CYSE 301: Cybersecurity Technique and Operations

Assignment 1: Traffic Tracing and Sniffing

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.

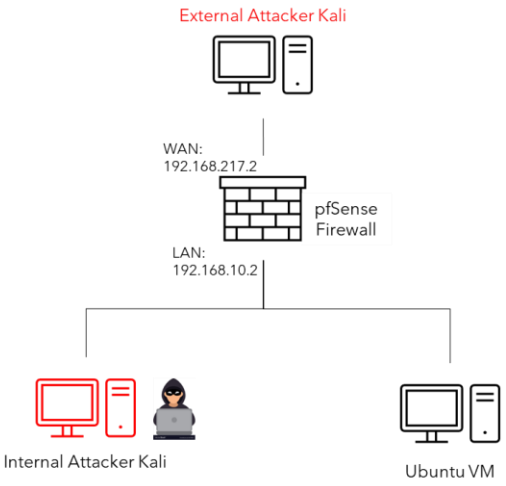


Figure 1 Required VMs for this assignment

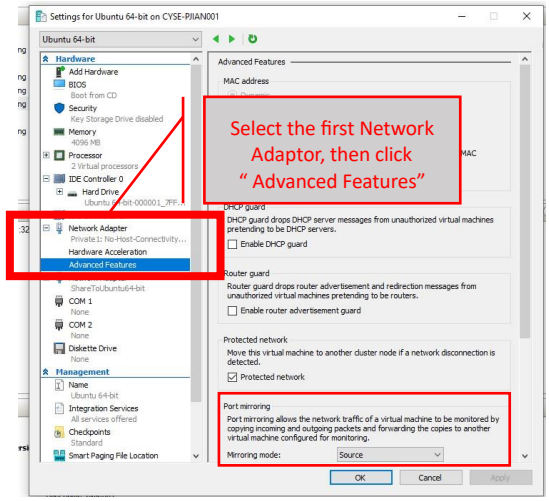


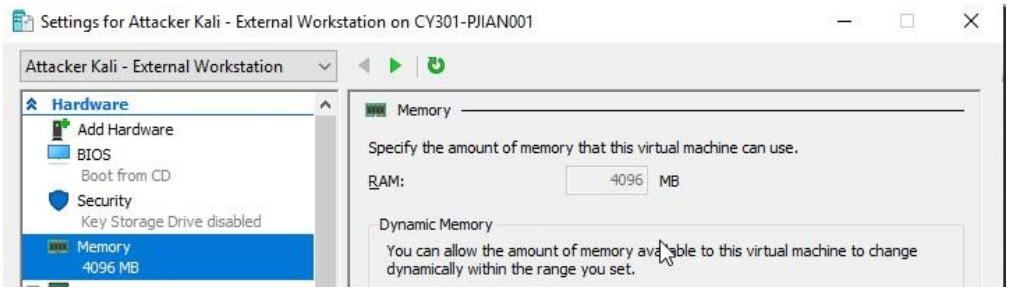
Figure 2 How to configure port mirroring in Hyper-V

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"

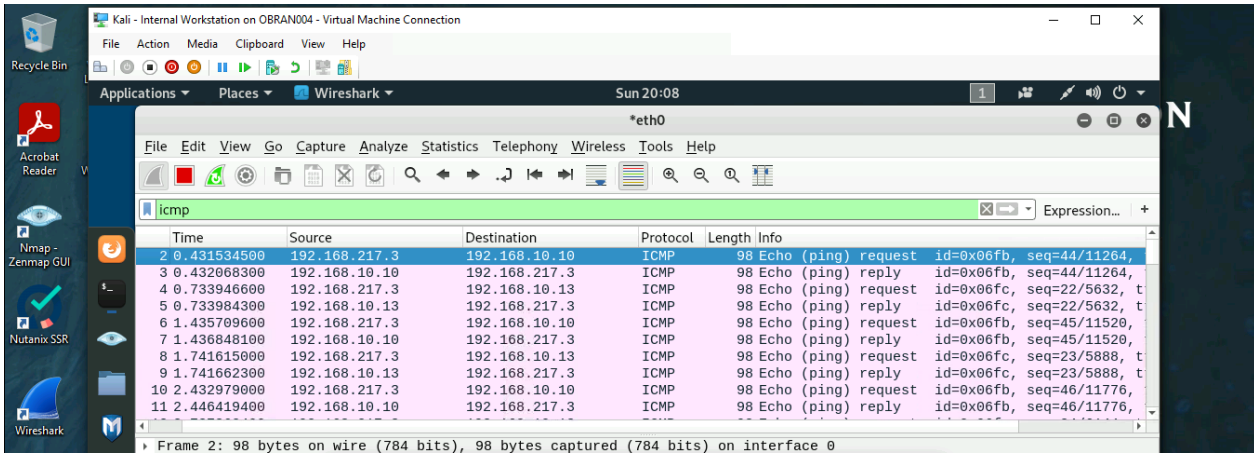
** Since each Windows 10 Host Machine has 20G memory. We need to adjust the assigned Memory for Internal Kali and External Kali from **8192** to **4096** MB to support 4 VM running simultaneously.



