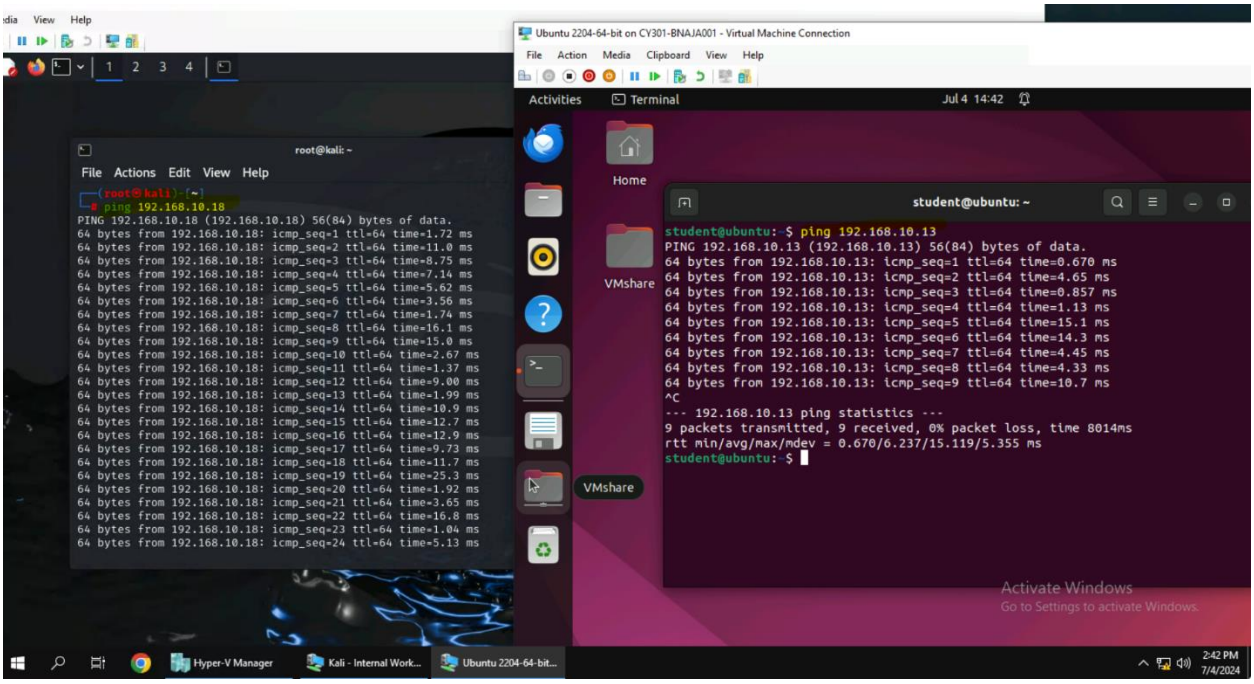
Assignment 2 Report

Traffic Tracing and Sniffing

Each student needs to login into the CCIA virtual environment to complete this assignment. Please make sure to power on the pfsense VM at all times to keep the VMs connected.

Task A: Get started with Wireshark (5 point each x 6 questions = 30 points)

In this task, you will be using Wireshark on External Kali to monitor the traffic when External Kali and Ubuntu VM are talking to each other.



You should keep Wireshark running in the background while performing the following tasks.

1. Open Wireshark on External Kali and listen on interface “eth0”.

2. Open a new terminal, then ping the Ubuntu VM for 5 – 10 seconds.

3. Open a new web browser tab in Kali Linux (even if no webpage will be displayed), and keep it for

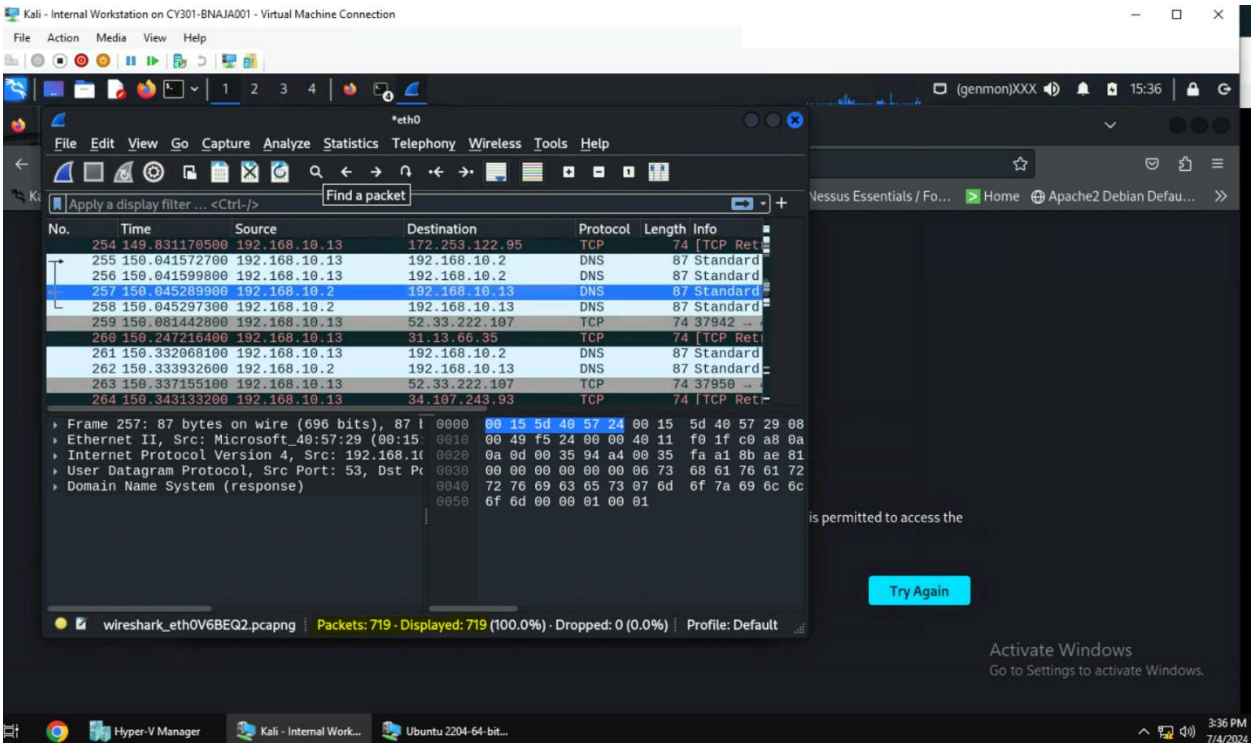
a couple of seconds.

