Course Title: Information and Networking Security
Term: Spring 2025

Laboratory Exercise 3.1– Masscan

1. Overview

For this lesson, students will use the Cyber Range: Kali Linux with Metasploitable3 Environment to complete a subnet scan using Masscan. During the scan, Wireshark will be used for packet analysis and Htop will be used to monitor PC performance.

2. Resources required

This exercise requires the latest Kali Linux Metasploitable3 Environment running in the Cyber Range.

3. Initial Setup

For this exercise, you will log in to the Cyber Range account and select the Kali Linux with Metasploitable3 Environment, then click “start” to start your environment and “join” to get to your Linux desktop login. Log in using these credentials:

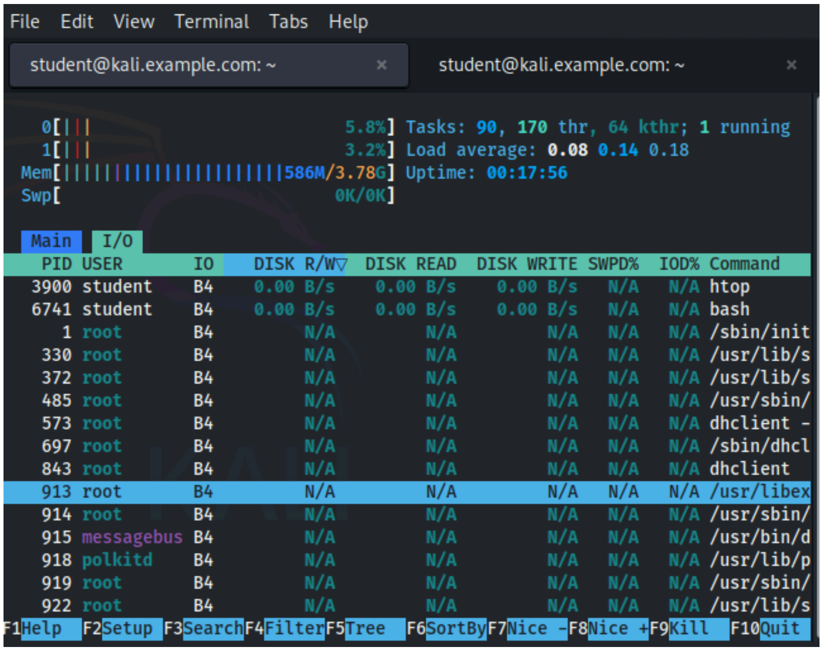
Username: **`student`**
Password: **`student`**

4. Tasks

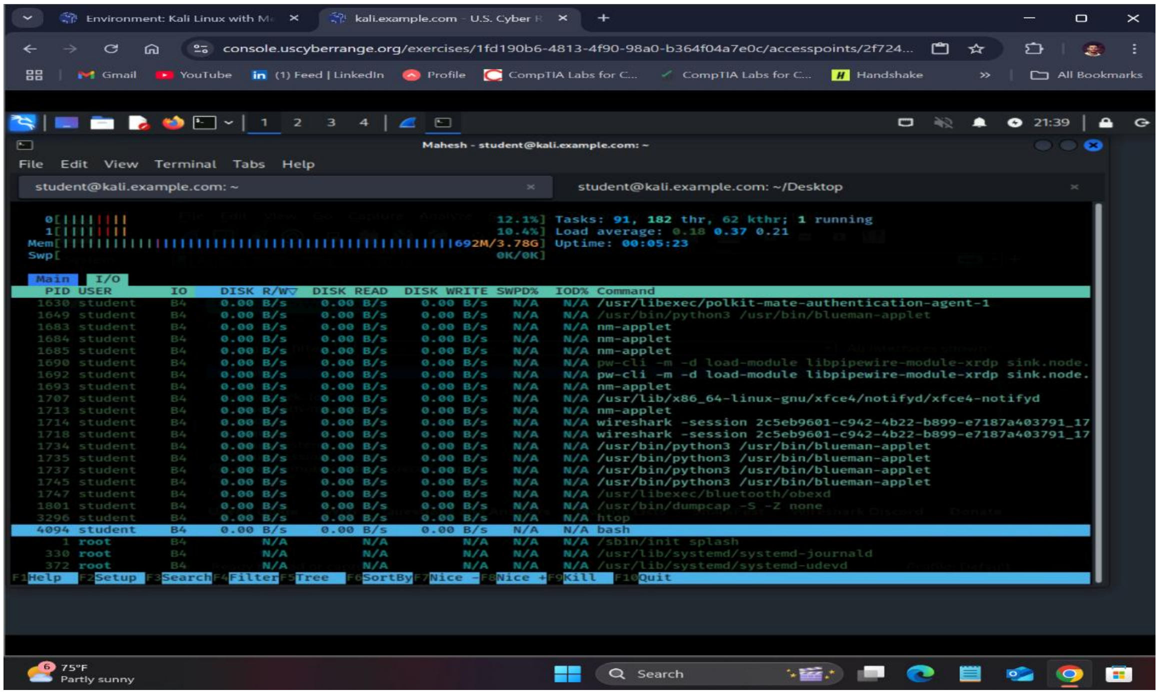
Task 1: Start and Run Htop

- Open Gedit by typing **`gedit &`**
- Return to the terminal
- Type **`htop`** to run it and open a new tab under file to run your commands

Htop will show you all the processes running and the user who is running the process. To kill a process, type **`kill <PID>`** (where PID is the process ID number) and then hit enter. For this example, we will choose the gedit PID. Locate the gedit PID and kill it. There will be multiple gedit PIDs. Any of them will work.


File Edit View Terminal Tabs Help
student@kali.example.com: ~
student@kali.example.com: ~

```
    0[|||                          5.8%] Tasks: 90, 170 thr, 64 kthr; 1 running
    1[|||                          3.2%] Load average: 0.08 0.14 0.18
  Mem[||||||||||||||||||||||586M/3.78G] Uptime: 00:17:56
  Swp[                            0K/0K]

  Main  I/O
  PID USER       IO   DISK R/W▽  DISK READ  DISK WRITE  SWPD%  IOD% Command
 3900 student    B4   0.00 B/s   0.00 B/s   0.00 B/s    N/A   N/A htop
 6741 student    B4   0.00 B/s   0.00 B/s   0.00 B/s    N/A   N/A bash
    1 root       B4        N/A        N/A        N/A    N/A   N/A /sbin/init
  330 root       B4        N/A        N/A        N/A    N/A   N/A /usr/lib/s
  372 root       B4        N/A        N/A        N/A    N/A   N/A /usr/lib/s
  485 root       B4        N/A        N/A        N/A    N/A   N/A /usr/sbin/
  573 root       B4        N/A        N/A        N/A    N/A   N/A dhclient -
  697 root       B4        N/A        N/A        N/A    N/A   N/A /sbin/dhcl
  843 root       B4        N/A        N/A        N/A    N/A   N/A dhclient
  913 root       B4        N/A        N/A        N/A    N/A   N/A /usr/libex
  914 root       B4        N/A        N/A        N/A    N/A   N/A /usr/sbin/
  915 messagebus B4        N/A        N/A        N/A    N/A   N/A /usr/bin/d
  918 polkitd    B4        N/A        N/A        N/A    N/A   N/A /usr/lib/p
  919 root       B4        N/A        N/A        N/A    N/A   N/A /usr/sbin/
  922 root       B4        N/A        N/A        N/A    N/A   N/A /usr/lib/s
F1Help  F2Setup F3SearchF4FilterF5Tree  F6SortByF7Nice -F8Nice +F9Kill  F10Quit
```

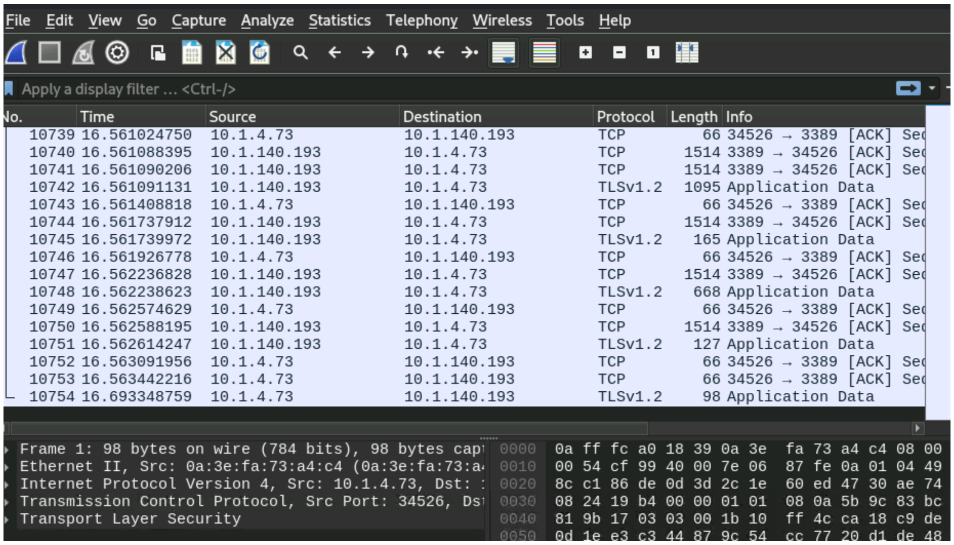

Environment: Kali Linux with M
kali.example.com - U.S. Cyber R
console.uscyberrange.org/exercises/1fd190b6-4813-4f90-98a0-b364f04a7e0c/accesspoints/2f724...
Gmail
YouTube
(1) Feed | LinkedIn
Profile
CompTIA Labs for C...
CompTIA Labs for C...
Handshake
All Bookmarks
1 2 3 4
21:39
Mahesh - student@kali.example.com: ~
File Edit View Terminal Tabs Help
student@kali.example.com: ~
student@kali.example.com: ~/Desktop
75°F
Partly sunny
Search

```
    0[||||||||                   12.1%] Tasks: 91, 182 thr, 62 kthr; 1 running
    1[||||||||                   10.4%] Load average: 0.18 0.37 0.21
  Mem[|||||||||||||||||||||||||||||||||||||||||||692M/3.78G] Uptime: 00:05:23
  Swp[                             0K/0K]

  Main  I/O
  PID USER       IO   DISK R/W▽  DISK READ  DISK WRITE  SWPD%  IOD% Command
 1630 student    B4   0.00 B/s   0.00 B/s   0.00 B/s    N/A   N/A /usr/libexec/polkit-mate-authentication-agent-1
 1649 student    B4   0.00 B/s   0.00 B/s   0.00 B/s    N/A   N/A /usr/bin/python3 /usr/bin/blueman-applet
 1683 student    B4   0.00 B/s   0.00 B/s   0.00 B/s    N/A   N/A nm-applet
 1684 student    B4   0.00 B/s   0.00 B/s   0.00 B/s    N/A   N/A nm-applet
 1685 student    B4   0.00 B/s   0.00 B/s   0.00 B/s    N/A   N/A nm-applet
 1690 student    B4   0.00 B/s   0.00 B/s   0.00 B/s    N/A   N/A pw-cli -m -d load-module libpipewire-module-xrdp sink.node.
 1692 student    B4   0.00 B/s   0.00 B/s   0.00 B/s    N/A   N/A pw-cli -m -d load-module libpipewire-module-xrdp sink.node.
 1693 student    B4   0.00 B/s   0.00 B/s   0.00 B/s    N/A   N/A nm-applet
 1707 student    B4   0.00 B/s   0.00 B/s   0.00 B/s    N/A   N/A /usr/lib/x86_64-linux-gnu/xfce4/notifyd/xfce4-notifyd
 1713 student    B4   0.00 B/s   0.00 B/s   0.00 B/s    N/A   N/A nm-applet
 1714 student    B4   0.00 B/s   0.00 B/s   0.00 B/s    N/A   N/A wireshark -session 2c5eb9601-c942-4b22-b899-e7187a403791_17
 1718 student    B4   0.00 B/s   0.00 B/s   0.00 B/s    N/A   N/A wireshark -session 2c5eb9601-c942-4b22-b899-e7187a403791_17
 1734 student    B4   0.00 B/s   0.00 B/s   0.00 B/s    N/A   N/A /usr/bin/python3 /usr/bin/blueman-applet
 1735 student    B4   0.00 B/s   0.00 B/s   0.00 B/s    N/A   N/A /usr/bin/python3 /usr/bin/blueman-applet
 1737 student    B4   0.00 B/s   0.00 B/s   0.00 B/s    N/A   N/A /usr/bin/python3 /usr/bin/blueman-applet
 1745 student    B4   0.00 B/s   0.00 B/s   0.00 B/s    N/A   N/A /usr/bin/python3 /usr/bin/blueman-applet
 1747 student    B4   0.00 B/s   0.00 B/s   0.00 B/s    N/A   N/A /usr/libexec/bluetooth/obexd
 1801 student    B4   0.00 B/s   0.00 B/s   0.00 B/s    N/A   N/A /usr/bin/dumpcap -S -Z none
 3296 student    B4   0.00 B/s   0.00 B/s   0.00 B/s    N/A   N/A htop
 4094 student    B4   0.00 B/s   0.00 B/s   0.00 B/s    N/A   N/A bash
    1 root       B4        N/A        N/A        N/A    N/A   N/A /sbin/init splash
  330 root       B4        N/A        N/A        N/A    N/A   N/A /usr/lib/systemd/systemd-journald
  372 root       B4        N/A        N/A        N/A    N/A   N/A /usr/lib/systemd/systemd-udevd
F1Help  F2Setup F3SearchF4FilterF5Tree  F6SortByF7Nice -F8Nice +F9Kill  F10Quit
```

