Old Dominion University

CYSE 301 Cybersecurity Techniques and Operations

Assignment #3 – Sword Vs. Shield

Ned Smith

01200384

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.

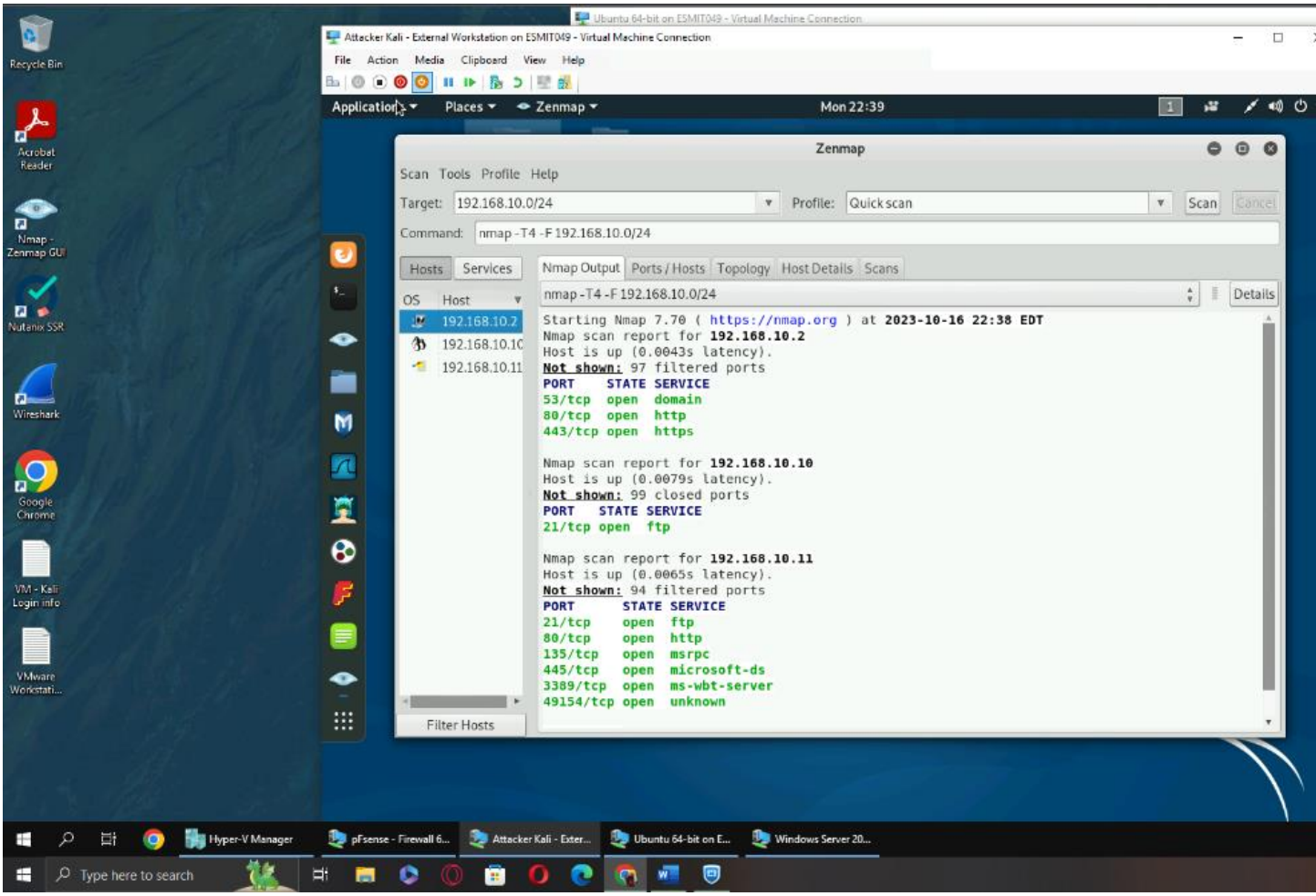
Task A: Sword - Network Scanning (20+ 20 = 40 points)

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.

