Old Dominon University

CYSE 301: Cybersecurity Technique and Operations

Assignment 3: Sword vs. Shield

Vwhskhq#Jlruj#

34565887

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.

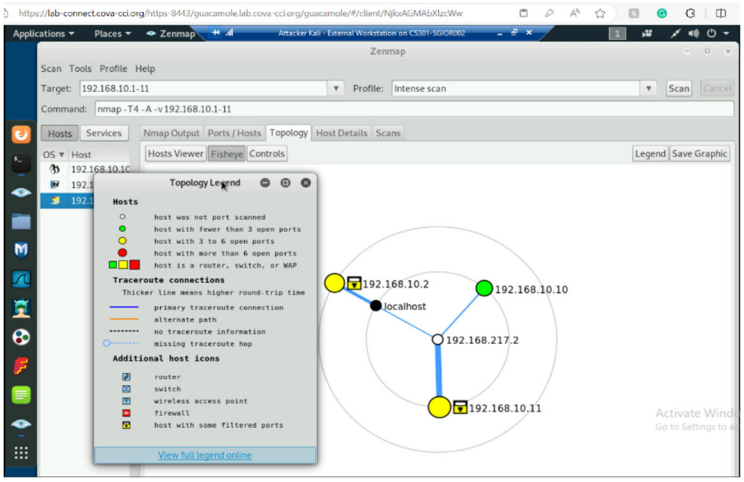
Task A: Sword - Network Scanning (20+ 20 = 40 points)

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)

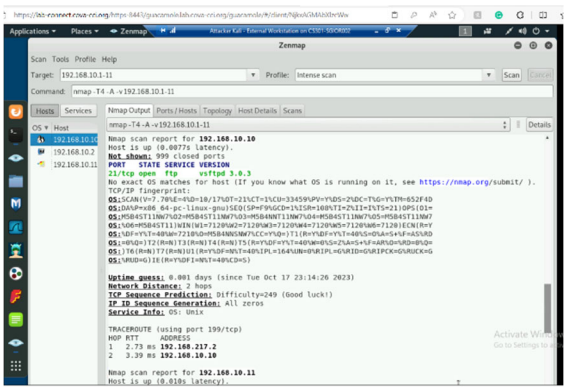
- External Kali
- pfSense
- Ubuntu
- Windows Server 2008

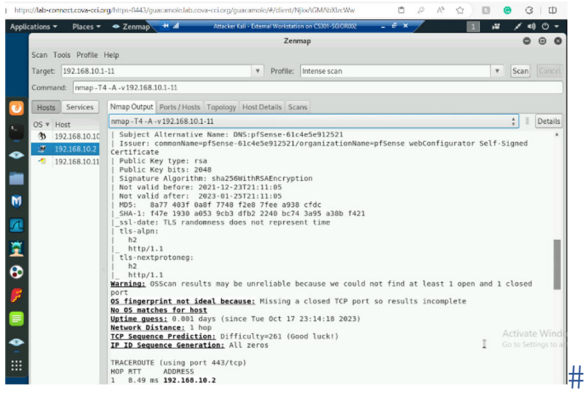
Make sure you didn't add/delete any firewall policy before continuing.

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.

