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 2008

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.
   After running nmap -O -sV 192.168.10.0/24, I found three Ips, 192.168.10.10, 192.168.10.11, and 192.168.10.2. The ports open on 192.168.10.10 is port 21/tcp for service ftp. The os that is running is linux, the service infor is Unix. 192.168.10.2 shows 53/tcp for the dns service, 80/tcp for http, and 443/tcp for https. There is no os match for this machine. On 192.168.10.11, 21/tcp for ftp, 80/tcp for http, 135/tcp for msrpc, 445/tcp for Microsoft-ds, 3389/tcp for tcpwrapped and 49154/tcp for msrpc are open. The OS is listed as Windows server 2008 R2.

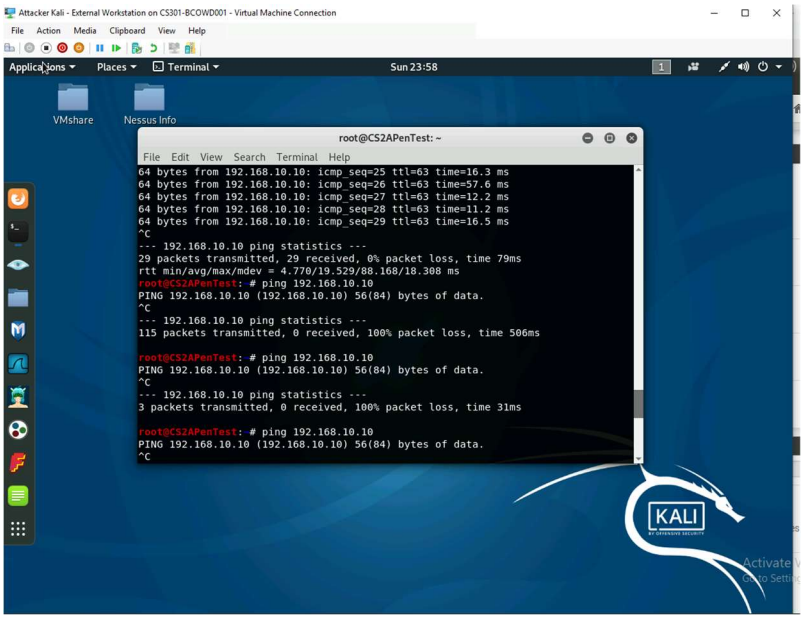
2. Run Wireshark in Ubuntu VM while External Kali is scanning the network. Discuss the traffic pattern you observed. What do you find? **Please write a 200-word essay to discuss your findings.**
   After scanning the network with nmap on the external kali machine, there were multiple TCP traffic patterns that were picked up that were all highlighted in red. These tcp connections were from 192.168.217.3. I can see that within a matter of seconds there are multiple of these packets between Ubuntu and the external kali machine. This traffic shows me that this machine is sending a packet to the Ubuntu machine and the workstation is receiving an acknowledgement as well which is giving the Kali machine the information it requires to attack. Also opening up one of the packets, it is shown that there is a reset highlighted in each one that is sent to the Ubuntu.

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.

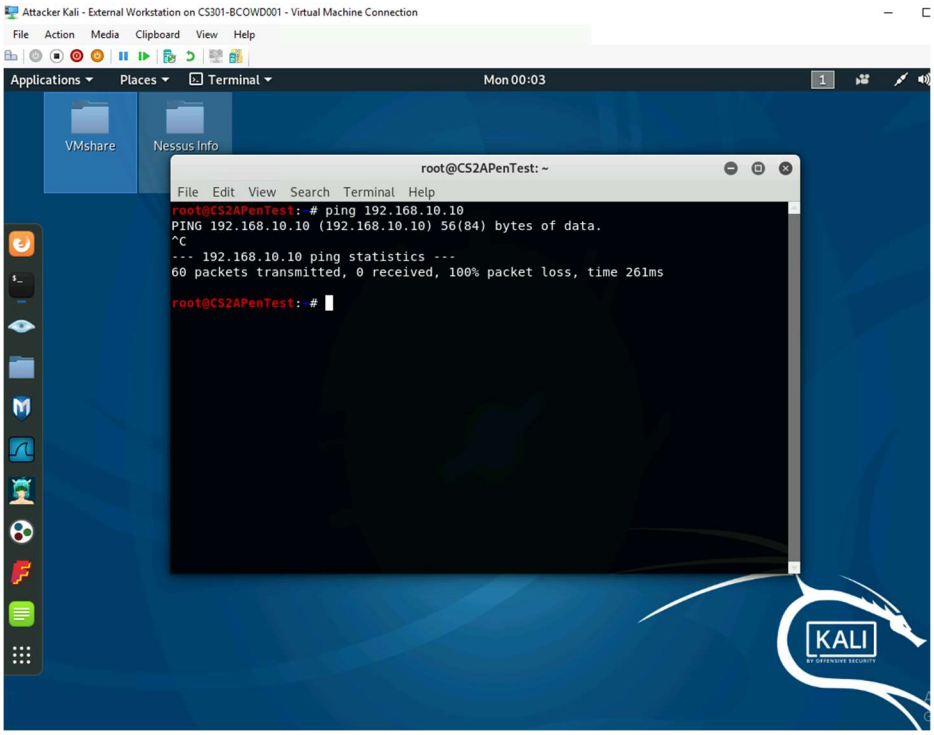
1. Configure the pfSense firewall rule to block the ICMP traffic from External Kali to Ubuntu VM.

