OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #2: Traffic Tracing and Sniffing

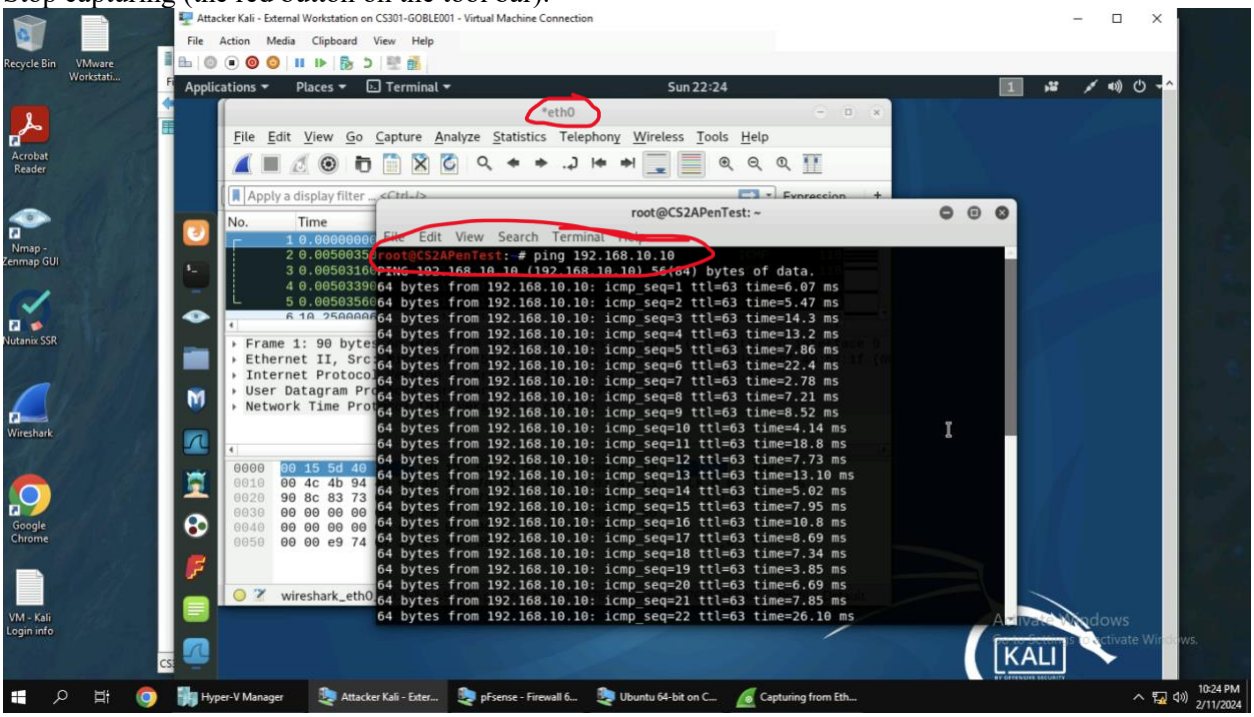
Giancarlo Oblena

01230538

TASK A – GET STARTED WITH WIRESHARK

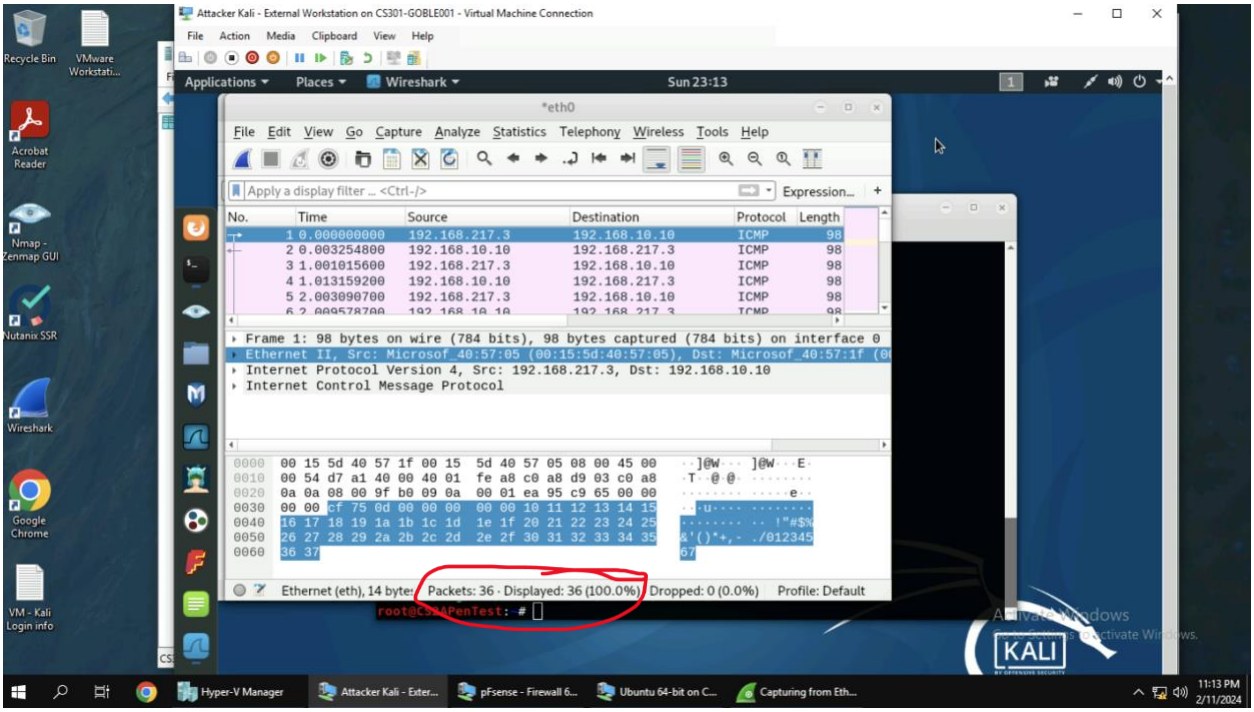
MY CLOCK IN THE CCIA IS AHEAD BY 5 HOURS!

1. Open Wireshark on External Kali and listen on interface “eth0”.
2. Open a new terminal then ping Ubuntu VM for 5-10 seconds.
3. Stop capturing (the red button on the tool bar).



