Old Dominion University

CYSE 301 Cybersecurity Techniques and Operations

Assignment #2 Traffic Tracing and Sniffing

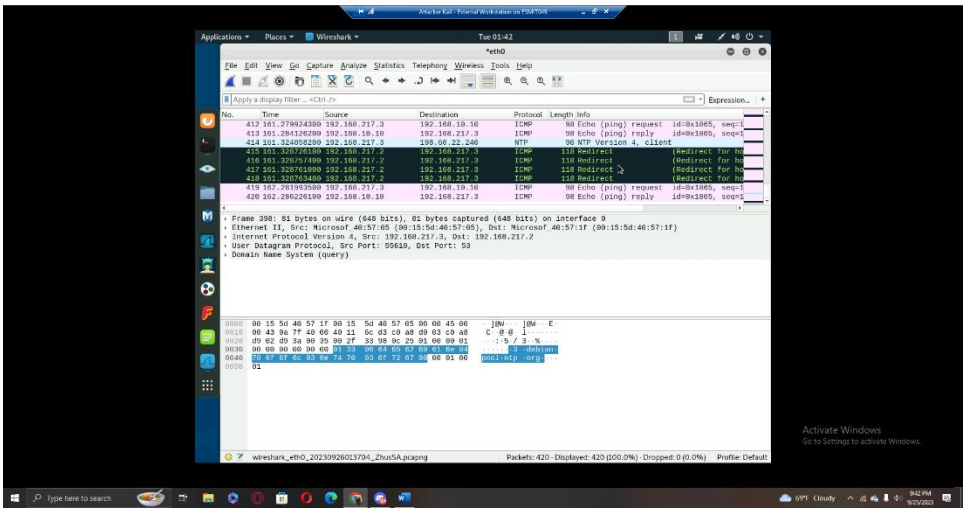
Ned Smith

01200384

Preface: I had to run the ping command for 2-3 minutes in order to get some DNS traffic, the TA's had mentioned doing this if you weren't getting any DNS traffic so I just wanted to explain why I had so many packets.

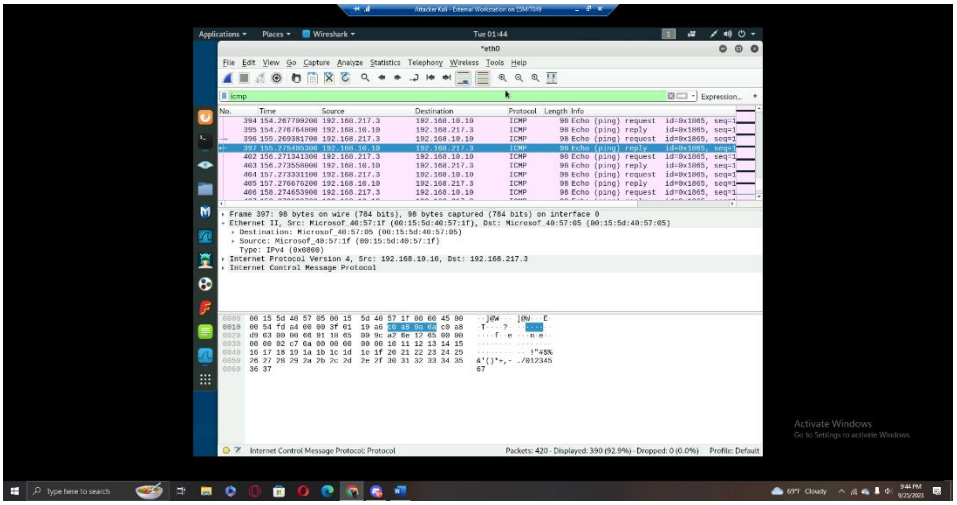
Task A

Question 1:



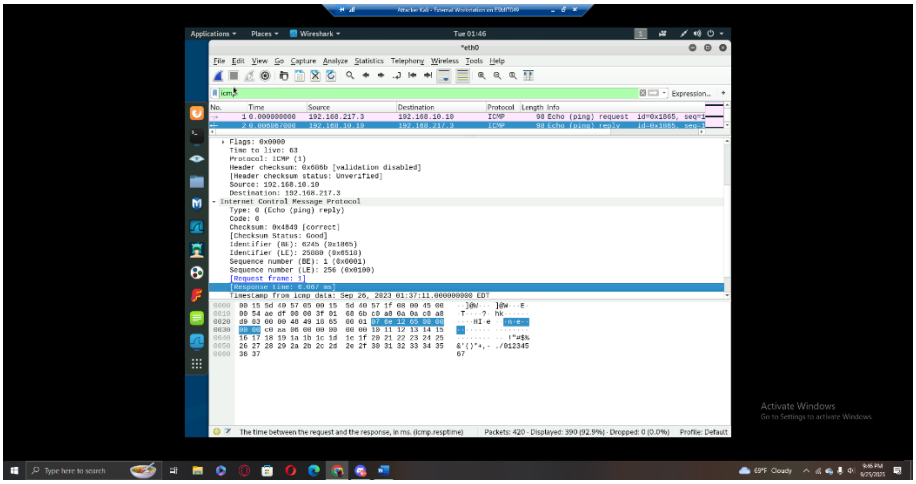
Explanation: There are a total of 420 packets have been captured and 420 packets have also been displayed.

Question 2:



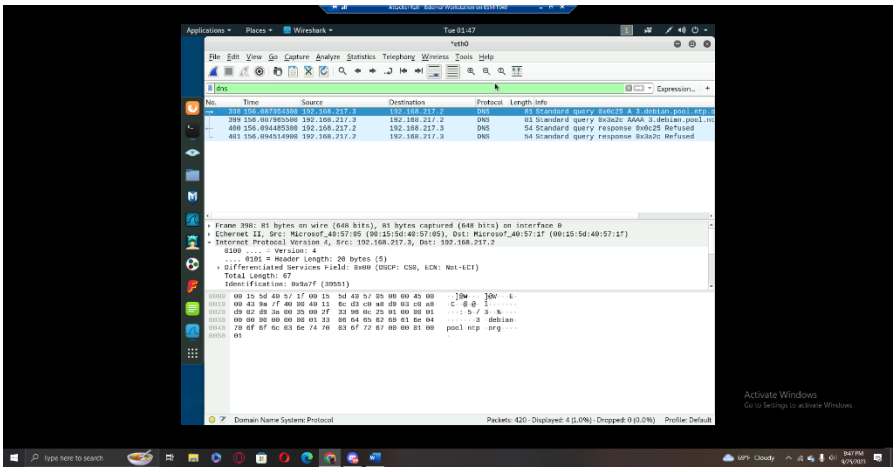
Explanation: There are a total of 420 packets have been captured, but there are only 390 packets being displayed due to the ICMP filter.

Question 3:



Explanation: The source IP is 192.168.10.10 and the destination IP is 192.168.217.3. The sequence number of this packet was 1/256 and the total size was 84 bytes. The response time is 6.067 ms (milliseconds).

Question 4:



Explanation: The total number of packets captured was 420, but only four packets were displayed due to the DNS filter.

