CYSE 301: Cybersecurity Technique and Operations

Assignment 3: Sword vs. Shield

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

The screenshot above shows the nmap for External Kali. The open port is 111 and its running service is rpcbind version 2-4 (RPC # 100000) and its operating system is Linux 3.7 - 3.10.

The screenshot above shows the nmap for Pfsense. It has three open ports. Port 53 is open with its service as tcpwrapped. Port 80 is open and provides HTTP service with the version of nginx. Port 443 is open and provides the HTTPS service with the version of nginx. Nmap was not able to find an OS for this host.

The screenshot above shows the nmap for Ubuntu. It has one open port in the form of port 21 for the service of FTP with the version vsftpd 3.0.3. Its operating system is linux.

The screenshot above shows the nmap for the Windows 2008 server. It has six open ports. Port 21 provides the service of FTP and its version is Microsoft ftpd. Port 80 provides TCP and its version is Microsoft IIS httpd 7.5. Port 135 provides the service of msrpc and its version is Microsoft Windows RPC. Port 445 provides the service of microsoft directory services and its version is Windows Server 2008 R2 Standard 7600 microsoft -ds. Port 3389 provides the service of tcpwrapped and there is no current version listed. Port 49154 provides the service of msrpc and its version is Microsoft Windows RPC. The operating system is Windows.

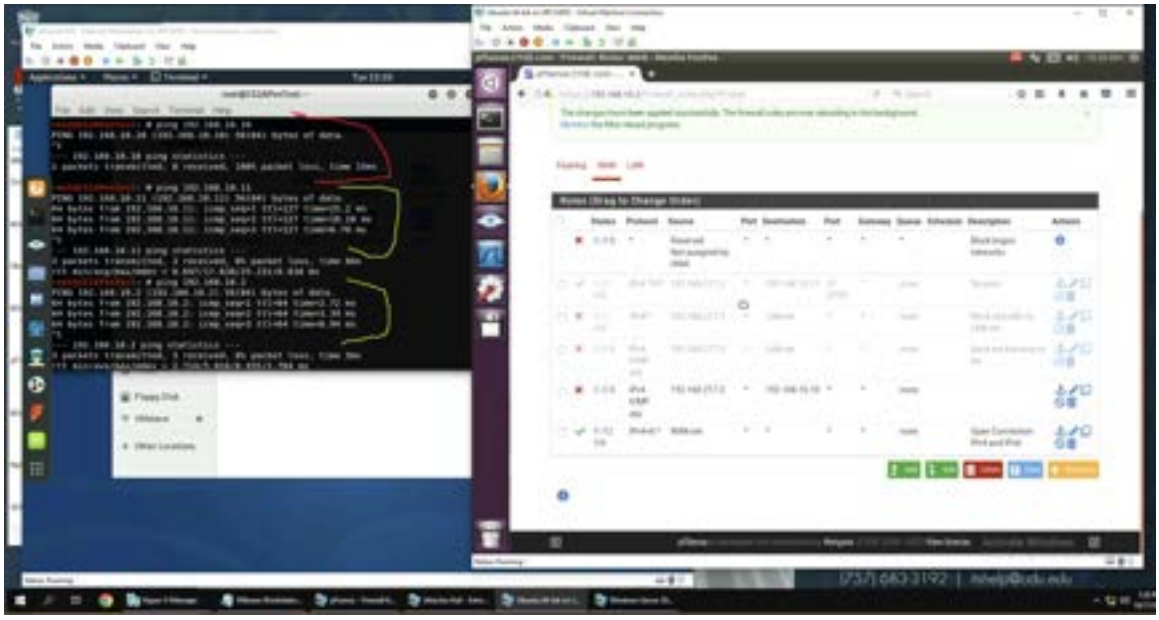
- Run Wireshark in Ubuntu VM while External Kali is scanning the network. Discuss the traffic pattern you observed. What do you find? **Please write a 200-word essay to discuss your findings.**

Task B: Shield – Protect your network with 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.

