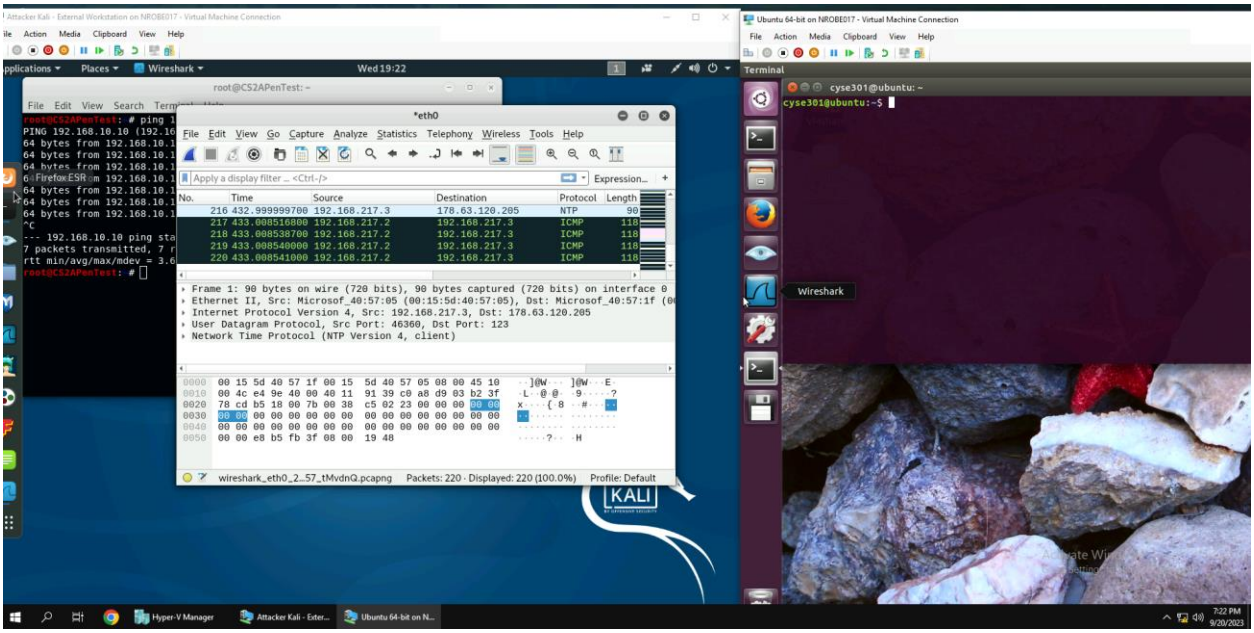
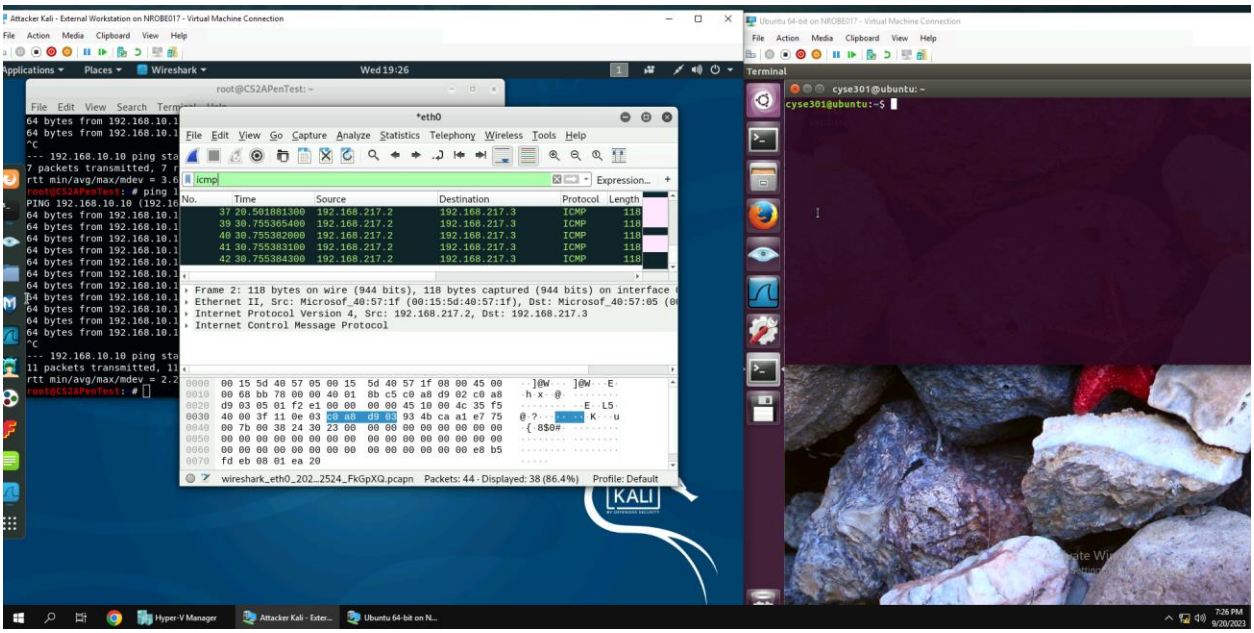
Nicholas Robertson

