OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #2 – Traffic Tracing and Sniffing

My Nguyen

01277464

February 19, 2025

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

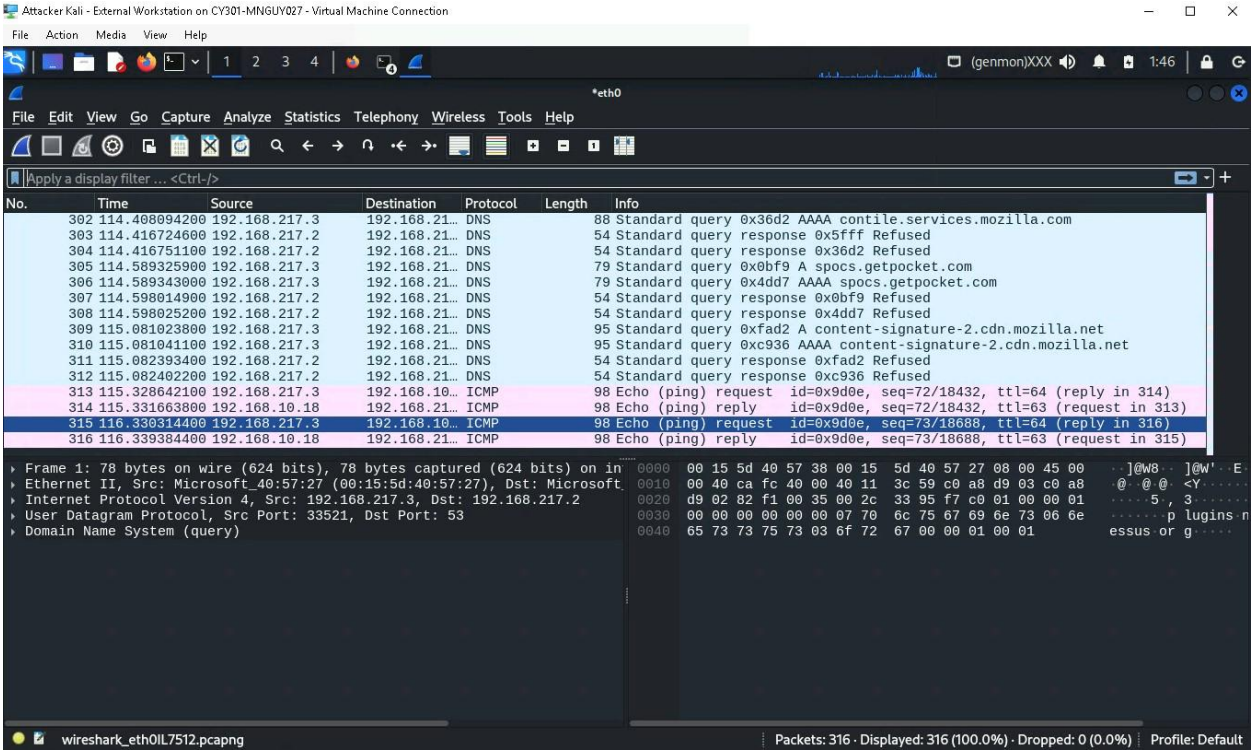
In this task, you will be using Wireshark on External Kali to monitor the traffic when External Kali and Ubuntu VM are talking to each other.

Tip: Please power on the pfsense VM and DO NOT revert to a previous checkpoint. You should keep Wireshark running in the background while performing the following tasks.

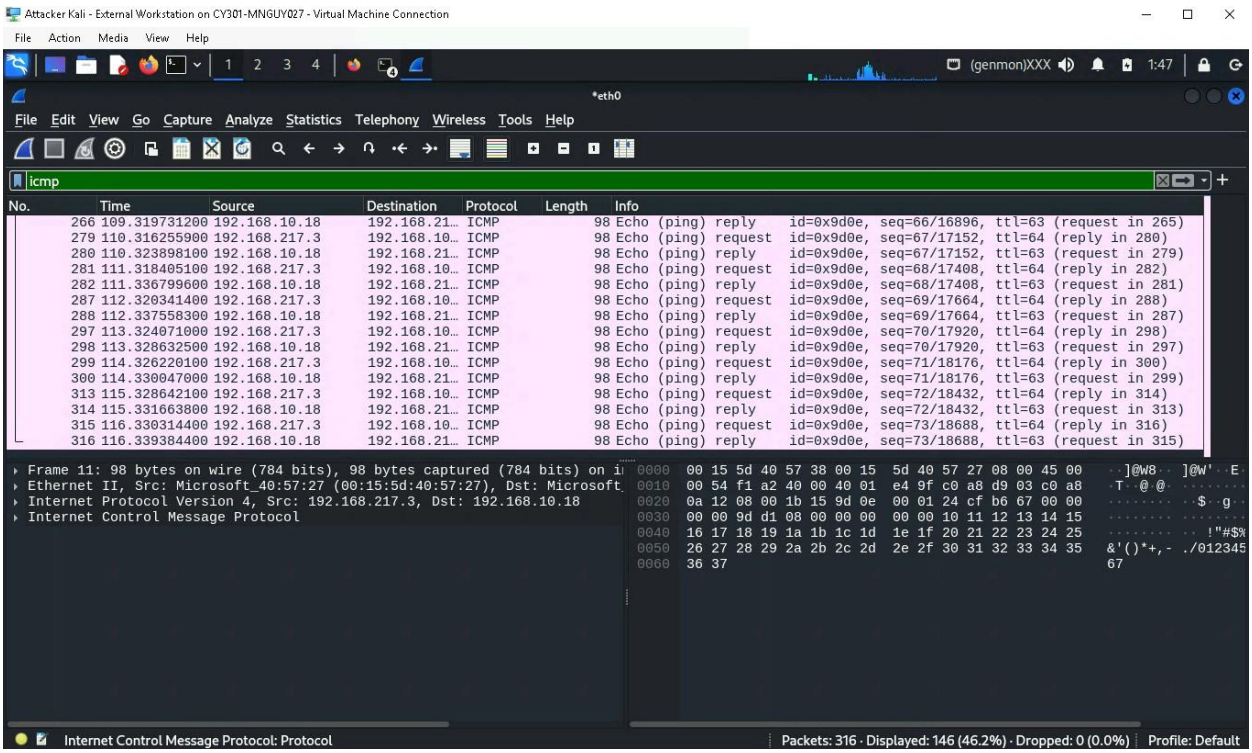
1. Open Wireshark on External Kali and listen on interface “eth0”.
2. Open a new terminal then ping Ubuntu VM for 5 – 10 seocnds.
3. Stop capturing (the red button on the tool bar).