4. Stop capturing (the red button on the tool bar).

Now, answer the following questions. You need to provide a screenshot that contains the answers

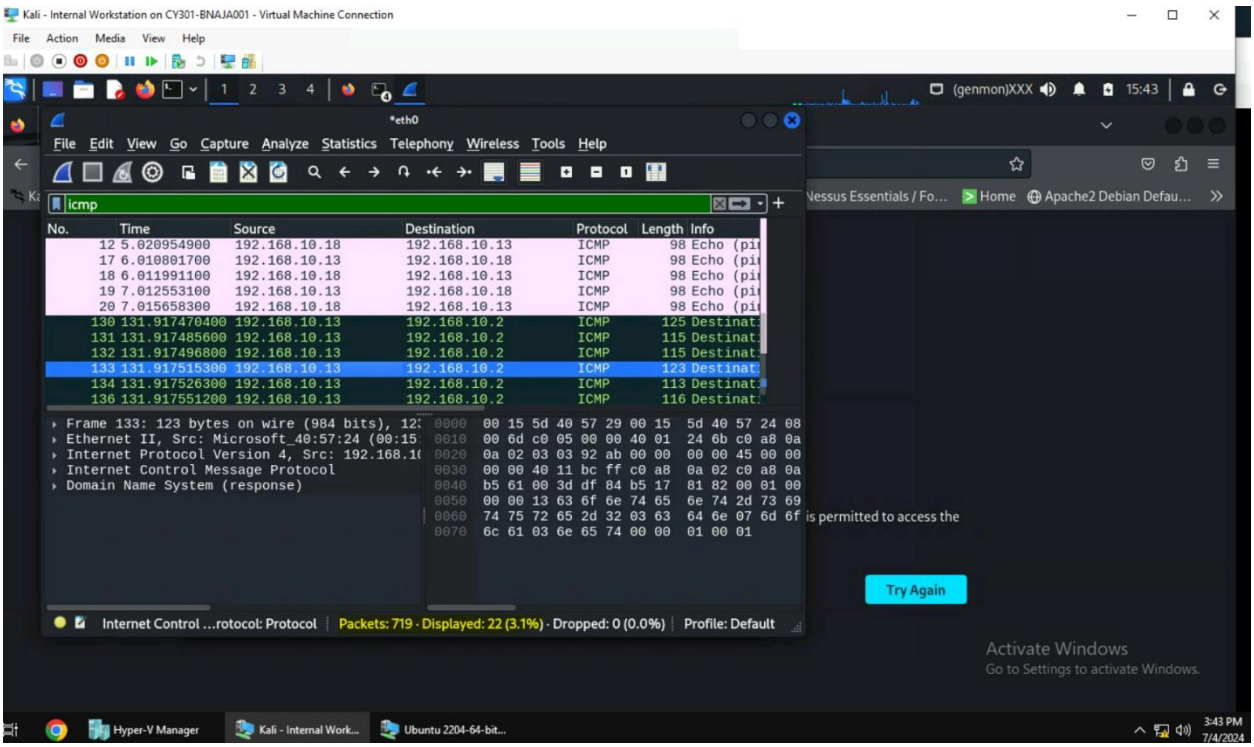
to each question.

Q1. How many packets are captured in total? How many packets are displayed?



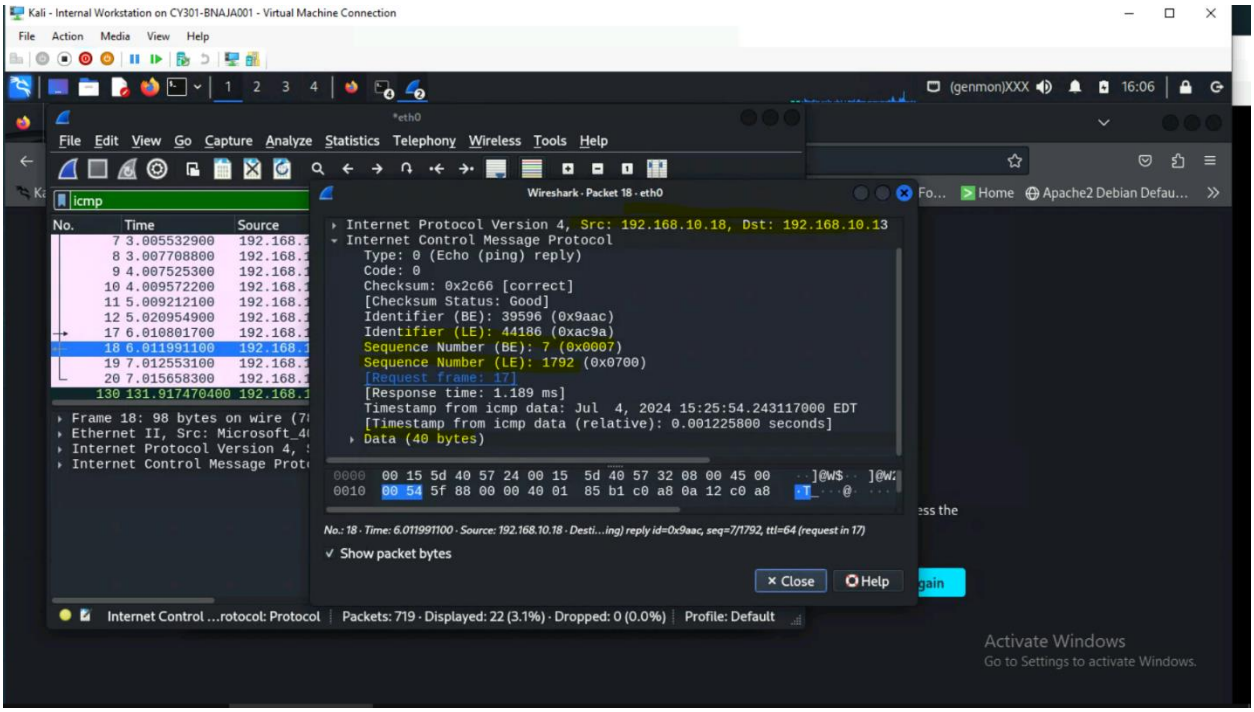
I was running for 1 minutes and captured 719 packets and displayed 719.