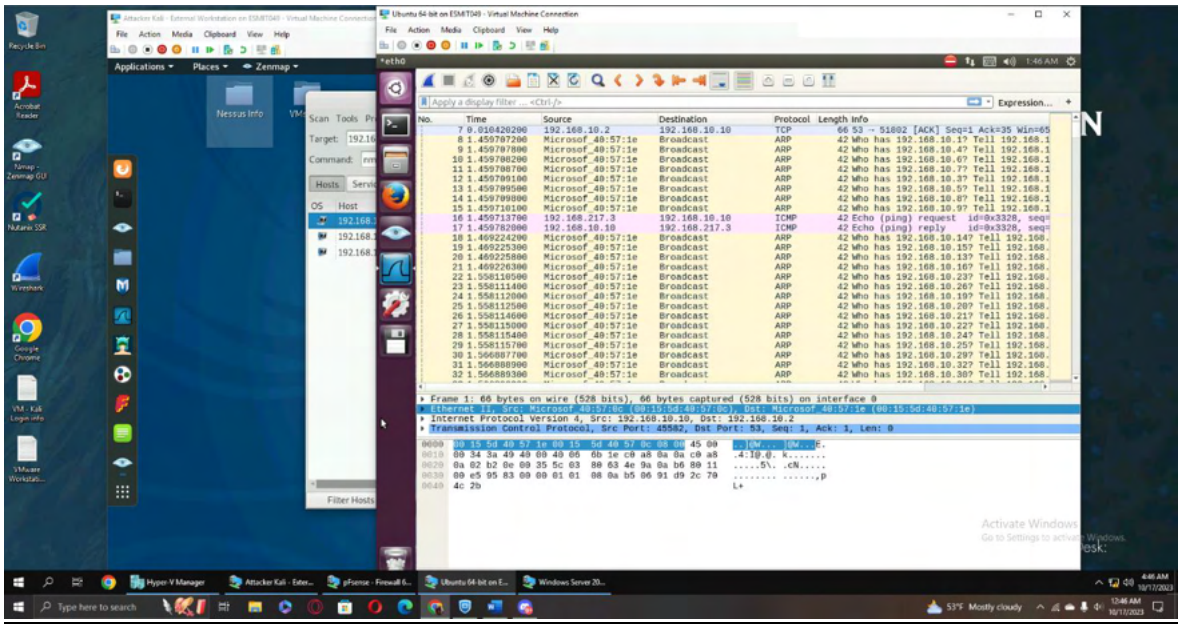


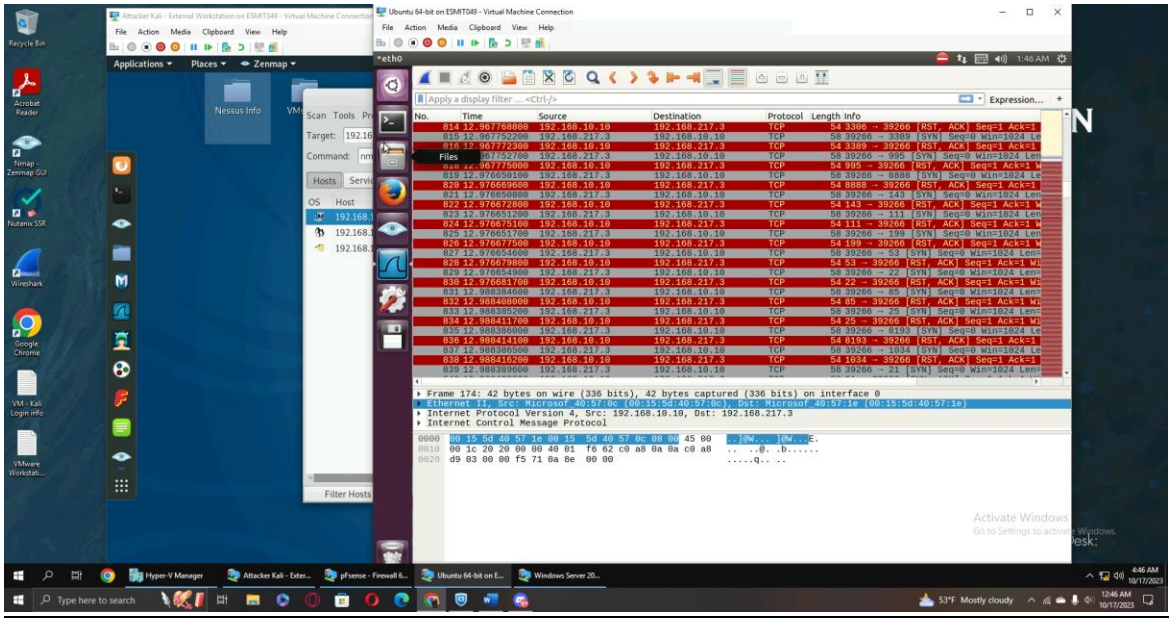
Explanation: The scan of all available networks shows the different ports, as well as their status and service. For the IP Address of 192.168.10.2, we can see that the 53, 80, and 443 ports are open and are all TCP ports. Port 53 deals with domain services (DNS), port 80 deals with HTTP protocol, and port 443 deals with HTTPS protocol, the more secure version of HTTP. For the IP Address of 192.168.10.10, or the