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

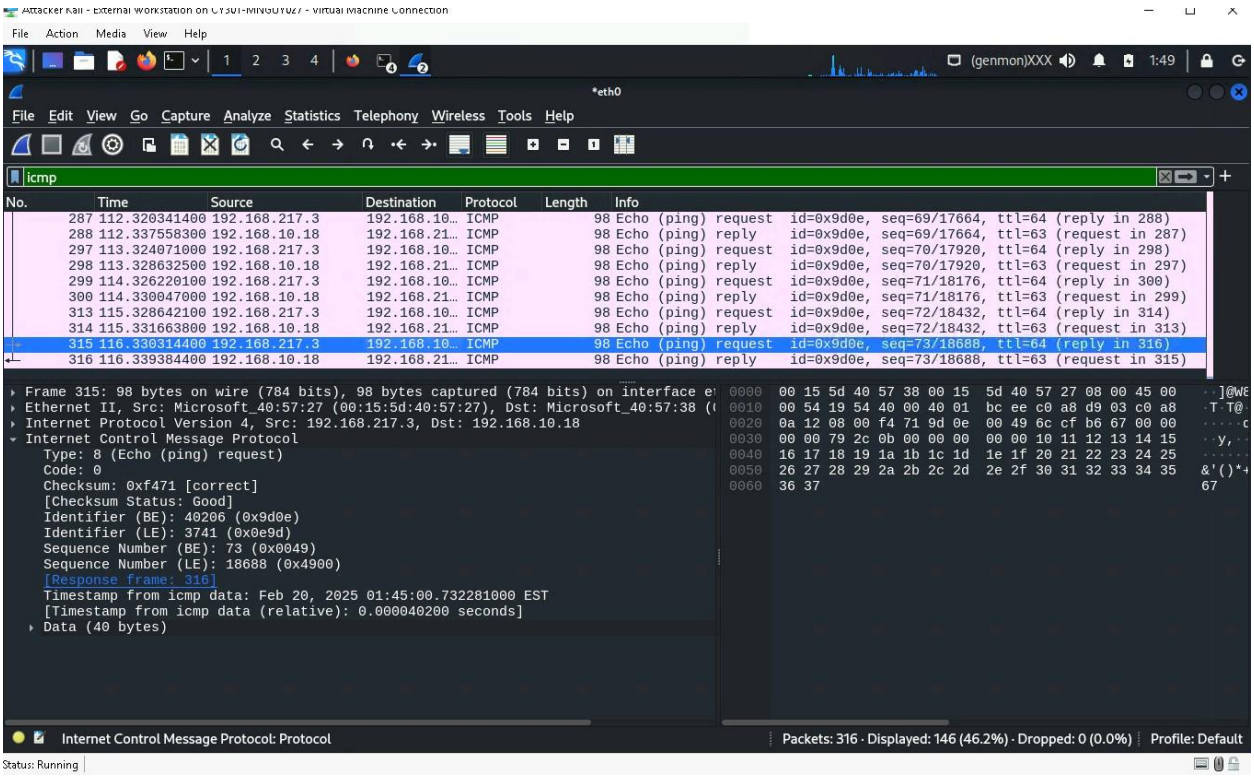
1. How many packets are captured in total? How many packets are displayed?
   There are a total of 316 captures, and 316 are displayed.



2. Apply “ICMP” as a display filter in Wireshark. Then repeat the previous question **There are a total of 316 captures, and 146 are displayed.**



