Assignment: Lab 2 – Traffic Tracing and Sniffing

By Justin White

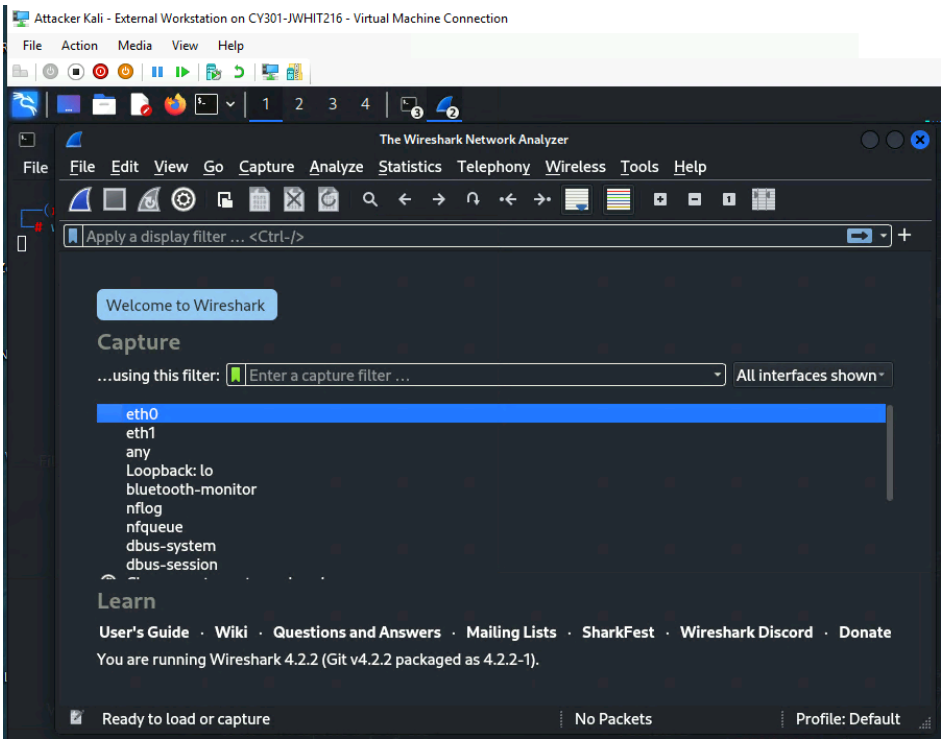
CYSE 301

Professor Vatsa

June 16th, 2025

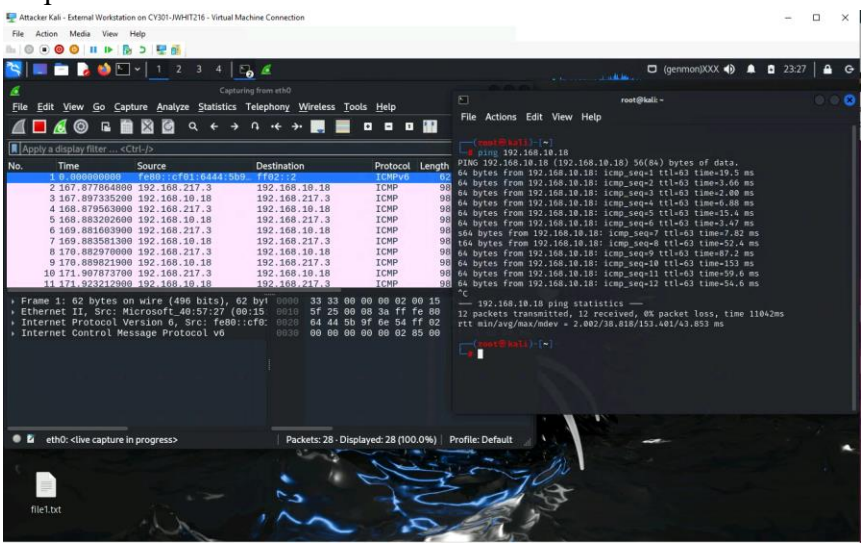
Task A

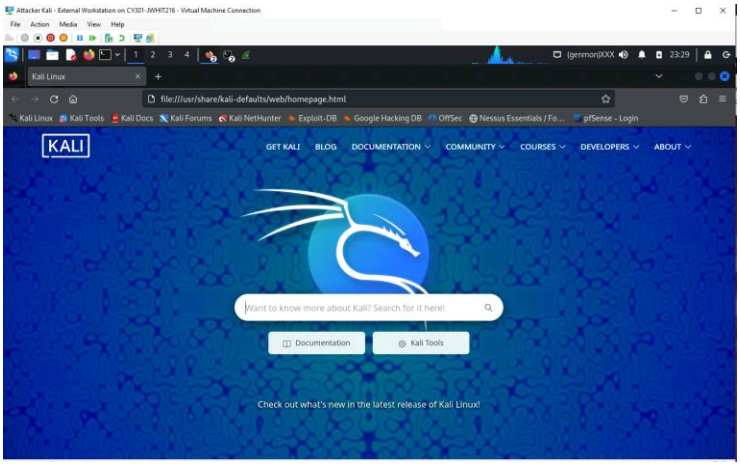
Step 1:



I launched wireshark on external kali and started capturing packets on the eth0 interface to monitor network traffic.

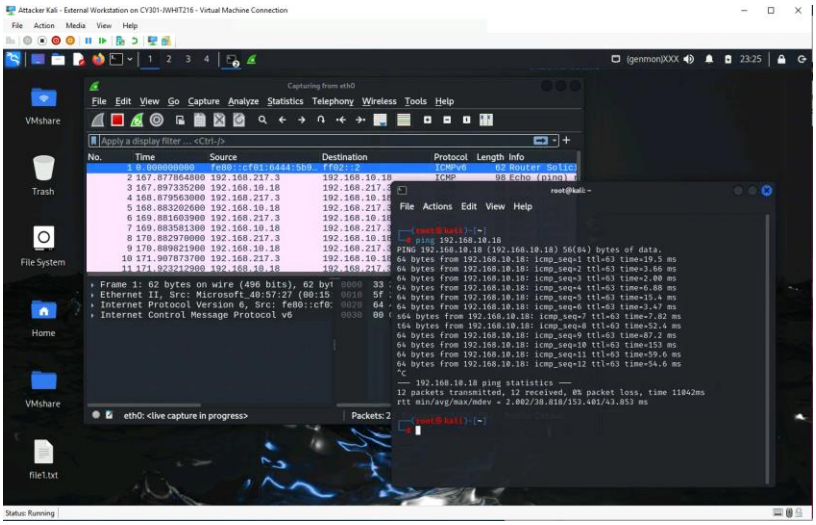
Step 2-3:





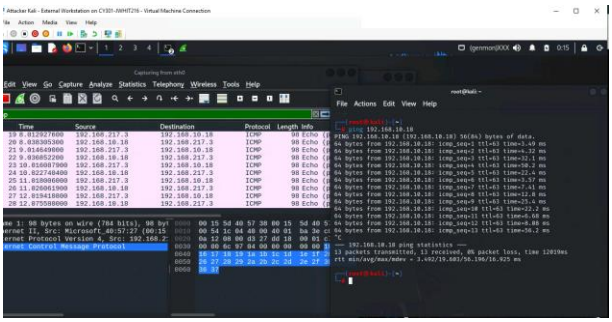
For this step I used the ping command from external kali to ubuntu to generate ICMP traffic that wireshark could capture for analysis as well as opened a web browser to trigger DNS and HTTP requests, simulating normal user behavior and increasing traffic for capture.

Step 4:

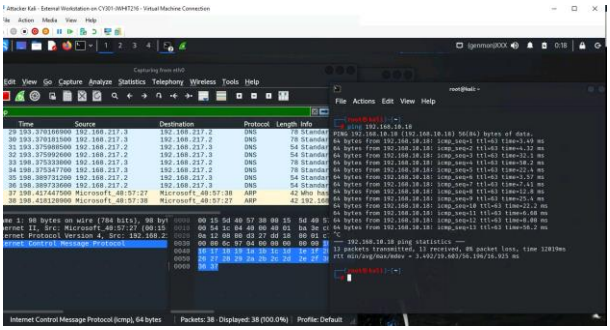


For the last step for task A I stopped wireshark from capturing after interactions were complete to analyze any and all collected data for further detail.

