Old Dominion University

CYSE 301 Cybersecurity Techniques and Operations

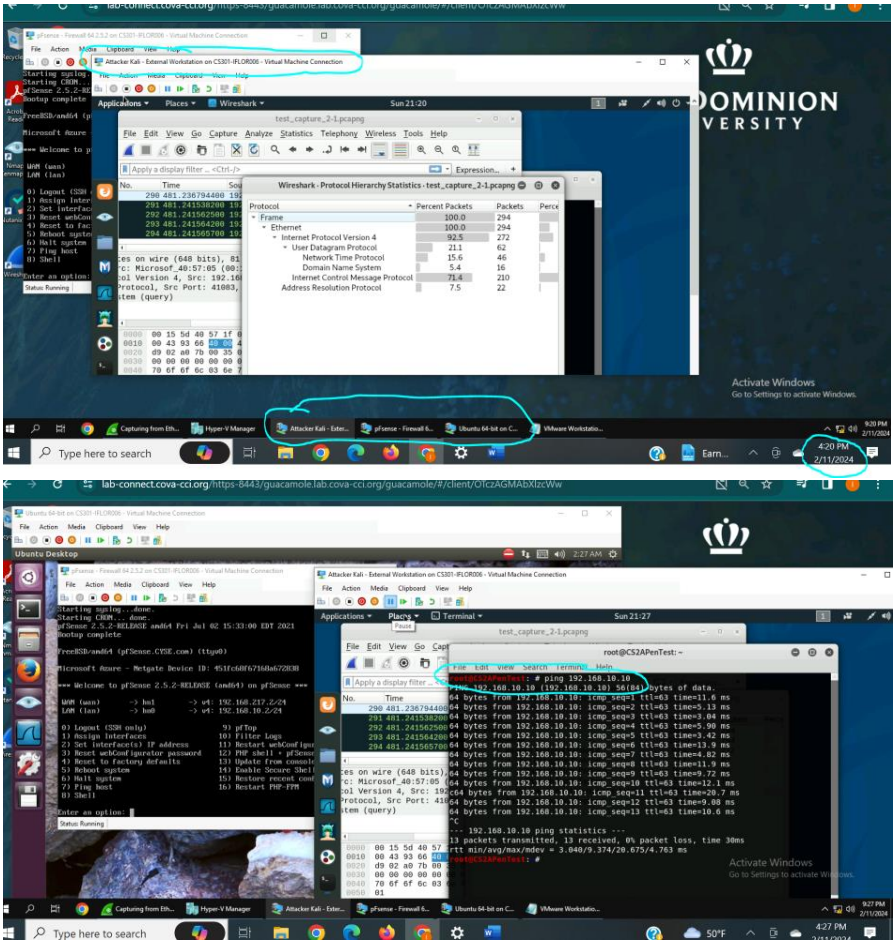
Assignment #2-1 Traffic Tracing and Sniffing

