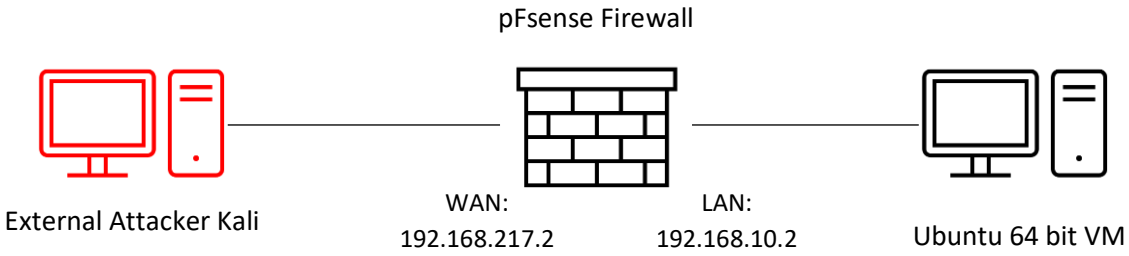
CYSE 301: Cybersecurity Technique and Operations

Assignment 2: Traffic Tracing and Sniffing

Each student needs to login into the **CCIA virtual environment** to complete this assignment. Please make sure to power on the pfsense VM at all times to keep the VMs connected.

Task A: Get started with Wireshark (5 point each x 6 questions = 30 points)

In this task, you will be using Wireshark on External Kali to monitor the traffic when External Kali and Ubuntu VM are talking to each other.



You should keep Wireshark running in the background while performing the following tasks.

1. Open Wireshark on External Kali and listen on interface "eth0".
2. Open a new terminal, then ping the Ubuntu VM for 5 – 10 seconds.
3. Open a new web browser tab in Kali Linux (even if no webpage will be displayed), and keep it for a couple of seconds.
4. **Stop capturing (the red button on the tool bar).**

Now, answer the following questions. You need to provide a screenshot that contains the answers to each question.

Q1. How many packets are captured in total? How many packets are displayed?

Q2. Apply "ICMP" as a display filter in Wireshark. Then repeat the previous question (Q1).

Q3. Select an Echo (replay) message from the list. What are the source and destination IPs of this packet? What are the sequence number and the size of the data? What is the response time?

Q4. Apply "DNS" as a display filter in Wireshark. How many packets are displayed?

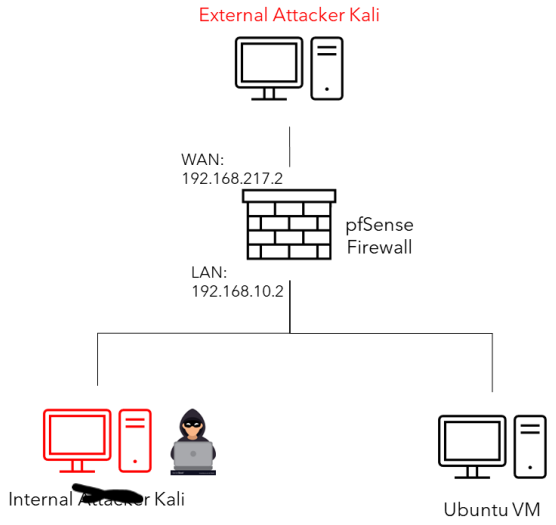
Q5. Find a DNS query packet. What is the domain name this host is trying to resolve? What is the source IP and port number, destination IP and port number? Please express in the format: **IP:port.**

Q6. Find the **corresponding** DNS response to the query you selected at the previous step, and what is the source IP and port number, destination IP and port number? What is the message replied from the DNS server?

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 keep the Wireshark/tshark running on Internal Kali all the time.