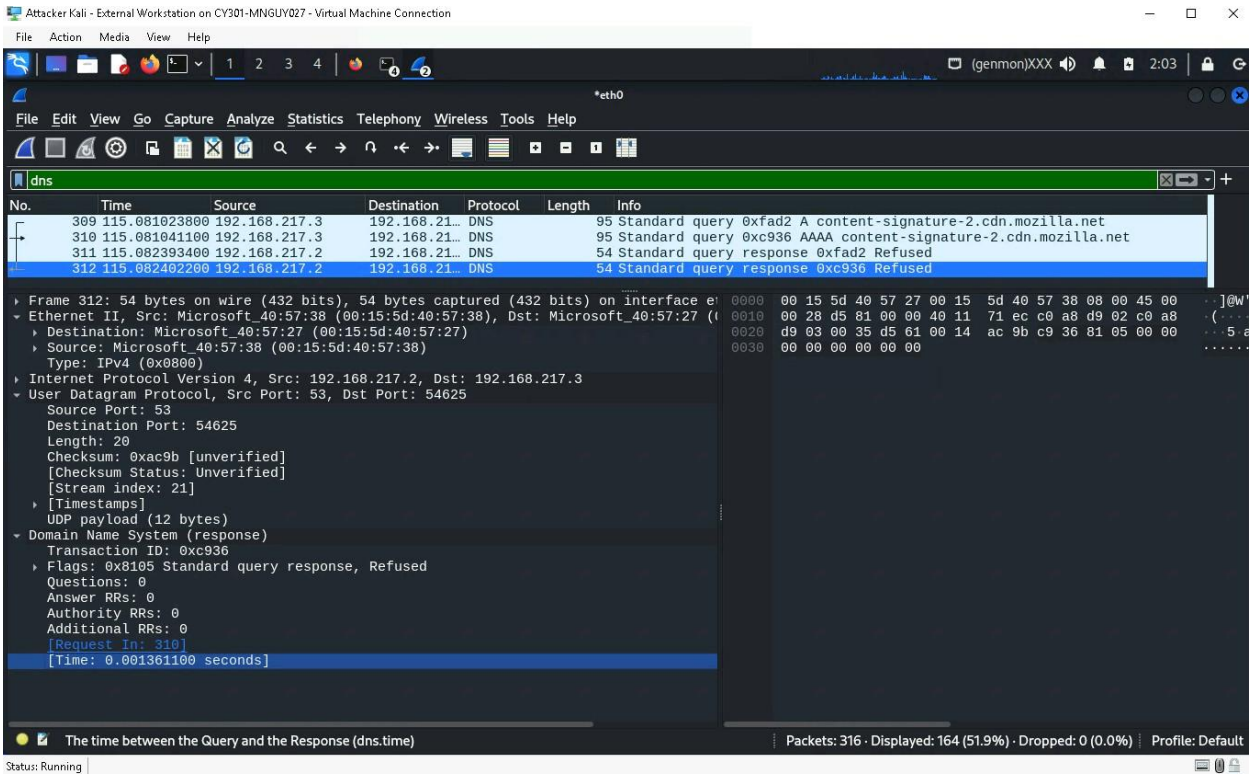
3. Select an Echo (replay) message from the list. What are the source and destination IPs of this packet? What are the sequence number and the size of the data? What is the response time?
   Source ip: 192.168.217.3 Destination ip: 192.168.10.18
   Sequence number: 73
   Size: 40 Bytes
   Response time: 0.000040200 s



4. Apply “DNS” as a display filter in Wireshark. How many packets are displayed? **There are 164 packets displayed.**

5. 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?
   Domain name: Transaction ID:0xc936
   Source ip: 192.168.217.3:54625 Destination: 192.168.217.2:53

6. 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?
   Source ip: 192.168.217.2:53 Destination: 192.168.217.3:54625. The message from the server says refused.



Task B: Sniff LAN traffic

In this task, you will be acting as an ATTACKER who sniffs the regular communications between peers (External Attacker Kali and Ubuntu) by using either Wireshark or tshark on Internal Attacker Kali VM. I would recommend you keeping the Wireshark/tshark running on Internal Kali all the time.

IMPORTANT NOTES!

* Because the current Hyper-V setting does not “broadcast” the communication between hosts in the same network, we need to enable port mirroring to allow Internal Kali to “see” other's communication. To be specific, you need to put the sniffer (Internal Kali) as the mirroring Destination, and the target VMs are mirroring Source (Figure 2). Since each VM has two network adapters, one for regular connection and the other is sharing with the CCIA server. We need to configure port mirroring on the first adapter. To be specific,

• Internal Kali: Set Mirroring mode to “Destination” in the “Port Mirroring”
• Ubuntu Kali: Set Mirroring mode to “Source” in the “Port Mirroring”
• External Kali: Set Mirroring mode to “Source” in the “Port Mirroring”

** Since each Windows 10 Host Machine has 20G memory. We need to adjust the assigned Memory for

Internal Kali and External Kali from 8192 to 4096 MB to support 4 VM running simultaneously. Figure 1 Required VMs for this assignment Figure 2 How to configure port mirroring in Hyper-V Select the first

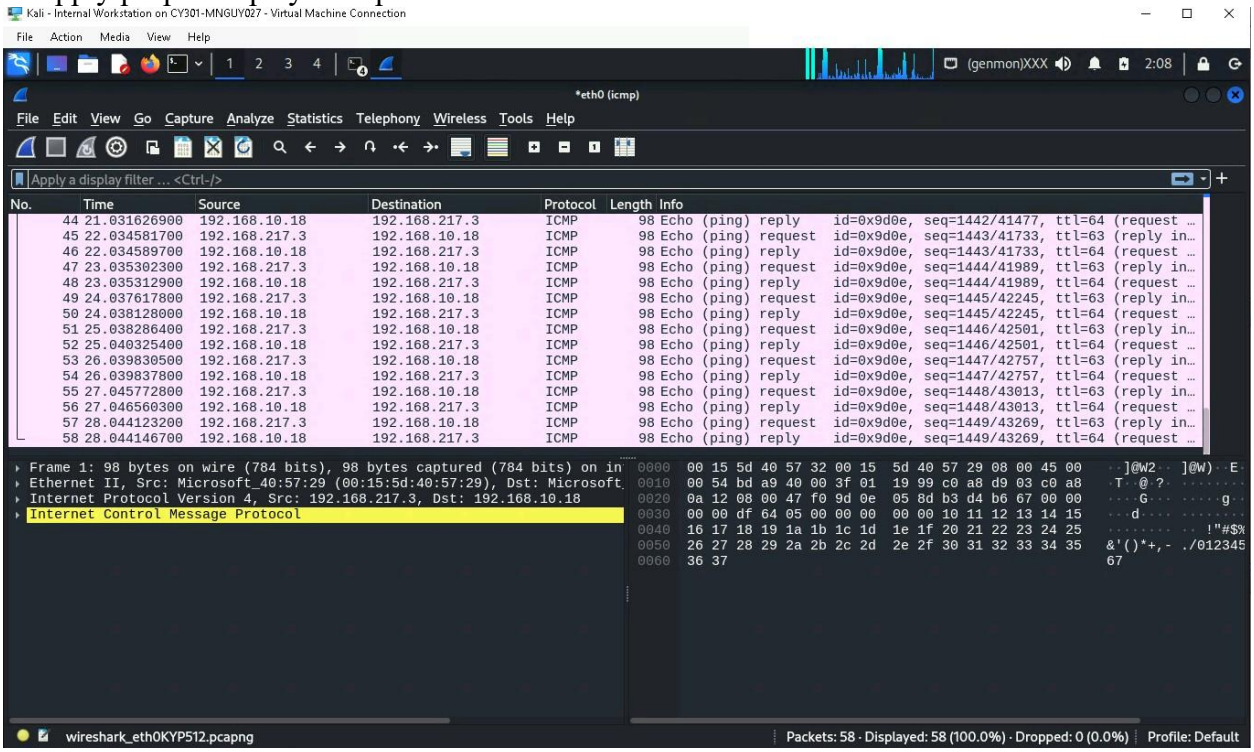
Network Adaptor, then click " Advanced Features"