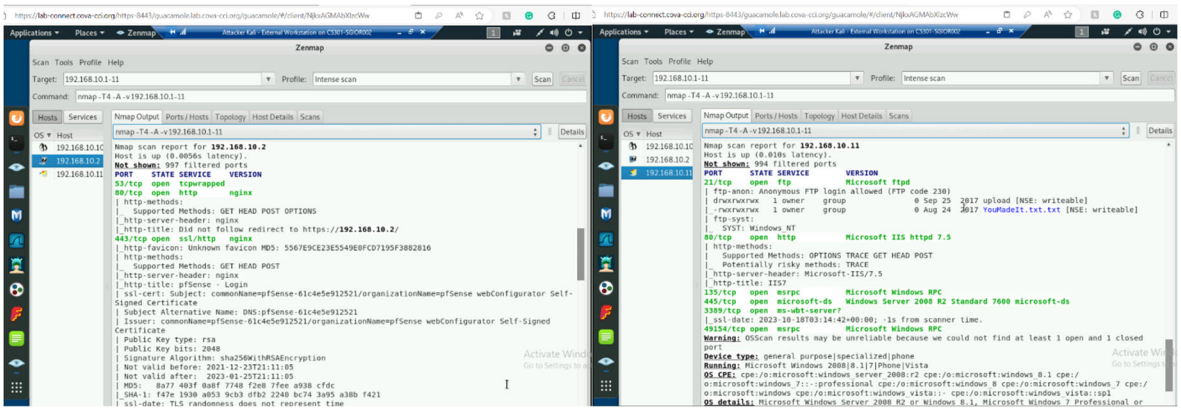


From the screenshot above you can see a visualization and summary of my Zenmap scan. From this you can see the amount of open ports for each VM with the ubuntu VM (.10.10) with the least amount of open ports and windows(.10.11) and pFsense(.10.2) with between 3 and 6 open ports. Take note that (.10.11) has the highest roundtrip time.





#



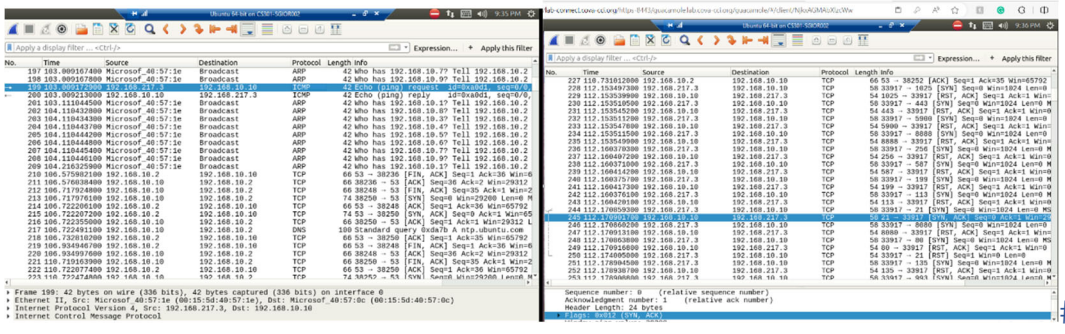
From the above screenshots which are the result of the "nmap -T4 -A -v 192.168.10.1-11" we can see more detailed findings. We can see the OS of each VM minus pFsense. We can see the open ports highlighted in green as well as their service and version and even any associated files and if they are writeable. We can see that the windows server has the most amount of open ports.

#

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.**

From when I performed my Nmap/Zenmap scan, there were many things that I could find about the subnet topology to include the OS of each VM, open ports for each VM, associated files for each port that may or may not be writable, and the software that is using each port. This could show me what systems in a topology are the most vunerable in the case that I was a threat actor, in this case I can see that the windows server is the most vunerable with the most amount of open ports.

We can get a better understanding of how Nmap is able to accomplish this with the use of Wireshark on the Ubuntu server. From the first of two screenshots below you can see that initially the scan starts with a ping between the two VMs, the only two packets that use ICMP protocol. Surrounding that is packets between the Ubuntu server and the pFsense firewall as well as multiple broadcast packets asking for difference IP's. The broadcast being the result of the Nmap scan command trying to find multiple hosts that are down. The second screenshot shows and map actively scanning the VMs by sinking with every individual avialabe port (1000 ports per VM) when it finds an open port it flags it SYN and AKC (like the highlighted packet) and then reports it to the user.



