CYSE 301: Cybersecurity Technique and Operations

Assignment 2: Traffic Tracing and Sniffing

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

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 **Ubuntu VM**. You need to use the following VMs to complete the assignment.

I recommend you keep the Wireshark/tshark running in the background all the time.

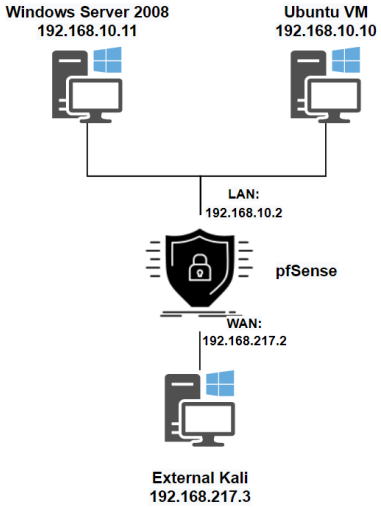


Figure 1 Required VMs for this assignment

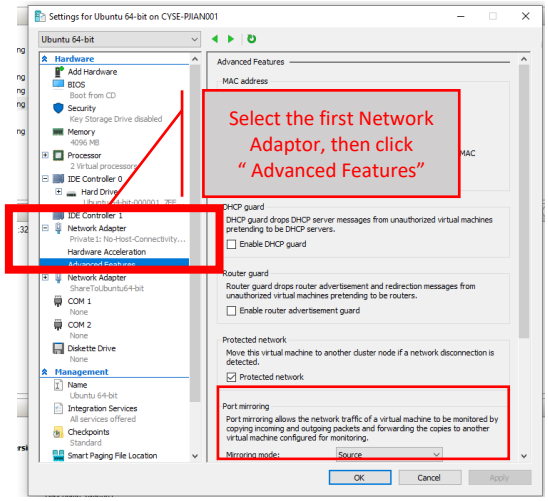


Figure 2 How to configure port mirroring in Hyper-V

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 (Ubuntu VM) as the ***mirroring Destination,*** and the target VMs are the ***mirroring Source*** (Figure 2).

To be specific,

- Ubuntu VM: Set Mirroring mode to "***Destination***" in the "Port Mirroring."
- Windows Server 2008: Set Mirroring mode to "***Source***" in the "Port Mirroring."
- External Kali: Set Mirroring mode to "***Source***" in the "Port Mirroring."

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

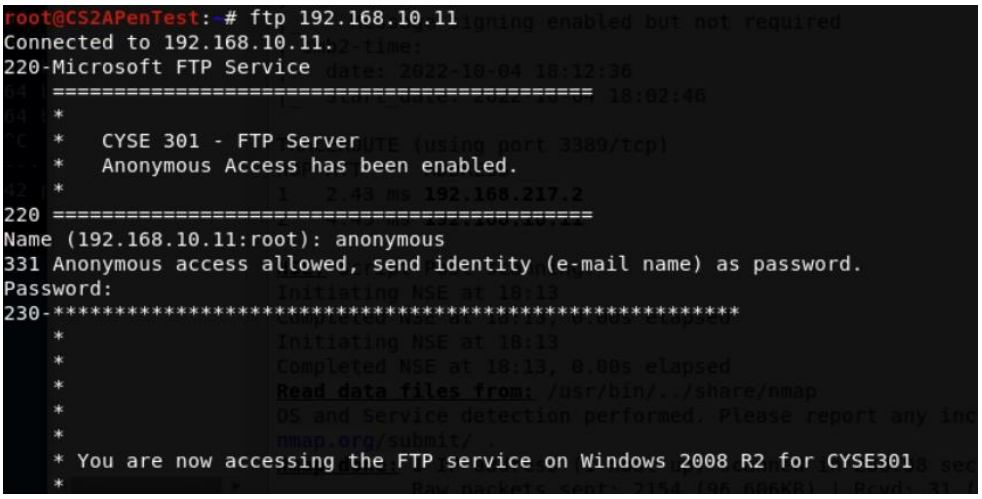
   1.1. In External Kali VM, ping Windows Server 2008 and Ubuntu VM from two separate terminals.

   1.2. Apply proper display or capture filter on **Ubuntu VM** to show all ping traffic (towards both Ubuntu and Windows Server 2008) (tip: you can filter the traffic by protocol type).

