# CYSE 301: Cybersecurity Technique and Operations

## Assignment 3: Sword vs. Shield

In this assignment, you will act as an attacker to identify the vulnerabilities in the LAN network and a defender to apply proper countermeasures. You need to provide a screenshot for each task below.

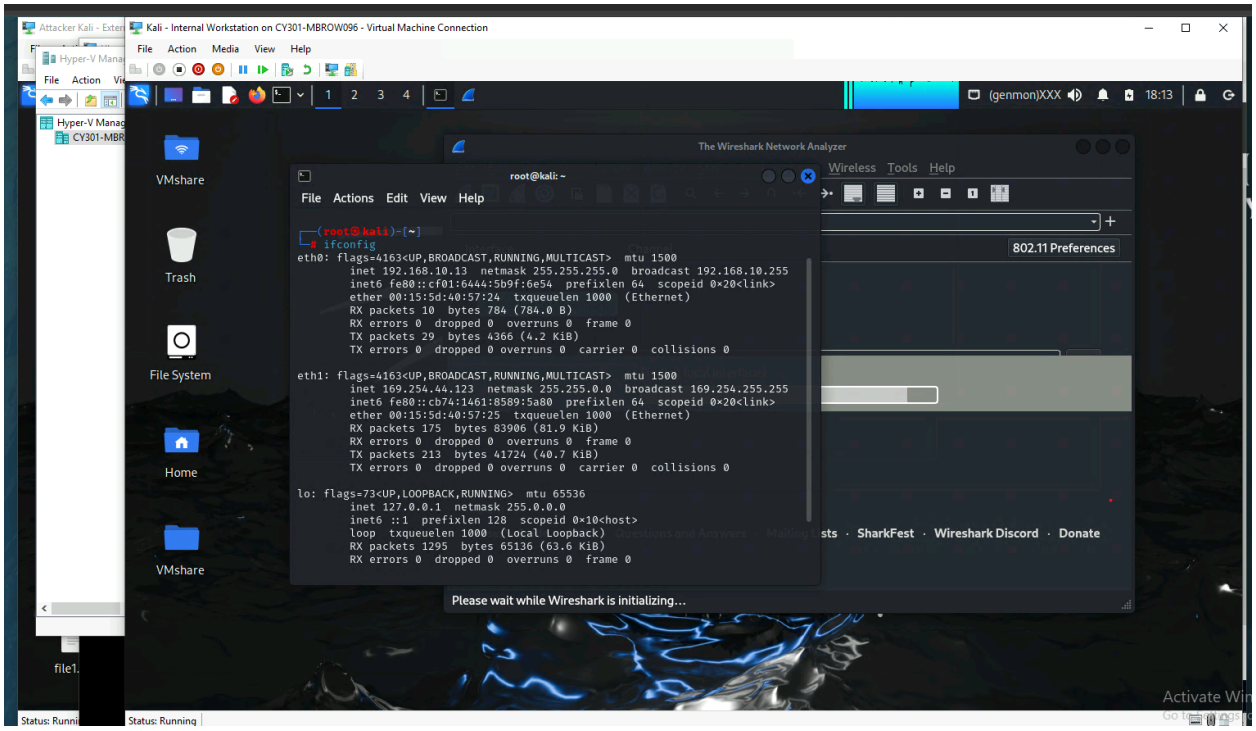
**Task A: Sword - Network Scanning (20+ 20 = 40 points)**

