OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment Lab #1 Traffic Tracing and Sniffing

John Wilson

01179411

TASK A: SNIFF LAN TRAFFIC

In this task, you will be acting as an **ATTACKER** who sniffers the internal communications between peers by using either Wireshark or tshark on **Internal Kali VM**. You need to use on the following VMs to complete the assignment.
I would recommend you keeping the Wireshark/tshark running on Internal Kali all the time.
IMPORTANT! Due to the different networking configurations in Hyper-V, you need to **Enable Port Mirroring for related VMs accordingly**. This is a helpful link to follow. To be specific, you need to put the sniffer (Internal Kali) as the ***mirroring Destination*,** and the target VMs are ***mirroring Source*** (Figure 2). To be sepcifc,

- • Internal Kali: Set Miorroing mode to "***Destination***" in the "Port Mirroiring"
- • Ubuntu Kali: Set Miorroing mode to "***Source***" in the "Port Mirroiring"
- • External Kali: Set Miorroing mode to "***Source***" in the "Port Mirroiring"

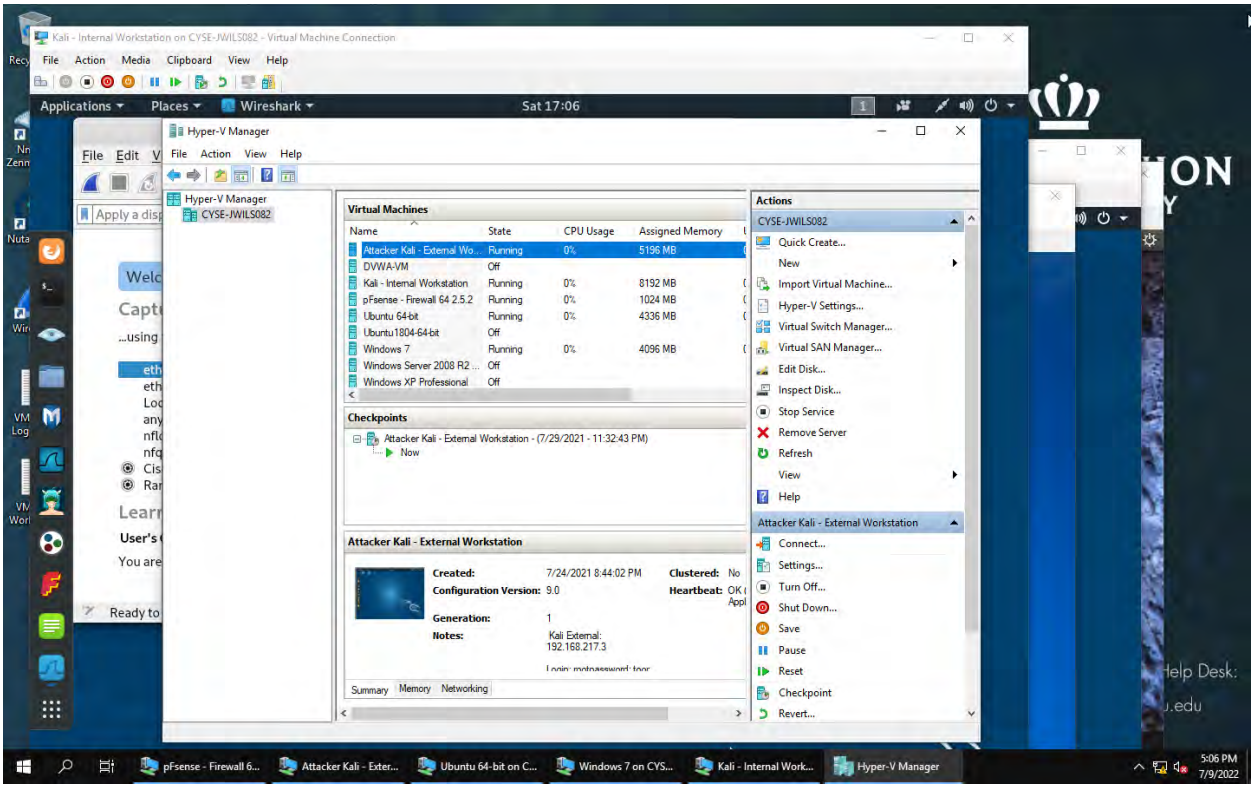


Figure 1. Screenshot of pre-exercise stuff.

- This screenshot is to illustrate that I have started/executed the computer systems External Kali, Internal Kali, Ubuntu 64-bit, pFense-firewall, and Windows 7.
- In addition, I implemented the port mirroring as instructed with the **source** being set to the External Kali and Ubuntu 64-bit, and Windows 7 and **destination** set for only the Internal Kali machines. If you did not set up the system this way, then you could not carry out and complete the exercise.

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

a. In External Kali VM, ping Windows 7 VM and Ubuntu VM from two separate terminals.

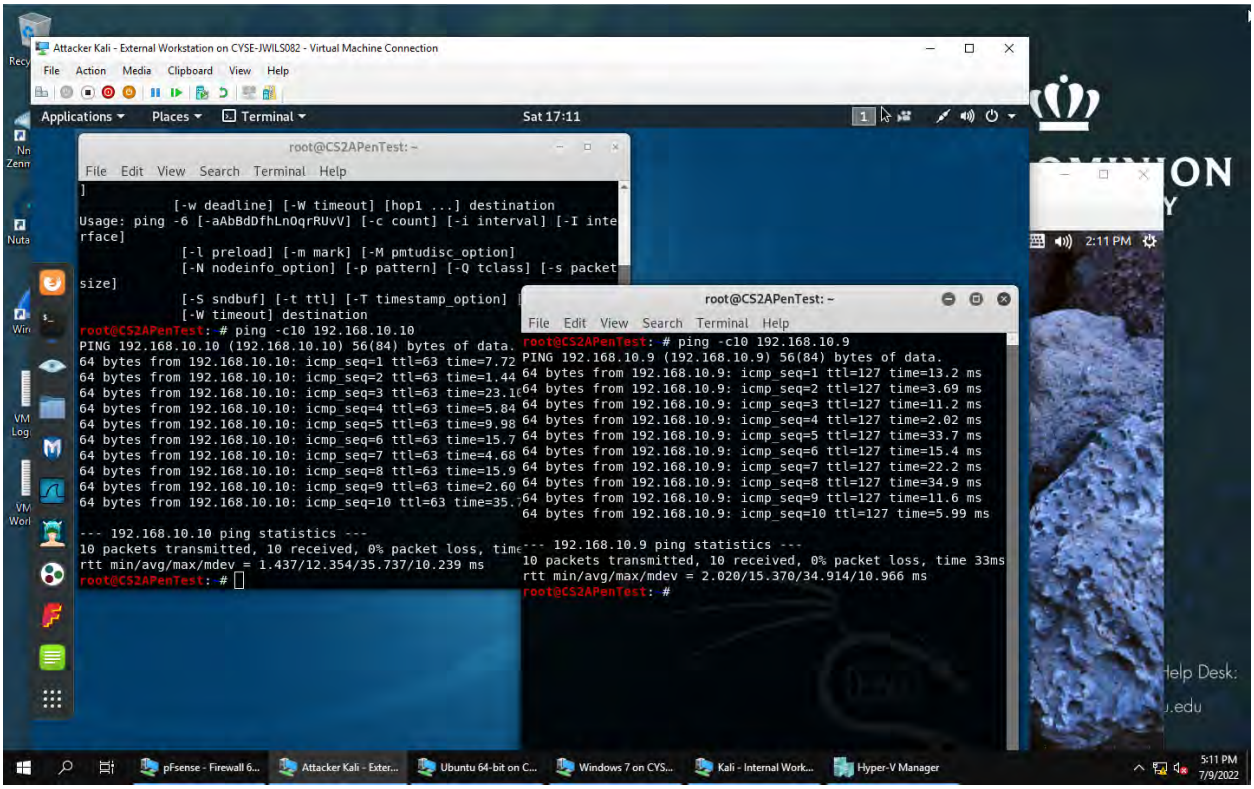


Figure 2. Screenshot of task 1.a

- This screenshot illustrates that I have opened two separate terminals on the External Kali machine to show the successful pings were sent to the Ubuntu 64-bit and Windows 7 computer systems.

