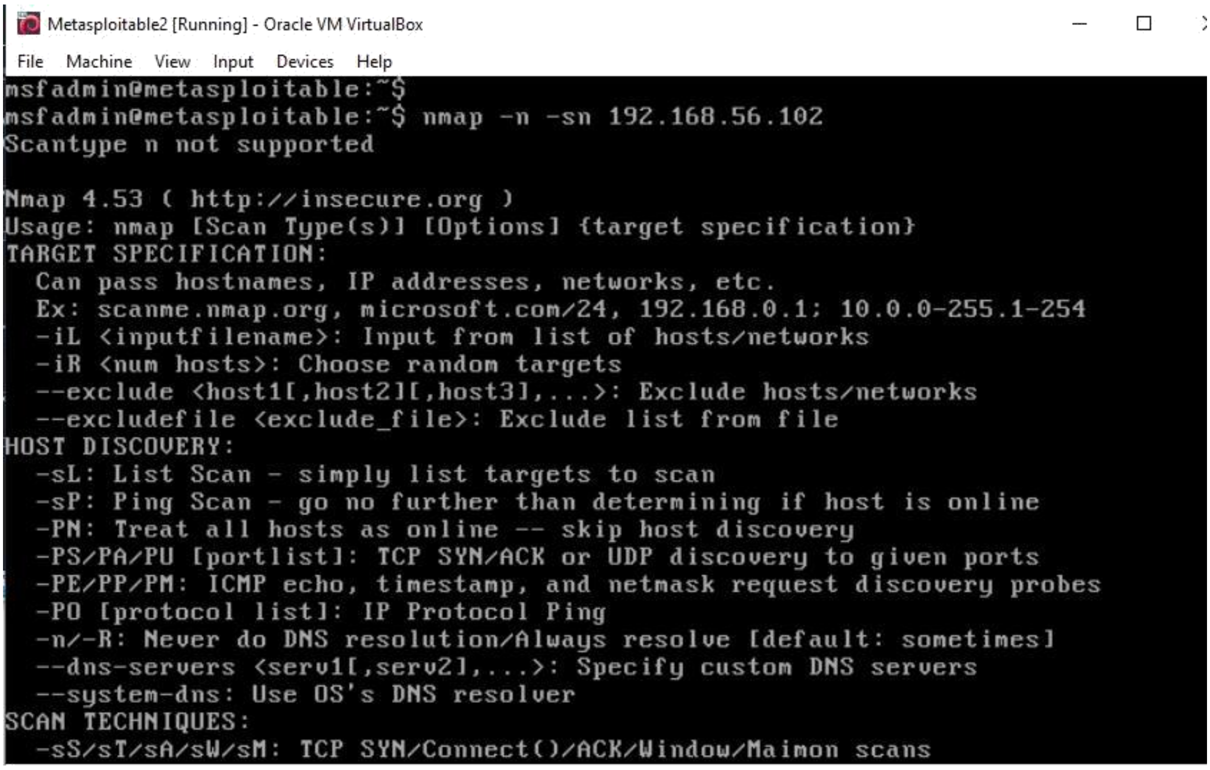
Task 2: Using nmap to conduct a reconnaissance of your network

1. **Use a broad ping scan to determine the hosts that are "up" on a portion of your lab network**
   nmap -n -sn IPaddress
   i) **Record the results.**
      a) Scanned 192.168.56.103 from kali linux machine.


Kali-Linux-2020.4-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
kali@kali: ~
08:05 PM
Trash
File System
Home
kali@kali: ~
File Actions Edit View Help
Right Ctrl

```
┌──(kali㉿kali)-[~]
└─$ nmap -n -sn 192.168.56.103
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-15 20:05 EST
Nmap scan report for 192.168.56.103
Host is up (0.0016s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

b) When scanned 192.168.56.102 from kali linux machine, getting Scantype n not supported.

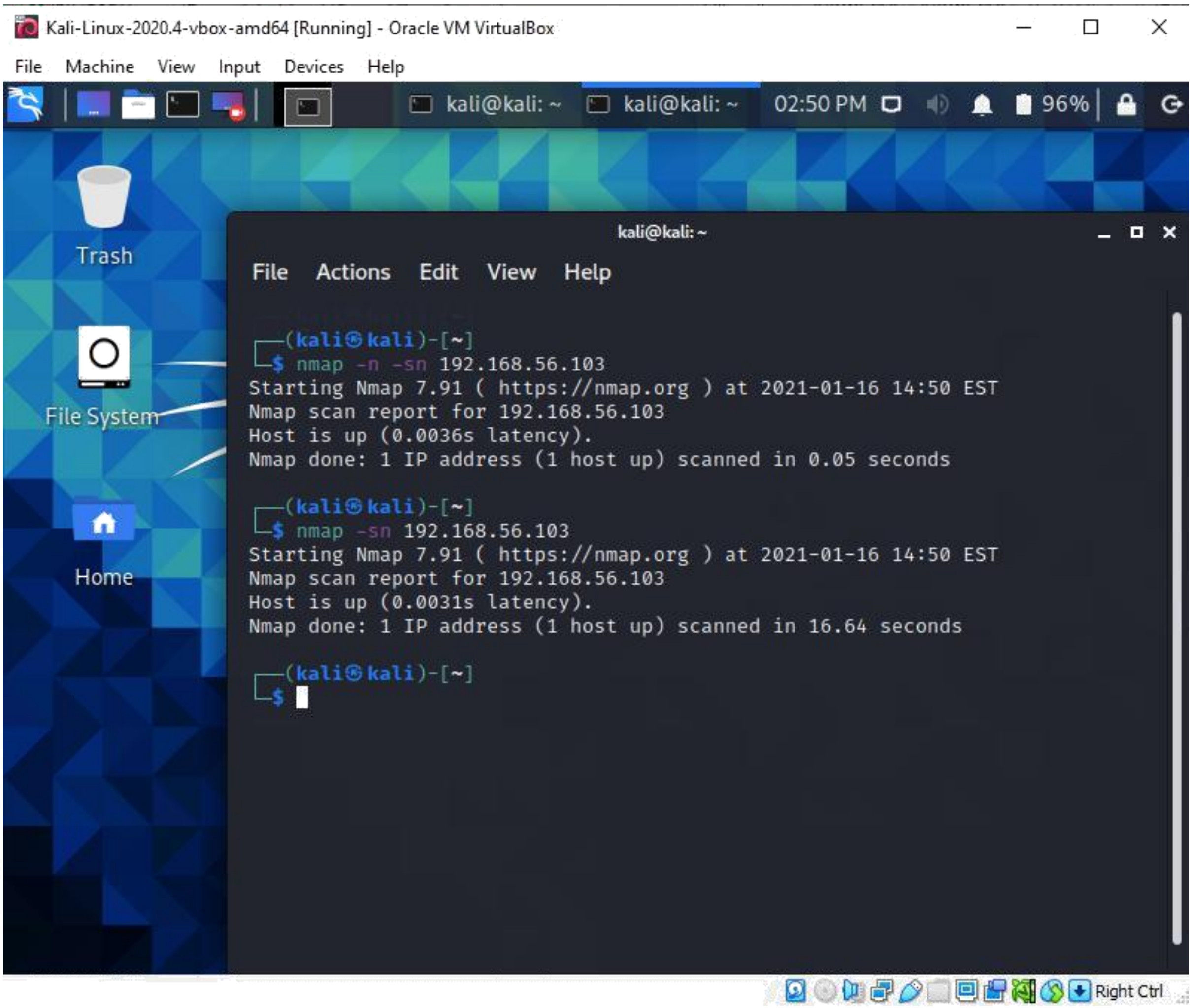


Metasploitable2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

```
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ nmap -n -sn 192.168.56.102
Scantype n not supported

