OLD DOMINION UNIVERSITY

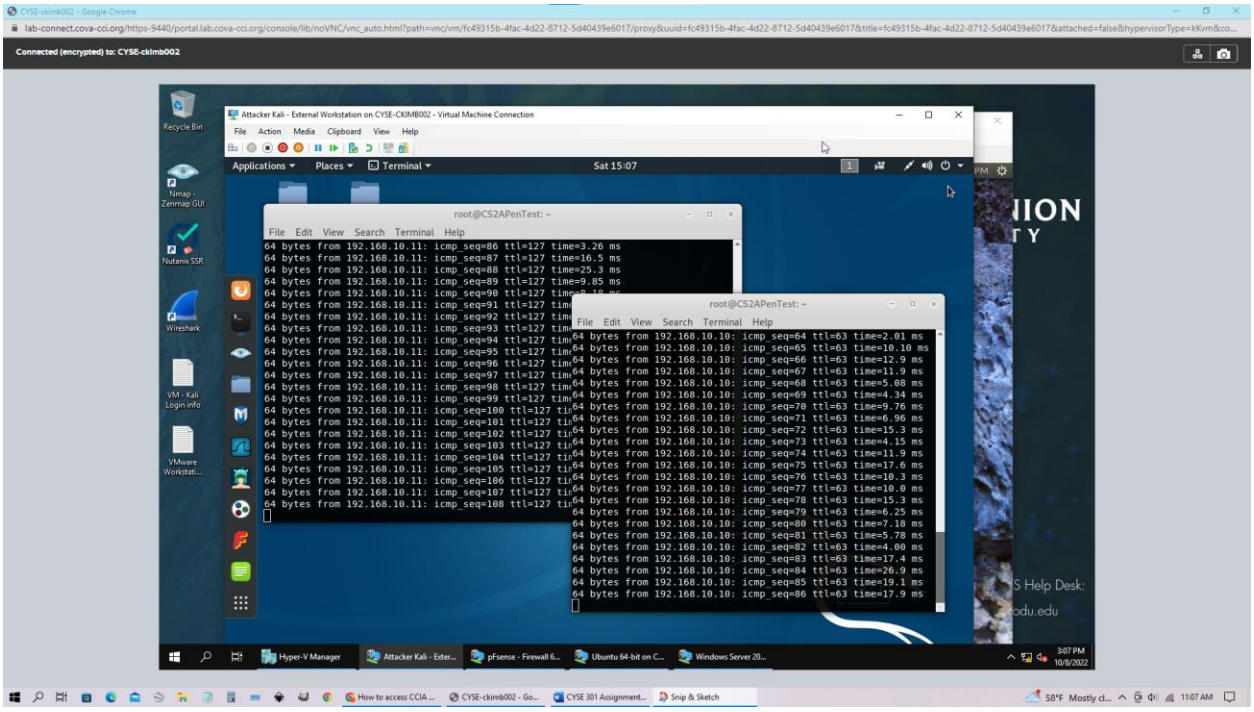
CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

ASSIGNMENT #2 TRAFFIC TRACING AND SNIFFING

Clarence V. Kimbrell Jr.

