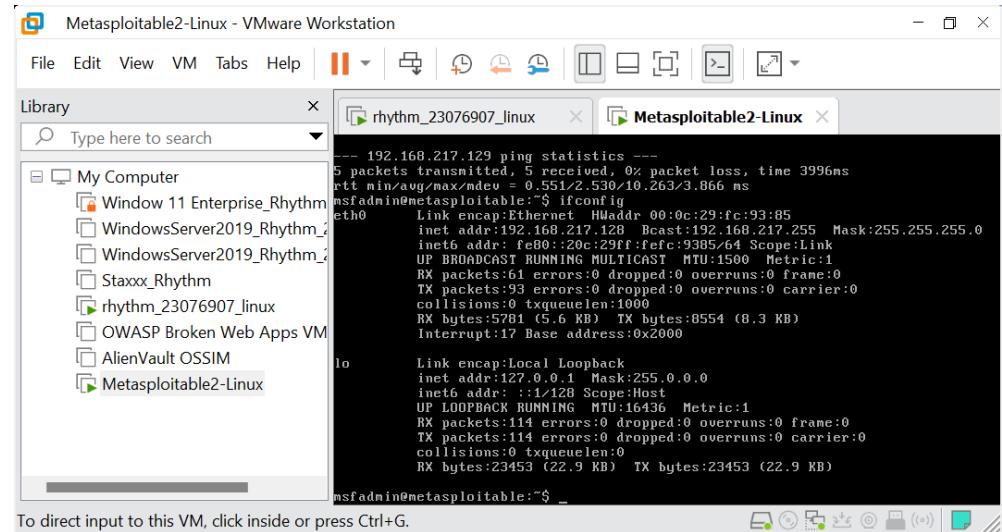


Activity 1: Scanning a Network (VirtualBox)

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

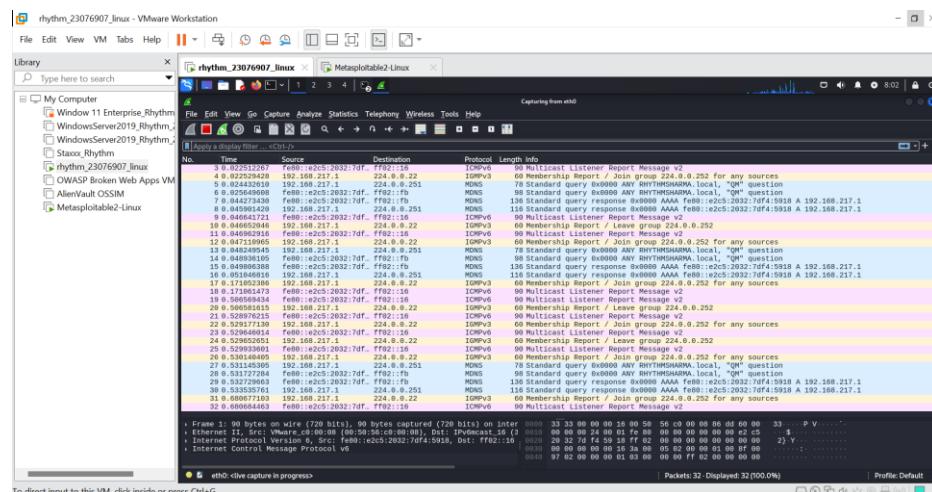
Part 1: Boot a Kali Linux system and a target system and set up the exercise.