Nmap 4.53 ( http://insecure.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
  -sP: Ping Scan - go no further than determining if host is online
  -PN: Treat all hosts as online -- skip host discovery
  -PS/PA/PU [portlist]: TCP SYN/ACK or UDP 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
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
```

ii) **Why is the -n option used? What happens if you rerun this command without the -n option?**

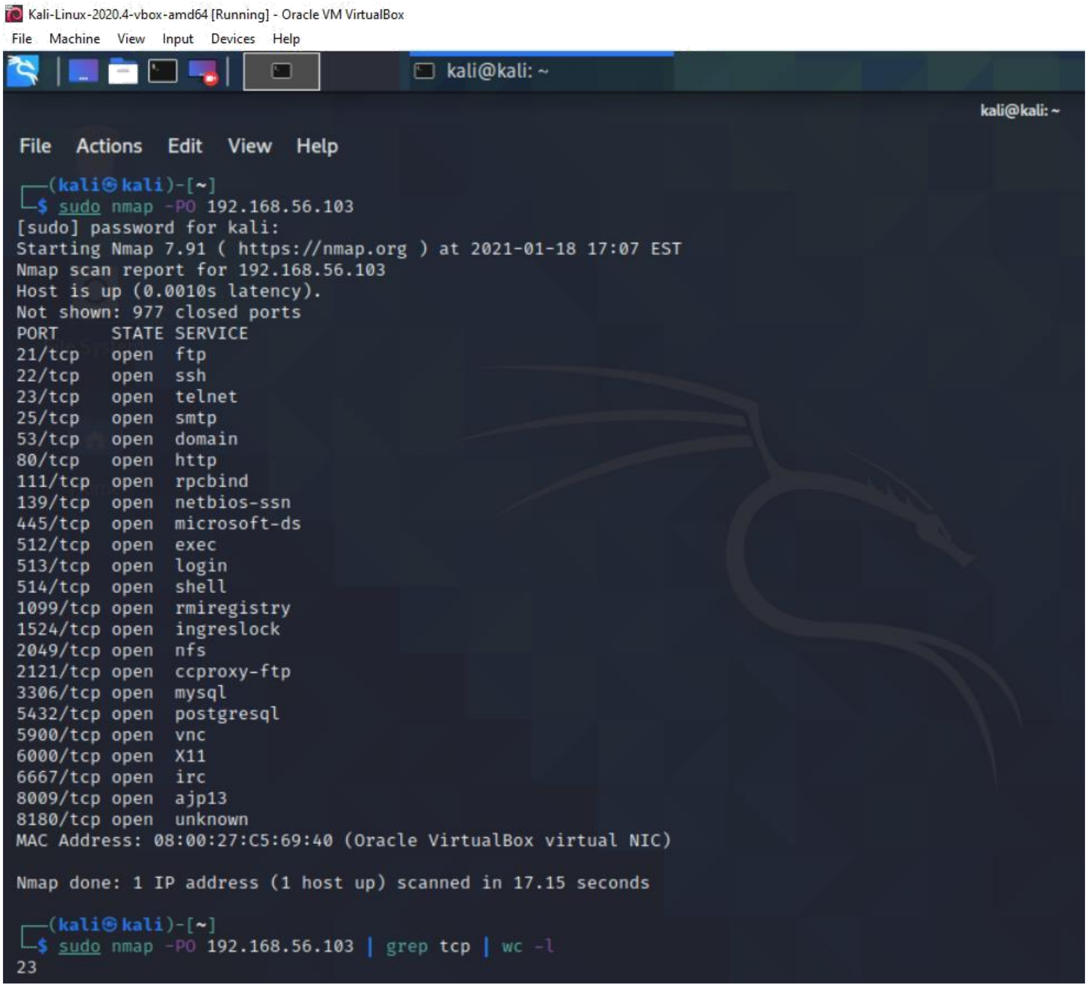
The -n option is used when IP address never do DNS resolution or always resolve. The scanning of IP address took longer time after re-running this command without the -n option.


Kali-Linux-2020.4-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
kali@kali: ~
02:50 PM
96%
Trash
File System
Home
kali@kali: ~
File Actions Edit View Help
Right Ctrl

```
┌──(kali㉿kali)-[~]
└─$ nmap -n -sn 192.168.56.103
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-16 14:50 EST
Nmap scan report for 192.168.56.103
Host is up (0.0036s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.56.103
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-16 14:50 EST
Nmap scan report for 192.168.56.103
Host is up (0.0031s latency).
Nmap done: 1 IP address (1 host up) scanned in 16.64 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

2. **Conduct an IP protocol ping (switch -PO / -PS / -PU) on the Common Network hosts. Note that for this scan "nmap needs to read raw responses off the wire"; you may need to use sudo to have sufficient privilege.**

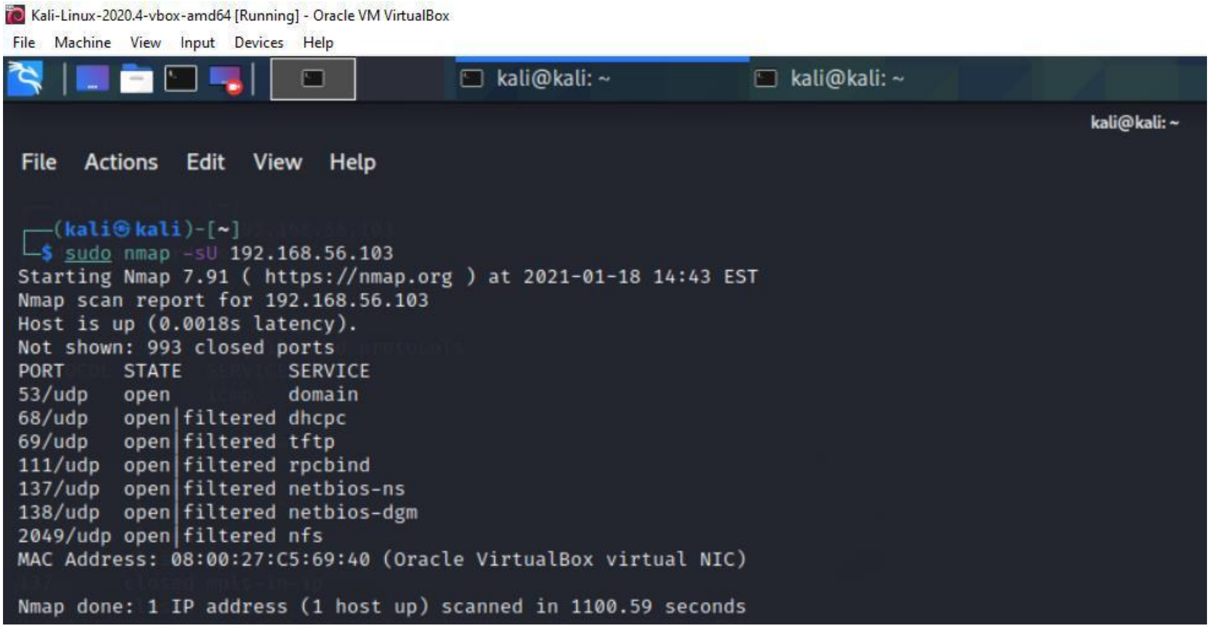
i) **How many TCP ports are open on each?** 23 TCP ports are open on each.


Kali-Linux-2020.4-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
kali@kali: ~
File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -PO 192.168.56.103
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-18 17:07 EST
Nmap scan report for 192.168.56.103
Host is up (0.0010s latency).
Not shown: 977 closed ports
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: 08:00:27:C5:69:40 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 17.15 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -PO 192.168.56.103 | grep tcp | wc -l
23
```

ii) Are there any UDP ports open on any machine?

Yes, there are few UDP ports open on metasploitable2 machine. Refer below snapshot showing the opened UDP ports.

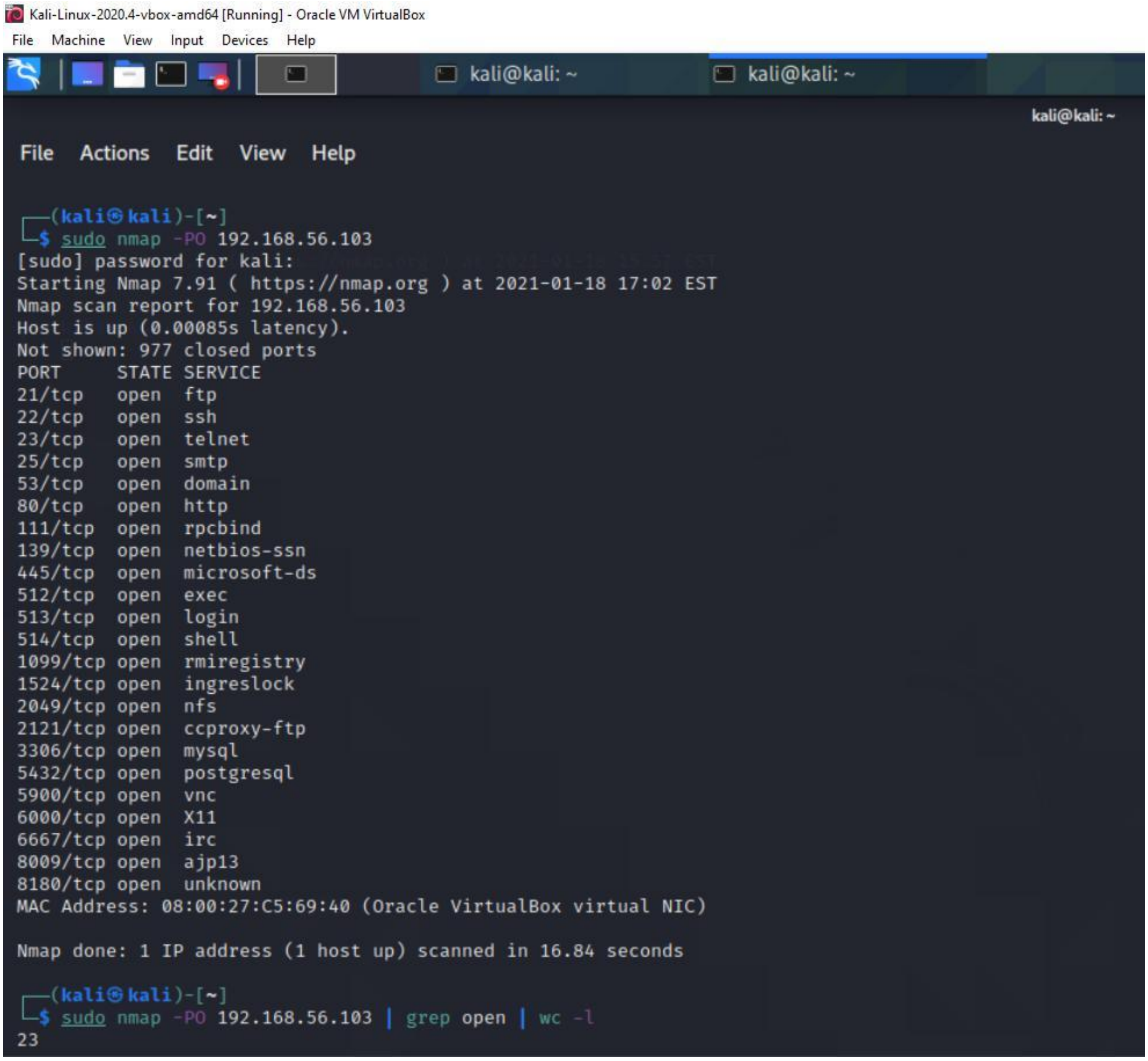

Kali-Linux-2020.4-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
kali@kali: ~
kali@kali: ~
File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU 192.168.56.103
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-18 14:43 EST
Nmap scan report for 192.168.56.103
Host is up (0.0018s latency).
Not shown: 993 closed ports
PORT     STATE         SERVICE
53/udp   open          domain
68/udp   open|filtered dhcpc
69/udp   open|filtered tftp
111/udp  open|filtered rpcbind
137/udp  open|filtered netbios-ns
138/udp  open|filtered netbios-dgm
2049/udp open|filtered nfs
MAC Address: 08:00:27:C5:69:40 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1100.59 seconds
```

3. Conduct an IP protocol ping on yourself.

i) How many ports are open?