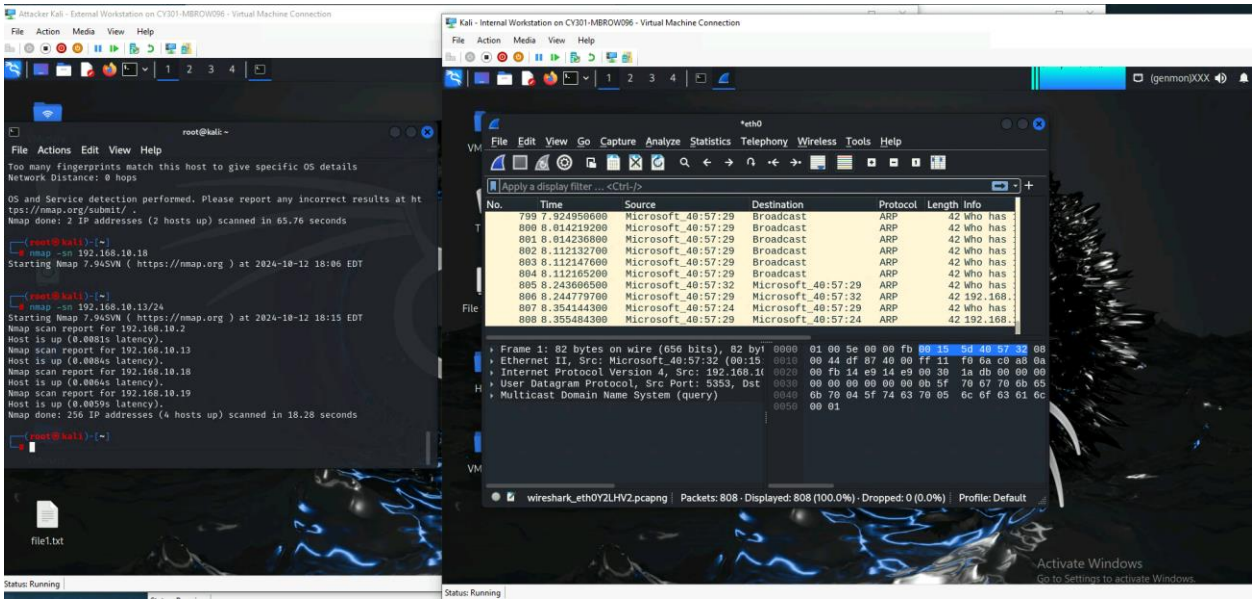
Power on the listed VMs and complete the following steps from the **External Kali** (you can use either nmap or zenmap to complete the assignment)

- External Kali
- pfSense
- Ubuntu
- Windows Server 2022

**Make sure you didn't add/delete any firewall policy before continuing.**

1. Use Nmap to profile the basic information about the **subnet** topology (including open ports information, operation systems, etc.) You need to get the **service** and **backend software** information associated with each opening port in each VM.






**2.** Run Wireshark in Internal Kali VM while External Kali is scanning the network. Discuss the traffic pattern you observed. What do you find? **Please write a 200-word essay to discuss your findings.**

To begin gathering information about the network, I used Nmap from the External Kali machine to scan the subnet and identify any live devices. I first scanned the subnet 192.168.217.3/24 and found two active hosts, including the pfSense virtual machine at 192.168.217.2. This helped me confirm that pfSense was operating on the network. I then ran another scan on a different subnet, 192.168.10.13/24, which revealed additional hosts, including IP addresses like 192.168.10.2, .13, .18, and .19. These are likely the other virtual machines in the network, such as the Ubuntu and Windows Server 2022 systems.

While the External Kali machine was scanning, I used Wireshark on the Internal Kali machine to observe the network traffic. During the scan, Wireshark captured traffic related to the devices trying to communicate with each other, specifically using ARP (Address Resolution Protocol). This traffic showed that devices were asking for each other's physical (MAC) addresses so they could communicate. There were also some DNS queries related to local network service discovery. Overall, the pattern of traffic showed devices learning each other's presence on the network as I conducted the scan.