Assignment #2

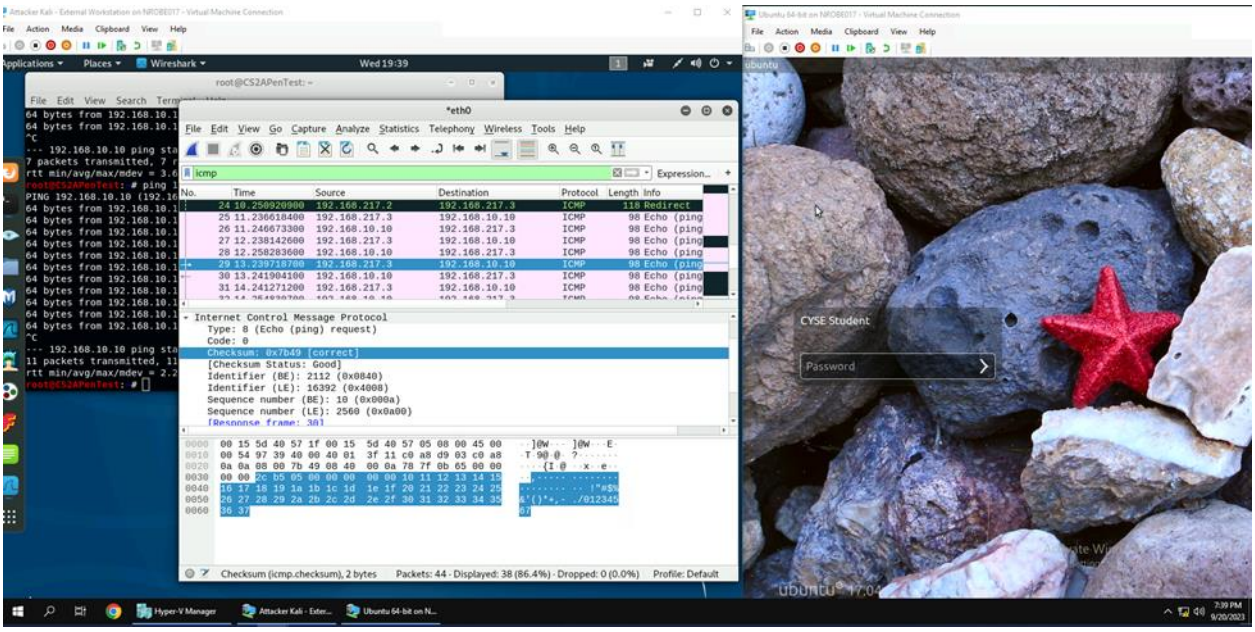
Task A

1. 

