Course: CYB301

Security Defense and Response

(Canadian Context)

Lab 10: Analyzing Indicators of Compromise

Coordinator and Instructor:

Muhammad Siddiqui

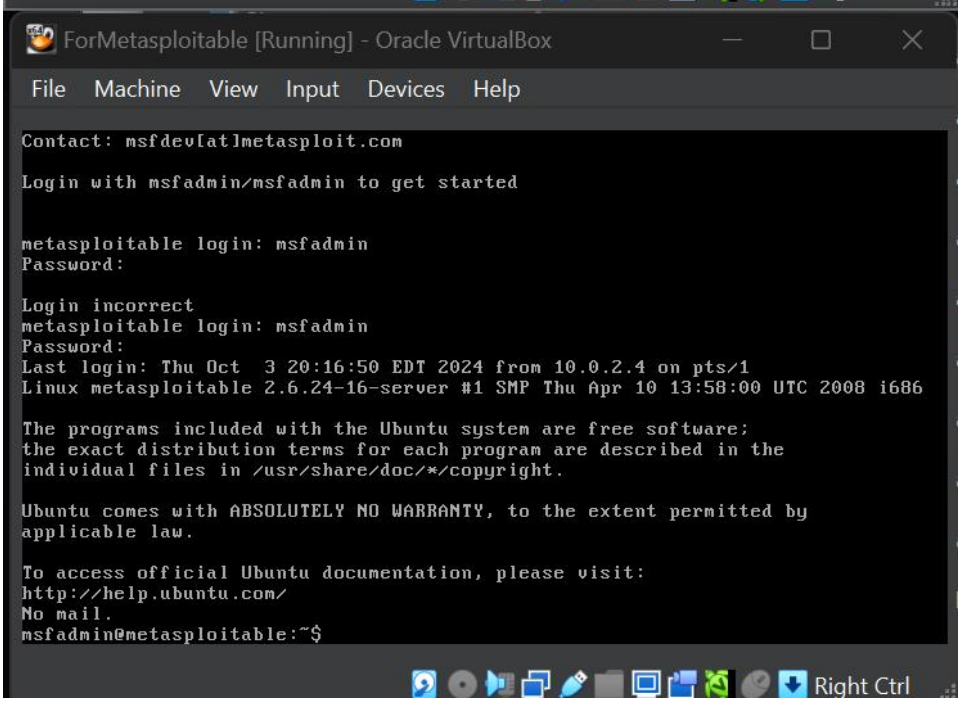
Student: Saiprasad Raman (23074624)

Activity 1: Scanning a Network (VirtualBox)

