OLD DOMINION UNIVERSITY

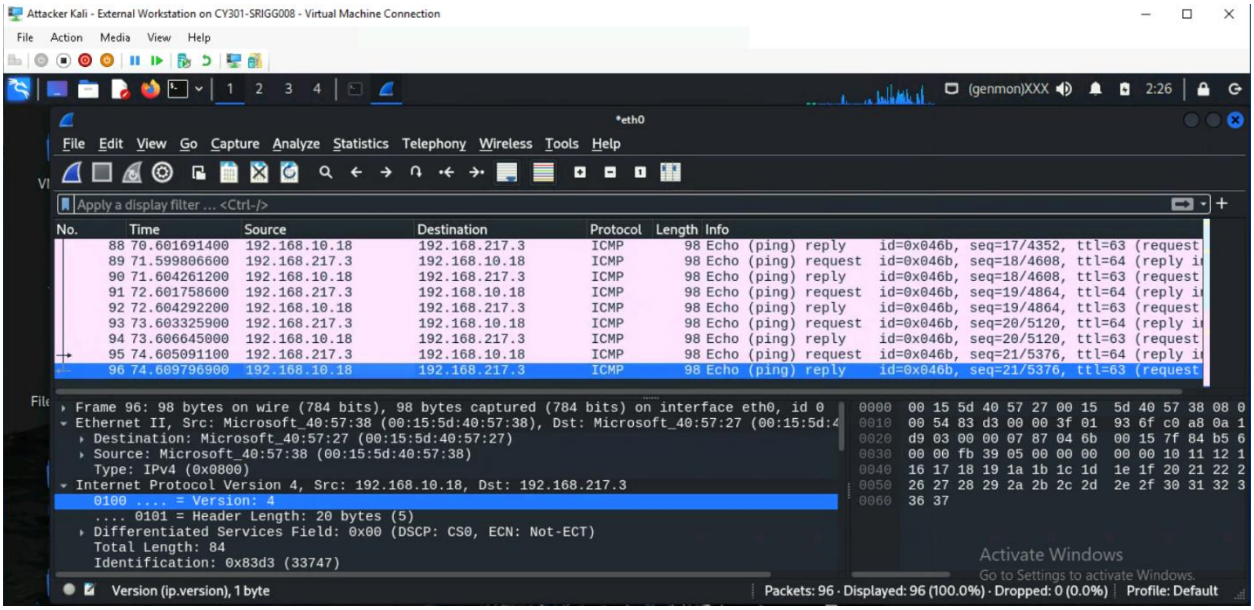
CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #2 Traffic Tracing and Sniffing