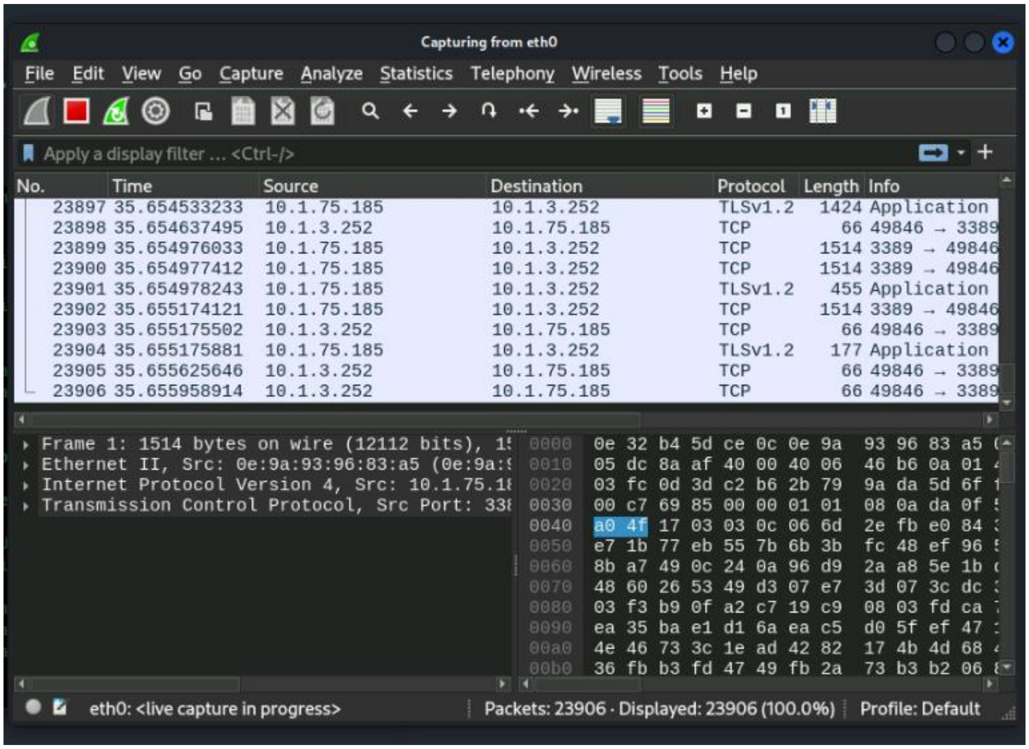
Task 2: Setup Wireshark to analyze packets

Open a new terminal window, become root, and type **`wireshark &`**.

Choose eth0 (double click on it) and let Wireshark capture packets for about 15 seconds then stop the scan by clicking the red square. Notice the subnets that were found from sniffing the network. One of the first things a pentester will do once on the internal network is scan the entire network. If a PC has been successfully exploited, a scan can be completed in a shell using a program like TCPdump (more on this later). Here we see that there are several 10.1.x.x IPs.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

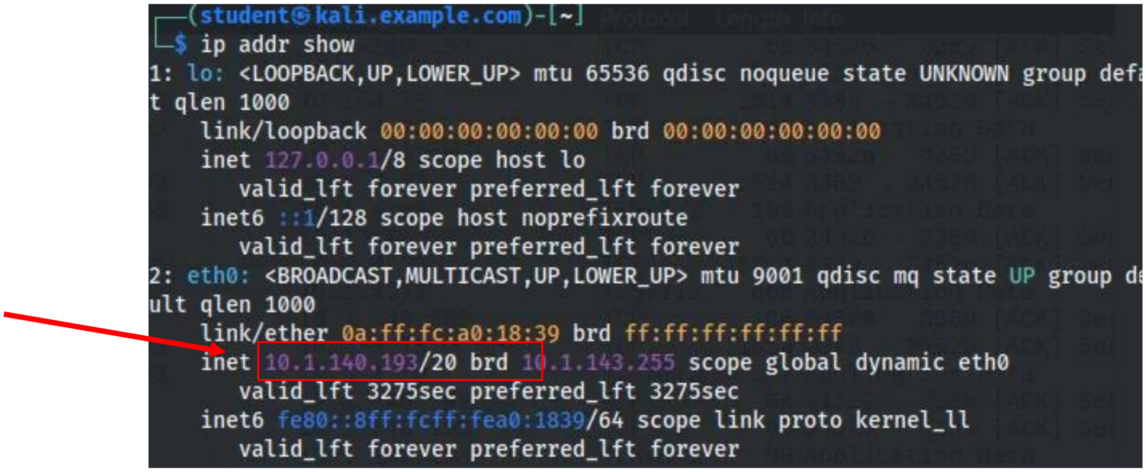
```
No.   Time         Source        Destination   Protocol Length Info
10739 16.561024750 10.1.4.73     10.1.140.193  TCP        66 34526 → 3389 [ACK] Sec
10740 16.561088395 10.1.140.193  10.1.4.73     TCP      1514 3389 → 34526 [ACK] Sec
10741 16.561090206 10.1.140.193  10.1.4.73     TCP      1514 3389 → 34526 [ACK] Sec
10742 16.561091131 10.1.140.193  10.1.4.73     TLSv1.2  1095 Application Data
10743 16.561408818 10.1.4.73     10.1.140.193  TCP        66 34526 → 3389 [ACK] Sec
10744 16.561737912 10.1.140.193  10.1.4.73     TCP      1514 3389 → 34526 [ACK] Sec
10745 16.561739972 10.1.140.193  10.1.4.73     TLSv1.2   165 Application Data
10746 16.561926778 10.1.4.73     10.1.140.193  TCP        66 34526 → 3389 [ACK] Sec
10747 16.562236828 10.1.140.193  10.1.4.73     TCP      1514 3389 → 34526 [ACK] Sec
10748 16.562238623 10.1.140.193  10.1.4.73     TLSv1.2   668 Application Data
10749 16.562574629 10.1.4.73     10.1.140.193  TCP        66 34526 → 3389 [ACK] Sec
10750 16.562588195 10.1.140.193  10.1.4.73     TCP      1514 3389 → 34526 [ACK] Sec
10751 16.562614247 10.1.140.193  10.1.4.73     TLSv1.2   127 Application Data
10752 16.563091956 10.1.4.73     10.1.140.193  TCP        66 34526 → 3389 [ACK] Sec
10753 16.563442216 10.1.4.73     10.1.140.193  TCP        66 34526 → 3389 [ACK] Sec
10754 16.693348759 10.1.4.73     10.1.140.193  TLSv1.2    98 Application Data

Frame 1: 98 bytes on wire (784 bits), 98 bytes capt     0000  0a ff fc a0 18 39 0a 3e  fa 73 a4 c4 08 00
Ethernet II, Src: 0a:3e:fa:73:a4:c4 (0a:3e:fa:73:a4     0010  00 54 cf 99 40 00 7e 06  87 fe 0a 01 04 49
Internet Protocol Version 4, Src: 10.1.4.73, Dst: 1     0020  8c c1 86 de 0d 3d 2c 1e  60 ed 47 30 ae 74
Transmission Control Protocol, Src Port: 34526, Dst     0030  08 24 19 b4 00 00 01 01  08 0a 5b 9c 83 bc
Transport Layer Security                                0040  81 9b 17 03 03 00 1b 10  ff 4c ca 18 c9 de
                                                        0050  0d 1e e3 c3 44 87 9c 54  cc 77 20 d1 de 48
```


Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

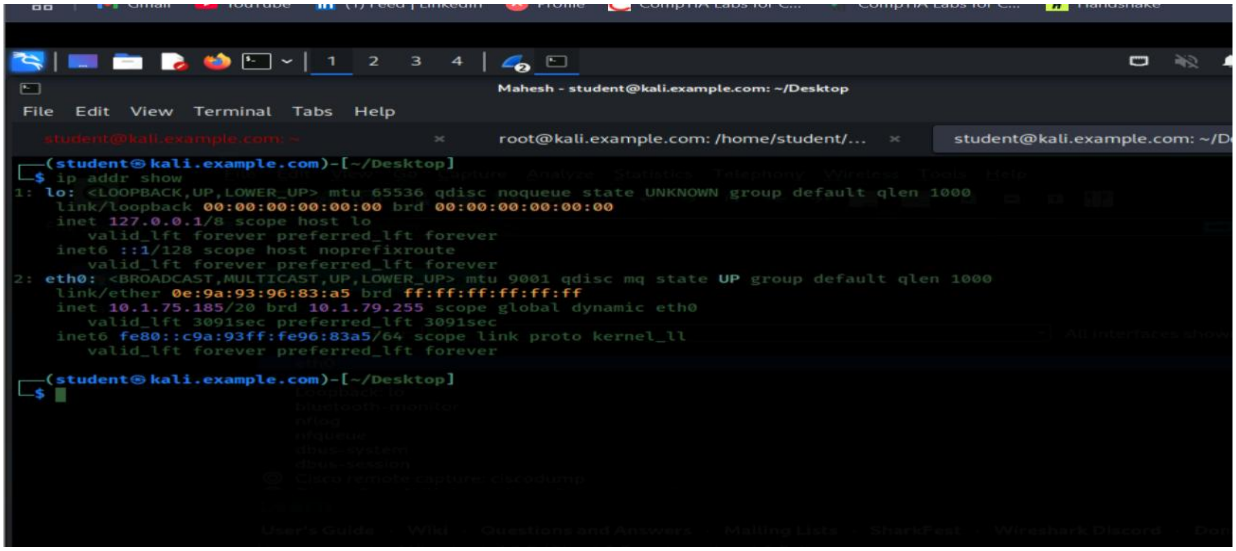
```
No.   Time         Source        Destination   Protocol Length Info
23897 35.654533233 10.1.75.185   10.1.3.252    TLSv1.2  1424 Application
23898 35.654637495 10.1.3.252    10.1.75.185   TCP        66 49846 → 3389
23899 35.654976033 10.1.75.185   10.1.3.252    TCP      1514 3389 → 49846
23900 35.654977412 10.1.75.185   10.1.3.252    TCP      1514 3389 → 49846
23901 35.654978243 10.1.75.185   10.1.3.252    TLSv1.2   455 Application
23902 35.655174121 10.1.75.185   10.1.3.252    TCP      1514 3389 → 49846
23903 35.655175502 10.1.3.252    10.1.75.185   TCP        66 49846 → 3389
23904 35.655175881 10.1.75.185   10.1.3.252    TLSv1.2   177 Application
23905 35.655625646 10.1.3.252    10.1.75.185   TCP        66 49846 → 3389
23906 35.655958914 10.1.3.252    10.1.75.185   TCP        66 49846 → 3389

Frame 1: 1514 bytes on wire (12112 bits), 15     0000  0e 32 b4 5d ce 0c 0e 9a  93 96 83 a5
Ethernet II, Src: 0e:9a:93:96:83:a5 (0e:9a:9     0010  05 dc 8a af 40 00 40 06  46 b6 0a 01
Internet Protocol Version 4, Src: 10.1.75.18     0020  03 fc 0d 3d c2 b6 2b 79  9a da 5d 6f
Transmission Control Protocol, Src Port: 338     0030  00 c7 69 85 00 00 01 01  08 0a da 0f
                                                 0040  a0 4f 17 03 03 0c 06 6d  2e fb e0 84
                                                 0050  e7 1b 77 eb 55 7b 6b 3b  fc 48 ef 96
                                                 0060  8b a7 49 0c 24 0a 96 d9  2a a8 5e 1b
                                                 0070  48 60 26 53 49 d3 07 e7  3d 07 3c dc
                                                 0080  03 f3 b9 0f a2 c7 19 c9  08 03 fd ca
                                                 0090  ea 35 ba e1 d1 6a ea c5  d0 5f ef 47
                                                 00a0  4e 46 73 3c 1e ad 42 82  17 4b 4d 68
                                                 00b0  36 fb b3 fd 47 49 fb 2a  73 b3 b2 06

eth0: <live capture in progress>   Packets: 23906 · Displayed: 23906 (100.0%)   Profile: Default
```

Task 3: Using Netdiscover to find IP ranges

First, let's find the subnet we are on by opening a new terminal window and typing **`ip addr show`**. Here I have 10.1.140.193/20 on eth0.



```
┌──(student㉿kali.example.com)-[~]
└─$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defa
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc mq state UP group de
ult qlen 1000
    link/ether 0a:ff:fc:a0:18:39 brd ff:ff:ff:ff:ff:ff
    inet 10.1.140.193/20 brd 10.1.143.255 scope global dynamic eth0
       valid_lft 3275sec preferred_lft 3275sec
    inet6 fe80::8ff:fcff:fea0:1839/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
```


1
2
3
4
Mahesh - student@kali.example.com: ~/Desktop
File
Edit
View
Terminal
Tabs
Help
student@kali.example.com: ~
root@kali.example.com: /home/student/...
student@kali.example.com: ~/De

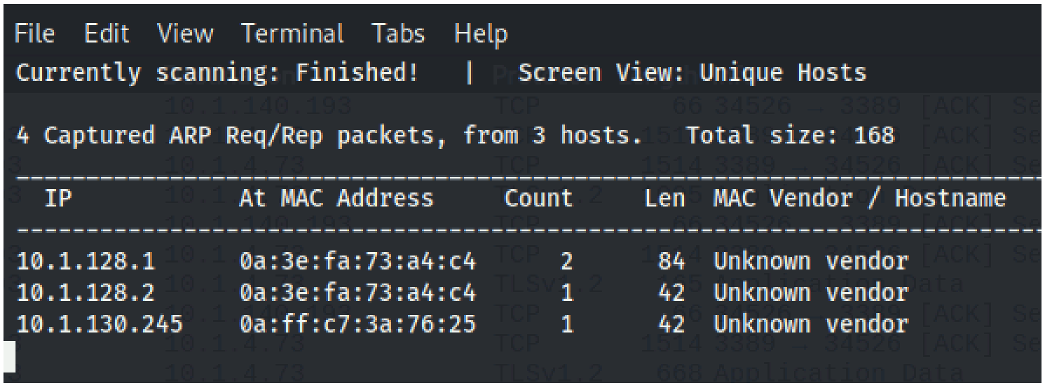
```
┌──(student㉿kali.example.com)-[~/Desktop]
└─$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc mq state UP group default qlen 1000
    link/ether 0e:9a:93:96:83:a5 brd ff:ff:ff:ff:ff:ff
    inet 10.1.75.185/20 brd 10.1.79.255 scope global dynamic eth0
       valid_lft 3091sec preferred_lft 3091sec
    inet6 fe80::c9a:93ff:fe96:83a5/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever

┌──(student㉿kali.example.com)-[~/Desktop]
└─$ 
```

Netdiscover is used to find live hosts by ARP scanning. This tool can be used for switched and wireless networks. Netdiscover will not work on a /20 so we need to use a /16 this will show a greater range of IP's. This may take a few minutes to pick up the IPs.