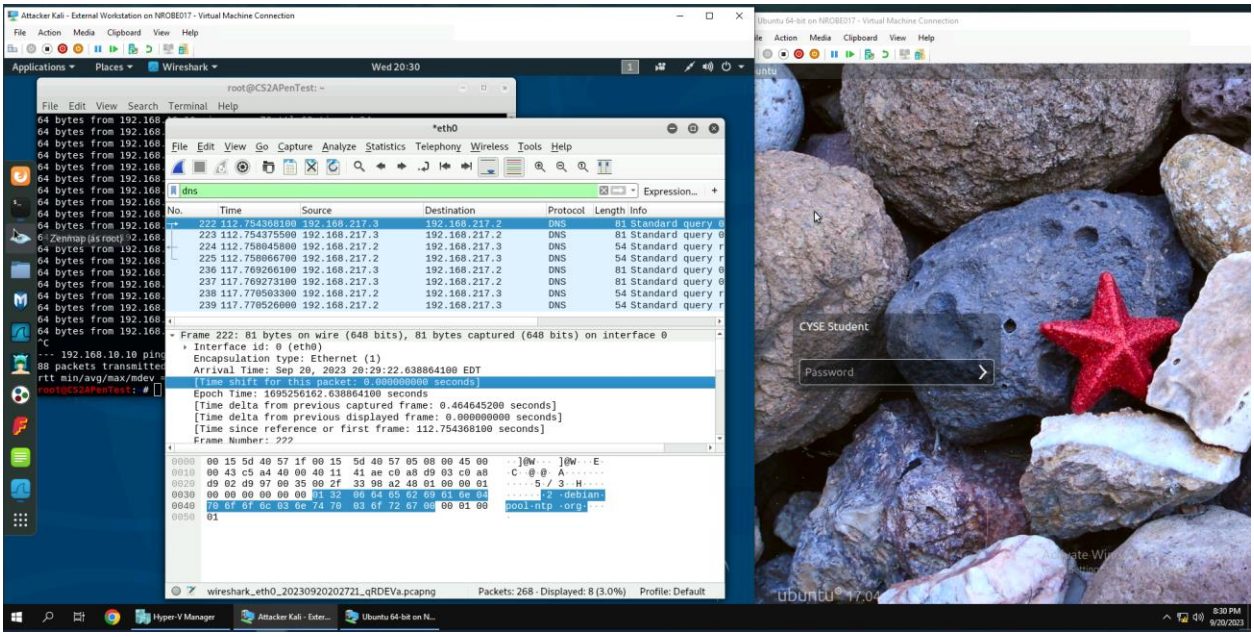
   In total there were 220 packets captured and all 220 of those packets were displayed.

2. 