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

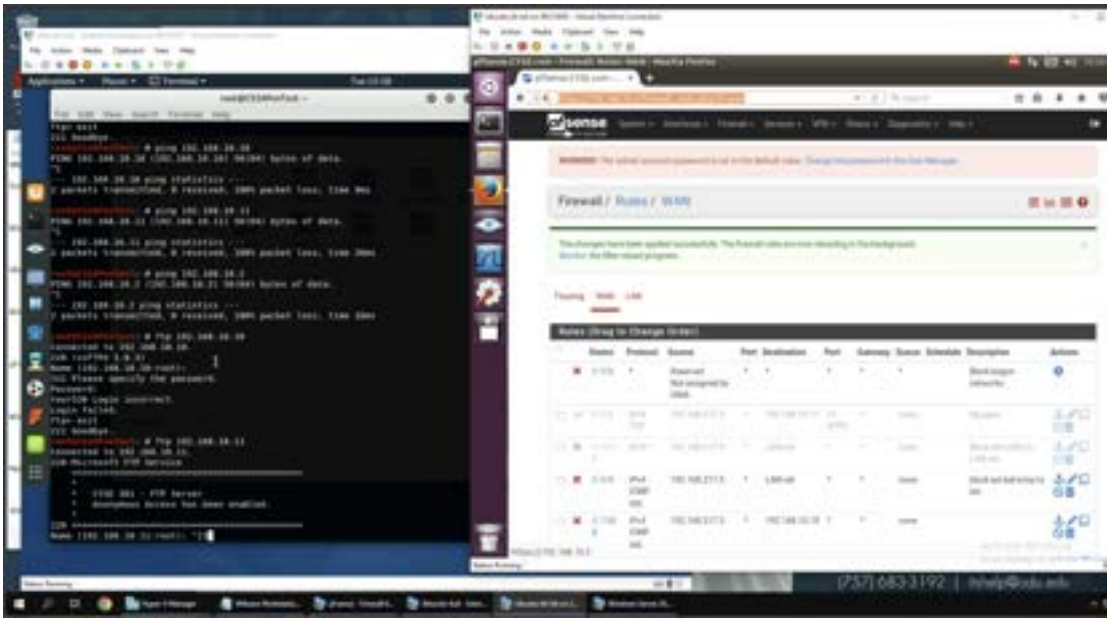
Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
1	Wan	Block	192.168.217.3	192.168.10.10	ICMP



In this firewall rule, I cannot ping Ubuntu, but I can ping anything else on the network.

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

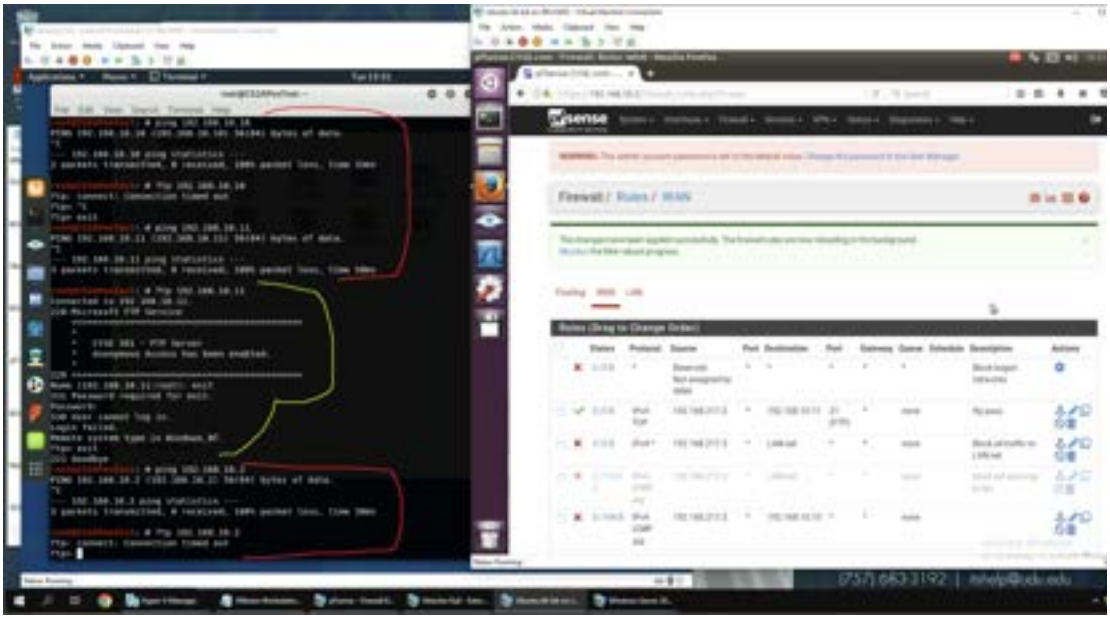
Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
1	WAN	Block	192.168.217.3	LAN net	ICMP