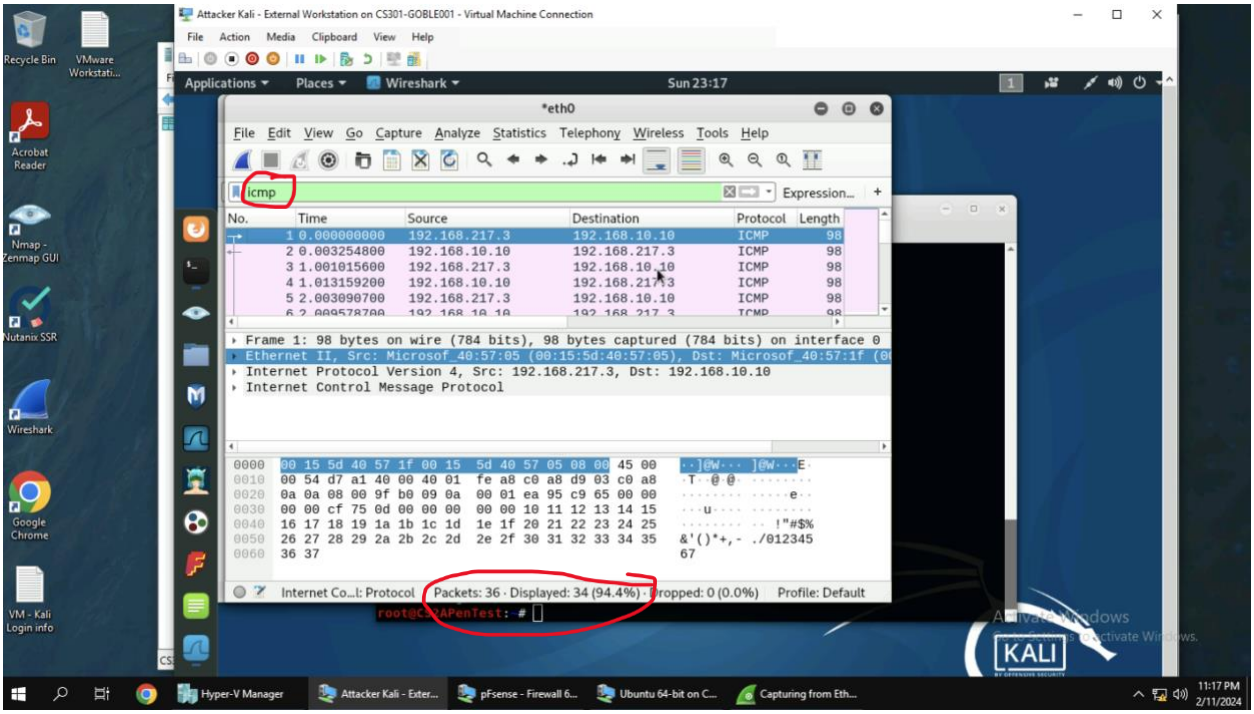
Used “ping 192.168.10.10” to Ubuntu VM

Q1. How many packets are captured in total? How many packets are displayed?



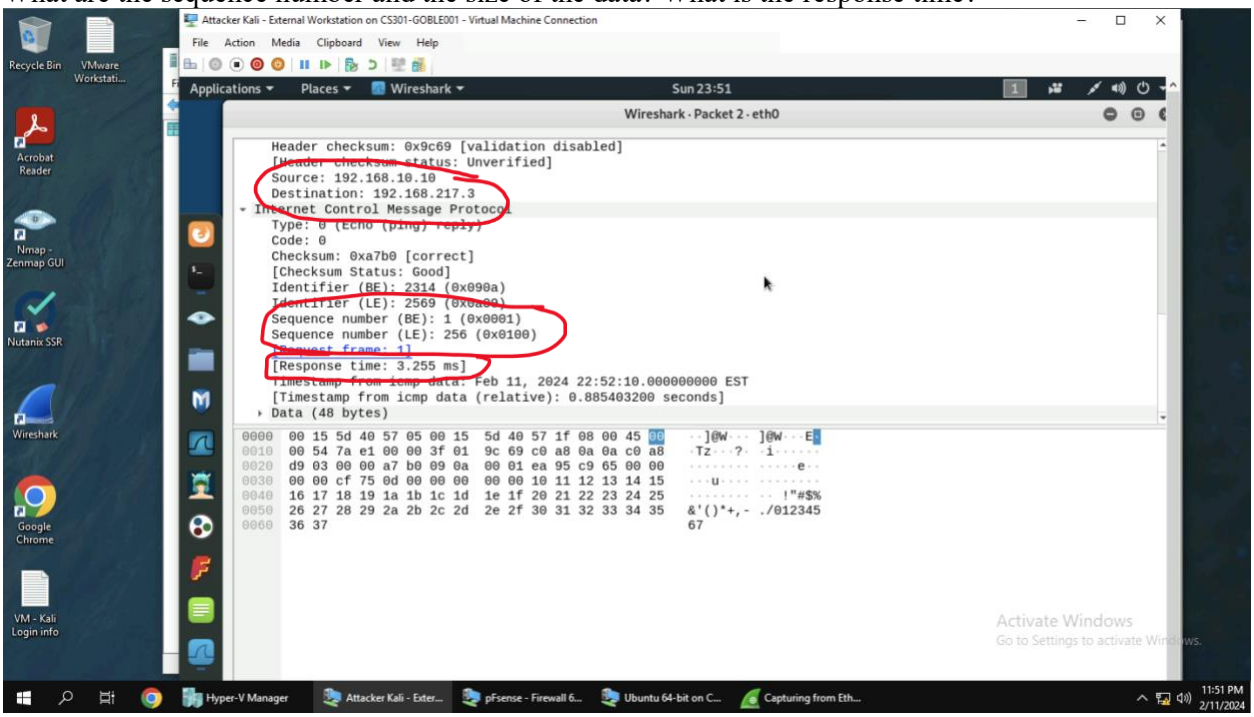
After a few seconds of capturing, 36 packets were captured, and 36 packets were displayed. This data is shown on the bottom of the Wireshark window.

Q2. Apply “ICMP” as a display filter in Wireshark. Then repeat the previous question (Q1).



