



Course: CYB301
Security Defense and Response
(Canadian Context)

Lab 10: Analyzing Indicators of Compromise

Coordinator and Instructor:
Muhammad Siddiqui

Student: Saiprasad Raman (23074624)

Activity 1: Scanning a Network (VirtualBox)

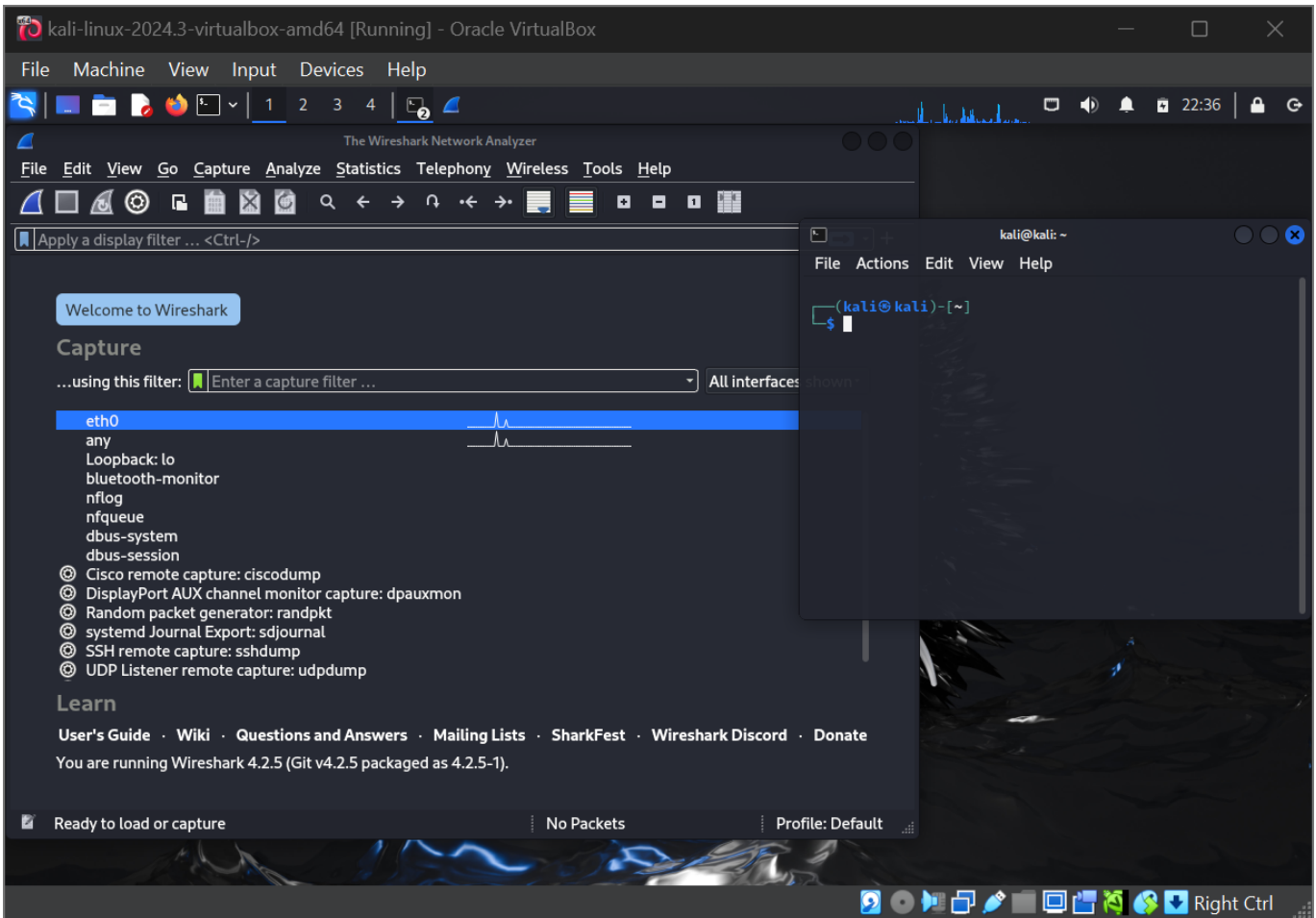
In this lab, you will use Wireshark to identify a network scan of a Linux system.