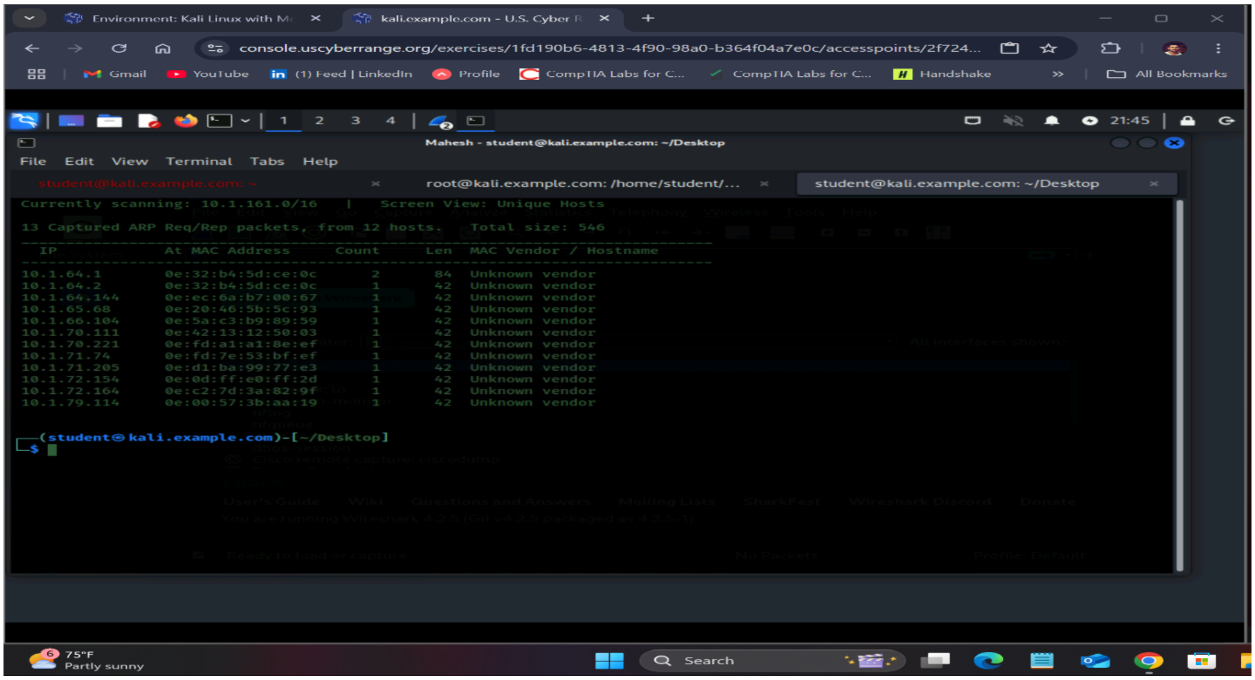
Type the following command, where IP is the IP address we just found on eth0, and then hit enter:

```
sudo netdiscover -r <IP>/16
```

You will see the prompt in the terminal window titled "currently scanning" as shown in the screenshot. The IP next to it will be counting up as it scans. When the scan is finished press CTRL+C to return to the terminal.



```
Currently scanning: Finished!   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 168
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
10.1.128.1      0a:3e:fa:73:a4:c4      2      84  Unknown vendor
10.1.128.2      0a:3e:fa:73:a4:c4      1      42  Unknown vendor
10.1.130.245    0a:ff:c7:3a:76:25      1      42  Unknown vendor
```

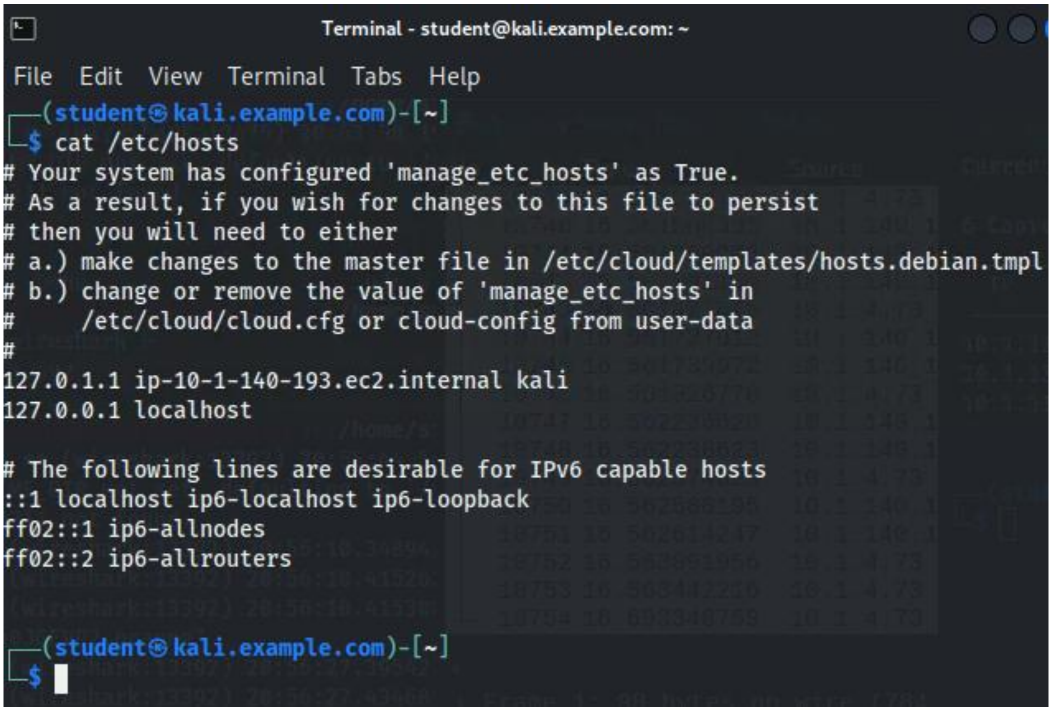


Environment: Kali Linux with M
kali.example.com - U.S. Cyber R
console.uscyberrange.org/exercises/1fd190b6-4813-4f90-98a0-b364f04a7e0c/accesspoints/2f724...
Gmail
YouTube
(1) Feed | LinkedIn
Profile
CompTIA Labs for C...
CompTIA Labs for C...
Handshake
All Bookmarks
1
2
3
4
21:45
Mahesh - student@kali.example.com: ~/Desktop
File Edit View Terminal Tabs Help
student@kali.example.com: ~
root@kali.example.com: /home/student/...
student@kali.example.com: ~/Desktop
75°F
Partly sunny
Search

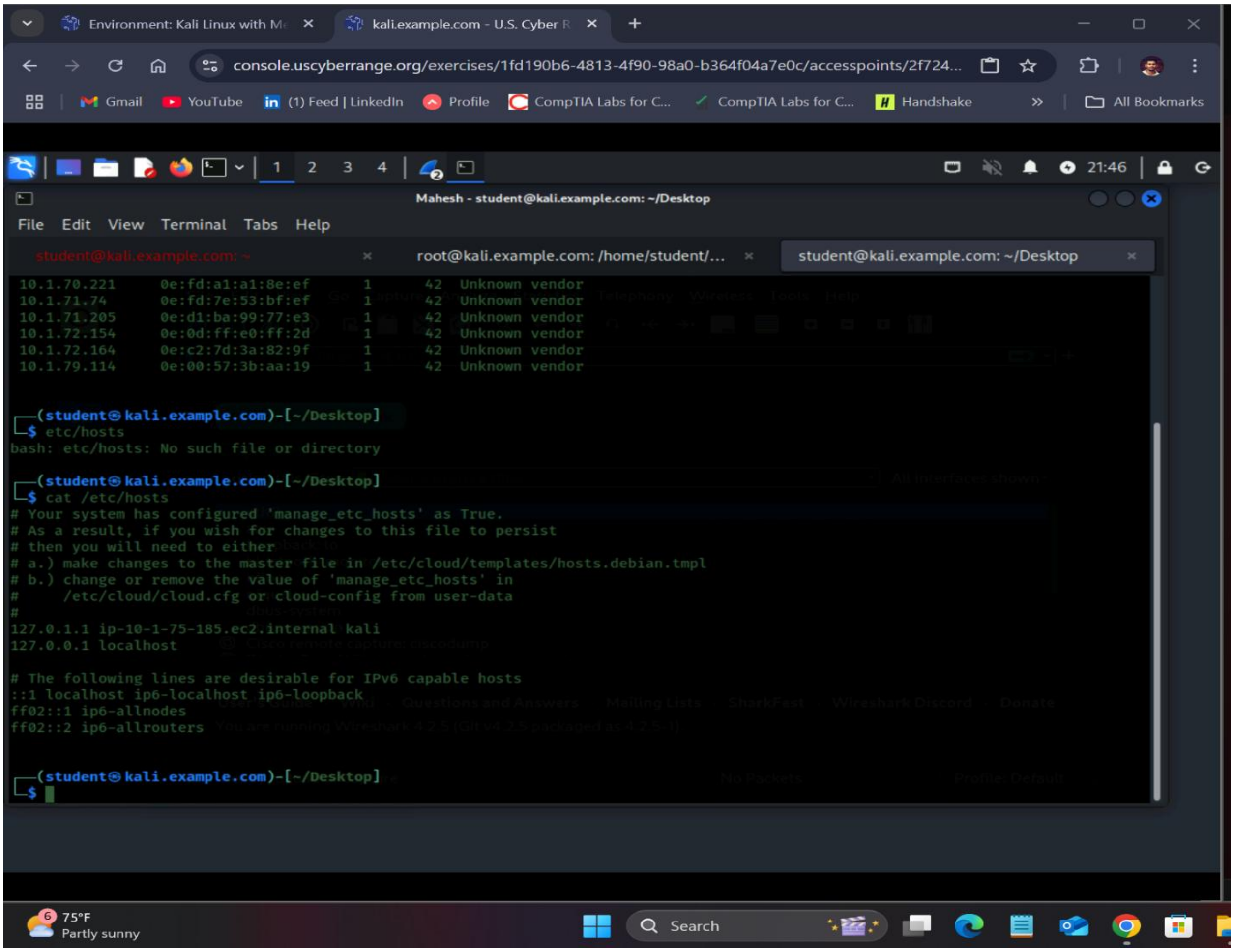
```
Currently scanning: 10.1.161.0/16   |   Screen View: Unique Hosts

13 Captured ARP Req/Rep packets, from 12 hosts.   Total size: 546
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
10.1.64.1       0e:32:b4:5d:ce:0c      2      84  Unknown vendor
10.1.64.2       0e:32:b4:5d:ce:0c      1      42  Unknown vendor
10.1.64.144     0e:ec:6a:b7:00:67      1      42  Unknown vendor
10.1.65.68      0e:20:46:5b:5c:93      1      42  Unknown vendor
10.1.66.104     0e:5a:c3:b9:89:59      1      42  Unknown vendor
10.1.70.111     0e:42:13:12:50:03      1      42  Unknown vendor
10.1.70.221     0e:fd:a1:a1:8e:ef      1      42  Unknown vendor
10.1.71.74      0e:fd:7e:53:bf:ef      1      42  Unknown vendor
10.1.71.205     0e:d1:ba:99:77:e3      1      42  Unknown vendor
10.1.72.154     0e:0d:ff:e0:ff:2d      1      42  Unknown vendor
10.1.72.164     0e:c2:7d:3a:82:9f      1      42  Unknown vendor
10.1.79.114     0e:00:57:3b:aa:19      1      42  Unknown vendor

┌──(student㉿kali.example.com)-[~/Desktop]
└─$ 
```

Task 4: Checking the Host File

Sometimes you can find IP information in the **/etc/hosts** file if you have compromised a machine and have a shell. A quick look is worth the time. Open a new terminal tab type **cat /etc/hosts** and then hit enter.