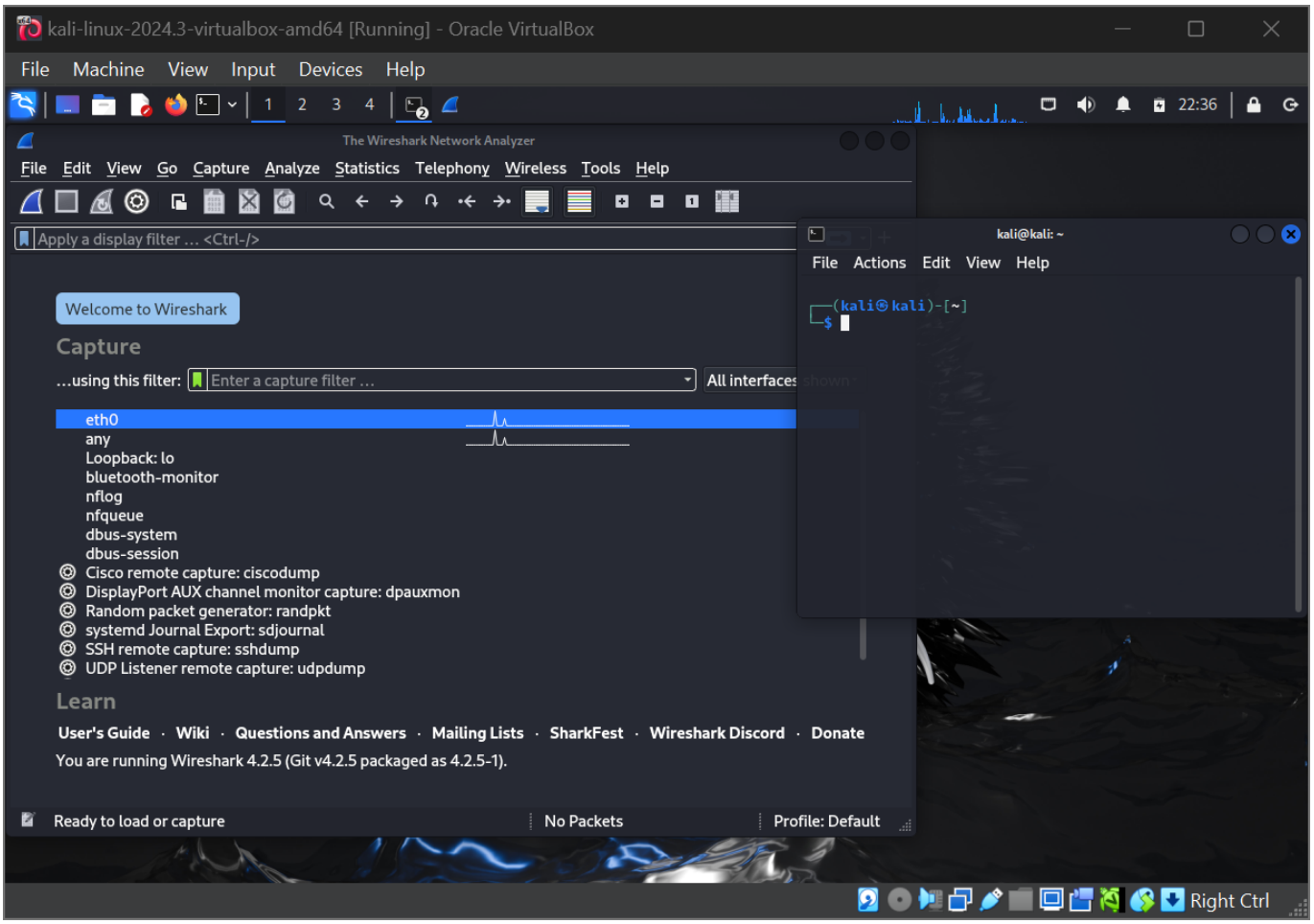
In this lab, you will use Wireshark to identify a network scan of a Linux system.