Samantha Riggs

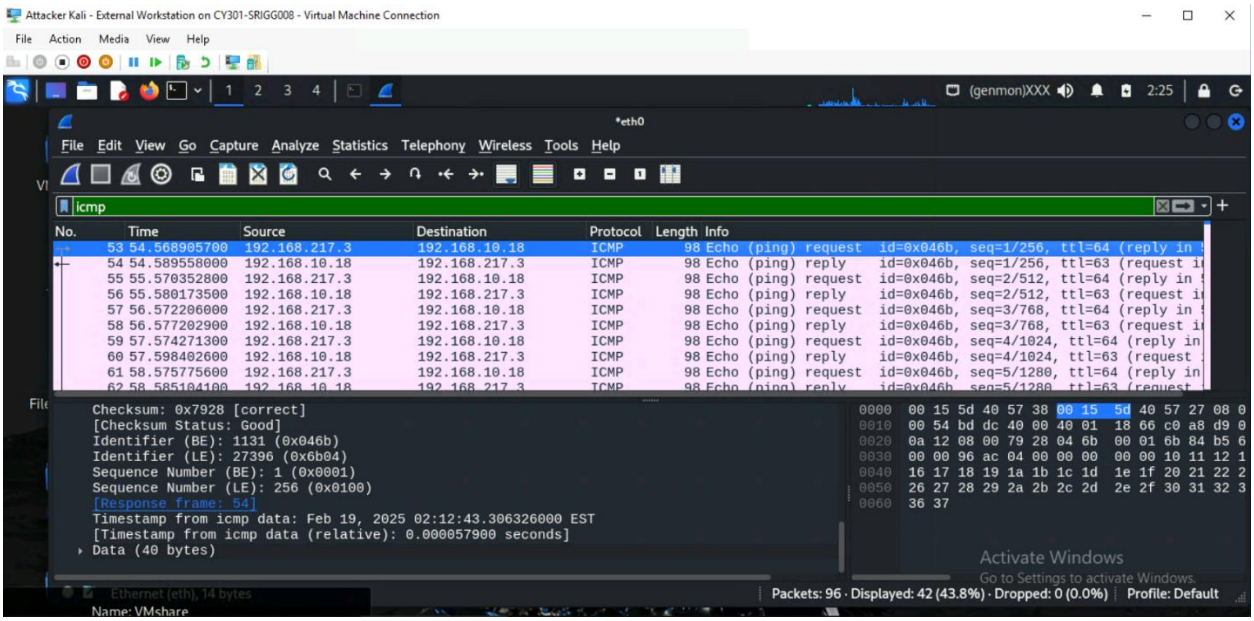
TASK A: GET STARTED WITH WIRESHARK

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



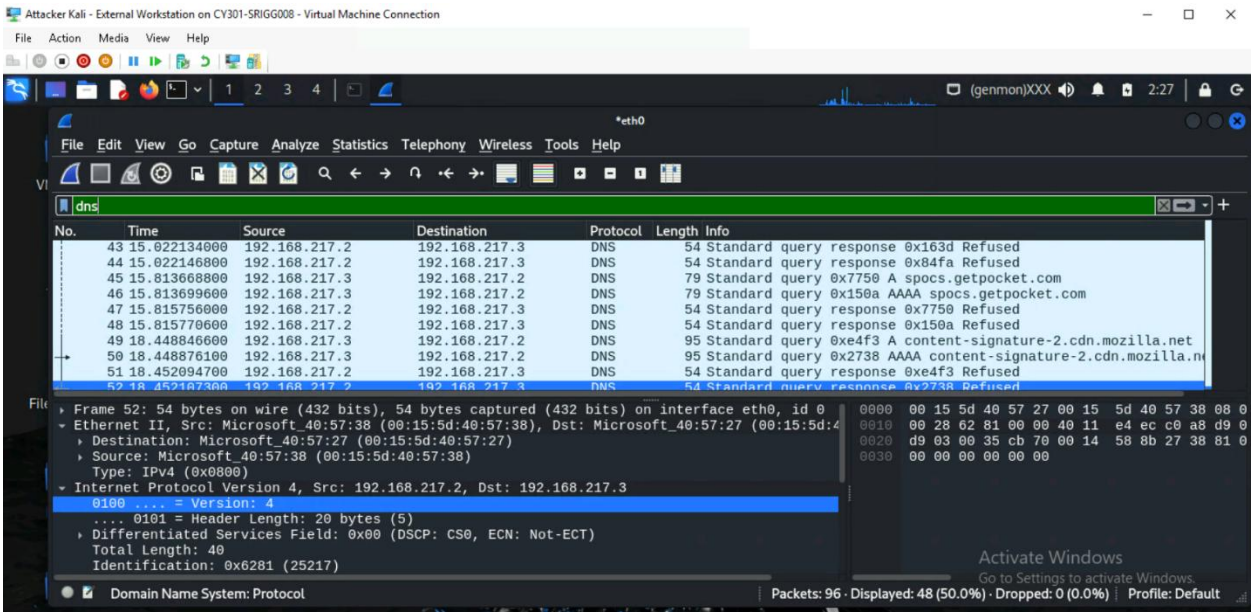
Wireshark states that 96 packets were received and 96 are displayed when no filter is applied.

2. Apply “ICMP” as a display filter in Wireshark then repeat question 1.
3. Select an Echo message from the list. What is the source and destination IP? What are the sequence numbers and the size of the data? What is the response time?