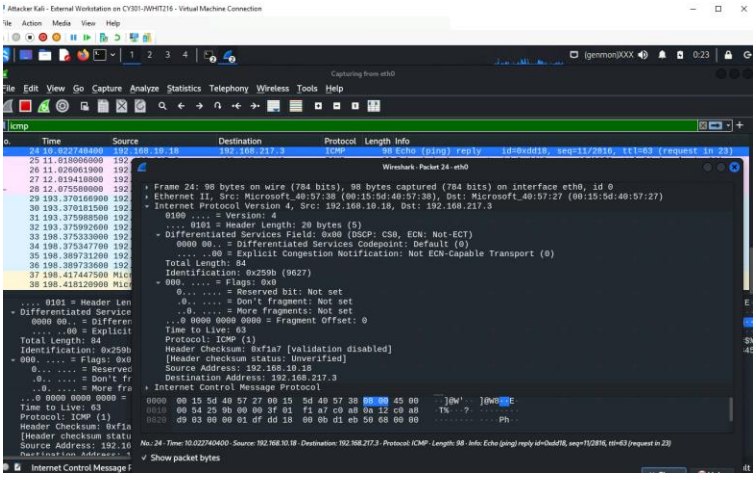
Q1 Answer: **The number of packets sent and received were 13 packets however when pinged in wireshark it was 28 packets.**



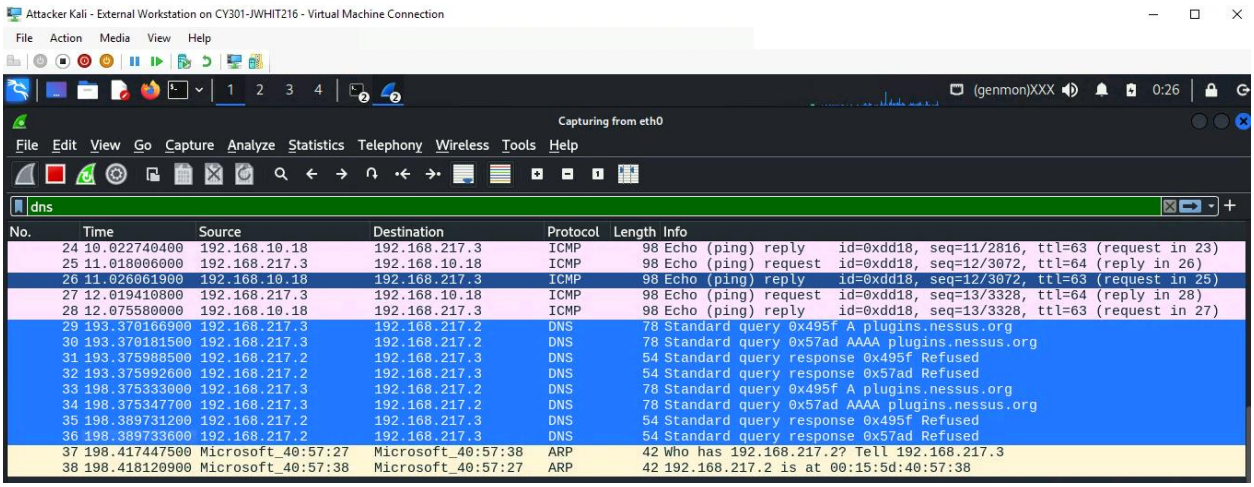
Q2: Answer: **When pining Ubuntu while having wireshark up and having the ICMP display applied the amount of packets were 38 and the amount displayed were 38.**



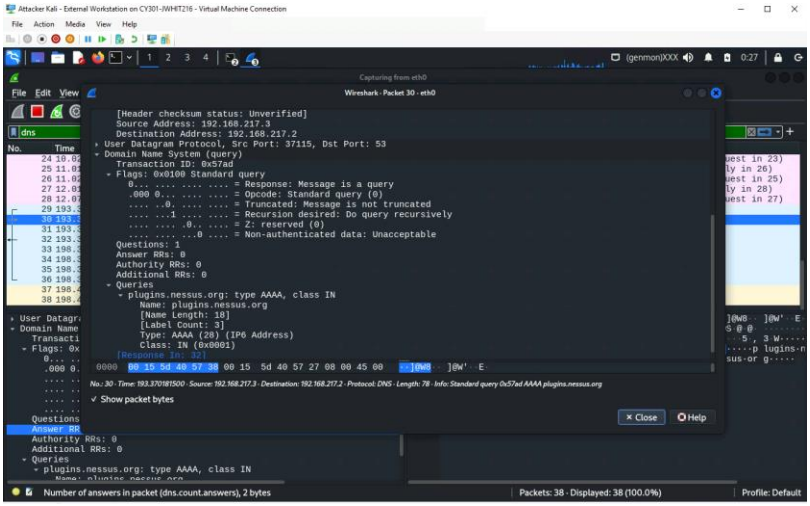
Q3 Answer: **The ICMP echo reply selected with source/destination IP, sequence number, and data size.**