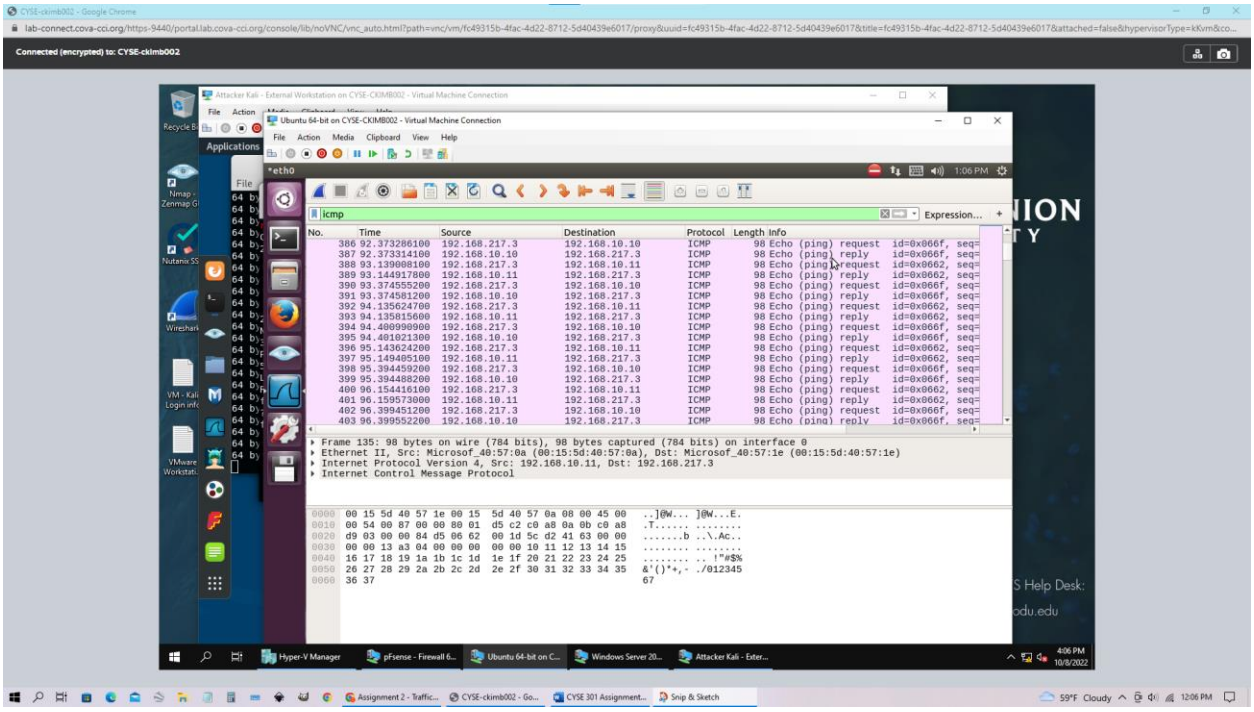
01207106

1.1



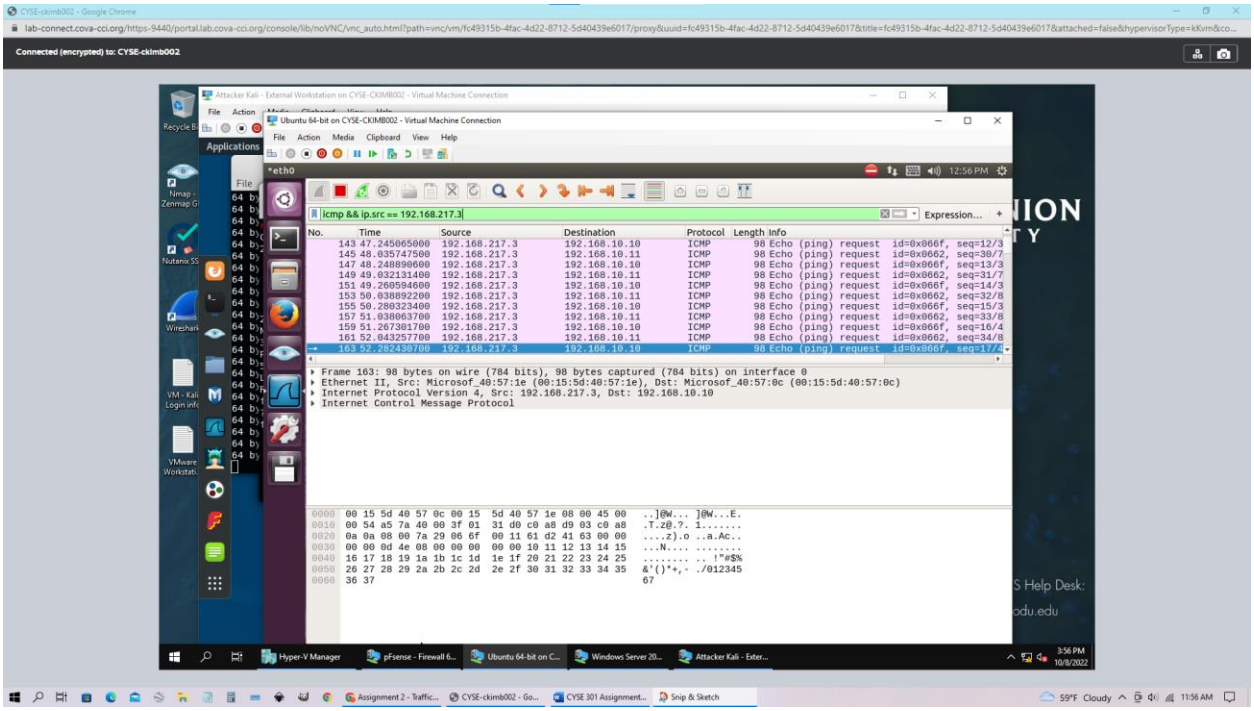
After opening two separate terminals I used the ping command to first window 2008 server and then ubuntu. The servers' IP addresses are very similar the only difference being the last two digits.