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

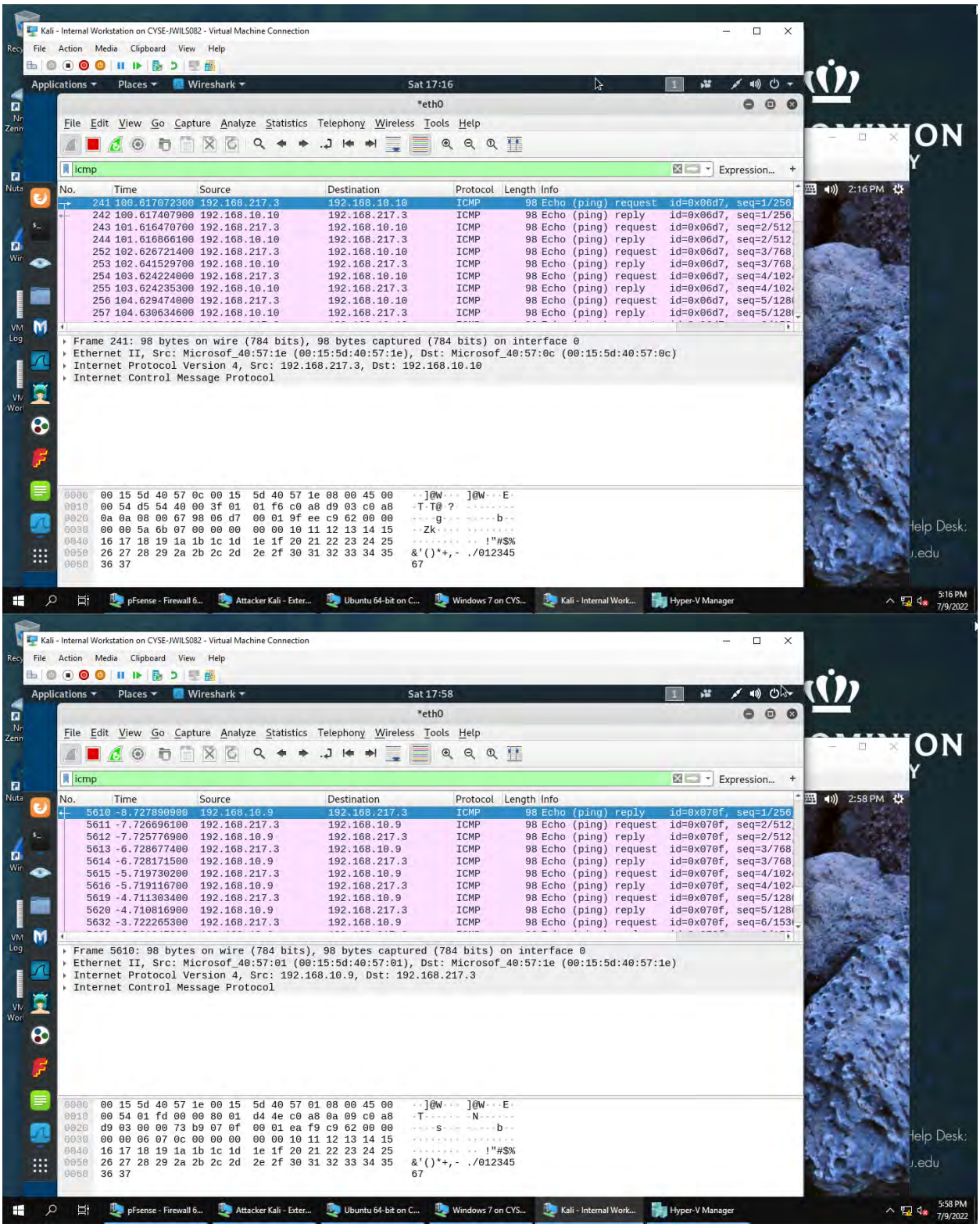


Figure 3 and 4. Screenshots of task 1.b

- These screenshots illustrate that I have opened the Wireshark application in the Internal Kali computer system and used the filter of “icmp” to show that the Internal Kali computer system can see the ping traffic originating from the External Kali computer system (which is IP 192.168.217.3) to computer systems Ubuntu 64-bit (which is IP 192.168.10.10) and Windows 7 (which is IP 192.168.10.9).
- FYI, I (made a mistake) forgot to save or accidentally deleted the screenshot to illustrate the Windows 7 system being pinged by the External Kali. So, I had to go back and recreate it, and this is the reason there is a forty-minute difference in timestamps.

c. 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.