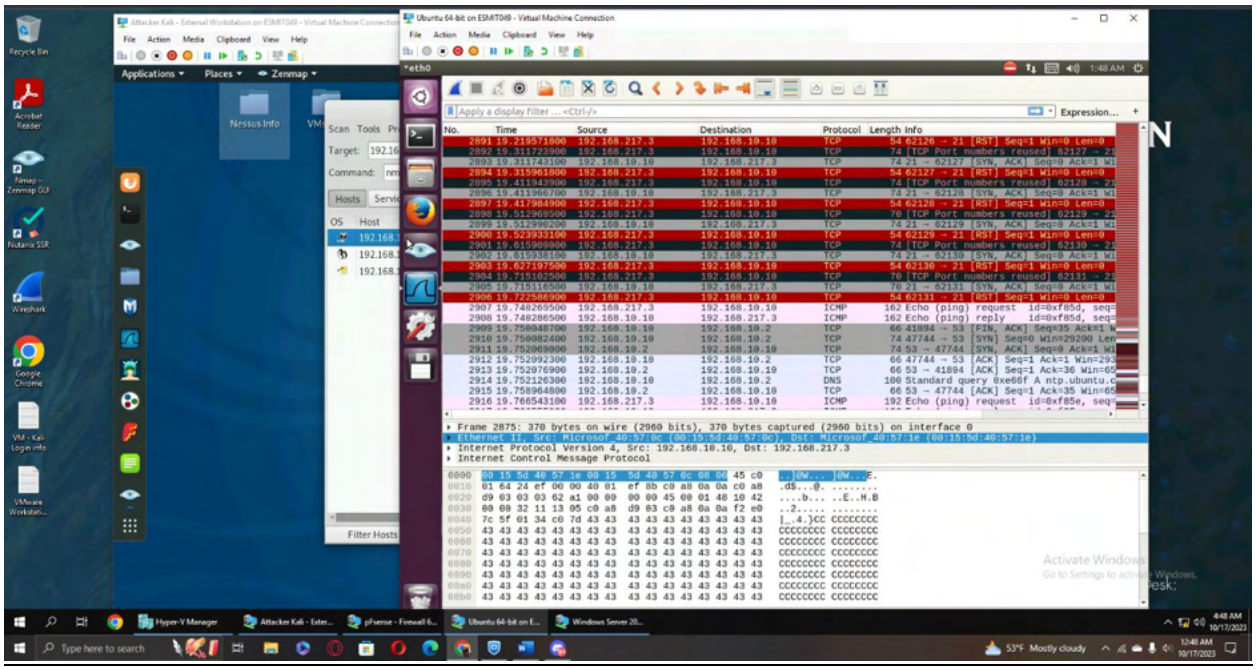
Ubuntu VM, we can see that just port 21 is open, which is a TCP port that deals with FTP protocol. The final IP Address we can see is 192.168.10.11, or the Windows Server 2008 R2 VM, which has the most ports. All of its ports are TCP ports and port 21 still deals with FTP protocol, while port 80 still deals with HTTP protocol as we mentioned before. Port 135 deals with MSRPC service, port 445 deals with microsoft-ds service, port 3389 deals with ms-wbt-server service, and 49154 deals with a service titled "unknown".

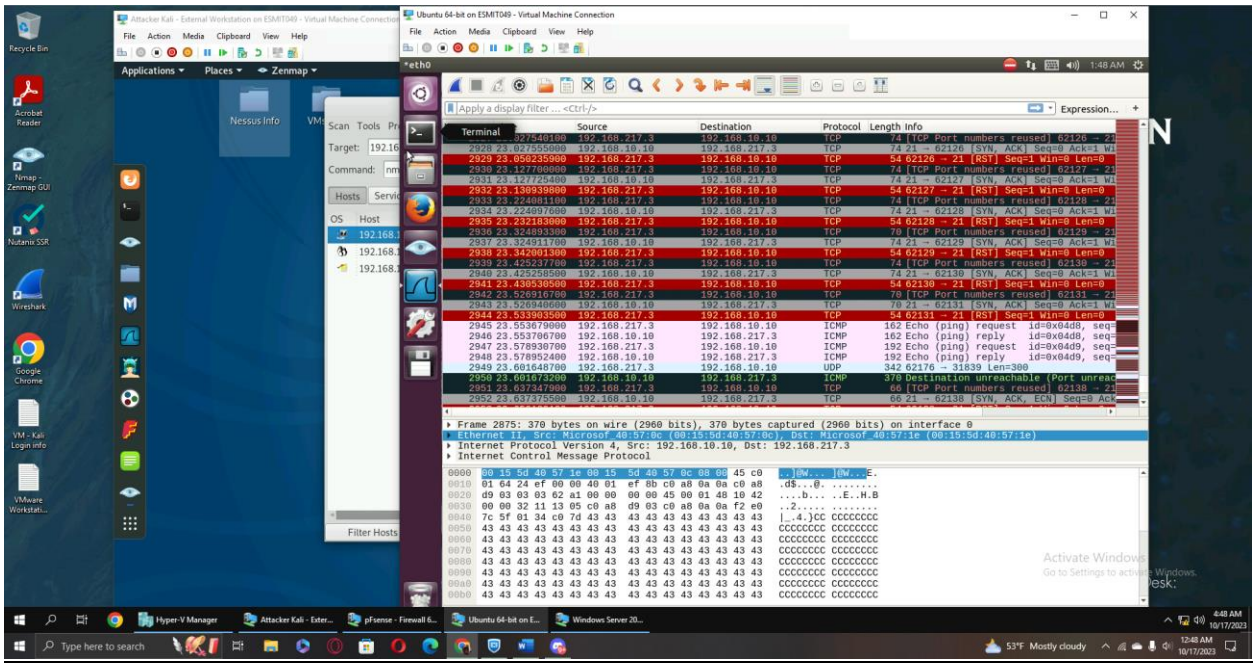
2. Run Wireshark in Ubuntu VM while External Kali is scanning the network. Discuss the traffic pattern you observed. What do you find? **Please write a 200-word essay to discuss your findings.**