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

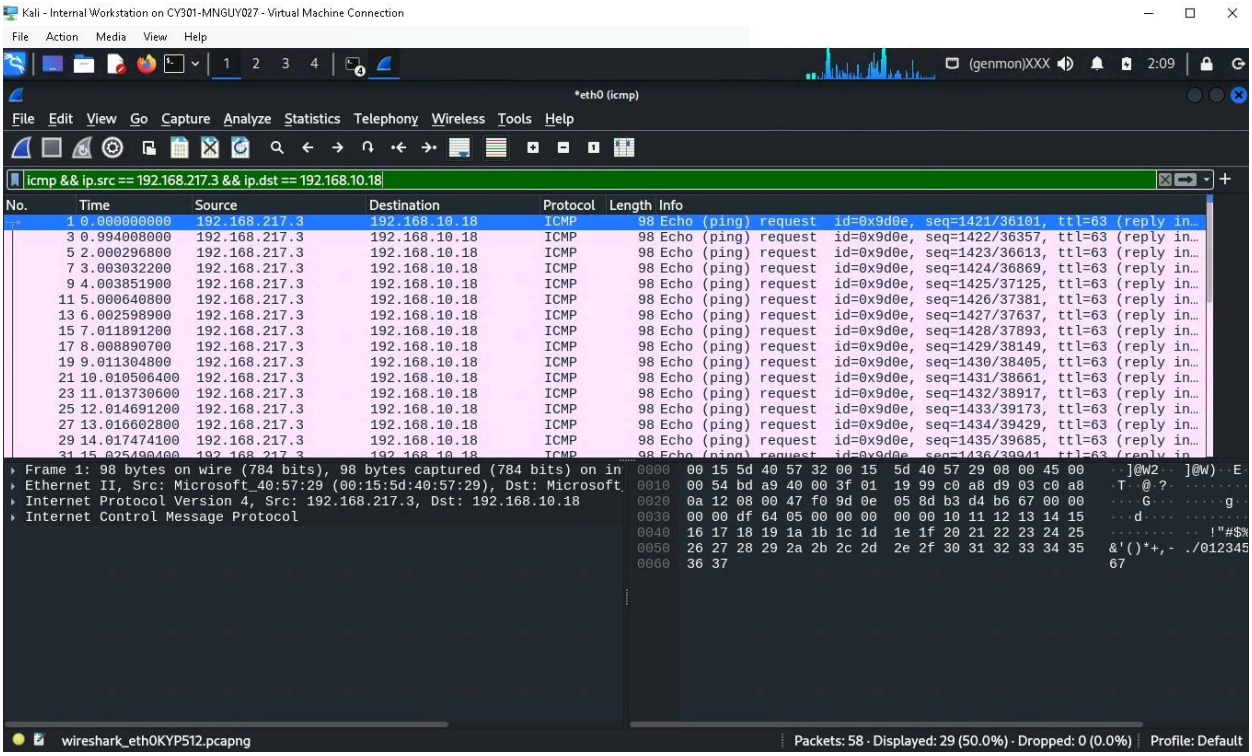
Open two terminals on External Kali VM. Use one ping Ubuntu VM, and use the other ping

Internal Kali.