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.

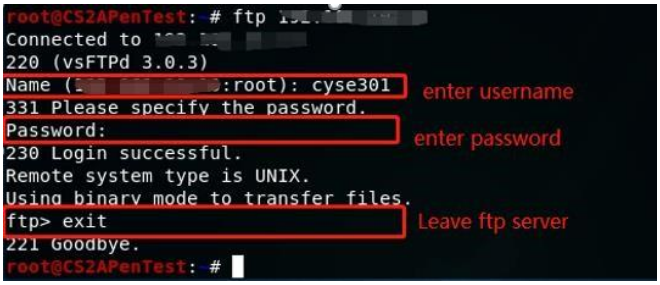


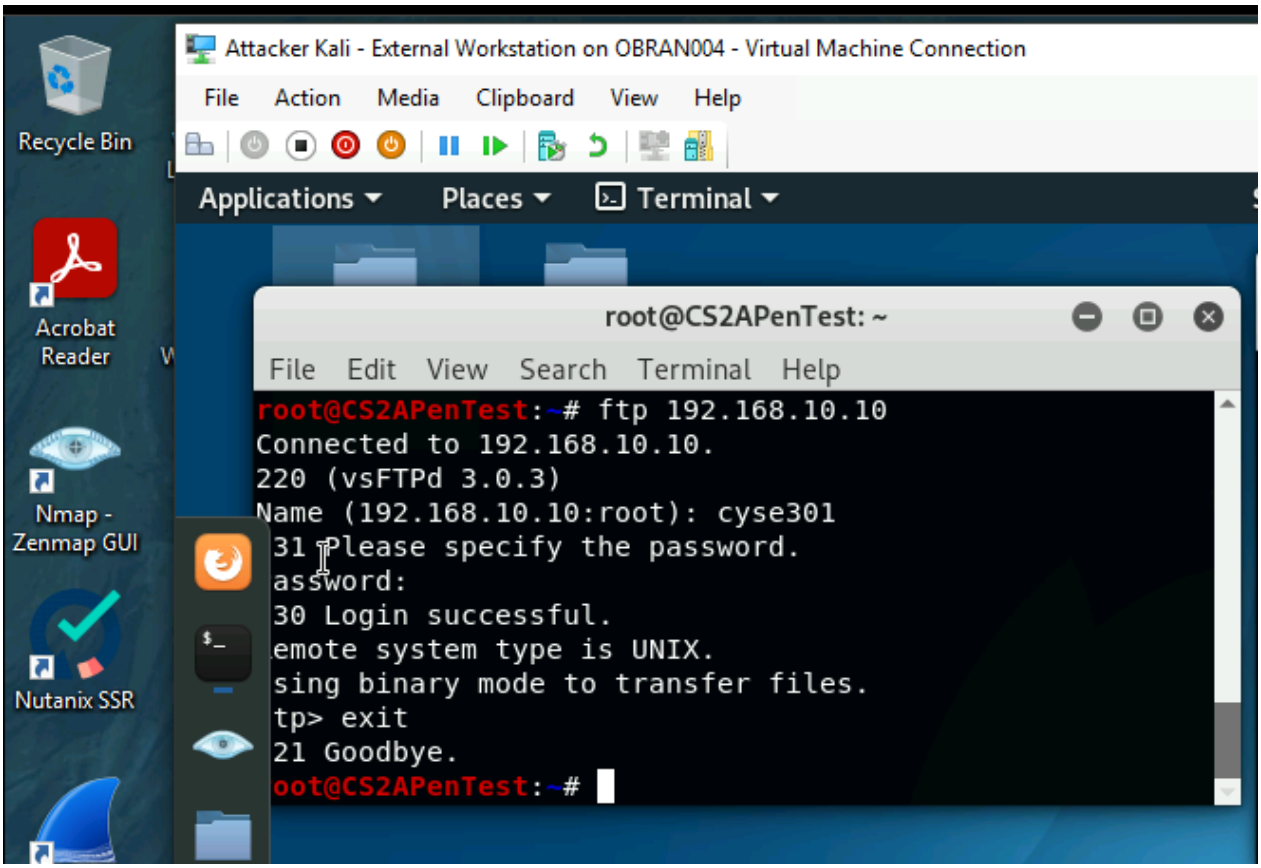
   b. Apply proper display or capture filter on **Internal Kali VM** that ONLY displays **ICMP request** originated from External Kali VM and goes to Ubuntu 64-bit VM.

```
1025 66.584800900  192.168.10.10   192.168.217.3   ICMP   98 Echo (ping) reply    id=0x06fb, seq=110/28
1034 66.866757900  192.168.217.3   192.168.10.13   ICMP   98 Echo (ping) request  id=0x06fc, seq=88/225
1035 66.866795100  192.168.10.13   192.168.217.3   ICMP   98 Echo (ping) reply    id=0x06fc, seq=88/225
1054 67.569304300  192.168.217.3   192.168.10.10   ICMP   98 Echo (ping) request  id=0x06fb, seq=111/28
1055 67.569708500  192.168.10.10   192.168.217.3   ICMP   98 Echo (ping) reply    id=0x06fb, seq=111/28
```

