CYSE 301: Cybersecurity Technique and Operations

Assignment 1: Traffic Tracing and Sniffing

Joshua Taylor

01031996

Each student needs to login into the **CCIA virtual environment** to complete this assignment.

Students use tshark will receive extra points.

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.

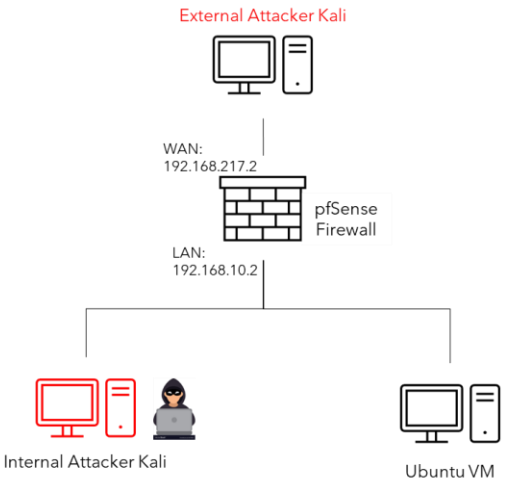


Figure 1 Required VMs for this assignment

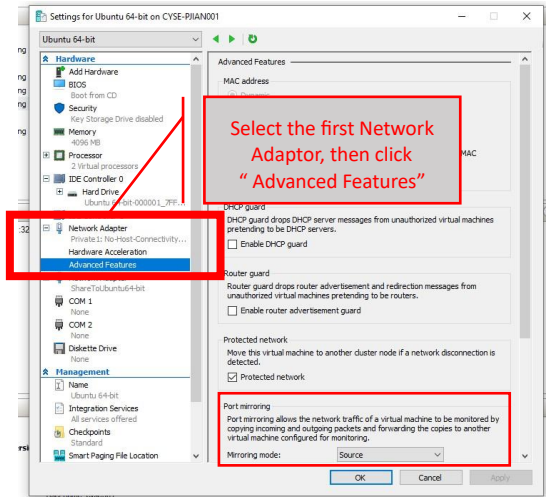


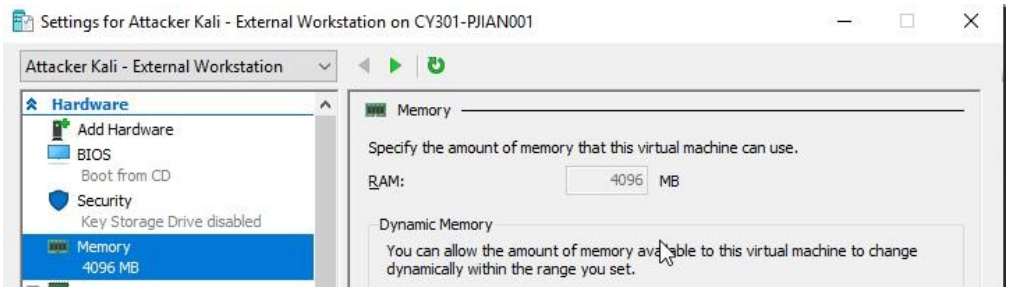
Figure 2 How to configure port mirroring in Hyper-V

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 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"