   1.3. Apply proper display or capture filter on **Ubuntu VM** that ONLY displays **ICMP request** originated from External Kali VM and goes to Windows Server 2008 (tip: you can filter the traffic by IP address).

2. **Sniff FTP traffic (60 points)**

   Windows Server 2008 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 Windows Server 2008]*. The username for the FTP server is **anonymous**, and the password is **password**. You can follow the steps below to access the FTP server.

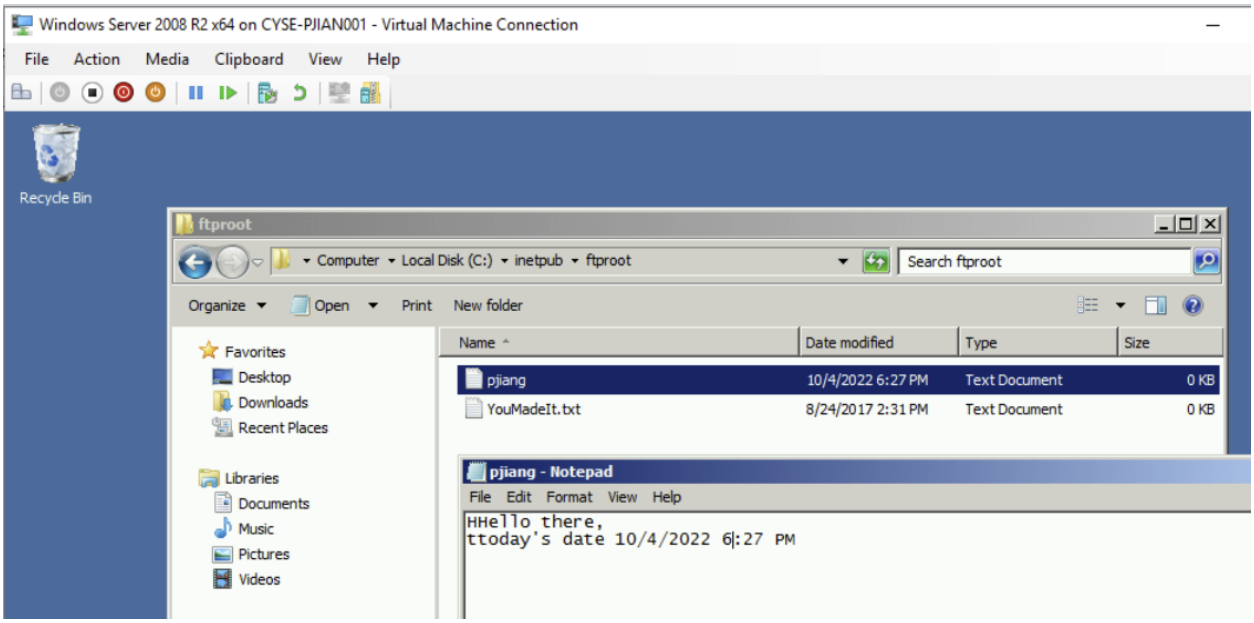


   2.1. **Unfortunately**, Ubuntu VM, the attacker, is also sniffing the internal communication by using **tshark**. So, all of your communication is exposed to the attacker. Now, you need to find out the username and password entered in the External Kali in the **Wireshark** running on Ubuntu VM. You need to screenshot and explain how you find the password.