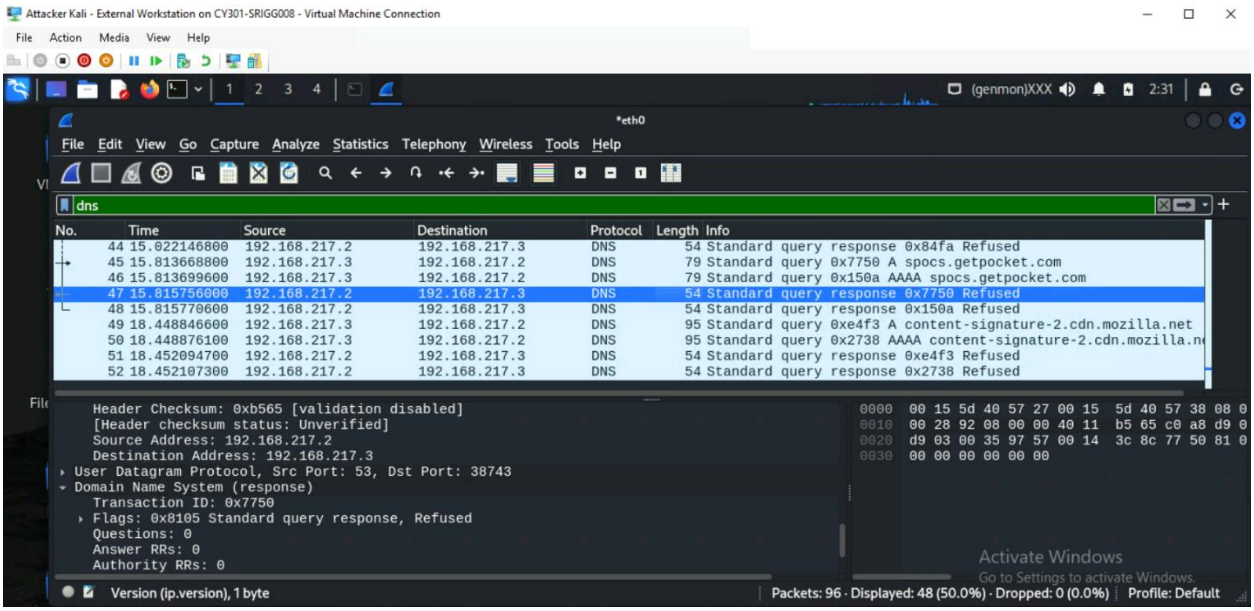
When ICMP is applied as a filter, 42 packets are displayed out of the 96 total packets. For the selected Echo message, the source IP is 192.168.217.3 and the destination IP is 192.168.10.18. The sequence number is 1/256 and the size of the data is 40 bytes. The response time is 0.0579 microseconds.

4. Apply “DNS” as a display filter. How many packets are displayed.



When the “DNS” filter is applied, 48 packets are displayed out of the 96 total packets.

5. Find a DNS query packet. What is the domain name that is trying to be resolved? What is the source IP and port number, destination IP and port number?
6. Find the corresponding DNS response. What is the source IP and port number, destination IP and port? What is the message replied from the DNS server?



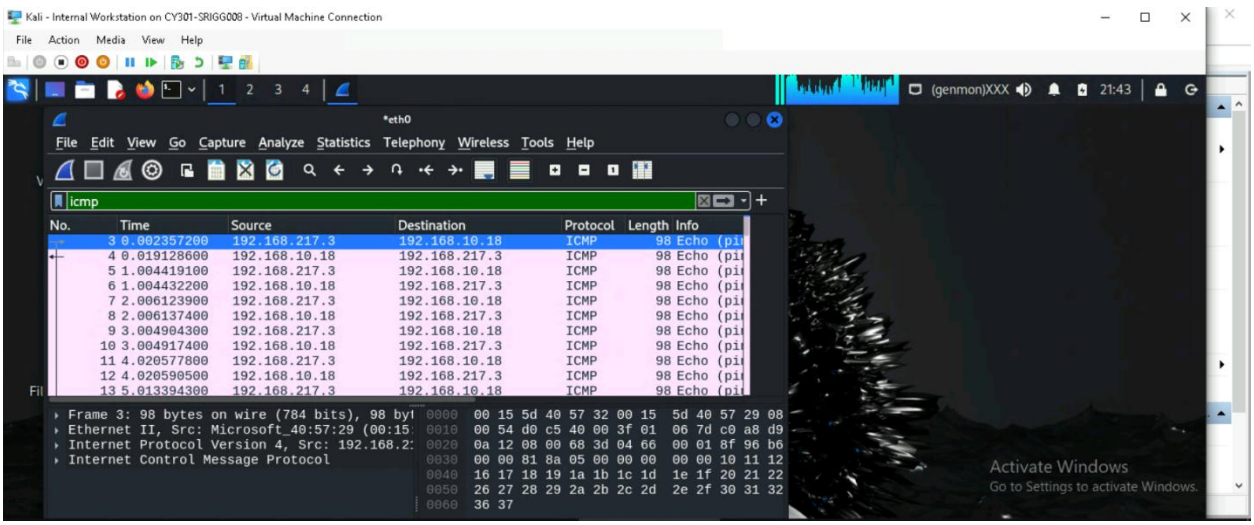
The domain name the host is trying to resolve is spocs.getpocket.com. The source IP and port number is 192.168.217.3: 38743 and the destination IP and port number is 192.168.217.2: 53.