** 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.

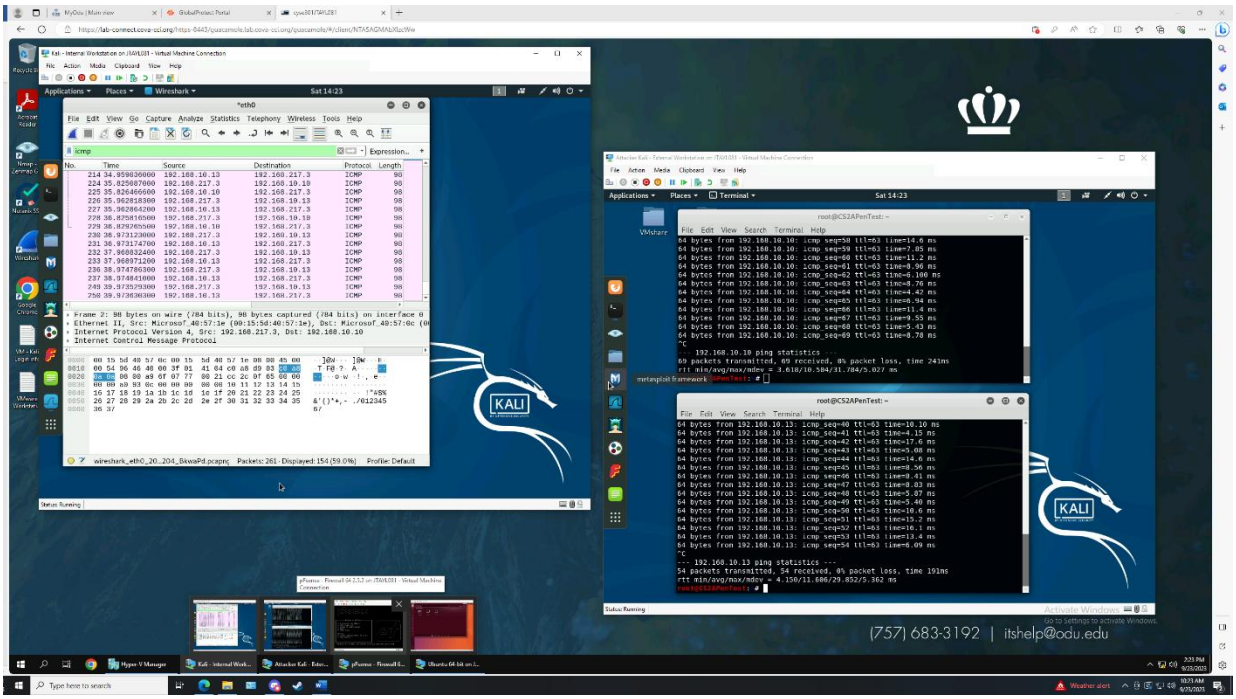


1. **Sniff ICMP traffic (10 + 10 = 20 points)**

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

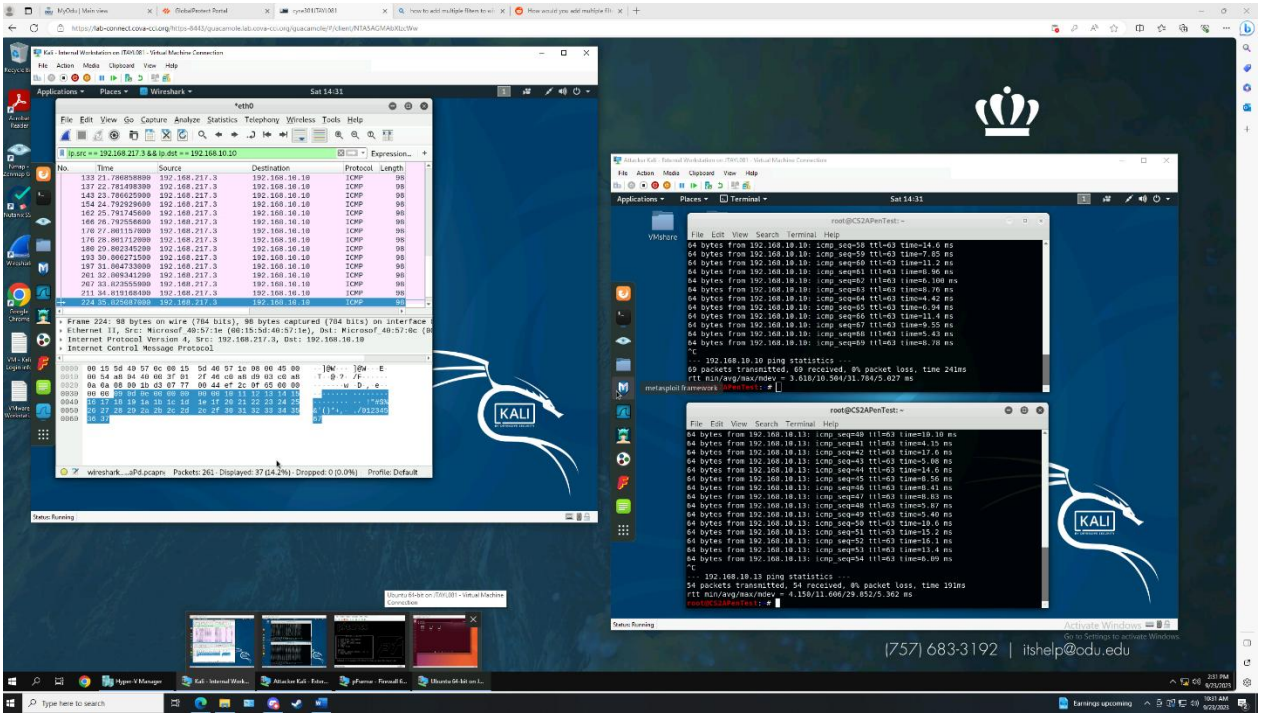
   a. Apply proper display or capture filter on **Internal Kali VM** to show active ICMP traffic.