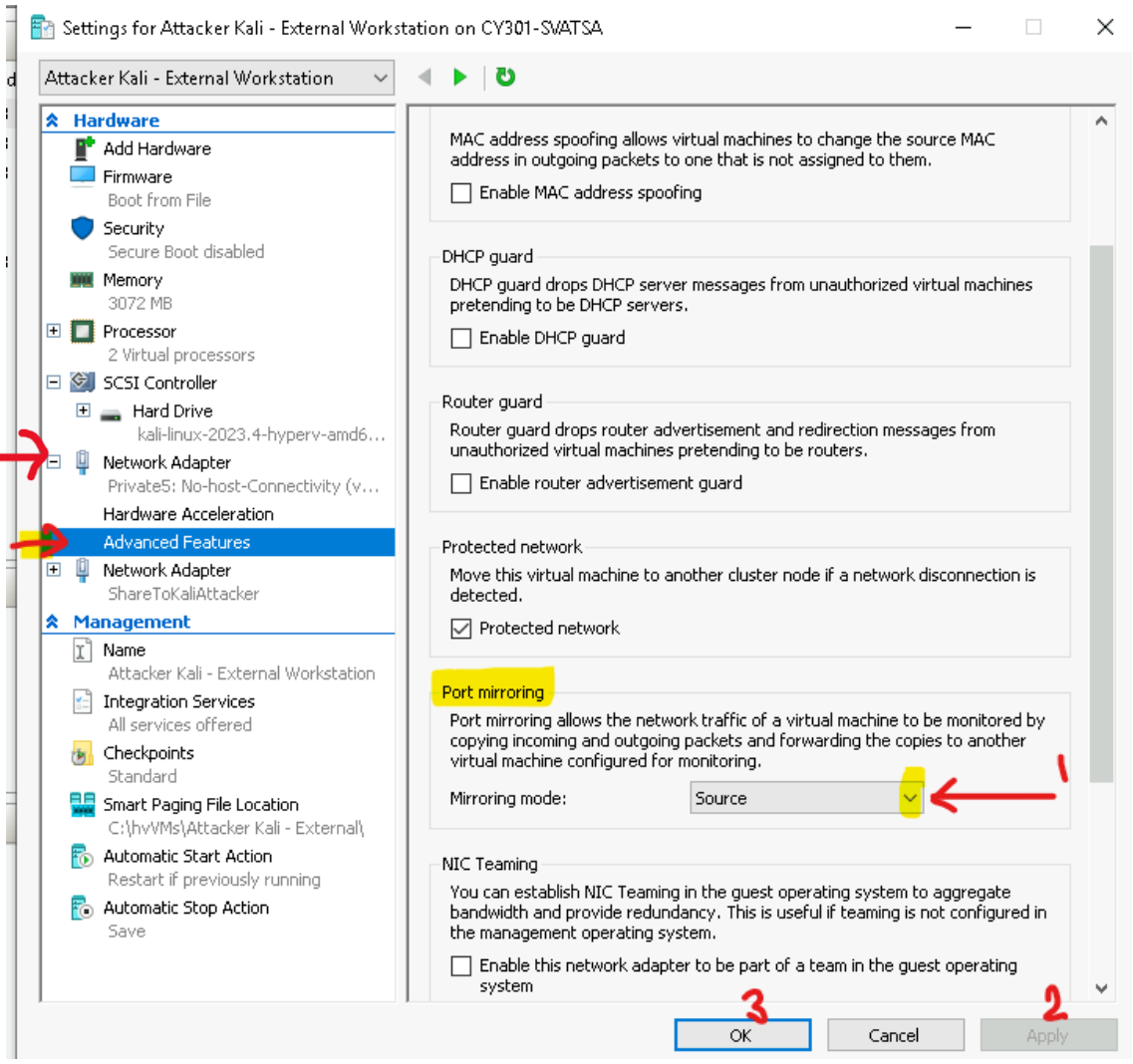


IMPORTANT NOTES!

