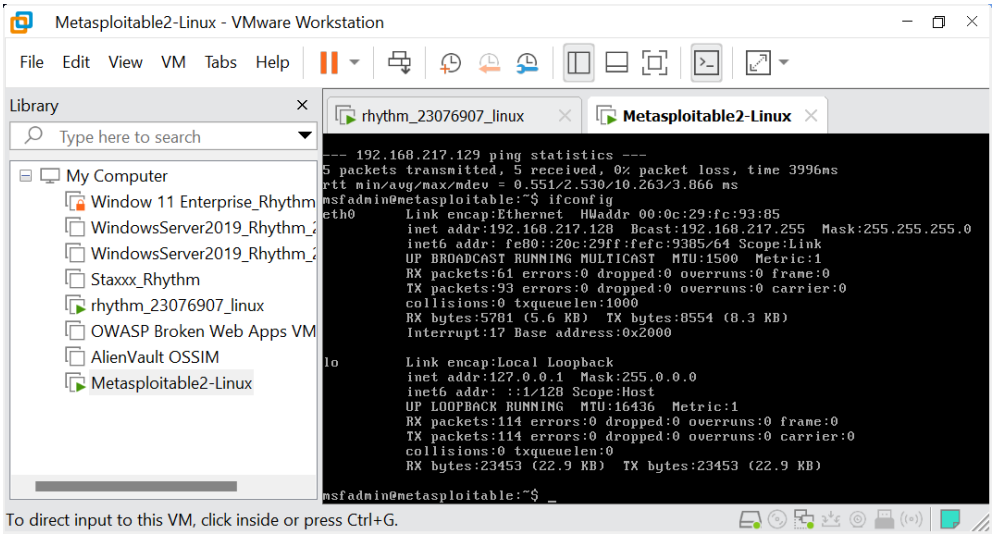
Activity 1: Scanning a Network (VirtualBox)

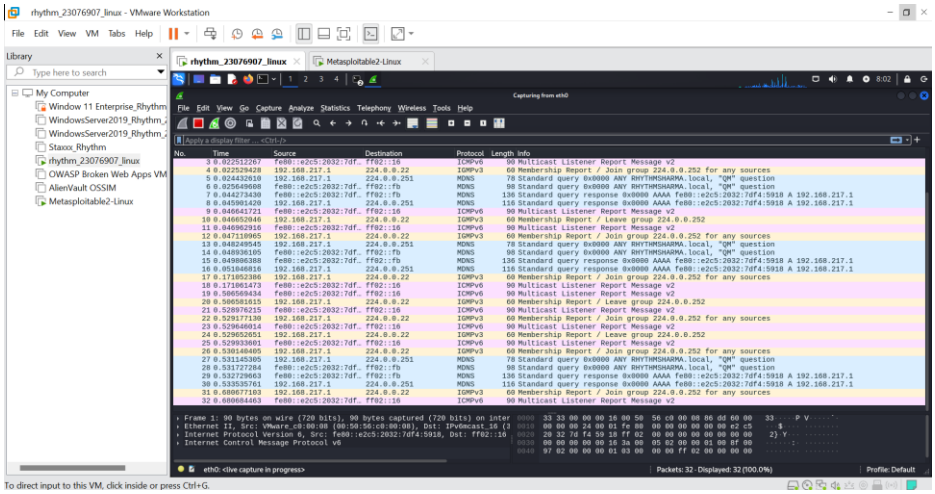
In this lab, you will use Wireshark to identify a network scan of a Linux system.