1.2



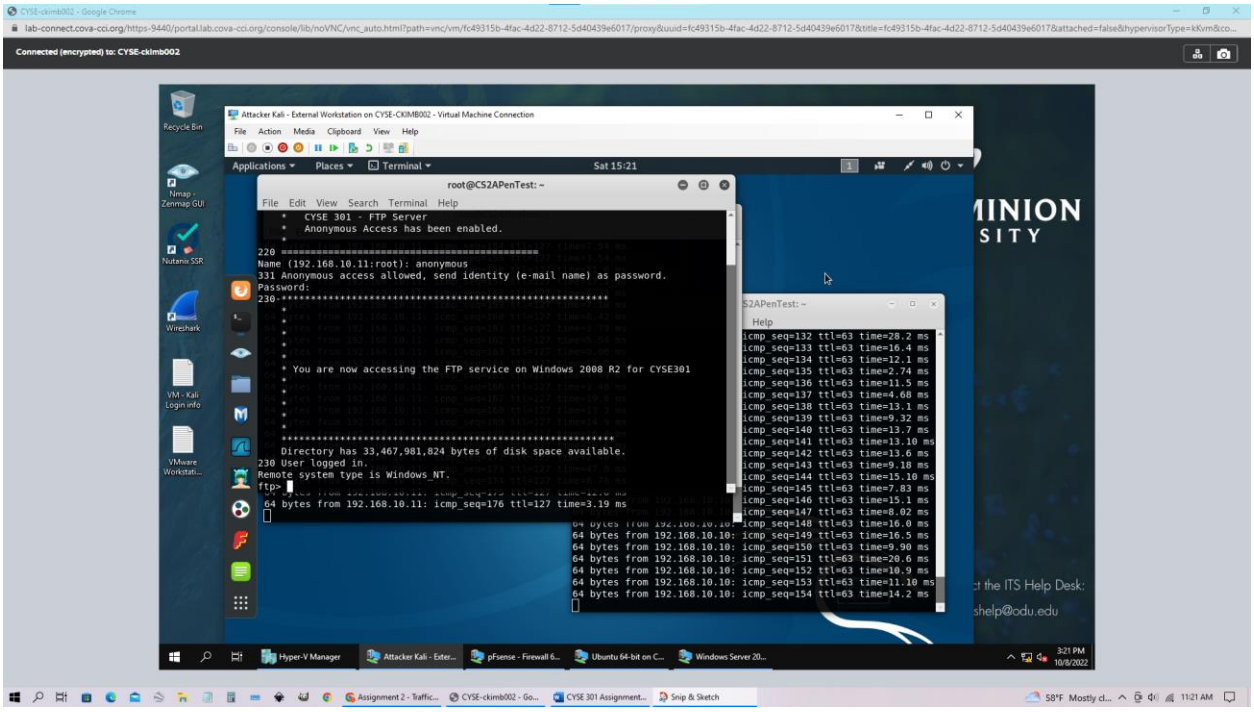
In the Ubuntu VM with Wireshark open, we can filter all ping traffic by using the ICMP filter. We can see where the packets are coming from by looking at the source and destination. As we can see above packets are coming from Ubuntu, Windows Server 2008, and Attacker Kali.

1.3



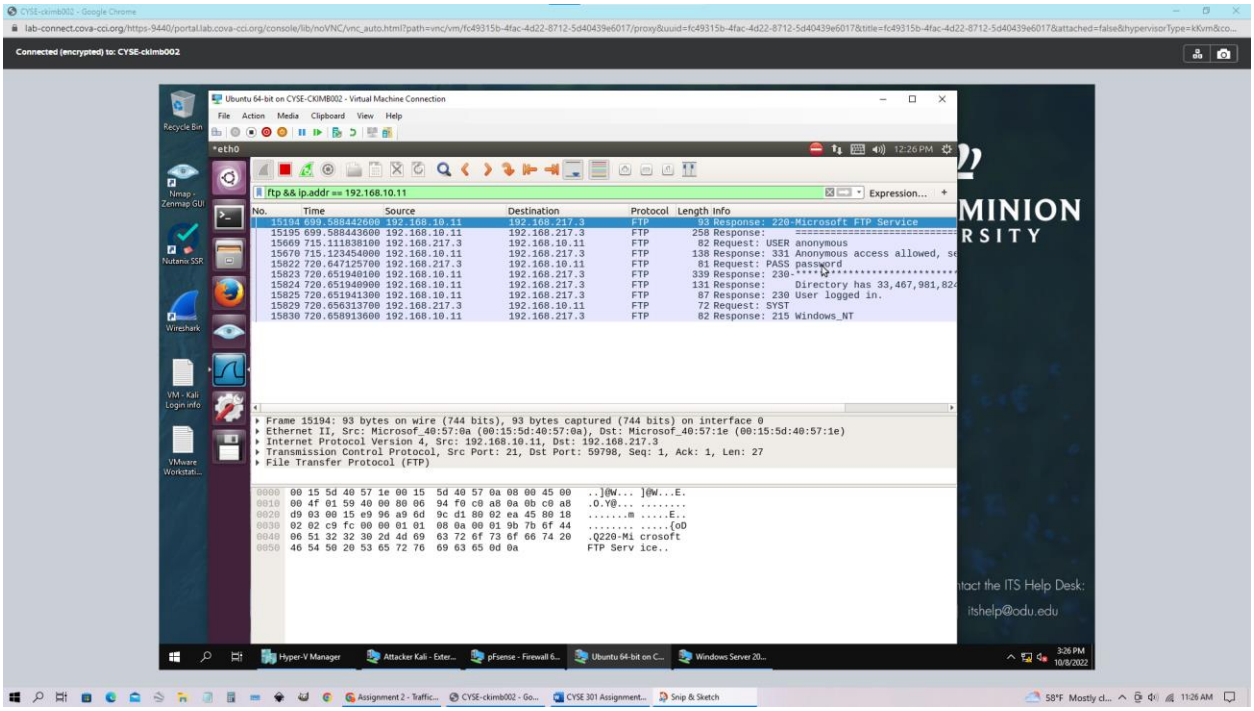
This is a further extension of the filter used in the previous step exploring the source of the packets. This is done but adding IP.src and then the IP address. This shortens the results significantly and is more precise.

