OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #3 Assignment 3: Sword vs. Shield

Stuart N. Howard

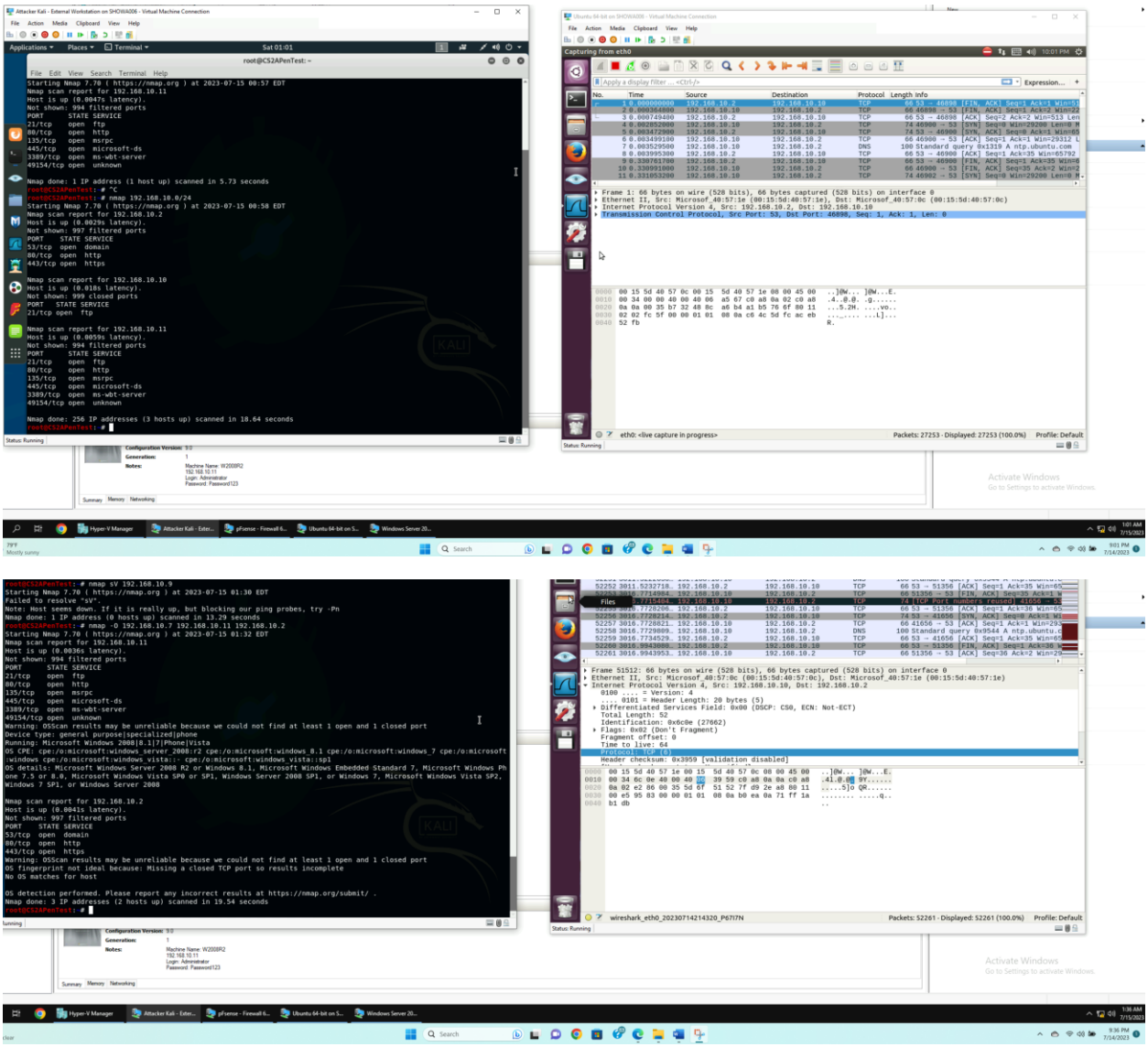
01241576

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

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.**

Task A.1

Use namp to scan the subnet using the Nmap 192.168.10.0/24



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

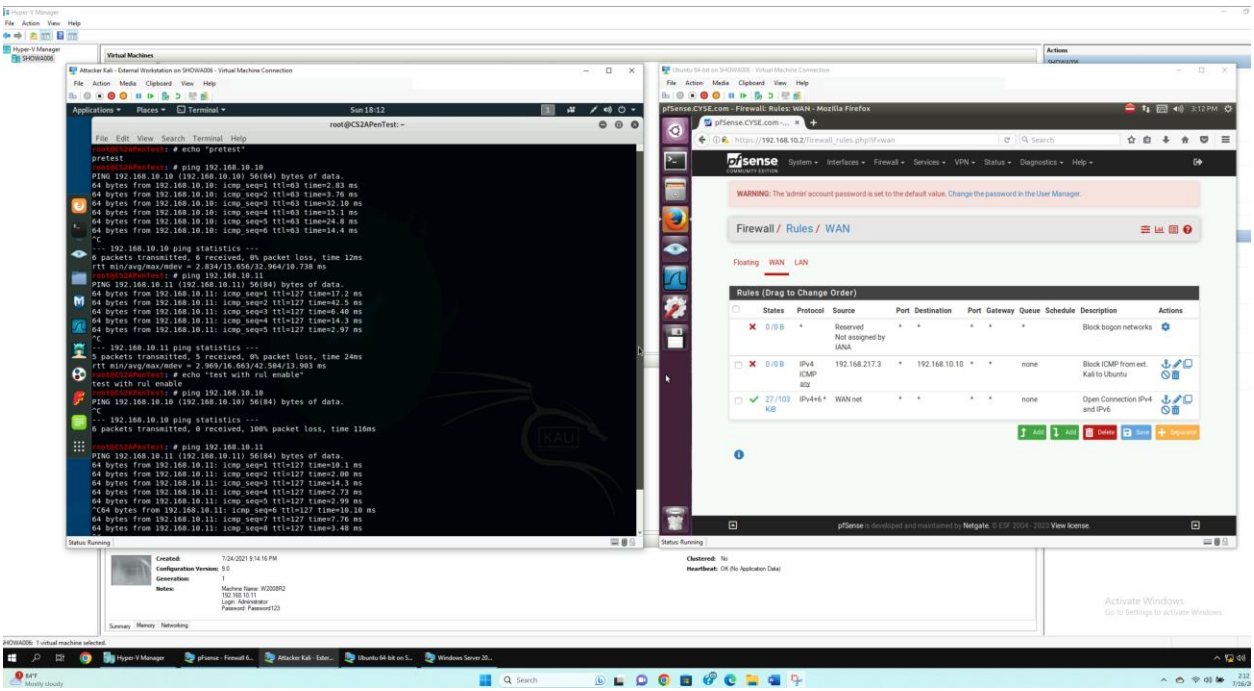
By analyzing the captured network traffic, we aim to gain insights into the traffic patterns, identify potential vulnerabilities, and understand the impact of the network scan on the LAN environment. The network scan caused an increase in ARP traffic. The Kali sent ARP requests to discover the MAC addresses of various IP addresses on the network, and the ARP replies containing their respective MAC addresses. Wireshark captured TCP and UDP packets showing port scanning activities probing different ports from the Nmap port scan. During the network scan, we observed ICMP traffic in the echo requests and responses (ping). The network traffic analysis during the External Kali network scan provided effective insights into the impact of the scanning activities. I was able to ARP traffic, port scanning activities, ICMP, and requests and responses for source and destination IPs. These findings aided in the verification of the Nmap process and the need for effectiveness. We can identify and mitigate potential security risks by analyzing the captured traffic patterns, such as open ports, to strengthen the overall network security posture.