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.)**

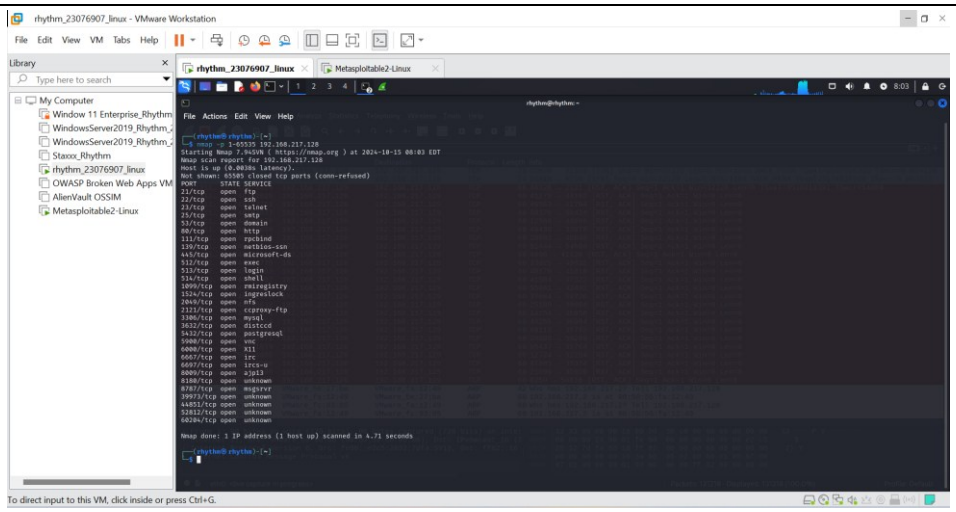


Part 2: Perform a network scan and visit the web server.

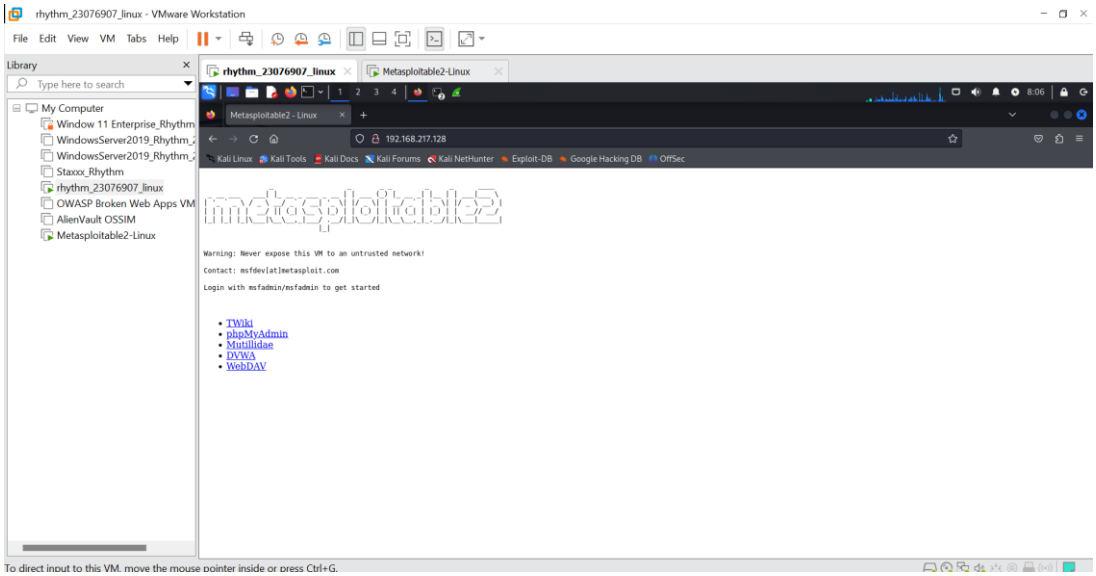
- From the terminal, execute the following command:

  nmap -p 1-65535 [*ip address of the Metasploitable machine*]

  Record one of the ports listed as open. **Take the screenshot.**

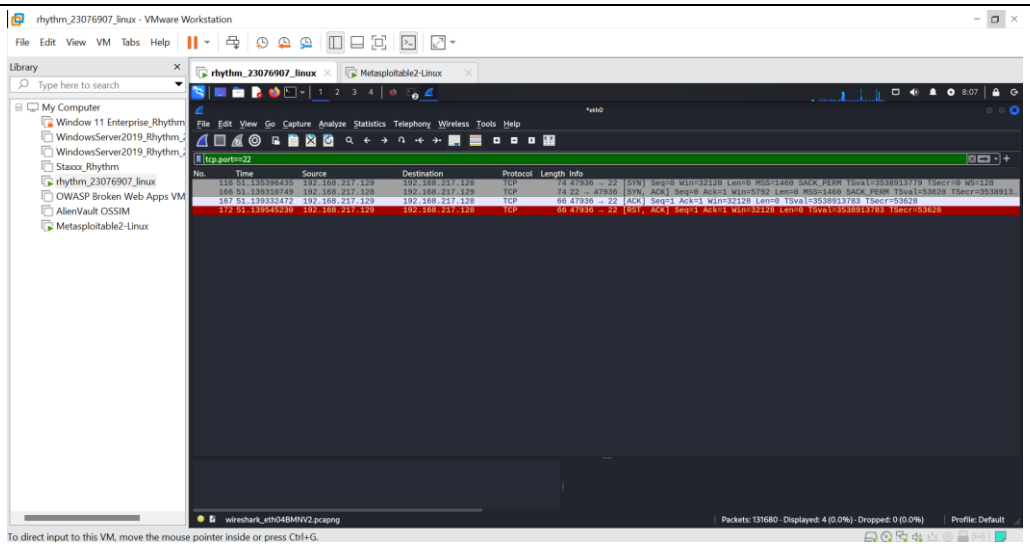


- Start the **IceWeasel/firefox** browser in Kali and navigate to the IP address of the Metasploitable system.