Screenshots:









200-word essay:

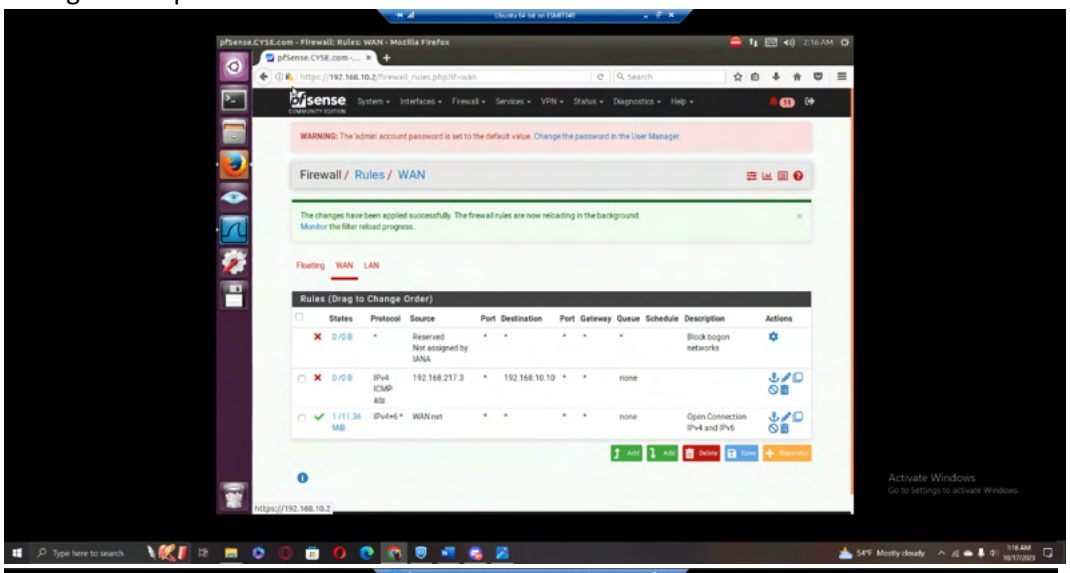
When the scan begins, Wireshark shows multiple ARP packet broadcasts being sent, each one asking who has certain IP addresses beginning with 192.168.10.1 and ranging to the end of the subnet. We see this for most addresses, but 192.168.10.10 instead shows an ICMP echo (ping) request followed by an ICMP reply. This is the address for the Ubuntu VM, so it seems that External Kali's Nmap Intense Scan is able to locate this IP Address because it is one of the only ones that is actually running, allowing it to send a ping request and receive a response. After External Kali continues to scan, we can see on Wireshark that External Kali is now attempting to establish the TCP three-way handshake with various ports on the Ubuntu VM by sending TCP SYN packets, but cannot because