Q2. Apply “ICMP” as a display filter in Wireshark. Then repeat the previous question (Q1).



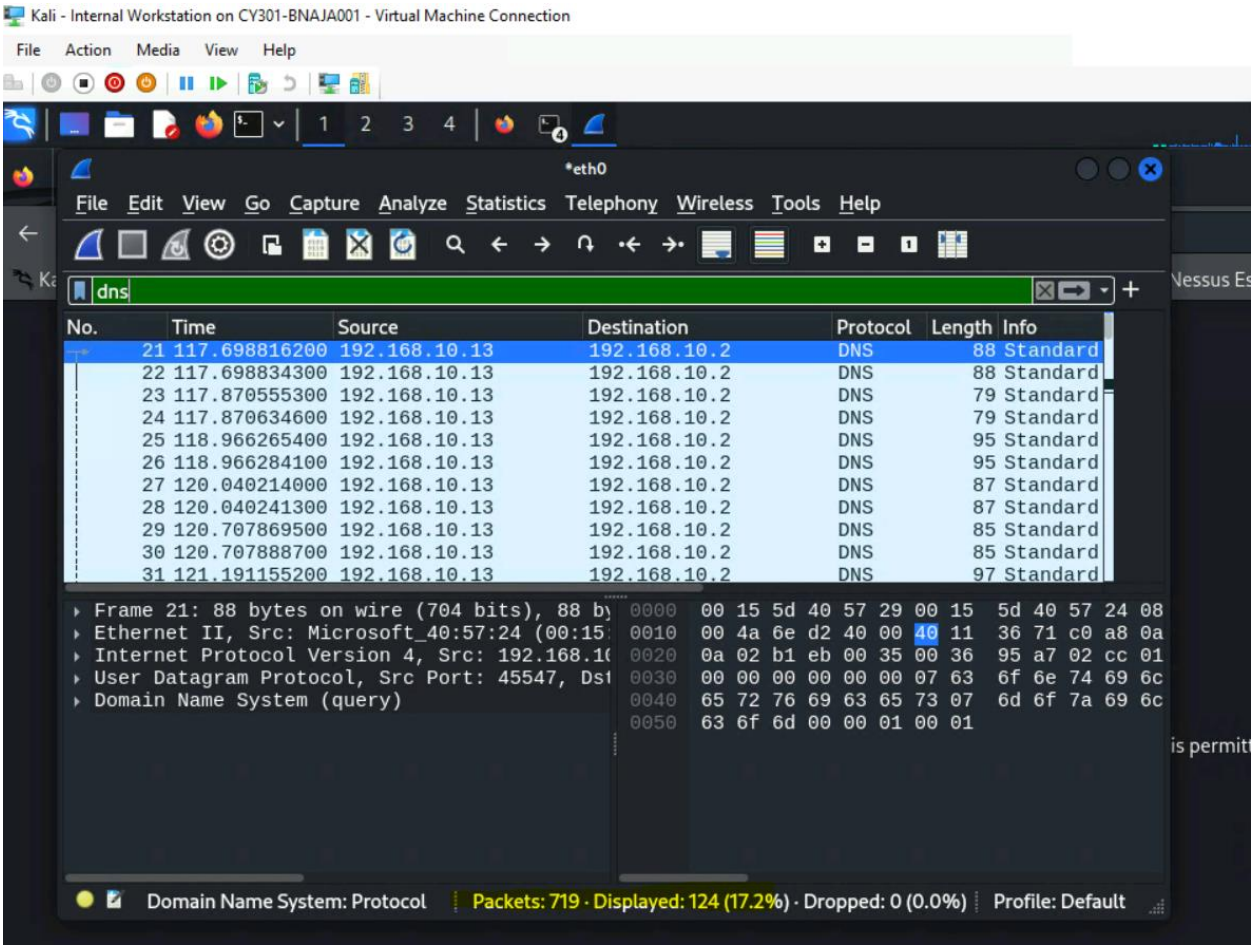
When I applied ICMP displayed packet changed to 22 and packets still the same 719.

Q3. Select an Echo (replay) message from the list. What are the source and destination IPs of this packet? What are the sequence number and the size of the data? What is the response time?



