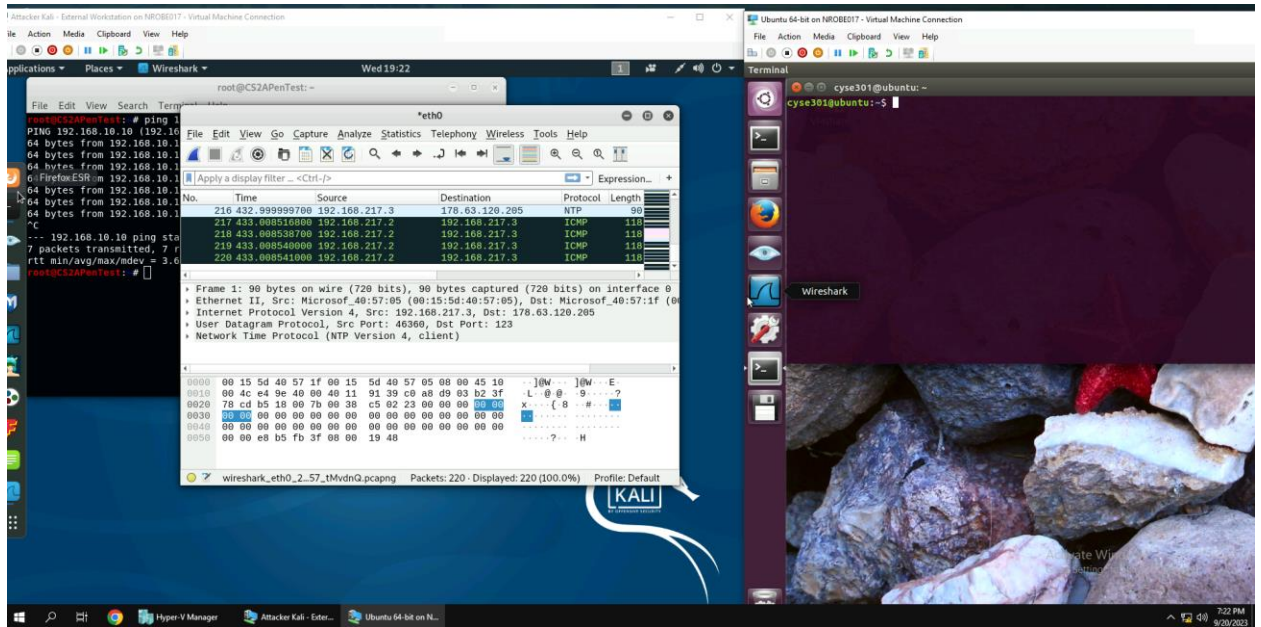


Nicholas Robertson

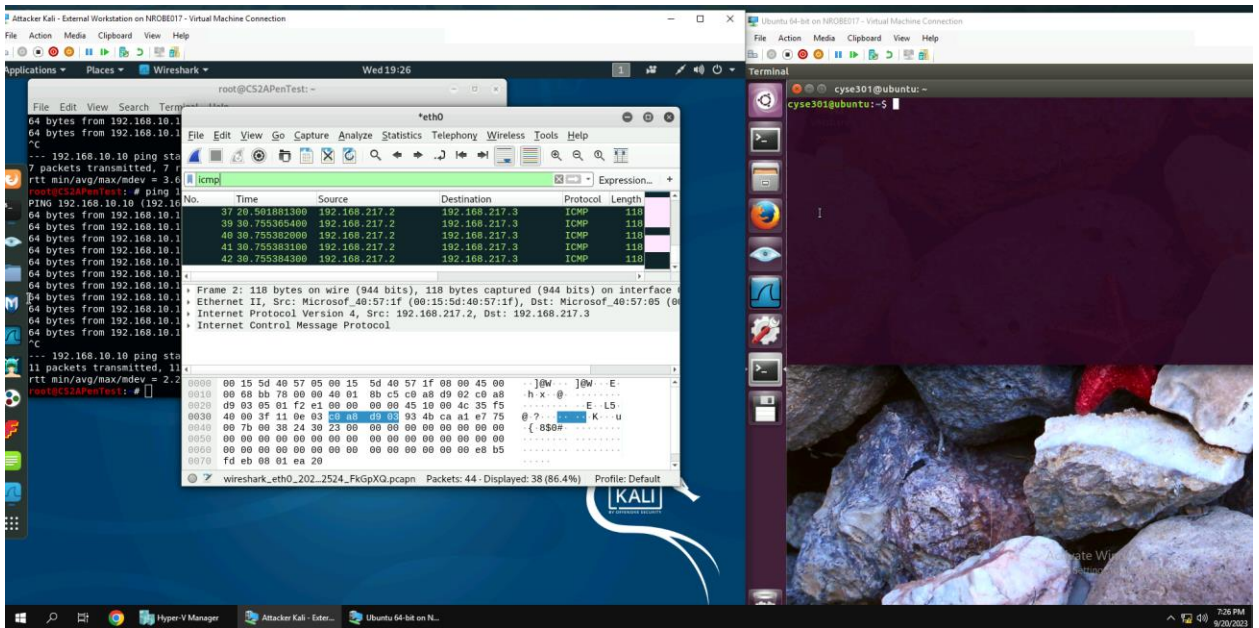
Assignment #2