23 ports are open. Refer below snapshot:


Kali-Linux-2020.4-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
kali@kali: ~
kali@kali: ~
File Actions Edit View Help

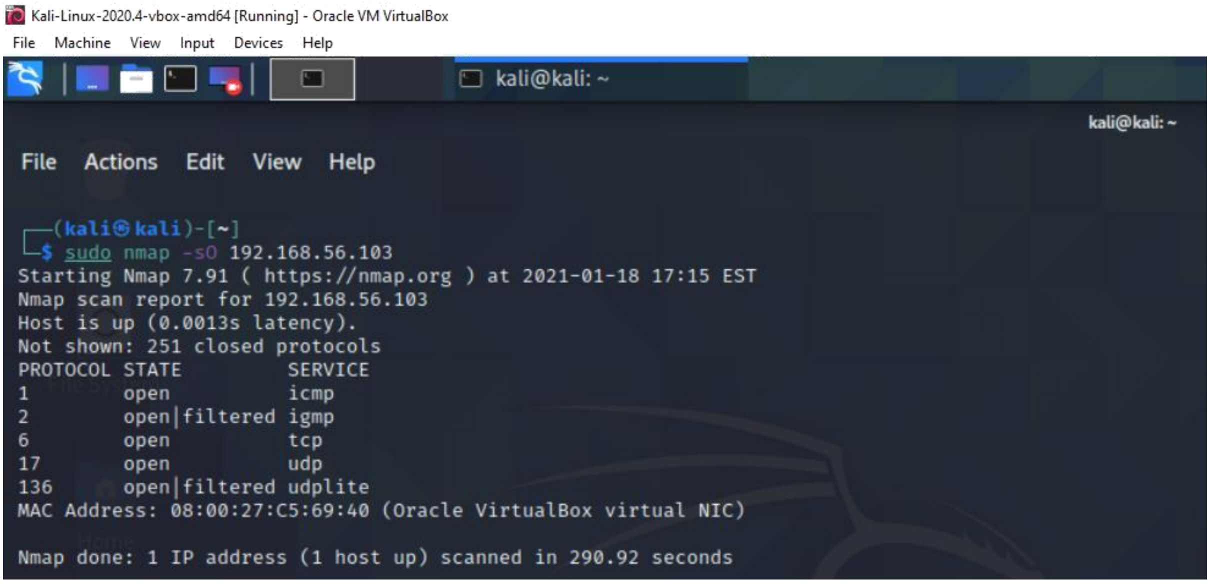
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -PO 192.168.56.103
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-18 17:02 EST
Nmap scan report for 192.168.56.103
Host is up (0.00085s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
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: 08:00:27:C5:69:40 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.84 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -PO 192.168.56.103 | grep open | wc -l
23
```

4. Conduct an IP protocol scan (switch -sO) on target host; note that you may have to use sudo to have sufficient privilege for this scan. Be patient, this will take a while.

i) Are the results different than that attained with the IP protocol ping? Explain. The results of IP protocol scan are different than that attained with the IP protocol ping.

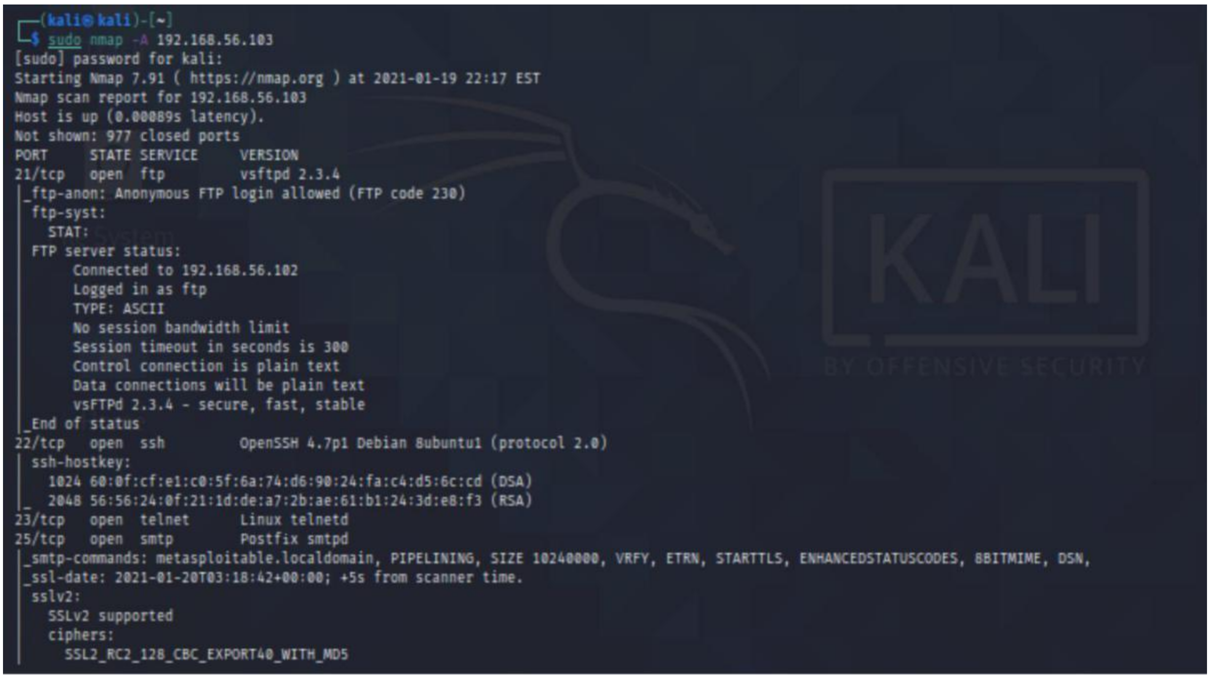
IP protocol scan allows you to determine which IP protocols (TCP, ICMP, IGMP, etc.) are supported by target machines.

IP protocol ping sends IP packets with the specified protocol number set in their IP header.

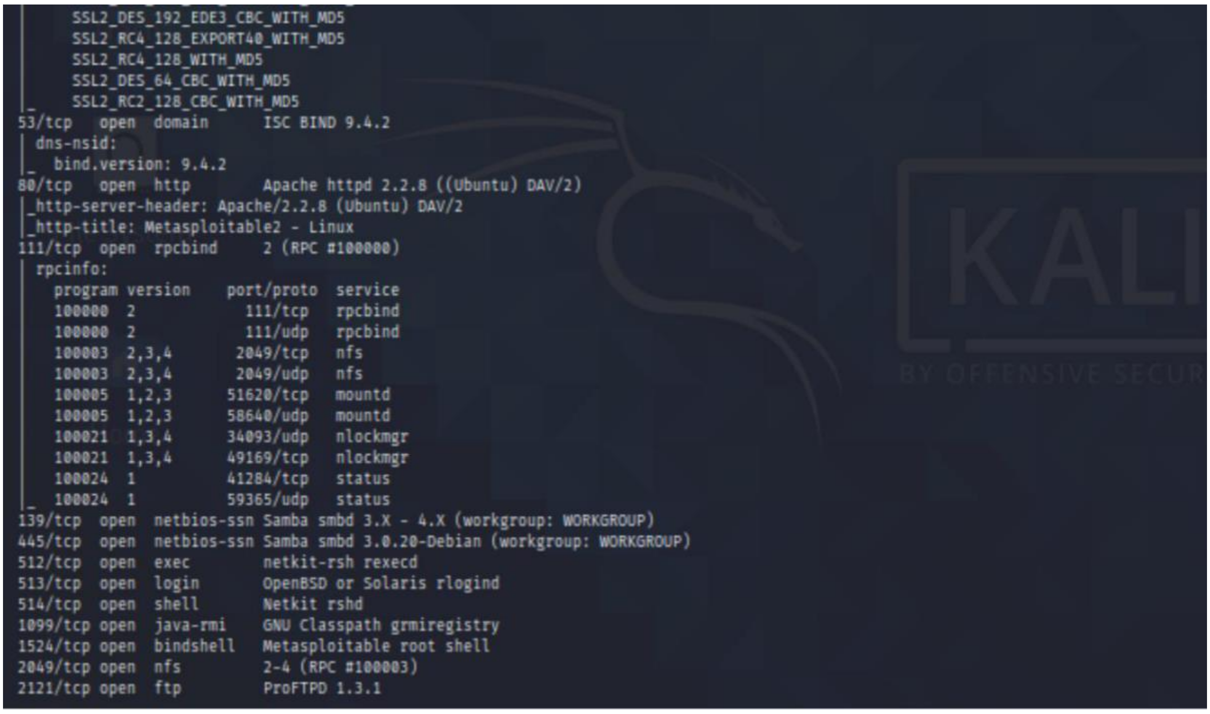

Kali-Linux-2020.4-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
kali@kali: ~
File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sO 192.168.56.103
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-18 17:15 EST
Nmap scan report for 192.168.56.103
Host is up (0.0013s latency).
Not shown: 251 closed protocols
PROTOCOL STATE         SERVICE
1        open          icmp
2        open|filtered igmp
6        open          tcp
17       open          udp
136      open|filtered udplite
MAC Address: 08:00:27:C5:69:40 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 290.92 seconds
```