- 

In this firewall rule, I cannot ping anything on the LAN side, but I can use FTP on anything I want because the rule only blocks ICMP traffic.

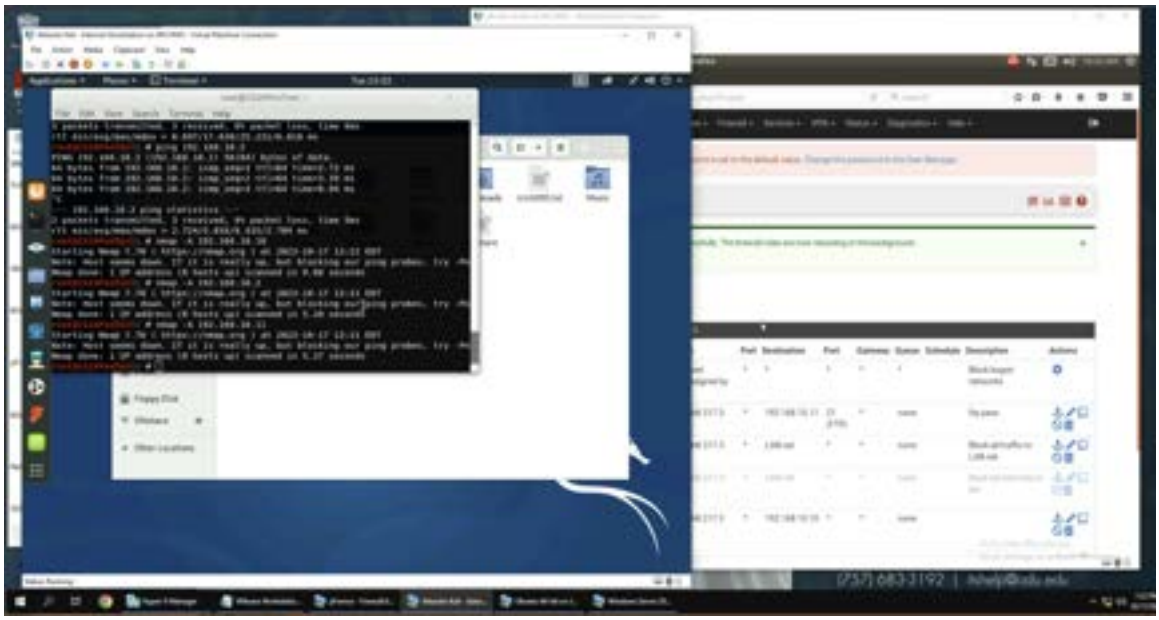
- Clear the previous firewall policies and configure the pfSense firewall to block ALL traffic from External Kali to the LAN side, except for the FTP protocol towards Windows Server 2008.

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
1	WAN	Pass	192.168.217.3	192.168.10.11	TCP (21) (FTP)
2	WAN	Block	192.168.217.3	LAN net	IPv4

- 

In this firewall rule, I cannot use ping on anything within the LAN network. FTP only works on the Windows server, and nothing else within the LAN network.

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



The difference between the first time I used nmap and the second time is that nmap will not be able to reach anything on the LAN network, leaving its details unknown to us.

Extra credit (15 points): Use NESSUS to enumerate the security vulnerabilities of Microsoft Windows Server 2008 VM in the CCIA network.