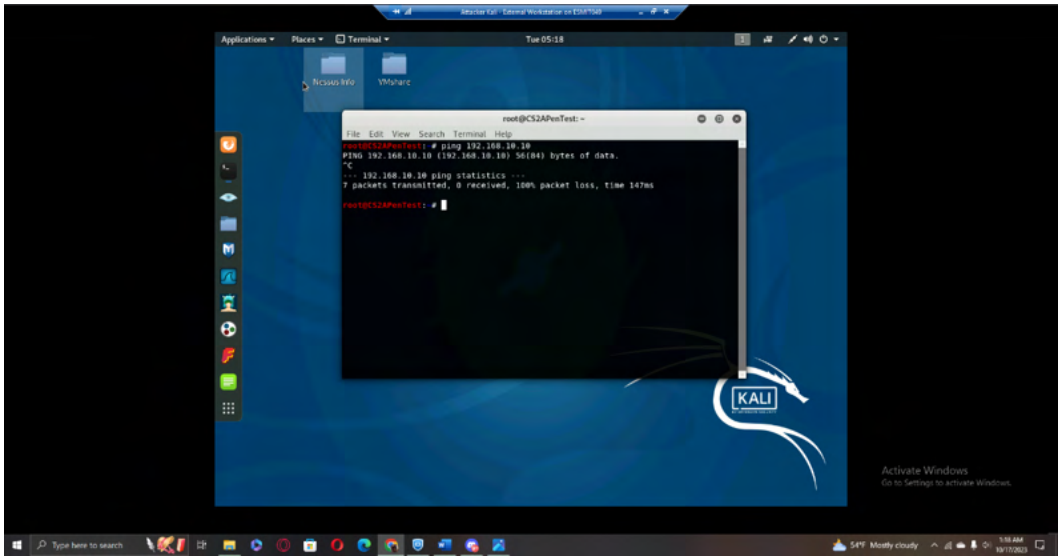
none of the ports it is attempting to connect with are open. It then comes across Ubuntu VM port 21, and it continuously sends a TCP SYN packet from various External Kali ports to check if port 21 is open. Port 21 responds to almost all of them with TCP SYN packets of its own, showing that it is open. Near the end of the scan, we see the TCP SYN packets from both sides halt and we see a few more ICMP packets get sent from External Kali, which Ubuntu responds to as anticipated with an ICMP reply.

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.

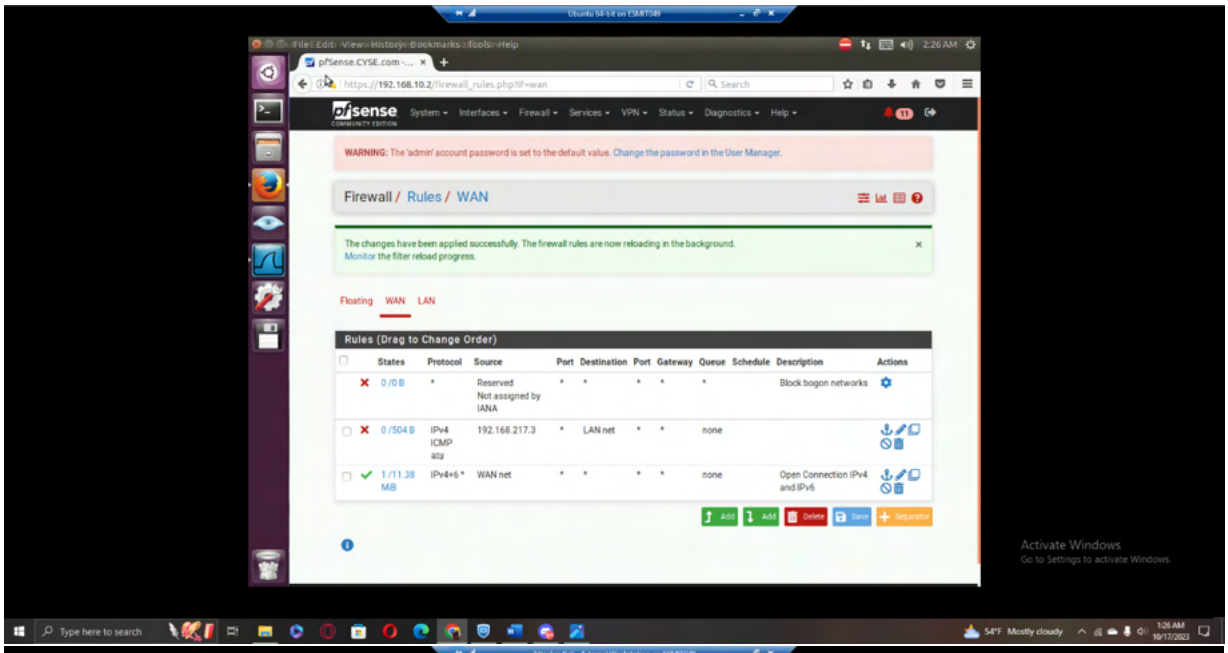
1. Configure the pfSense firewall rule to block the ICMP traffic from External Kali to Ubuntu VM.