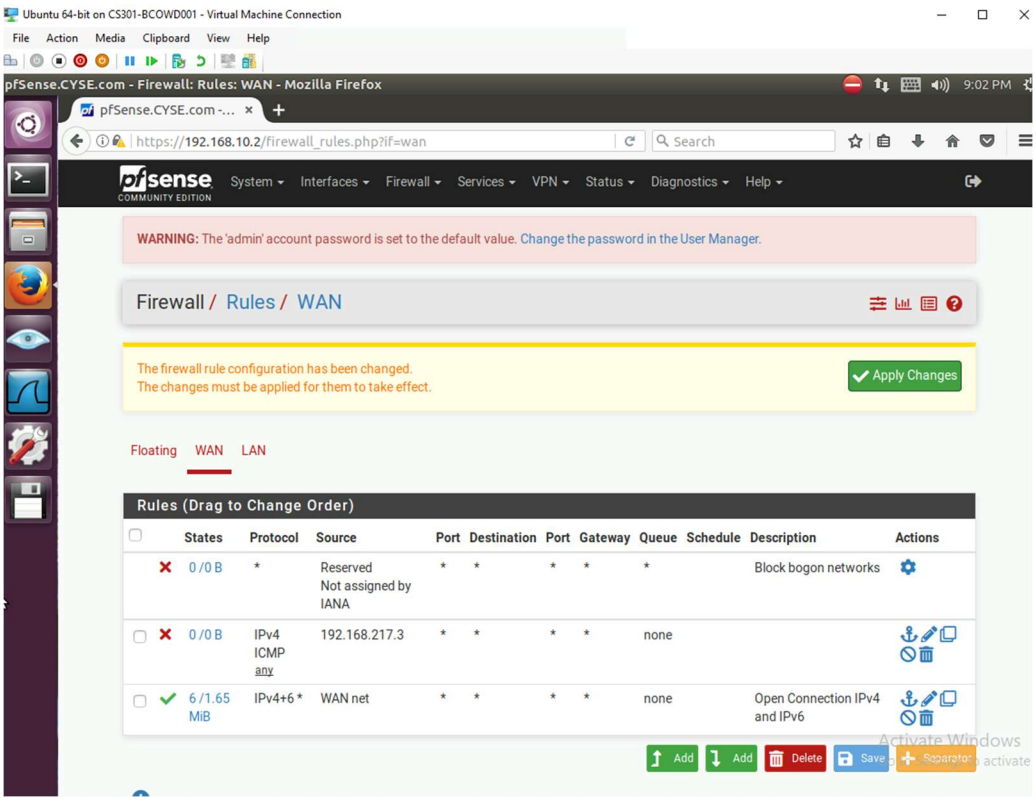
Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
1	WAN	Block	192.168.217.3	192.168.10.10	ICMP



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

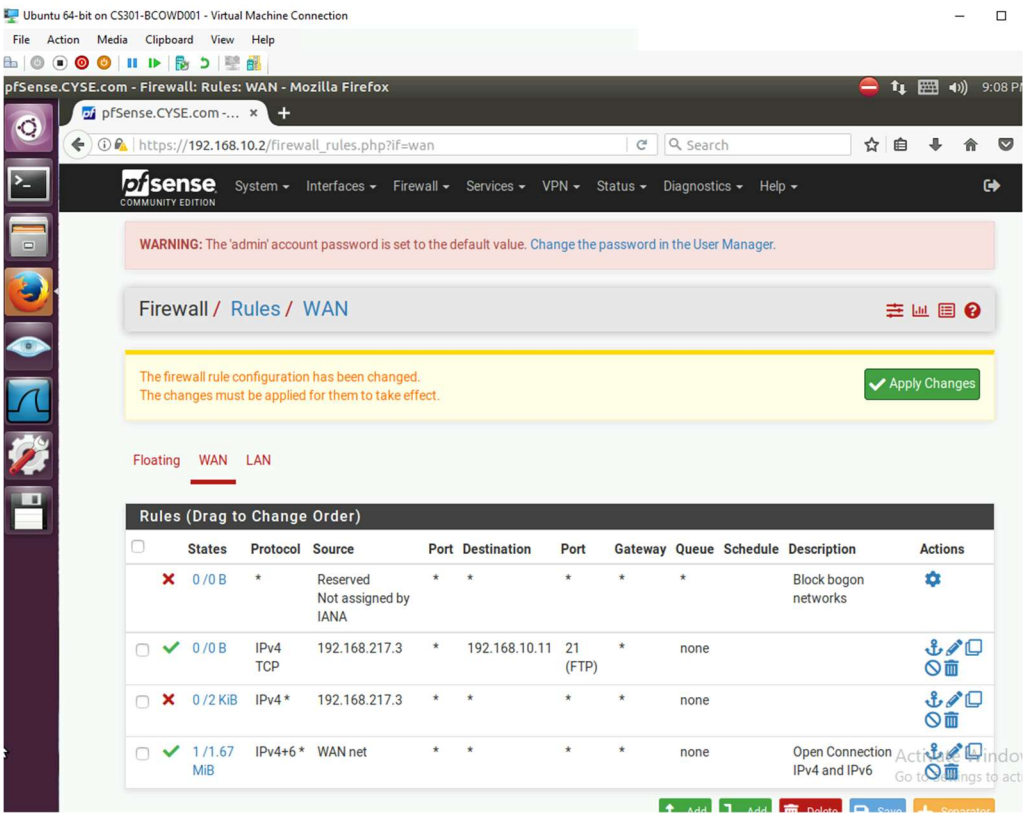
Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
1	WAN	Block	192.168.217.3	ANY	ICMP