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

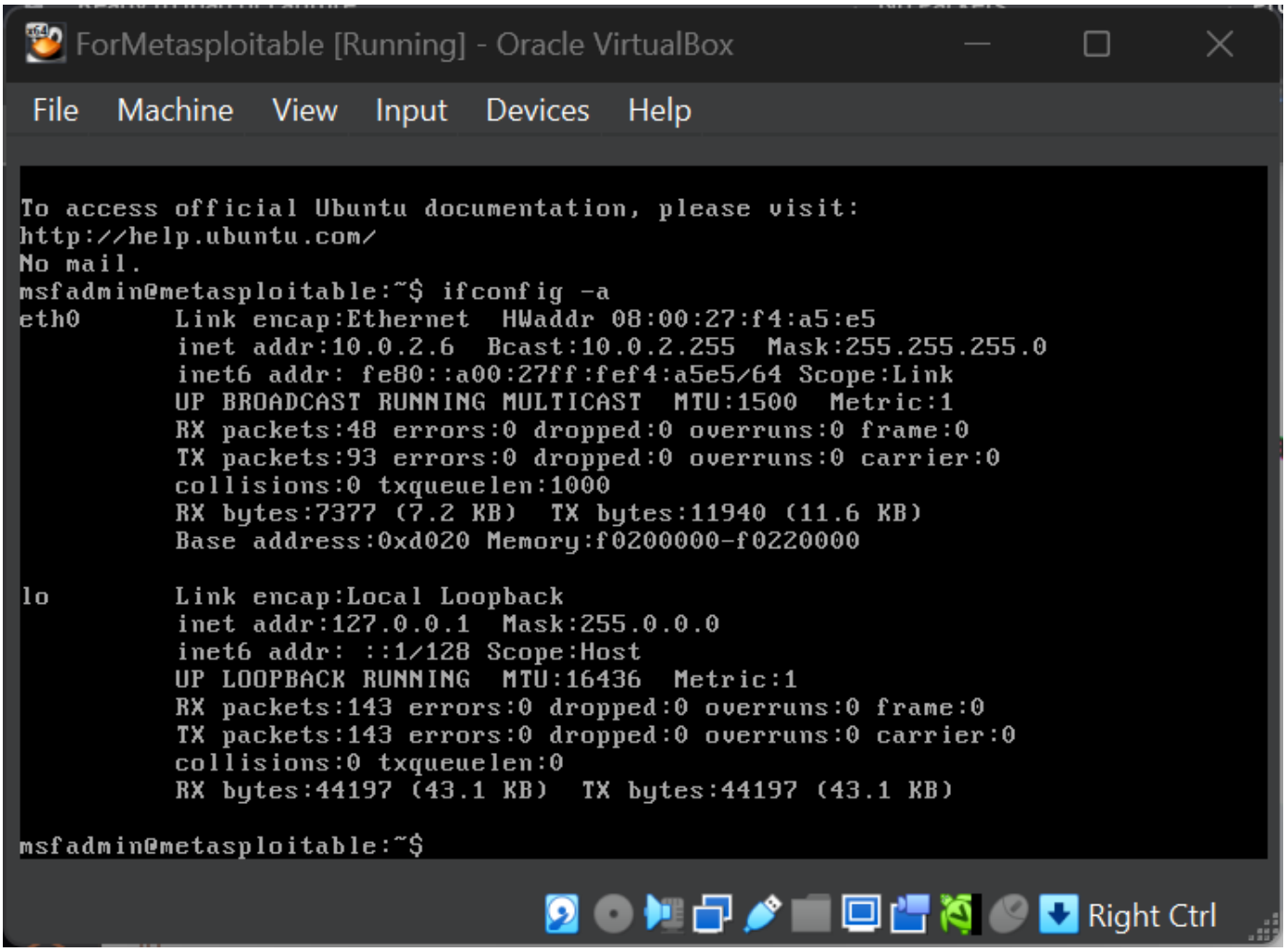
- Start your Kali Linux virtual machine and the Metasploitable virtual machine; log in to both.