Terminal - student@kali.example.com: ~
File Edit View Terminal Tabs Help

```
┌──(student㉿kali.example.com)-[~]
└─$ cat /etc/hosts
# Your system has configured 'manage_etc_hosts' as True.
# As a result, if you wish for changes to this file to persist
# then you will need to either
# a.) make changes to the master file in /etc/cloud/templates/hosts.debian.tmpl
# b.) change or remove the value of 'manage_etc_hosts' in
#     /etc/cloud/cloud.cfg or cloud-config from user-data
#
127.0.1.1 ip-10-1-140-193.ec2.internal kali
127.0.0.1 localhost

# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

┌──(student㉿kali.example.com)-[~]
└─$ 
```


Environment: Kali Linux with M
kali.example.com - U.S. Cyber R
console.uscyberrange.org/exercises/1fd190b6-4813-4f90-98a0-b364f04a7e0c/accesspoints/2f724...
Gmail
YouTube
(1) Feed | LinkedIn
Profile
CompTIA Labs for C...
CompTIA Labs for C...
Handshake
All Bookmarks
1
2
3
4
21:46
Mahesh - student@kali.example.com: ~/Desktop
File Edit View Terminal Tabs Help
student@kali.example.com: ~
root@kali.example.com: /home/student/...
student@kali.example.com: ~/Desktop
75°F
Partly sunny
Search

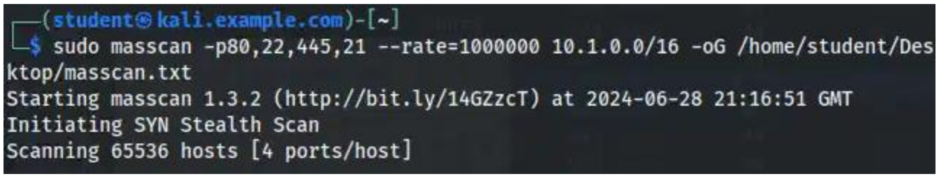
```
10.1.70.221     0e:fd:a1:a1:8e:ef      1      42  Unknown vendor
10.1.71.74      0e:fd:7e:53:bf:ef      1      42  Unknown vendor
10.1.71.205     0e:d1:ba:99:77:e3      1      42  Unknown vendor
10.1.72.154     0e:0d:ff:e0:ff:2d      1      42  Unknown vendor
10.1.72.164     0e:c2:7d:3a:82:9f      1      42  Unknown vendor
10.1.79.114     0e:00:57:3b:aa:19      1      42  Unknown vendor


┌──(student㉿kali.example.com)-[~/Desktop]
└─$ etc/hosts
bash: etc/hosts: No such file or directory

┌──(student㉿kali.example.com)-[~/Desktop]
└─$ cat /etc/hosts
# Your system has configured 'manage_etc_hosts' as True.
# As a result, if you wish for changes to this file to persist
# then you will need to either
# a.) make changes to the master file in /etc/cloud/templates/hosts.debian.tmpl
# b.) change or remove the value of 'manage_etc_hosts' in
#     /etc/cloud/cloud.cfg or cloud-config from user-data
#
127.0.1.1 ip-10-1-75-185.ec2.internal kali
127.0.0.1 localhost

# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters


┌──(student㉿kali.example.com)-[~/Desktop]
└─$ 
```

An attacker can also change the hosts' file to redirect internet traffic.

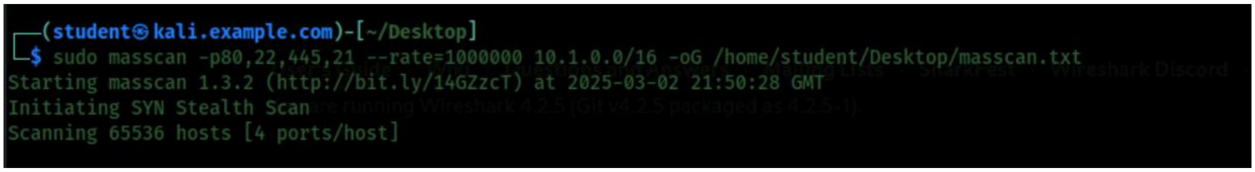
Task 5: Scan using Masscan

Masscan is an excellent tool for finding subnet ranges, open ports, and IPs. It is extremely fast because it uses asynchronous stateless TCP scanning. There are many ways to use the tool. First, you want to check with the client to clear the use of this tool. Masscan can burn up the recipient resources quickly so it will need to be used during low traffic hours. Be sure that your IP starts with 10.1. If this is not the case, you will need to change these octets to match. The syntax is simple, type the following:

```
sudo masscan -p80,22,445,21 --rate=1000000 10.1.0.0/16 -oG
/home/student/Desktop/masscan.txt
```

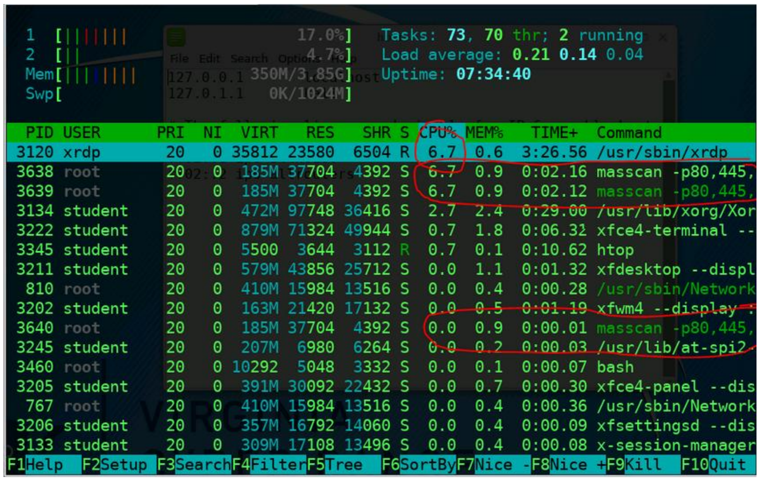


```
┌──(student㉿kali.example.com)-[~]
└─$ sudo masscan -p80,22,445,21 --rate=1000000 10.1.0.0/16 -oG /home/student/Des
ktop/masscan.txt
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2024-06-28 21:16:51 GMT
Initiating SYN Stealth Scan
Scanning 65536 hosts [4 ports/host]
```

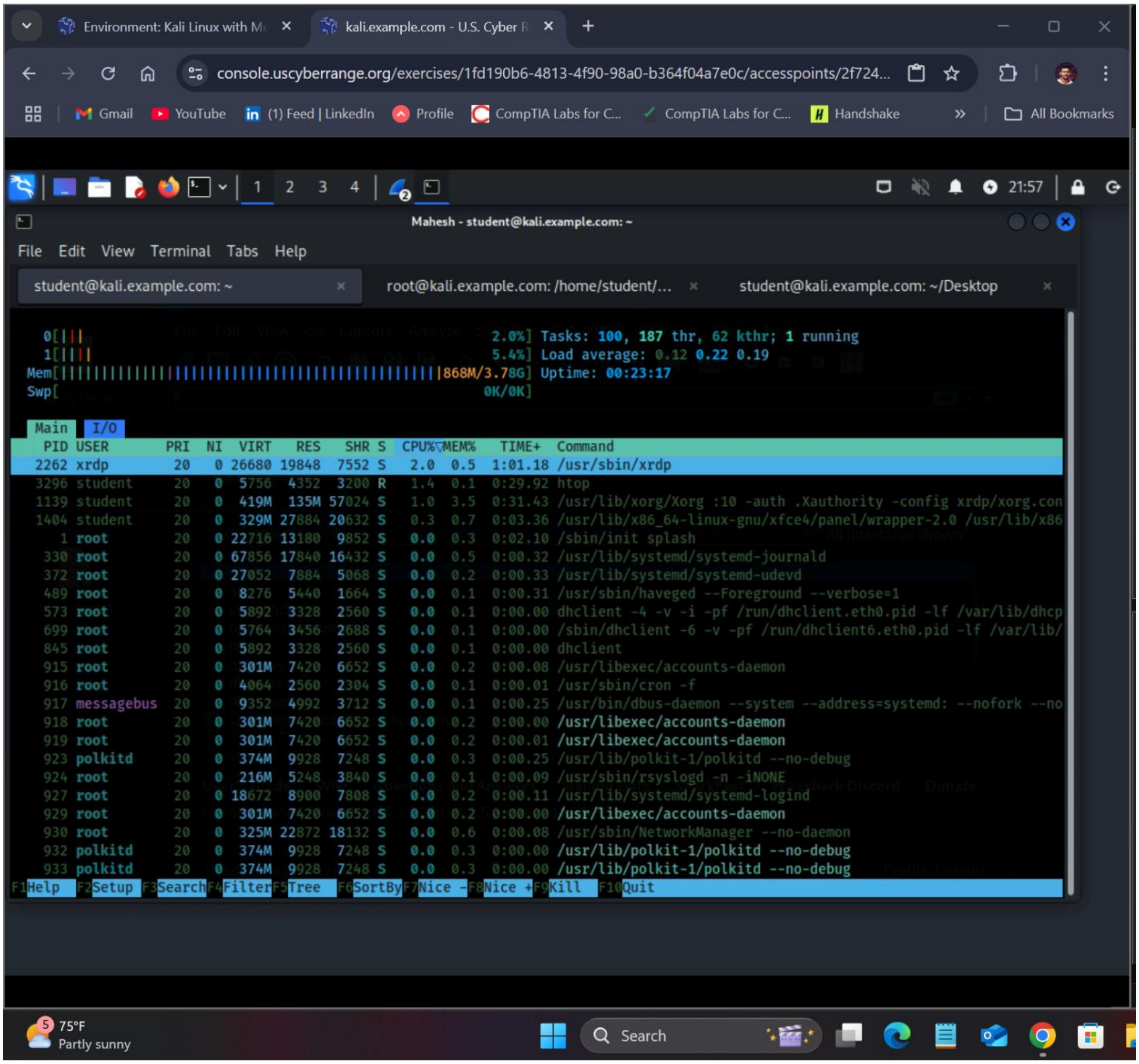


```
┌──(student㉿kali.example.com)-[~/Desktop]
└─$ sudo masscan -p80,22,445,21 --rate=1000000 10.1.0.0/16 -oG /home/student/Desktop/masscan.txt
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2025-03-02 21:50:28 GMT
Initiating SYN Stealth Scan
Scanning 65536 hosts [4 ports/host]
```

Return to **htop**. You will have to do this while Masscan is running. Generally, it uses very little CPU for the scan compared to Nmap. Your results may vary depending on your setup (graphics card). Keep in mind though, that the receiving end is being sent many packets and may detect this as a DoS attack. This can burn up resources as the recipient is trying to resolve the packets.

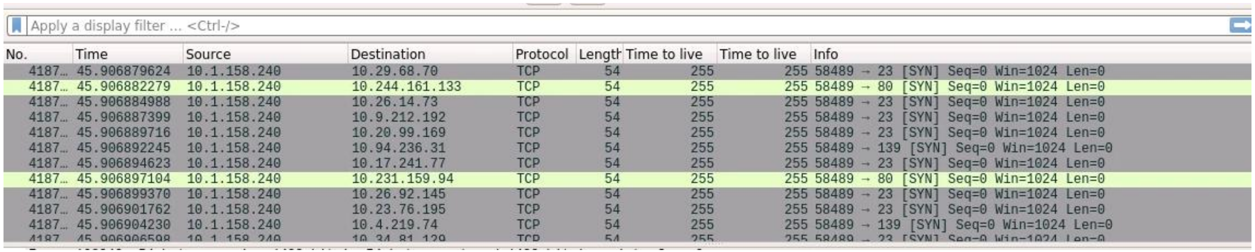


```
  1  [||||||||                17.0%]   Tasks: 73, 70 thr; 2 running
  2  [||                       4.7%]   Load average: 0.21 0.14 0.04
  Mem[||||||||           350M/3.85G]   Uptime: 07:34:40
  Swp[                      0K/1024M]

  PID USER      PRI  NI  VIRT   RES   SHR S CPU% MEM%   TIME+  Command
 3120 xrdp       20   0 35812 23580  6504 R  6.7  0.6  3:26.56 /usr/sbin/xrdp
 3638 root       20   0  185M 37704  4392 S  6.7  0.9  0:02.16 masscan -p80,445,
 3639 root       20   0  185M 37704  4392 S  6.7  0.9  0:02.12 masscan -p80,445,
 3134 student    20   0  472M 97748 36416 S  2.7  2.4  0:29.00 /usr/lib/xorg/Xor
 3222 student    20   0  879M 71324 49944 S  0.7  1.8  0:06.32 xfce4-terminal --
 3345 student    20   0  5500  3644  3112 R  0.7  0.1  0:10.62 htop
 3211 student    20   0  579M 43856 25712 S  0.0  1.1  0:01.32 xfdesktop --displ
  810 root       20   0  410M 15984 13516 S  0.0  0.4  0:00.28 /usr/sbin/Network
 3202 student    20   0  163M 21420 17132 S  0.0  0.5  0:01.19 xfwm4 --display :
 3640 root       20   0  185M 37704  4392 S  0.0  0.9  0:00.01 masscan -p80,445,
 3245 student    20   0  207M  6980  6264 S  0.0  0.2  0:00.03 /usr/lib/at-spi2
 3460 root       20   0 10292  5048  3332 S  0.0  0.1  0:00.07 bash
 3205 student    20   0  391M 30092 22432 S  0.0  0.7  0:00.30 xfce4-panel --dis
  767 root       20   0  410M 15984 13516 S  0.0  0.4  0:00.36 /usr/sbin/Network
 3206 student    20   0  357M 16792 14060 S  0.0  0.4  0:00.09 xfsettingsd --dis
 3133 student    20   0  309M 17108 13496 S  0.0  0.4  0:00.08 x-session-manager
F1Help  F2Setup F3SearchF4FilterF5Tree  F6SortByF7Nice -F8Nice +F9Kill  F10Quit
```