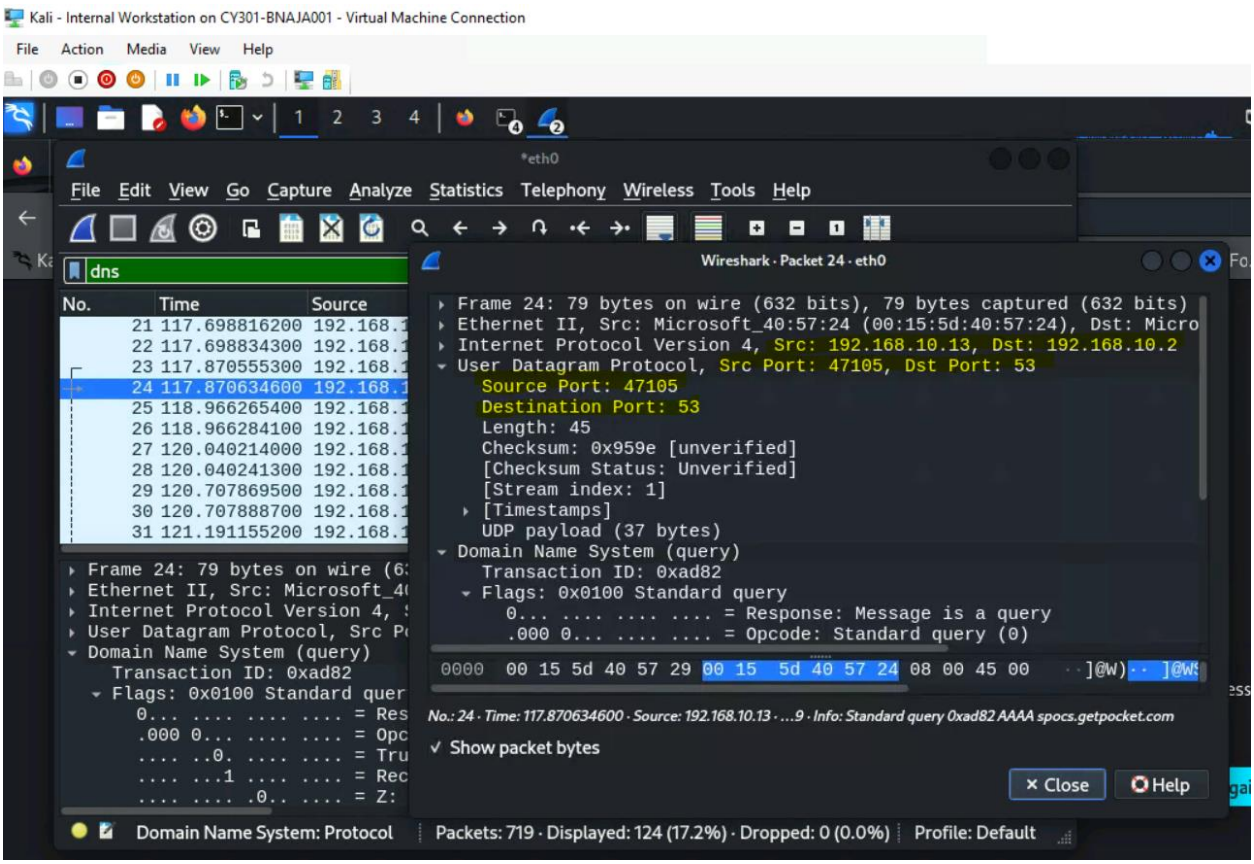
The Source is 192.163.10.18 and destination is 192.168.10.13. the sequence number (BE) is 7 and (LE) is 1792 and size of the data is 40 bytes. The respond time 1.189 millisecond.

Q4. Apply “DNS” as a display filter in Wireshark. How many packets are displayed?



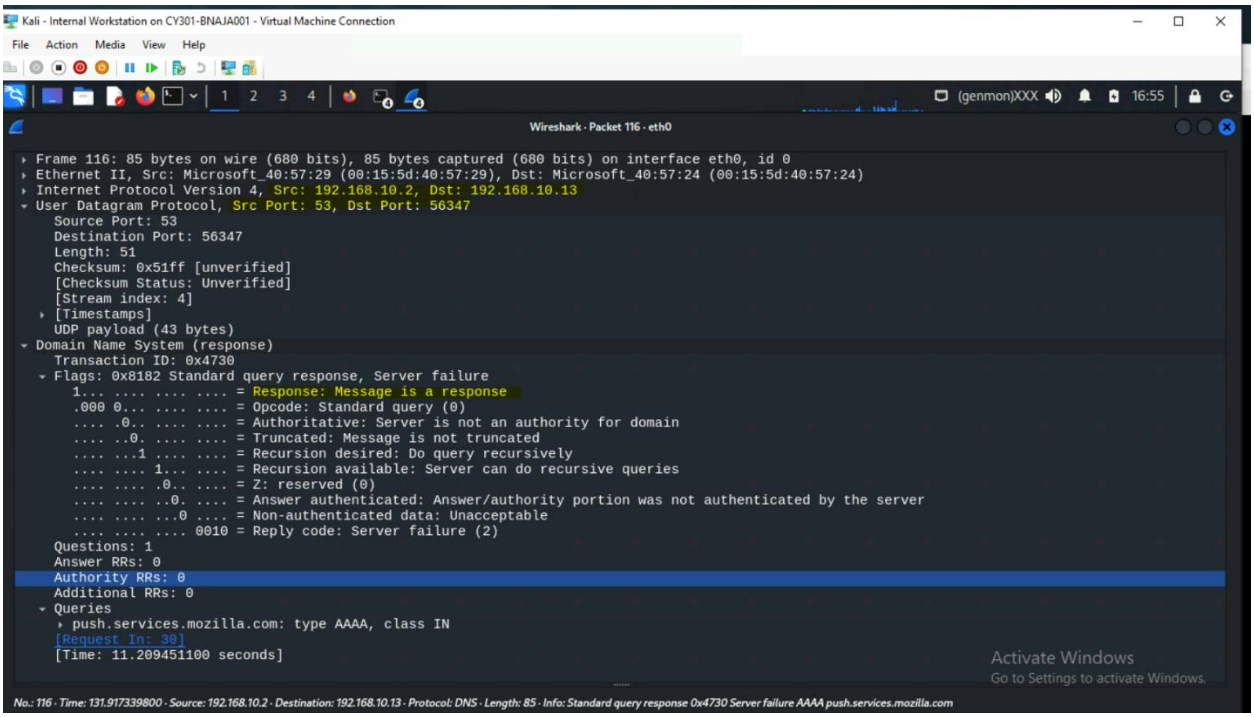
Above I highlighted Pckets:719 and Displayed: 124

Q5. Find a DNS query packet. What is the domain name this host is trying to resolve? What is the source IP and port number, destination IP and port number? Please express in the format: IP:port.



Above on the screenshot I highlighted the source IP and port number, destination IP and port number.

Q6. Find the corresponding DNS response to the query you selected at the previous step, and what is the source IP and port number, destination IP and port number? What is the message replied from the DNS server?

