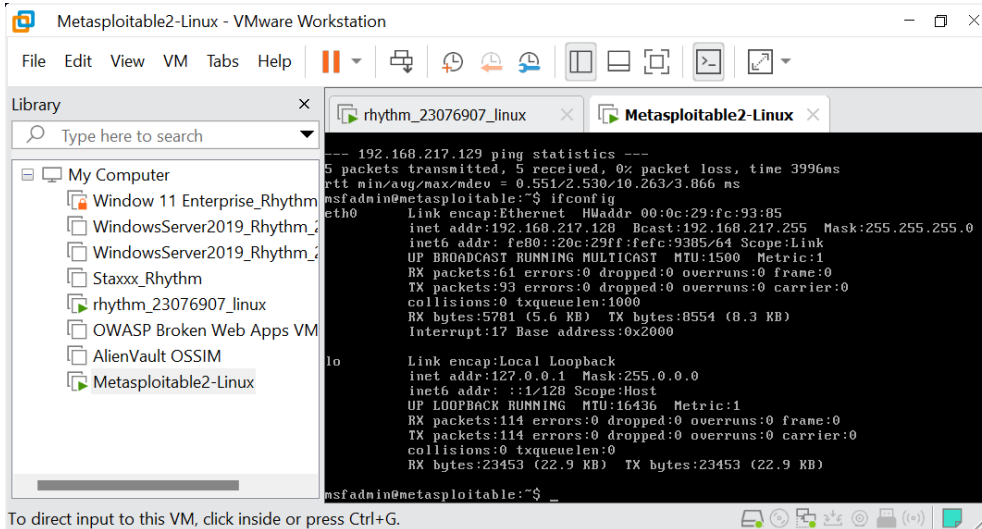


Activity 1: Scanning a Network (VirtualBox)

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.



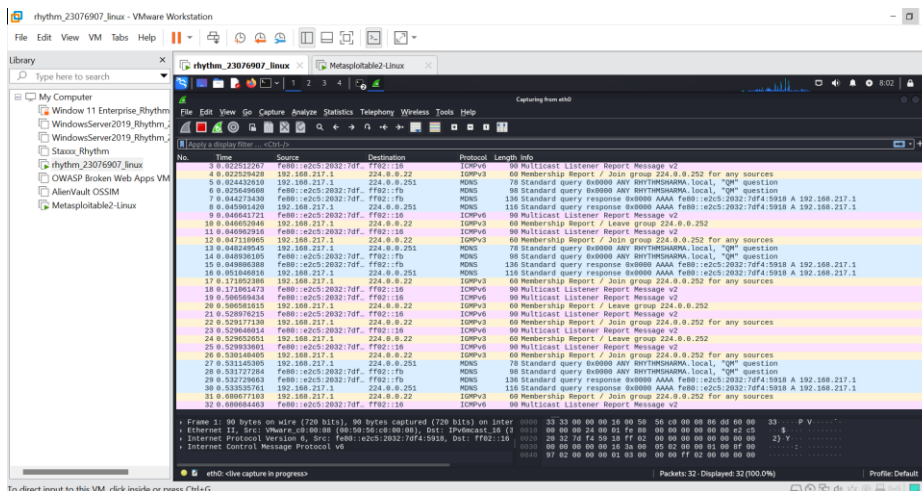
```
Metasploitable2-Linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Window 11 Enterprise_Rhythm
WindowsServer2019_Rhythm
WindowsServer2019_Rhythm
Staxxx_Rhythm
rhythm_23076907_linux
OWASP Broken Web Apps VM
AlienVault OSSIM
Metasploitable2-Linux
rhythm_23076907_linux x Metasploitable2-Linux x
--- 192.168.217.129 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3996ms
rtt min/avg/max/mdev = 0.551/2.530/10.263/3.866 ms
msfadmin@metasploitable:~$ ifconfig
eth0:
Link encap:Ethernet HWaddr 00:0c:29:fc:93:85
inet addr:192.168.217.128 Bcast:192.168.217.255 Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:fe9c:9385 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:61 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:5781 (5.6 KB) TX bytes:8554 (8.3 KB)
Interrupt:17 Base address:0x2000

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:114 errors:0 dropped:0 overruns:0 frame:0
TX packets:114 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:23453 (22.9 KB) TX bytes:23453 (22.9 KB)

msfadmin@metasploitable:~$
```

To direct input to this VM, click inside or press Ctrl+G.

