OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment 1: Traffic Tracing and Sniffing

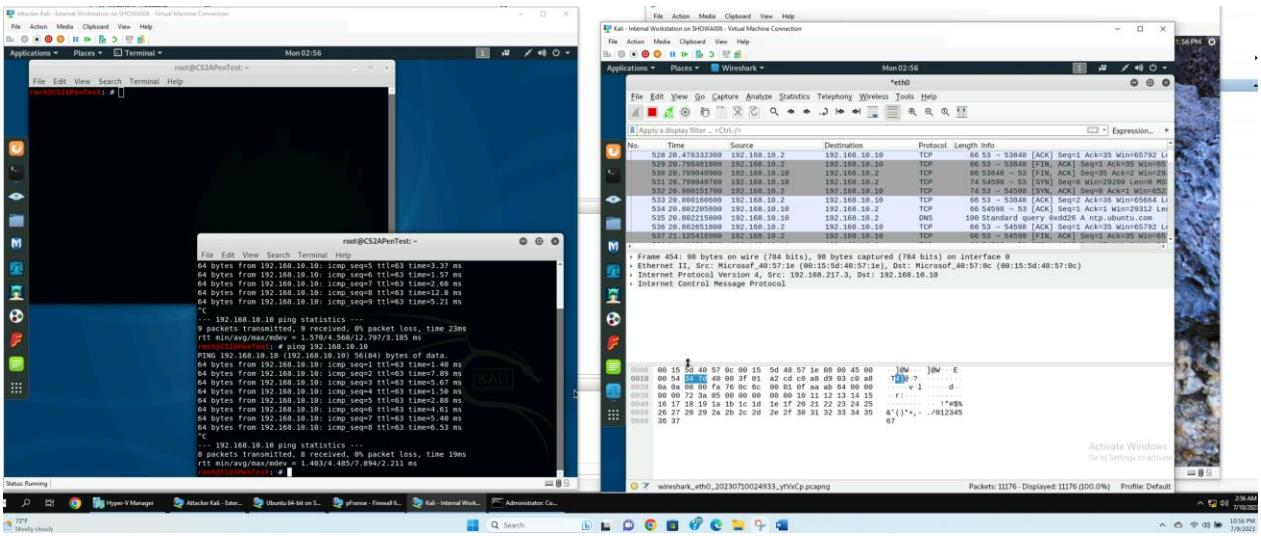
Stuart N. Howard

01241576

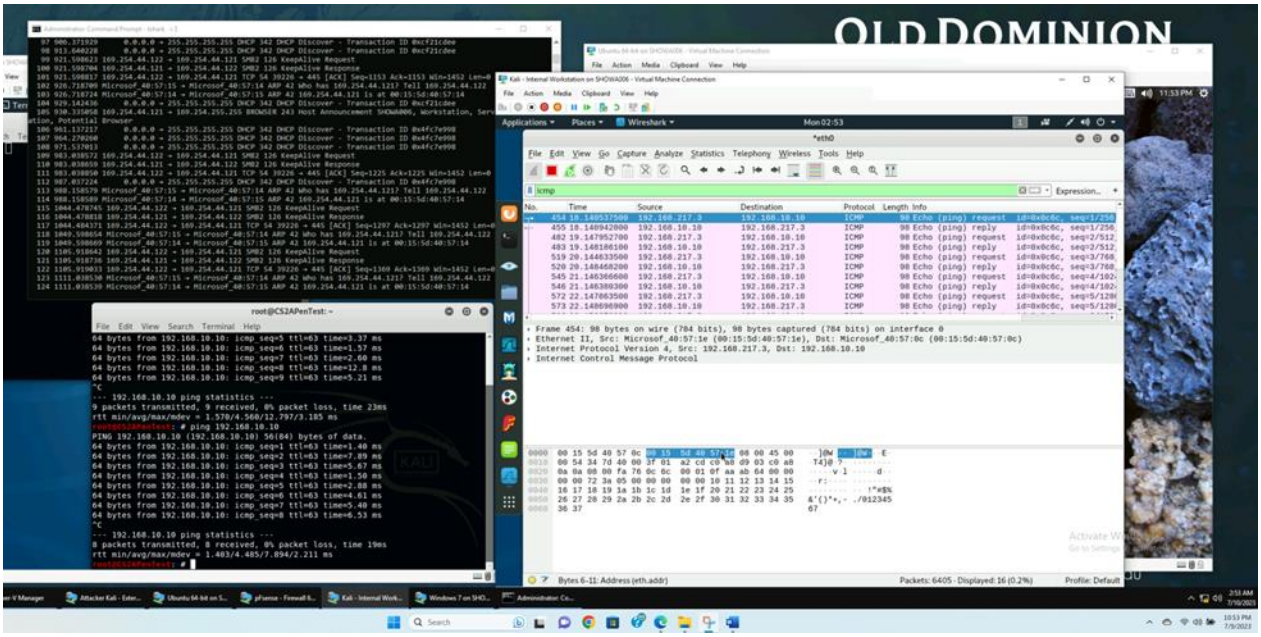
Task B: Sniff LAN traffic