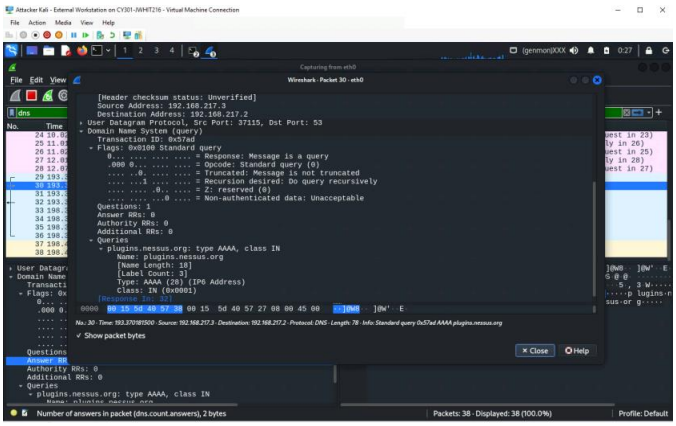
Q4 Answer: **Displayed DNS packets are 8 in total**



Q5 Answer: **The DNS query packet showing the domain name and source/destination IP shown within the domain name section**

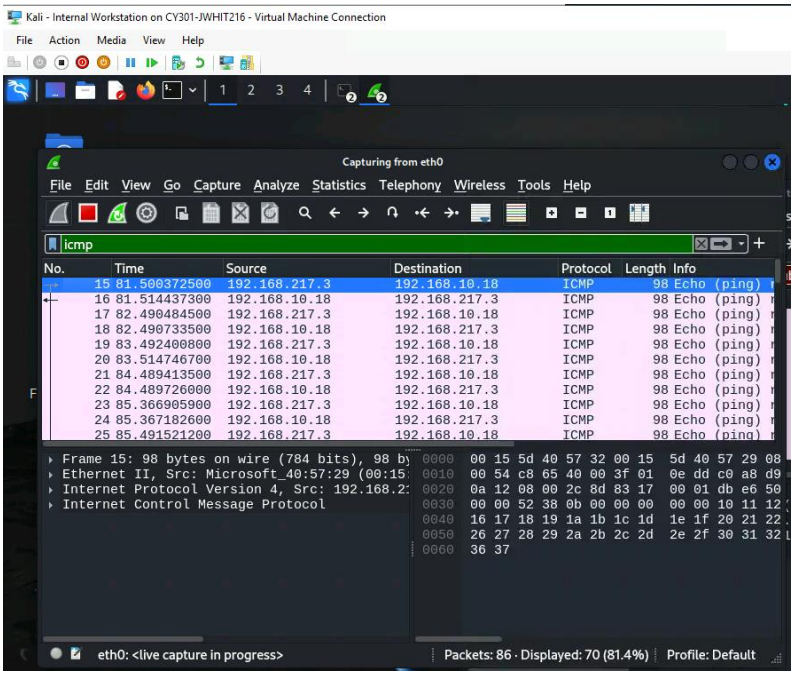


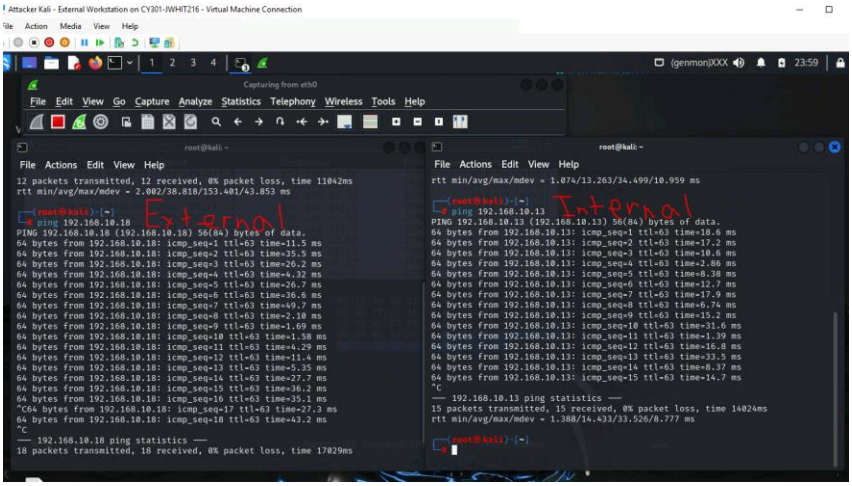
Q6 Answer: **The source from the query is shown to have the same IP destination but received a denial is a reply.**