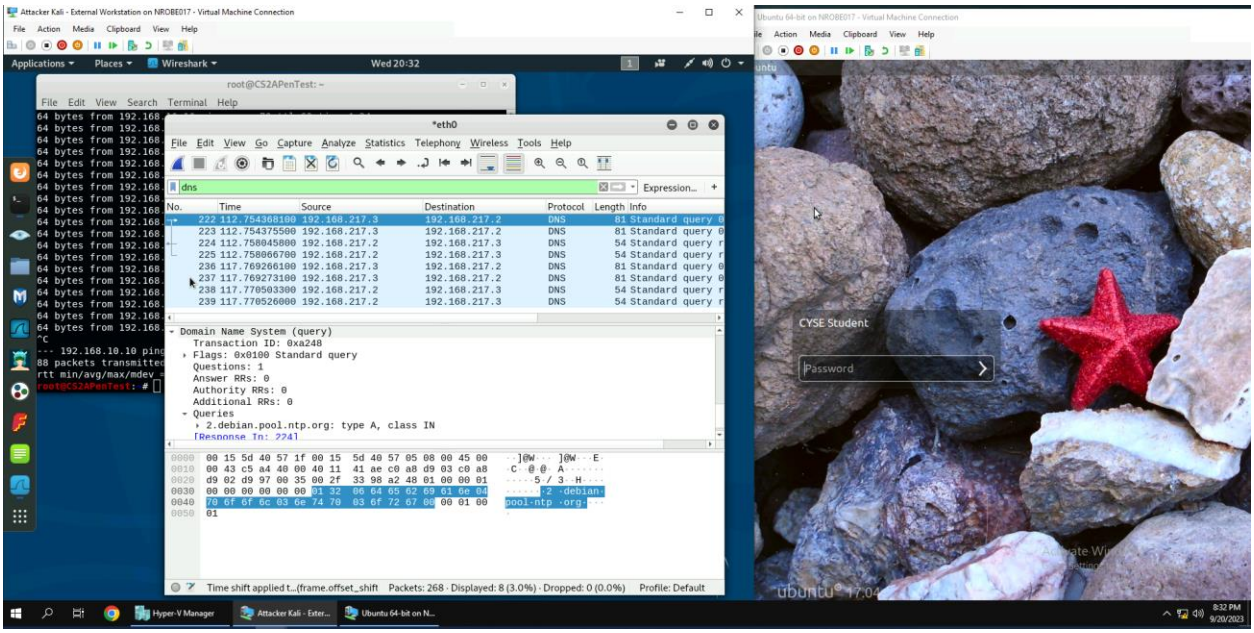
After applying “ICMP” in the display filter, there was a total of 44 packets captured with 38 of those packets being displayed.

3. 

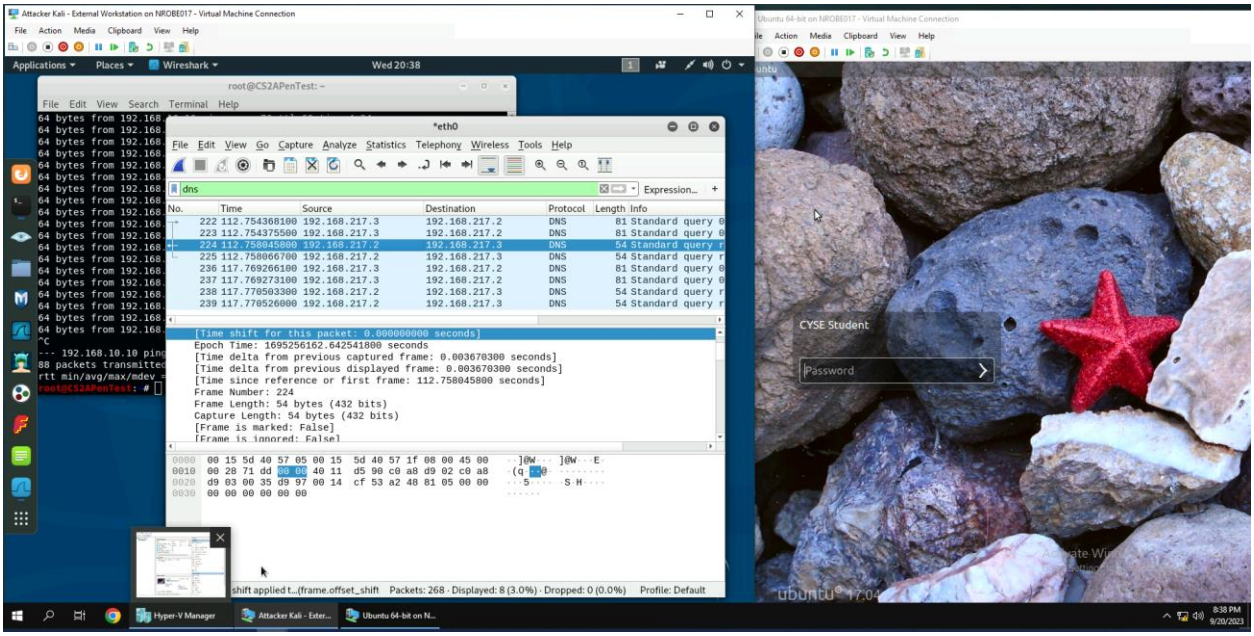
With the filter still on the source IP address is 192.168.217.3 and the destination IP is 192.168.10.10. The sequence number (BE) is 10 and the sequence number (LE) is 2560. The size of the data is 48 bytes and the response time was 13.559 ms.