Part 1: Boot a Kali Linux system and a target system and set up the exercise.

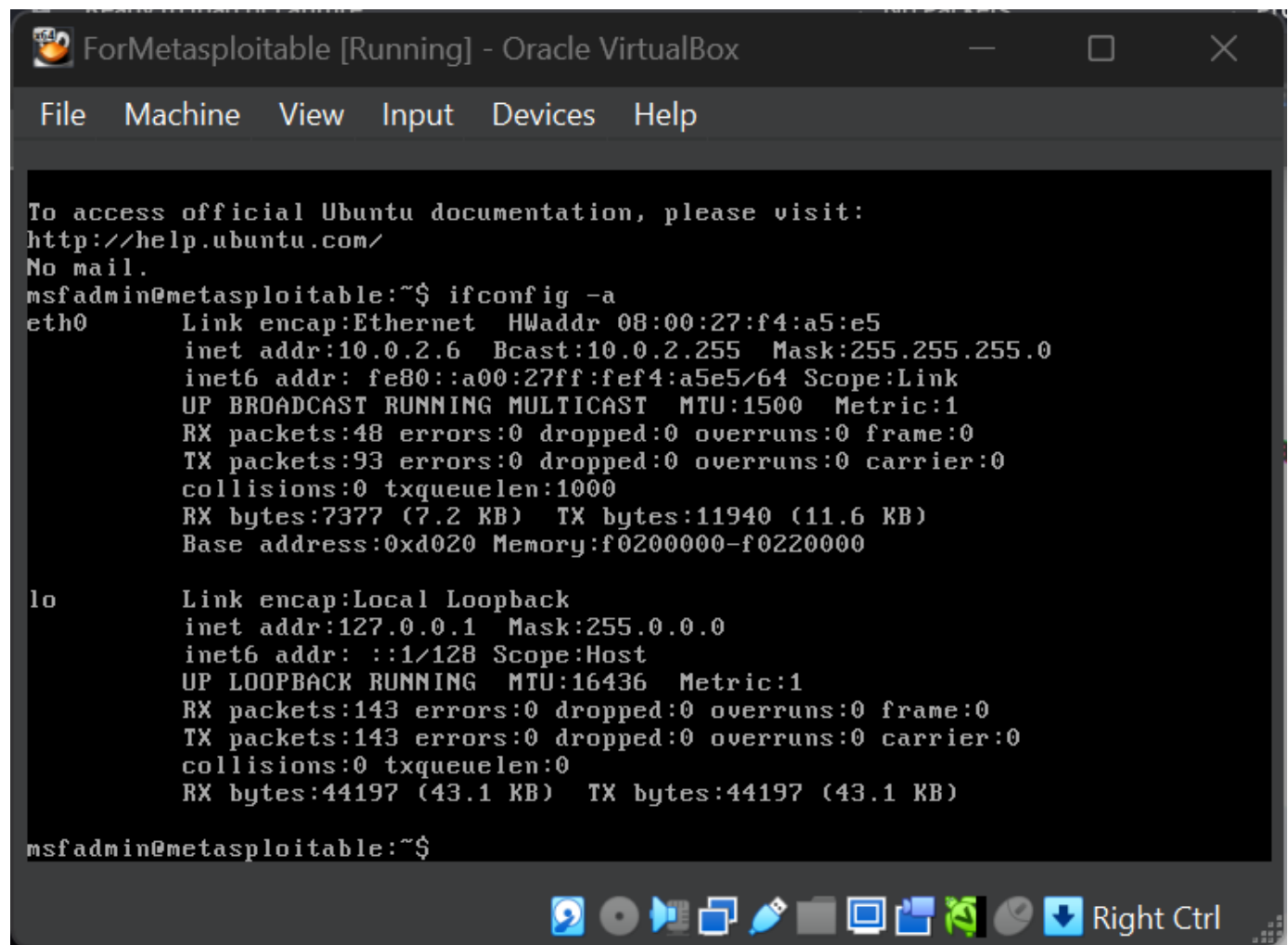
- Start your Kali Linux virtual machine and the Metasploitable virtual machine; log in to both.