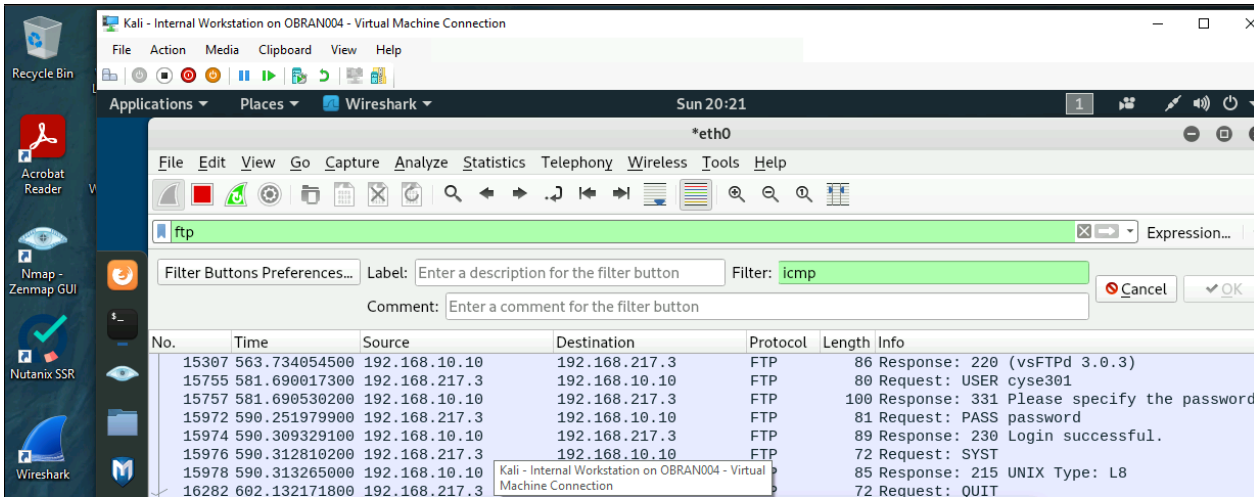
2. **Sniff FTP traffic (10 + 15 + 15 = 40 pts points)**

   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.





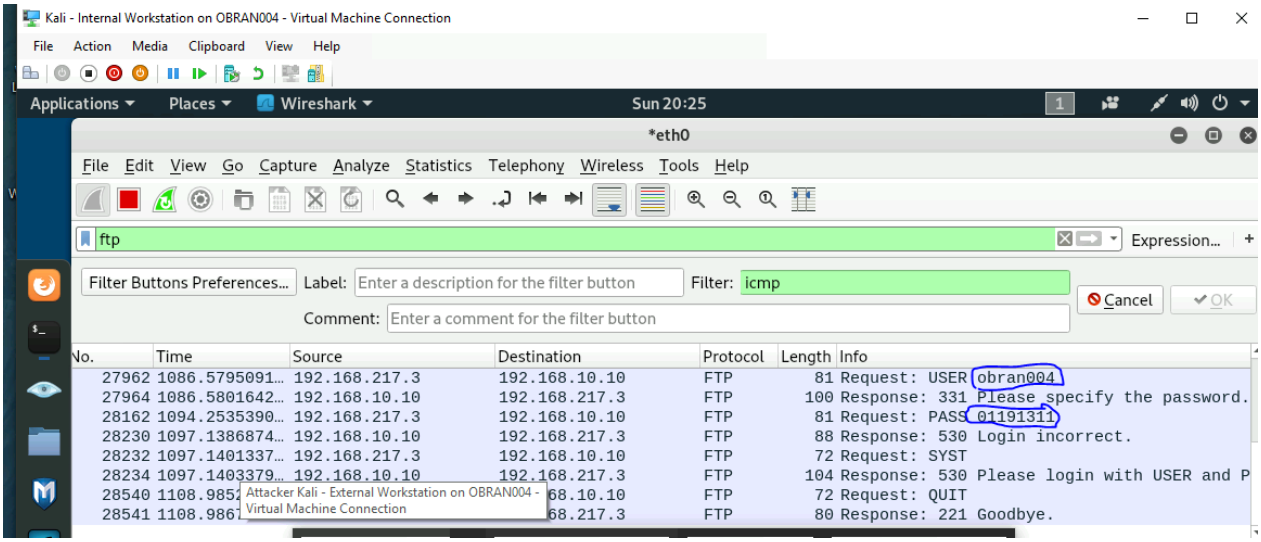
b. **Unfortunately**, Internal Kali, the attacker, is also sniffing to the communication. Therefore, all of your communication is exposed to the attacker. Now, you need to find out the **password** used by External Kali to access the FTP server from the intercepted traffic on Internal Kali. You need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



I filtered to ftp and once that was did the username and password showed in clear text.

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)