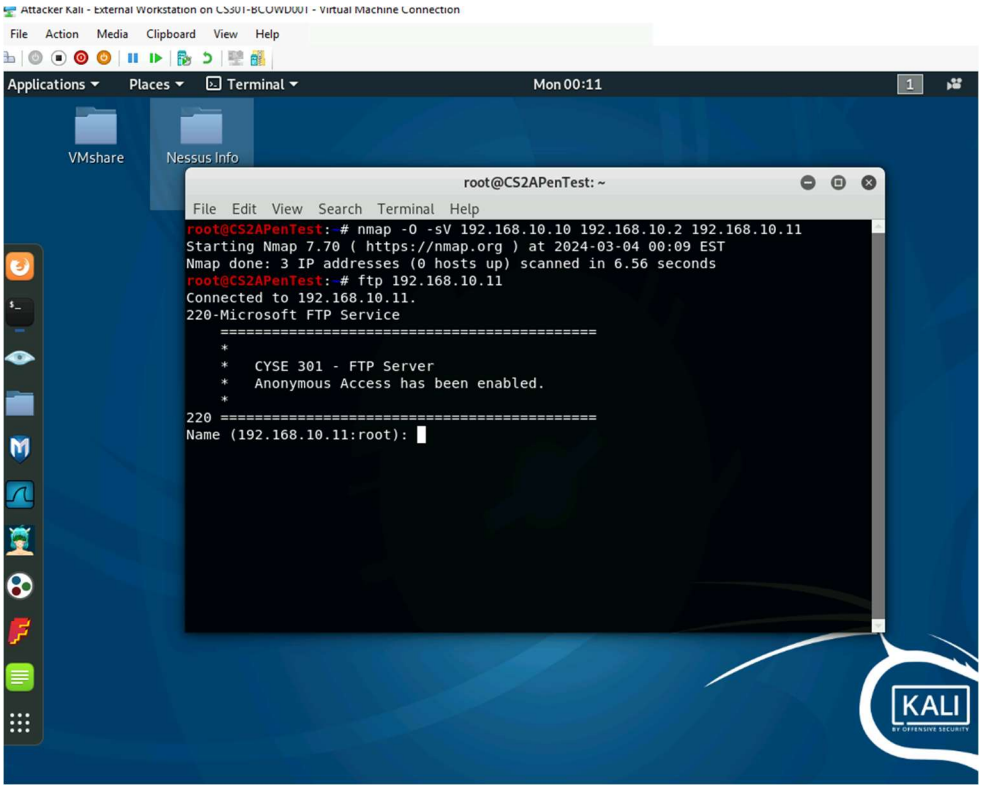
3. Clear the previous firewall policies and configure the pfSense firewall to block ALL traffic from External Kali to the LAN side, except for the FTP protocol towards Windows Server 2008.

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
1	WAN	Pass	192.168.217.3	192.168.10.11	FTP (Port 21)
2	WAN	Block	192.168.217.3	ANY	ANY



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

With these changes that were made, I can no longer see all of the information gathered in Task A. I cannot see the ips, os, open ports, or services. After moving the pass rule above the blocking rule I can however, ftp into 192.168.10.11.


Attacker Kali - External Workstation on CS301-BCOWD001 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Mon 00:11
VMshare
Nessus Info
root@CS2APenTest: ~
File Edit View Search Terminal Help
root@CS2APenTest:~# nmap -O -sV 192.168.10.10 192.168.10.2 192.168.10.11
Starting Nmap 7.70 (https://nmap.org) at 2024-03-04 00:09 EST
Nmap done: 3 IP addresses (0 hosts up) scanned in 6.56 seconds
root@CS2APenTest:~# ftp 192.168.10.11
Connected to 192.168.10.11.
220-Microsoft FTP Service
* CYSE 301 - FTP Server
* Anonymous Access has been enabled.
220
Name (192.168.10.11:root):
KALI