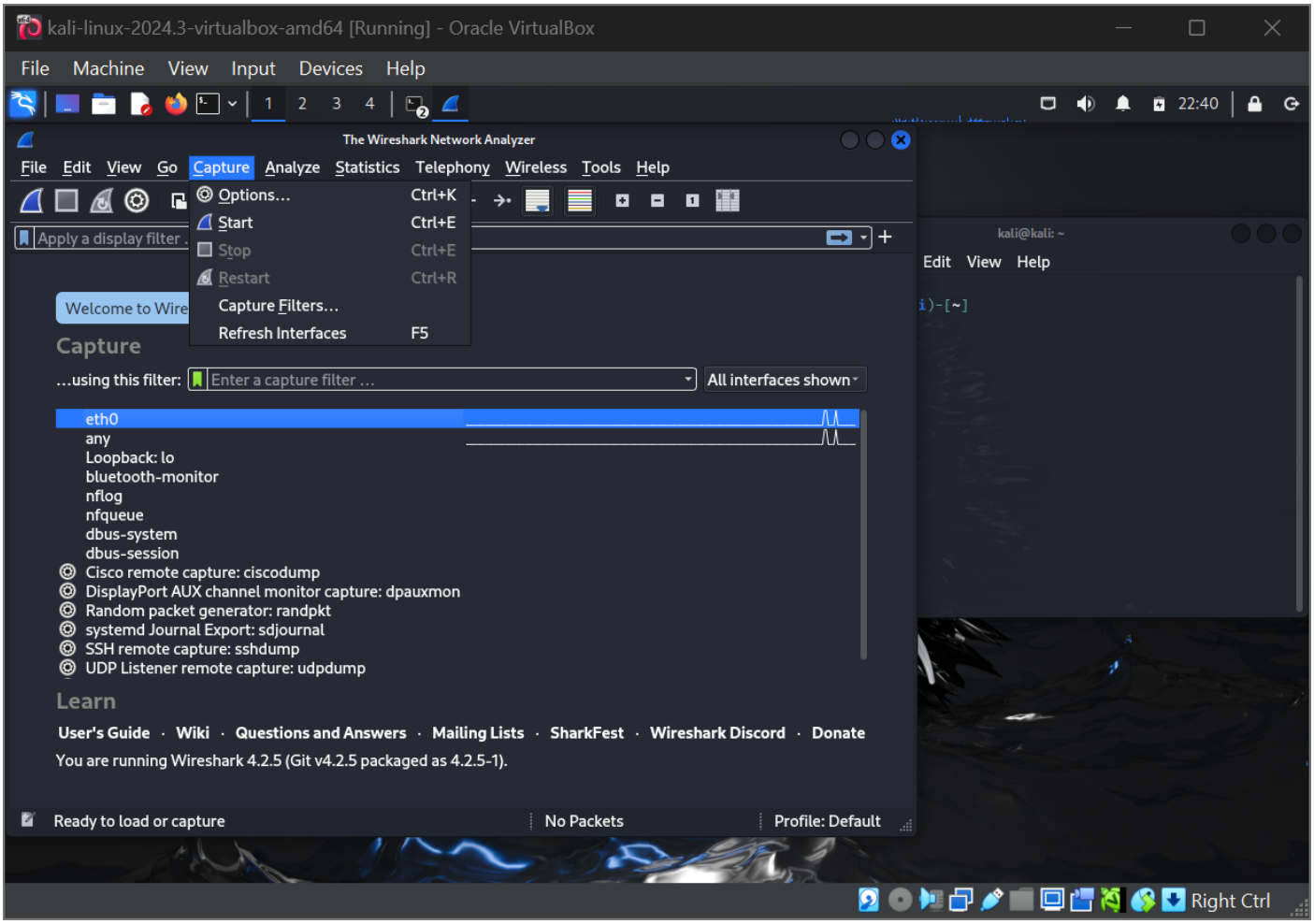
- Open a terminal window and Wireshark on the Kali Linux system (Wireshark can be found in the Applications menu under option 09 Sniffing & Spoofing).