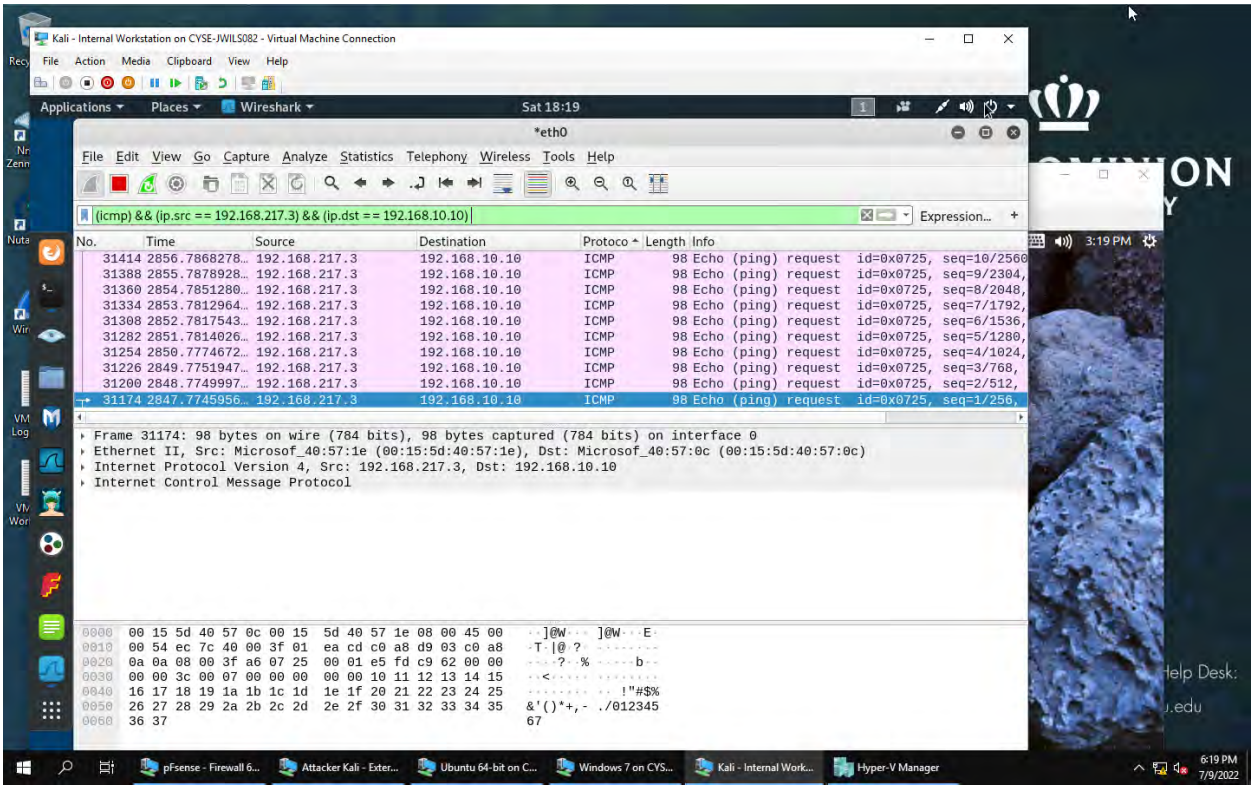


Figure 5. Screenshots of task 1.c

- These screenshots illustrates that I used the filter option of "**(icmp) && (ip.src == 192.168.217.3) && (ip.dst == 192.168.10.10)**" to show only the icmp traffic from the External Kali computer system (which is IP **192.168.217.3**) to computer systems Ubuntu 64-bit (which is IP **192.168.10.10**). The filter says that I only want to see the ping messages (**icmp**) that originated from IP source (**ip.src**) 192.168.217.3 to (**&&**) the IP destination (**ip.dst**) 192.168.10.10.

2. Sniff FTP traffic (60 points)

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.

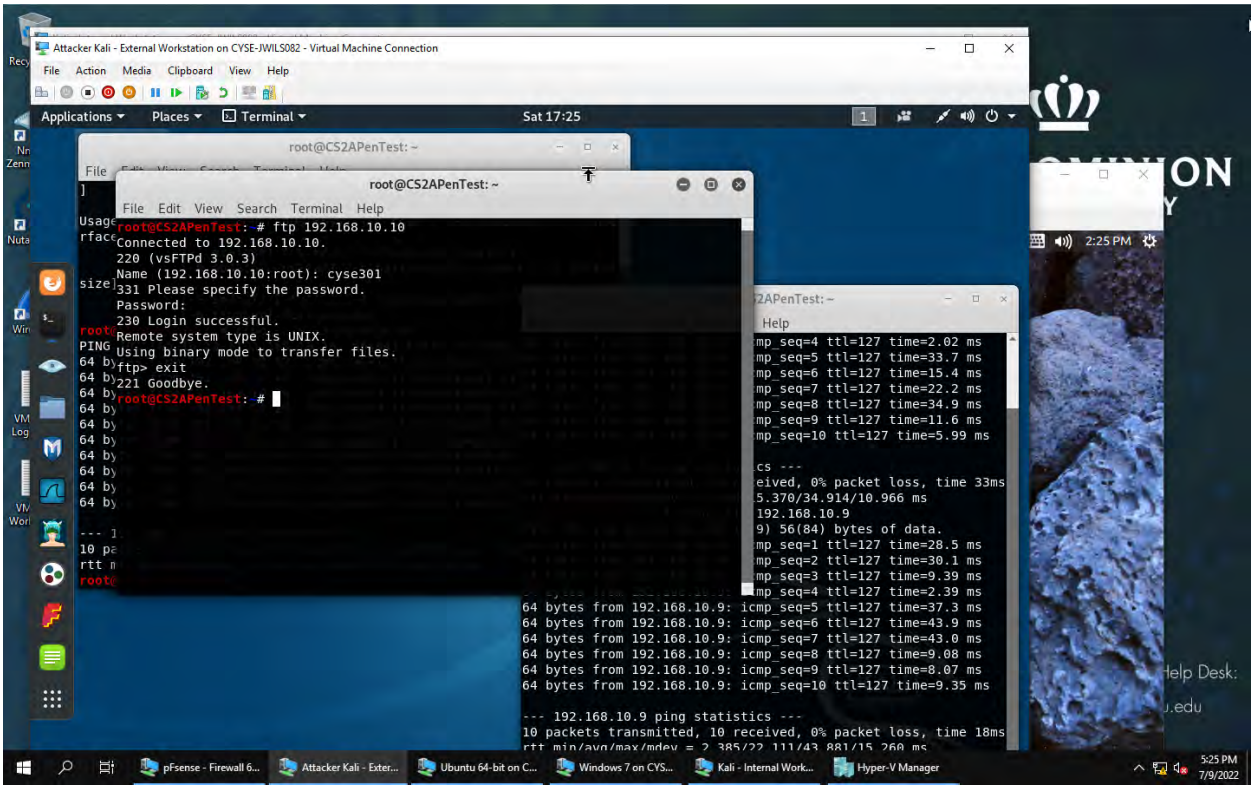


Figure 1. Screenshots of task 2.a

- This screenshot illustrates that I used the External Kali computer system (which is IP **192.168.217.3**) terminal to access the FTP server on the computer system Ubuntu 64-bit (which is IP **192.168.10.10**).

a. **Unfortunately**, Internal Kali, the attacker, is also sniffing to the internal communication by using **tshark**. 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 in the **Wireshark** running on Internal Kali VM. You need to screenshot and explain how you find the password.

