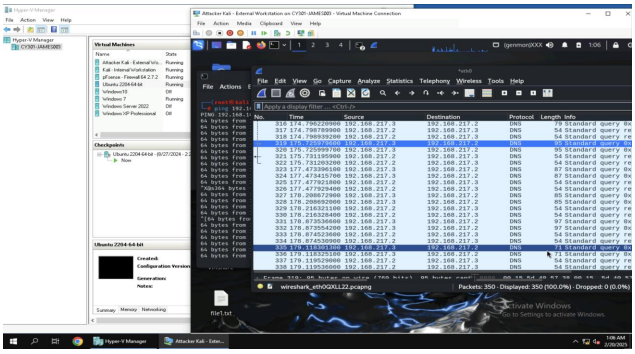
OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #2 Traffic Tracing and Analysis

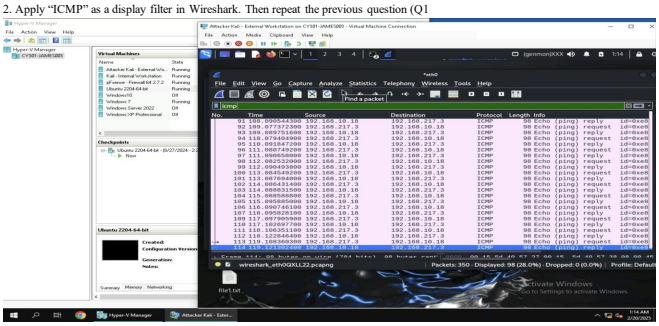
February 19, 2025

Dr. Shabha Vasta



There were 350 packets displayed and captured for this step. I completed this step by making sure virtual machines were running including Wireshark. Using the command in Kali Linux External. While using the odu,edu website (that didnt load but expected it not to). After some seconds I stopped the capture on Wireshark and ended up with 350 packets in the amount of 3 minutes tops.

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

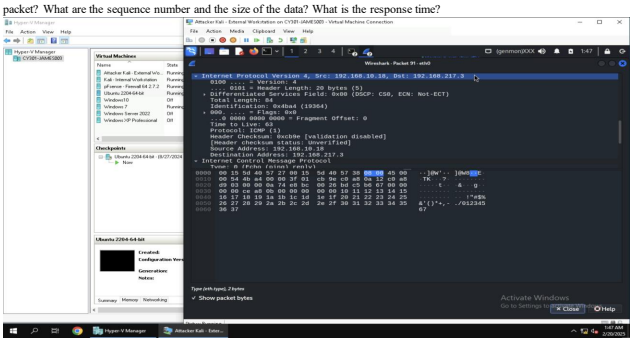


After completely question 2 using "ICMP" in the Wireshark display filter and looking through the packets there is now 350 packets captures and only 98 Displayed.

TASK A

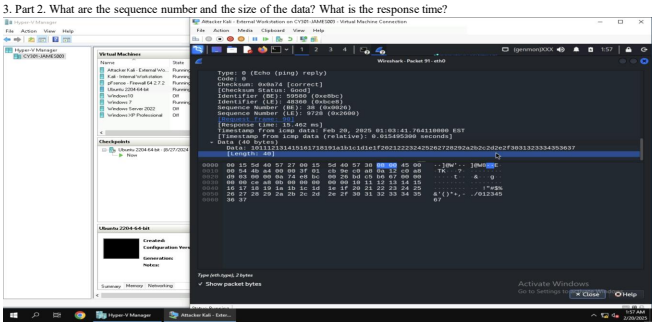
1. How many packets are captured in total? How many packets are displayed?

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?



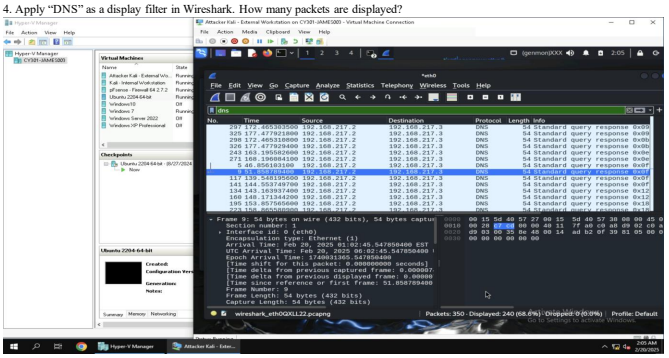
Picking the Echo (replay) packet 91 and looking into the Internet Protocol drop down we can see the Source IP is 192.168.10.18 and Destination IP as 192.168.217.3

3. Part 2. What are the sequence number and the size of the data? What is the response time?



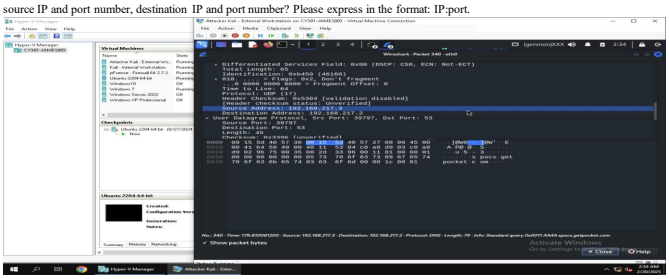
Scrolling down we the Sequence (BE): 38 and Sequence (LE): 9728. When I drop down the Data bar, we see that the size/length of this data is 40 bytes and a time stamp of 0.015495300 seconds.