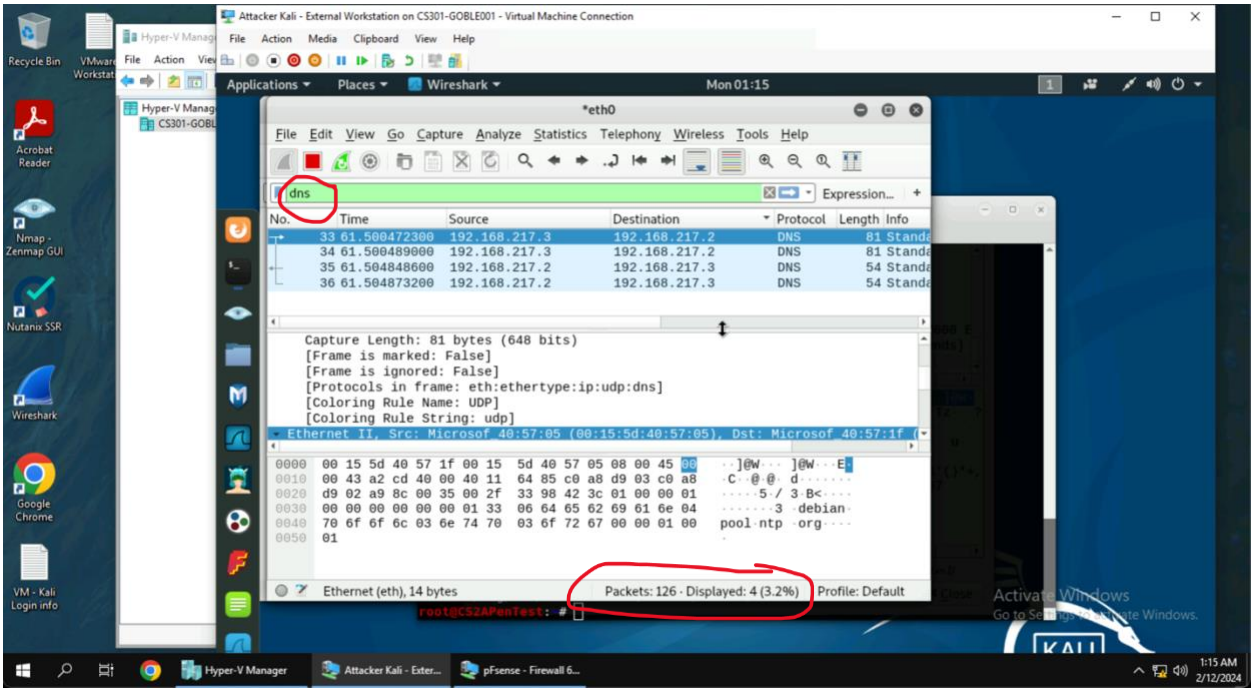
After inputting “icmp” in the display filter, 36 packets were captured, but only 34 were displayed as icmp.

Q3. 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?



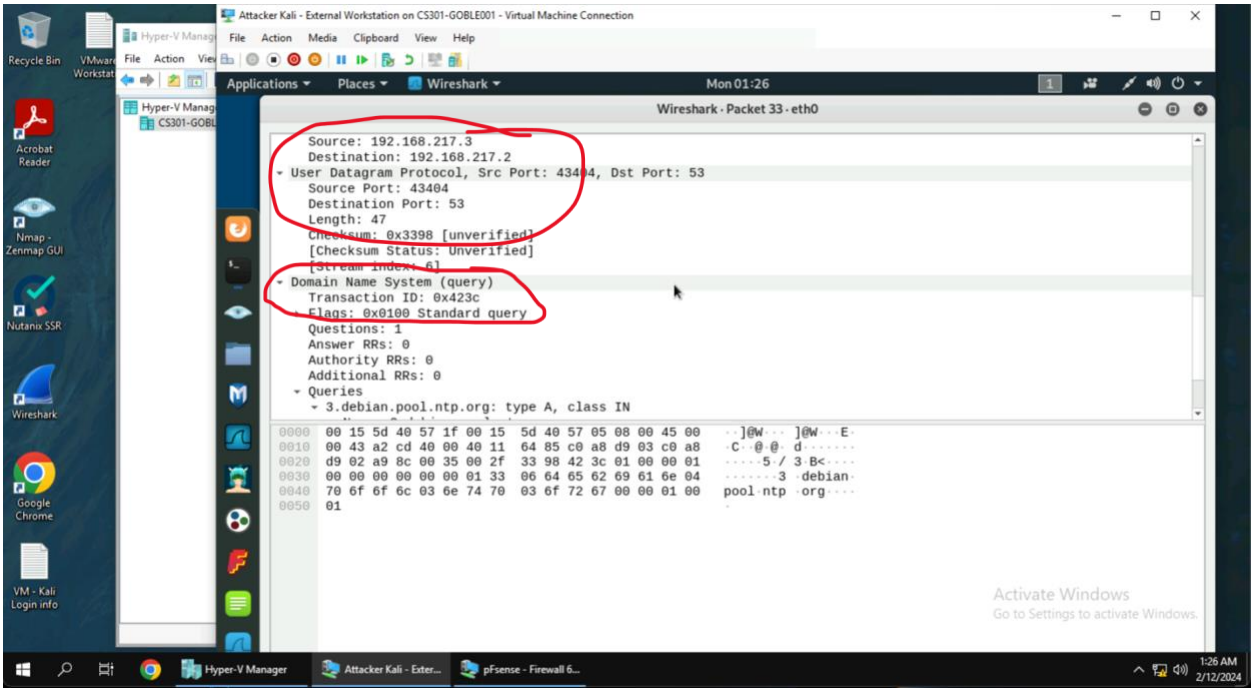
I chose packet 2, the source IP of this packet is 192.168.10.10. The destination IP address is 192.168.217.3. The sequence number BE is 1 and the sequence number LE is 256. The response time was 3.255 milliseconds.