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

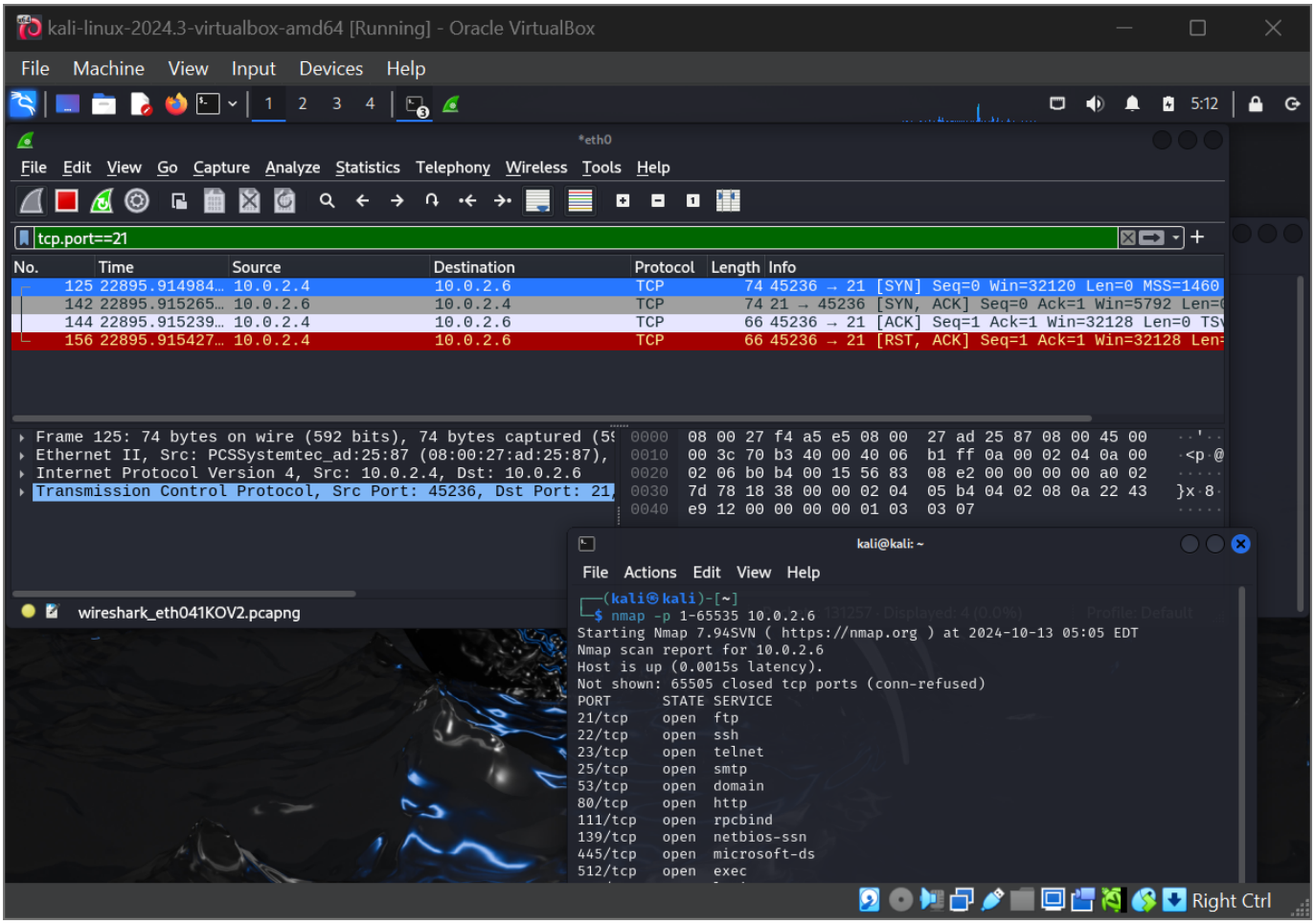


- Start the Wireshark capture. Select the eth0 interface and then choose **Capture ➢ Start**. **(Take the screenshot.)**