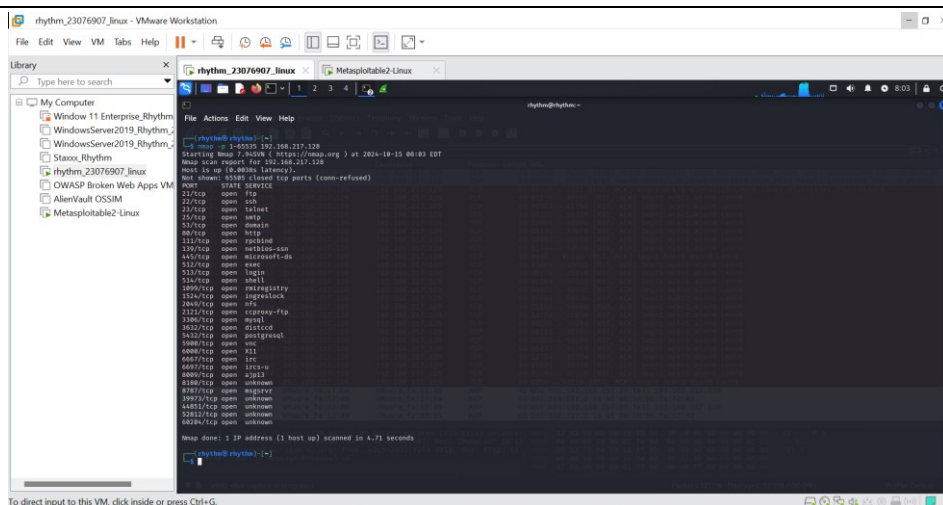
- Start the Wireshark capture. Select the eth0 interface and then choose **Capture > Start**. (Take the screenshot.)



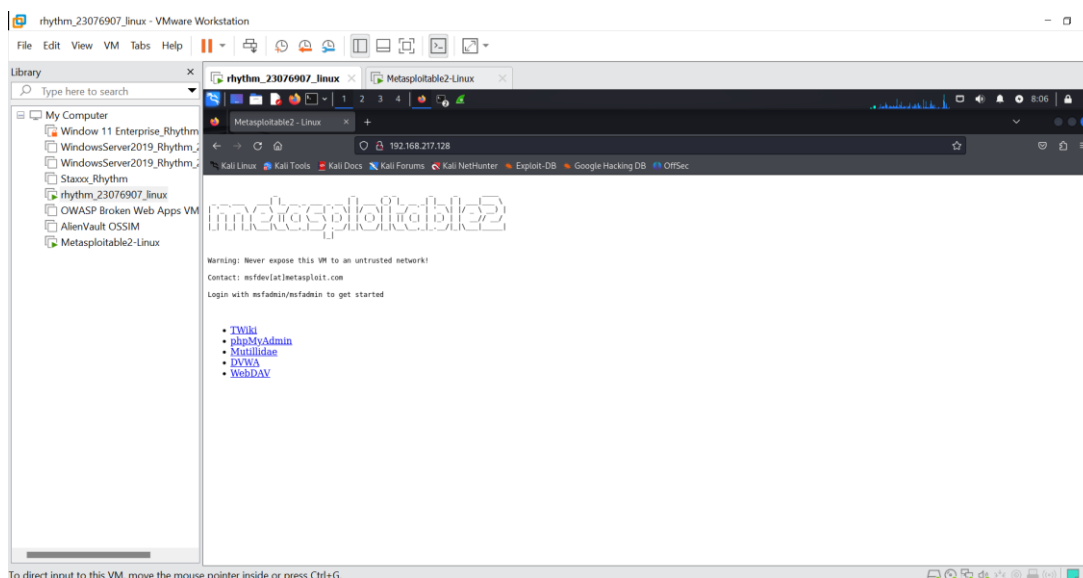
To direct input to this VM, click inside or press Ctrl+G.