Task A



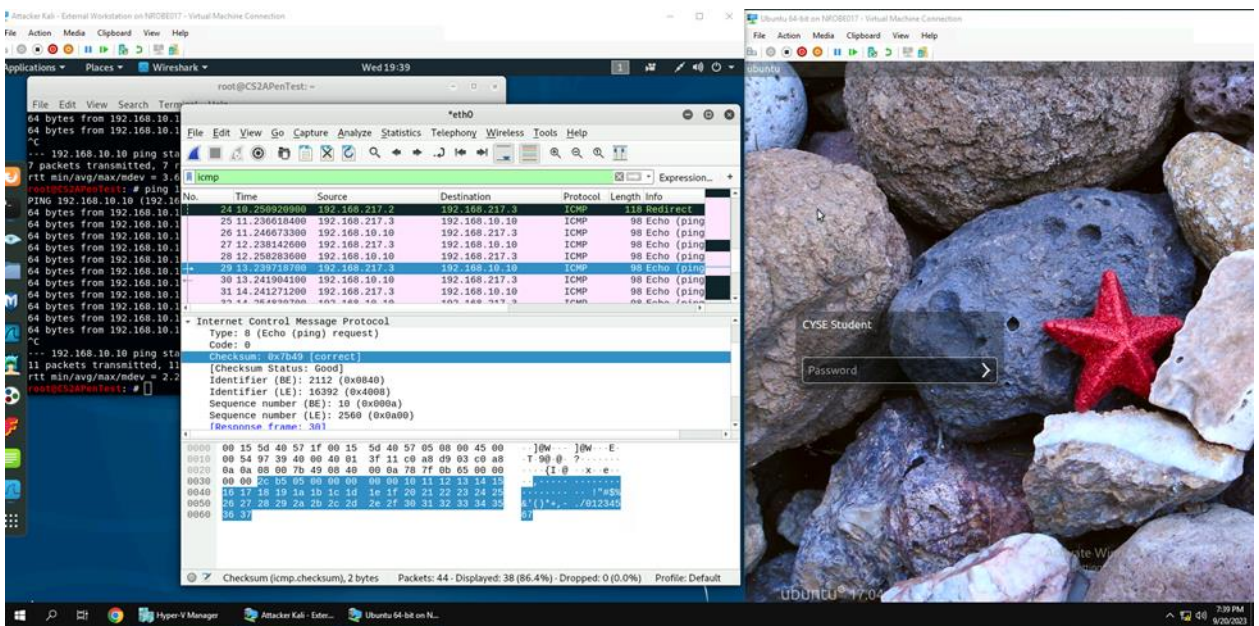
1.

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



2.