Isaac Flores

01270428

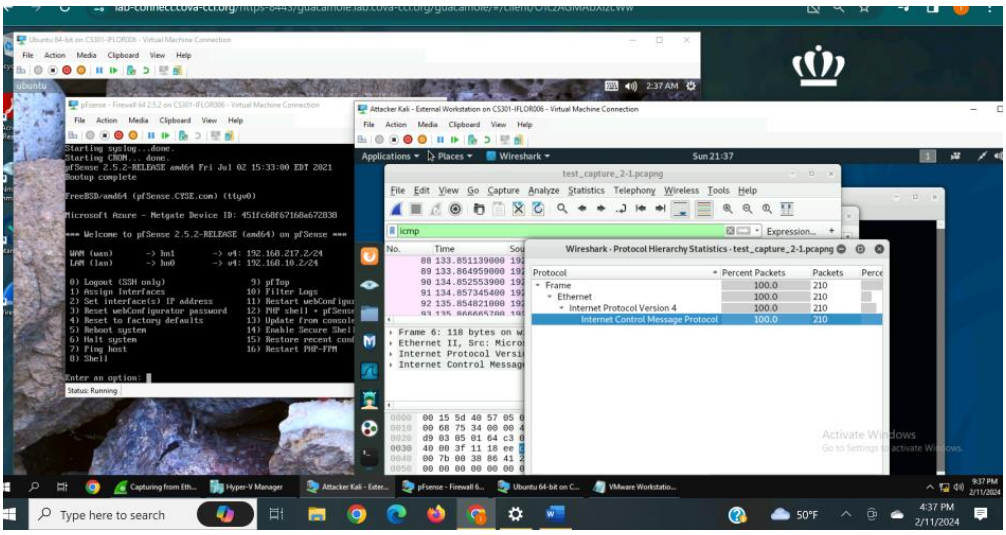
Task A

1. How many packets are captured in total? How many packets are displayed?



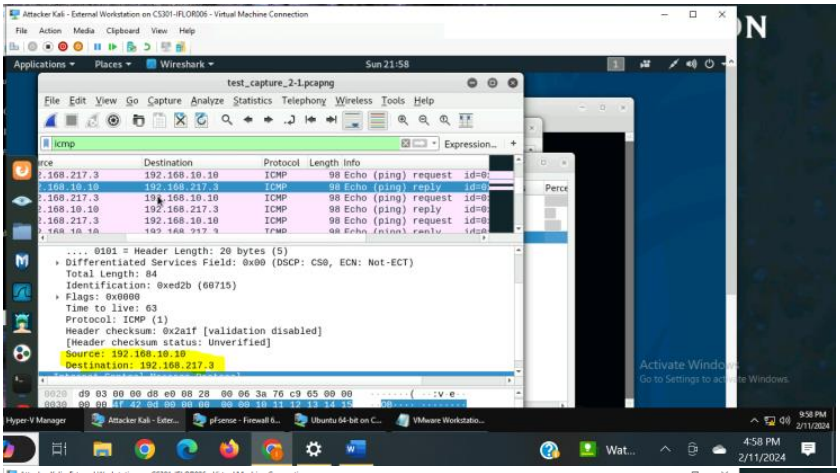
I powered on the Ubuntu, external kali, and pfsense virtual machines. I opened Wireshark in the external kali virtual machine and also opened a terminal where the ping command was used to ping the Ubuntu virtual machine Ip address. I navigated back to Wireshark to stop capturing and saved the Wireshark file. I used the statistics protocol hierarchy to check for number of packets. Thirteen packets were shown in the terminal while 294 packets were shown in Wireshark.

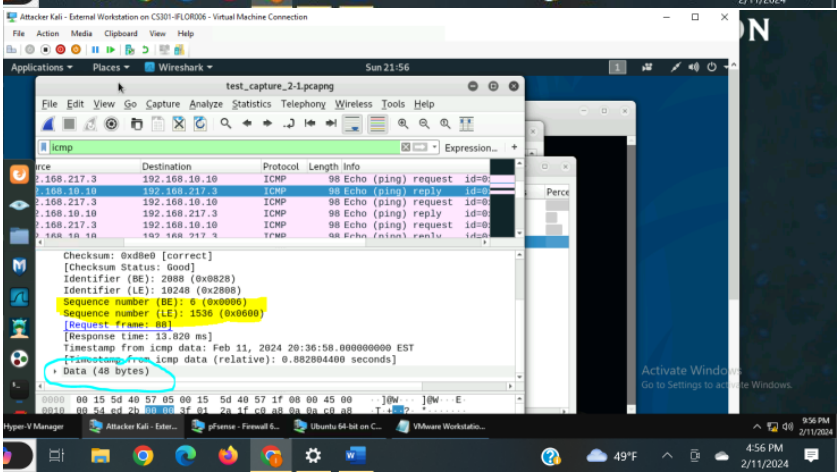
2. Apply “ICMP” as a display filter in Wireshark. Then repeat the previous question (Q1).