For the corresponding DNS response to the query, the source IP and port number is 192.168.217.2: 53 and the destination IP and port number is 192.168.217.3: 38743. The message returned is Refused.

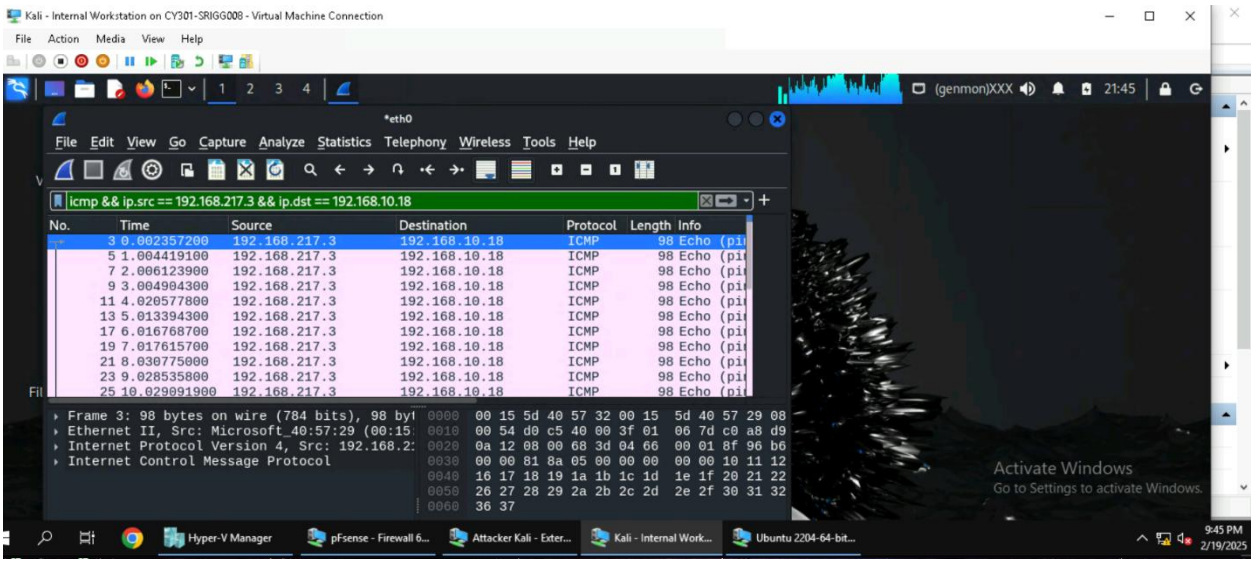
TASK B: SNIFF LAN TRAFFIC

1. Sniff ICMP Traffic

a. Apply proper display in Wireshark to show active ICMP traffic