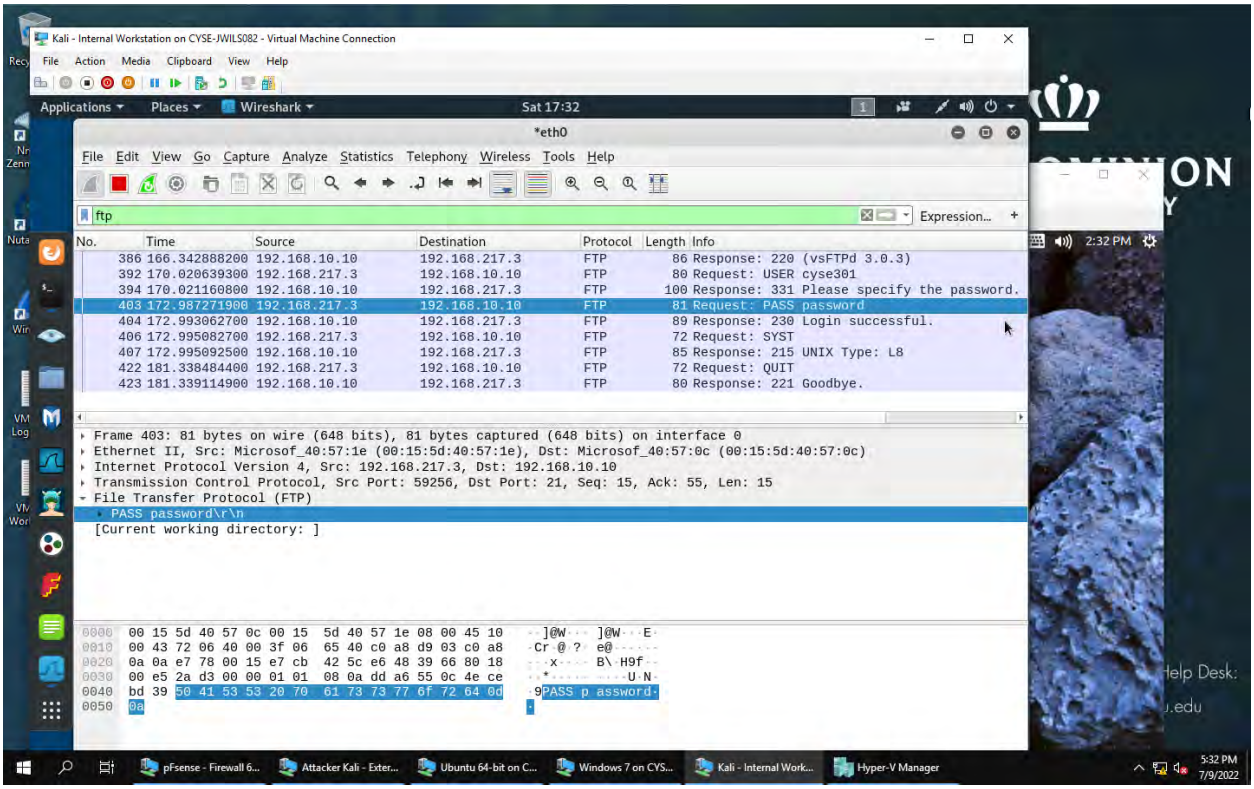


Figure 2. Screenshots of task 2.b

- This screenshot illustrates that I used the Wireshark application on the Internal Kali computer system (which is IP **192.168.10.13**) to see the message traffic to the FTP server which is located on the computer system Ubuntu 64-bit (which is IP **192.168.10.10**). I used the filter "FTP" and it showed all the FTP protocol messages.
- Within these messages you can clearly see in the info section that a system with the source IP of **192.168.217.3** (which is the External Kali computer system) successfully logged onto the FTP server.
- The messages tagged with the line no:
    - # 392 shows that the username of "**cyse301"** was used
    - # 403 shows the password "**password**" was used
    - # 404 shows the system successfully logged into the FTP server with the response "**Login successful**"

b. After you successfully sniffed the username & password from the FTP traffic, repeat the previous step, 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**.

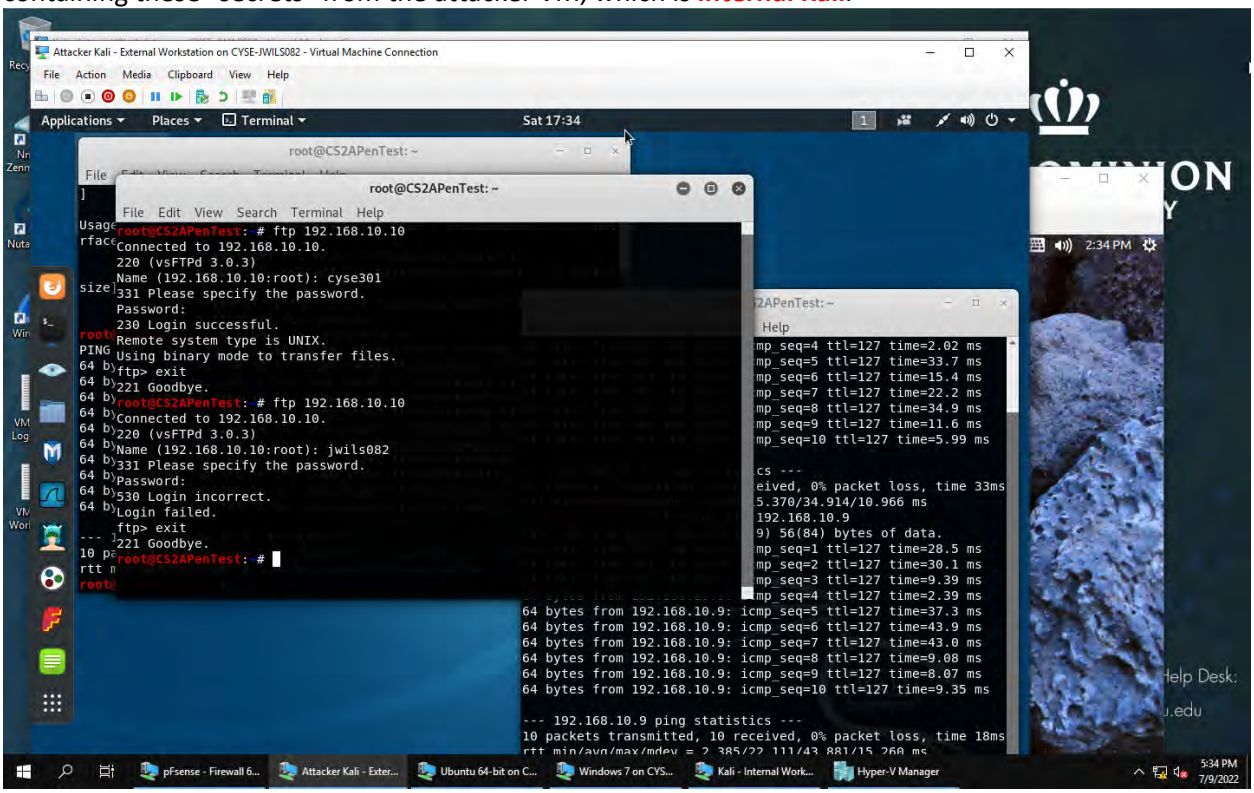
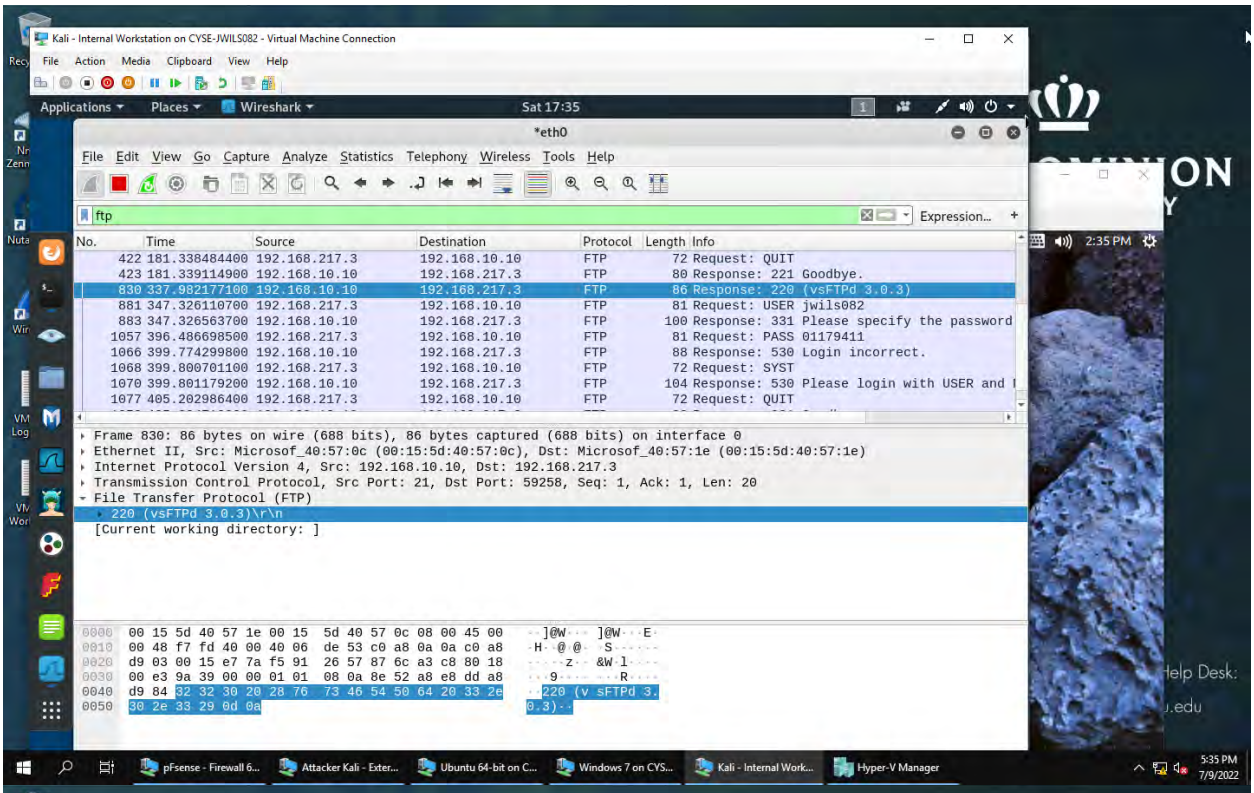
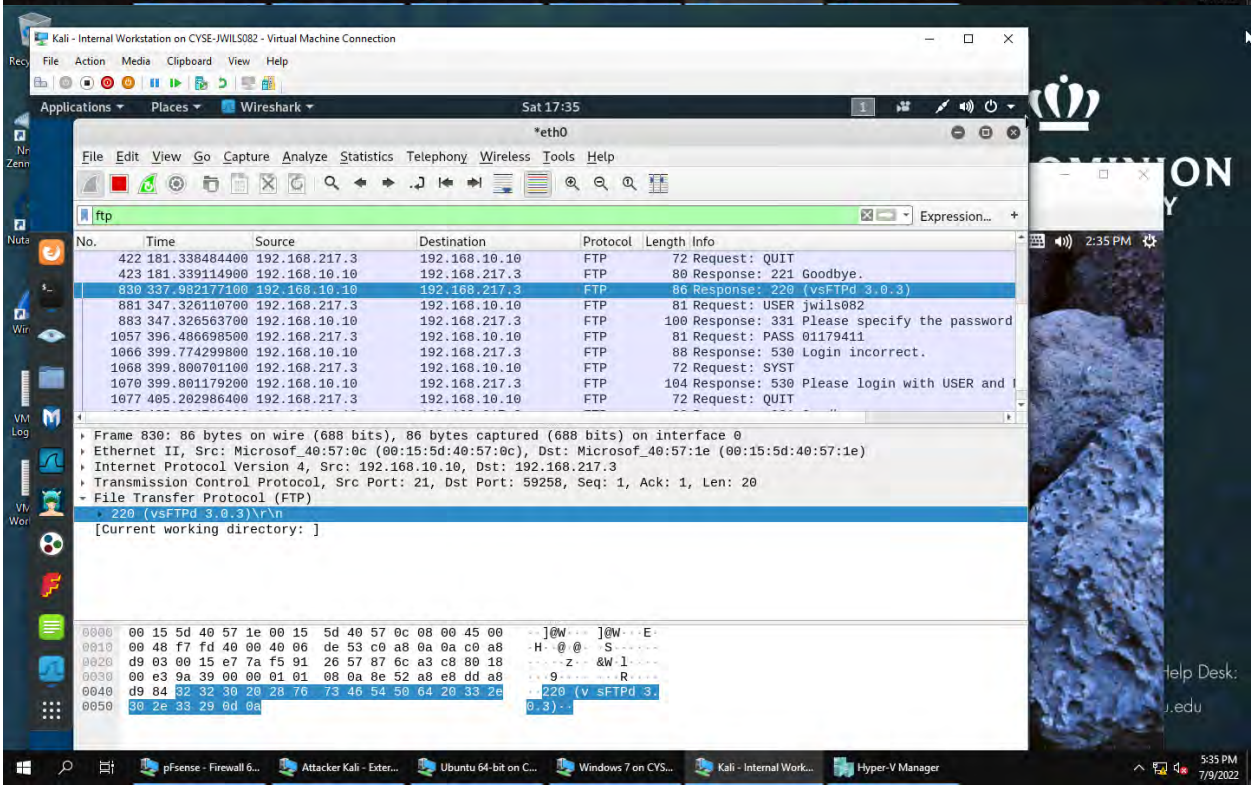