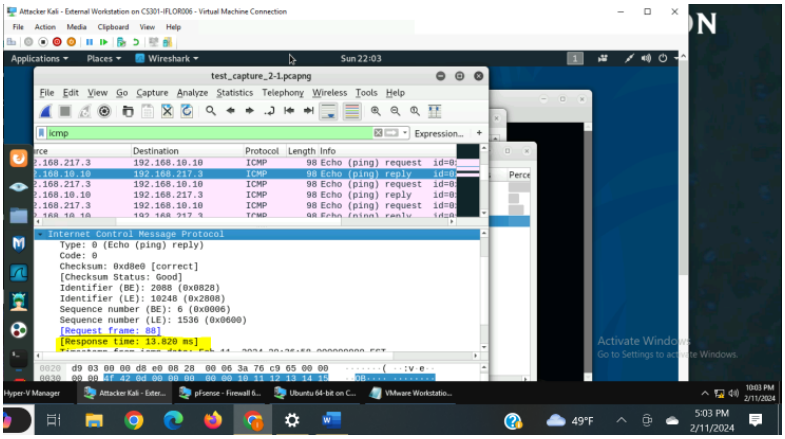


I clicked Internet Control Message Protocol in the hierarchy statistics where it was displayed that the number of packets was 210.

3. Select an Echo (replay) message from the list. What are the source and destination IPs of this packet? What are the sequence number and the size of the data? What is the response time?

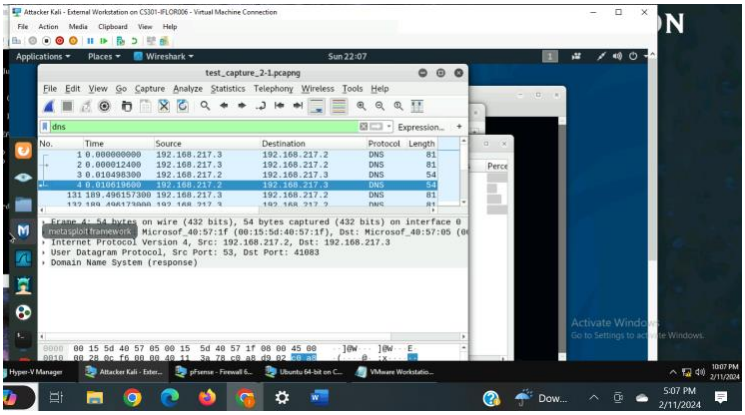
4. 





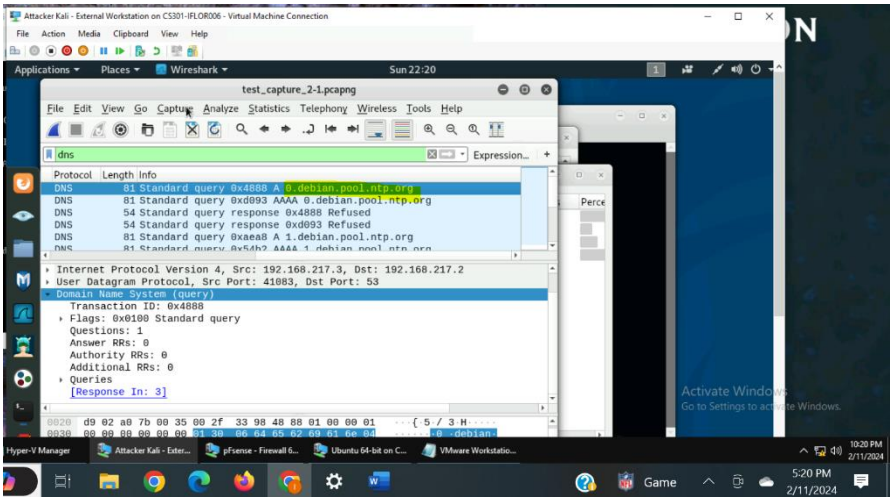
I clicked on an echo reply packet. I used the Internet Protocol Version 4 tab to view the destination and source Ip address. I used the Internet Control Message Protocol tab to view that the response time was 13.820 ms. I used the Internet Control Message Protocol tab to find the sequence number to be big endian 6 and little endian 1536. I viewed the data tab to find that the data size is 48 bytes.

5. (Question 4 not 5) Apply “DNS” as a display filter in Wireshark. How many packets are displayed?