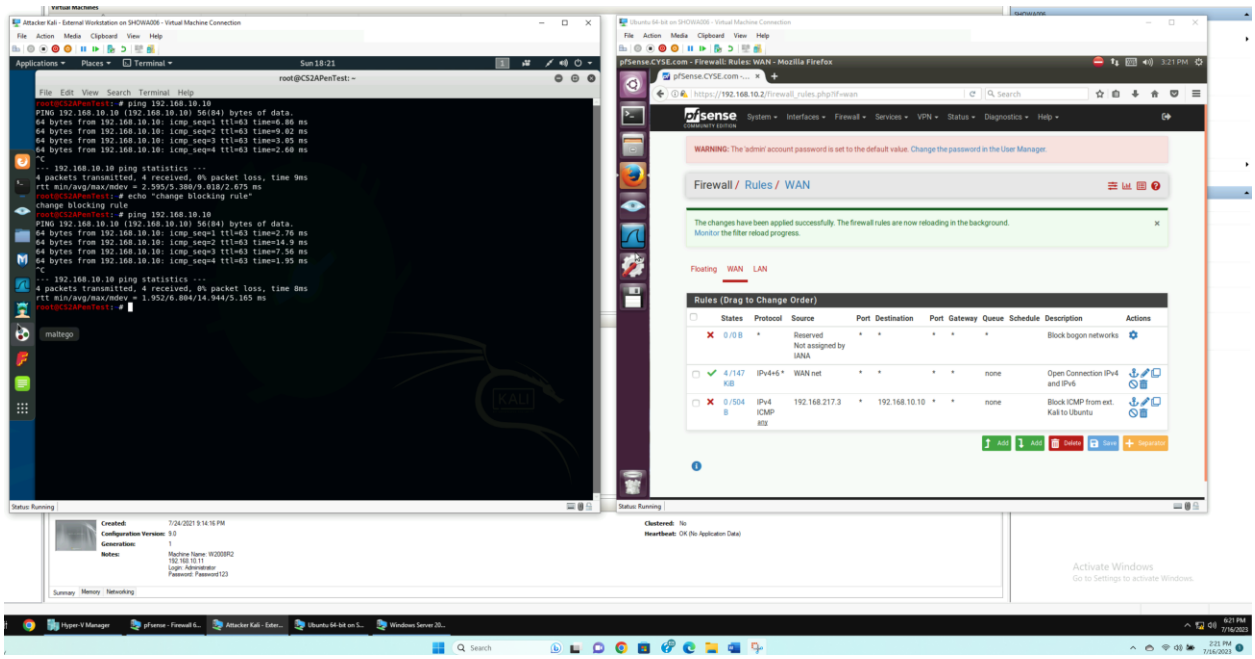
Task B: Shield – Protect your network with firewall (10 + 10+ 20 + 20 = 60 points)

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)
	WAN	Block/reject	192.168.217.2	192.168.10.10	ICMP