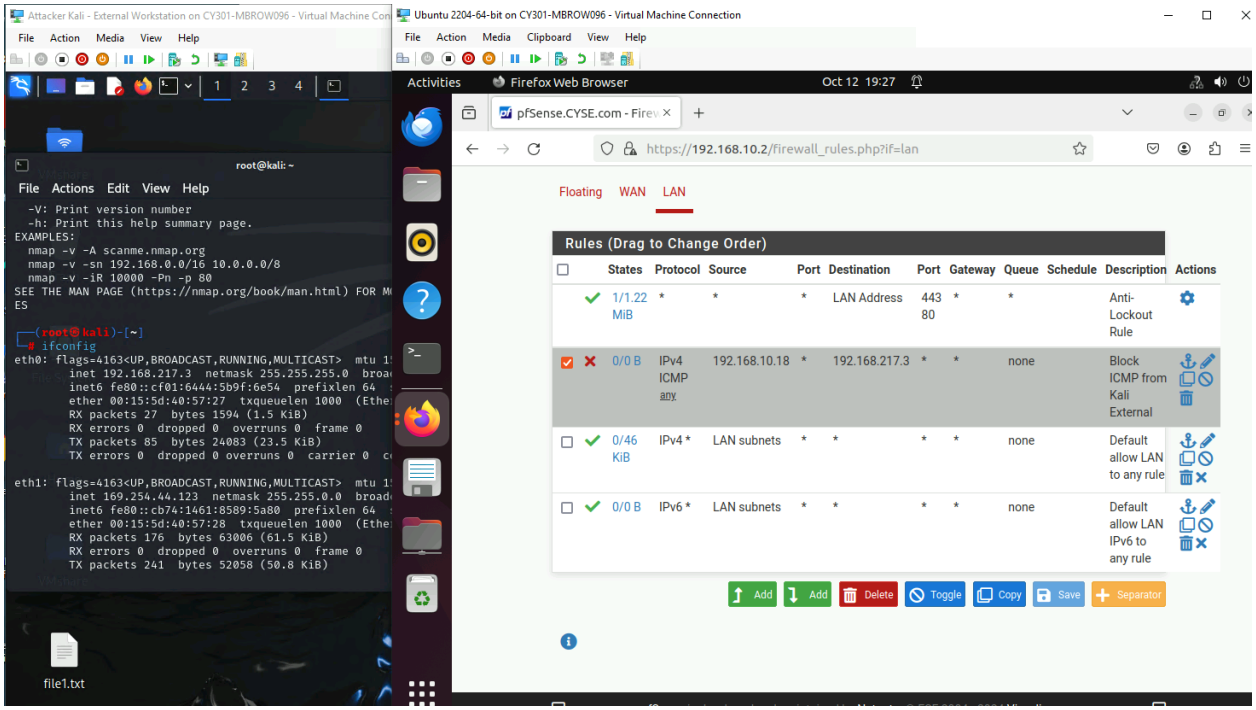
**Task B: Shield – Protect your network with a firewall (10 + 10+ 20 + 20 = 60 points)**

**In order to receive full credits, you need to fill the table (add more rows if needed), implement the firewall rule(s), show me the screenshot of your firewall table, and verify the results.**

1. Configure the pfSense firewall rule to block the ICMP traffic from External Kali to Ubuntu VM.

| Rule # | Interface | Action | Source IP | Destination IP | Protocol (port # if appliable) |
|---|---|---|---|---|---|
| 2 | LAN | Block | 192.168.10.18 | 192.168.217.3 | IPv4 \| ICMP:any |