2



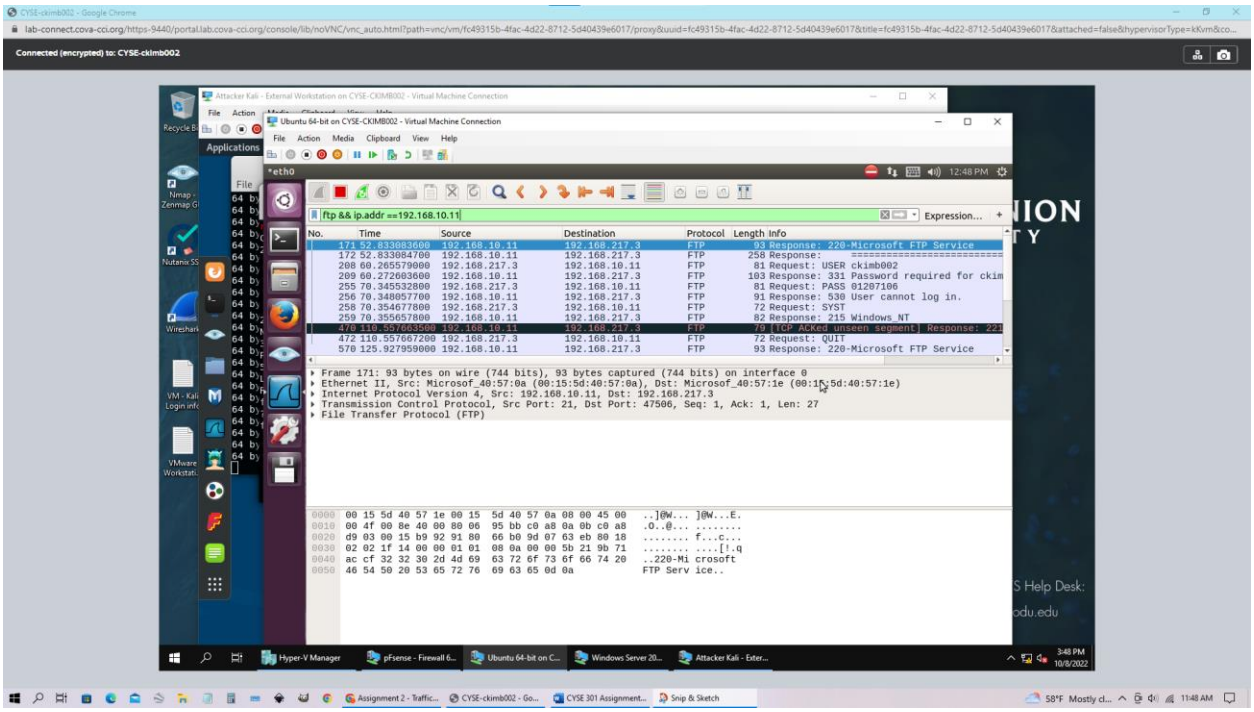
The above image displays a packet from Kali to the Windows server with login credentials. This is done by using the FTP command and then listing the Windows server IP address.

2.1



The command used in the above image is a tool used for sniffing internal communications. This is done by filtering with the same command used to send the information. Then add the IP address it was sent to in this case it was the windows server. Finally, the information is displayed in the info tab showing the username and password.

2.2



This was done in a very similar manner to the above image. But in this case, it simulates a real-world scenario by using a username and password that is not given to us. Although I was not able to log in with this information, I was still able to sniff the packets on the attack Wireshark in Ubuntu. Which displays my username which is my MIDAS ID and my password which was my UIN.