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 (5 + 15+ 20 = 40 points)

Power on the listed VMs,

- External Kali
- pfSense
- Ubuntu
- Windows Server 2022

Make sure not to add/delete any firewall rule/policies before continuing.

1. Run Wireshark in the Internal Kali VM while External Kali is scanning the network.
2. Use **Nmap in External Kali** to profile the basic information about the **subnet** topology (including open ports information, operating systems, etc.)

   [Add the screenshot here]

   You need to submit a table summarizing the following (please add more rows if required):

IP address Of the VMs	Open ports	Service versions	Operating System detection	Backend software information

3. Please write a **200-word** critical evaluation.

Task B: Shield – Protect your network with a firewall (10 + 15+ 15 + 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), attach the screenshot of your rule configured in the firewall table, and attach the screenshot of the rule and the Ping test verification of the rules.

Important: Open Pfsense using a browser on the Internal Kali.

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

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if applicable)

[Add the screenshot here]

[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)

[Add the screenshot for Firewall Rules and Ping test here]

[Add the screenshot here]

Add your Reflection (~150 words):

- What security advantages does blocking ICMP provide?
- What operational disadvantages might occur?

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 directed towards Ubuntu. You can add more rows in the table here, if necessary.

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if applicable)

[Add the screenshot here]

[Add the screenshot here]

4. Keep the firewall policies you created in Task B.3 and repeat Task A.1 to rescan the subnet using nmap in External Kali.

Now, compare the results/ findings, and complete the following table and add your reflection as asked here:

Before Firewall Rules	**After Firewall Rule**
Open Ports	Eg. Filtered/Blocked
OS Detection Accuracy	
Service Enumeration	

Write in your own words (~ 200 words) explaining:

a. Why does Nmap show "filtered" instead of "closed", if there is any.
b. How firewall behavior affects scan results
c. What information is hidden from attackers

Extra credit (15 points): Use NESSUS to enumerate the security vulnerabilities of the Microsoft Windows Server 2022 VM in the CCIA network and submit the following in a PDF file:

- Prioritize vulnerabilities
- Recommend remediation strategy
- Identify the highest real-world risk
- CVSS scores
- Your own judgment