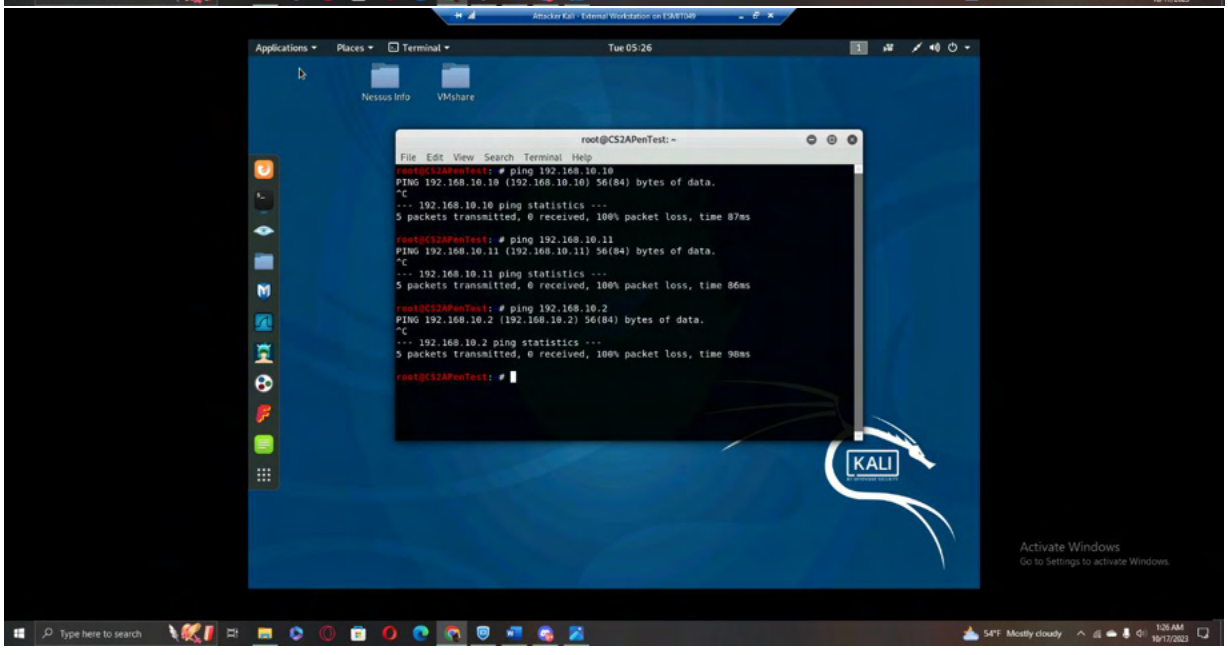




Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
1	WAN	block	192.168.217.3	192.168.10.10	N/A

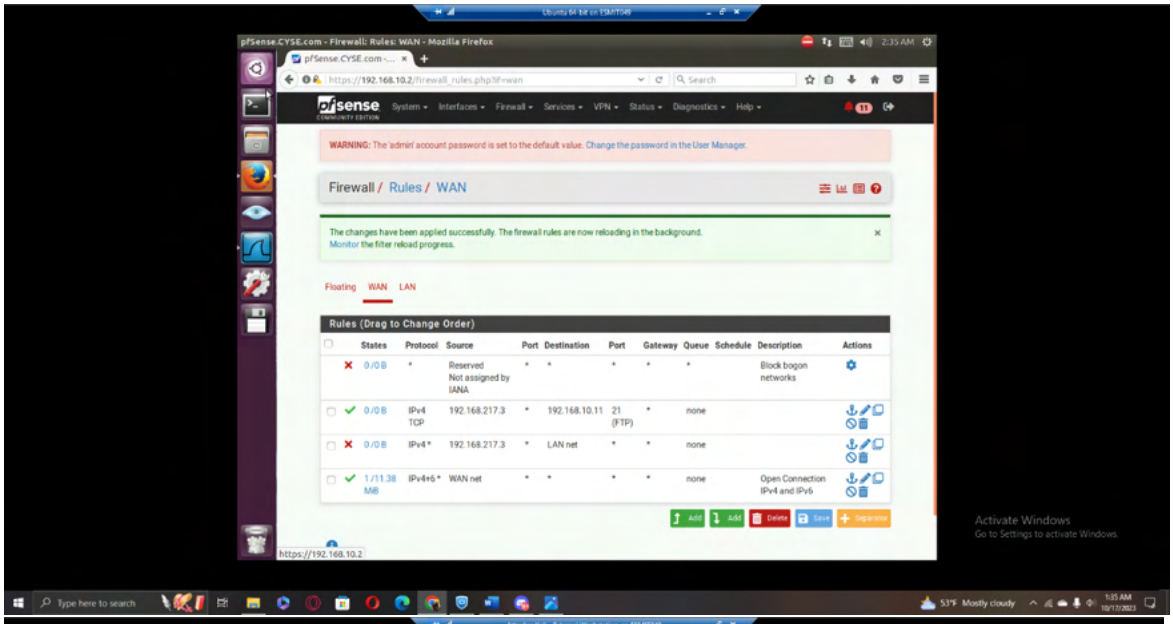
2. Clear the previous firewall policies and configure the pfSense firewall to block all ICMP traffic from External Kali to the LAN side.