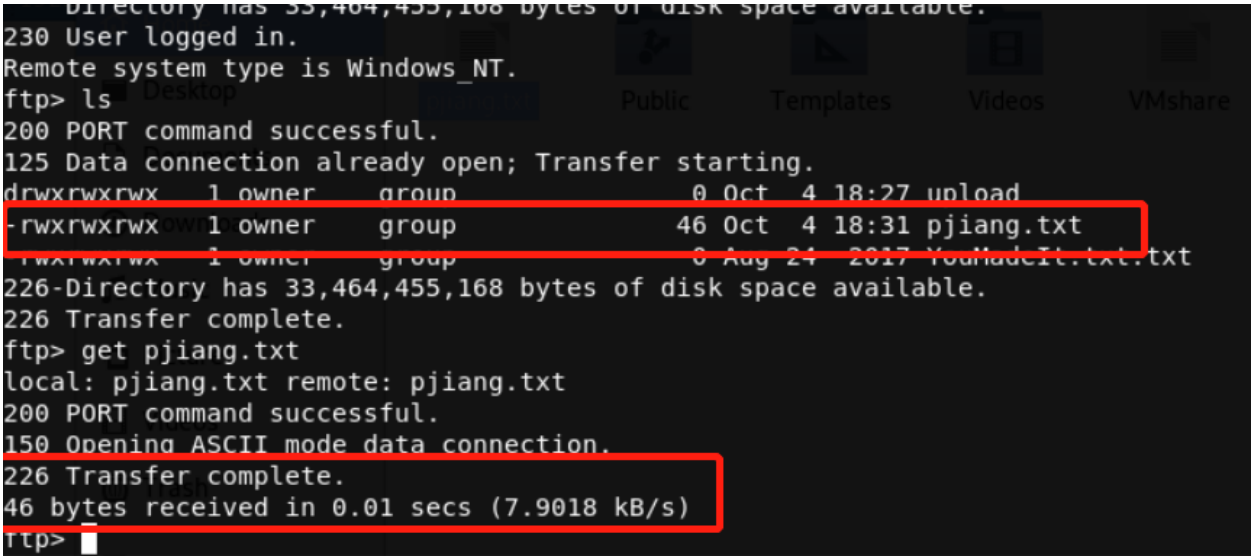
   2.2. After you successfully sniffed the username & password from the FTP traffic, repeat the previous step, and use your **MIDAS ID** as the username and **UIN** as the password to reaccess the FTP server from External Kali. Although External Kali may not access the FTP server, you need to intercept the packets containing these “secrets” from the attacker VM, which is **Ubuntu Kali**.

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

Log in to Windows Server 2008 VM, and create a file in "C:/inetpub/ftproot/" named "YOUR_MIDAS.txt". Put the current timestamp and your name in the file.

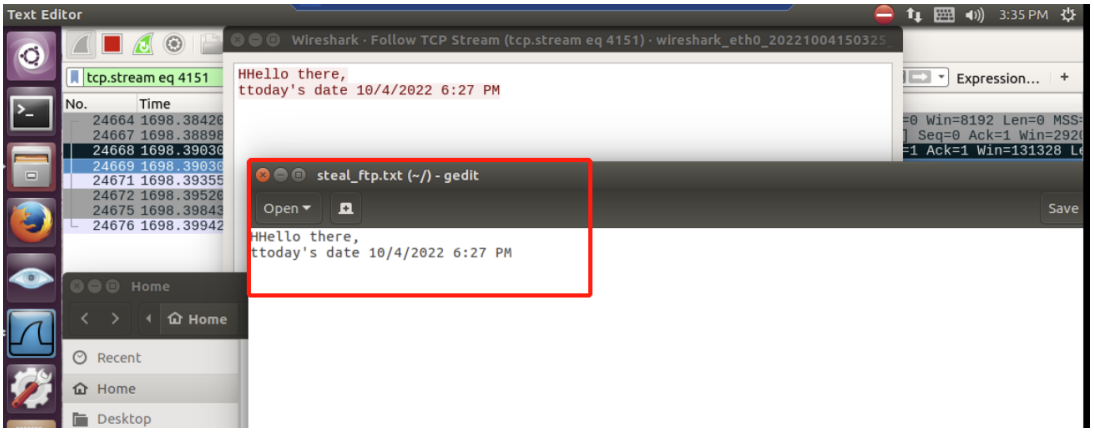


Once you have the file ready in Windows Server 2008, switch back to **External Kali**. Get the file you just created with FTP protocol remotely. Below is an example.



As an attacker, you need to complete the following tasks in Ubuntu VM to steal the file just transferred :

1. Apply a proper display filter to display the **FTP-DATA** packets between External Kali and Windows Server 2008.
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 Ubuntu VM and view the content. Below is an example.


Text Editor
3:35 PM
Wireshark · Follow TCP Stream (tcp.stream eq 4151) · wireshark_eth0_20221004150325
HHello there,
ttoday's date 10/4/2022 6:27 PM
tcp.stream eq 4151
Expression...
No.
Time
24664 1698.38420
24667 1698.38898
24668 1698.39030
24669 1698.39036
24671 1698.39355
24672 1698.39520
24675 1698.39843
24676 1698.39942
steal_ftp.txt (~/) - gedit
Open
Save
HHello there,
ttoday's date 10/4/2022 6:27 PM
Home
Recent
Home
Desktop