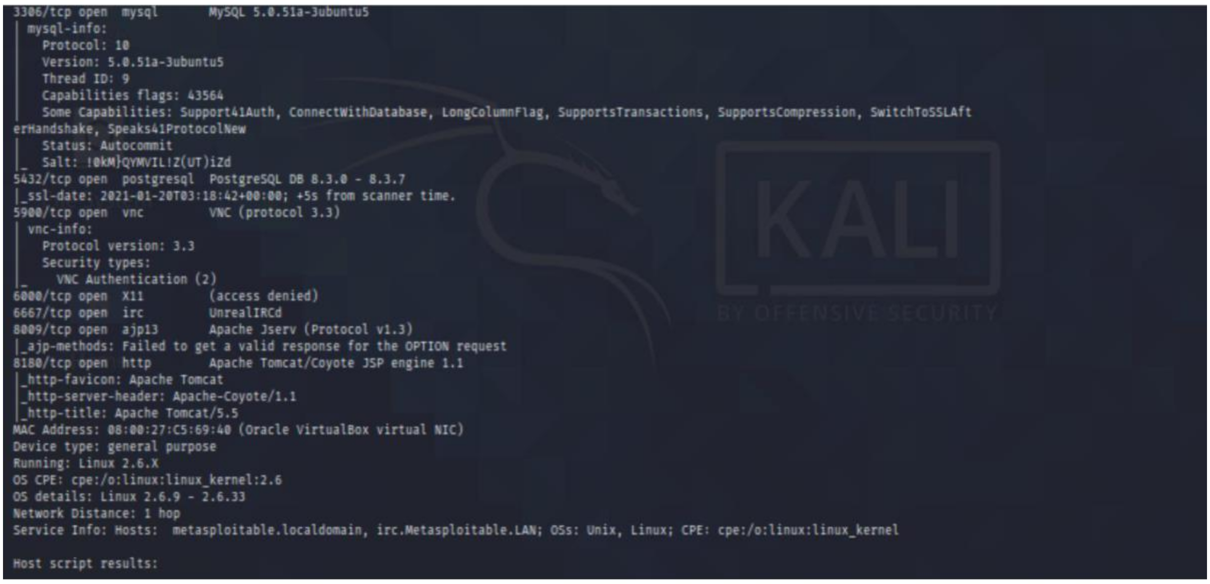
5. **nmap is often capable of determining the operating system of a scanned host. {Hint: read the OS Detection section of the man pages and again note that you may need to use sudo to have sufficient privilege.}**
   Which OS is running on the host? "OS Fingerprinting"
   Linux OS is running on the host.



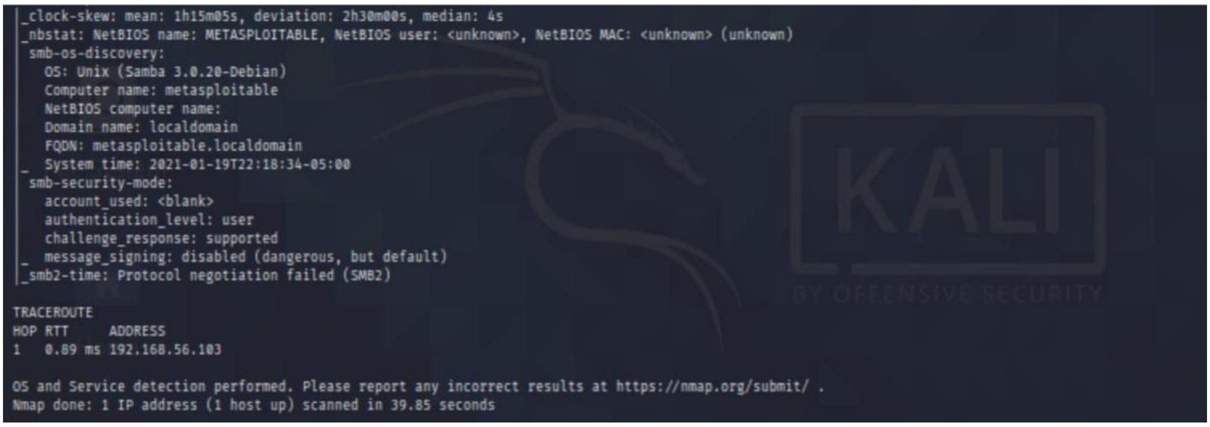
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A 192.168.56.103
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-19 22:17 EST
Nmap scan report for 192.168.56.103
Host is up (0.00089s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.56.102
|      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 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (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: 2021-01-20T03:18:42+00:00; +5s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
```



```
|       SSL2_DES_192_EDE3_CBC_WITH_MD5
|       SSL2_RC4_128_EXPORT40_WITH_MD5
|       SSL2_RC4_128_WITH_MD5
|       SSL2_DES_64_CBC_WITH_MD5
|_      SSL2_RC2_128_CBC_WITH_MD5
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      51620/tcp   mountd
|   100005  1,2,3      58640/udp   mountd
|   100021  1,3,4      34093/udp   nlockmgr
|   100021  1,3,4      49169/tcp   nlockmgr
|   100024  1          41284/tcp   status
|_  100024  1          59365/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  shell       Netkit rshd
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: 9
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, ConnectWithDatabase, LongColumnFlag, SupportsTransactions, SupportsCompression, SwitchToSSLAft
erHandshake, Speaks41ProtocolNew
|   Status: Autocommit
|_  Salt: !0kM}QYMVIL!Z(UT)iZd
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2021-01-20T03:18:42+00:00; +5s 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-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
MAC Address: 08:00:27:C5:69:40 (Oracle VirtualBox virtual NIC)
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:
```



```
|_clock-skew: mean: 1h15m05s, deviation: 2h30m00s, median: 4s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2021-01-19T22:18:34-05:00
| 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   0.89 ms 192.168.56.103

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 39.85 seconds
```

i. **What operating system does nmap think your Server VM is running?** Linux 2.6.X

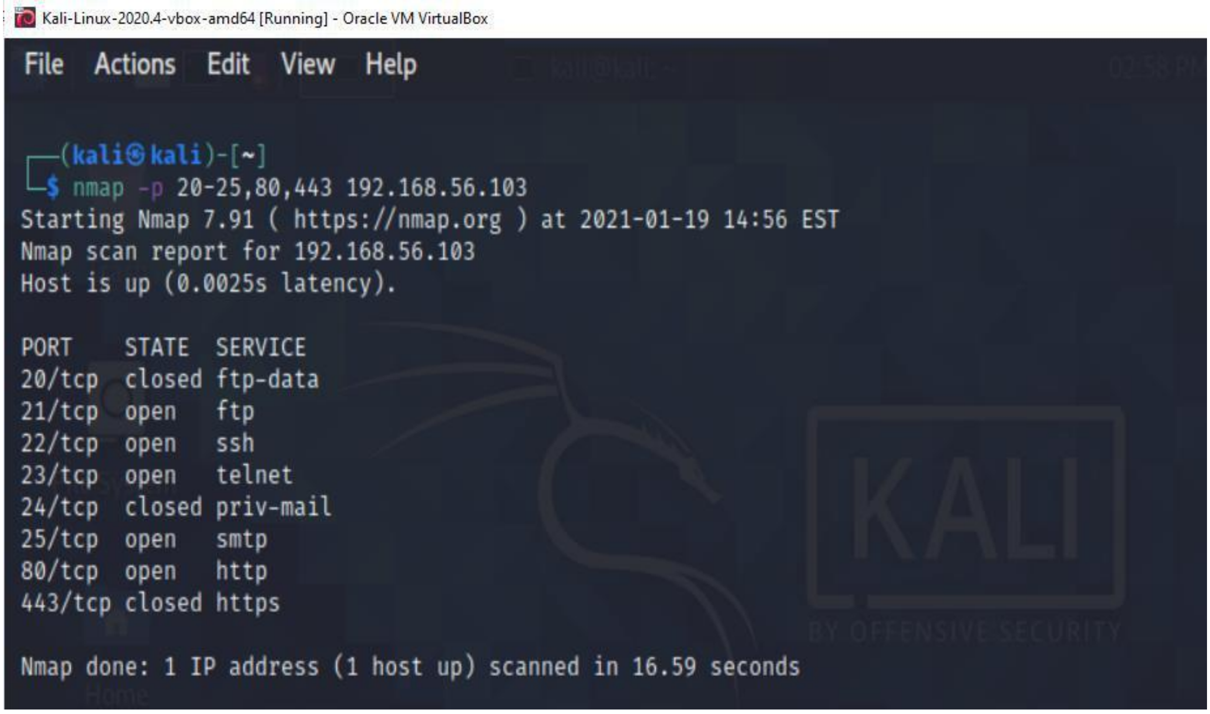
ii. **What is its MAC address?**
Its MAC address is *08:00:27:C5:69:40*

iii. **What operating system does nmap think your Linux VM is running?**
Unix

6. **nmap is also often able to determine the version number of various services running as software applications**

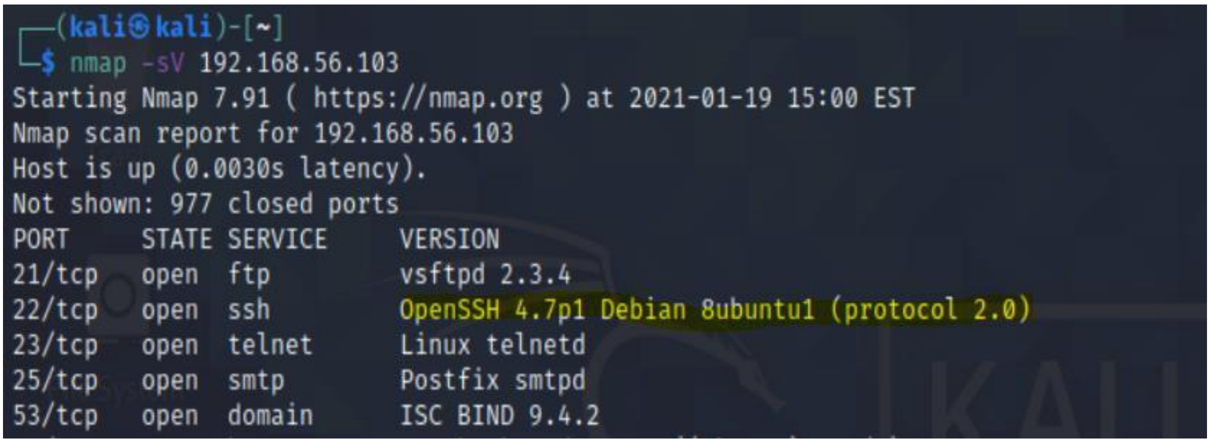
i. **Investigate how to restrict the application scans to specific sets of port numbers, otherwise your scans may take a long time to complete.**
nmap -p 20-25,80,443 192.168.56.103 command the application (here

192.168.56.103) scans will be restrict to specific port numbers. Hence, instead of scanning all the ports, it will scan the ports ranging from 20 to 25, 80 and 443. Refer below snapshot:


Kali-Linux-2020.4-vbox-amd64 [Running] - Oracle VM VirtualBox
File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 20-25,80,443 192.168.56.103
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-19 14:56 EST
Nmap scan report for 192.168.56.103
Host is up (0.0025s latency).

PORT    STATE  SERVICE
20/tcp  closed ftp-data
21/tcp  open   ftp
22/tcp  open   ssh
23/tcp  open   telnet
24/tcp  closed priv-mail
25/tcp  open   smtp
80/tcp  open   http
443/tcp closed https

Nmap done: 1 IP address (1 host up) scanned in 16.59 seconds
```