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

    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.**

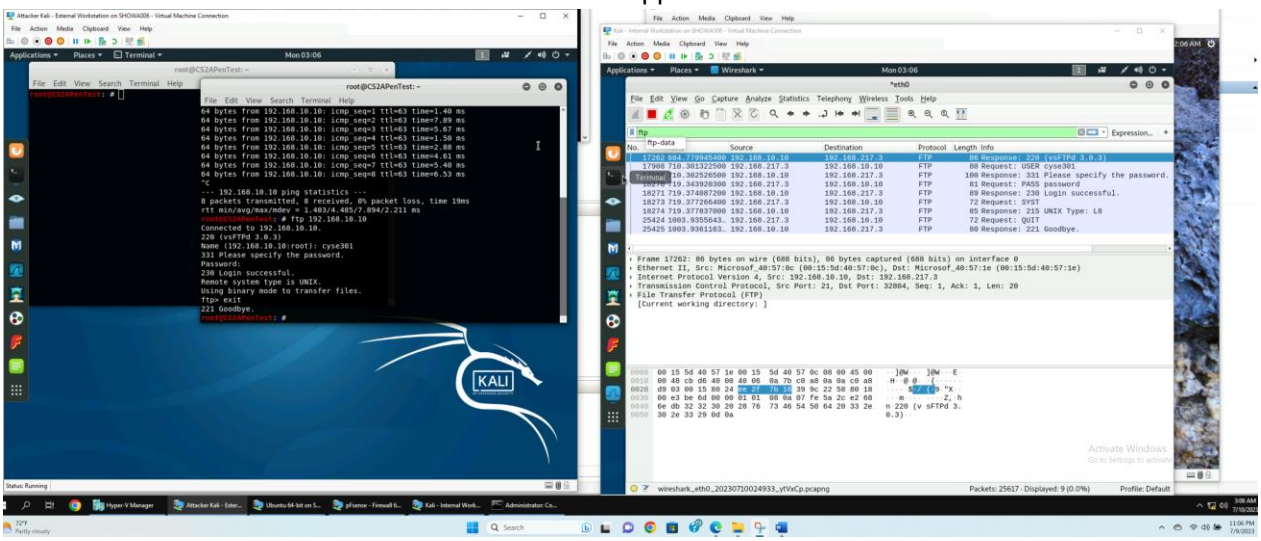


2. **Sniff FTP traffic (10 + 15 + 15 = 40 pts points)**