4. 

With the DNS filter enabled, there are 8 packets that are displayed.

5. 

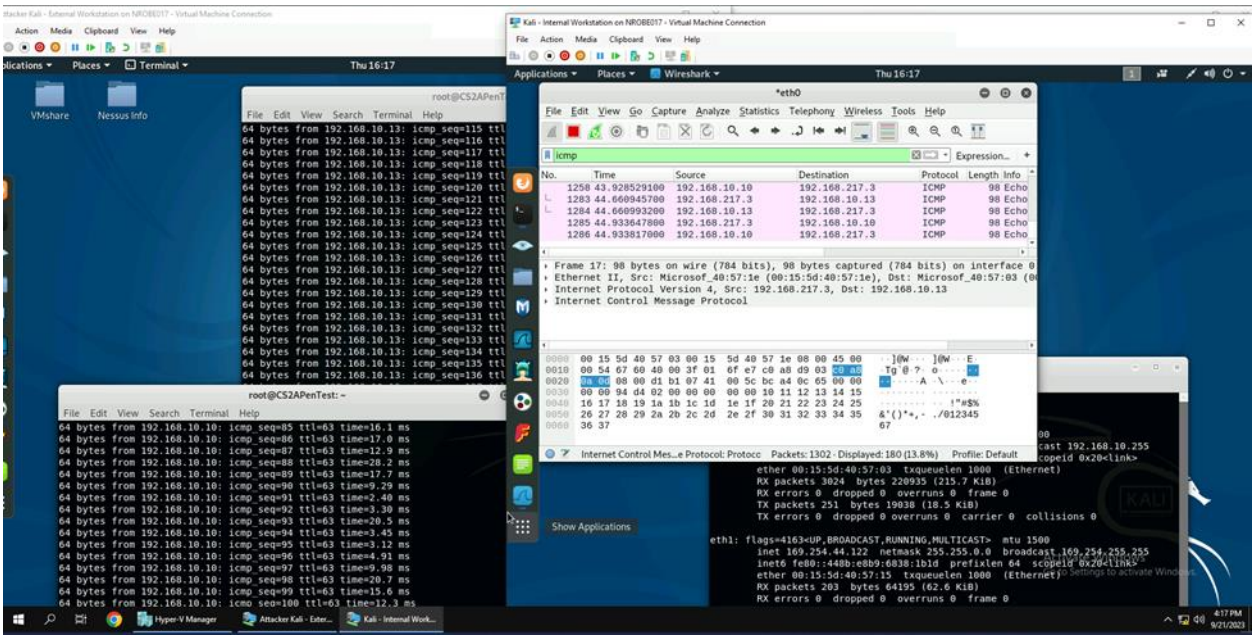
The domain name that this host is trying to resolve is 2.debian.pool.ntp.org: type A, class IN. The source IP and port number is 192.168.217.3:55703 and the destination IP and port number is 192.168.217.2:53.

