Old Dominion University

CYSE 301 Cybersecurity Techniques and Operations

Assignment #2-2 Traffic Tracing and Sniffing

Isaac Flores

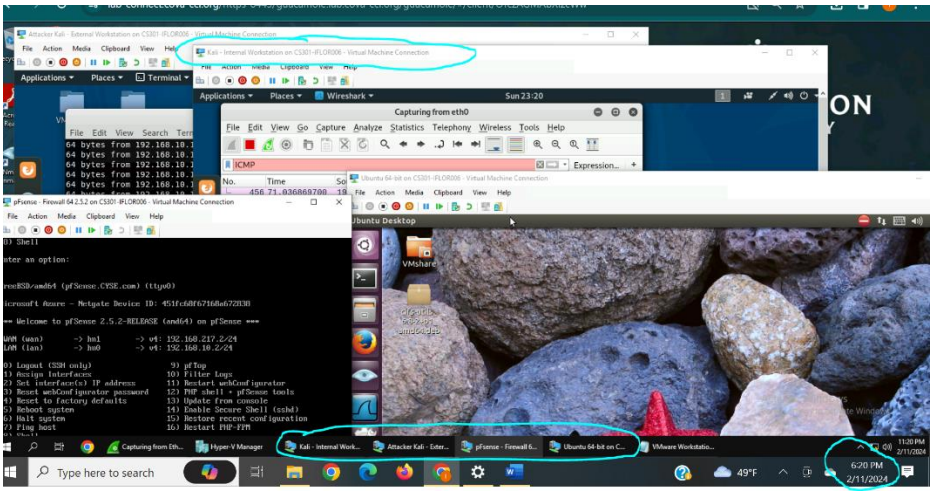
01270428

Task B

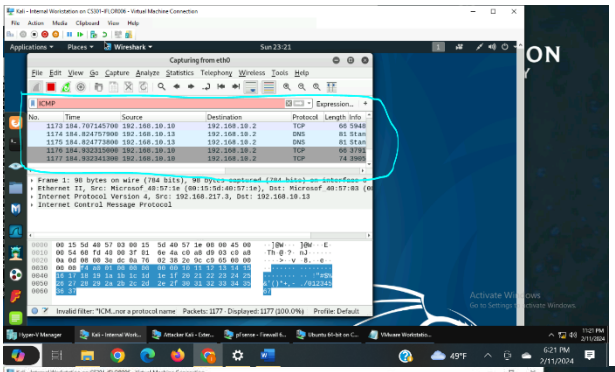
Open two terminals on External Kali VM. Use one ping Ubuntu VM, and use the other ping Internal Kali.

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

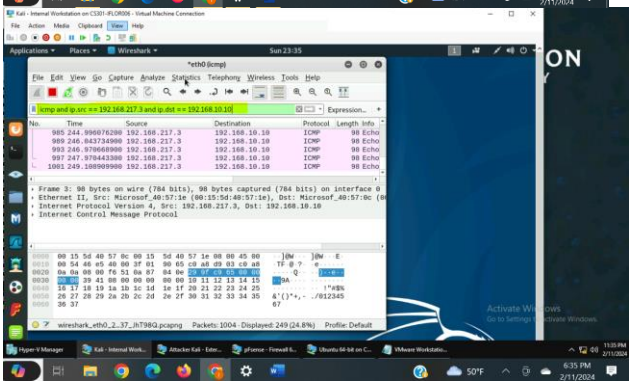
b. Apply proper display or capture filter on Internal Kali VM that ONLY displays ICMP request originated from External Kali VM and goes to Ubuntu 64-bit VM.



The image should show the timestamp of the work, virtual machines, and the running session.