* 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). Each VM has two network adapters, one for regular connection and the other for sharing with the CCIA server. We need to configure port mirroring on the **first** adapter. To be specific,

- Internal Kali: Set Mirroring mode to "***Destination***" in the "Port Mirroring"
- Ubuntu Kali: Set Mirroring mode to "***Source***" in the "Port Mirroring"
- External Kali: Set Mirroring mode to "***Source***" in the "Port Mirroring"

Figure 1 Required VMs for this assignment


Settings for Attacker Kali - External Workstation on CY301-SWATSA
Attacker Kali - External Workstation
Hardware
Add Hardware
Firmware
Boot from File
Security
Secure Boot disabled
Memory
3072 MB
Processor
2 Virtual processors
SCSI Controller
Hard Drive
kali-linux-2023.4-hyperv-amd6...
Network Adapter
Private5: No-host-Connectivity (v...
Hardware Acceleration
Advanced Features
Network Adapter
ShareToKaliAttacker
Management
Name
Attacker Kali - External Workstation
Integration Services
All services offered
Checkpoints
Standard
Smart Paging File Location
C:\hvVMs\Attacker Kali - External\
Automatic Start Action
Restart if previously running
Automatic Stop Action
Save
MAC address spoofing allows virtual machines to change the source MAC address in outgoing packets to one that is not assigned to them.
Enable MAC address spoofing
DHCP guard
DHCP guard drops DHCP server messages from unauthorized virtual machines pretending to be DHCP servers.
Enable DHCP guard
Router guard
Router guard drops router advertisement and redirection messages from unauthorized virtual machines pretending to be routers.
Enable router advertisement guard
Protected network
Move this virtual machine to another cluster node if a network disconnection is detected.
Protected network
Port mirroring
Port mirroring allows the network traffic of a virtual machine to be monitored by copying incoming and outgoing packets and forwarding the copies to another virtual machine configured for monitoring.
Mirroring mode:
Source
NIC Teaming
You can establish NIC Teaming in the guest operating system to aggregate bandwidth and provide redundancy. This is useful if teaming is not configured in the management operating system.
Enable this network adapter to be part of a team in the guest operating system
1
2
3
OK
Cancel
Apply

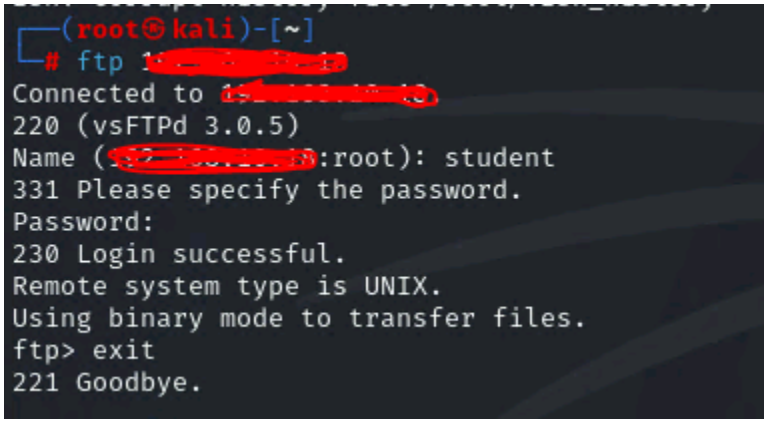
1. **Sniff ICMP traffic (10 + 10 = 20 points)**

   Please turn on Attacker/External Kali, internal kali, pfsense, and Ubuntu
   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 in Wireshark on **Internal Kali VM** to show active ICMP traffic.
   b. Apply a proper display or capture filter on the internal Kali VM that ONLY displays the ICMP request that originated from the external Kali VM and goes to the 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 student, and the password is **password**. You can follow the steps below to access the FTP server.