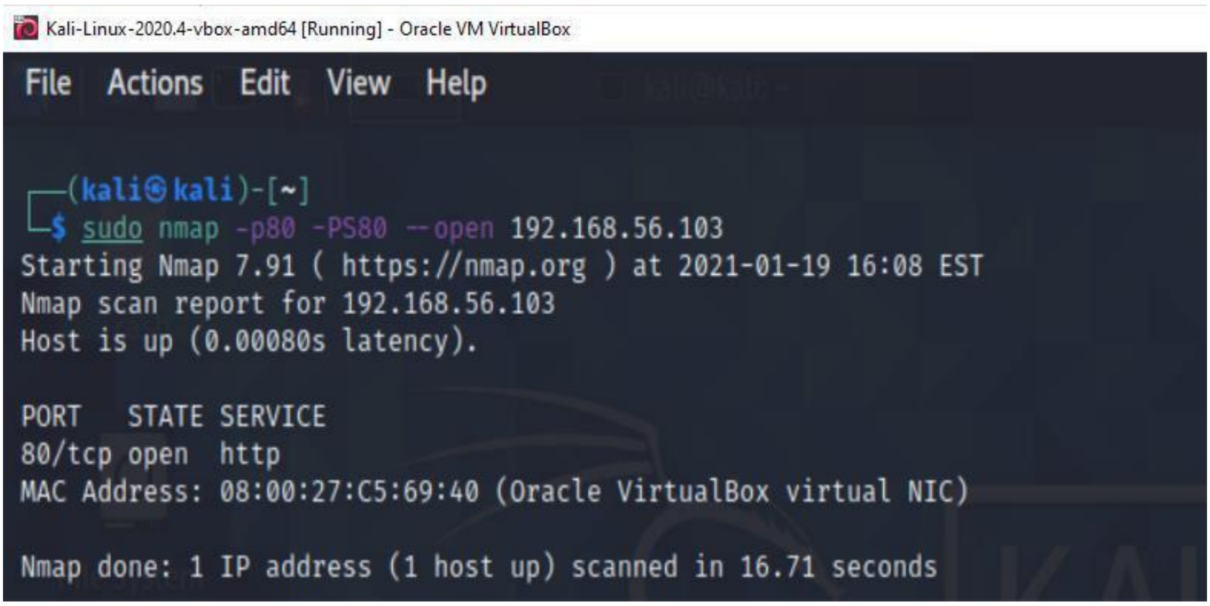
ii. **What version of ssh (or choose any other service) is running on your target host?** Version of ssh running on target host:
OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.56.103
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-19 15:00 EST
Nmap scan report for 192.168.56.103
Host is up (0.0030s latency).
Not shown: 977 closed ports
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
```

iii. **What web server is running on your target host?**

Apache HTTP web server is running on target host. Refer below snapshot:



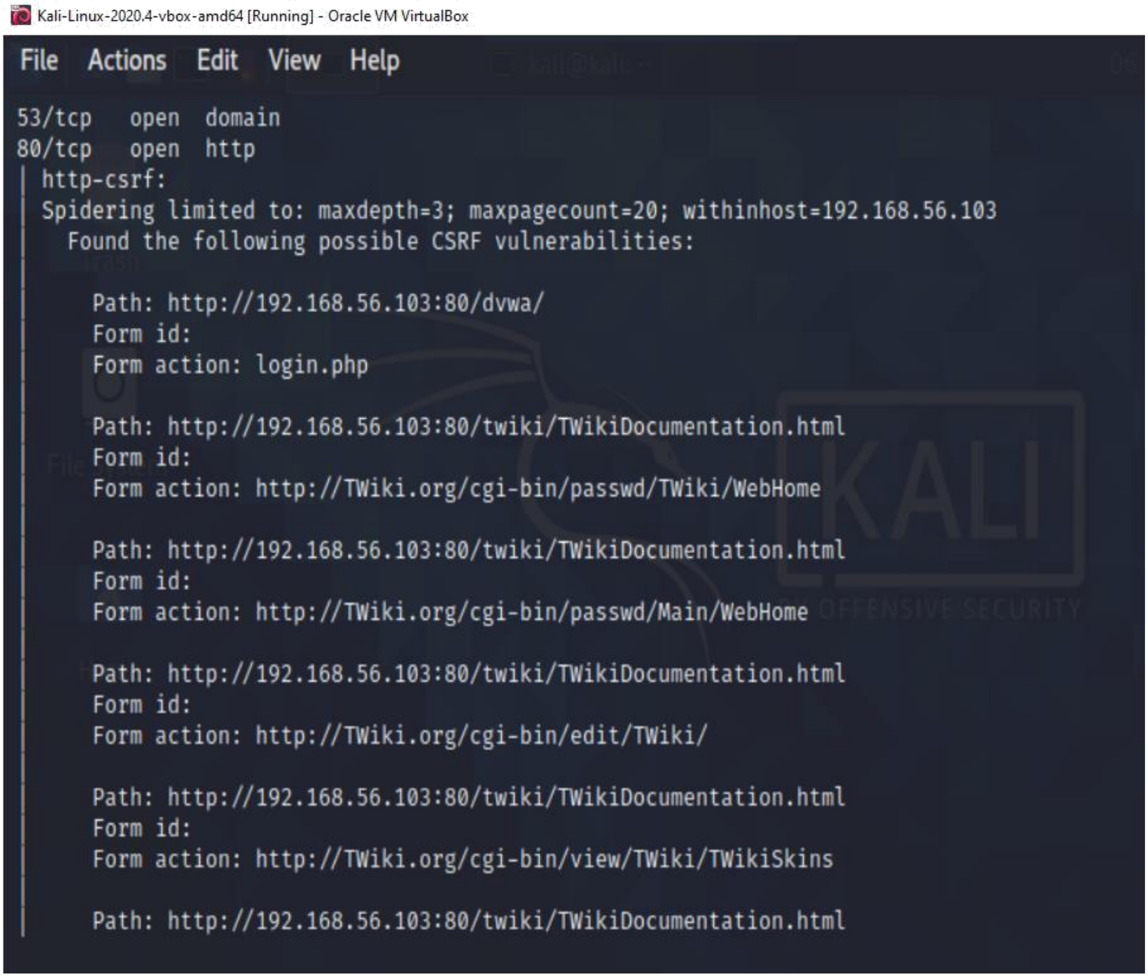
Kali-Linux-2020.4-vbox-amd64 [Running] - Oracle VM VirtualBox

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p80 -PS80 --open 192.168.56.103
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-19 16:08 EST
Nmap scan report for 192.168.56.103
Host is up (0.00080s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 08:00:27:C5:69:40 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.71 seconds
```