- Open a terminal window and Wireshark on the Kali Linux system (Wireshark can be found in the Applications menu under option 09 Sniffing & Spoofing).



- Determine the IP address of the target system. From the command prompt on the Metasploitable system, enter **ifconfig -a** and record its IP address.



The screenshot shows a terminal window titled "ForMetasploitable [Running] - Oracle VirtualBox". The terminal displays the following text:

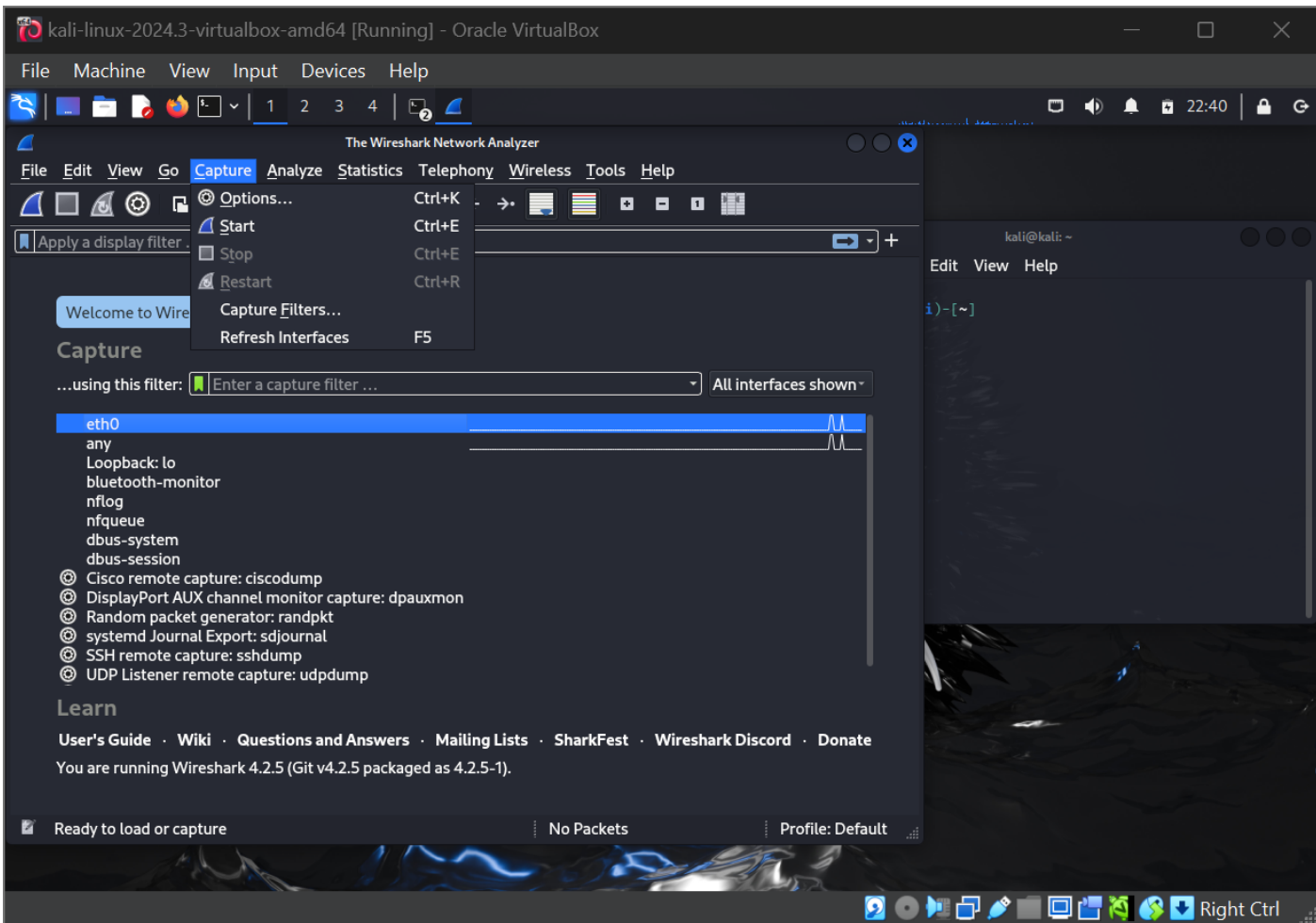
```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig -a
eth0      Link encap:Ethernet  HWaddr 08:00:27:f4:a5:e5
          inet addr:10.0.2.6  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fef4:a5e5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:48 errors:0 dropped:0 overruns:0 frame:0
          TX packets:93 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7377 (7.2 KB)  TX bytes:11940 (11.6 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:143 errors:0 dropped:0 overruns:0 frame:0
          TX packets:143 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:44197 (43.1 KB)  TX bytes:44197 (43.1 KB)

msfadmin@metasploitable:~$
```