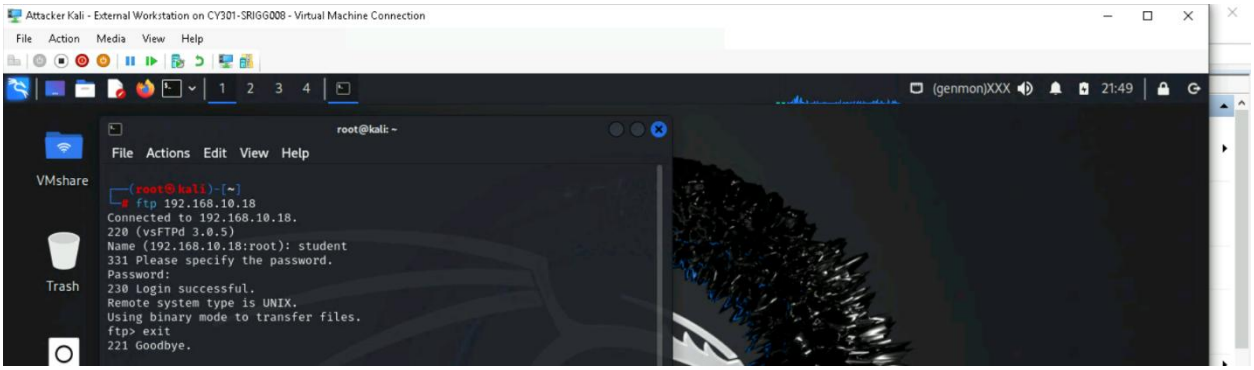
b. Display ICMP request that originated from the external Kali VM and goes to the Ubuntu VM.



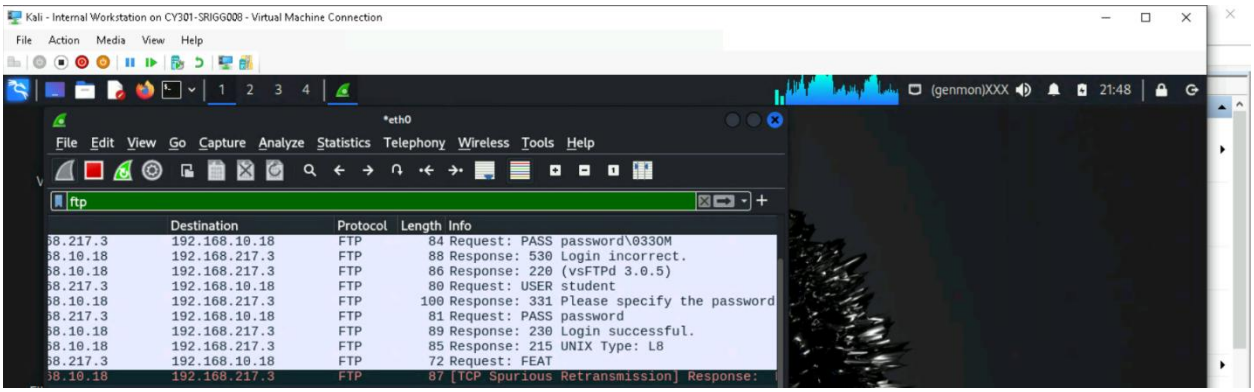
Adding the source IP and destination IP displays traffic that specifically came from the external Kali VM and went to the Ubuntu VM.

