CYSE 301: Cybersecurity Technique and Operations

Assignment 3: Sword vs. Shield

Harold B. Vernon IV

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 (192.168.10.19)

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.**

While running the scan from Internal Kali, it was easy to pick up on select repetitive patterns. The results of the Wireshark scan showed that all the three-way handshakes were completed between Internal Kali and the other systems. External Kali also completed its three-way handshakes. While this may seem inconsistent with the results gathered from nmap, this in truth is perfectly consistent with the results of the nmap scan, where the ports of Ubuntu, Windows, and pfSense were all in ignored states. This divergence can be explained by the possibility of how the pfSense firewall treats the two machines differently.

No nmap scan was run from Internal Kali as such a procedure was not instructed, however it is likely that a scan would result in connections being made to Ubuntu, Windows, and pfSense's ports. The filtering methods appeared to be largely silent going off the information gathered in the Wireshark scan. The hypotheses crafted in analyzing the Wireshark scan's results were confirmed by observing the firewall's rules. Silent filtering was used instead of RSTs. Likewise the External Kali machine was actively blocked from connecting with the rest of the network. In sum, the scan showed effective application of the pfSense firewall.

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	WAN	Block	192.168.217.3	192.168.10.18	ICMP

Unable to do with student perms. Above is what the policies should be.

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

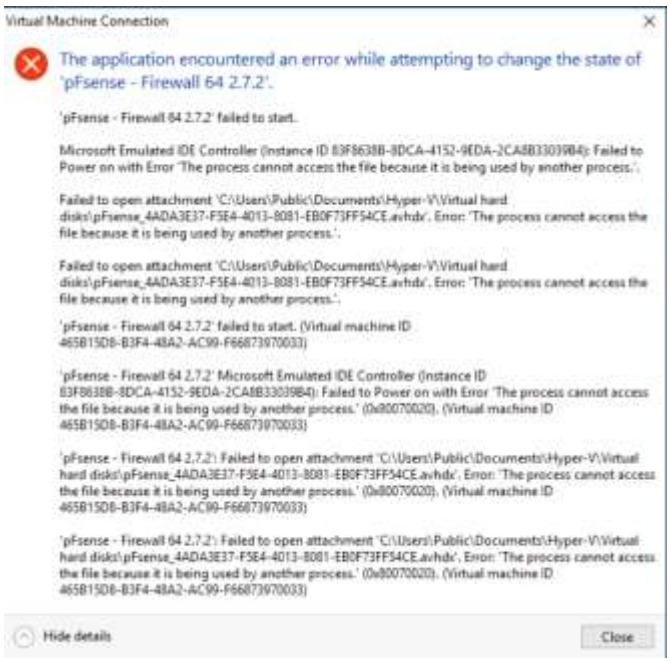
Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
1	LAN	Block	192.168.217.3	LAN net	ICMP

Unable to do with student perms. Above is what the policies should be.

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	Any	Pass	192.168.217.3	192.168.10.18	21
2	LAN	Block	192.168.217.3	LAN net	Any

Unable to do with student perms. Above is what the policies should be.



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

   The policies should prevent External Kali from connecting at all to the Ubuntu machine. Thus demonstrating the importance of firewalls in cybersecurity as they can prevent unwanted traffic such as threat actors monitoring a network without authorization.

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