Q4. Apply “DNS” as a display filter in Wireshark. How many packets are displayed?



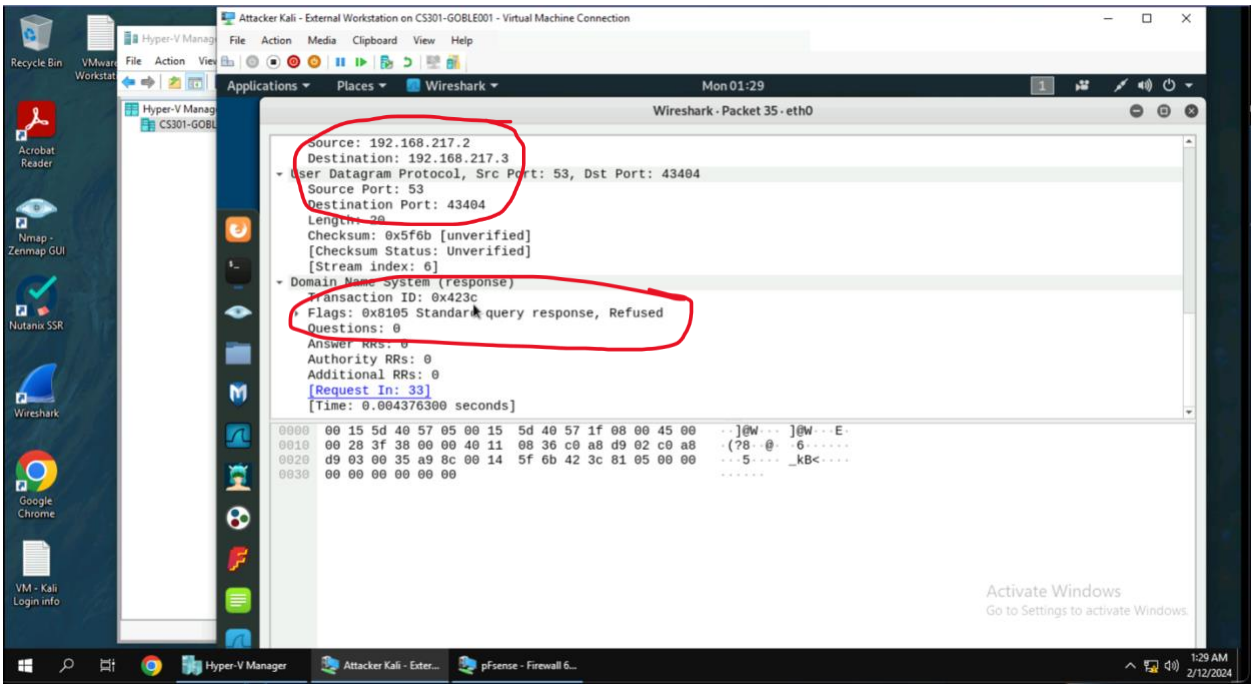
When “dns” was inputted in the display filter, 126 packets were captured, but only 4 of those were dns.

Q5. 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.



The domain system name (query) and the Transaction ID is 0x423c. The source IP and port is 192.168.217.3 : 43404. The destination IP and port number is 192.168.217.2 : 53.

Q6. 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?