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

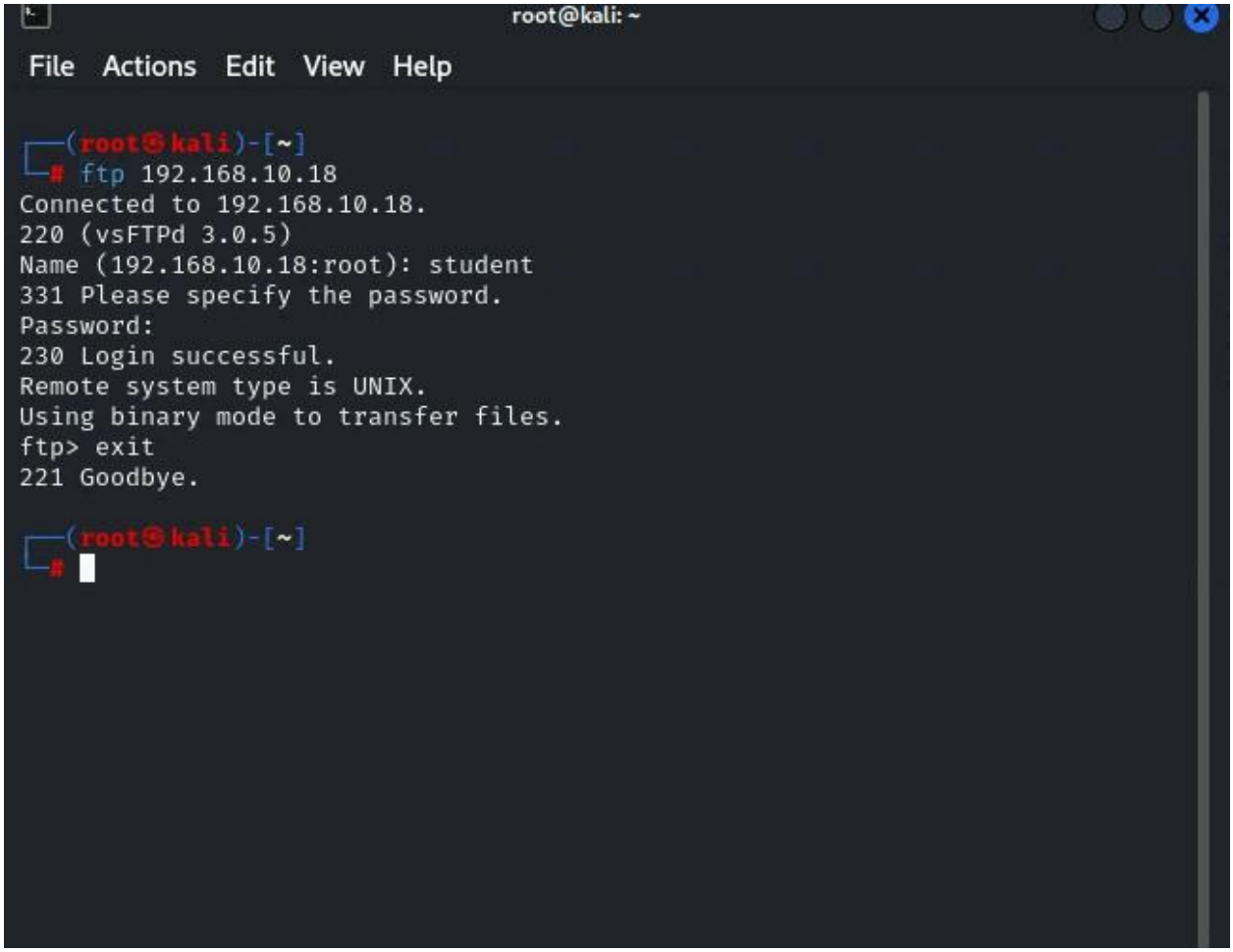


B. Apply proper display or capture filter on Internal Kali VM that ONLY displays ICMP request originated from External Kali VM and goes to Ubuntu 64-bit VM

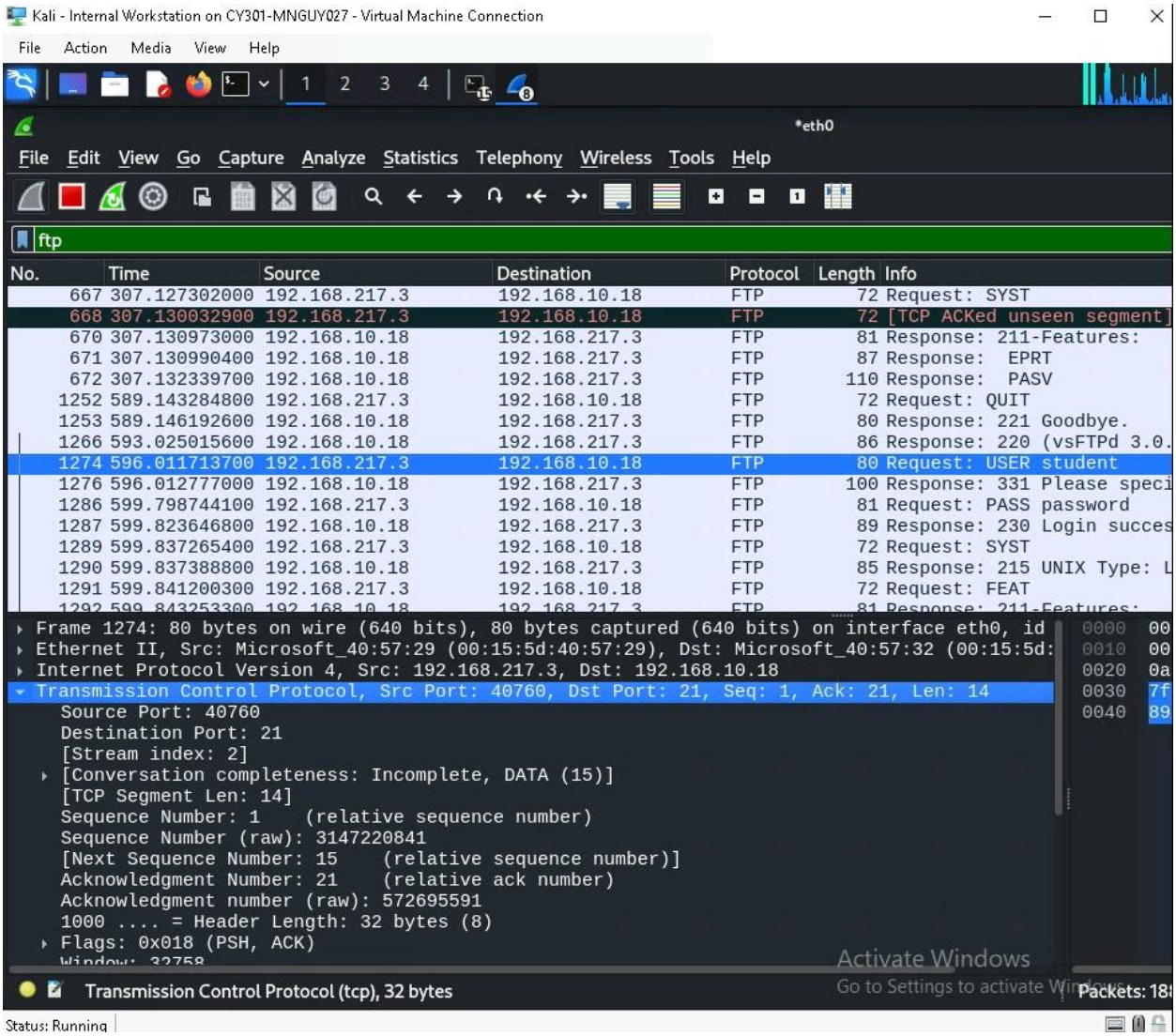


2. Sniff FTP traffic (10 + 15 + 15 = 40 pts points)

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.