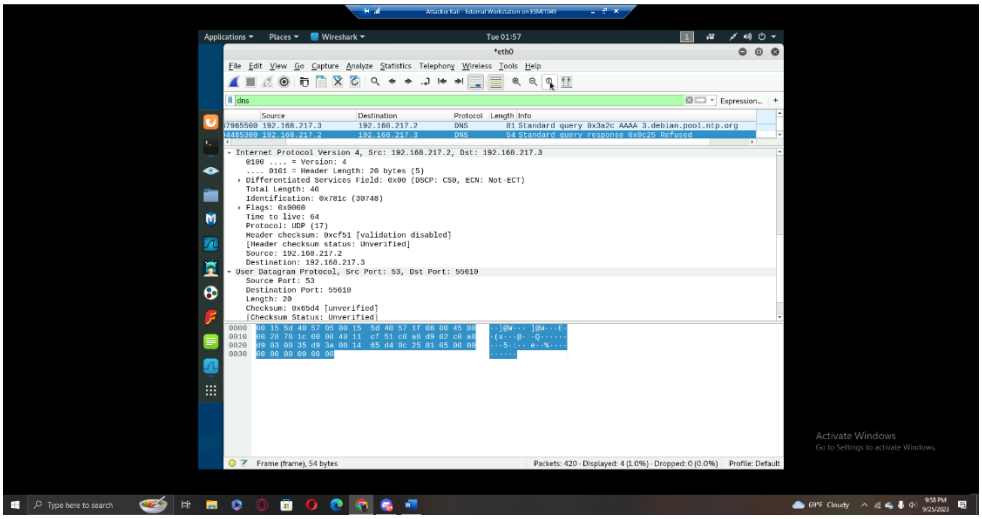
Question 5:

Explanation: I'm not sure if I did something wrong but this was the only DNS traffic I captured, the domain name it was trying to resolve was 3.debian.pool.ntp.org. The source IP/port and destination IP/port are displayed below:

Source: 192.168.217.3/55610

Destination: 192.168.217.2/53

Question 6:



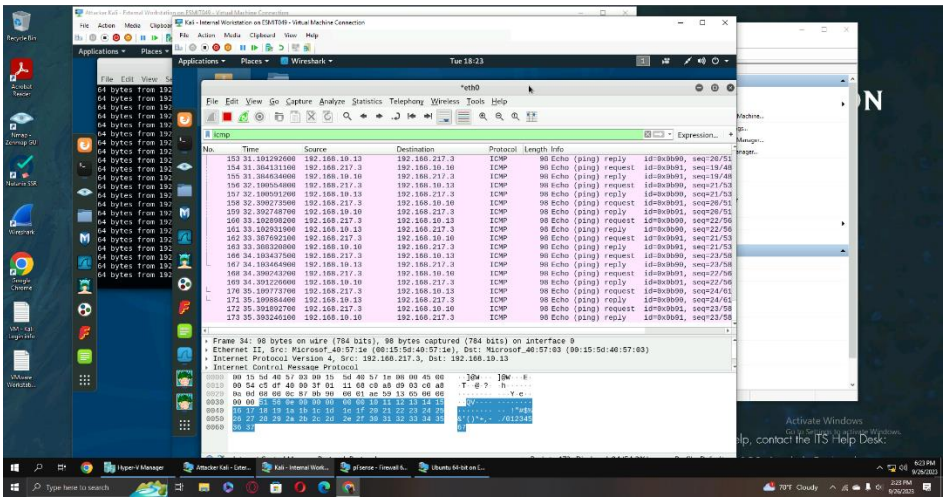
Explanation: The message replied from the server is “Refused” and the source IP/port and destination IP/port are displayed below:

Source: 192.168.217.2/53

Destination: 192.168.217.3/55610

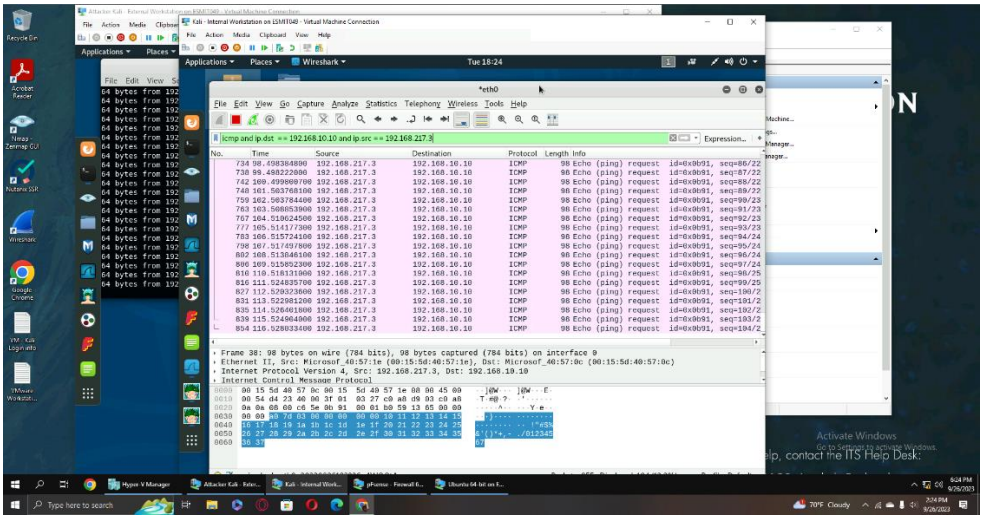
Task B

Question 1a:



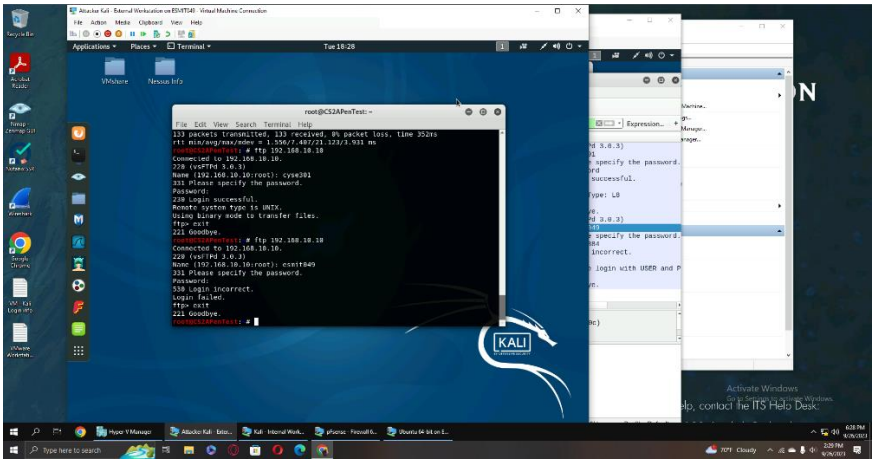
Explanation: I applied the capture filter “ICMP” to capture all current ICMP packets being transmitted between all sources and destinations.

Question 1b.



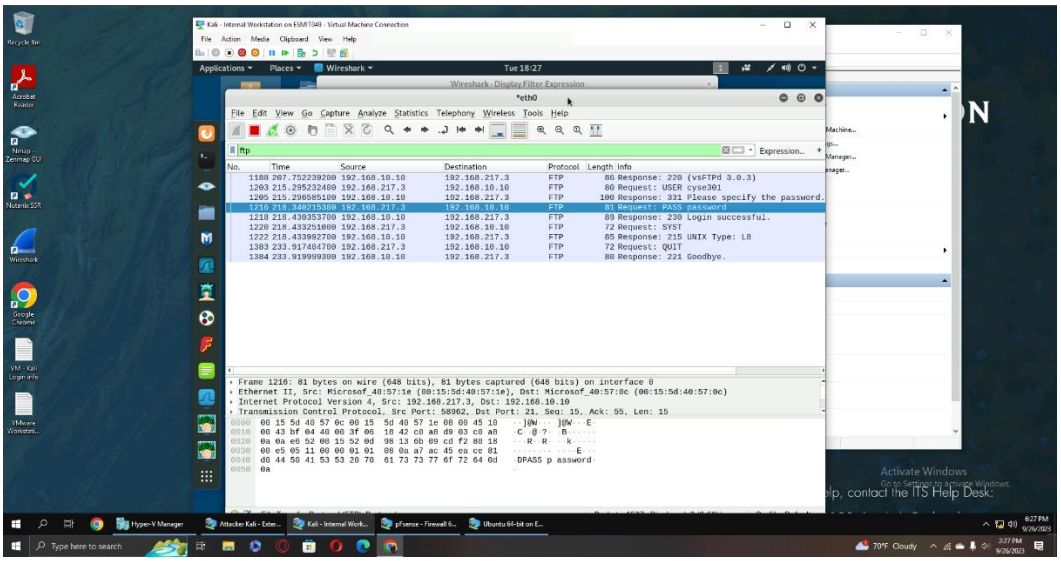
Explanation: I applied a capture filter that specified the packet must be an ICMP packet as well as have a source IP of 192.168.217.3 (the IP address of External Kali) and a destination IP of 192.168.10.10 (the IP address of the Ubuntu VM). This showed only ICMP request packets from External Kali and to Ubuntu VM.