The terminal window has a menu bar with "File", "Machine", "View", "Input", "Devices", and "Help". At the bottom, there is a taskbar with various icons and a "Right Ctrl" button.

- Start the Wireshark capture. Select the eth0 interface and then choose **Capture > Start**. (Take the screenshot.)



Part 2: Perform a network scan and visit the web server.

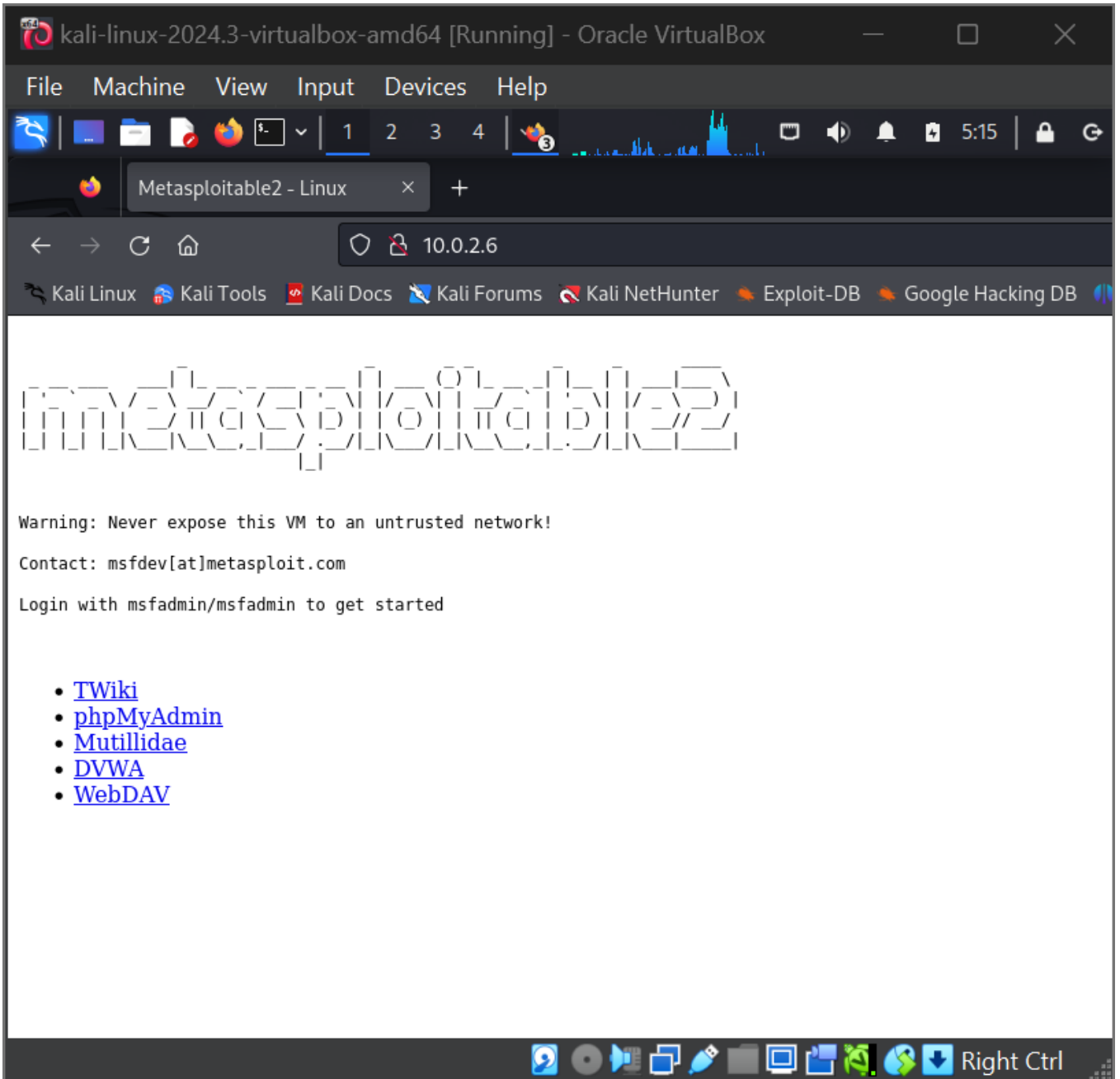
- From the terminal, execute the following command: **nmap -p 1-65535 [ip address of the Metasploitable machine]** Record one of the ports listed as open. Take the screenshot.