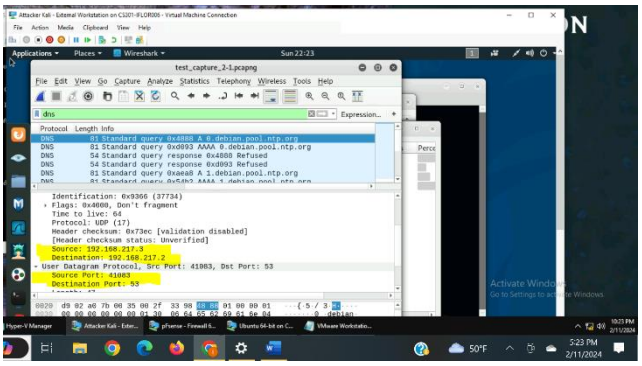


I typed DNS in the filter text box and pressed enter. The output was 16 DNS packets.

6. (Question 5 not 6) Find a DNS query packet. What is the domain name this host is trying to resolve? What is the source IP and port number, destination IP and port number? Please express in the format: IP:port.

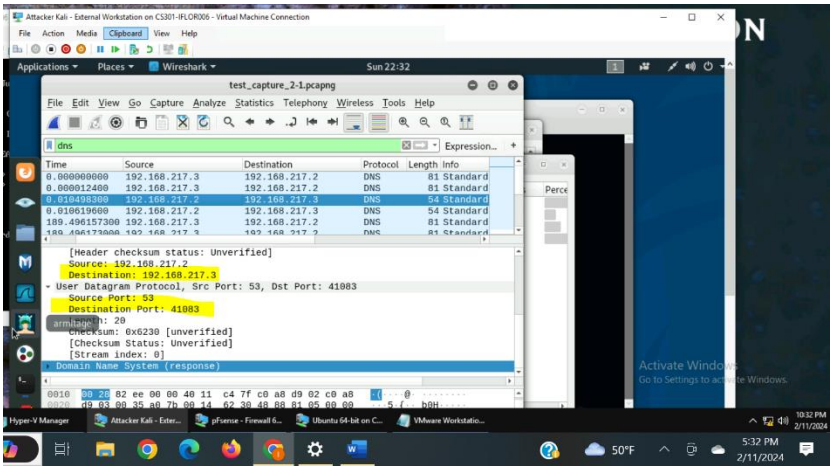


I checked the DNS query packet to see that the domain name is 0.debian.pool.ntp.org.

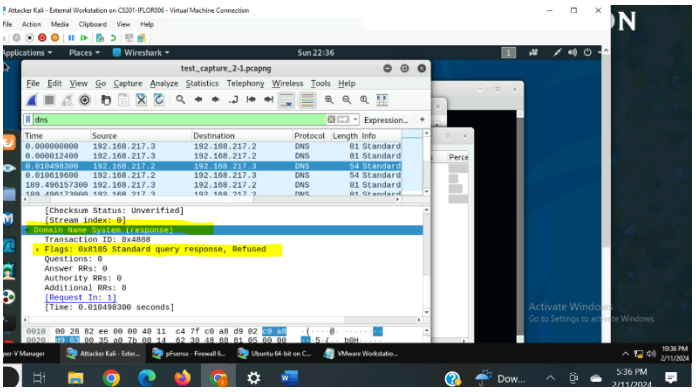


I used the Internet Protocol Version 4 tab to find the Ip address. I used the User Datagram Protocol to find the source and destination port numbers. Source Ip 192.168.217.3: source port 41083. Destination Ip address 192.168.217.2: destination port 53.

7. (Question 6 not 7) Find the corresponding DNS response to the query you selected at the previous step, and what is the source IP and port number, destination IP and port number? What is the message replied from the DNS server?



I clicked on the packet response form the destination Ip address. I used the Internet Protocol Version 4 and the User Datagram protocol tab to find the port numbers. Source Ip address 192.168.217.2: source port number 53. Destination Ip address 192.168.217.3: destination port number 41083.



I used the Domain Name System tab to find the response which was refused.