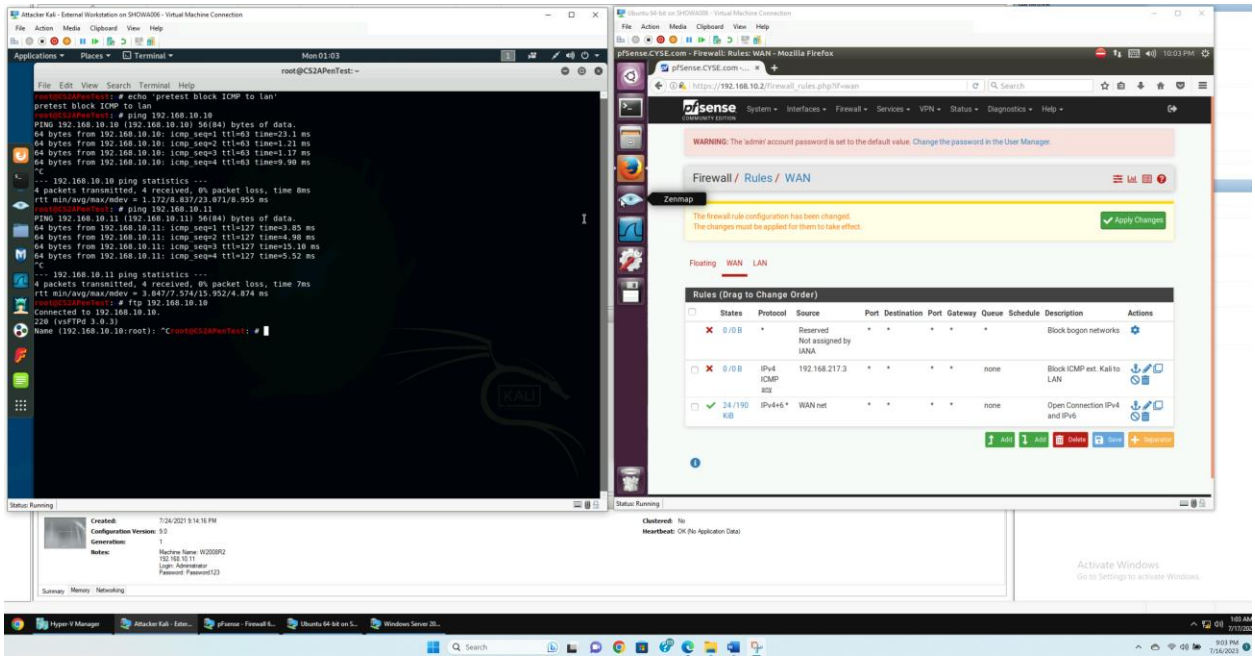




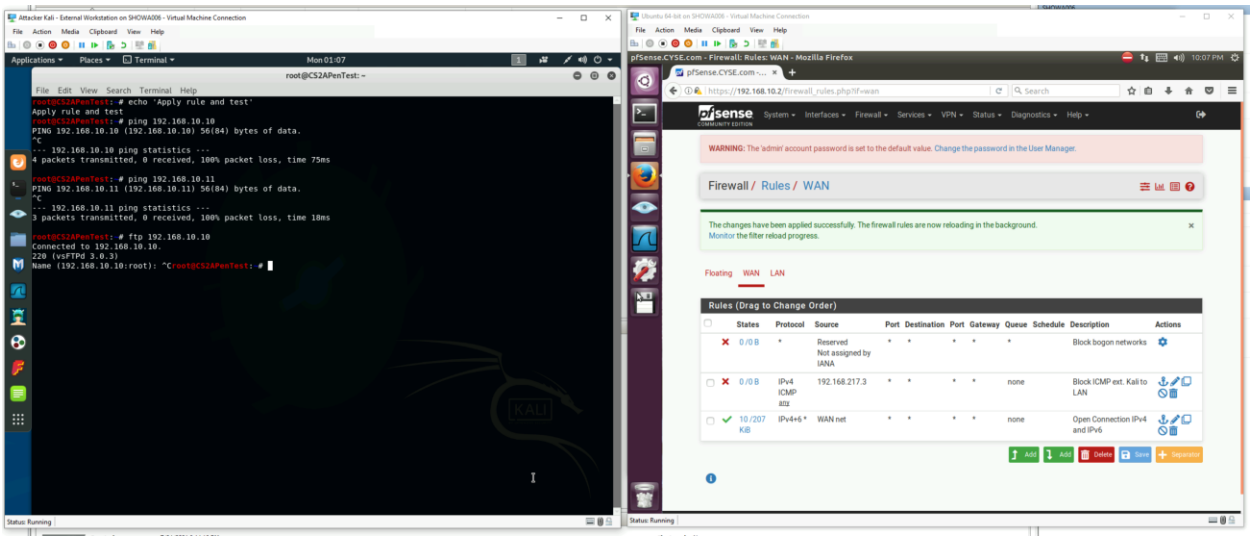
2. Clear the previous firewall policies and configure the pfSense firewall to block all ICMP traffic from External Kali to the LAN side.