Figure 3. Screenshots of task 2.c

- This screenshot illustrates that I used the External Kali computer system (which is IP **192.168.217.3**) terminal to attempt to access the FTP server on the computer system Ubuntu 64-bit (which is IP **192.168.10.10**) using the credentials:
    - Username: jwils082
    - Password: 01179411.
- The login is will be unsuccessful as you can see in the terminal.


Kali - Internal Workstation on CYSE-JWILS082 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Wireshark Sat 17:35
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ftp
Expression...
No. Time Source Destination Protocol Length Info
422 181.338484400 192.168.217.3 192.168.10.10 FTP 72 Request: QUIT
423 181.339114900 192.168.10.10 192.168.217.3 FTP 80 Response: 221 Goodbye.
830 337.982177100 192.168.10.10 192.168.217.3 FTP 86 Response: 220 (vsFTPd 3.0.3)
881 347.326110700 192.168.217.3 192.168.10.10 FTP 81 Request: USER jwils082
883 347.326563700 192.168.10.10 192.168.217.3 FTP 100 Response: 331 Please specify the password
1057 396.486698500 192.168.217.3 192.168.10.10 FTP 81 Request: PASS 01179411
1066 399.774299800 192.168.10.10 192.168.217.3 FTP 88 Response: 530 Login incorrect.
1068 399.800701100 192.168.217.3 192.168.10.10 FTP 72 Request: SYST
1070 399.801179200 192.168.10.10 192.168.217.3 FTP 104 Response: 530 Please login with USER and
1077 405.202986400 192.168.217.3 192.168.10.10 FTP 72 Request: QUIT
Frame 830: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
Ethernet II, Src: Microsof_40:57:0c (00:15:5d:40:57:0c), Dst: Microsof_40:57:1e (00:15:5d:40:57:1e)
Internet Protocol Version 4, Src: 192.168.10.10, Dst: 192.168.217.3
Transmission Control Protocol, Src Port: 21, Dst Port: 59258, Seq: 1, Ack: 1, Len: 20
File Transfer Protocol (FTP)
220 (vsFTPd 3.0.3)\r\n
[Current working directory:]
0000 00 15 5d 40 57 1e 00 15 5d 40 57 0c 08 00 45 00
0010 00 48 f7 fd 40 00 40 06 de 53 c0 a8 0a 0a c0 a8
0020 d9 03 00 15 e7 7a f5 91 26 57 87 6c a3 c8 80 18
0030 00 e3 9a 39 00 00 01 01 08 0a 8e 52 a8 e8 dd a8
0040 d9 84 32 32 30 20 28 76 73 46 54 50 64 20 33 2e
0050 30 2e 33 29 0d 0a
2:35 PM
pFsense - Firewall 6...
Attacker Kali - Exter...
Ubuntu 64-bit on C...
Windows 7 on CYS...
Kali - Internal Work...
Hyper-V Manager
5:35 PM
7/9/2022