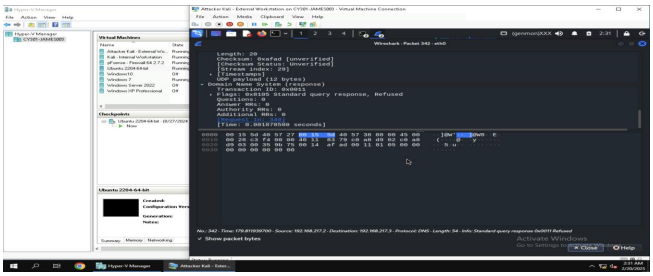
4. Apply "DNS" as a display filter in Wireshark. How many packets are displayed?



When inserting DNS in the display filter in Wireshark there is 350 packets captured and 240 displayed under Domain Service Name.

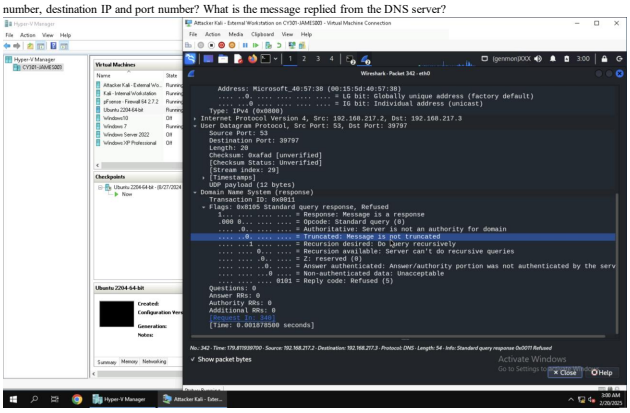
5. Find a DNS query packet. What is the domain name this host is trying to resolve? What is the source IP and port number, destination IP and port number? Please express in the format: IP:port.





With using port 340 to find the answer to the domain dame query I had to find the answer in port 342 the Standard Query refused. The source IP: 192.168.217.2, Port Number: 39797. Destination IP: 192.168.217.3, Port Number: 53.

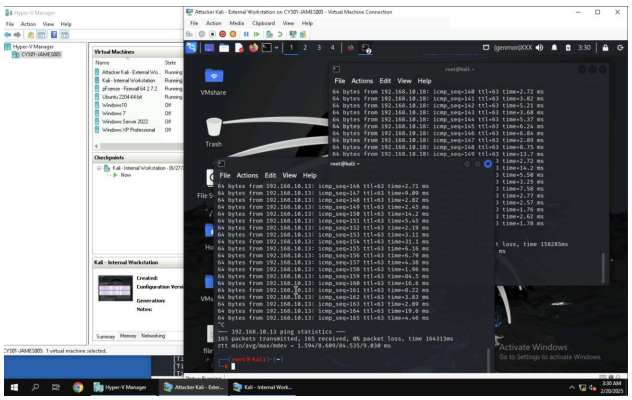
6. Find the corresponding DNS response to the query you selected at the previous step, and what is the source IP and port number, destination IP and port number? What is the message replied from the DNS server?



Going to the corresponding DNS response and scrolled down a bit we see in the screenshot Source IP: 192.168.217.2, Port Number: 53. Destination IP: 192.168.217.3, Port Number: 39797 and message as " A message is a response"

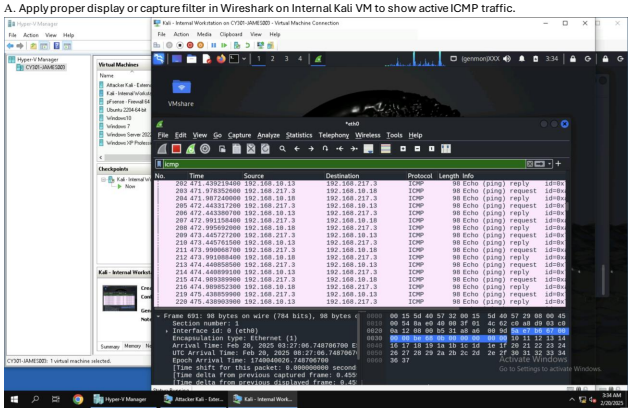
TASK B

1. Please turn on Attacker/External Kali, internal kali, pfsense, and Ubuntu
   Open two terminals on External Kali VM. Use one ping Ubuntu VM, and use the other ping Internal Kali.