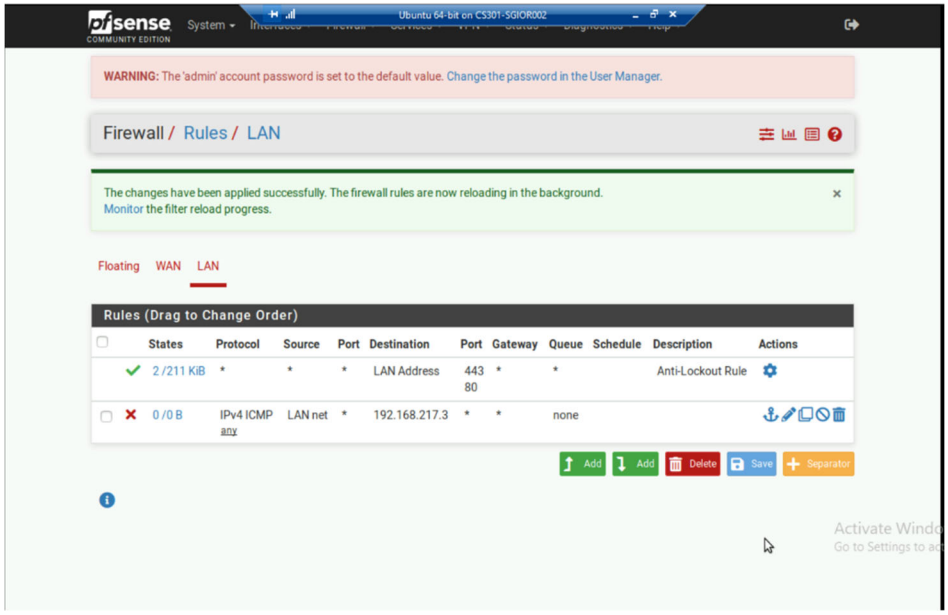
#

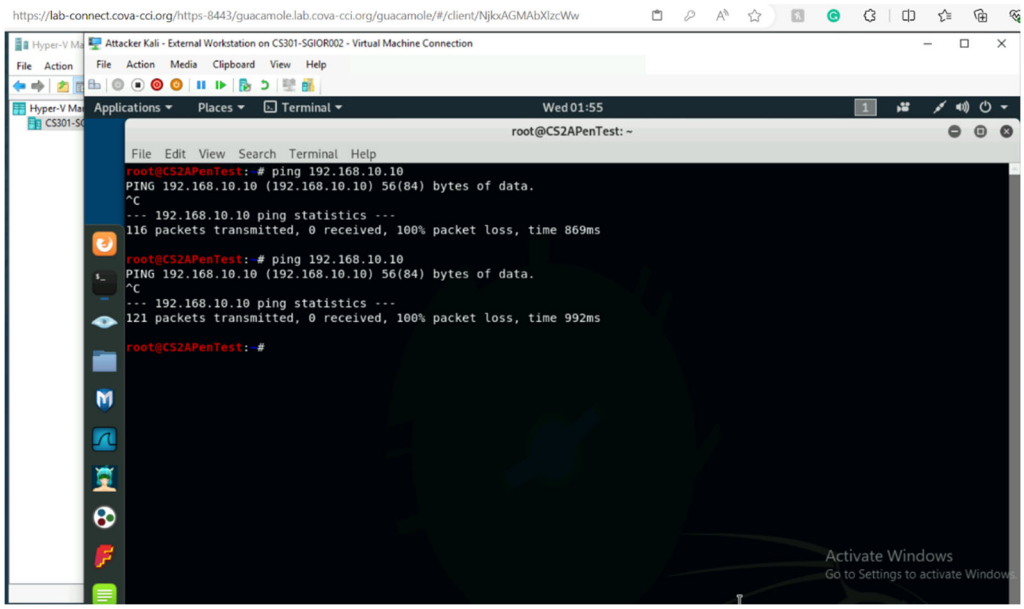
Task B: Shield – Protect your network with firewall (10 + 10+ 20 + 20 = 60 points)

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.

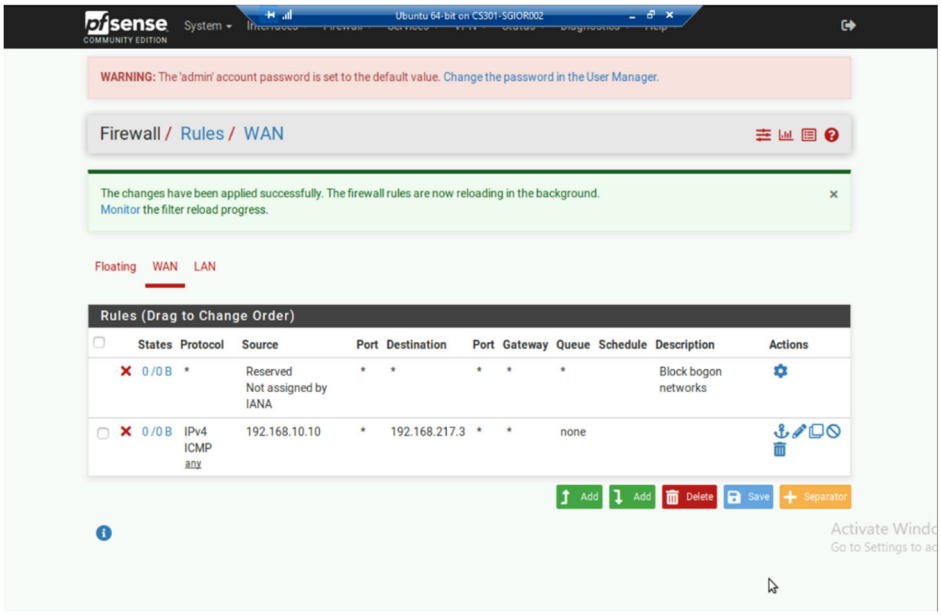
Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
2	WAN	Block	192.168.10.10	192.168.217.3	IPv4 ICMP(any)