7. **Test if any (vulnerable) services available? "Port Scanning"**

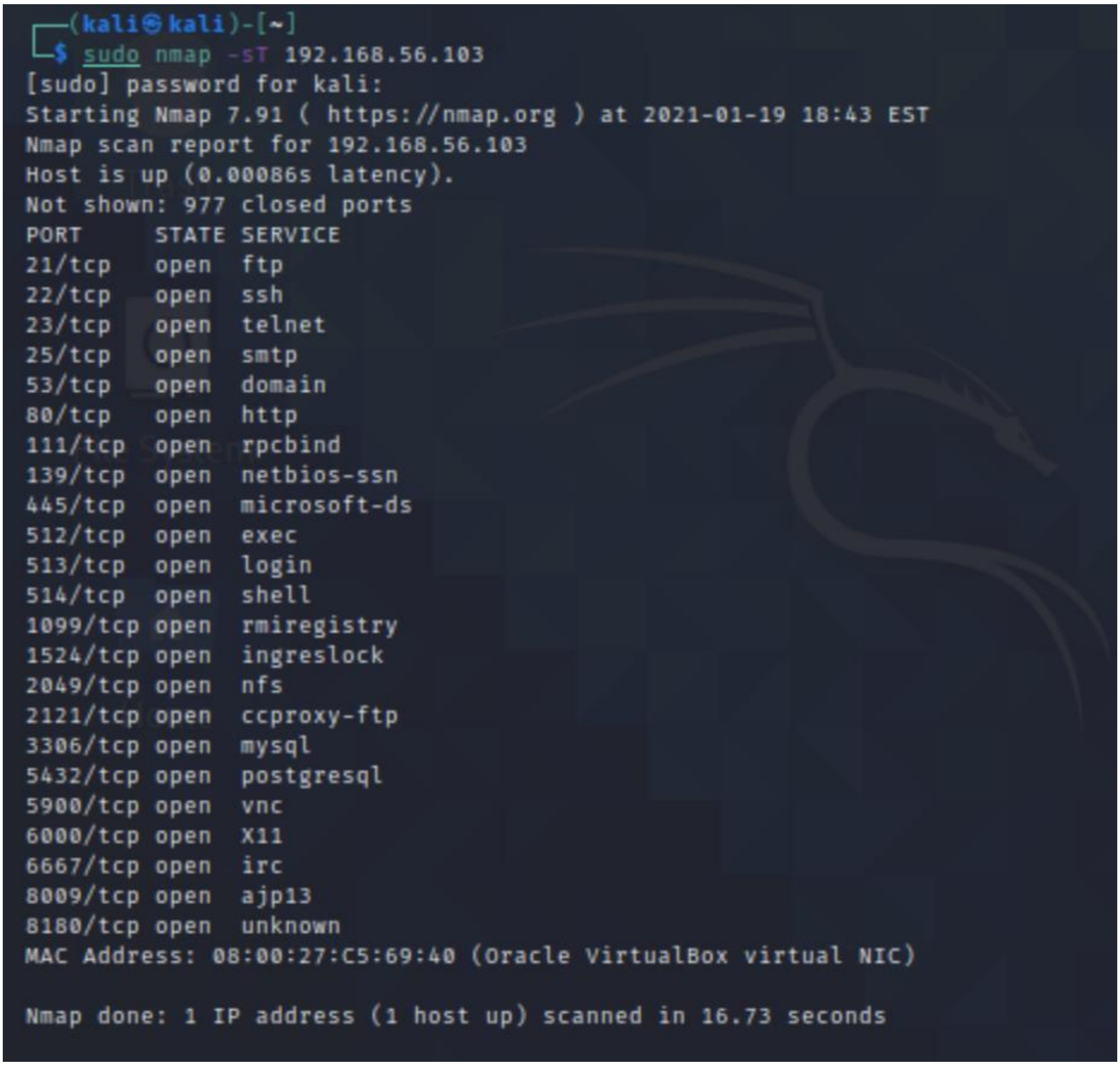
Executed given command to verify any vulnerable service available or not. *sudo nmap -v --script vuln 192.168.56.103*

Found few vulnerable services available. Refer below snapshot:


Kali-Linux-2020.4-vbox-amd64 [Running] - Oracle VM VirtualBox
File Actions Edit View Help

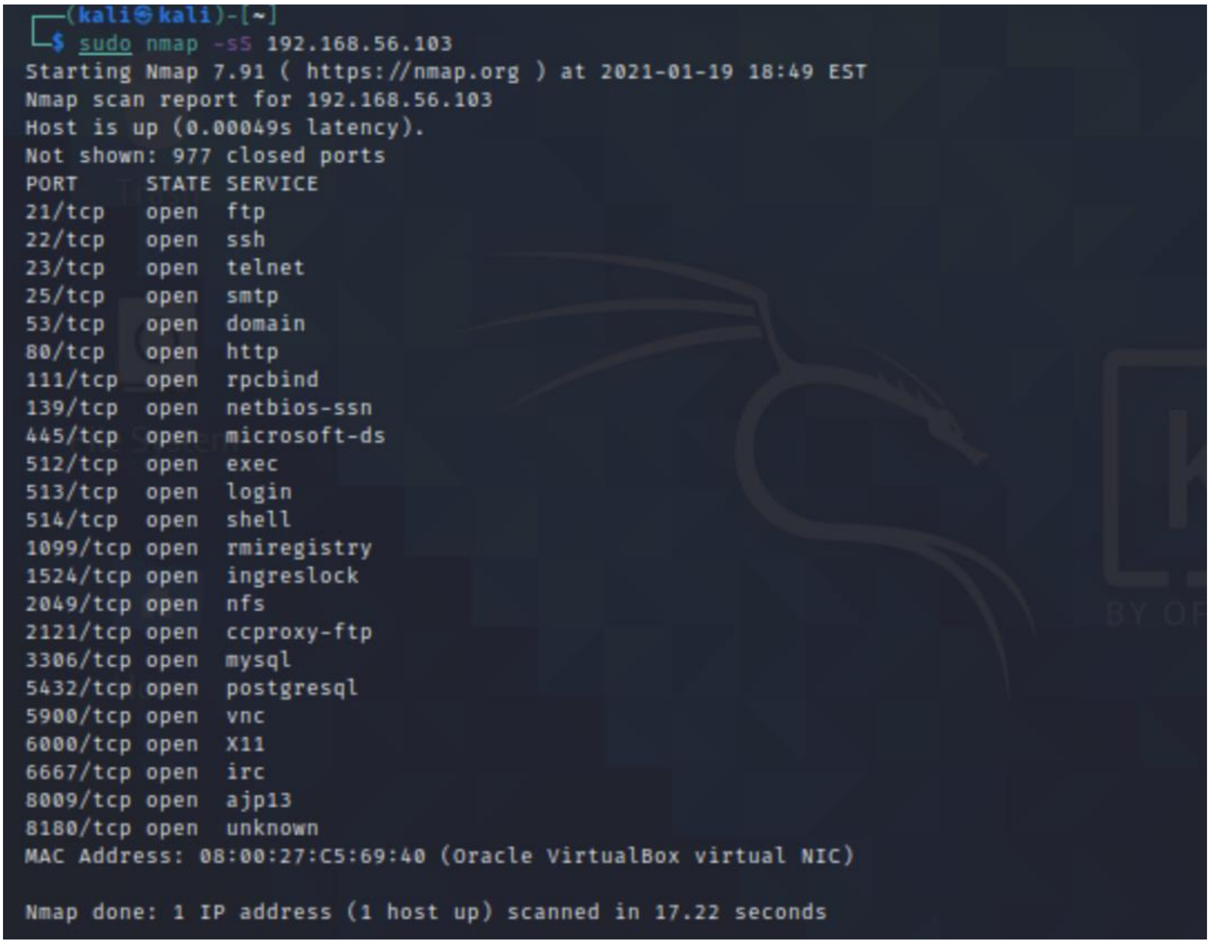
```
53/tcp   open  domain
80/tcp   open  http
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.56.103
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://192.168.56.103:80/dvwa/
|     Form id:
|     Form action: login.php
|
|     Path: http://192.168.56.103:80/twiki/TWikiDocumentation.html
|     Form id:
|     Form action: http://TWiki.org/cgi-bin/passwd/TWiki/WebHome
|
|     Path: http://192.168.56.103:80/twiki/TWikiDocumentation.html
|     Form id:
|     Form action: http://TWiki.org/cgi-bin/passwd/Main/WebHome
|
|     Path: http://192.168.56.103:80/twiki/TWikiDocumentation.html
|     Form id:
|     Form action: http://TWiki.org/cgi-bin/edit/TWiki/
|
|     Path: http://192.168.56.103:80/twiki/TWikiDocumentation.html
|     Form id:
|     Form action: http://TWiki.org/cgi-bin/view/TWiki/TWikiSkins
|
|     Path: http://192.168.56.103:80/twiki/TWikiDocumentation.html
```

- **Different types of port scans are provided by Nmap: TCP connect, TCP SYN, Stealth FIN, Xmas Tree, and Null, as well as UDP scans. Demonstrate at least a few of these scans.**
  - **TCP connect:** TCP connect scan(-sT) is the default TCP scan type when SYN scan is not an option. This is the case when a user does not have raw packet privileges. Instead of writing raw packets as most other scan types do, Nmap asks the underlying operating system to establish a connection with the target machine and port by issuing the connect system call. This is the same high-level system call that web browsers, P2P clients, and most other network-enabled applications use to establish a connection.