2. Sniff FTP Traffic

a. Use external Kali to access the FTP server

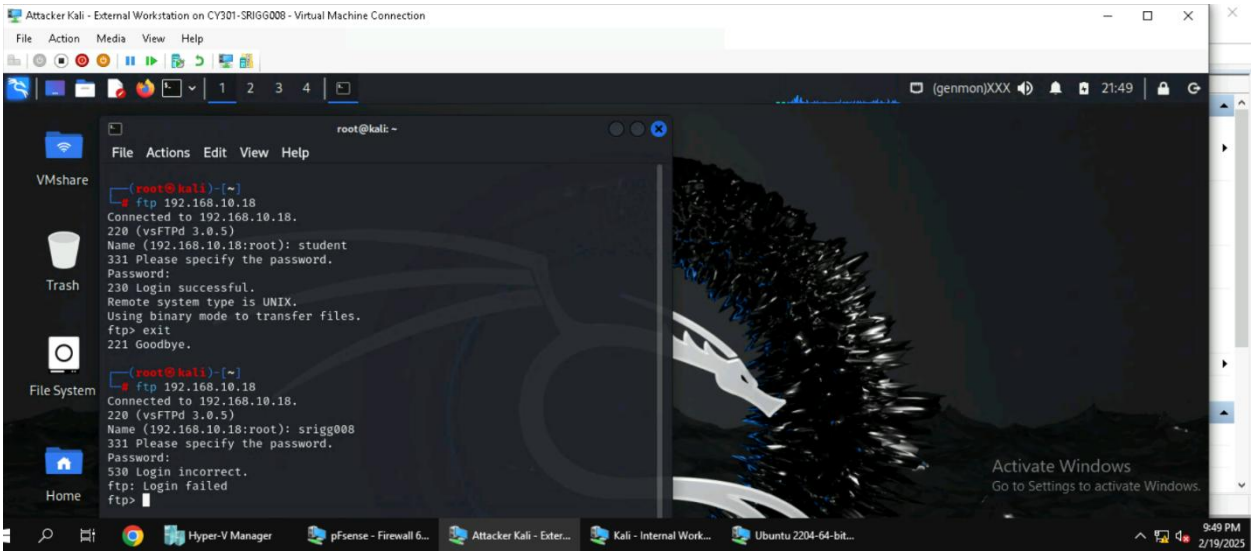


b. Find the password used by External Kali to access the FTP server from the intercepted traffic on Internal Kali

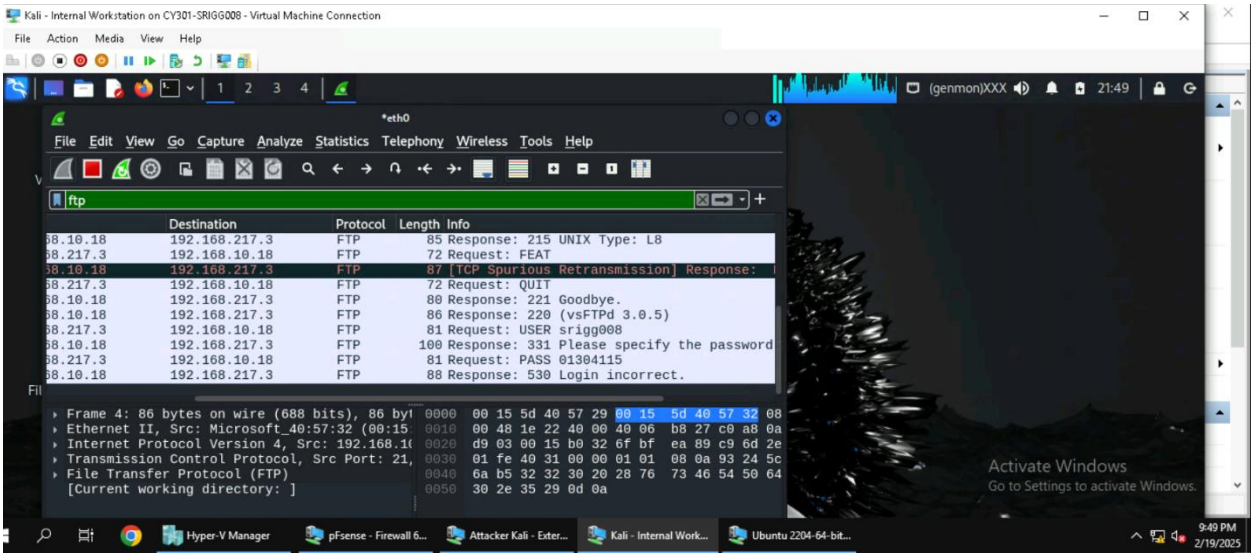


By using the ftp filter in Wireshark on Internal Kali, the intercepted traffic can be found that states the username and password used for a successful login on the Ubuntu FTP server.

c. Repeat the steps in 2.a using your MIDAS ID for the username and UIN for the password to re-access the server and show the intercepted login attempt.