Kali - Internal Workstation on CYSE-JWILS082 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Wireshark Sat 17:35
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ftp
Expression...
No. Time Source Destination Protocol Length Info
422 181.338484400 192.168.217.3 192.168.10.10 FTP 72 Request: QUIT
423 181.339114900 192.168.10.10 192.168.217.3 FTP 80 Response: 221 Goodbye.
830 337.982177100 192.168.10.10 192.168.217.3 FTP 86 Response: 220 (vsFTPd 3.0.3)
881 347.326110700 192.168.217.3 192.168.10.10 FTP 81 Request: USER jwils082
883 347.326563700 192.168.10.10 192.168.217.3 FTP 100 Response: 331 Please specify the password
1057 396.486698500 192.168.217.3 192.168.10.10 FTP 81 Request: PASS 01179411
1066 399.774299800 192.168.10.10 192.168.217.3 FTP 88 Response: 530 Login incorrect.
1068 399.800701100 192.168.217.3 192.168.10.10 FTP 72 Request: SYST
1070 399.801179200 192.168.10.10 192.168.217.3 FTP 104 Response: 530 Please login with USER and
1077 405.202986400 192.168.217.3 192.168.10.10 FTP 72 Request: QUIT
Frame 830: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
Ethernet II, Src: Microsof_40:57:0c (00:15:5d:40:57:0c), Dst: Microsof_40:57:1e (00:15:5d:40:57:1e)
Internet Protocol Version 4, Src: 192.168.10.10, Dst: 192.168.217.3
Transmission Control Protocol, Src Port: 21, Dst Port: 59258, Seq: 1, Ack: 1, Len: 20
File Transfer Protocol (FTP)
220 (vsFTPd 3.0.3)\r\n
[Current working directory:]
0000 00 15 5d 40 57 1e 00 15 5d 40 57 0c 08 00 45 00
0010 00 48 f7 fd 40 00 40 06 de 53 c0 a8 0a 0a c0 a8
0020 d9 03 00 15 e7 7a f5 91 26 57 87 6c a3 c8 80 18
0030 00 e3 9a 39 00 00 01 01 08 0a 8e 52 a8 e8 dd a8
0040 d9 84 32 32 30 20 28 76 73 46 54 50 64 20 33 2e
0050 30 2e 33 29 0d 0a
2:35 PM
pFsense - Firewall 6...
Attacker Kali - Exter...
Ubuntu 64-bit on C...
Windows 7 on CYS...
Kali - Internal Work...
Hyper-V Manager
5:35 PM
7/9/2022

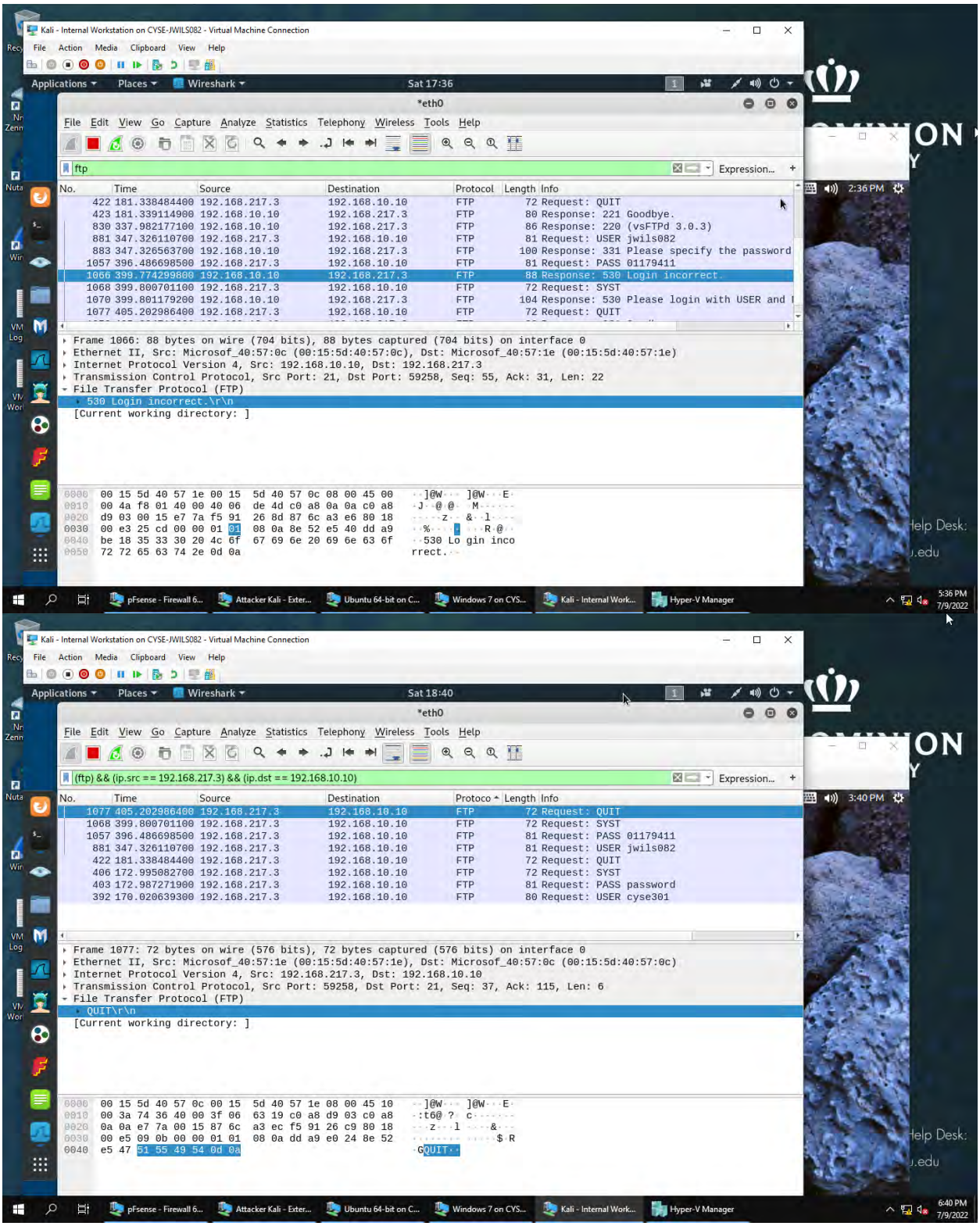


Figure 4, 5, 6, 7. Screenshots of task 2.c

- This screenshot illustrates that I used the Wireshark application on the Internal Kali computer system (which is IP **192.168.10.13**) to see the message traffic to the FTP server which is located on the computer system Ubuntu 64-bit (which is IP **192.168.10.10**). In

screenshots 4, 5, 6, and 7, I used the filter “FTP” and it showed all the FTP protocol messages.

- Within these messages you can clearly see in the info section that a system with the source IP of **192.168.217.3** (which is the External Kali computer system) attempted to log onto the FTP server using different credentials.
- The messages tagged with the line no:
    - # 881 shows that the username of “**jwils082”** was used
    - # 1057 shows the password “**01179411**” was used
    - # 1066 shows the system denied the logon attempt to the FTP server with the response “**Login incorrect**”
- In addition, in screenshot 7 used a different filtering method to show the attempts to logon to the FTP server from the source IP of **192.168.217.3** (which is the External Kali computer system). I did this to illustrate there is more than one way to look at this traffic such as in this case I just wanted to see the direct request traffic from the source IP of **192.168.217.3** (which is the External Kali computer system) to the computer system Ubuntu 64-bit (which is IP **192.168.10.10**).
- This is actually pretty scary stuff if you think about it as any bad actor that has successfully got into your system/network can sit back and capture all of this traffic and use it for whatever motivations (financial, political, excitement, etc.) they see fit.