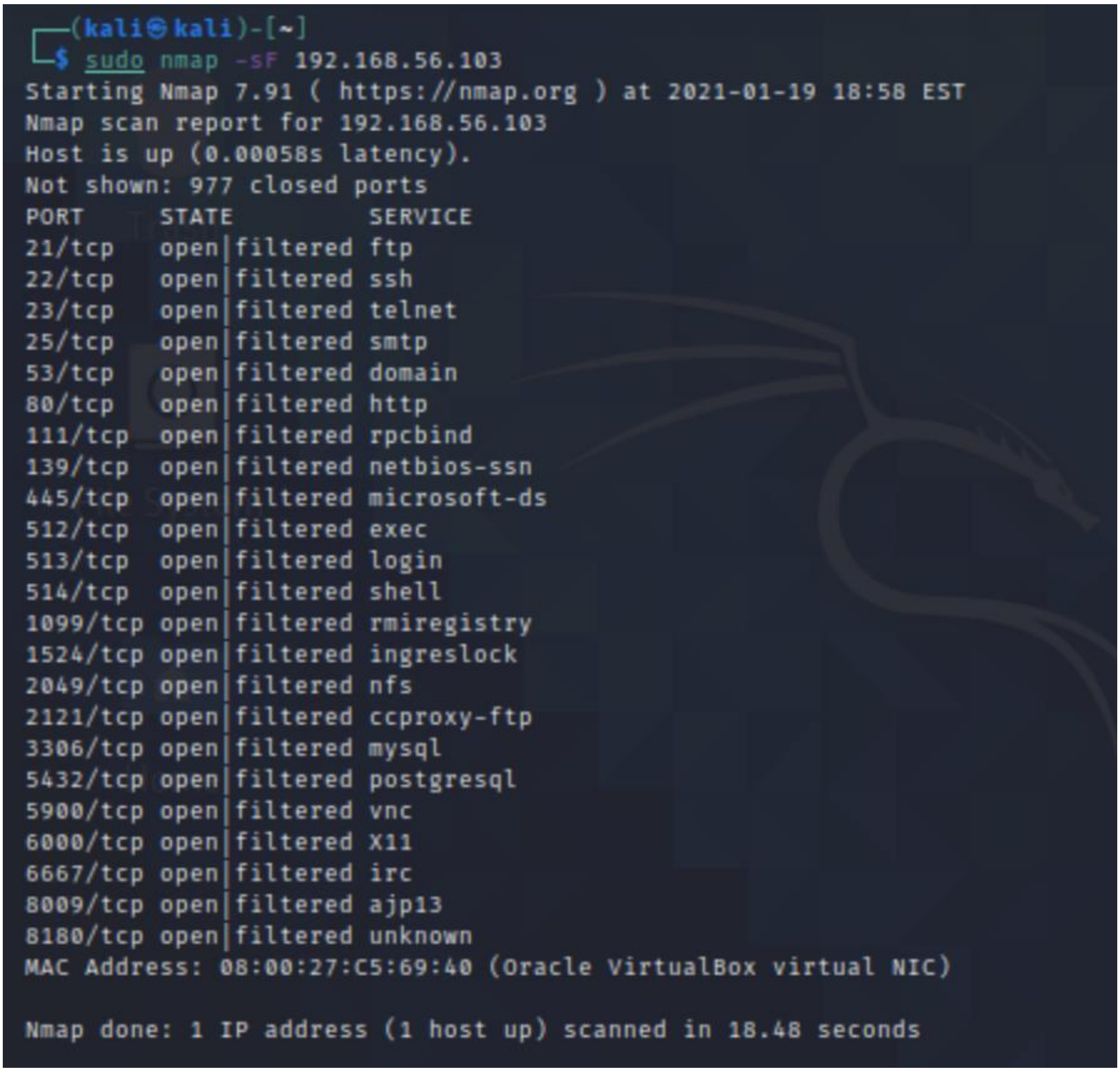
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.56.103
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-19 18:43 EST
Nmap scan report for 192.168.56.103
Host is up (0.00086s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
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: 08:00:27:C5:69:40 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.73 seconds
```

- **TCP SYN:** TCP SYN can be performed quickly, scanning thousands of ports per second on a fast network not hampered by restrictive firewalls. It is also relatively unobtrusive and stealthy since it never completes TCP connections. SYN scan works against any compliant TCP stack rather than depending on idiosyncrasies of specific platforms as Nmap's FIN/NULL/Xmas, Maimon and idle scans do.



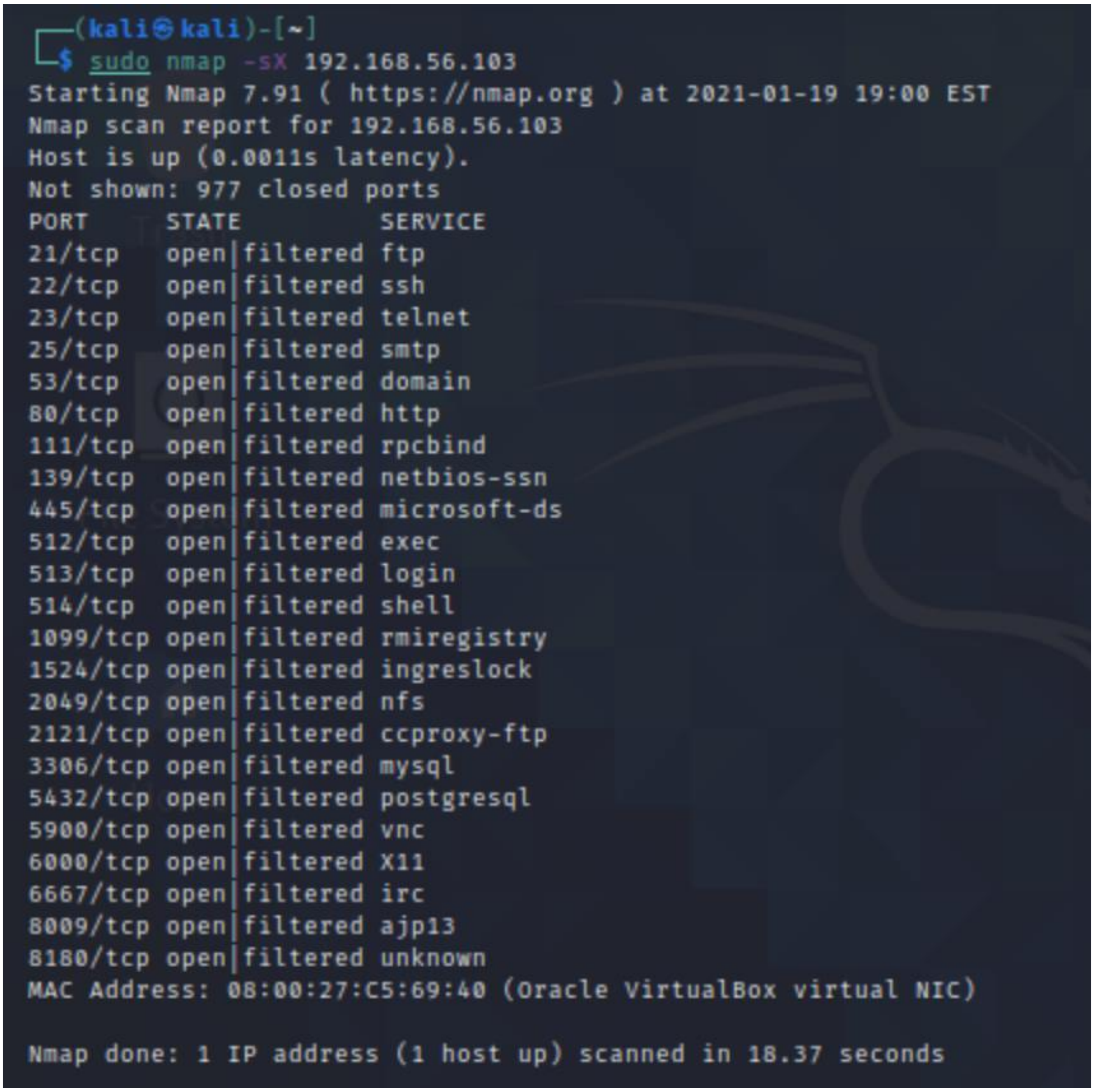
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.56.103
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-19 18:49 EST
Nmap scan report for 192.168.56.103
Host is up (0.00049s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   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: 08:00:27:C5:69:40 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 17.22 seconds
```

- **Stealth FIN:** Stealth FIN(-sF) sets just the TCP FIN bit.