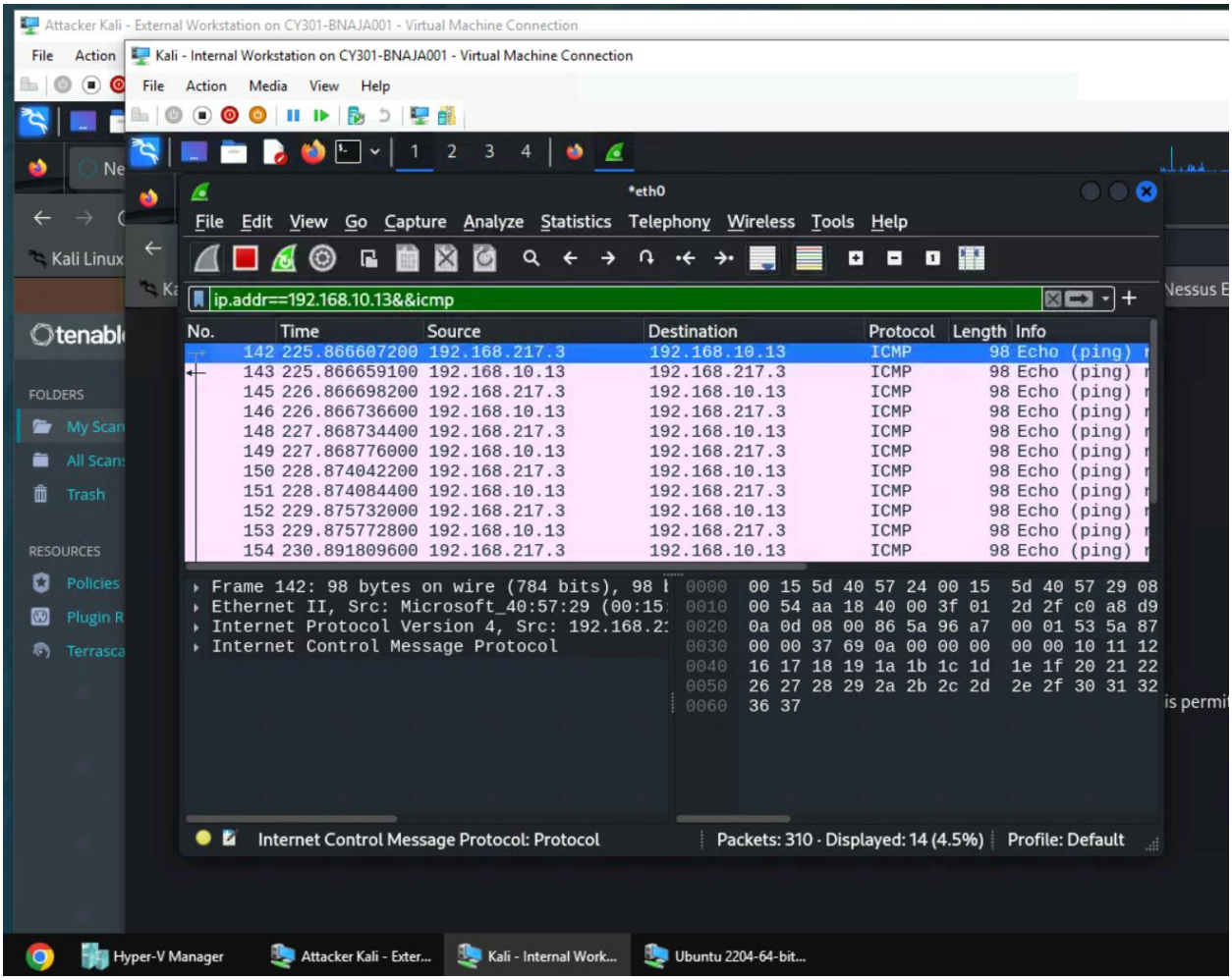


Task B: Sniff LAN traffic

1. Sniff ICMP traffic (10 + 10 = 20 points)

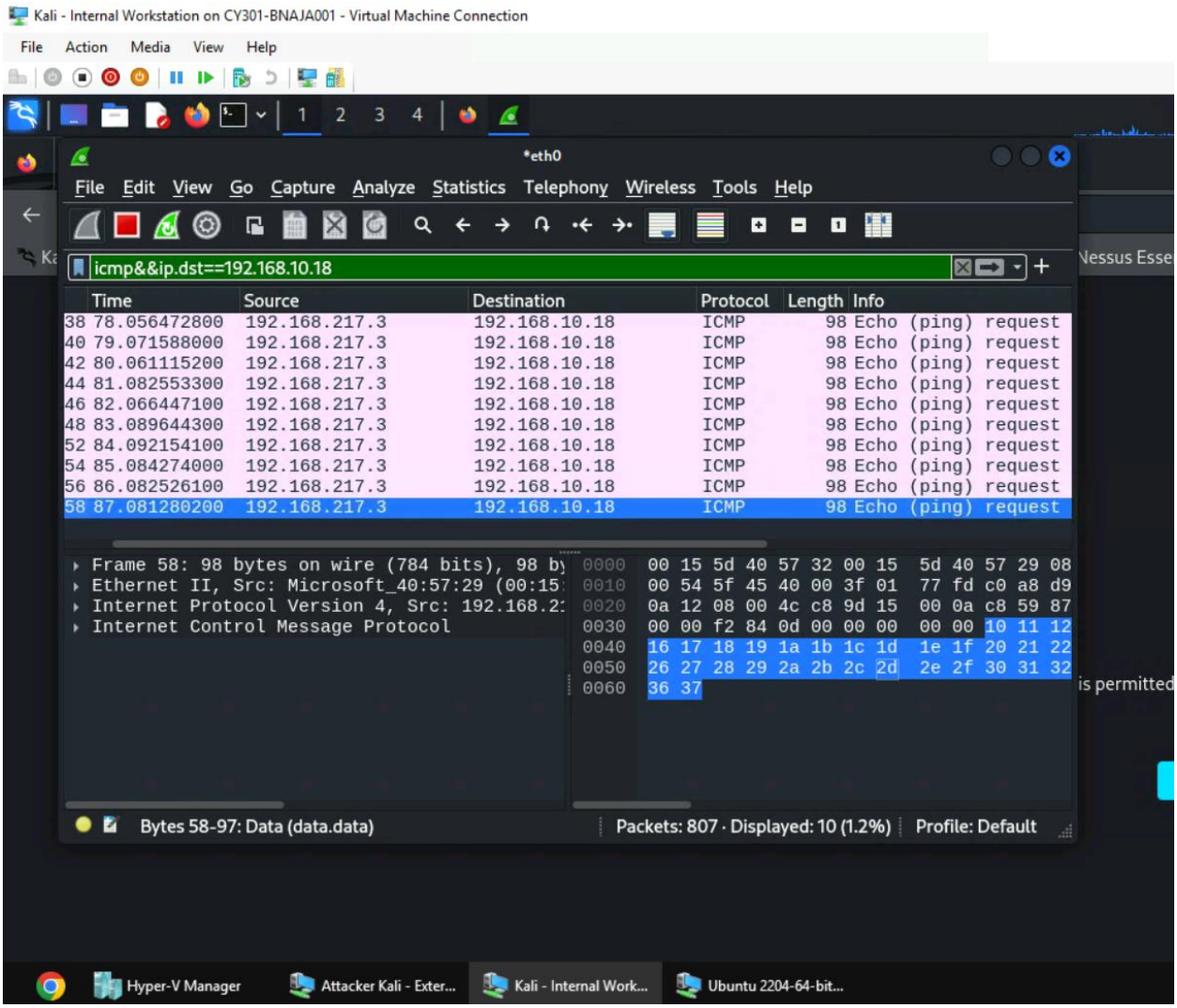
Open two terminals on External Kali VM. Use one ping Ubuntu VM, and use the other ping Internal Kali.

a. Apply proper display or capture filter on Internal Kali VM to show active ICMP traffic.