Question 2a:



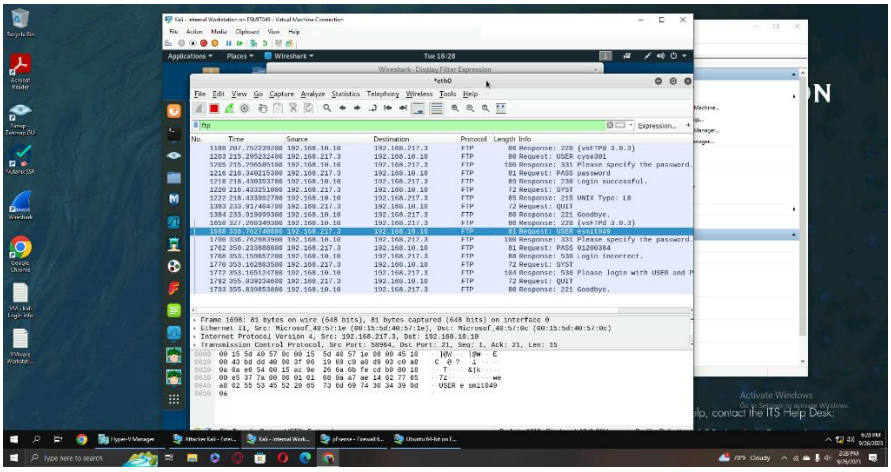
Explanation: This screenshot shows both the normal login for the Ubuntu VM and the login I was instructed to use for question 2c. One is username “cyse301” and password “password” and the other is my MIDAS and UIN.

Question 2b:



Explanation: The password used on External Kali to access the FTP server was “password” as shown in the screenshot above. By applying the “FTP” filter to Wireshark, we can find the username and password that was used to access the FTP server as well as see that the login was successful.

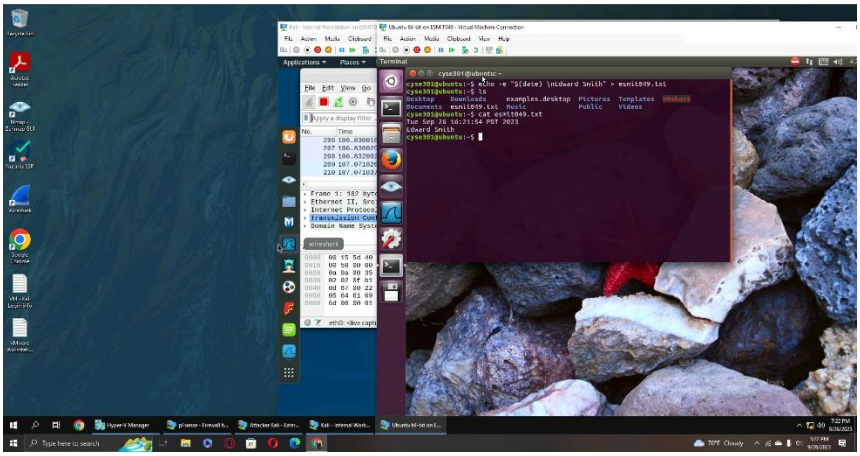
Question 2c:



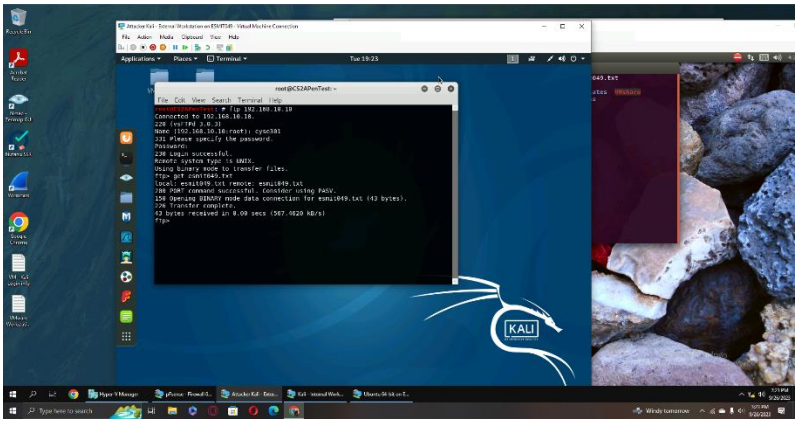
Explanation: This screenshot shows that Wireshark was able to again find out what was input for the username and password to the FTP server, this time being my MIDAS and UIN information. It was also able to see that the login was unsuccessful, similar to how it was able to see that the previous login was successful.

Task C (Extra Credit)

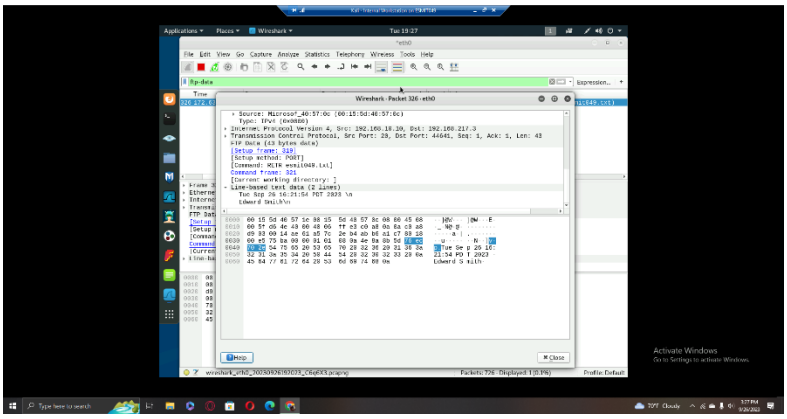
Question 1:



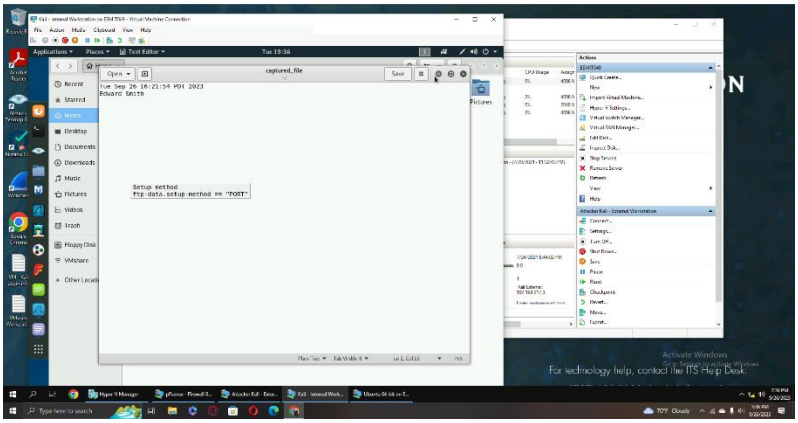
Explanation: This image shows me creating and saving the file that will soon be transferred over to the External Kali VM.



Explanation: This image shows me performing an FTP file transfer to transfer the file created in screenshot one over to the External Kali VM from the Ubuntu VM.



Explanation: This image shows that the FTP file transfer was captured by Wireshark on the Internal Kali VM.



Explanation: This image shows that the text file and its contents were properly saved to a text file on the Internal Kali VM from what was found during the Wireshark sniffing.