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.**

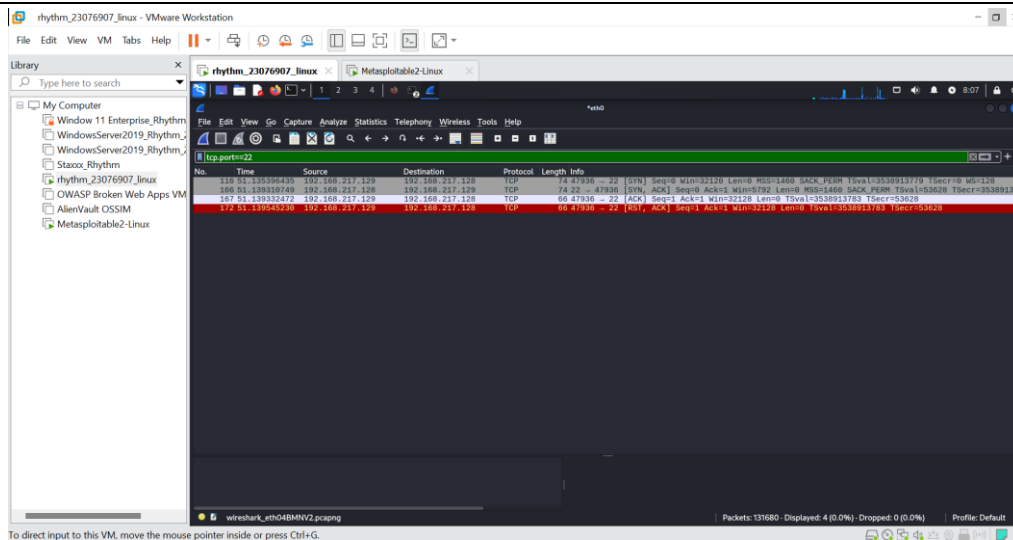


- Start the **IceWeasel/firefox** browser in Kali and navigate to the IP address of the Metasploitable system.



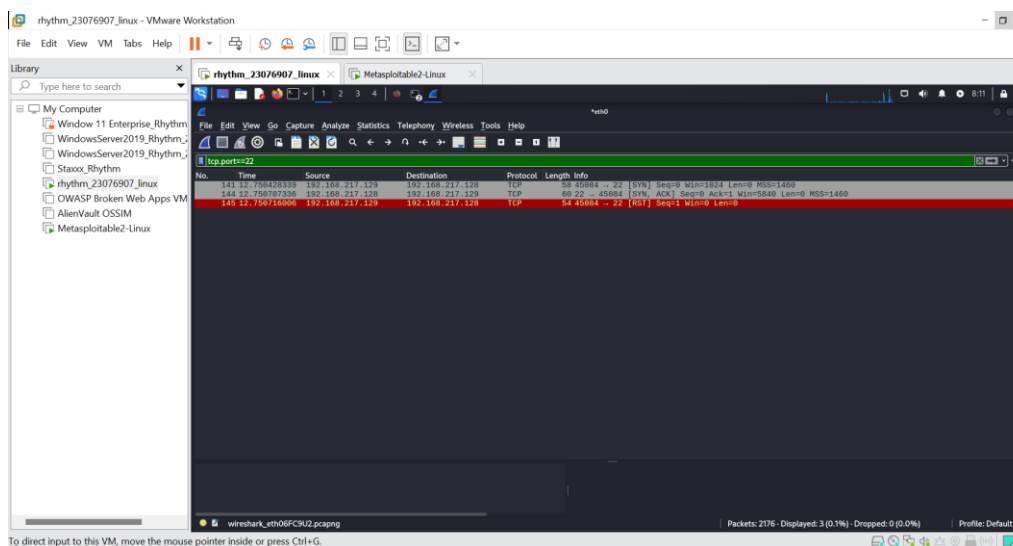
Part 3: Identify scan traffic.

- 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.

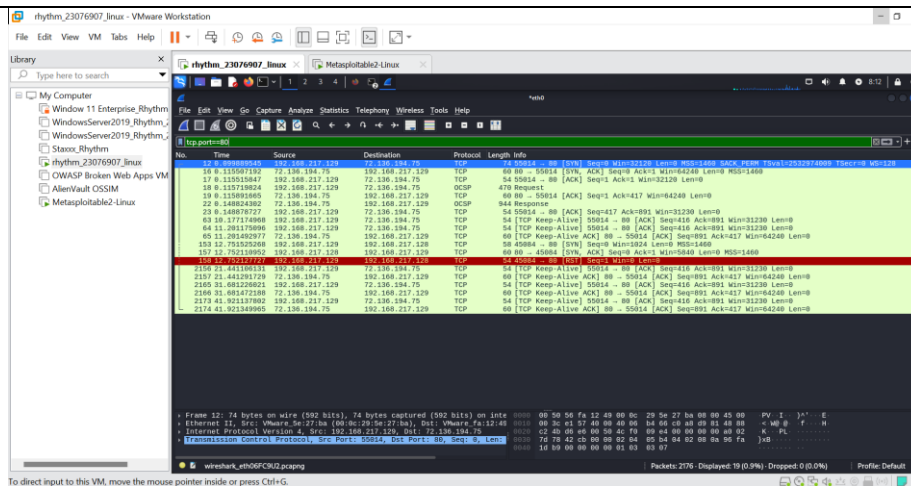


(Take the screenshot.)

- 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.