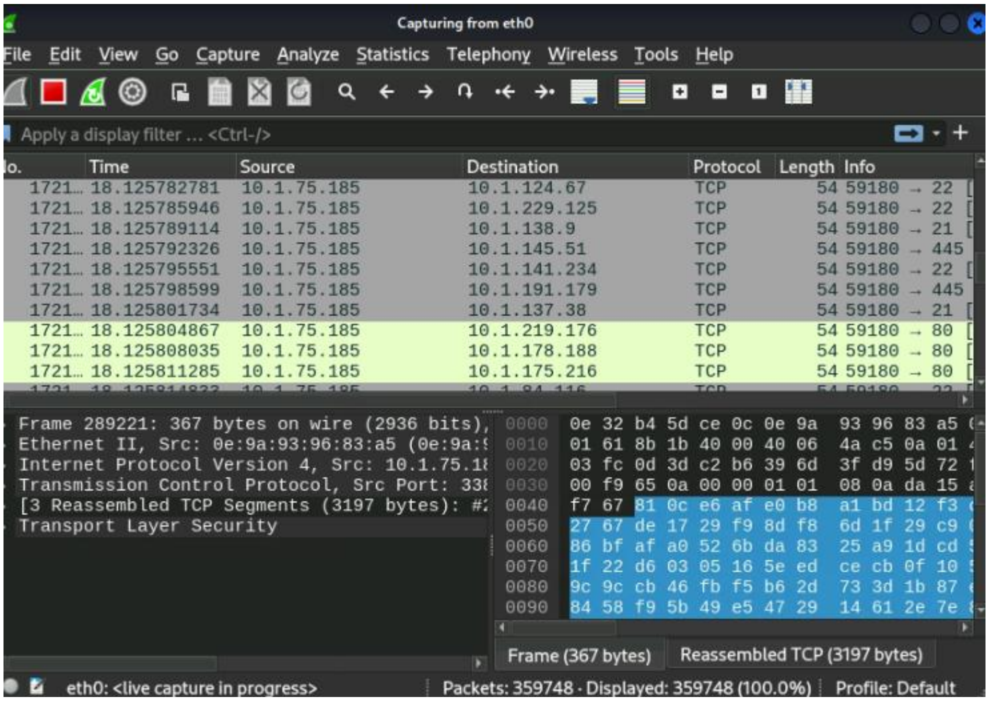

Environment: Kali Linux with M
kali.example.com - U.S. Cyber R
console.uscyberrange.org/exercises/1fd190b6-4813-4f90-98a0-b364f04a7e0c/accesspoints/2f724...
Gmail
YouTube
(1) Feed | LinkedIn
Profile
CompTIA Labs for C...
CompTIA Labs for C...
Handshake
All Bookmarks
1 2 3 4
21:57
Mahesh - student@kali.example.com: ~
File Edit View Terminal Tabs Help
student@kali.example.com: ~
root@kali.example.com: /home/student/...
student@kali.example.com: ~/Desktop
75°F
Partly sunny
Search

```
  0[|||                                          2.0%] Tasks: 100, 187 thr, 62 kthr; 1 running
  1[||||                                         5.4%] Load average: 0.12 0.22 0.19
Mem[||||||||||||||||||||||||||||||||||||||||||868M/3.78G] Uptime: 00:23:17
Swp[                                             0K/0K]

 Main  I/O
  PID USER       PRI  NI  VIRT   RES   SHR S  CPU%▽MEM%   TIME+  Command
 2262 xrdp        20   0 26680 19848  7552 S   2.0  0.5  1:01.18 /usr/sbin/xrdp
 3296 student     20   0  5756  4352  3200 R   1.4  0.1  0:29.92 htop
 1139 student     20   0  419M  135M 57024 S   1.0  3.5  0:31.43 /usr/lib/xorg/Xorg :10 -auth .Xauthority -config xrdp/xorg.con
 1404 student     20   0  329M 27884 20632 S   0.3  0.7  0:03.36 /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86
    1 root        20   0 22716 13180  9852 S   0.0  0.3  0:02.10 /sbin/init splash
  330 root        20   0 67856 17840 16432 S   0.0  0.5  0:00.32 /usr/lib/systemd/systemd-journald
  372 root        20   0 27052  7884  5068 S   0.0  0.2  0:00.33 /usr/lib/systemd/systemd-udevd
  489 root        20   0  8276  5440  1664 S   0.0  0.1  0:00.31 /usr/sbin/haveged --Foreground --verbose=1
  573 root        20   0  5892  3328  2560 S   0.0  0.1  0:00.00 dhclient -4 -v -i -pf /run/dhclient.eth0.pid -lf /var/lib/dhcp
  699 root        20   0  5764  3456  2688 S   0.0  0.1  0:00.00 /sbin/dhclient -6 -v -pf /run/dhclient6.eth0.pid -lf /var/lib/
  845 root        20   0  5892  3328  2560 S   0.0  0.1  0:00.00 dhclient
  915 root        20   0  301M  7420  6652 S   0.0  0.2  0:00.08 /usr/libexec/accounts-daemon
  916 root        20   0  4064  2560  2304 S   0.0  0.1  0:00.01 /usr/sbin/cron -f
  917 messagebus  20   0  9352  4992  3712 S   0.0  0.1  0:00.25 /usr/bin/dbus-daemon --system --address=systemd: --nofork --no
  918 root        20   0  301M  7420  6652 S   0.0  0.2  0:00.00 /usr/libexec/accounts-daemon
  919 root        20   0  301M  7420  6652 S   0.0  0.2  0:00.01 /usr/libexec/accounts-daemon
  923 polkitd     20   0  374M  9928  7248 S   0.0  0.3  0:00.25 /usr/lib/polkit-1/polkitd --no-debug
  924 root        20   0  216M  5248  3840 S   0.0  0.1  0:00.09 /usr/sbin/rsyslogd -n -iNONE
  927 root        20   0 18672  8900  7808 S   0.0  0.2  0:00.11 /usr/lib/systemd/systemd-logind
  929 root        20   0  301M  7420  6652 S   0.0  0.2  0:00.00 /usr/libexec/accounts-daemon
  930 root        20   0  325M 22872 18132 S   0.0  0.6  0:00.08 /usr/sbin/NetworkManager --no-daemon
  932 polkitd     20   0  374M  9928  7248 S   0.0  0.3  0:00.00 /usr/lib/polkit-1/polkitd --no-debug
  933 polkitd     20   0  374M  9928  7248 S   0.0  0.3  0:00.00 /usr/lib/polkit-1/polkitd --no-debug
F1Help  F2Setup F3SearchF4FilterF5Tree  F6SortByF7Nice -F8Nice +F9Kill  F10Quit
```

Return to Wireshark and start another scan. Notice how the IPs are randomized when observing Masscan through Wireshark. This is what asynchronous stateless TCP scanning looks like. Though it is not hard to detect, it does seem like a massive amount of traffic from many machines, setting different flags all at one time. This can be confusing to Admins who have not seen this type of scan before. If the organization has any choke points (Intrusion Prevention System (IPS)?), this scan could slow or stop traffic.



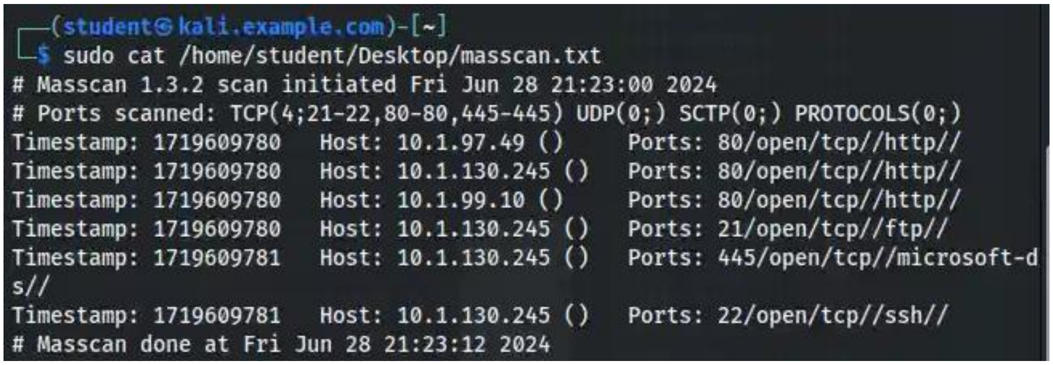
No.	Time	Source	Destination	Protocol	Length	Time to live	Time to live	Info
4187…	45.906879624	10.1.158.240	10.29.68.70	TCP	54	255	255	58489 → 23 [SYN] Seq=0 Win=1024 Len=0
4187…	45.906882279	10.1.158.240	10.244.161.133	TCP	54	255	255	58489 → 80 [SYN] Seq=0 Win=1024 Len=0
4187…	45.906884988	10.1.158.240	10.26.14.73	TCP	54	255	255	58489 → 23 [SYN] Seq=0 Win=1024 Len=0
4187…	45.906887399	10.1.158.240	10.9.212.192	TCP	54	255	255	58489 → 23 [SYN] Seq=0 Win=1024 Len=0
4187…	45.906889716	10.1.158.240	10.20.99.169	TCP	54	255	255	58489 → 23 [SYN] Seq=0 Win=1024 Len=0
4187…	45.906892245	10.1.158.240	10.94.236.31	TCP	54	255	255	58489 → 139 [SYN] Seq=0 Win=1024 Len=0
4187…	45.906894623	10.1.158.240	10.17.241.77	TCP	54	255	255	58489 → 23 [SYN] Seq=0 Win=1024 Len=0
4187…	45.906897104	10.1.158.240	10.231.159.94	TCP	54	255	255	58489 → 80 [SYN] Seq=0 Win=1024 Len=0
4187…	45.906899370	10.1.158.240	10.26.92.145	TCP	54	255	255	58489 → 23 [SYN] Seq=0 Win=1024 Len=0
4187…	45.906901762	10.1.158.240	10.23.76.195	TCP	54	255	255	58489 → 23 [SYN] Seq=0 Win=1024 Len=0
4187…	45.906904230	10.1.158.240	10.4.219.74	TCP	54	255	255	58489 → 139 [SYN] Seq=0 Win=1024 Len=0
4187…	45.906906598	10.1.158.240	10.34.81.129	TCP	54	255	255	58489 → 23 [SYN] Seq=0 Win=1024 Len=0


Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

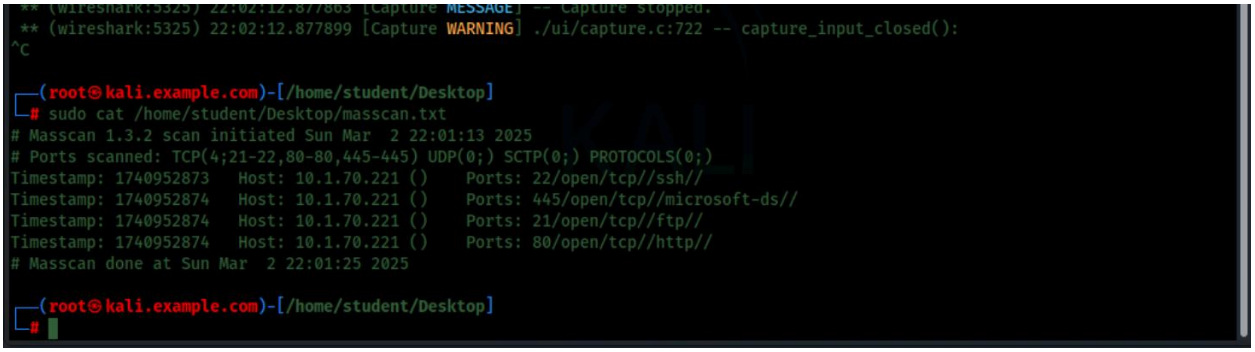
```
o.       Time              Source          Destination      Protocol  Length Info
 1721… 18.125782781   10.1.75.185    10.1.124.67       TCP          54 59180 → 22 [
 1721… 18.125785946   10.1.75.185    10.1.229.125      TCP          54 59180 → 22 [
 1721… 18.125789114   10.1.75.185    10.1.138.9        TCP          54 59180 → 21 [
 1721… 18.125792326   10.1.75.185    10.1.145.51       TCP          54 59180 → 445
 1721… 18.125795551   10.1.75.185    10.1.141.234      TCP          54 59180 → 22 [
 1721… 18.125798599   10.1.75.185    10.1.191.179      TCP          54 59180 → 445
 1721… 18.125801734   10.1.75.185    10.1.137.38       TCP          54 59180 → 21 [
 1721… 18.125804867   10.1.75.185    10.1.219.176      TCP          54 59180 → 80 [
 1721… 18.125808035   10.1.75.185    10.1.178.188      TCP          54 59180 → 80 [
 1721… 18.125811285   10.1.75.185    10.1.175.216      TCP          54 59180 → 80 [

Frame 289221: 367 bytes on wire (2936 bits),   0000  0e 32 b4 5d ce 0c 0e 9a  93 96 83 a5
Ethernet II, Src: 0e:9a:93:96:83:a5 (0e:9a:    0010  01 61 8b 1b 40 00 40 06  4a c5 0a 01
Internet Protocol Version 4, Src: 10.1.75.18   0020  03 fc 0d 3d c2 b6 39 6d  3f d9 5d 72
Transmission Control Protocol, Src Port: 338   0030  00 f9 65 0a 00 00 01 01  08 0a da 15
[3 Reassembled TCP Segments (3197 bytes): #2   0040  f7 67 81 0c e6 af e0 b8  a1 bd 12 f3
Transport Layer Security                       0050  27 67 de 17 29 f9 8d f8  6d 1f 29 c9
                                               0060  86 bf af a0 52 6b da 83  25 a9 1d cd
                                               0070  1f 22 d6 03 05 16 5e ed  ce cb 0f 10
                                               0080  9c 9c cb 46 fb f5 b6 2d  73 3d 1b 87
                                               0090  84 58 f9 5b 49 e5 47 29  14 61 2e 7e

                                               Frame (367 bytes)  Reassembled TCP (3197 bytes)
eth0: <live capture in progress>   Packets: 359748 · Displayed: 359748 (100.0%)   Profile: Default
```

Masscan can be paused and restarted. To pause masscan, press **CTRL+C** (you may have to do this several times). This will create a config file called paused.conf. To resume, type **sudo masscan --resume paused.conf** and then hit enter.