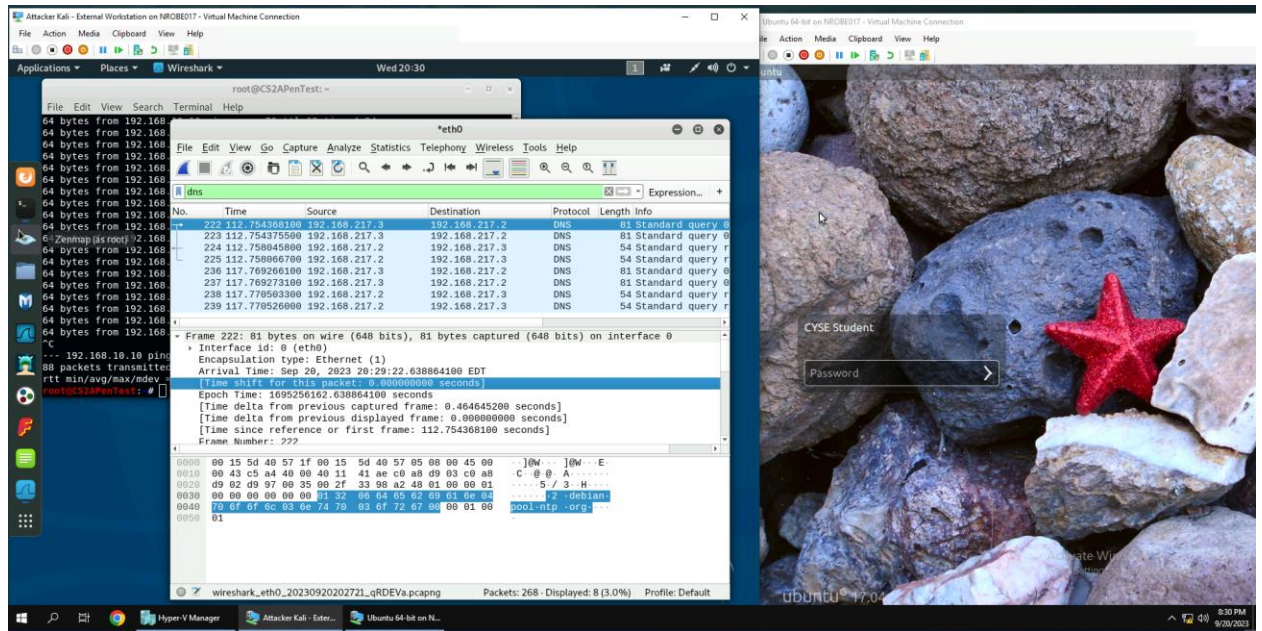
After applying “ICMP” in the display filter, there was a total of 44 packets captured with 38 of those packets being displayed.



3.

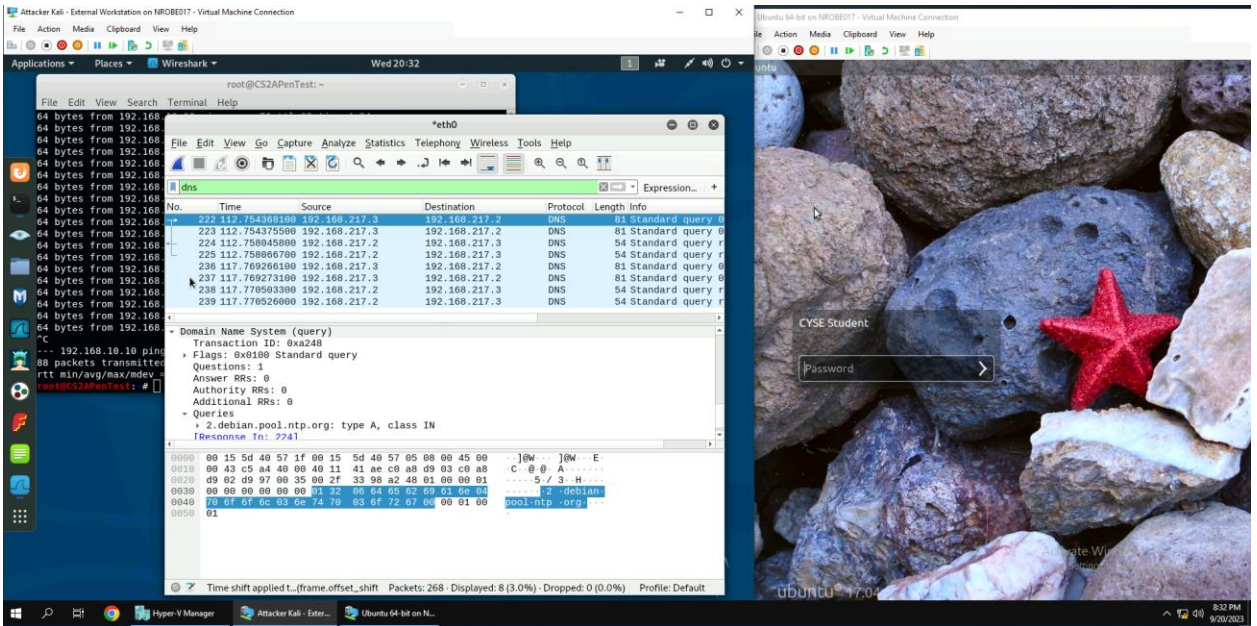
With the filter still on the source IP address is 192.168.217.3 and the destination IP is 192.168.10.10. The sequence number (BE) is 10 and the sequence number (LE) is 2560.