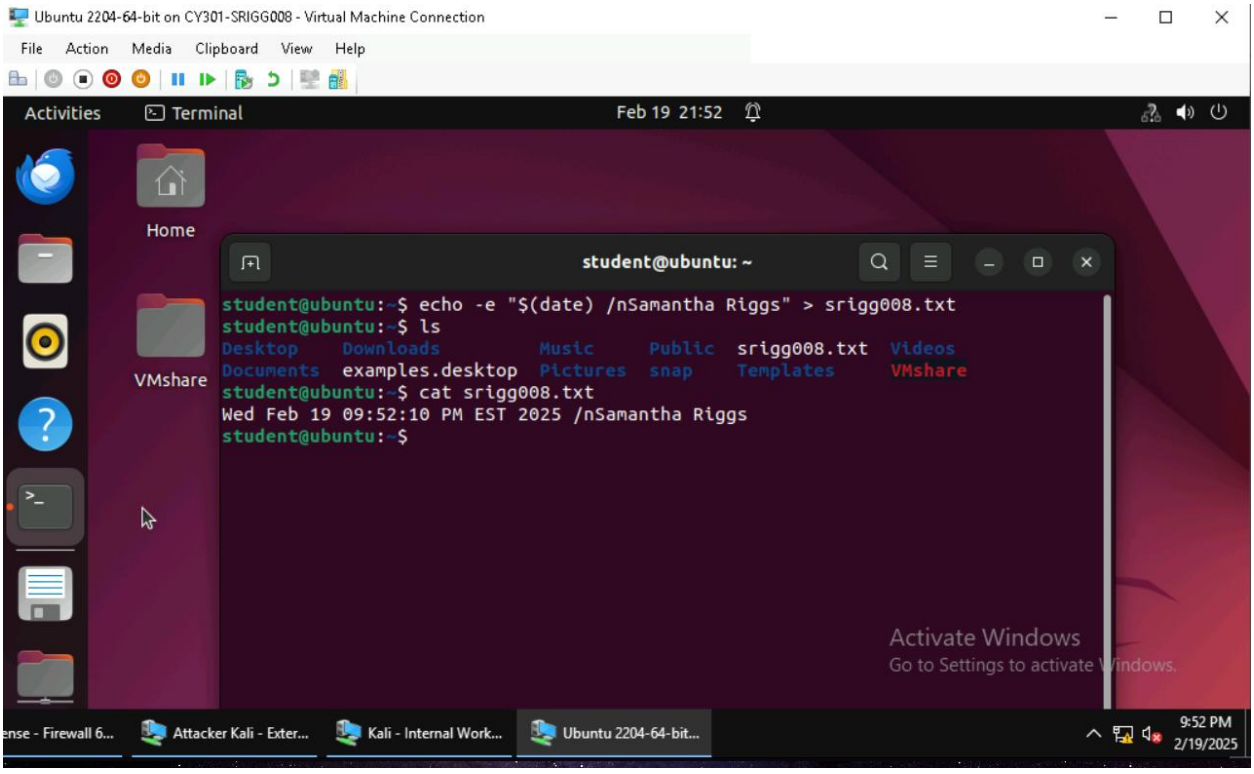


Above shows the login attempt to re-access the FTP server.