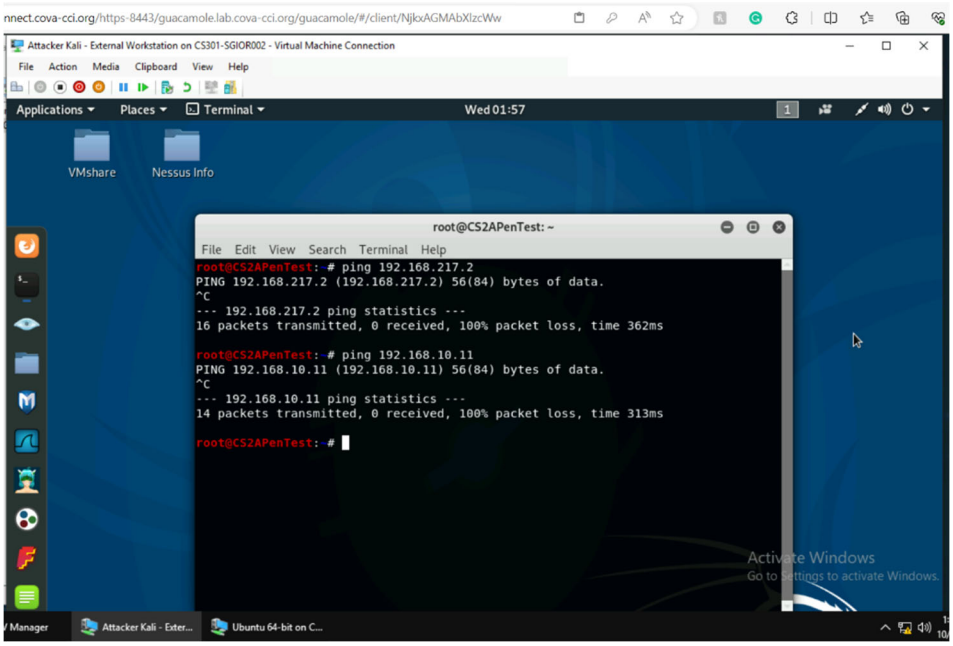




2. Clear the previous firewall policies and configure the pfSense firewall to block all ICMP traffic from External Kali to the LAN side.

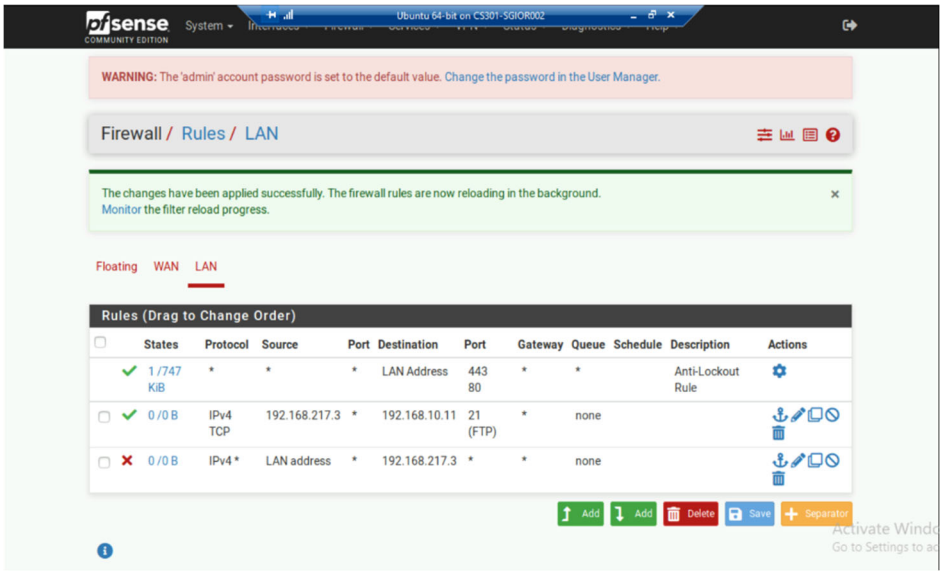
Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
2	LAN	Block	LAN address	192.168.217.3	IPV4 ICMP(any)