    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***

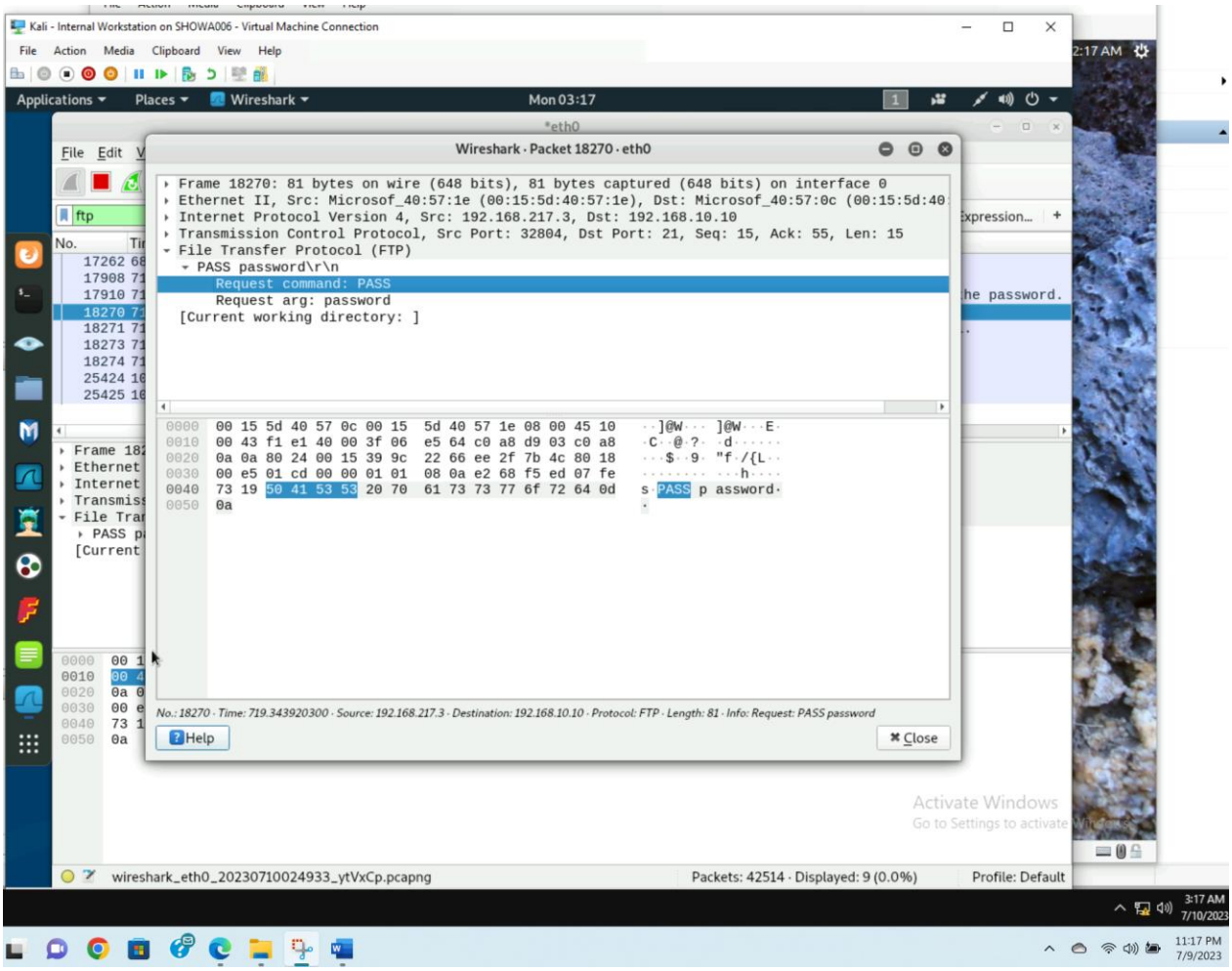
***ubuntu VM]*. The username for the FTP server is cyse301, and the password is password. You can follow the steps below to access the FTP server.**