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
	LAN	Block	192.168.217.3	192.168.10.2	

- Pre-test
- ping to Ubuntu (PASS)
- ping to WS 2008 (PASS)
- FTP to Ubuntu (PASS)



- Apply the rule
- Test the rule
- ping to Ubuntu (No response/ blocked)
- ping to WS 2008 (No response/ blocked)
- FTP to Ubuntu/WS 2008 (PASS

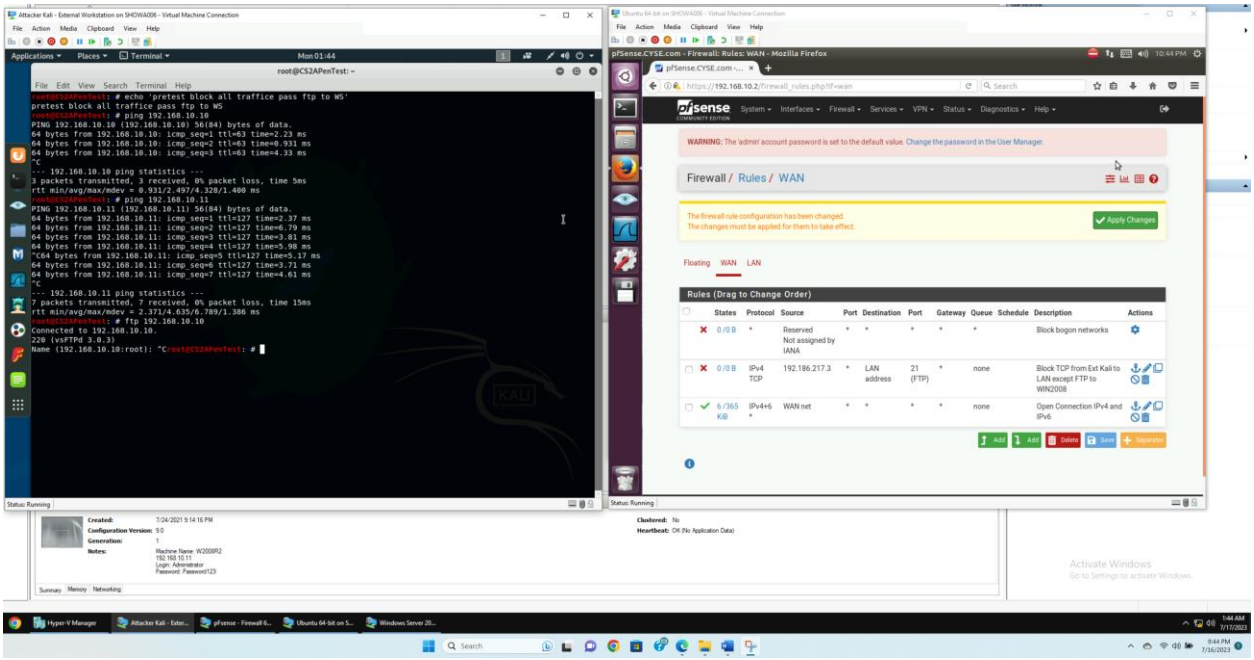


3. Clear the previous firewall policies and configure the pfSense firewall to block ALL traffic from External Kali to the LAN side, except for the FTP protocol towards Windows Server 2008.

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
2	WAN	Block	192.168.217.3	LAN Address	TCP

Pre-test

- ping to Ubuntu (PASS)
- ping to WS 2008 (PASS)
- FTP to Ubuntu (PASS)



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

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