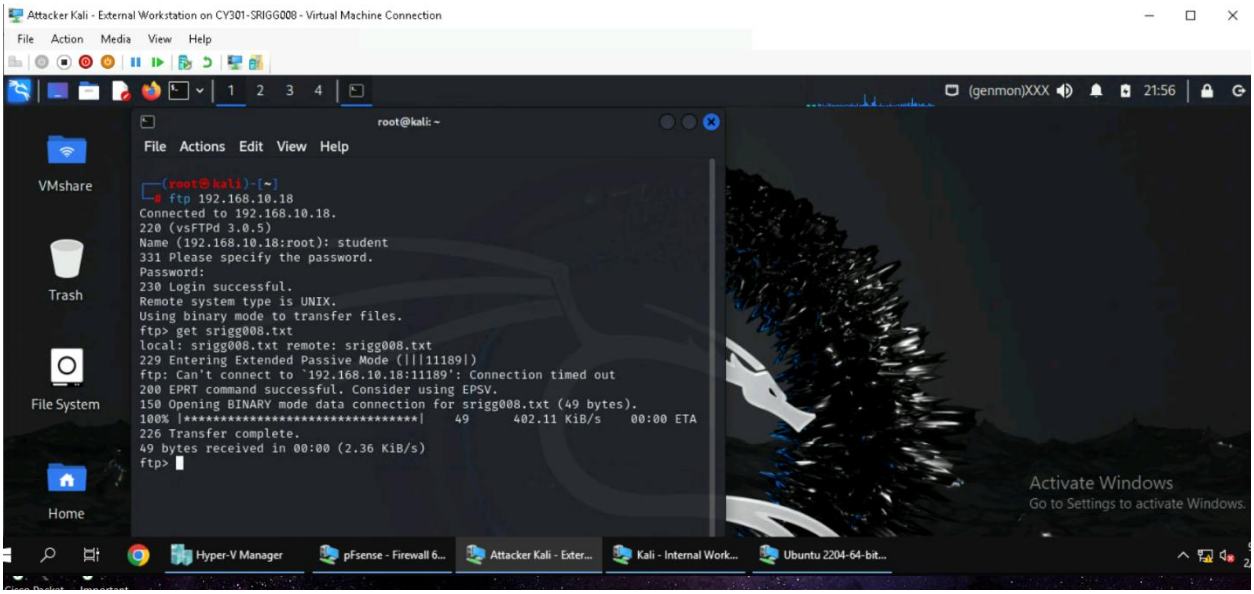


The intercepted username and password can be found again by using the ftp filter on Wireshark on Internal Kali, even though the attempt was not successful.

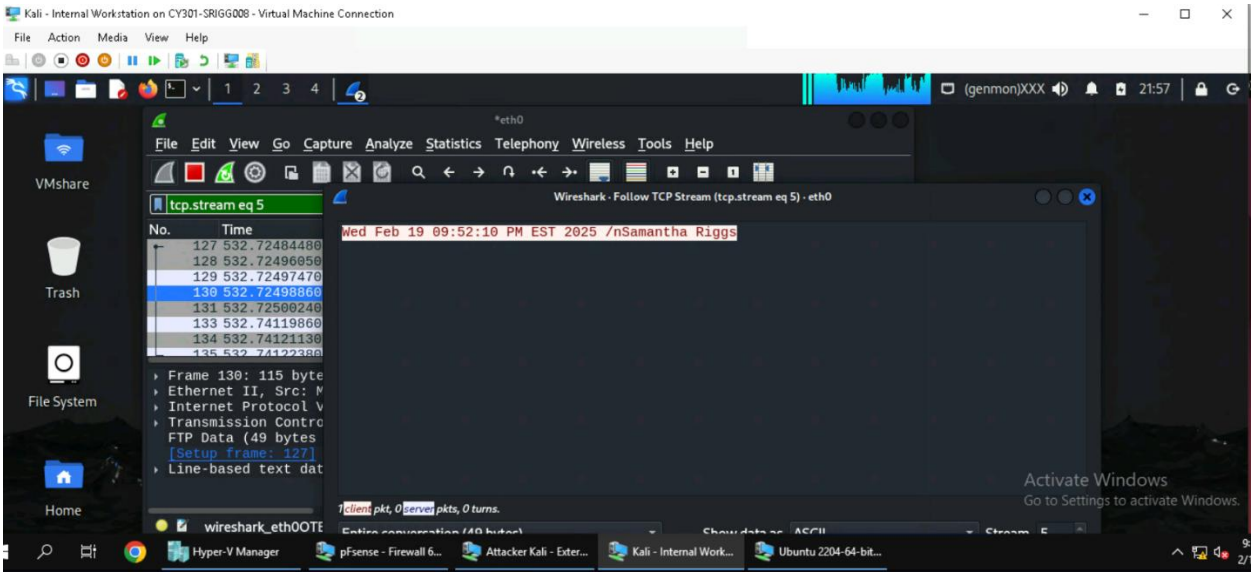
TASK C: STEAL FILES WITH WIRESHARK



Above is the creation of the file in Ubuntu (I accidentally used a forward slash instead of backslash to make a new line, but the timestamp and name is still present).



In External Kali using FTP Protocol, I used the command “get srigg008.txt” to get the file from Ubuntu.



After using the ftp-data filter in Wireshark and following the TCP stream, the contents of the file can be viewed.