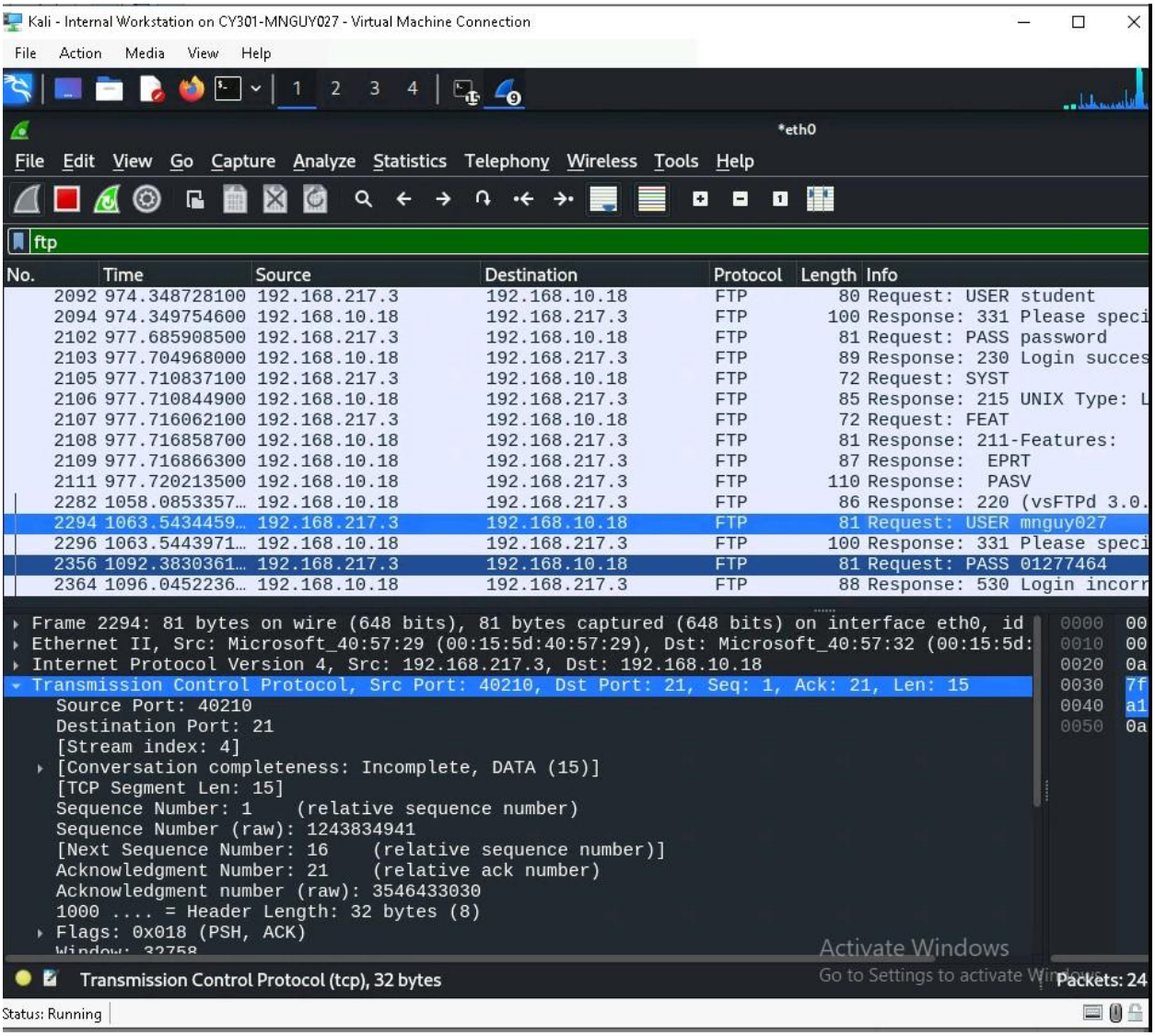
B. Unfortunately, Internal Kali, the attacker, is also sniffing to the communication. Therefore, all of your communication is exposed to the attacker. Now, you need to find out the password used by External Kali to access the FTP server from the intercepted traffic on Internal Kali. You need to screenshot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



FTP is an unencrypted protocol, meaning login credentials are sent in plain text. By sniffing traffic on Internal Kali, we intercepted the FTP login request. Using Wireshark, we captured the USER and PASS commands. The password "password" was visible in clear text in the packet capture.

C. After you successfully find the username & password from the FTP traffic, repeat the previous step

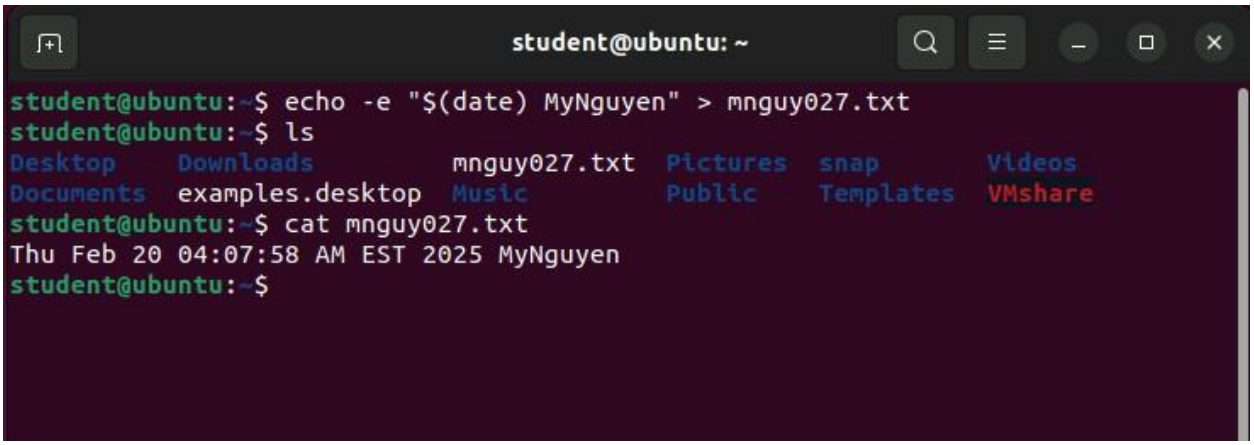
(2.a), and use your MIDAS ID as the username and UIN as the password to reaccess the FTP server from External Kali. Although External Kali may not access the FTP server, you need to intercept the packets containing these "secrets" from the attacker VM, which is Internal Kali.