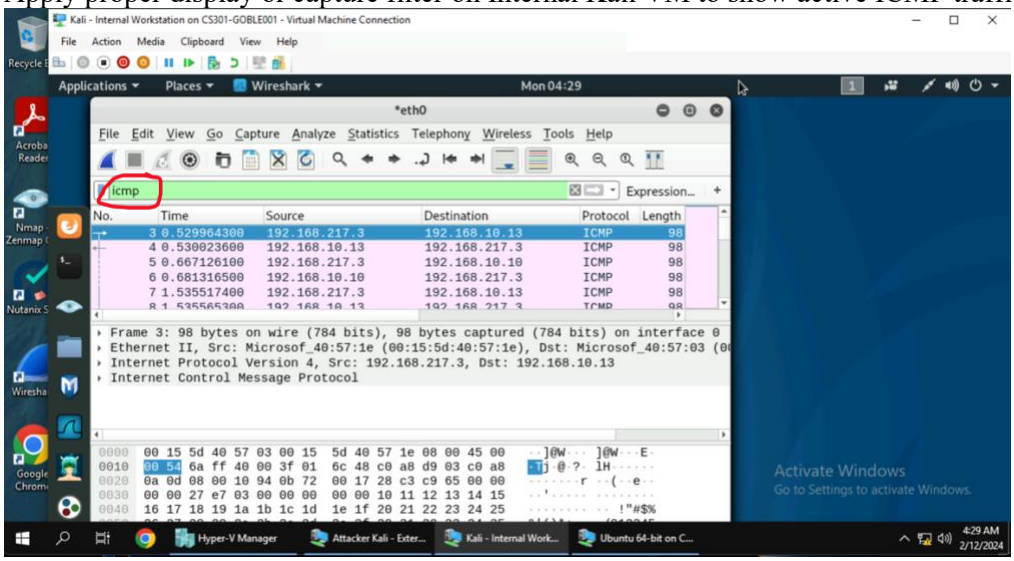
The source IP and port is 192.168.217.2 : 53 The destination IP and port number is 192.168.217.3 : 43404. The response from the DNS is, “Standard query response, Refused.” The authentication was not authenticated by the server and therefore unacceptable.

TASK B – SNIFF LAN TRAFFIC

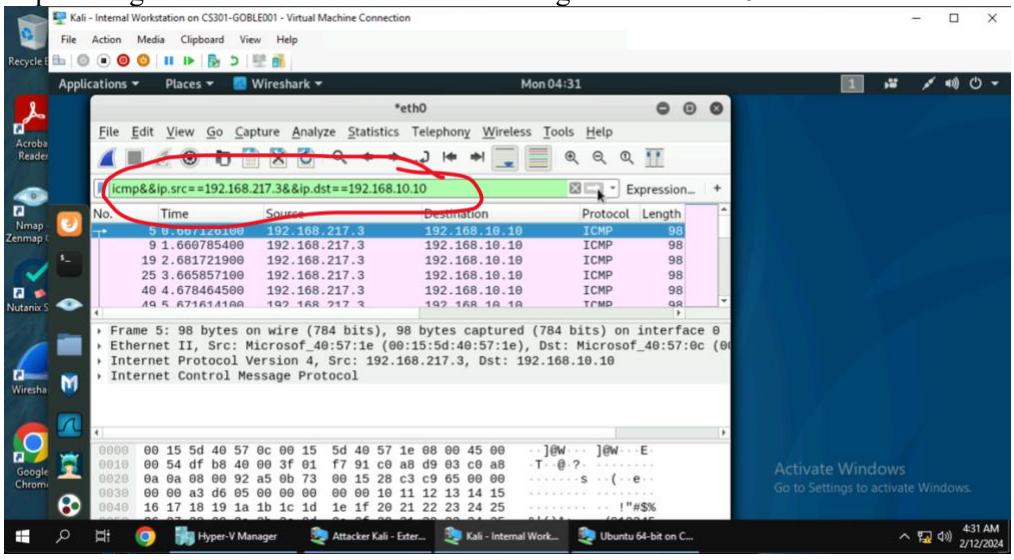
1. Sniff ICMP traffic:

   Open two terminals on External Kali VM. Use one ping Ubuntu VM, and use the other ping Internal Kali.
   To ping ubuntu I pinged 192.168.10.10 and to ping Internal Kali I pinged 192.168.217.3