Task B – 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.

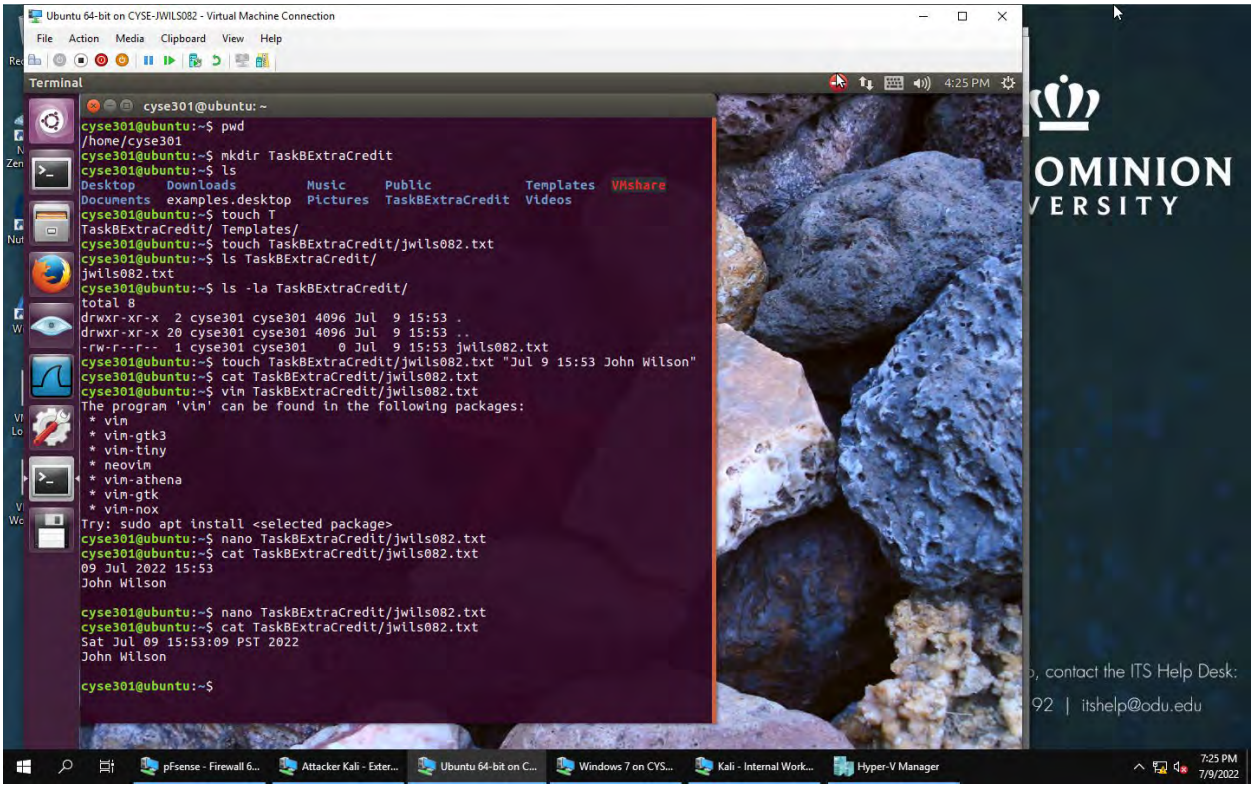


Figure 1. Screenshot of Task B

- This screenshot that I made the directory “TaskBExtraCredit” and a placed a file named “jwils082.txt” with the appropriate information inside the file on the Ubuntu system.

Once you have the file ready in Ubuntu, switch back to **External Kali**. Get the file you just created with FTP protocol remotely. 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 the example.

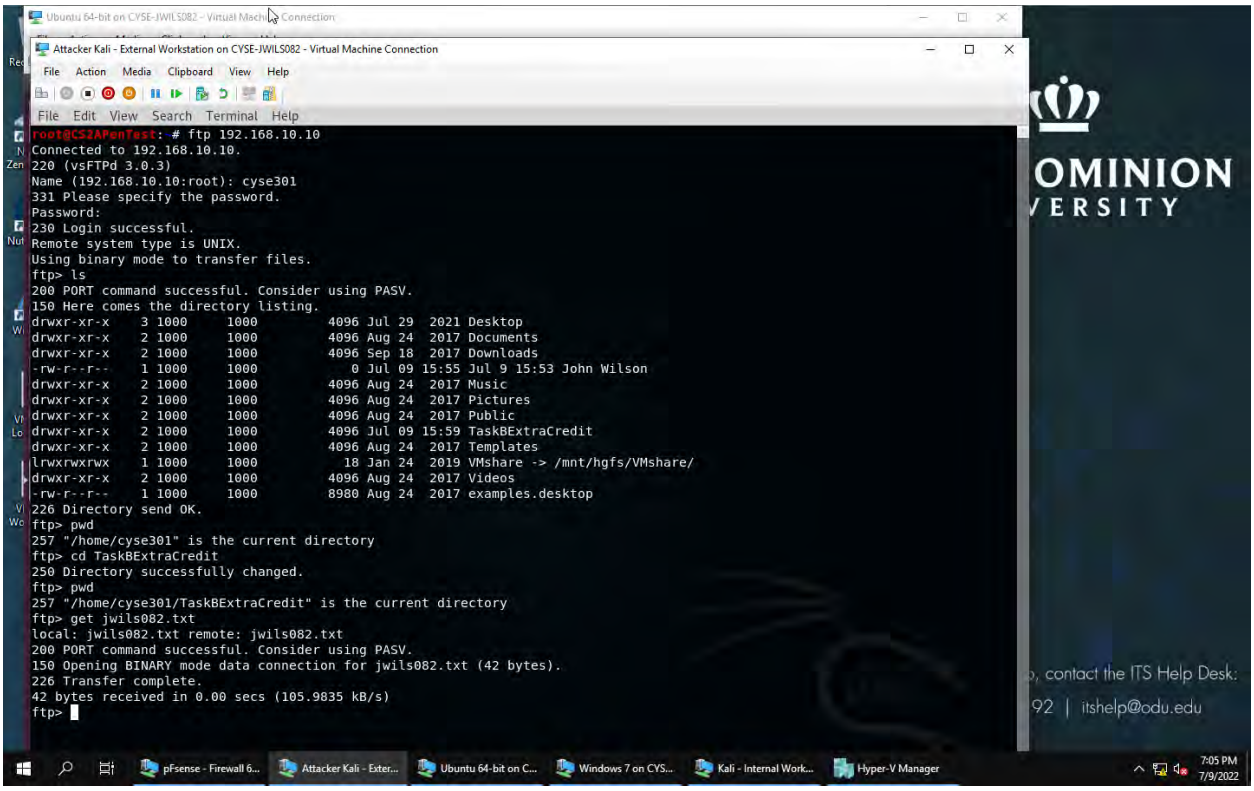
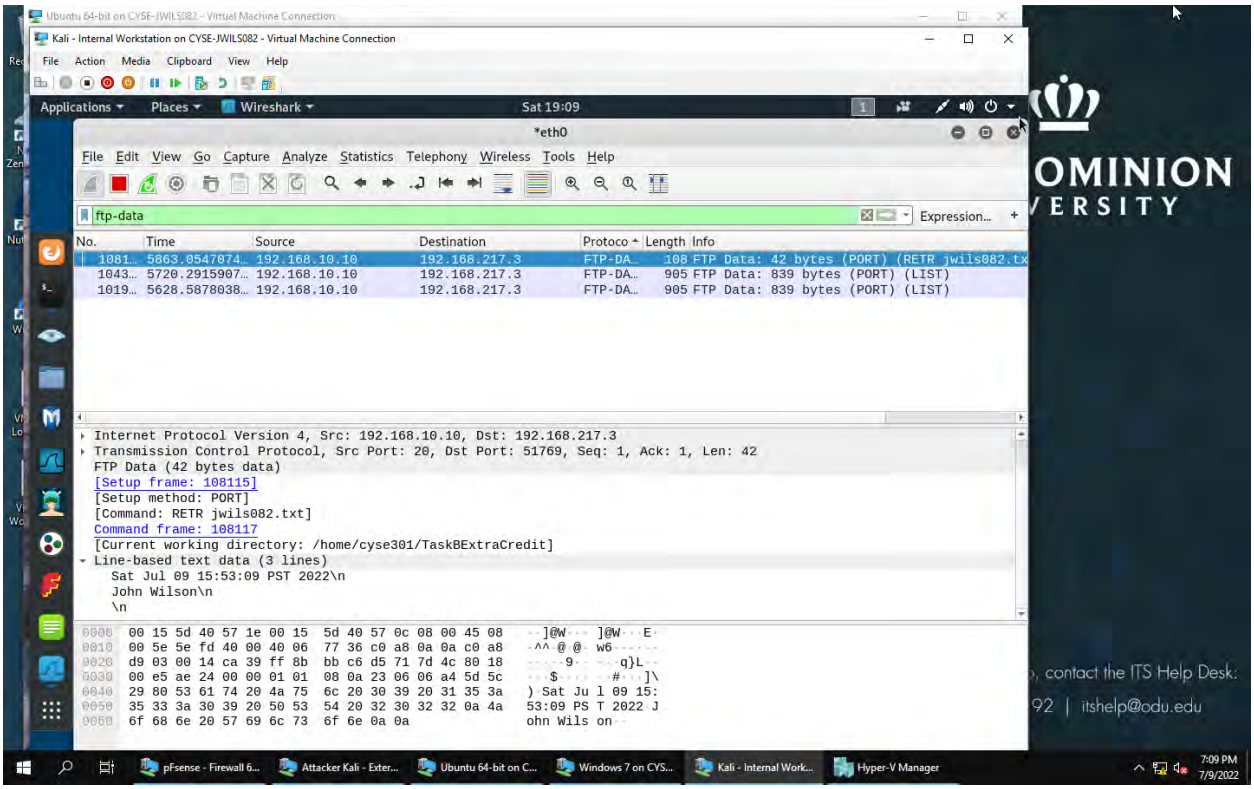