The screenshot displays a Kali Linux virtual machine environment. The main window is Wireshark, showing a packet capture on the `eth0` interface. The filter is set to `tcp.port==21`. The packet list shows several TCP packets, with packet 125 selected. The packet details pane shows the structure of the selected packet: Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol (Src Port: 45236, Dst Port: 21). The packet bytes pane shows the raw data in hexadecimal and ASCII.

In the bottom right corner, a terminal window is open, showing the execution of the `nmap` command:

```
(kali@kali)-[~]
$ nmap -p 1-65535 10.0.2.6
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-13 05:05 EDT
Nmap scan report for 10.0.2.6
Host is up (0.0015s 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
```

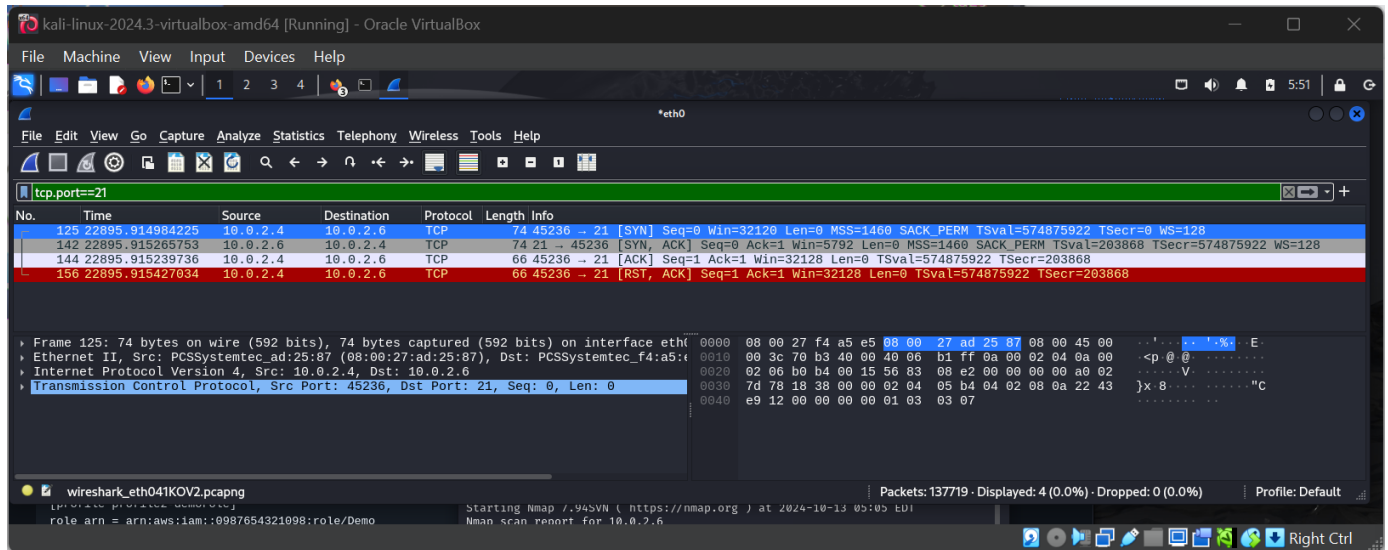
- Start the **IceWeasel/firefox** browser in Kali and navigate to the IP address of the Metasploitable system.