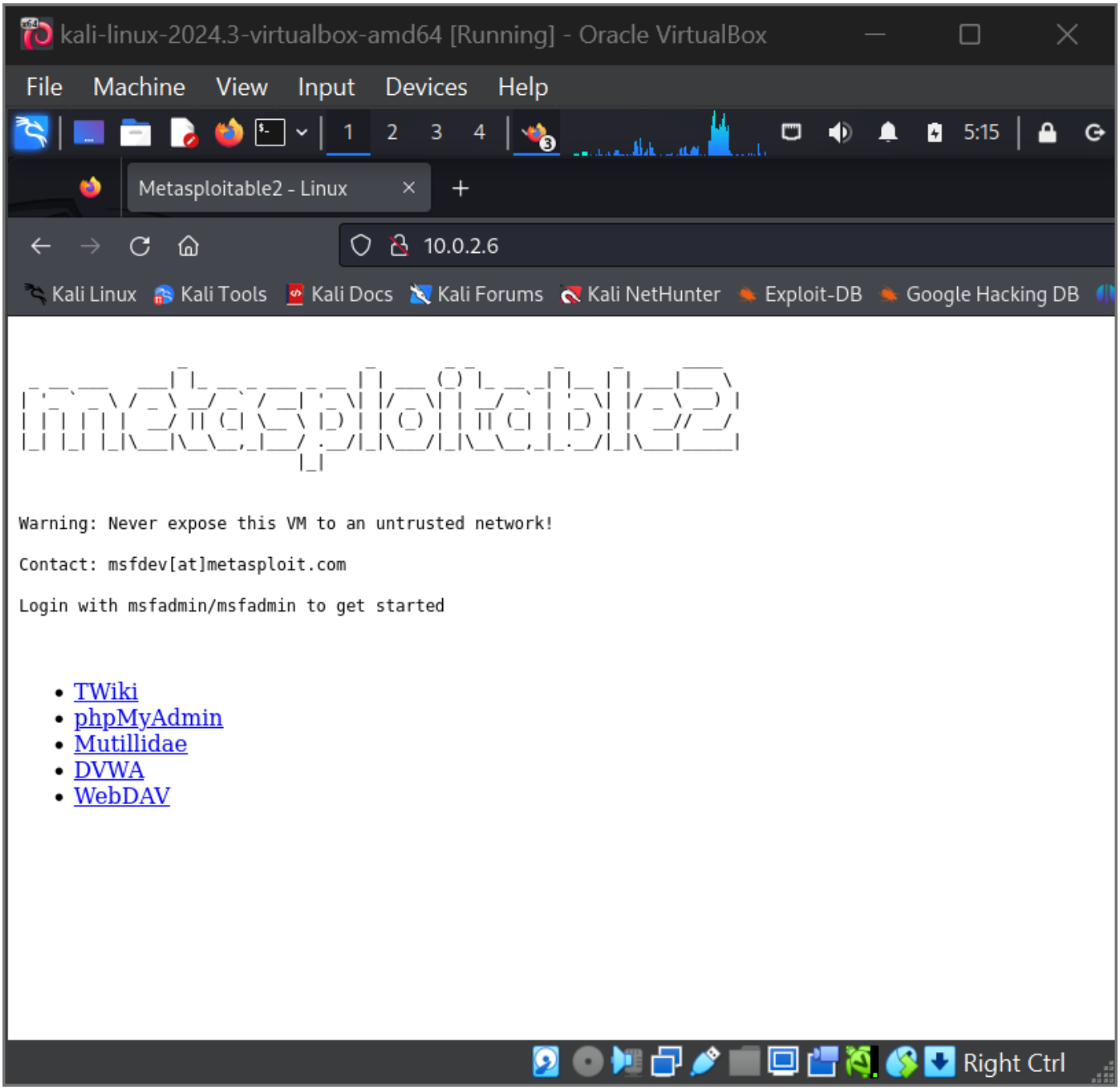


Part 2: Perform a network scan and visit the web server.

- 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.**



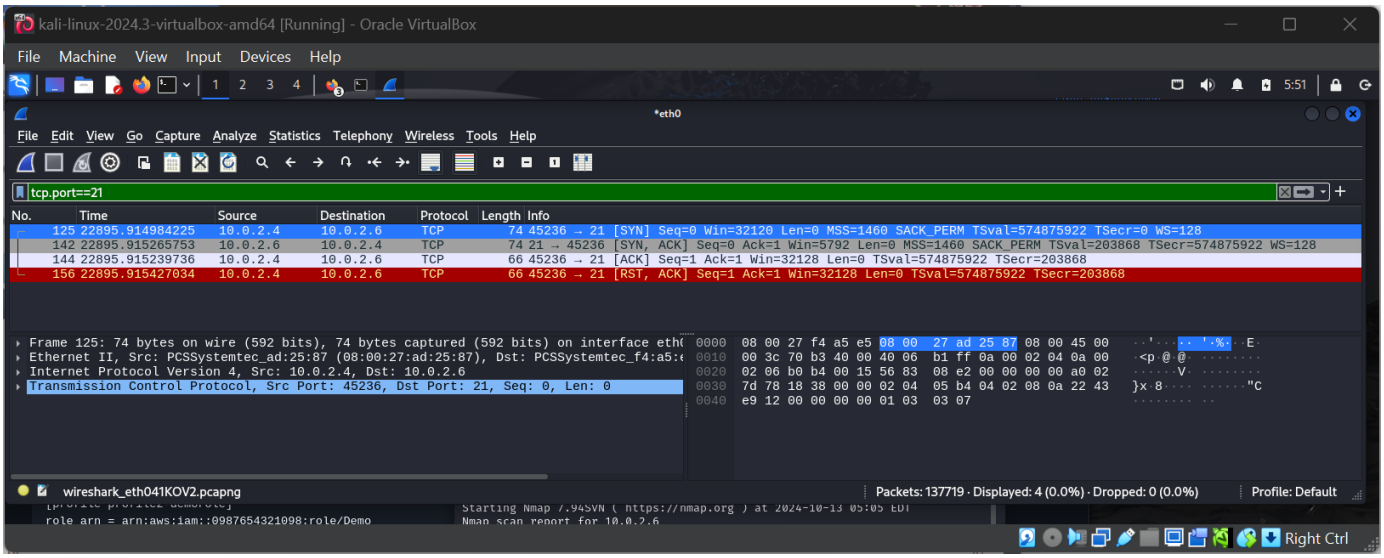
- Start the **IceWeasel/firefox** browser in Kali and navigate to the IP address of the Metasploitable system.