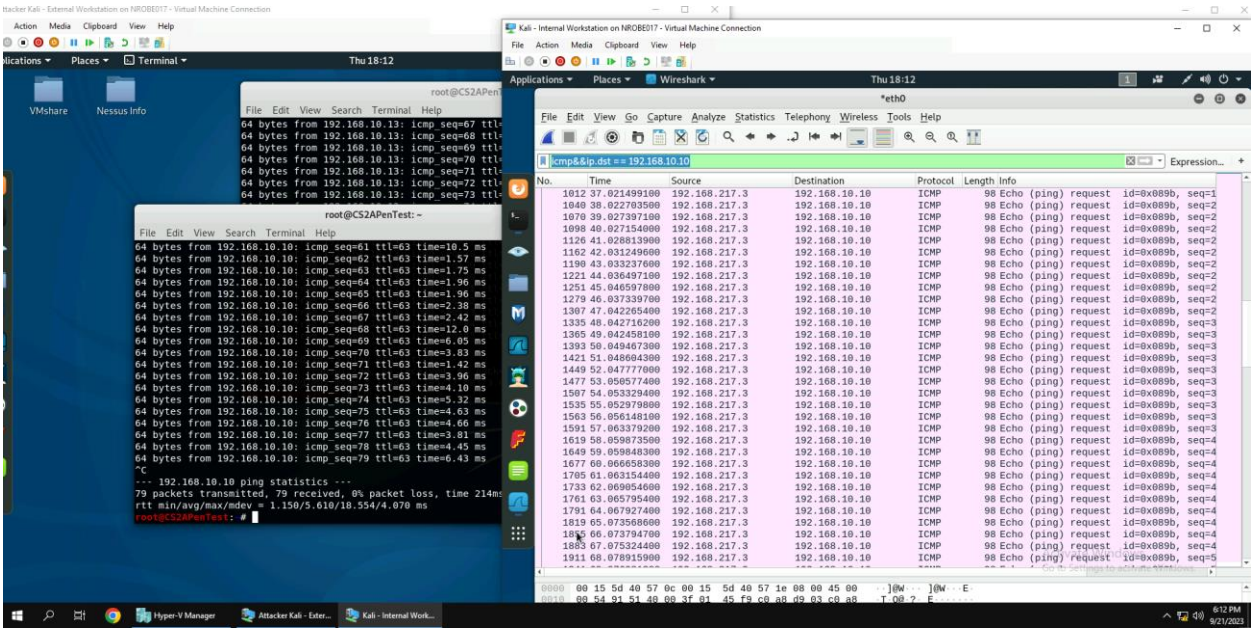
6. 

The source IP and its port number for the response query is 192.168.217.2:53 and the destination IP and its port number is 192.168.217.3:55703. The message that was replied from the DNS server was “refused”.