The results should look similar to the below screenshot. You can open the results in Gedit or type **sudo cat /home/student/Desktop/masscan.txt** to see them in the terminal.



```
┌──(student㉿kali.example.com)-[~]
└─$ sudo cat /home/student/Desktop/masscan.txt
# Masscan 1.3.2 scan initiated Fri Jun 28 21:23:00 2024
# Ports scanned: TCP(4;21-22,80-80,445-445) UDP(0;) SCTP(0;) PROTOCOLS(0;)
Timestamp: 1719609780   Host: 10.1.97.49 ()     Ports: 80/open/tcp//http//
Timestamp: 1719609780   Host: 10.1.130.245 ()   Ports: 80/open/tcp//http//
Timestamp: 1719609780   Host: 10.1.99.10 ()     Ports: 80/open/tcp//http//
Timestamp: 1719609780   Host: 10.1.130.245 ()   Ports: 21/open/tcp//ftp//
Timestamp: 1719609781   Host: 10.1.130.245 ()   Ports: 445/open/tcp//microsoft-d
s//
Timestamp: 1719609781   Host: 10.1.130.245 ()   Ports: 22/open/tcp//ssh//
# Masscan done at Fri Jun 28 21:23:12 2024
```



```
** (wireshark:5325) 22:02:12.877863 [Capture MESSAGE] -- Capture stopped.
** (wireshark:5325) 22:02:12.877899 [Capture WARNING] ./ui/capture.c:722 -- capture_input_closed():
^C

┌──(root㉿kali.example.com)-[/home/student/Desktop]
└─# sudo cat /home/student/Desktop/masscan.txt
# Masscan 1.3.2 scan initiated Sun Mar  2 22:01:13 2025
# Ports scanned: TCP(4;21-22,80-80,445-445) UDP(0;) SCTP(0;) PROTOCOLS(0;)
Timestamp: 1740952873   Host: 10.1.70.221 ()    Ports: 22/open/tcp//ssh//
Timestamp: 1740952874   Host: 10.1.70.221 ()    Ports: 445/open/tcp//microsoft-ds//
Timestamp: 1740952874   Host: 10.1.70.221 ()    Ports: 21/open/tcp//ftp//
Timestamp: 1740952874   Host: 10.1.70.221 ()    Ports: 80/open/tcp//http//
# Masscan done at Sun Mar  2 22:01:25 2025

┌──(root㉿kali.example.com)-[/home/student/Desktop]
└─#
```

There you have it! Scanning for subnets on the 10.1.x.x network. This is a quick way to start when pen-testing. Note that adding other common ports to mascan such as 139, and 9200 can be rewarding but will slow the scan down.

Course Title MCIS 6173 Information and Networking Security
Term: Spring 2025

Laboratory Exercise 3.2 – Overview of Pen Testing

1. Overview

For this lesson, students will review Nmap scanning techniques with an emphasis on a penetration methodology.

2. Resources required

This exercise requires the latest **Kali Linux with Metasploitable3** environment running in the Cyber Range.

3. Initial Setup

For this exercise, you will log in to your Cyber Range account and select the latest **Kali Linux with Metasploitable3** environment, then click “start” to start your environment and “join” to get to your Linux desktop.

4. Tasks

Task 1: Nmap Scanning Review

For this course, you should already be familiar with Nmap and the switches. This lesson will cover a quick review of the Nmap scanning methodology.

Complete the following:

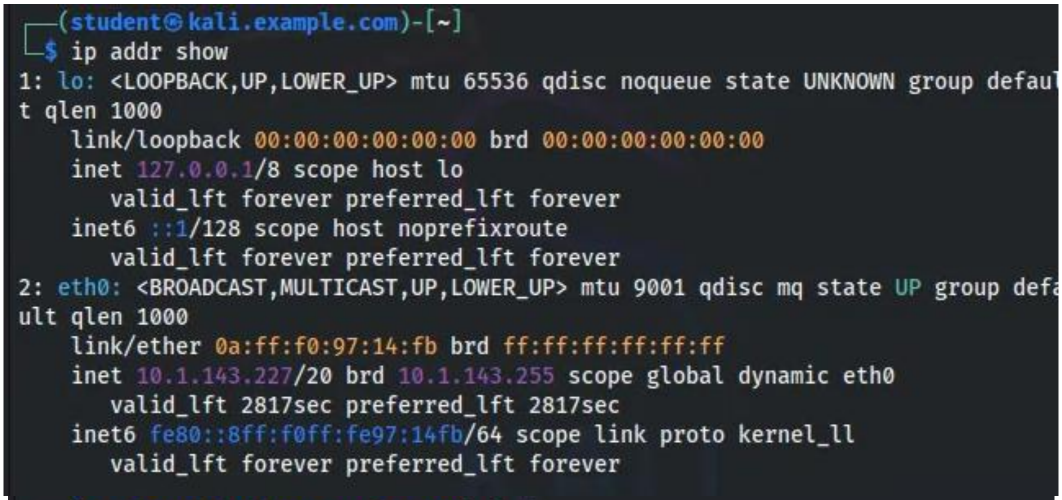
1. The first step to an internal penetration test is to find live systems. We do not need to perform a port scan to find the host, but we do need to scan the entire subnet. Remember that your IP address will be different than mine. Open a terminal and at the command prompt, complete the following:

   View the subnet

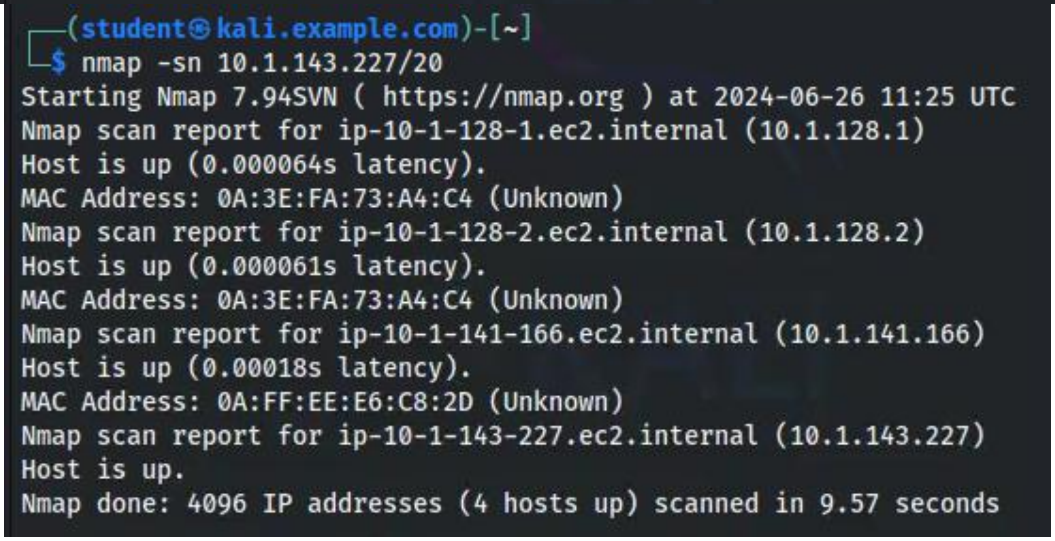
   ```
   ip addr show
   ```

   Scan for live systems

   ```
   nmap -sn <IP/20>
   ```

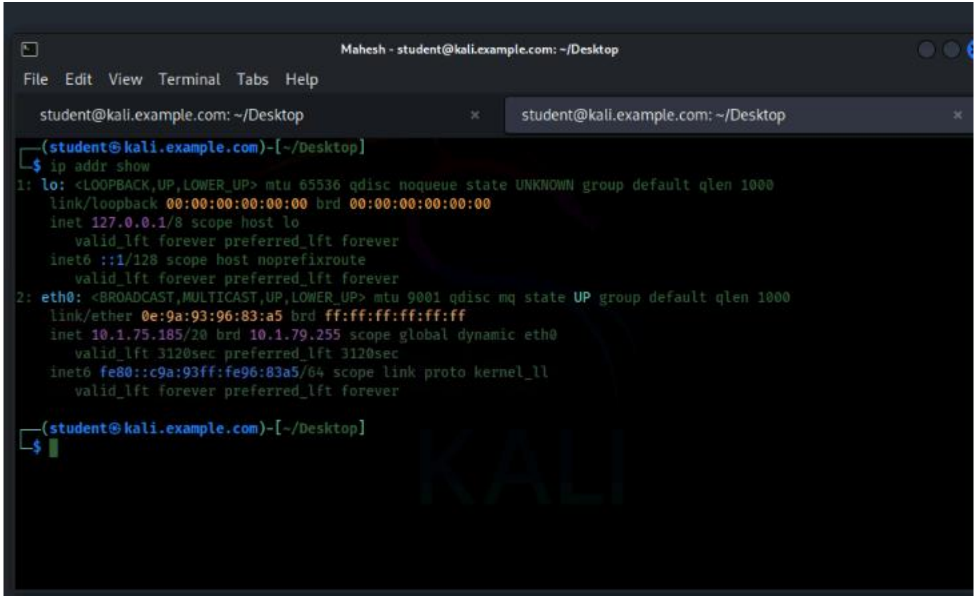


```
┌──(student㉿kali.example.com)-[~]
└─$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc mq state UP group defa
ult qlen 1000
    link/ether 0a:ff:f0:97:14:fb brd ff:ff:ff:ff:ff:ff
    inet 10.1.143.227/20 brd 10.1.143.255 scope global dynamic eth0
       valid_lft 2817sec preferred_lft 2817sec
    inet6 fe80::8ff:f0ff:fe97:14fb/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
```



```
┌──(student㉿kali.example.com)-[~]
└─$ nmap -sn 10.1.143.227/20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 11:25 UTC
Nmap scan report for ip-10-1-128-1.ec2.internal (10.1.128.1)
Host is up (0.000064s latency).
MAC Address: 0A:3E:FA:73:A4:C4 (Unknown)
Nmap scan report for ip-10-1-128-2.ec2.internal (10.1.128.2)
Host is up (0.000061s latency).
MAC Address: 0A:3E:FA:73:A4:C4 (Unknown)
Nmap scan report for ip-10-1-141-166.ec2.internal (10.1.141.166)
Host is up (0.00018s latency).
MAC Address: 0A:FF:EE:E6:C8:2D (Unknown)
Nmap scan report for ip-10-1-143-227.ec2.internal (10.1.143.227)
Host is up.
Nmap done: 4096 IP addresses (4 hosts up) scanned in 9.57 seconds
```

nmapnmacxd



Mahesh - student@kali.example.com: ~/Desktop
File Edit View Terminal Tabs Help
student@kali.example.com: ~/Desktop
student@kali.example.com: ~/Desktop

```
┌──(student㉿kali.example.com)-[~/Desktop]
└─$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc mq state UP group default qlen 1000
    link/ether 0e:9a:93:96:83:a5 brd ff:ff:ff:ff:ff:ff
    inet 10.1.75.185/20 brd 10.1.79.255 scope global dynamic eth0
       valid_lft 3120sec preferred_lft 3120sec
    inet6 fe80::c9a:93ff:fe96:83a5/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever

┌──(student㉿kali.example.com)-[~/Desktop]
└─$
```

In my case, four hosts were found. You may have found more or fewer hosts than I did. For now, I want you to understand that finding live systems is the first step to an internal penetration test.

2. The second step is to see what doors are open on these hosts. This will greatly narrow the amount of systems we enumerate, as many hosts will be filtered. Let's scan for open ports. Either **-sS** or **-sT** will work. Using **-sS** is a half-open scan and will prevent the scan from getting logged. Whereas **sT** is a full connect and will be logged. To execute the Nmap command with these options, you must be root. You can **sudo <command>** or you can **sudo su** to switch the user to root in that terminal. On the blue team (defense side) it is recommended to not switch to the root user. However, we are the red team and live on the edge.

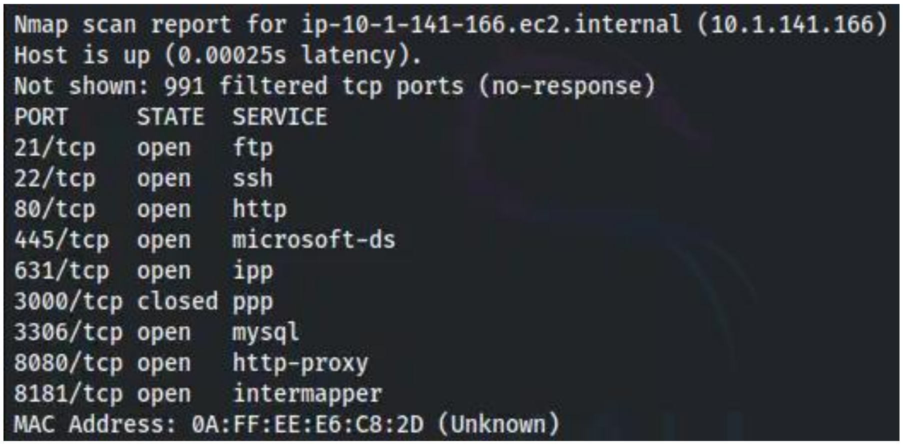
   So, at the command prompt, type **sudo su** to become root. Next, type the following:

   - **nmap -T4 -sS <IP/20>**

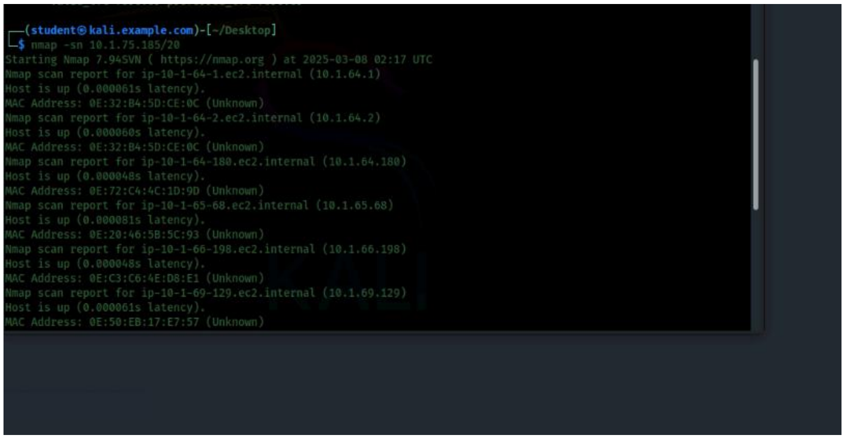
   In my case:

   - **nmap -T4 -sS 10.1.143.227/20**

There will be a lot of information printed on the screen. Scroll down until you find results that look like the screenshot below. There should only be one machine with several ports open (excluding your IP address).



```
Nmap scan report for ip-10-1-141-166.ec2.internal (10.1.141.166)
Host is up (0.00025s 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 open   intermapper
MAC Address: 0A:FF:EE:E6:C8:2D (Unknown)
```



```
┌──(student㉿kali.example.com)-[~/Desktop]
└─$ nmap -sn 10.1.75.185/20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-08 02:17 UTC
Nmap scan report for ip-10-1-64-1.ec2.internal (10.1.64.1)
Host is up (0.000061s latency).
MAC Address: 0E:32:B4:5D:CE:0C (Unknown)
Nmap scan report for ip-10-1-64-2.ec2.internal (10.1.64.2)
Host is up (0.000060s latency).
MAC Address: 0E:32:B4:5D:CE:0C (Unknown)
Nmap scan report for ip-10-1-64-180.ec2.internal (10.1.64.180)
Host is up (0.000048s latency).
MAC Address: 0E:72:C4:4C:1D:9D (Unknown)
Nmap scan report for ip-10-1-65-68.ec2.internal (10.1.65.68)
Host is up (0.000081s latency).
MAC Address: 0E:20:46:5B:5C:93 (Unknown)
Nmap scan report for ip-10-1-66-198.ec2.internal (10.1.66.198)
Host is up (0.000048s latency).
MAC Address: 0E:C3:C6:4E:D8:E1 (Unknown)
Nmap scan report for ip-10-1-69-129.ec2.internal (10.1.69.129)
Host is up (0.000061s latency).
MAC Address: 0E:50:EB:17:E7:57 (Unknown)
```

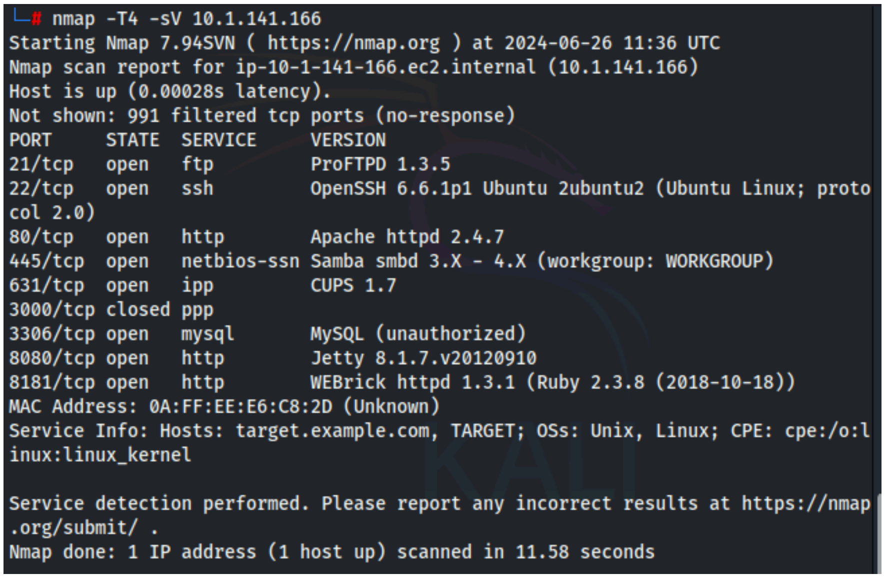
3. Now we need to find the service versions. At the command prompt, type the following:

- **`nmap -T4 -sV <IP Address of Host>`**

In my case:

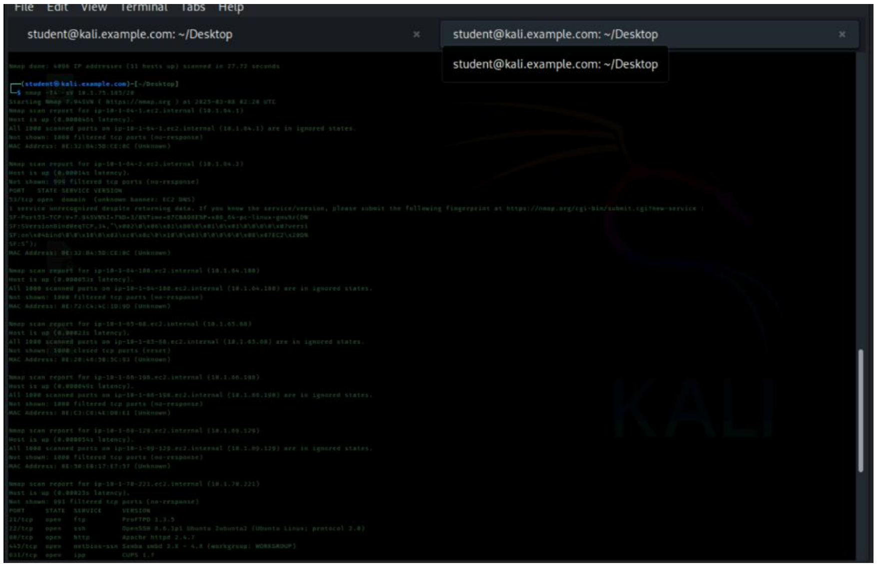
- **`nmap -T4 -sV 10.1.141.166`**

Your results should be similar to the screenshot below.

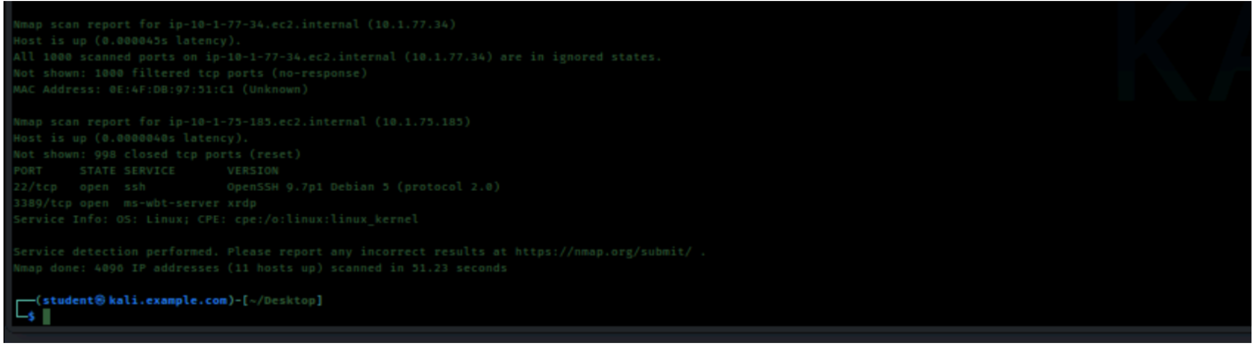


```
└─# nmap -T4 -sV 10.1.141.166
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 11:36 UTC
Nmap scan report for ip-10-1-141-166.ec2.internal (10.1.141.166)
Host is up (0.00028s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE     VERSION
21/tcp   open   ftp         ProFTPD 1.3.5
22/tcp   open   ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; proto
col 2.0)
80/tcp   open   http        Apache httpd 2.4.7
445/tcp  open   netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp  open   ipp         CUPS 1.7
3000/tcp closed ppp
3306/tcp open   mysql       MySQL (unauthorized)
8080/tcp open   http        Jetty 8.1.7.v20120910
8181/tcp open   http        WEBrick httpd 1.3.1 (Ruby 2.3.8 (2018-10-18))
MAC Address: 0A:FF:EE:E6:C8:2D (Unknown)
Service Info: Hosts: target.example.com, TARGET; OSs: Unix, Linux; CPE: cpe:/o:l
inux: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 11.58 seconds
```

inm


File Edit View Terminal Tabs Help
student@kali.example.com: ~/Desktop
student@kali.example.com: ~/Desktop
student@kali.example.com: ~/Desktop

```
Nmap done: 4096 IP addresses (11 hosts up) scanned in 27.72 seconds

┌──(student㉿kali.example.com)-[~/Desktop]
└─$ nmap -T4 -sV 10.1.75.185/20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-08 02:28 UTC
Nmap scan report for ip-10-1-64-1.ec2.internal (10.1.64.1)
Host is up (0.000046s latency).
All 1000 scanned ports on ip-10-1-64-1.ec2.internal (10.1.64.1) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 0E:32:84:5D:CE:0C (Unknown)

Nmap scan report for ip-10-1-64-2.ec2.internal (10.1.64.2)
Host is up (0.00014s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
53/tcp open  domain  (unknown banner: EC2 DNS)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.94SVN%I=7%D=3/8%Time=67CBA08E%P=x86_64-pc-linux-gnu%r(DN
SF:SVersionBindReqTCP,34,"\x002\0\x06\x81\x80\0\x01\0\x01\0\0\0\0\x07versi
SF:on\x04bind\0\0\x10\0\x03\xc0\x0c\0\x10\0\x03\0\0\0\0\0\x08\x07EC2\x20DN
SF:S");
MAC Address: 0E:32:84:5D:CE:0C (Unknown)

Nmap scan report for ip-10-1-64-100.ec2.internal (10.1.64.100)
Host is up (0.000053s latency).
All 1000 scanned ports on ip-10-1-64-100.ec2.internal (10.1.64.100) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 0E:72:C4:4C:1D:9D (Unknown)

Nmap scan report for ip-10-1-65-88.ec2.internal (10.1.65.88)
Host is up (0.00023s latency).
All 1000 scanned ports on ip-10-1-65-88.ec2.internal (10.1.65.88) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 0E:20:48:58:5C:93 (Unknown)

Nmap scan report for ip-10-1-66-198.ec2.internal (10.1.66.198)
Host is up (0.000049s latency).
All 1000 scanned ports on ip-10-1-66-198.ec2.internal (10.1.66.198) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 0E:C3:C8:4E:D8:E1 (Unknown)

Nmap scan report for ip-10-1-69-129.ec2.internal (10.1.69.129)
Host is up (0.000054s latency).
All 1000 scanned ports on ip-10-1-69-129.ec2.internal (10.1.69.129) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 0E:50:E8:17:E7:57 (Unknown)

Nmap scan report for ip-10-1-70-221.ec2.internal (10.1.70.221)
Host is up (0.00023s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE     VERSION
21/tcp   open   ftp         ProFTPD 1.3.5
22/tcp   open   ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2.0)
80/tcp   open   http        Apache httpd 2.4.7
445/tcp  open   netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp  open   ipp         CUPS 1.7
```



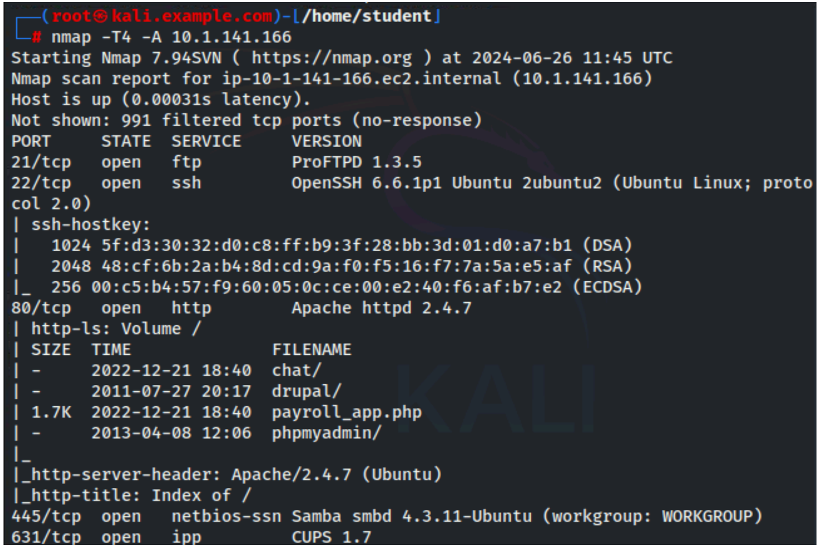
```
Nmap scan report for ip-10-1-77-34.ec2.internal (10.1.77.34)
Host is up (0.000045s latency).
All 1000 scanned ports on ip-10-1-77-34.ec2.internal (10.1.77.34) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 0E:4F:DB:97:51:C1 (Unknown)

Nmap scan report for ip-10-1-75-185.ec2.internal (10.1.75.185)
Host is up (0.0000040s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
22/tcp   open  ssh           OpenSSH 9.7p1 Debian 5 (protocol 2.0)
3389/tcp open  ms-wbt-server xrdp
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 4096 IP addresses (11 hosts up) scanned in 51.23 seconds

┌──(student㉿kali.example.com)-[~/Desktop]
└─$ 
```

4. Now we complete OS detection (enumeration). At the command prompt, type the following:

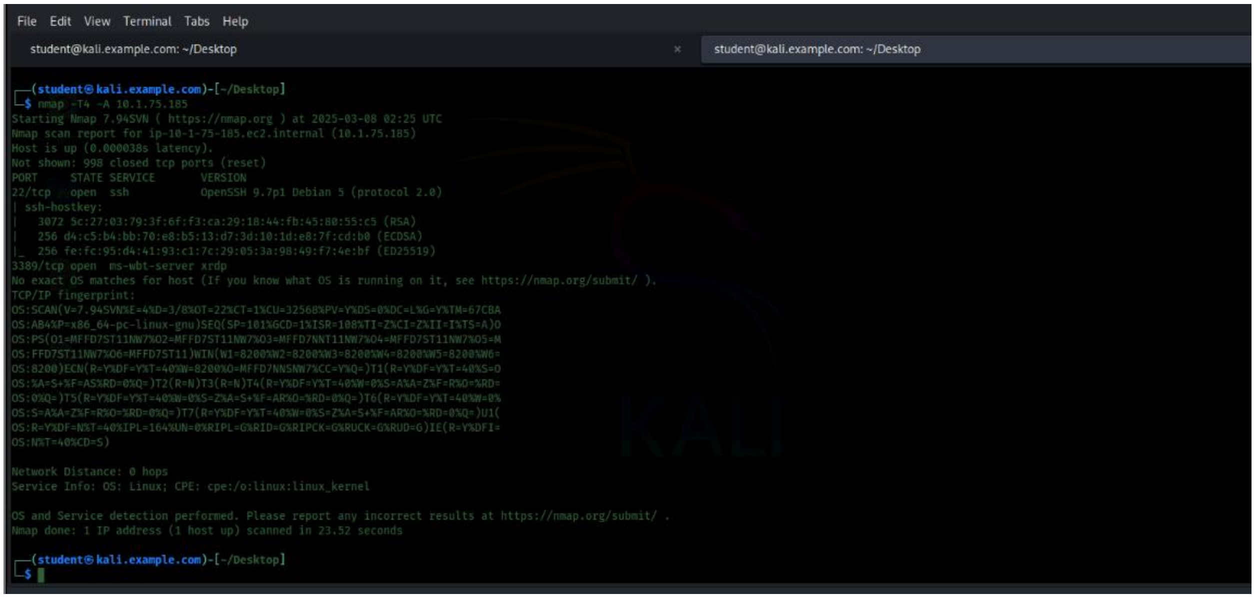
    - **`nmap -T4 -A <IP Address of Host>`**