To see the traffic from the internal kali and the attacker, I used command (ip.addr==192.168.10.13&&icmp), to display the traffic.

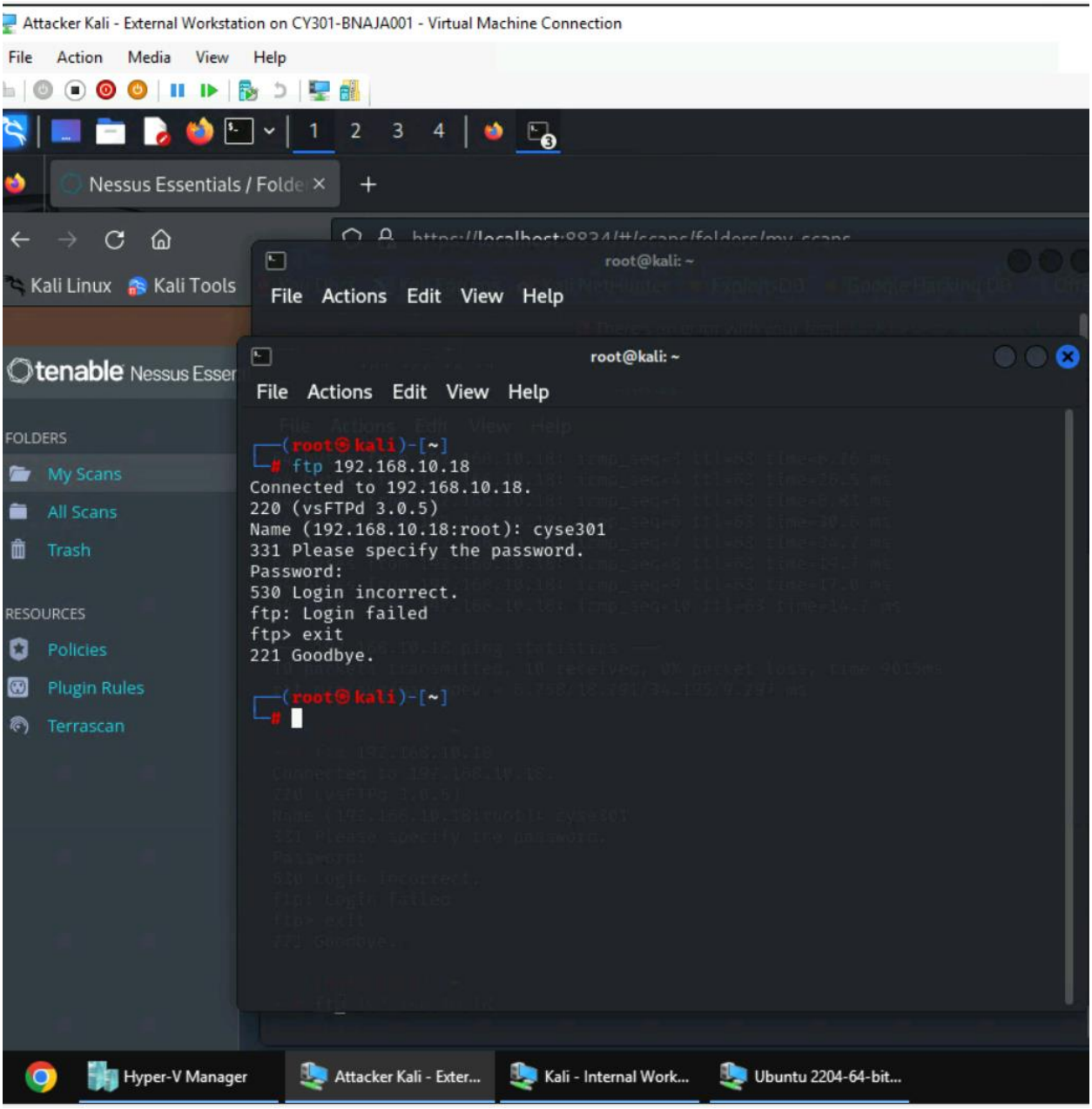
b. Apply a proper display or capture filter on the internal Kali VM that ONLY displays the ICMP request that originated from the external Kali VM and goes to the Ubuntu 64-bit VM.



The screenshot shows on display filter Wireshark the exact command that ONLY displays the ICMP request that originated from the external Kali VM