Ran FTP with ubuntu IP address and applied FTP filter on internal Kali wireshark



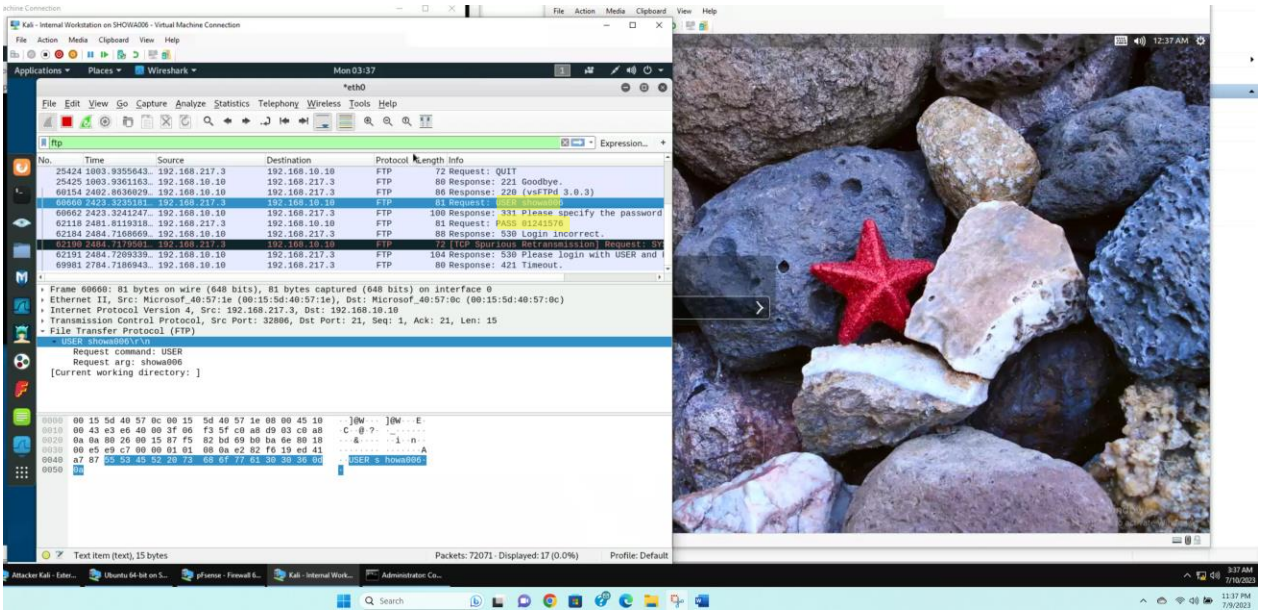
b. **Unfortunately, Internal Kali, the attacker, is also sniffing to the communication. Therefore, all of your communication is exposed to the attacker. Now, you need to find out the password used by External Kali to access the FTP server from the intercepted traffic on Internal Kali. You need to screenshot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

Analyze the internal Kali captured packets in to find the FTP communication between External Kali and the FTP server. Look for packets with information related to FTP . View the packet details in Wireshark to locate the password. Found a field that said "PASS" in the FTP protocol section.