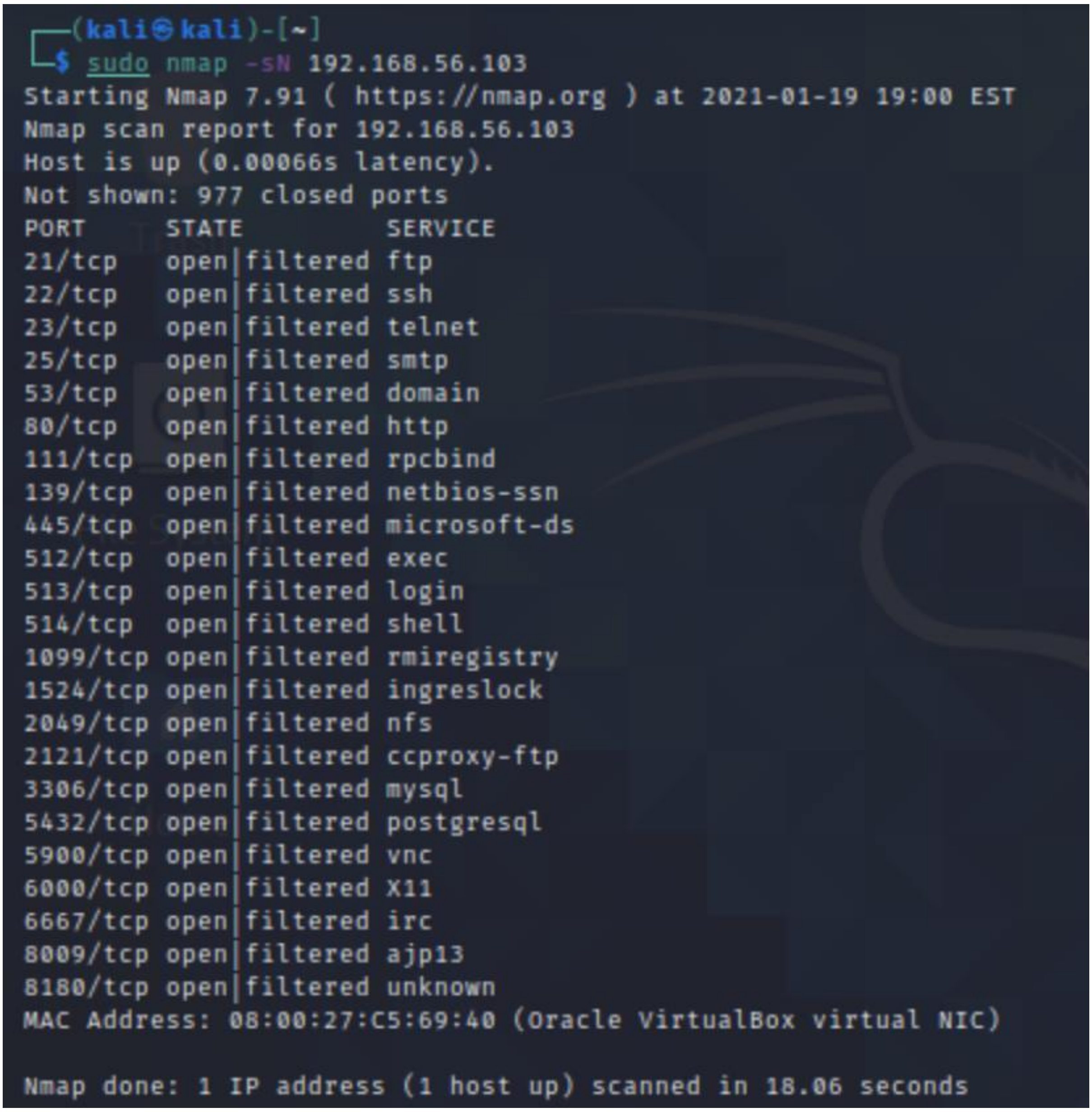
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sF 192.168.56.103
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-19 18:58 EST
Nmap scan report for 192.168.56.103
Host is up (0.00058s latency).
Not shown: 977 closed ports
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
23/tcp   open|filtered telnet
25/tcp   open|filtered smtp
53/tcp   open|filtered domain
80/tcp   open|filtered http
111/tcp  open|filtered rpcbind
139/tcp  open|filtered netbios-ssn
445/tcp  open|filtered microsoft-ds
512/tcp  open|filtered exec
513/tcp  open|filtered login
514/tcp  open|filtered shell
1099/tcp open|filtered rmiregistry
1524/tcp open|filtered ingreslock
2049/tcp open|filtered nfs
2121/tcp open|filtered ccproxy-ftp
3306/tcp open|filtered mysql
5432/tcp open|filtered postgresql
5900/tcp open|filtered vnc
6000/tcp open|filtered X11
6667/tcp open|filtered irc
8009/tcp open|filtered ajp13
8180/tcp open|filtered unknown
MAC Address: 08:00:27:C5:69:40 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 18.48 seconds
```

- **Xmas Tree:** Xmas tree(-sX) sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.



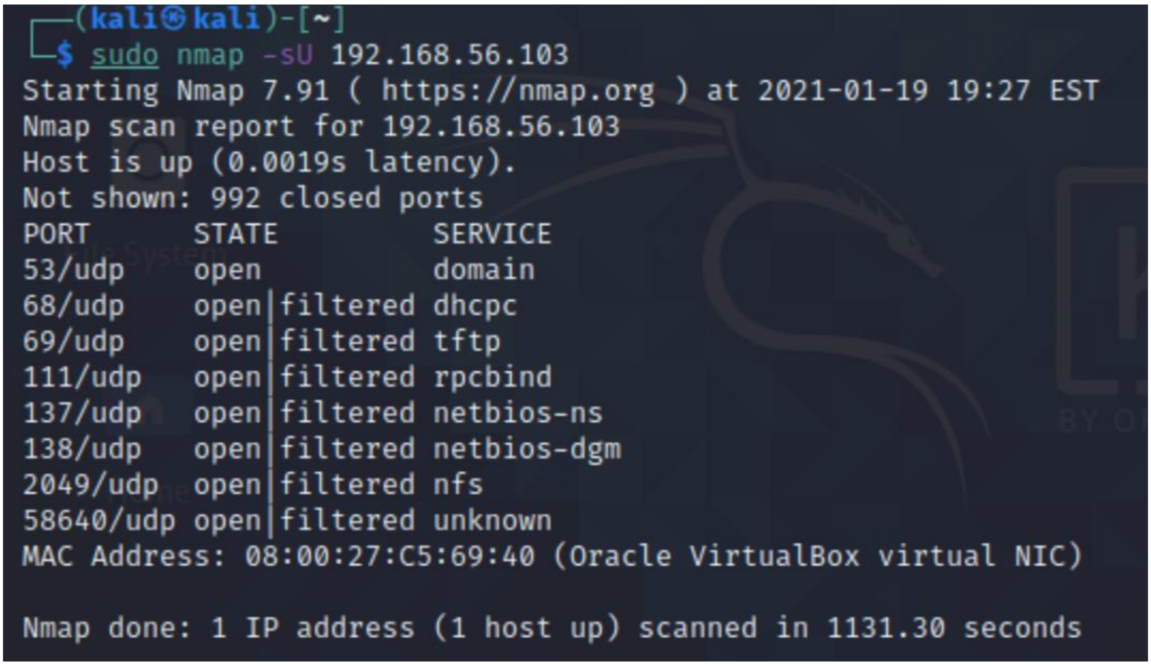
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sX 192.168.56.103
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-19 19:00 EST
Nmap scan report for 192.168.56.103
Host is up (0.0011s latency).
Not shown: 977 closed ports
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
23/tcp   open|filtered telnet
25/tcp   open|filtered smtp
53/tcp   open|filtered domain
80/tcp   open|filtered http
111/tcp  open|filtered rpcbind
139/tcp  open|filtered netbios-ssn
445/tcp  open|filtered microsoft-ds
512/tcp  open|filtered exec
513/tcp  open|filtered login
514/tcp  open|filtered shell
1099/tcp open|filtered rmiregistry
1524/tcp open|filtered ingreslock
2049/tcp open|filtered nfs
2121/tcp open|filtered ccproxy-ftp
3306/tcp open|filtered mysql
5432/tcp open|filtered postgresql
5900/tcp open|filtered vnc
6000/tcp open|filtered X11
6667/tcp open|filtered irc
8009/tcp open|filtered ajp13
8180/tcp open|filtered unknown
MAC Address: 08:00:27:C5:69:40 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 18.37 seconds
```

- **Null:** Null scan(-sN) does not set any bits (TCP flag header is 0)



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sN 192.168.56.103
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-19 19:00 EST
Nmap scan report for 192.168.56.103
Host is up (0.00066s latency).
Not shown: 977 closed ports
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
23/tcp   open|filtered telnet
25/tcp   open|filtered smtp
53/tcp   open|filtered domain
80/tcp   open|filtered http
111/tcp  open|filtered rpcbind
139/tcp  open|filtered netbios-ssn
445/tcp  open|filtered microsoft-ds
512/tcp  open|filtered exec
513/tcp  open|filtered login
514/tcp  open|filtered shell
1099/tcp open|filtered rmiregistry
1524/tcp open|filtered ingreslock
2049/tcp open|filtered nfs
2121/tcp open|filtered ccproxy-ftp
3306/tcp open|filtered mysql
5432/tcp open|filtered postgresql
5900/tcp open|filtered vnc
6000/tcp open|filtered X11
6667/tcp open|filtered irc
8009/tcp open|filtered ajp13
8180/tcp open|filtered unknown
MAC Address: 08:00:27:C5:69:40 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 18.06 seconds
```

- **UDP scans:** UDP scans(-sU) are slower than TCP scans. UDP scans work best when you send a specific payload to the target.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU 192.168.56.103
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-19 19:27 EST
Nmap scan report for 192.168.56.103
Host is up (0.0019s latency).
Not shown: 992 closed ports
PORT      STATE         SERVICE
53/udp    open          domain
68/udp    open|filtered dhcpc
69/udp    open|filtered tftp
111/udp   open|filtered rpcbind
137/udp   open|filtered netbios-ns
138/udp   open|filtered netbios-dgm
2049/udp  open|filtered nfs
58640/udp open|filtered unknown
MAC Address: 08:00:27:C5:69:40 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1131.30 seconds
```

References:

https://nmap.org/book/scan-methods-connect-scan.html

https://www.varonis.com/blog/port-scanning-techniques