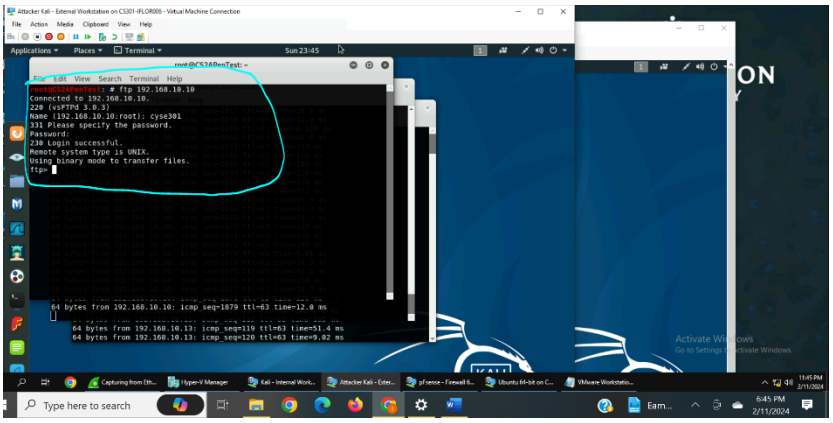
The image should show the use of the capture filter to display INTERNET Control Message Protocol (ICMP) packets.



The image should show the use of the

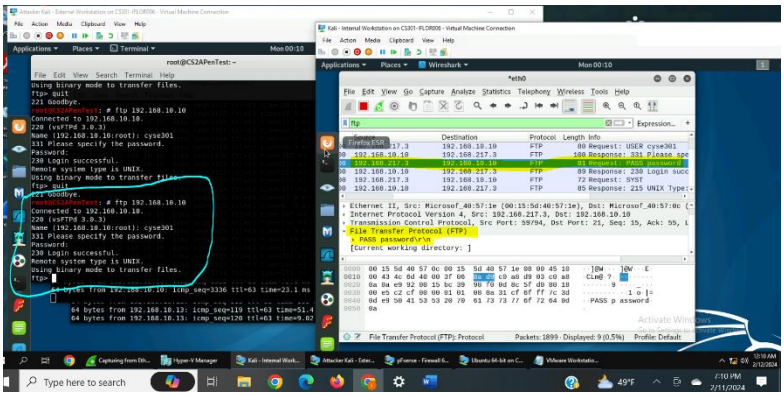
icmp and ip.src. == 192.168.217.3 and ip.dst == 192.168.10.10 command used in Wireshark to filter only icmp packets that are sent to the Ubuntu virtual machine from the External Kali virtual machine.

2. 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



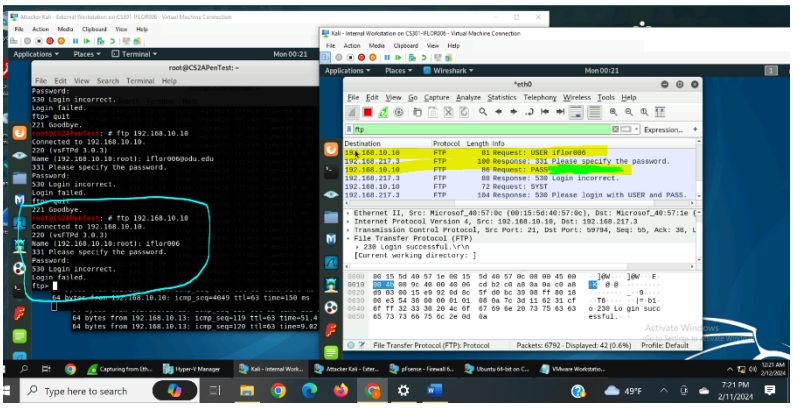
The image should show a new terminal window in External Kali to use the ftp 192.168.10.10. The username is specified as cyse301 and the password is password.

3. 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.



The image should display the ftp 192.168.10.10 command being used in the External Kali virtual machine terminal. Wireshark is used on the Internal Kali virtual machine to filter for ftp protocol packets using the ftp command. One of the packets had a password in the info section which is where I found the password. I also clicked on the packet and used the File Transfer Protocol (FTP) tab to find the password which was password.

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.



The image should show the use of the ftp 192.168.10.10 command in the External Kali virtual machine. Wireshark was used on the Internal Kali virtual machine to filter for FTP traffic using the ftp command to find the username and password. For privacy reasons, I decided to use the Pen tool in the Snipping Tool to mark on the password part in the info section.