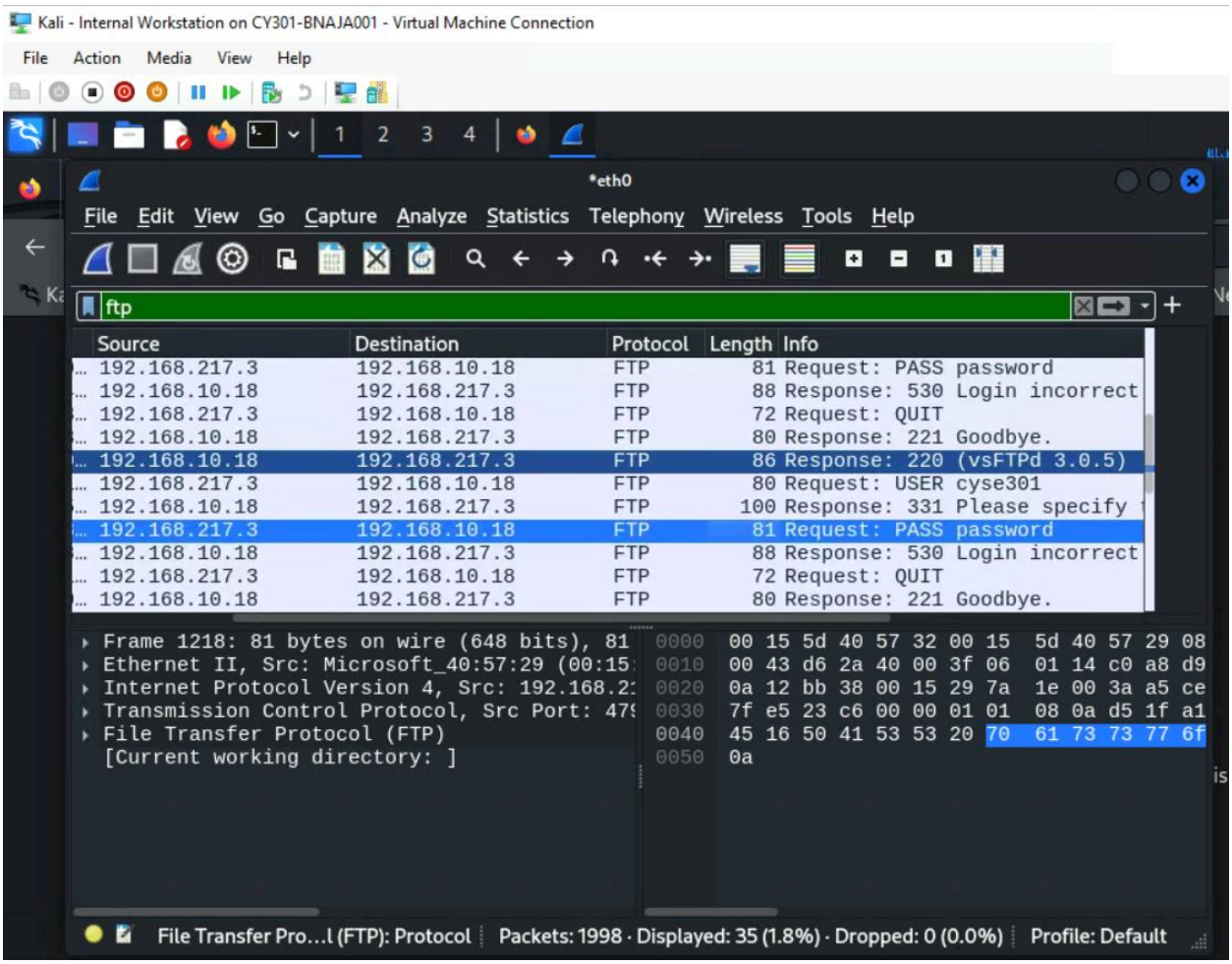
2. Sniff FTP traffic (10 + 15 + 15 = 40 pts points)

a. Ubuntu VM is also serving as an FTP server inside the LAN network. Now, you need to use External Kali to access this FTP server by using the command: ftp [ip_addr of ubuntu VM]. The username for the FTP server is cyse301, and the password is password. You can follow the steps below to access the FTP server.



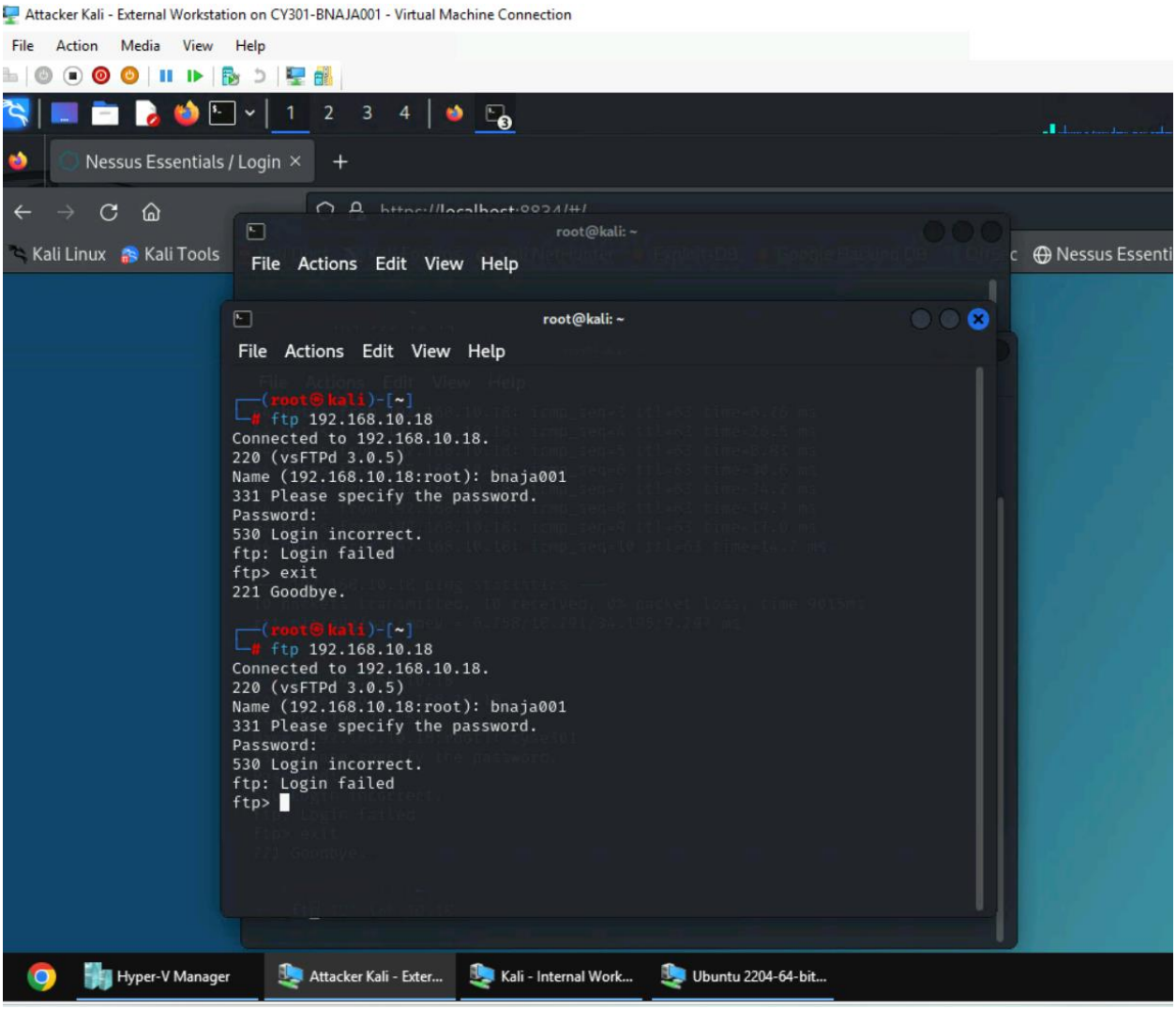
I don't know, if I open the wrong terminal but every time I tried it, it says incorrect login, I can't move forward, see the screenshot above.