- 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.**

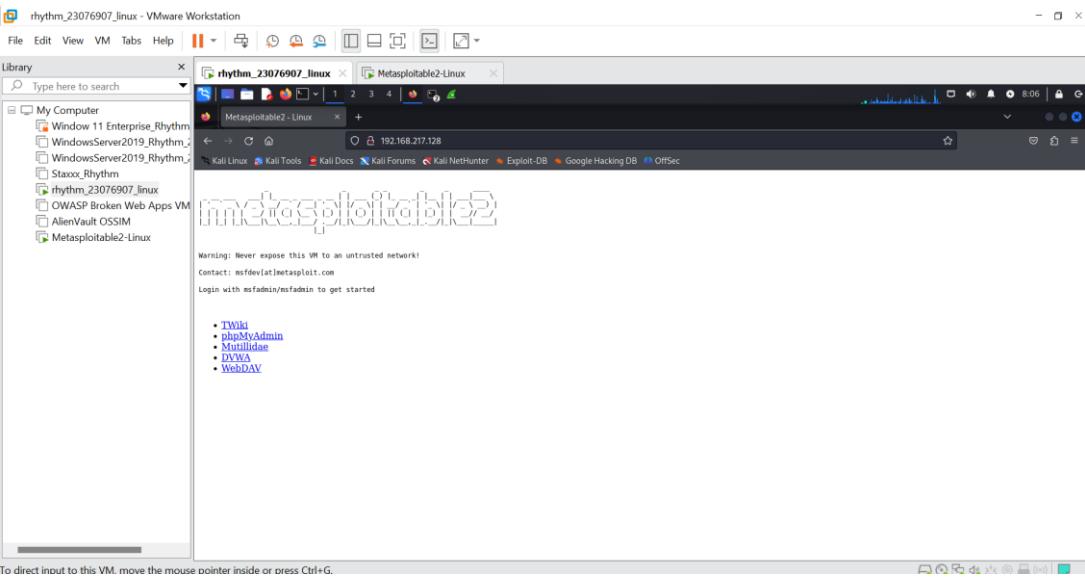
```

rhythm@rhythm:~$ nmap -sV 192.168.217.128
Nmap scan report for 192.168.217.128
Not shown: 65595 closed TCP ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
3306/tcp  open  mysql
80/tcp    open  http
80/tcp    open  https
113/tcp   open  redis
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1723/tcp  open  msrpc
5353/tcp  open  login
1900/tcp  open  msirenregistry
2232/tcp  open  msrmgrlock
2604/tcp  open  mrtg
2711/tcp  open  cisco-ftp
3389/tcp  open  msTerminalService
3632/tcp  open  distcd
1394/tcp  open  msftsgui
5900/tcp  open  vnc
4460/tcp  open  msftsgui
6667/tcp  open  irc
4455/tcp  open  msftsgui
5800/tcp  open  aej13
5800/tcp  open  msftsgui
3785/tcp  open  msftsgui
39973/tcp open  unknown
1523/tcp  open  msftsgui
32827/tcp open  unknown
40204/tcp open  unknown

Map done: 1 IP address (1 host up) scanned in 4.71 seconds

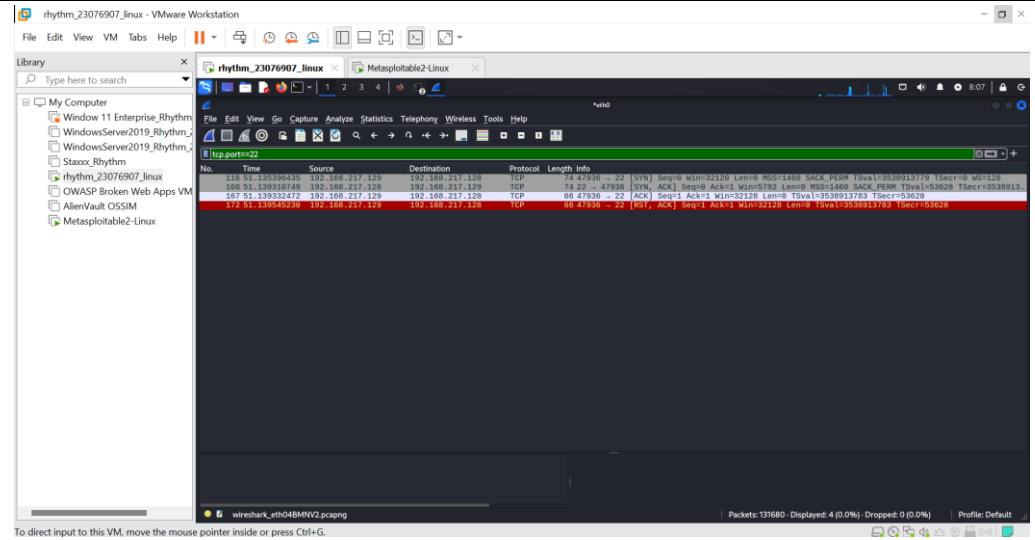
```

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



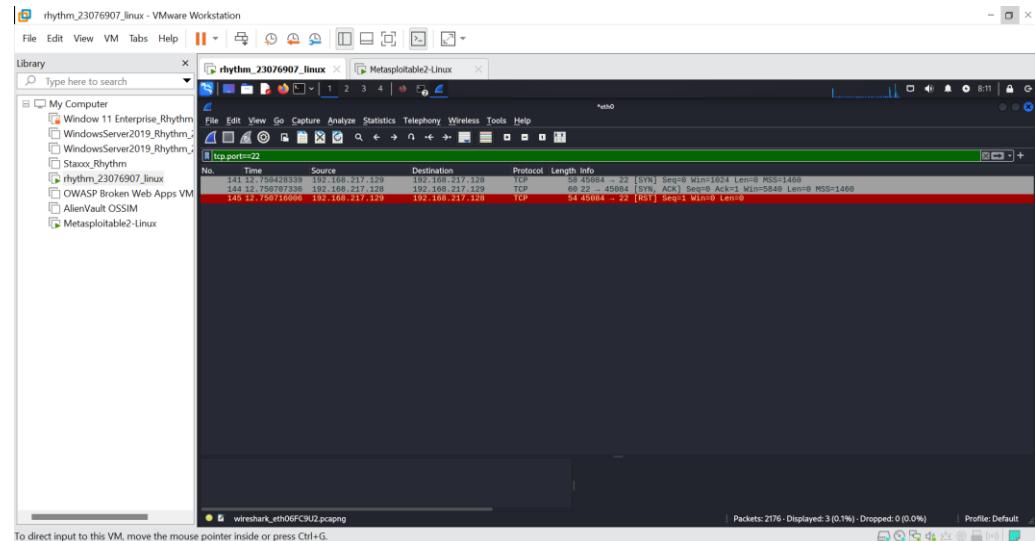
Part 3: Identify scan traffic.