    In my case:

    - **`nmap -T4 -A 10.1.141.166`**



```
┌──(root㉿kali.example.com)-[/home/student]
└─# nmap -T4 -A 10.1.141.166
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-26 11:45 UTC
Nmap scan report for ip-10-1-141-166.ec2.internal (10.1.141.166)
Host is up (0.00031s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE     VERSION
21/tcp   open   ftp         ProFTPD 1.3.5
22/tcp   open   ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; proto
col 2.0)
| ssh-hostkey:
|   1024 5f:d3:30:32:d0:c8:ff:b9:3f:28:bb:3d:01:d0:a7:b1 (DSA)
|   2048 48:cf:6b:2a:b4:8d:cd:9a:f0:f5:16:f7:7a:5a:e5:af (RSA)
|_  256 00:c5:b4:57:f9:60:05:0c:ce:00:e2:40:f6:af:b7:e2 (ECDSA)
80/tcp   open   http        Apache httpd 2.4.7
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2022-12-21 18:40  chat/
| -     2011-07-27 20:17  drupal/
| 1.7K  2022-12-21 18:40  payroll_app.php
| -     2013-04-08 12:06  phpmyadmin/
|_
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Index of /
445/tcp  open   netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
631/tcp  open   ipp         CUPS 1.7
```


File Edit View Terminal Tabs Help
student@kali.example.com: ~/Desktop
student@kali.example.com: ~/Desktop

```
┌──(student㉿kali.example.com)-[~/Desktop]
└─$ nmap -T4 -A 10.1.75.185
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-08 02:25 UTC
Nmap scan report for ip-10-1-75-185.ec2.internal (10.1.75.185)
Host is up (0.000038s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
22/tcp   open  ssh           OpenSSH 9.7p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   3072 5c:27:03:79:3f:6f:f3:ca:29:18:44:fb:45:80:55:c5 (RSA)
|   256 d4:c5:b4:bb:70:e8:b5:13:d7:3d:10:1d:e8:7f:cd:b0 (ECDSA)
|_  256 fe:fc:95:d4:41:93:c1:7c:29:05:3a:98:49:f7:4e:bf (ED25519)
3389/tcp open  ms-wbt-server xrdp
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=3/8%OT=22%CT=1%CU=32568%PV=Y%DS=0%DC=L%G=Y%TM=67CBA
OS:AB4%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=108%TI=Z%CI=Z%II=I%TS=A)O
OS:PS(O1=MFFD7ST11NW7%O2=MFFD7ST11NW7%O3=MFFD7NNT11NW7%O4=MFFD7ST11NW7%O5=M
OS:FFD7ST11NW7%O6=MFFD7ST11)WIN(W1=8200%W2=8200%W3=8200%W4=8200%W5=8200%W6=
OS:8200)ECN(R=Y%DF=Y%T=40%W=8200%O=MFFD7NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O
OS:%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=
OS:0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%
OS:S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(
OS:R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=
OS:N%T=40%CD=S)

Network Distance: 0 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

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 23.52 seconds

┌──(student㉿kali.example.com)-[~/Desktop]
└─$ 
```

Now we will look at Nmap reports. Briefly, the Nmap output formats are as follows:

-oN - Normal Nmap output
-oX - XML format
-oS - Script kiddie output
-oG - Grepable format
-oA - All 3 formats

For more information on these types of Nmap outputs, please read about them here.

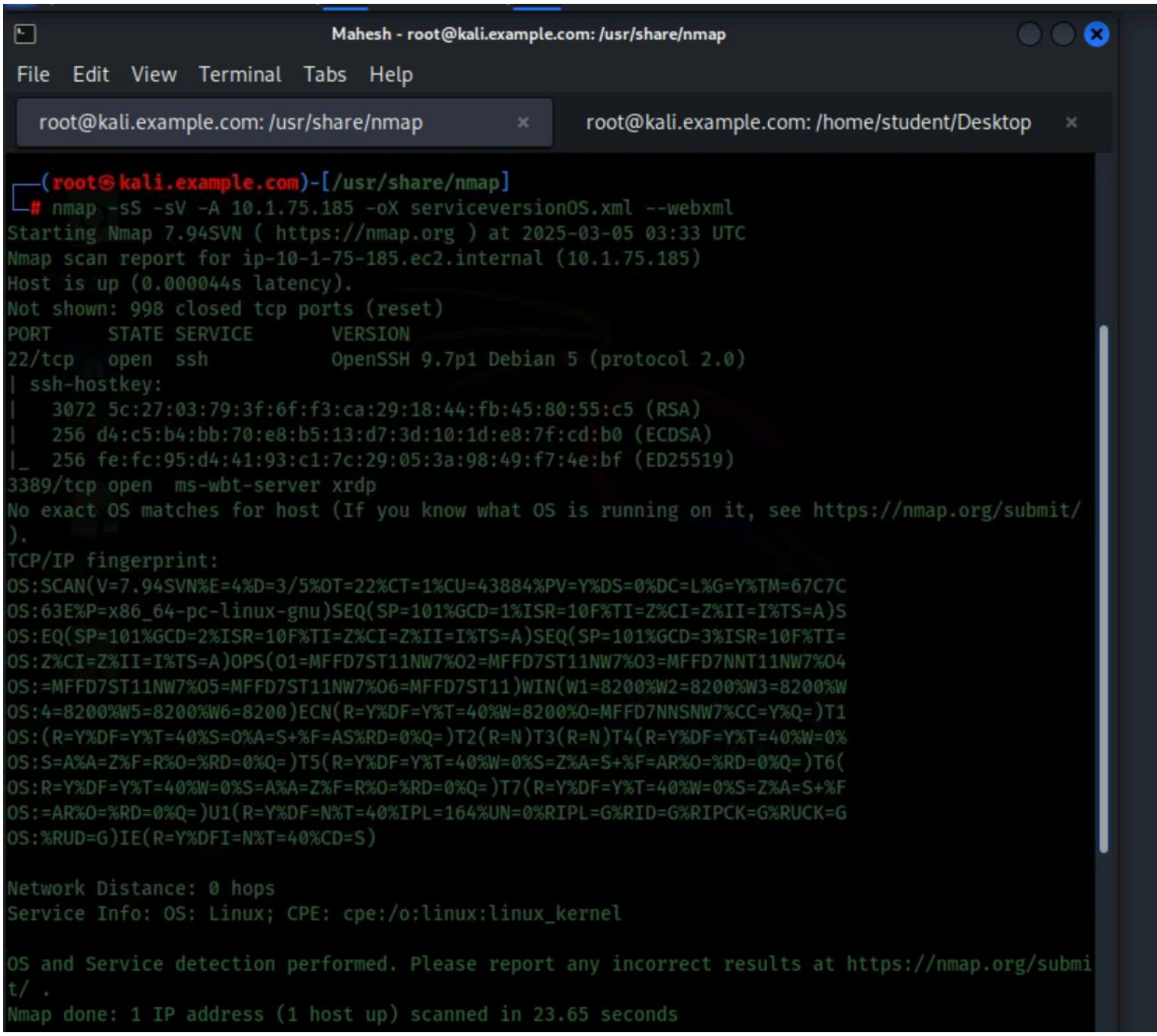
a. First, we need to navigate to the Nmap directory; this way the script will work properly. In the root terminal, type the following:

   - **`cd /usr/share/nmap/`**

b. We will complete an XML format output. At the command prompt, type the following:

   In my case:

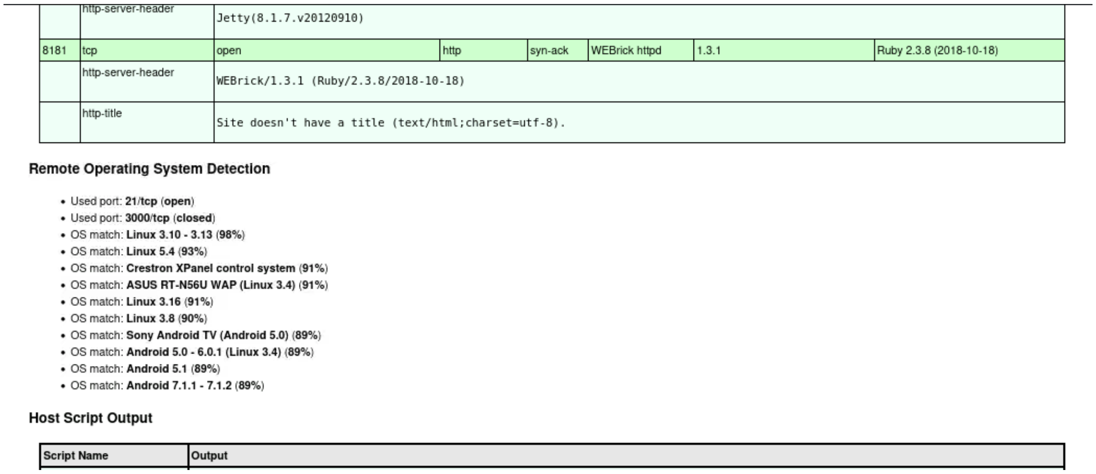
   - **`nmap -sS -sV -A 10.1.141.166 -oX serviceversionOS.xml --webxml`**


Mahesh - root@kali.example.com: /usr/share/nmap
File Edit View Terminal Tabs Help
root@kali.example.com: /usr/share/nmap
root@kali.example.com: /home/student/Desktop

```
┌──(root㉿kali.example.com)-[/usr/share/nmap]
└─# nmap -sS -sV -A 10.1.75.185 -oX serviceversionOS.xml --webxml
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-05 03:33 UTC
Nmap scan report for ip-10-1-75-185.ec2.internal (10.1.75.185)
Host is up (0.000044s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
22/tcp   open  ssh           OpenSSH 9.7p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   3072 5c:27:03:79:3f:6f:f3:ca:29:18:44:fb:45:80:55:c5 (RSA)
|   256 d4:c5:b4:bb:70:e8:b5:13:d7:3d:10:1d:e8:7f:cd:b0 (ECDSA)
|_  256 fe:fc:95:d4:41:93:c1:7c:29:05:3a:98:49:f7:4e:bf (ED25519)
3389/tcp open  ms-wbt-server xrdp
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/
).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=3/5%OT=22%CT=1%CU=43884%PV=Y%DS=0%DC=L%G=Y%TM=67C7C
OS:63E%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=10F%TI=Z%CI=Z%II=I%TS=A)S
OS:EQ(SP=101%GCD=2%ISR=10F%TI=Z%CI=Z%II=I%TS=A)SEQ(SP=101%GCD=3%ISR=10F%TI=
OS:Z%CI=Z%II=I%TS=A)OPS(O1=MFFD7ST11NW7%O2=MFFD7ST11NW7%O3=MFFD7NNT11NW7%O4
OS:=MFFD7ST11NW7%O5=MFFD7ST11NW7%O6=MFFD7ST11)WIN(W1=8200%W2=8200%W3=8200%W
OS:4=8200%W5=8200%W6=8200)ECN(R=Y%DF=Y%T=40%W=8200%O=MFFD7NNSNW7%CC=Y%Q=)T1
OS:(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%
OS:S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(
OS:R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F
OS:=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G
OS:%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 0 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submi
t/ .
Nmap done: 1 IP address (1 host up) scanned in 23.65 seconds
```

c. This scan will reveal what ports, services, and operating systems are running on the host that we discovered. Once the Nmap scan is complete, do the following:

- Click on the **File** menu in the *terminal window* and click **Open Tab**.
- Navigate to the Nmap folder by typing **`cd /usr/share/nmap`** and then **ENTER**.
- To open the xml file, type **`xdg-open .`** and press **ENTER**.
- Double-click on the file "serviceversionOS.xml" to view the output.



	http-server-header	Jetty(8.1.7.v20120910)					
8181	tcp	open	http	syn-ack	WEBrick httpd	1.3.1	Ruby 2.3.8 (2018-10-18)
	http-server-header	WEBrick/1.3.1 (Ruby/2.3.8/2018-10-18)					
	http-title	Site doesn't have a title (text/html;charset=utf-8).					

Remote Operating System Detection

- Used port: **21/tcp** (**open**)
- Used port: **3000/tcp** (**closed**)
- OS match: **Linux 3.10 - 3.13** (**98%**)
- OS match: **Linux 5.4** (**93%**)
- OS match: **Crestron XPanel control system** (**91%**)
- OS match: **ASUS RT-N56U WAP (Linux 3.4)** (**91%**)
- OS match: **Linux 3.16** (**91%**)
- OS match: **Linux 3.8** (**90%**)
- OS match: **Sony Android TV (Android 5.0)** (**89%**)
- OS match: **Android 5.0 - 6.0.1 (Linux 3.4)** (**89%**)
- OS match: **Android 5.1** (**89%**)
- OS match: **Android 7.1.1 - 7.1.2** (**89%**)

Host Script Output

Script Name	Output

Remember, in a real penetration test you would scan all 65535 ports. We only scanned the top 1000 ports due to the time it takes to complete a full scan of all the ports. This is also only the scanning phase of a penetration test. We will discuss more penetration steps and how to speed up the scanning process in later modules.

5. References:

https://nmap.org/book/man-output.html

[This portion of the lab exercise is provided for instructors who will be using this lab in a class they are teaching.]