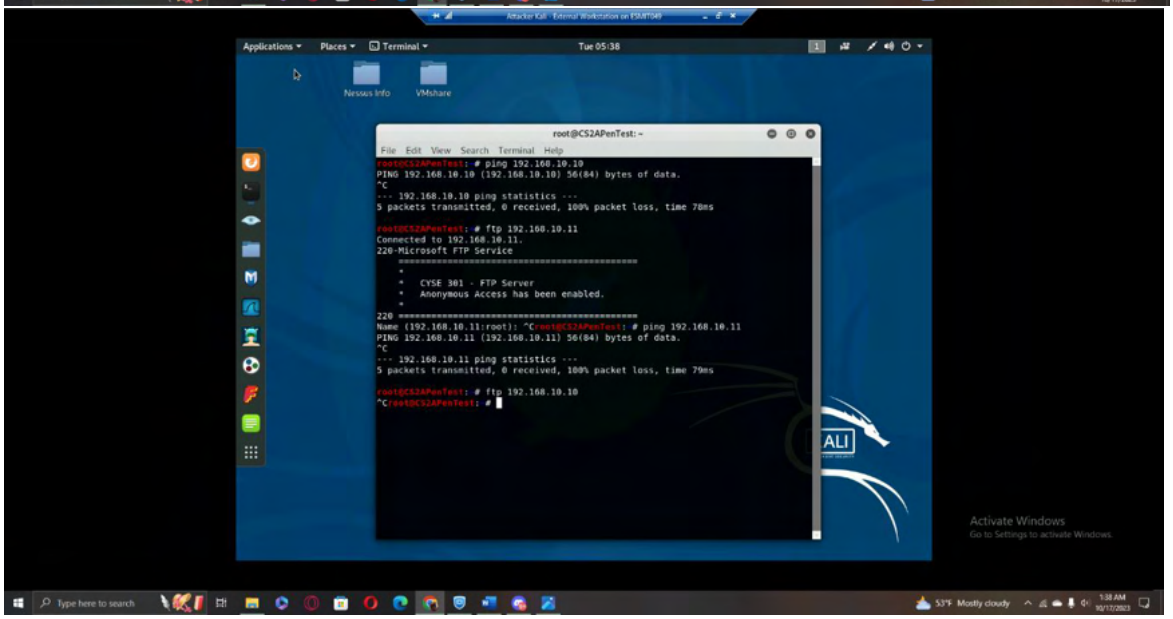




Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
1	WAN	Block	192.168.217.3	LAN net	N/A

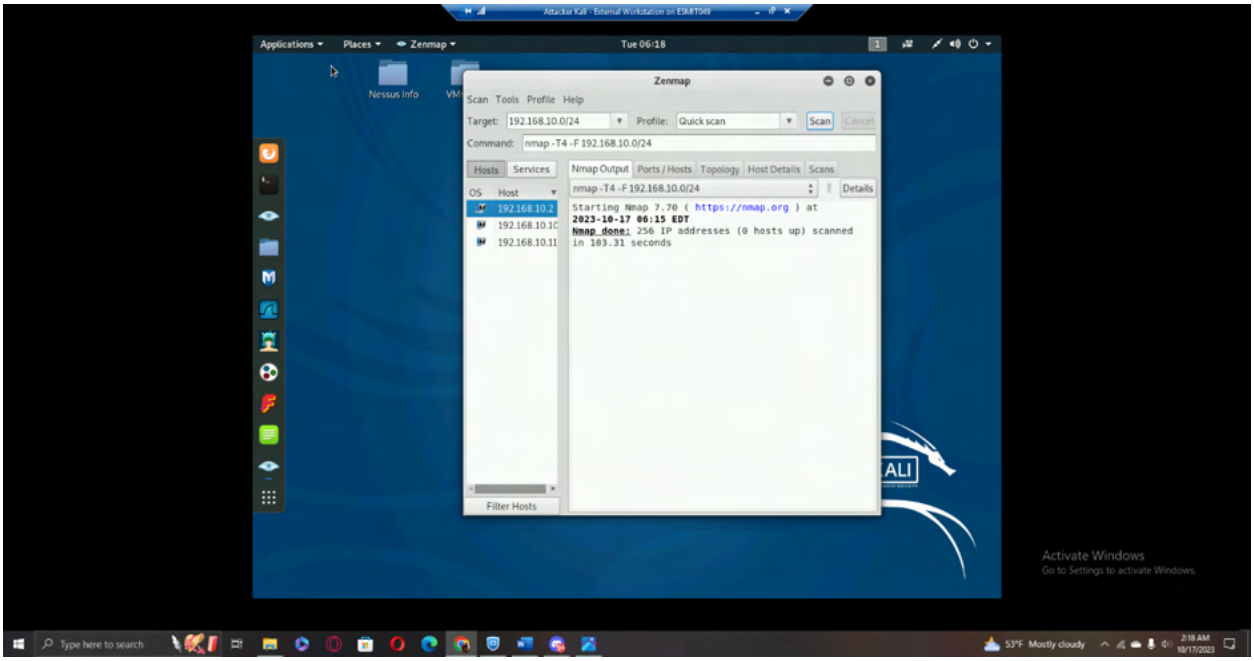
3. Clear the previous firewall policies and configure the pfSense firewall to block ALL traffic from External Kali to the LAN side, except for the FTP protocol towards Windows Server 2008.