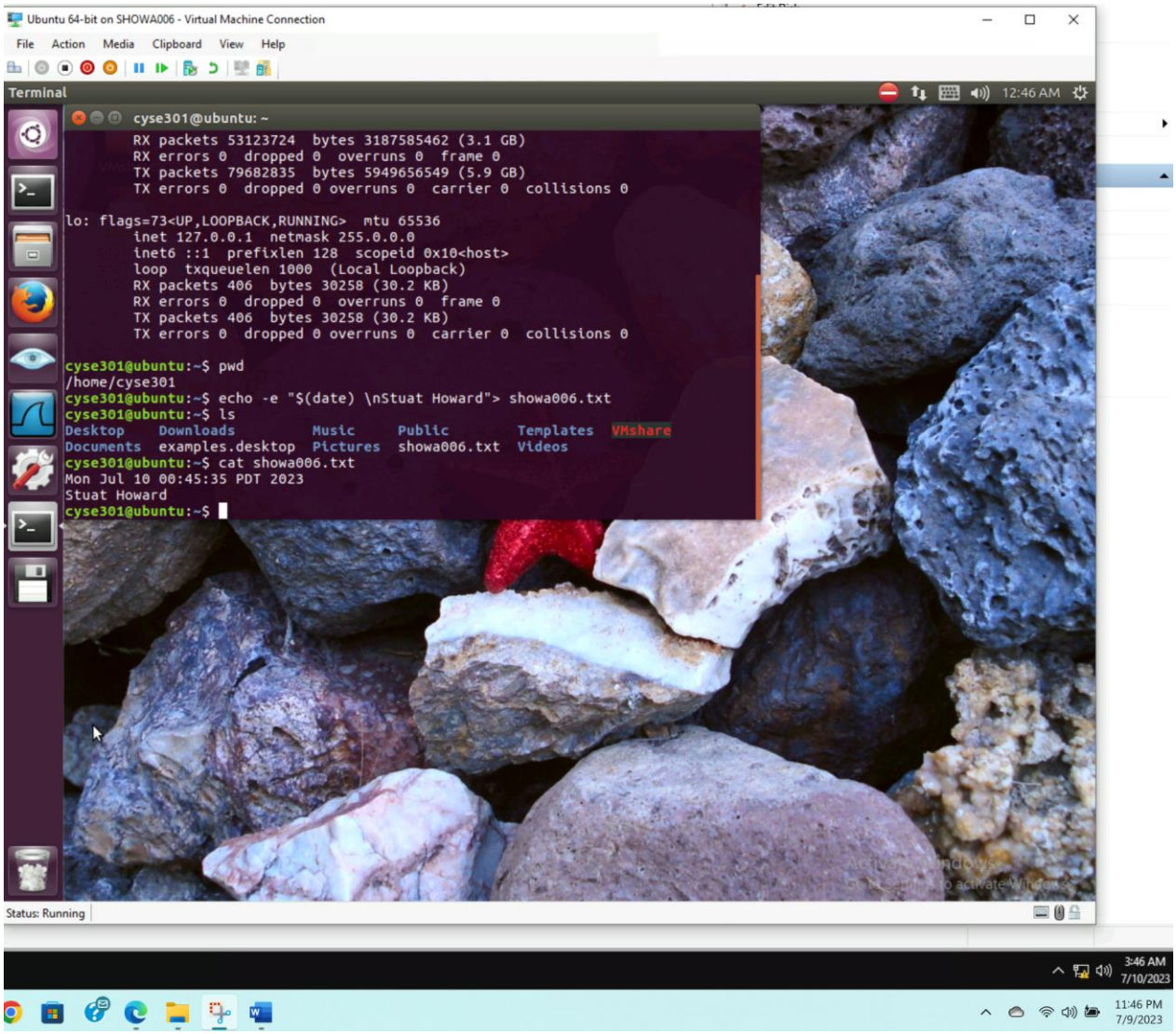
c. **After you successfully find the username & password from the FTP traffic, repeat the previous step (2.a), and use your MIDAS ID as the username and UIN as the password to reaccess the FTP server from External Kali. Although External Kali may not access the FTP server, you need to intercept the packets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

Analyze the internal Kali captured packets in to find the FTP communication between External Kali and the FTP server. Look for packets with information related to FTP . View the packet details in Wireshark to locate the password. Found a fields that captured used new and password the FTP protocol section.



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 with FTP protocol remotely. Below is an example.

To retrieve the from the Ubuntu VM using the FTP protocol

- Use the ftp command to connect to the FTP server running on Ubuntu.
- enter the FTP username (cyse301) and password (password) to authenticate and establish the FTP connection.
- Once connected, use the `get` command to download the file from the FTP server. Enter the

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.**

   Open the capture file containing the FTP traffic between External Kali and the Ubuntu VM. Enter display filter to show only FTP-DATA packets