   - On the external kali machine, I opened to terminals and pinged the 192.168.10.10 and 192.168.10.13, the ubuntu VM and internal Kali VM respectively. On the internal Kali VM I had Wireshark sniffing on ICMP traffic only.



   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.

   - In order to display only the ICMP requests originated from the external Kali (192.168.217.3) to the Ubuntu VM (192.168.10.10) I set the display filter as “ip.src == 192.168.217.3 && ip.dst == 192.168.10.10”. This filter allows for only the source IP of 192.168.217.3 and destination IP of 192.168.10.10 to be displayed.



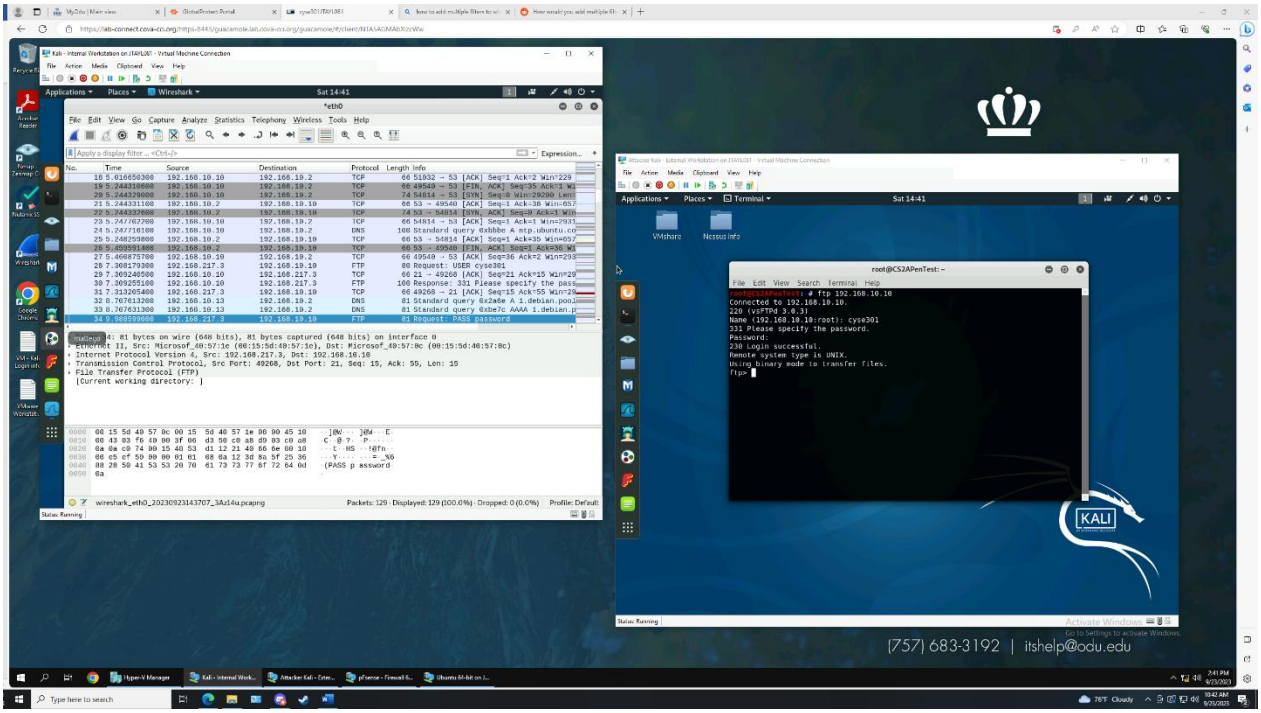
2. Sniff FTP traffic (10 + 15 + 15 = 40 pts points)

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.