- 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.

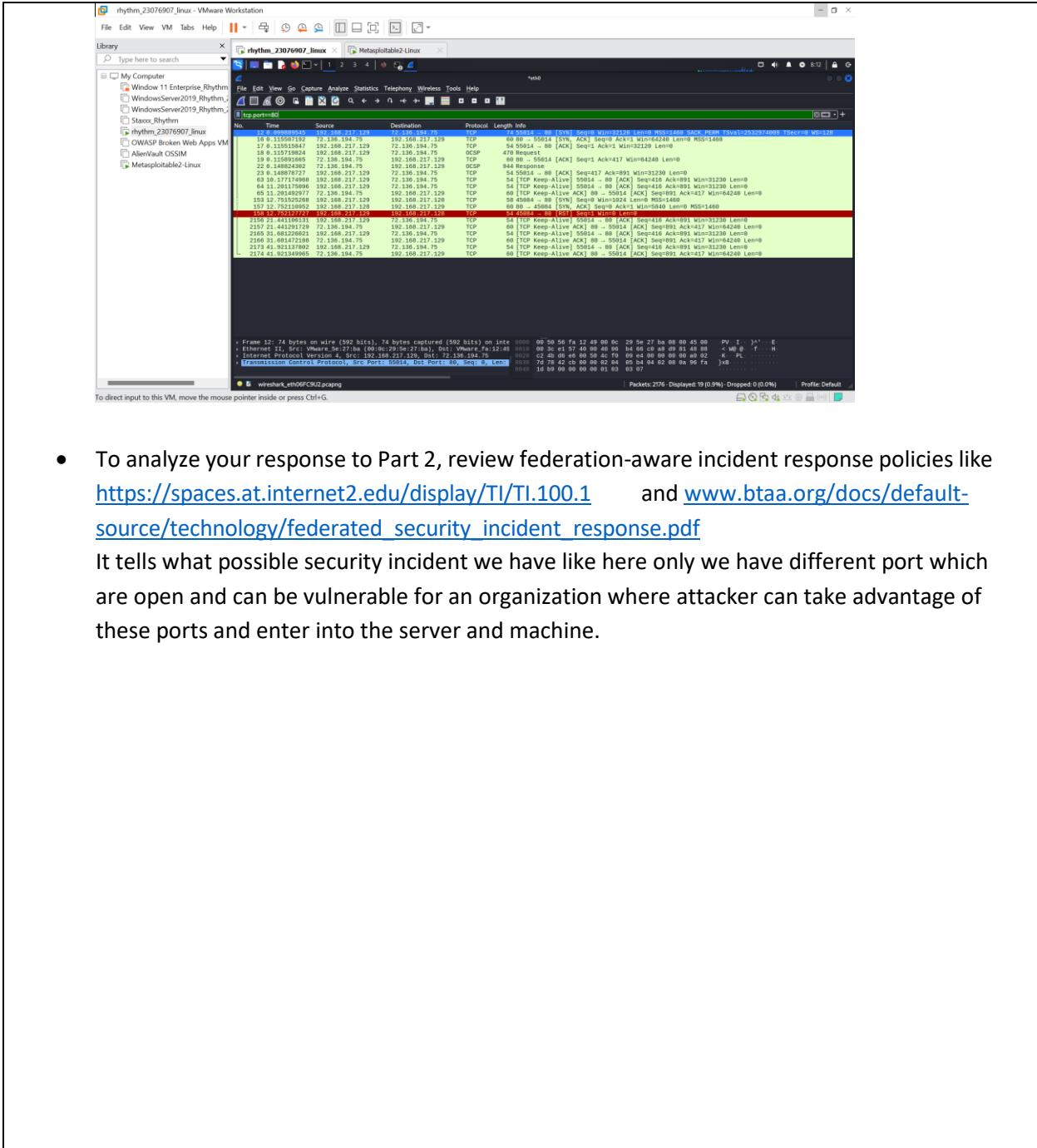


(Take the screenshot.)

- 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.