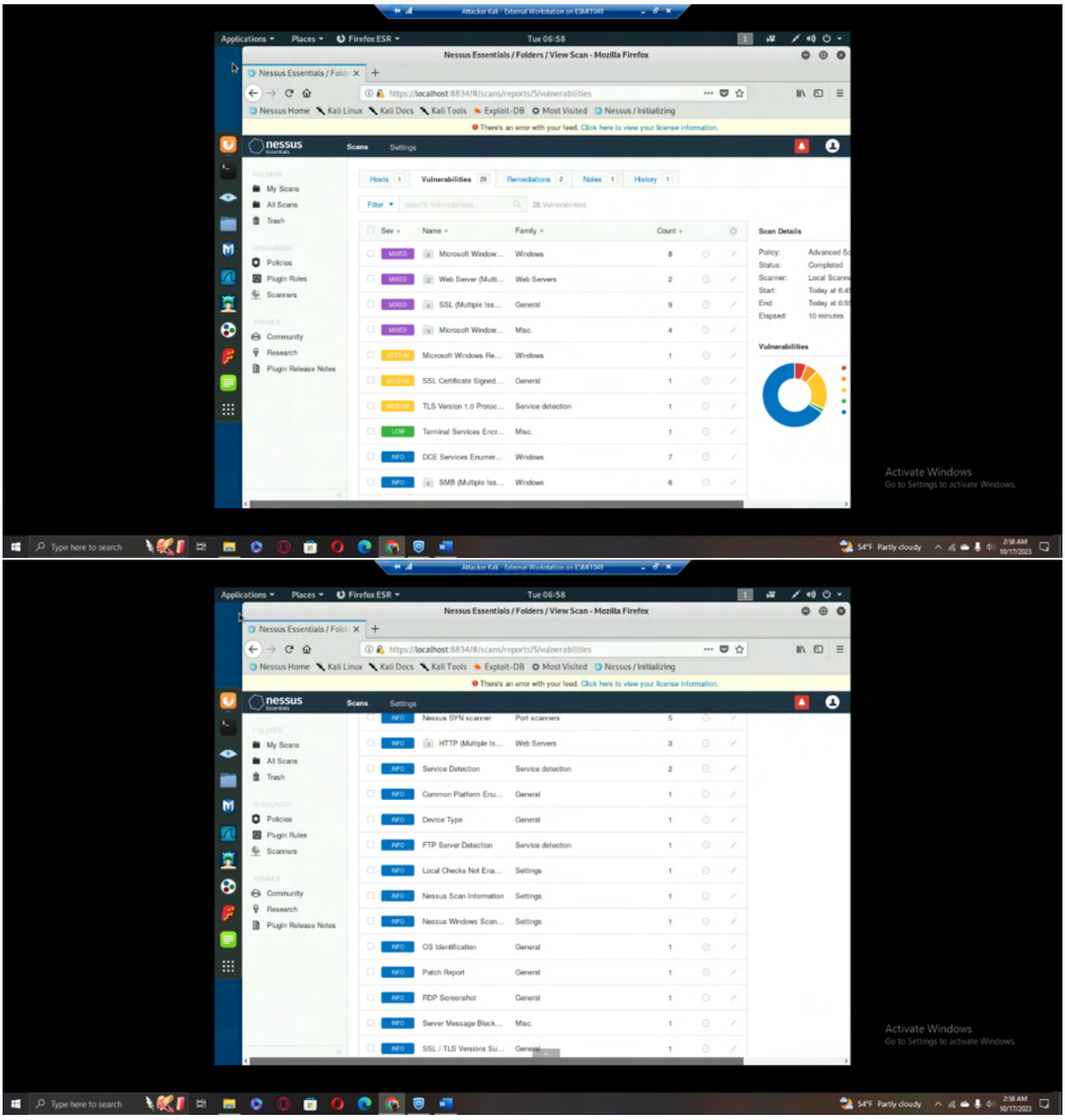
Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
1	WAN	pass	192.168.217.3	192.168.10.11	FTP (port 21)
2	WAN	Block	192.168.217.3	LAN net	N/A

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



Explanation: The Nmap scan is not picking up any hosts or open ports, including port 21 (FTP port) for IP Address 192.168.10.11 (Windows Server 2008 R2 VM).

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



Explanation: There were 28 total vulnerabilities found in the NESSUS Scan of Microsoft Windows Server 2008 R2 VM. Of the 28 found vulnerabilities, four were considered mixed severity, three were considered medium severity, one was considered low severity, and the other 20 were considered “info” severity, which seems to be a level under low severity.