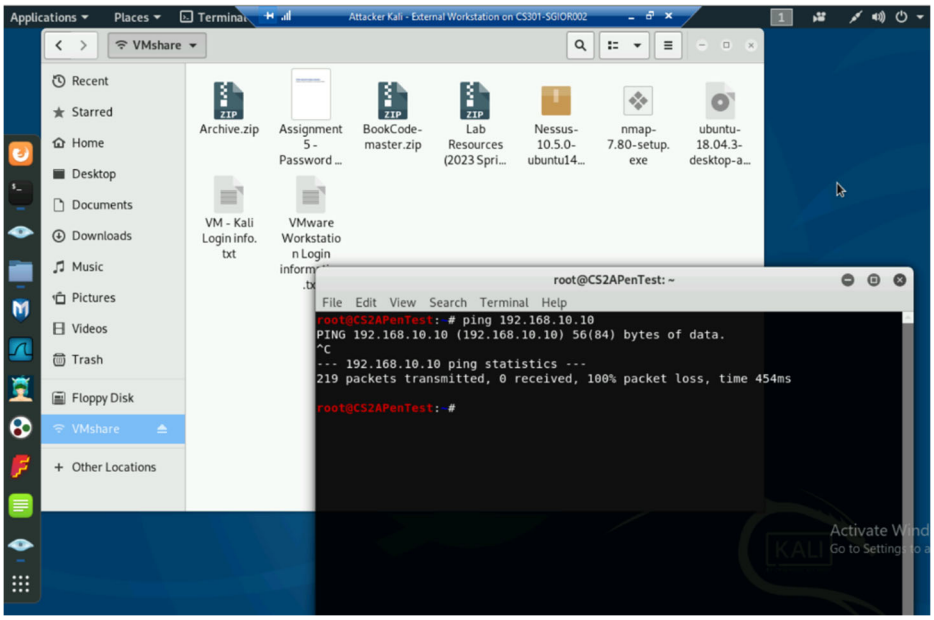




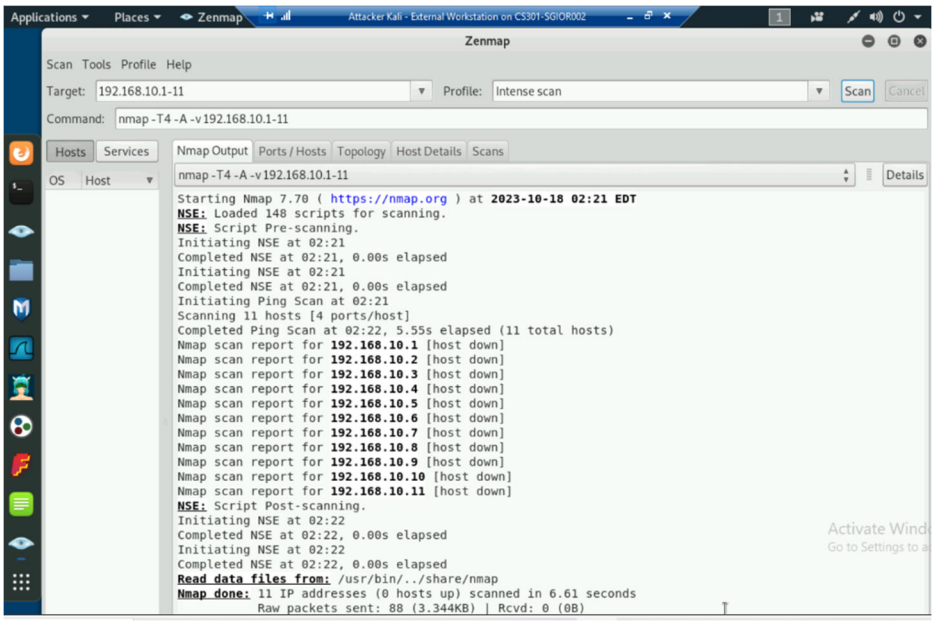
3. Clear the previous firewall policies and configure the pfSense firewall to block ALL traffic from External Kali to the LAN side, except for the FTP protocol towards Windows Server 2008.

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
2	LAN	pass	192.168.217.3	192.168.10.11	IPv4 TCP port 21
3	LAN	Block	LAN address	192.168.213.3	IPv4 any





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



The Nmap reads all the hosts as if they are down, but can still access VMshare.

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