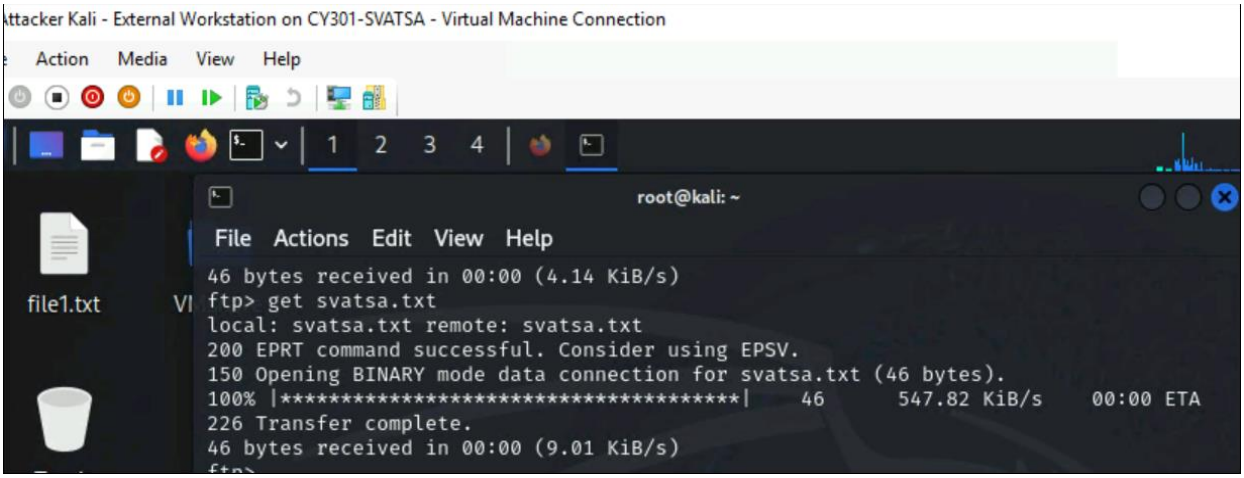
   b. **Unfortunately**, Internal Kali, the attacker, is also sniffing into the communication. Therefore, all of your communication is exposed to the attacker. Now, you need to find out the **password** used by External Kali to access the FTP server from the intercepted traffic on Internal Kali. You need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

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.

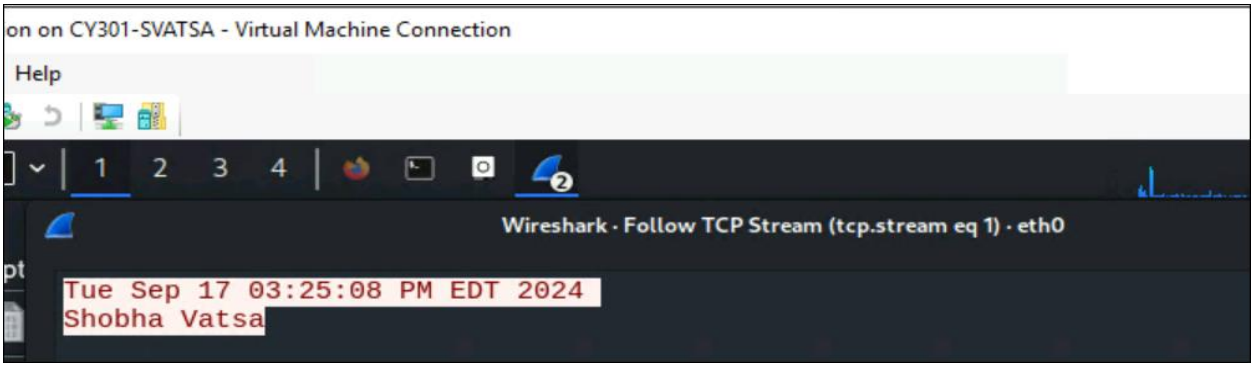
```
student@ubuntu:~$ echo -e "$(date) \nShobha Vatsa" > svatsa.txt
student@ubuntu:~$ ls
Desktop     examples.desktop  newDir1       Public  svatsa.txt  Videos
Documents   forVatsa.txt      passwd_Vatsa  snap    Templates   VMshare
Downloads   Music             Pictures      svatsa  Vatsa
student@ubuntu:~$ cat svatsa.txt
Tue Sep 17 03:25:08 PM EDT 2024
Shobha Vatsa
student@ubuntu:~$
```

Once you have the file ready in Ubuntu, switch back to **External Kali**. Get the file you just created remotely using the FTP protocol. 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 an example.


on on CY301-SVATSA - Virtual Machine Connection
Help
1
2
3
4
Wireshark · Follow TCP Stream (tcp.stream eq 1) · eth0
Tue Sep 17 03:25:08 PM EDT 2024
Shobha Vatsa