The size of the data is 48 bytes and the response time was 13.559 ms.



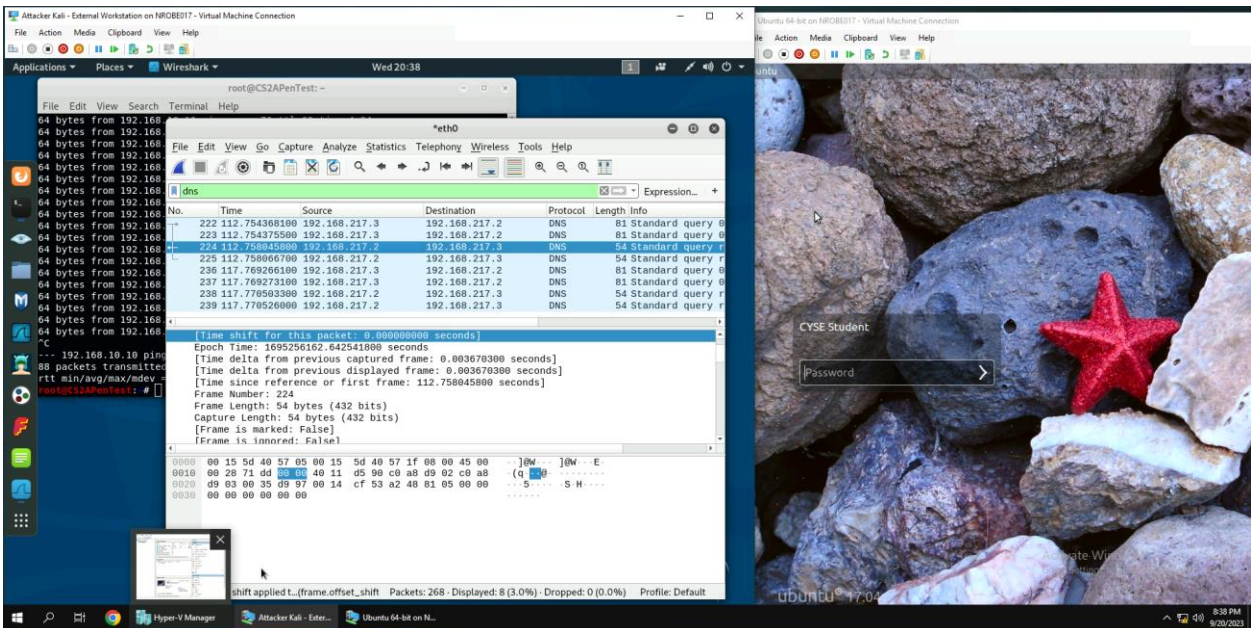
4.

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.

The screenshot displays a Kali Linux virtual machine environment with three main windows:

- Terminal (root@CS2APent):** Shows a series of ICMP echo requests from 192.168.10.10 to 192.168.10.13. The output for each request is: "64 bytes from 192.168.10.13: icmp_seq=115 ttl=63 time=16.1 ms" through "icmp_seq=136".
- Wireshark:** Shows a list of captured ICMP Echo (ping) packets. The table below summarizes the visible entries:

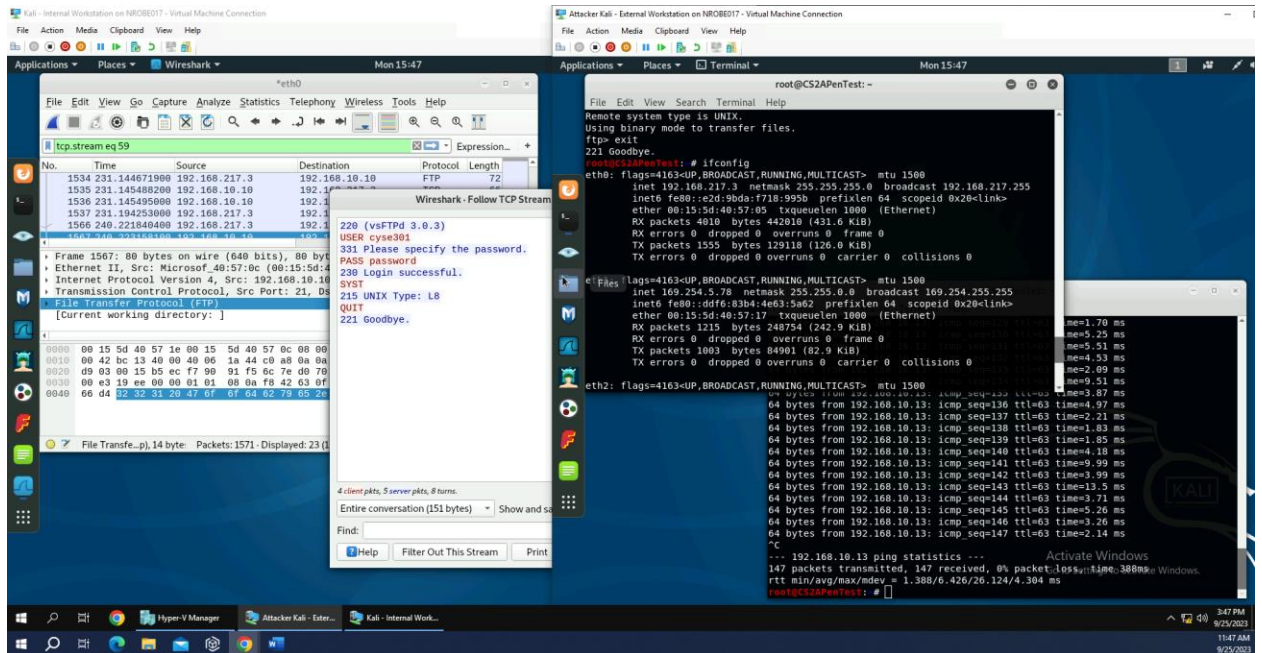
No.	Time	Source	Destination	Protocol	Length	Info
1250	43.928529160	192.168.10.10	192.168.217.3	ICMP	98	Echo
1283	44.660945700	192.168.217.3	192.168.10.13	ICMP	98	Echo
1284	44.660993200	192.168.10.13	192.168.217.3	ICMP	98	Echo
1285	44.933647800	192.168.217.3	192.168.10.10	ICMP	98	Echo
1286	44.933837000	192.168.10.10	192.168.217.3	ICMP	98	Echo

The detailed view of the selected packet (No. 17) shows it is an Internet Control Message Protocol (ICMP) Echo (ping) packet. The source is 192.168.217.3 and the destination is 192.168.10.13. The packet structure is shown in hexadecimal and ASCII below:

```
0000 00 15 5d 40 57 03 00 15 5d 40 57 1e 08 00 45 00  ...|@|...|...|E|
0010 00 54 67 60 40 00 3f 01 6f e7 c0 a8 d9 03 50 15  ...|Tg|@?|0...|...|
0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...|...|...|...|...|
0030 00 00 94 04 02 00 00 00 00 10 11 12 13 14 15  ...|...|...|...|...|
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  ...|...|...|...|...|
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  ...|...|...|...|...|
0060 36 37
```

The interface configuration for eth0 is also visible:

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 169.254.44.122 netmask 255.255.0.0 broadcast 169.254.255.255
inet6 fe80::448b:e8b9:6038:1b1d prefixlen 64 scopeid 0x20<link>
ether 00:15:5d:40:57:15 txqueuelen 1000 (Ethernet)
RX packets 209 bytes 64199 (62.0 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

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 ftp 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.