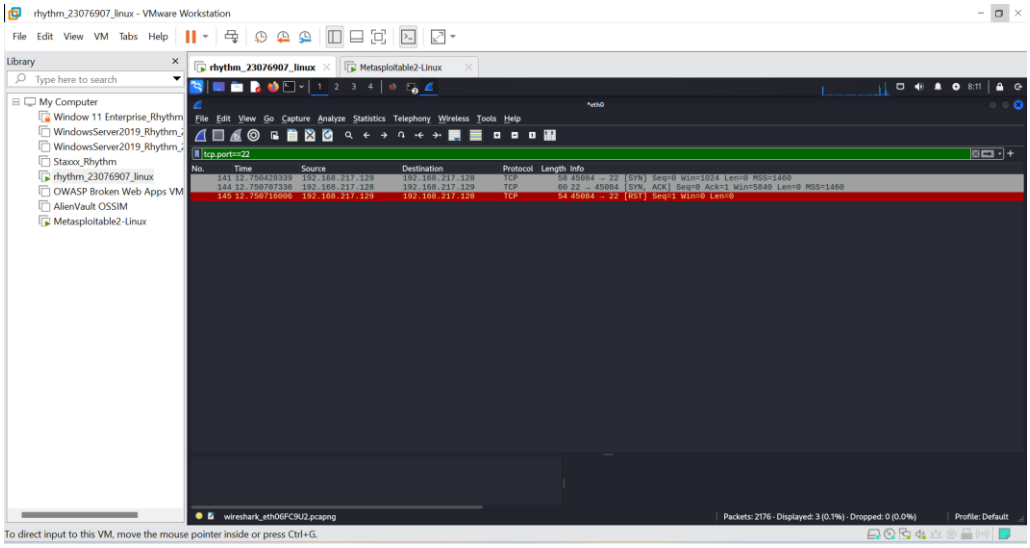
Part 3: Identify scan traffic.

- 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 Filter box.

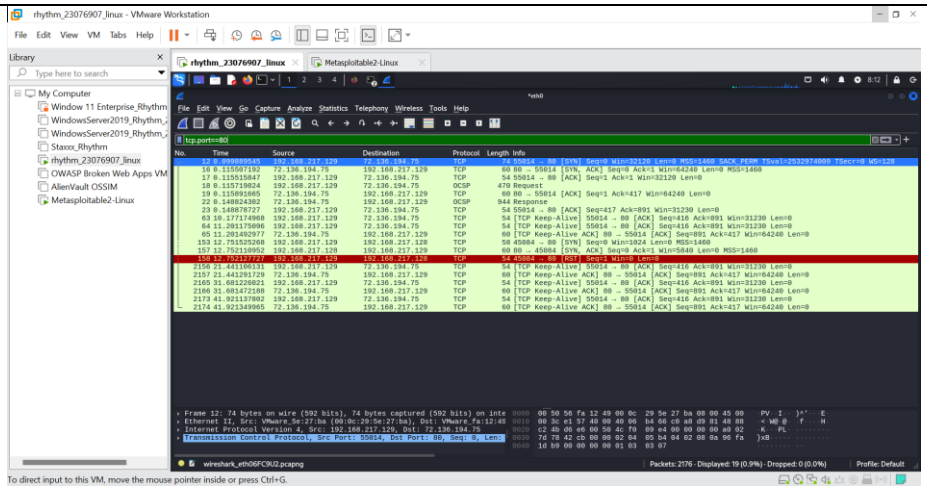


(Take the screenshot.)

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



- 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?



- To analyze your response to Part 2, review federation-aware incident response policies like https://spaces.at.internet2.edu/display/TI/TI.100.1 and www.btaa.org/docs/default-source/technology/federated_security_incident_response.pdf
  It tells what possible security incident we have like here only we have different port which are open and can be vulnerable for an organization where attacker can take advantage of these ports and enter into the server and machine.