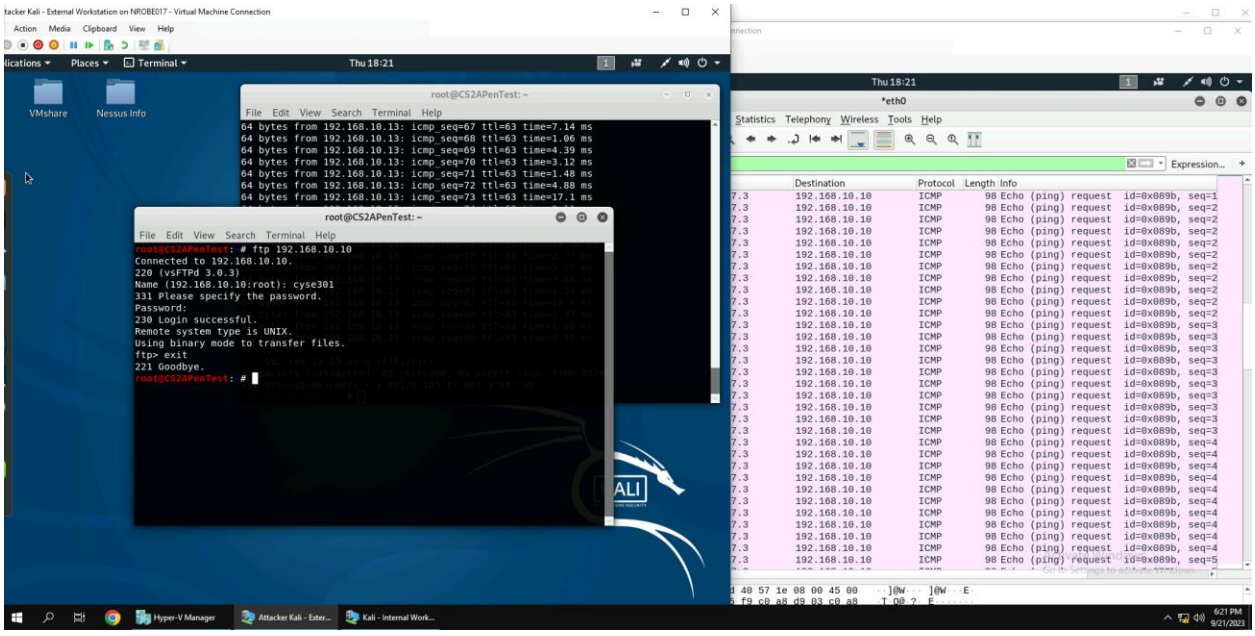
Task B

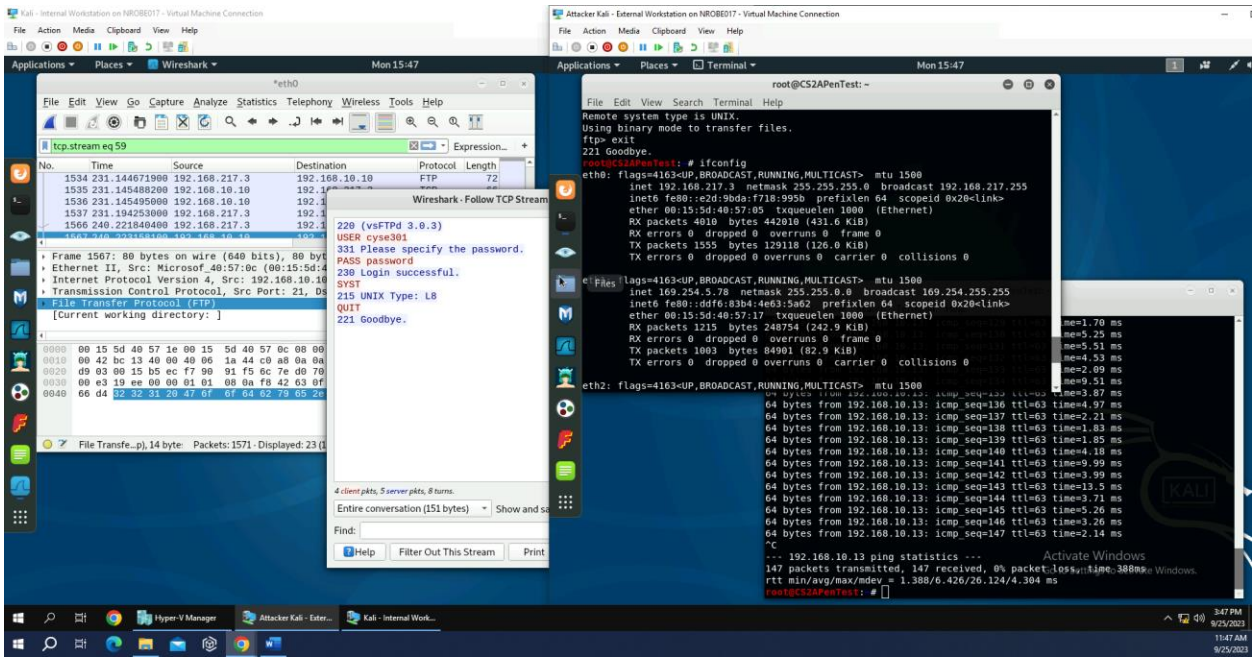
1. Sniff ICMP traffic

a. 

b. 