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 box.

(Take the screenshot.)

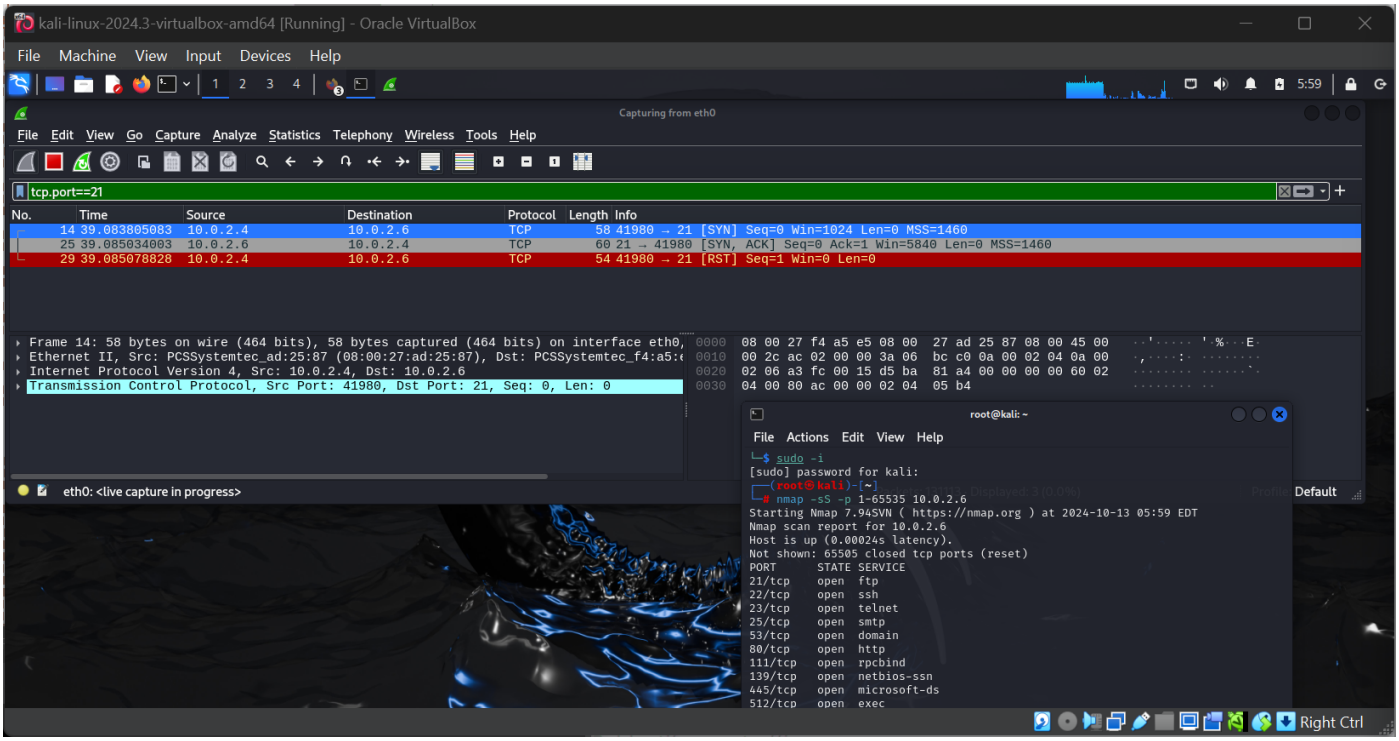


- What traffic was sent? If you rerun this scan with other TCP connection options like **-sS** or **-ST**, does this change?