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

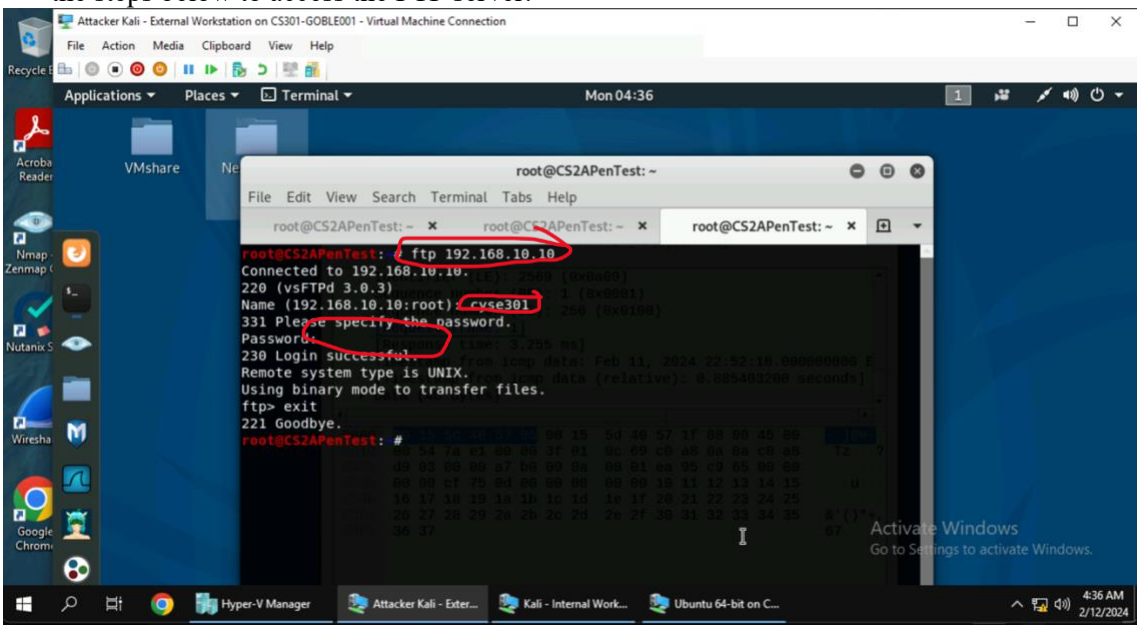


   b. Apply proper display or capture filter on Internal Kali VM that ONLY displays ICMP request originated from External Kali VM and goes to Ubuntu 64-bit VM.



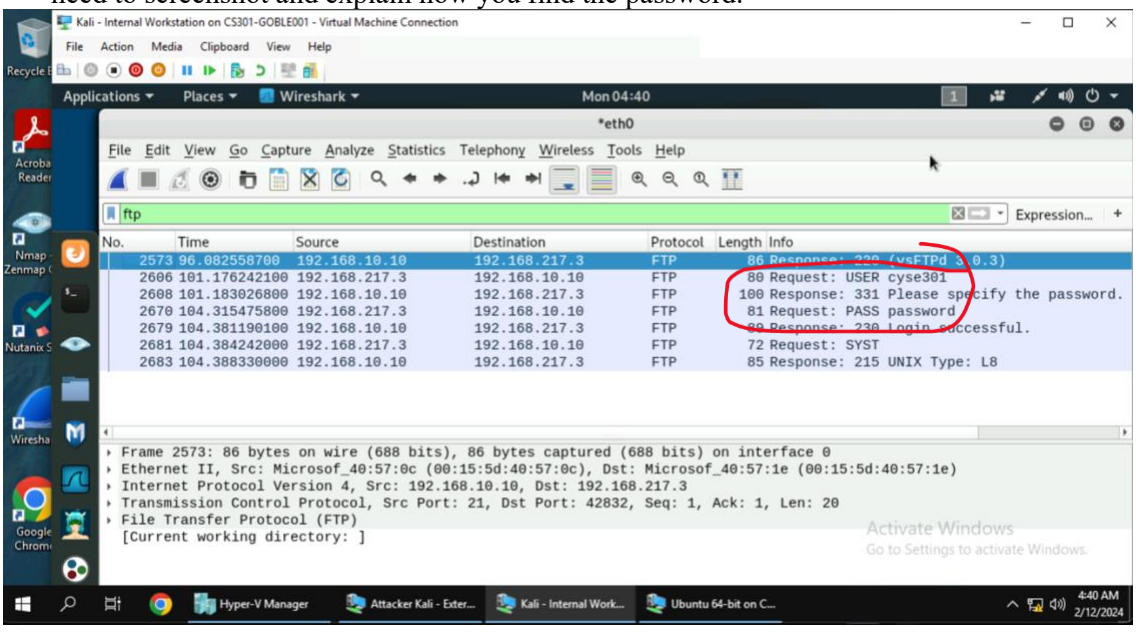
2. Sniff FTP traffic:

   a. Ubuntu VM is also serving as an FTP server inside the LAN network. Now, you need to use External Kali to access this FTP server by using the command: ftp [ip_addr of ubuntu VM]. The username for the FTP server is cyse301, and the password is password. You can follow the steps below to access the FTP server.



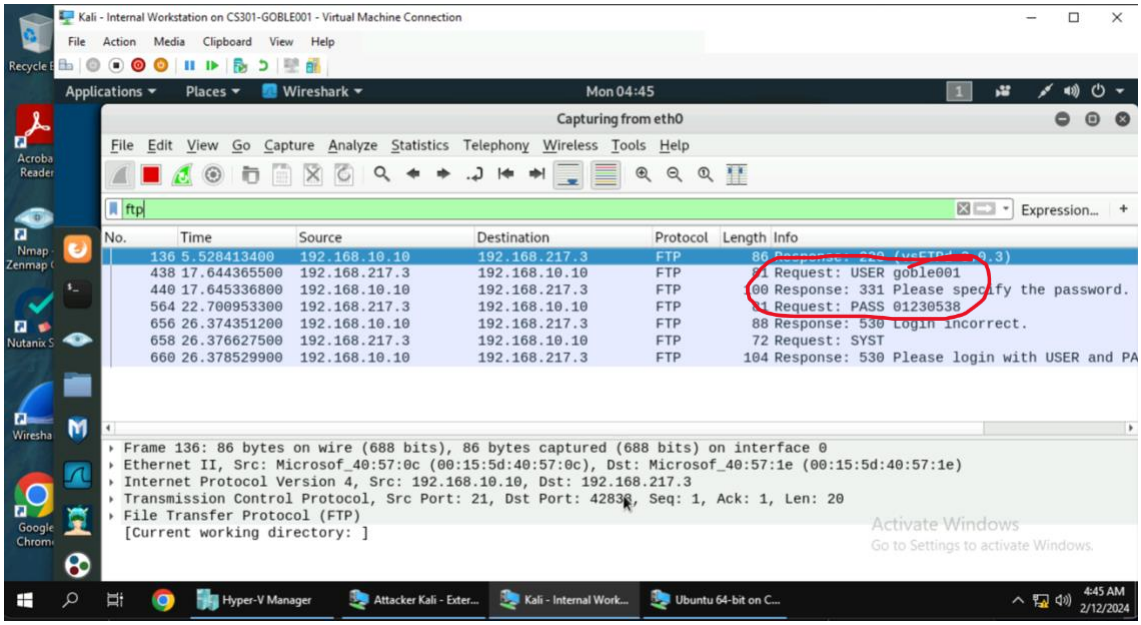
I inputted the command ftp 192.168.10.10 to access the the ftp server. I used the name cyse301 and password as the password.

   b. Unfortunately, Internal Kali, the attacker, is also sniffing to the communication. Therefore, all your communication is exposed to the attacker. Now, you need to find out the password used by External Kali to access the FTP server from the intercepted traffic on Internal Kali. You need to screenshot and explain how you find the password.



In order to find the password used by External Kali, I did the same thing, but started the capture on Internal Kali before inputting the ftp command. This allowed me to capture the ftp packets and find out the name and password inputted in the External Kali.

c. After you successfully find the username & password from the FTP traffic, repeat the previous step (2.a), and use your MIDAS ID as the username and UIN as the password to reaccess the FTP server from External Kali. Although External Kali may not access the FTP server, you need to intercept the packets containing these "secrets" from the attacker VM, which is Internal Kali.



Just like in step 2a and 2b., I inputted the ftp command in External Kali, but before that I started the Wireshark capture in Internal Kali. After this I inputted my MIDAS ID as the name and my UIN as the password. I was able to see my information from the capture in Internal Kali using the ftp display filter.