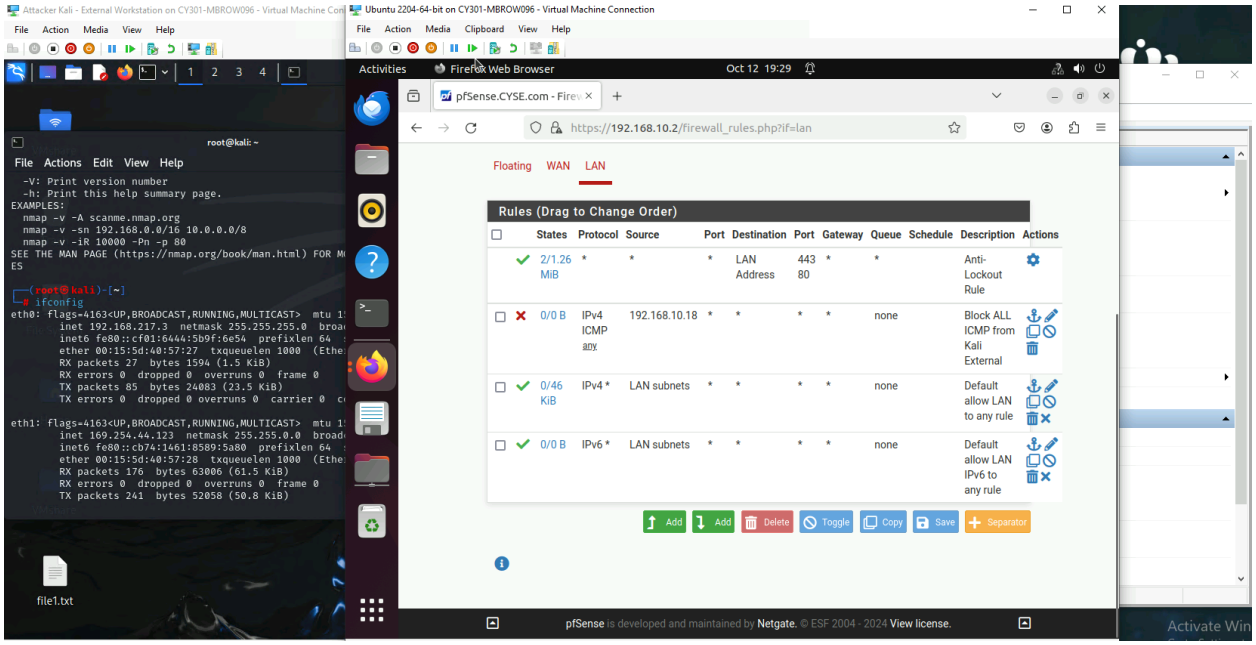
*[Add the screenshot here]*




2. Clear the previous firewall policies and configure the pfSense firewall to block all ICMP traffic from External Kali to the LAN side.

| Rule # | Interface | Action | Source IP | Destination IP | Protocol (port # if appliable) |
|---|---|---|---|---|---|
| 2 | LAN | Block | 192.168.10.18 | LAN network | IPv4 \| ICMP:any |

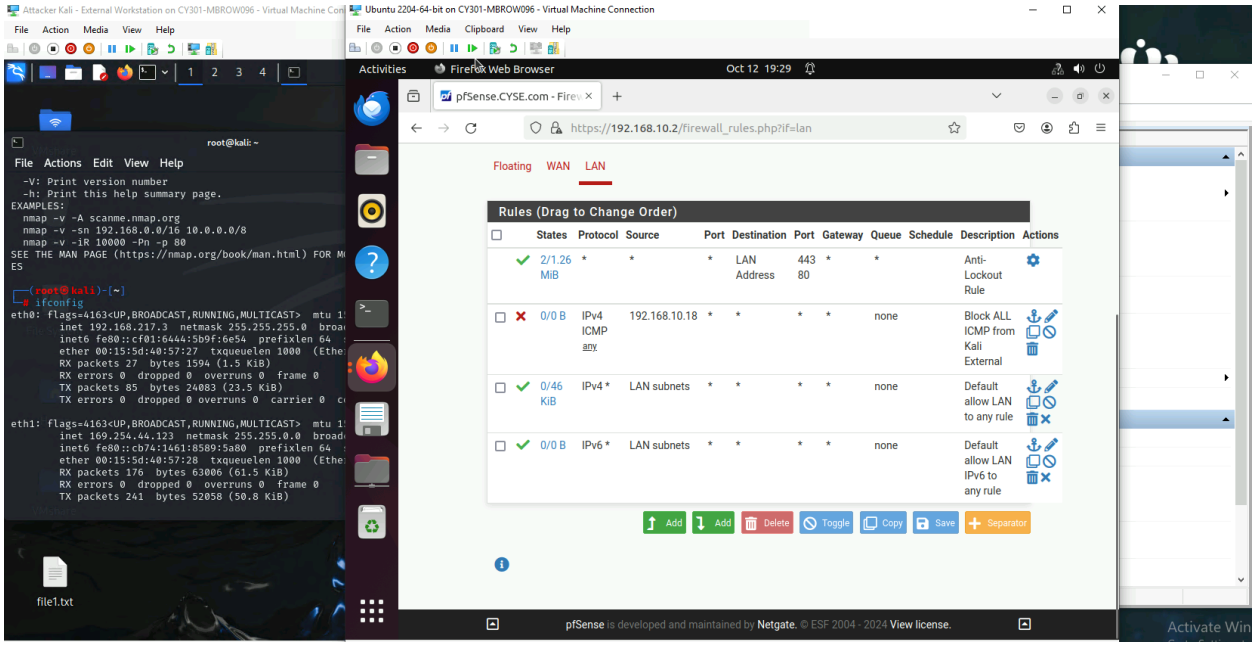
*[Add the screenshot here]*




3. Clear the previous firewall policies and configure the pfSense firewall to block ALL traffic from External Kali to the LAN side, except for the FTP protocol towards Ubuntu.

| Rule # | Interface | Action | Source IP | Destination IP | Protocol (port # if appliable) |
|---|---|---|---|---|---|
| 2 | LAN | Block | 192.168.10.18 | LAN network | IPv4 \| ALL TRAFFIC |

*[Add the screenshot here]*



4. Keep the firewall policies you created in Task B.3 and repeat Task A.1. What's the difference?

**Extra credit (15 points): Use NESSUS to enumerate the security vulnerabilities of Microsoft Windows Server 2022 VM in the CCIA network.**