Part 3: Identify scan traffic.

- Stop the Wireshark capture. Click the red square stop button at the top left of the Wireshark screen.
- Review the traffic you captured. Search for the port you found by entering **tcp.port==[port you identified]** in the filter box.

(Take the screenshot.)



- What traffic was sent? If you rerun this scan with other TCP connection options like **-sS** or **-sT**, does this change?

Ans.

The traffic sent was SYN-ACK packets.

If we rerun the scan with TCP connection option **-sS**, it doesn't complete the TCP handshake

The screenshot shows a Kali Linux virtual machine running Wireshark and a terminal. The terminal window displays the command `nmap -sS -p 1-65535 10.0.2.6` and its output, which indicates that the host is up and lists several open ports. The Wireshark interface shows a packet capture on the `eth0` interface, with a packet list table showing a SYN-ACK packet from 10.0.2.6 to 10.0.2.4 on port 21.

No.	Time	Source	Destination	Protocol	Length	Info
14	39.083885083	10.0.2.4	10.0.2.6	TCP	58	41980 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
25	39.085634083	10.0.2.6	10.0.2.4	TCP	60	21 → 41980 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
29	39.085978828	10.0.2.4	10.0.2.6	TCP	54	41980 → 21 [RST] Seq=1 Win=0 Len=0

While **-sT** performs a full TCP handshake.

The screenshot shows a Kali Linux virtual machine running Wireshark and a terminal. The terminal window displays the command `nmap -sT -p 1-65535 10.0.2.6` and its output, which indicates that the host is up and lists several open ports. The Wireshark interface shows a packet capture on the `eth0` interface, with a packet list table showing a full TCP handshake sequence: a SYN packet from 10.0.2.4 to 10.0.2.6 on port 21, a SYN-ACK packet from 10.0.2.6 to 10.0.2.4 on port 21, and an ACK packet from 10.0.2.4 to 10.0.2.6 on port 21.

No.	Time	Source	Destination	Protocol	Length	Info
25	19.938209450	10.0.2.4	10.0.2.6	TCP	74	38866 → 21 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=577779397 TSecr=0 WS=128
57	19.938715829	10.0.2.6	10.0.2.4	TCP	74	21 → 38866 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=494130 TSecr=577779397
60	19.938685440	10.0.2.4	10.0.2.6	TCP	66	38866 → 21 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=577779398 TSecr=494130
74	19.938992390	10.0.2.4	10.0.2.6	TCP	66	38866 → 21 [RST, ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=577779398 TSecr=494130

- Review traffic for port **80**. You should see both the scan and a visit from the Kali Linux web browser.
- Take the screenshot.** How do these differ?

Ans:

Note: Metasploitable's IP address has changed here as this part of the assignment is done at a different network.

After performing a scan in Nmap and opening a browser. Here are the differences that were found:

NMAP	Kali Linux Web Browser
Consists of SYN or SYN-ACK and RST packets	Consists of HTTP GET (420) requests and responses
Packets sent and received are fewer as it just checks if the port is open.	Packets sent and received are much more, as it includes multiple requests and responses
Doesn't consist of payload data	Consists of payload data, images, HTML.
It is used to determine the status of the port.	It retrieves the content of the website from the Server.

The screenshot displays a Wireshark interface within a Kali Linux virtual machine. The top pane shows a list of network packets. Packet 131377 is selected, and its details are shown in the bottom pane. The packet is identified as an HTTP GET request for 'http://10.10.10.10/420'. The packet list shows a SYN scan from 192.168.1.105 to 192.168.1.4 on port 80. The packet details show the HTTP request structure, including the GET method and the requested URI.