CYSE 301: Cybersecurity Technique and Operations

Assignment 3: Sword vs. Shield

1. Emmanuel Dade :01249296

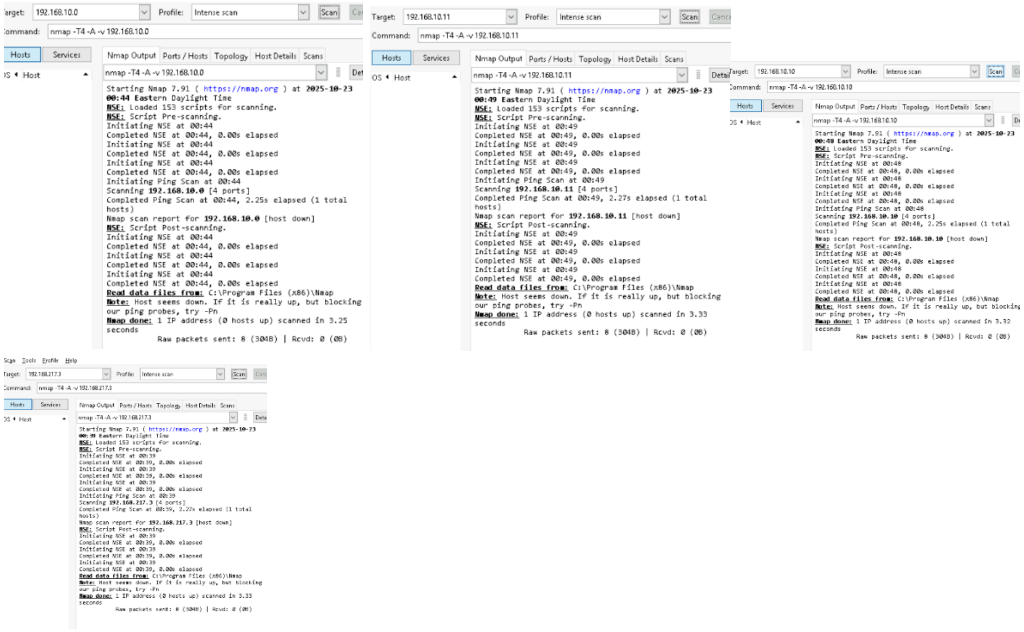
In this assignment, you will act as an attacker to identify the vulnerabilities in the LAN network and a defender to apply proper countermeasures. **You need to provide a screenshot for each task below.**

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

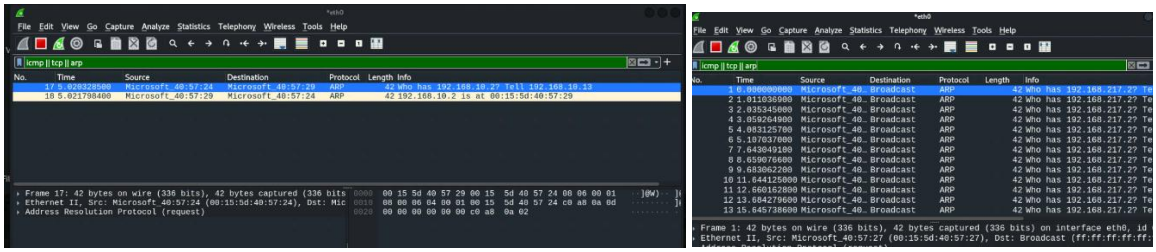
Power on the listed VMs and complete the following steps from the **External Kali** (you can use either nmap or zenmap to complete the assignment)

- 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.**

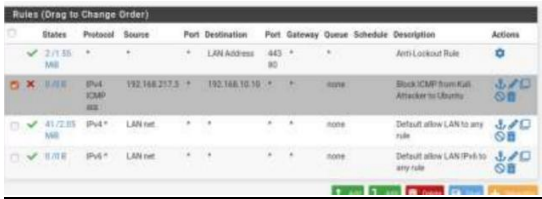


When I took Wireshark on the Internal Kali VM while the External Kali was scanning, I noticed some patterns that honestly intrigued me—even shocked me—how much was sent over the network. For instance, obviously, I recognized a huge amount of TCP SYN packets that flooded the network. They were sent to almost every port available to the target machines and unsurprisingly so as this is the first stage nmap uses to determine what ports are open.
Moreover, I noted the response patterns sent back to the scanner. For every open port, there was a SYN-ACK packet received back which indicated that those services were up and listening. On the other hand, for every closed port, I received an RST (reset) packet which told the scanner "no go, nothing here." There were many filtered ports as well, that as I hypothesized, the firewall dropped many packets and did not respond.
I didn't expect so many packets to be sent from the simple scan. I expected maybe 100 packets or so but within a few minutes over 1500 packets were sent—multiple thousands. Furthermore, at the very beginning of the scanning process, there was a simple ping—it was an ICMP process of nmap checking what hosts were alive on the subnet. Thus, from the moment nmap began its scanning through sending various packets to assessing the responses it seemed like an interactive communication process. It opened up my eyes to see how information is shared about port availability as well as services and firewall considerations.

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

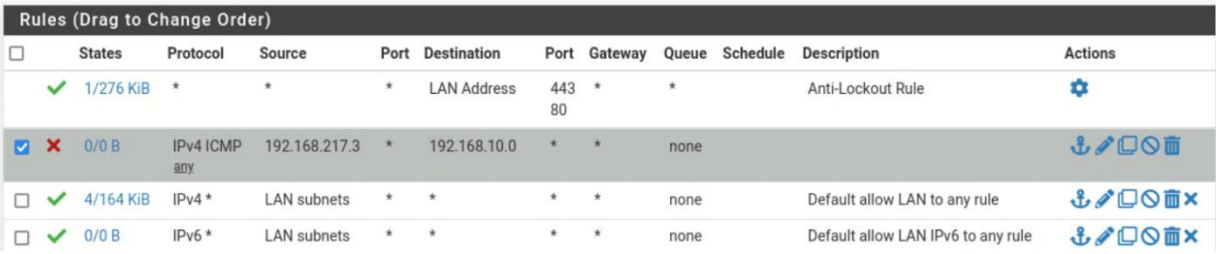
In order to receive full credits, you need to fill the table (add more rows if needed), implement the firewall rule(s), show me the screenshot of your firewall table, and verify the results.

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)
1	Lan	Block	192.168.217.3	192.168.10.10	IMCP

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	Vlock	192.168.217.3	192.168.10.0	Icmp

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)
1	lan	Allow	192.168.217.3	Lan	Any

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

   The difference is files stopped transferring .After implementing the firewall rules from Task B.3, the second scan showed dramatically different results. The most noticeable change was that many ports that previously showed as "open" were now appearing as "filtered" or weren't responding at all.

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