Task C – Extra credit: Steal files with Wireshark (15 points)

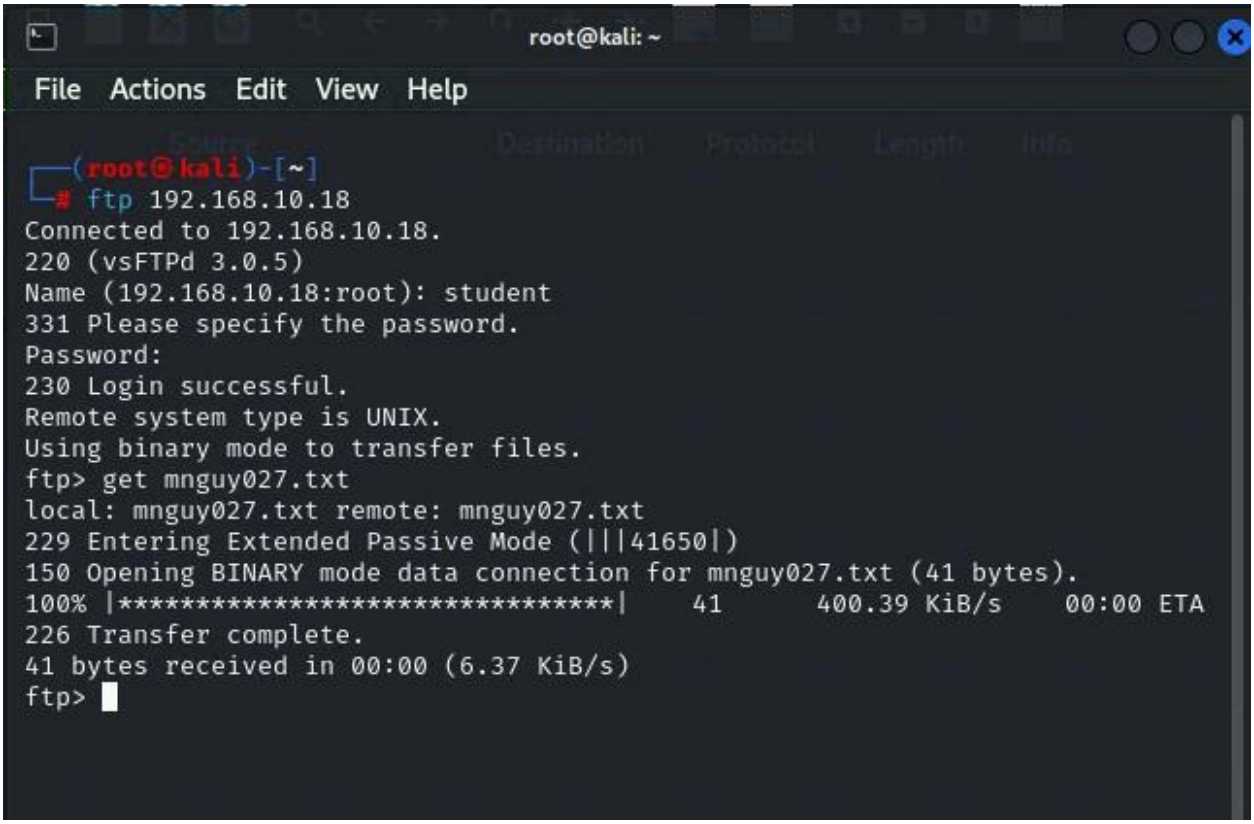
Login to Ubuntu VM, and create a file in your home directory named "YOUR_MIDAS.txt". Put the current timestamp and your name in the file. You can use the following command in the example below to do the job.

Once you have the file ready in Ubuntu, switch back to External Kali. Get the file you just created remotely using the FTP protocol. Below is an example.