Task B

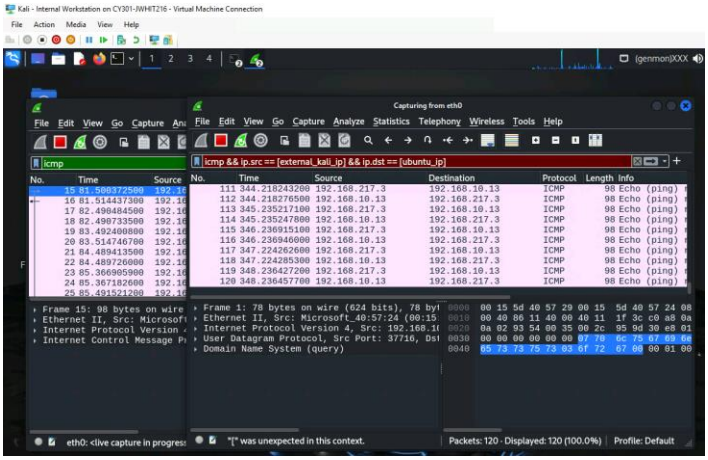
Step 1a:

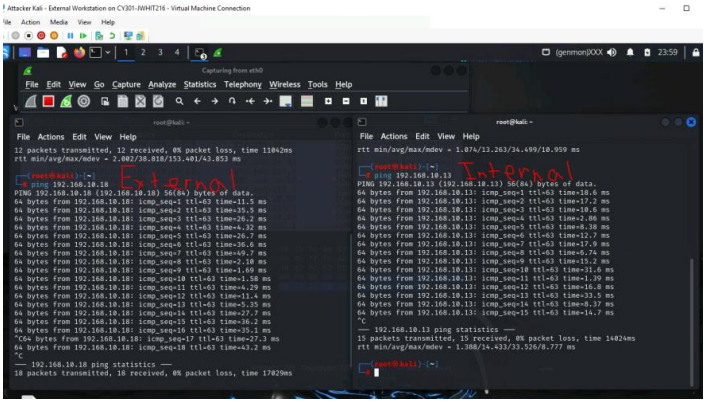




I started on wireshark on internal kali with a filter to capture general ICMP traffic between the two hosts being external kali and ubuntu within the LAN.

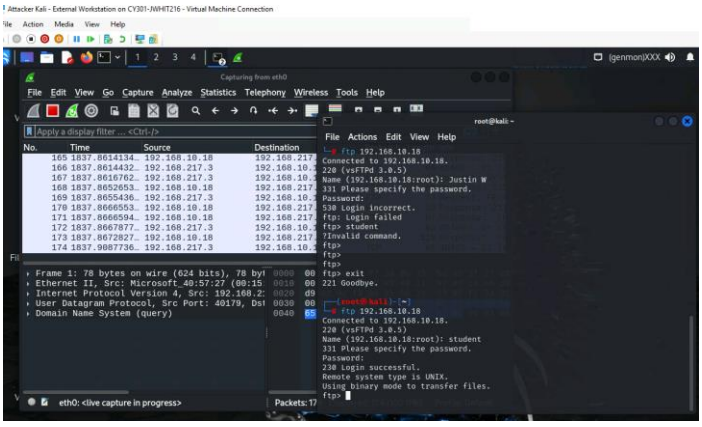
Step 1b:





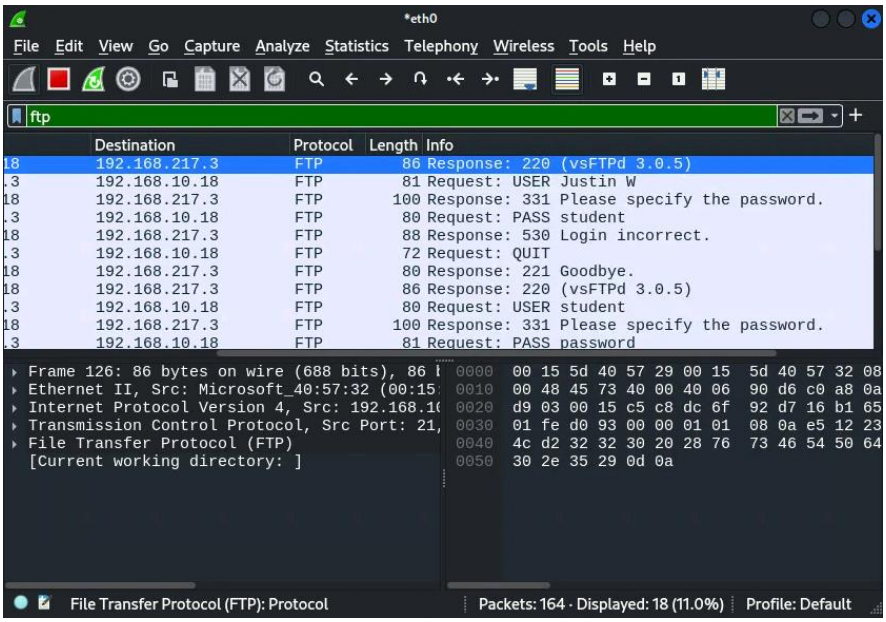
I applied for an ICMP filter to isolate the packets specifically from external kali to ubuntu, to simulate what targeted traffic monitoring looks like.

Step 2a:



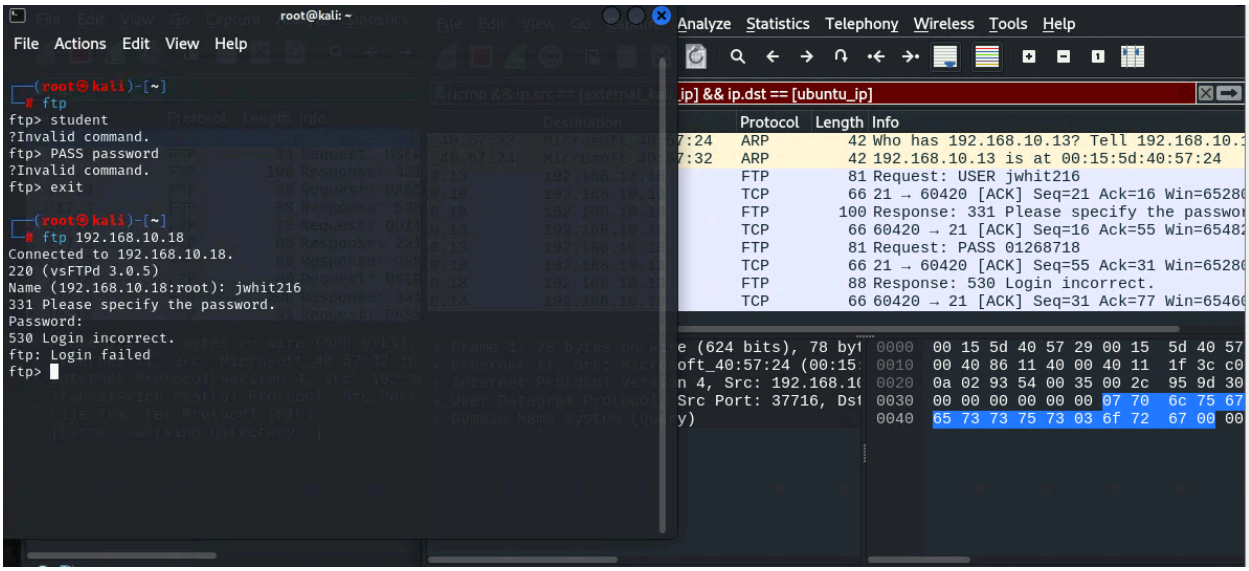
I initiated FTP connection from external kali to ubuntu using the provided credentials which generated the FTP login traffic for the simulated interception of the traffic.

Step 2b:



In this step I intercepted and inspected FTP control traffic on internal kali to reveal login credentials in the plaintext using the FTP display filter.

Step 2c:



For the final step I repeated the FTP login using personal credentials to demonstrate how sensitive information is exposed over unencrypted protocols.