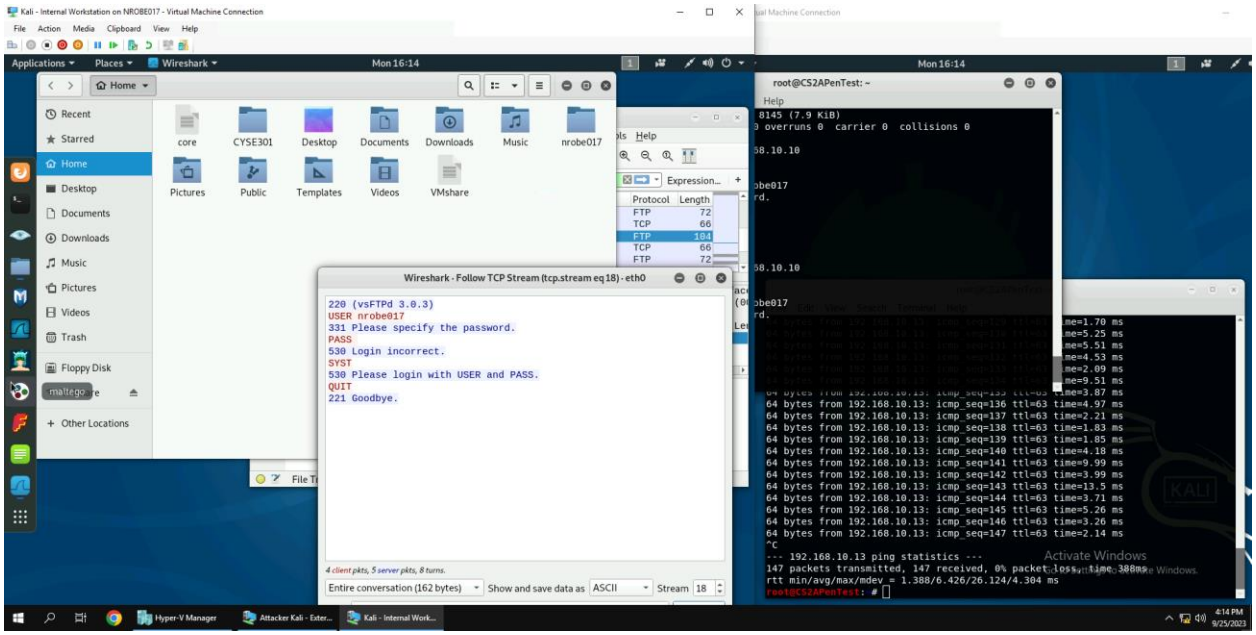
2. Sniff FTP traffic

a. 

b. 

How I was able to find the password used by external kali was to first find the IP address of the external kali using the ifconfig command. Afterword's you go into Wireshark and use the ip.addr == 192.168.217.3, which is the IP address for the external kali system. Before you hit enter in the search bar add && ftp to the end of it, to isolate the fpt packets that is coming and going from the external kali. Then you find one of the packets that has the source IP of the ubuntu virtual machine to the kali virtual machine (which was source: 192.168.10.10, destination: 192.168.217.3), while having the protocol of FTP. You right click on that packet then click follow, and TCP stream and there you will see the password and user.

C.


Kali - Internal Workstation on NROBE017 - Virtual Machine Connection
Wireshark - Follow TCP Stream (tcp.stream eq 18) - eth0
220 (vsFTPd 3.0.3)
USER nrobe017
331 Please specify the password.
PASS
530 Login incorrect.
SYST
530 Please login with USER and PASS.
QUIT
221 Goodbye.
root@CS2APenTest: ~
--- 192.168.10.13 ping statistics ---
147 packets transmitted, 147 received, 0% packet loss, time 388ms
rtt min/avg/max/mdev = 1.388/6.426/26.124/4.304 ms
Activate Windows