Figure 2. Screenshot of Task B

- This screenshot is to illustrate of the steps I did as the attacker from the External Kali computer system (which is IP **192.168.217.3**) terminal to attempt to access the FTP server on the computer system Ubuntu 64-bit (which is IP **192.168.10.10**).
- As you can see the file transferred successfully.



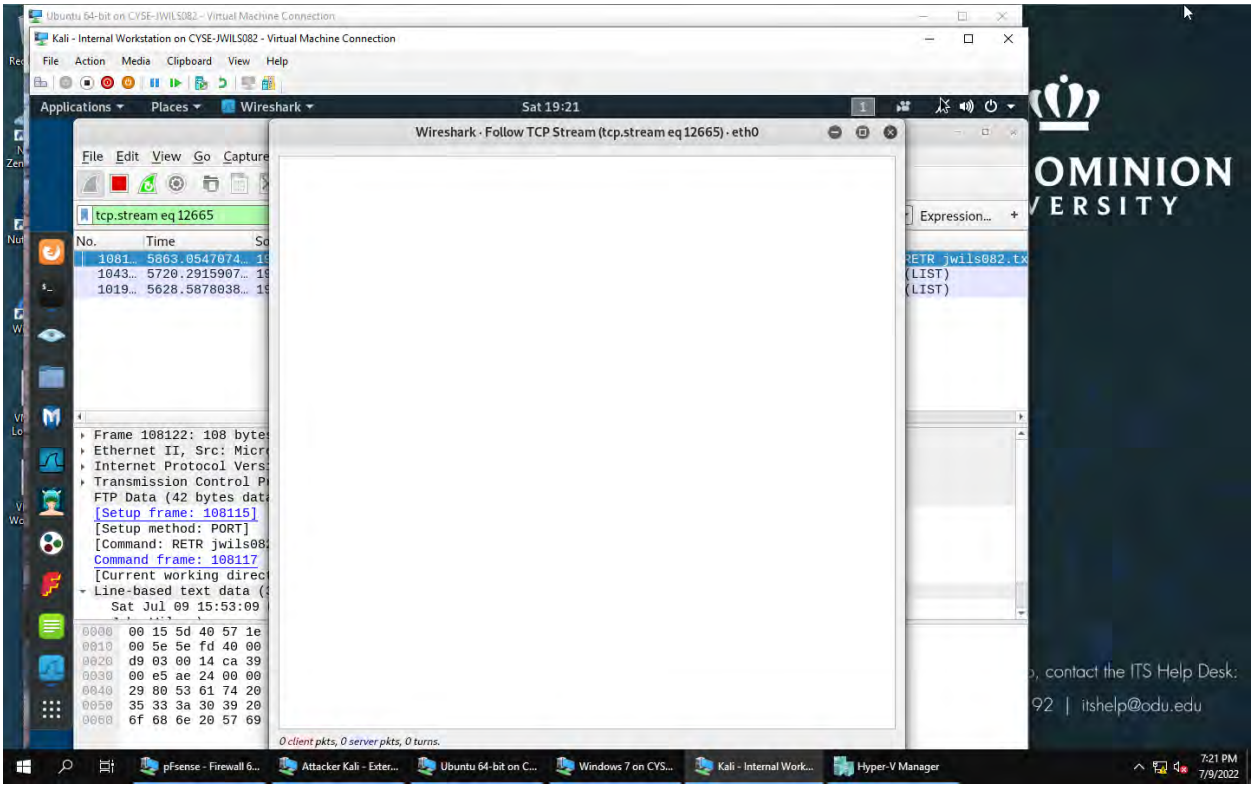


Figure 3 and 4. Screenshot of Task B

- This screenshot is to illustrate of the steps I attempted to trace the file being transferred from the Ubuntu 64-bit (which is IP **192.168.10.10**) to the External Kali computer system (which is IP **192.168.217.3**).
- I used the Wireshark application in the Internal Kali computer system and filtered out the traffic using the filter protocol “ftp-data”.
- On the line number 1081, I found the message that showed the file “**jwils082.txt**” that was transferred to the External Kali computer system. I also see that the information in the file is also present in this message.
- Unfortunately, my attempts to save the work did not work. I tried to use the follow TCP command to show the message and have the ability to save the information in a separate file. But as you can see the program would not allow me to accomplish this step. I am not sure as what else to do except to directly copy and paste the information into a document which is not what I am supposed to do. At any rate, I hope to receive partial credit for this attempt.