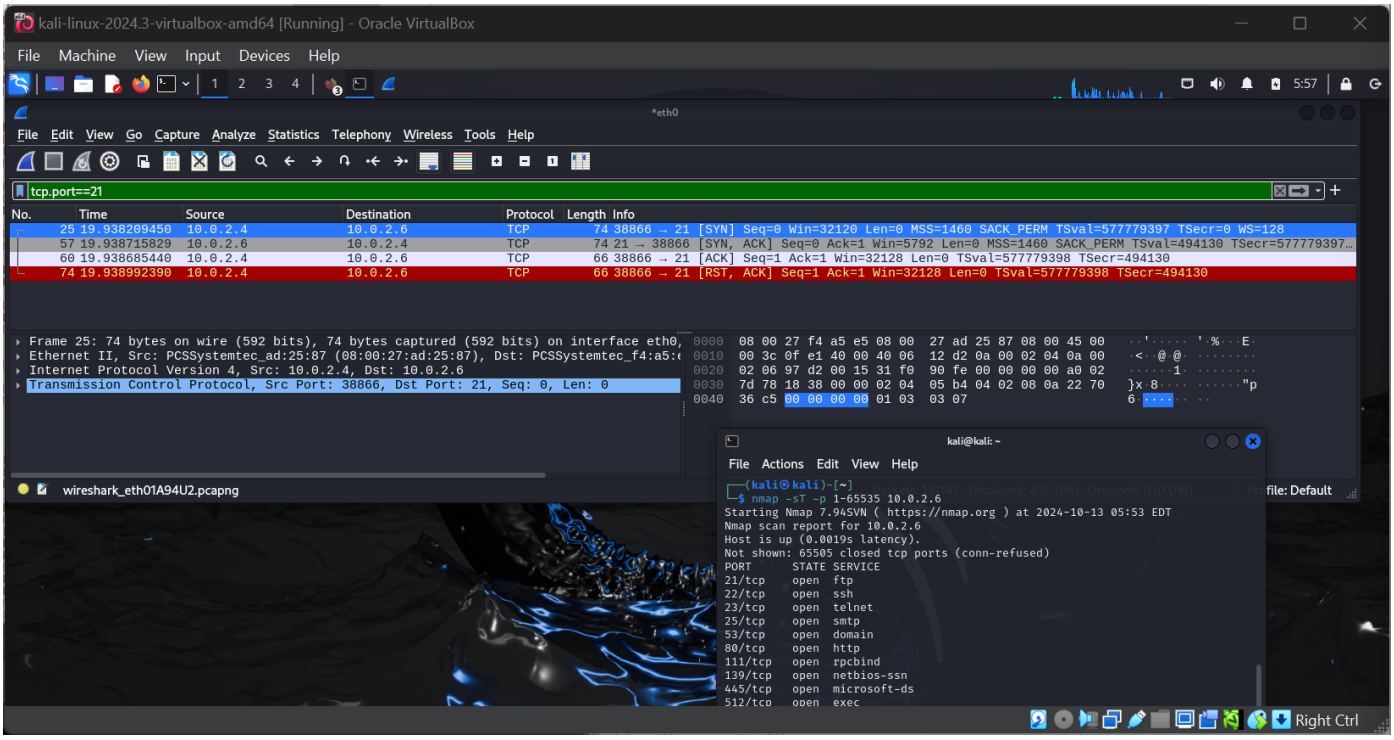
Ans.

The traffic sent was SYN-ACK packets.

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



While -sT performs a full TCP handshake.



- 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.