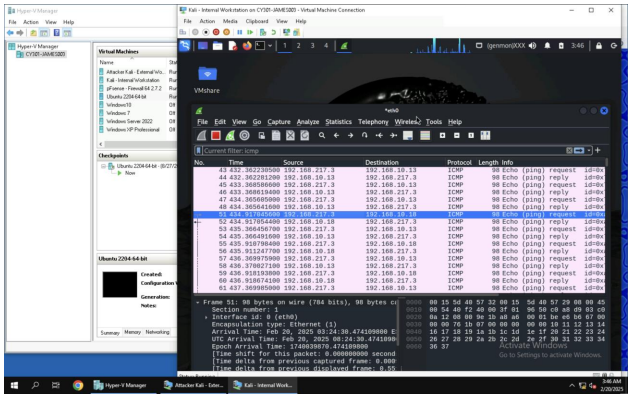
To make sure all virtual machines were active I pinged both Ubuntu & Internal Kali for about a minute while making sure wire shark and pfsense were running in the background. This is all done after editing the settings on the mirrors.

A. Apply proper display or capture filter in Wireshark on Internal Kali VM to show active ICMP traffic.



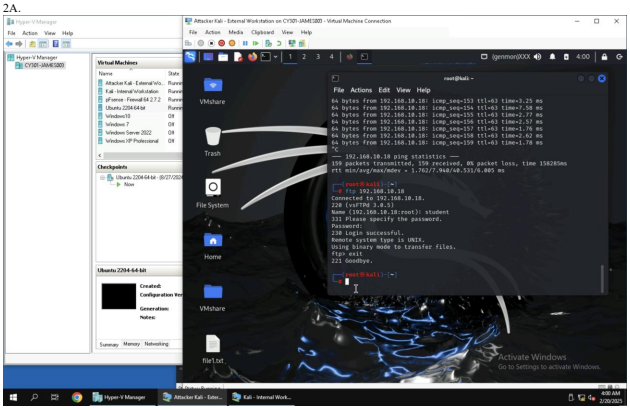
Using the ICMP display filter on Internal Kali we see all the 648 displayed packets in traffic.

B. Apply a proper display or capture filter on the internal Kahli VM that ONLY displays the ICMP request that originated from the external Kali VM and goes to the Ubuntu 64-bit VM.



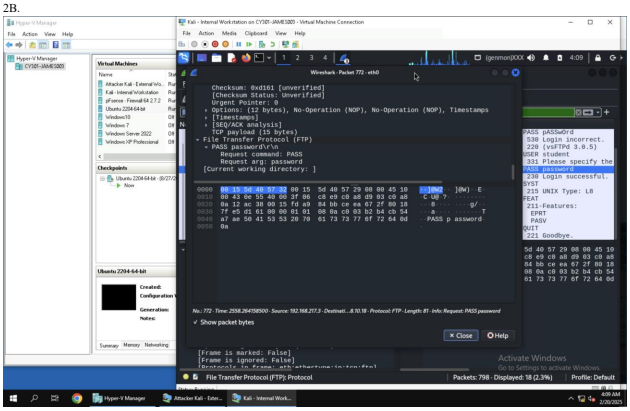
To find this request I matched up the first original request with the source IP address including the Destination IP address which are highlighted above.

2A.



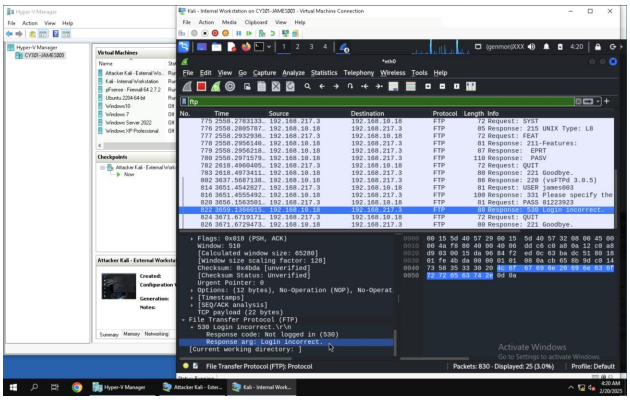
Using the ftp command and the IP address, inserting the username and password I was able to successfully log in and exit.

2B.



To find out how the External Kali had Intenal Kali password was to match the source IP address in FTP display filter. There you can see all my activities including my password to get into student.

2C.



After trying my MIDAS as usernam and UIN as password my login failed but we were able to see through Internal Kali packets where this actively happened. I highlighted at the bottom the "login incorrect".