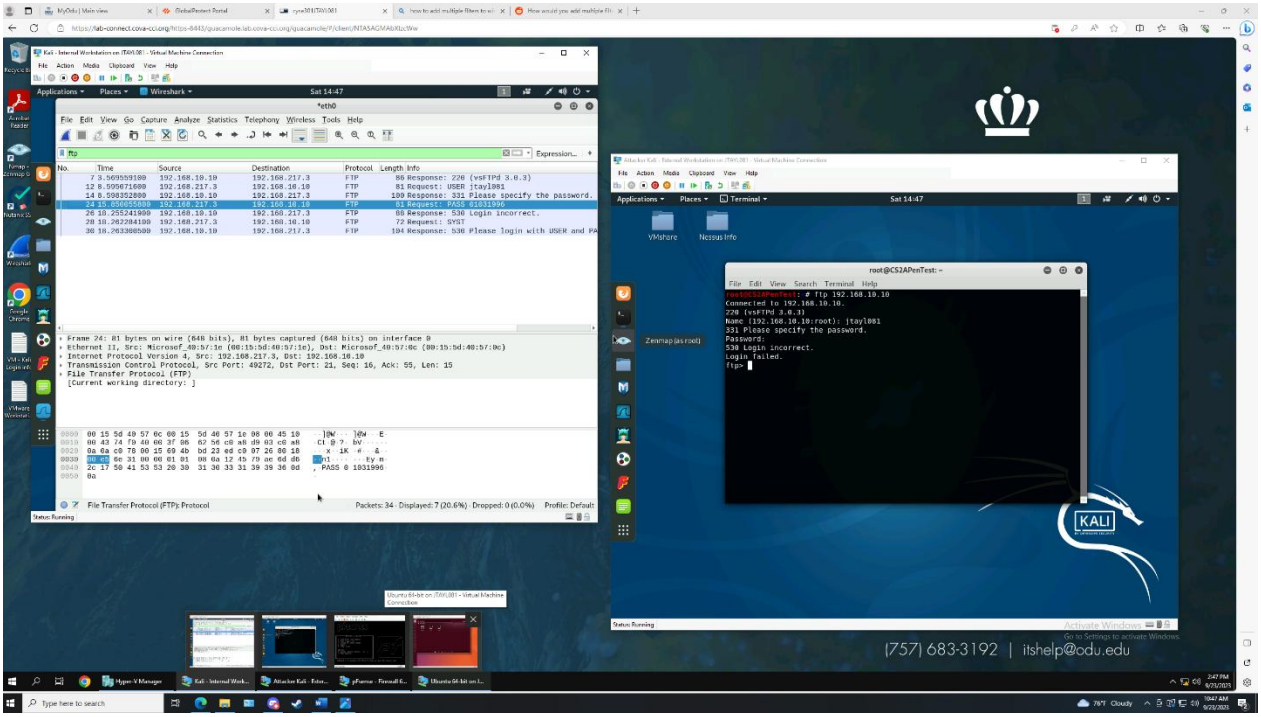
- After I began sniffing on the internal Kali machine, I conducted the login procedure indicated in the instructions above. After successfully logging in to the FTP server, I switched back to the internal Kali machine and looked for the protocol shown to be FTP. I did not put in the display filter “FTP” although it would have expedited my search for the correct packets. After located the FTP packets I looked in the info section of Wireshark for anything

indicating that it was the packet containing the cleartext username or password. In packet 28 and packet 34 I found the Username and Password respectively.



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**.

- Following the instructions, I attempted to regain entry to the ftp server using my Midas ID and UIN, which are jtayl081 and 01031996 respectively. The login attempt failed, however, after putting a display filter of “ftp” in Wireshark on the internal Kali machine I was able to locate in cleartext my attempt at logging in using those User and Passwords.

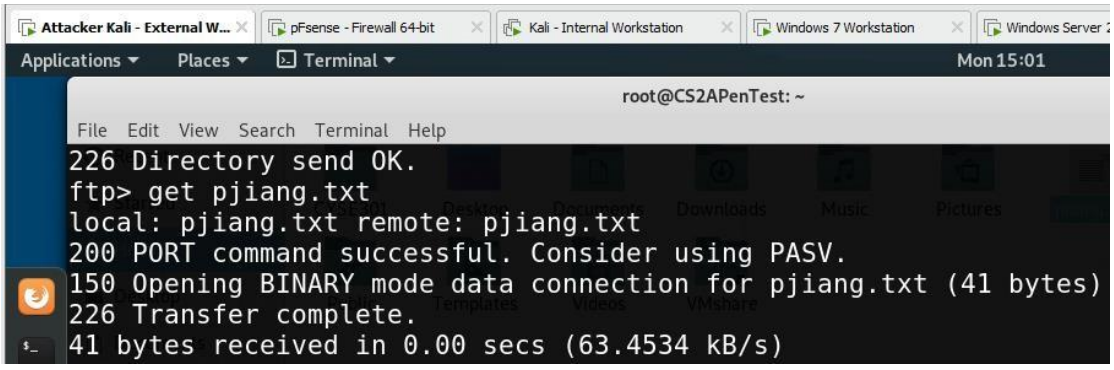


Task C – Extra credit: Steal files with Wireshark (15 points)

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.

```
cyse301@ubuntu:~$ echo -e "$(date) \nPeng Jiang"> pjiang.txt
cyse301@ubuntu:~$ ls
Desktop    Downloads          Music     pjiang.txt  Templates  VMshare
Documents  examples.desktop   Pictures  Public      Videos
cyse301@ubuntu:~$ cat pjiang.txt
Thu Feb 10 20:09:10 PST 2022
Peng Jiang
```

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.