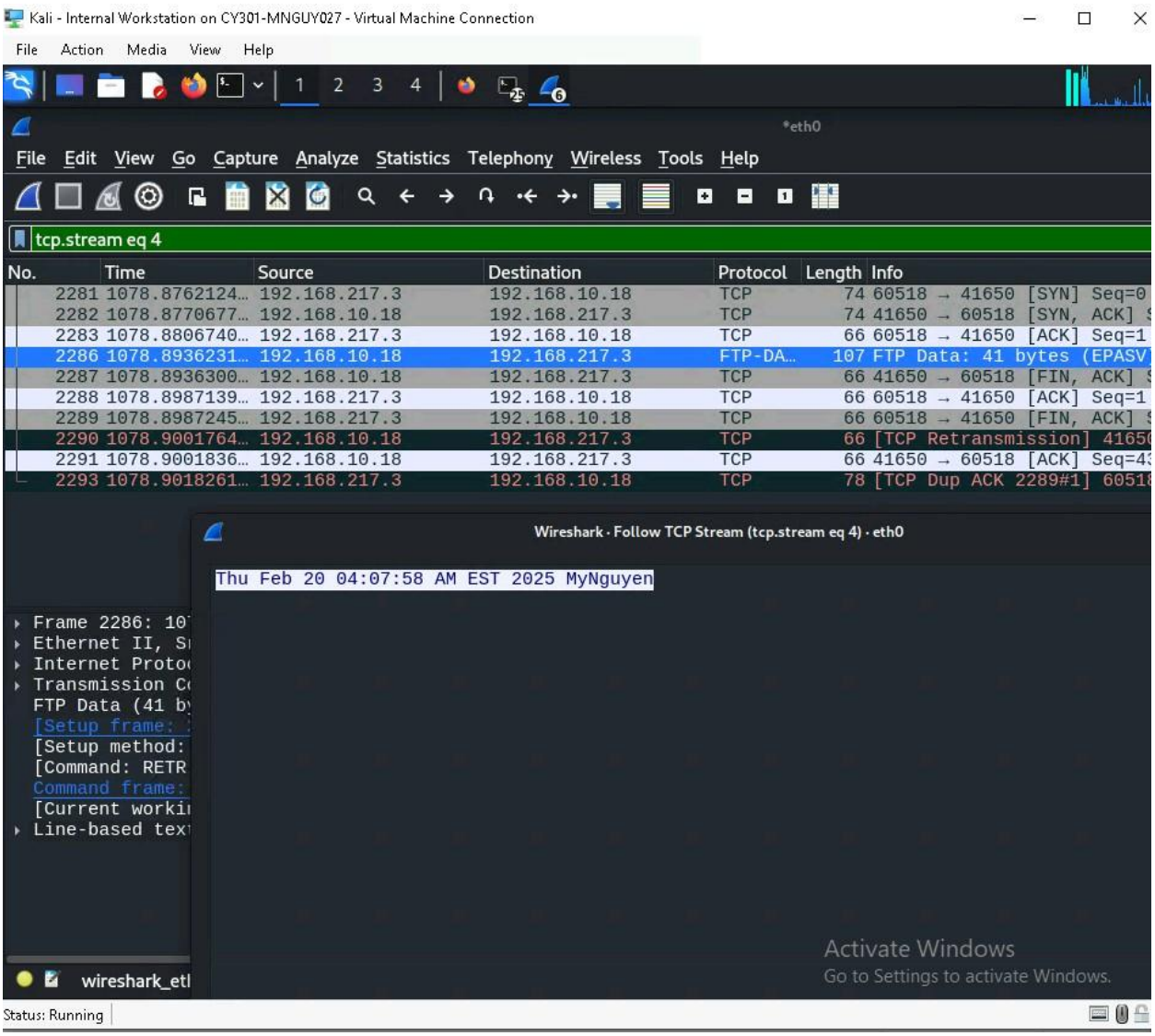


As an attacker, you need to complete the following tasks in Internal Kali:

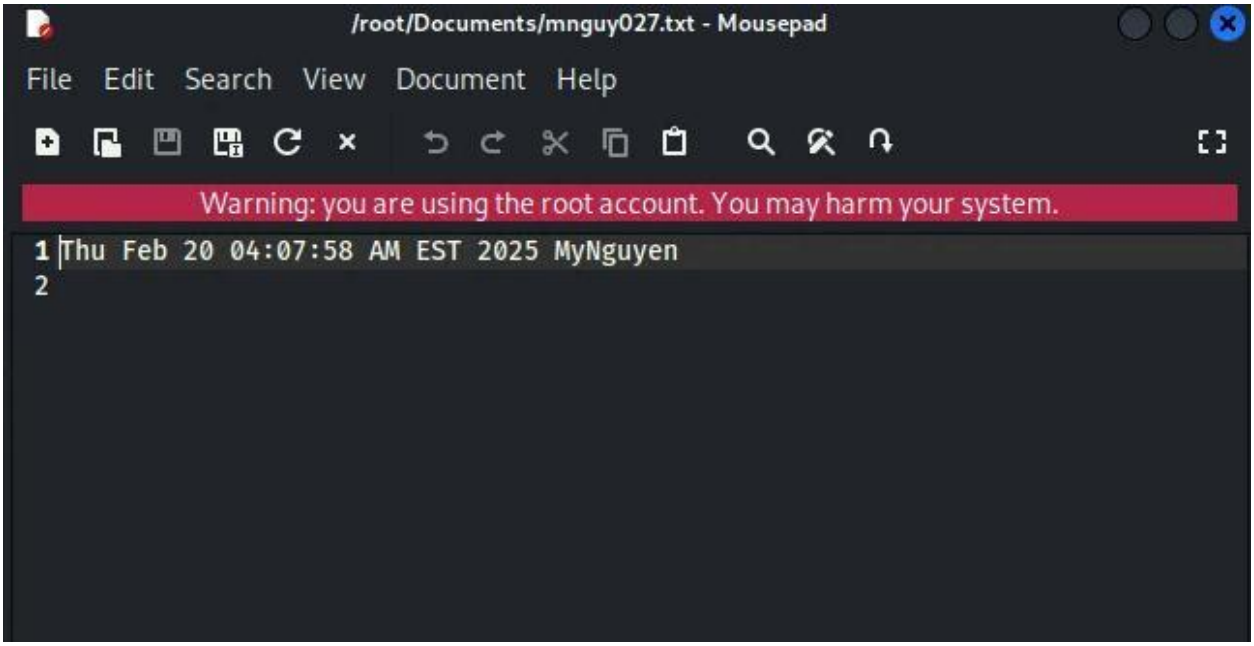
1. Apply a proper display filter to display the FTP-DATA packets between External Kali and Ubuntu VM.



2. Follow the TCP steam of the FTP-DATA packet and view the content of the file just transferred.



3. Export (Save) the transferred file as a text file in Internal Kali and view the content. Below is an example.


/root/Documents/mnguy027.txt - Mousepad
File Edit Search View Document Help
Warning: you are using the root account. You may harm your system.
1 Thu Feb 20 04:07:58 AM EST 2025 MyNguyen
2