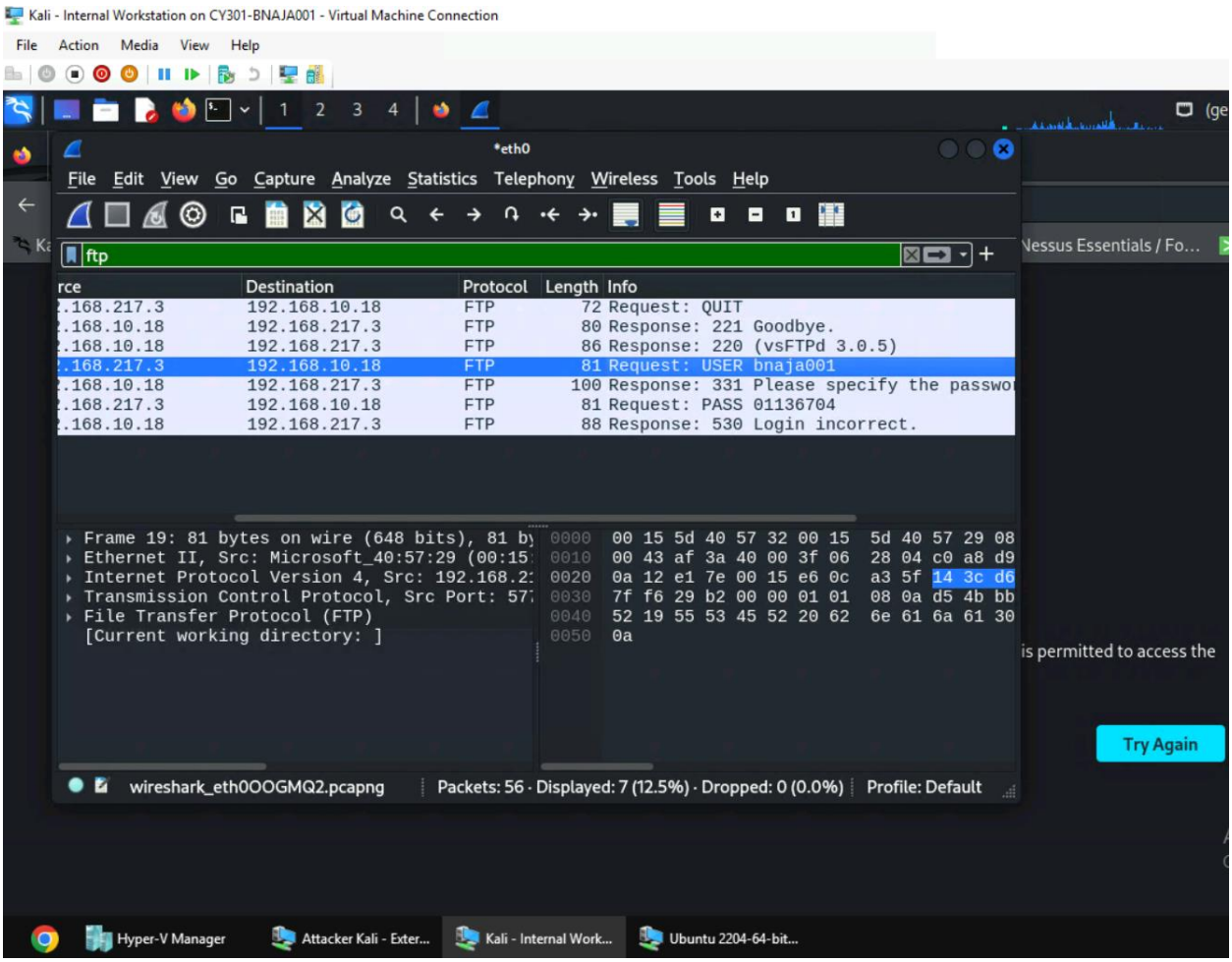
b. Unfortunately, Internal Kali, the attacker, is also sniffing into the communication. Therefore, all of your communication is exposed to the attacker. Now, you need to find out the password used by External Kali to access the FTP server from the intercepted traffic on Internal Kali. You need to take a screenshot and explain how you found the password.



I use ftp to display the data that is store in external kali, as a result login is incorrect. I believe I am doing something wrong I don't know what it is.

c. After you successfully find the username & password from the FTP traffic, repeat the previous step (2.a), and use your MIDAS ID as the username and UIN as the password to reaccess the FTP server from External Kali. Although External Kali may not access the FTP server, you need to intercept the packets containing these "secrets" from the attacker VM, which is Internal Kali.


Attacker Kali - External Workstation on CY301-BNAJA001 - Virtual Machine Connection
File Action Media View Help
Nessus Essentials / Login
Kali Linux
Kali Tools
root@kali: ~
File Actions Edit View Help
root@kali: ~
File Actions Edit View Help
(root㉿kali)-[~]
ftp 192.168.10.18
Connected to 192.168.10.18.
220 (vsFTPd 3.0.5)
Name (192.168.10.18:root): bnaja001
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp> exit
221 Goodbye.
(root㉿kali)-[~]
ftp 192.168.10.18
Connected to 192.168.10.18.
220 (vsFTPd 3.0.5)
Name (192.168.10.18:root): bnaja001
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp>
Hyper-V Manager
Attacker Kali - Exter...
Kali - Internal Work...
Ubuntu 2204-64-bit...



Same thing happened when I tried my MIDAS ID.