CYSE 301: Cybersecurity Technique and Operations

Assignment 3: Sword vs. Shield

Joshua Taylor
01031996

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)

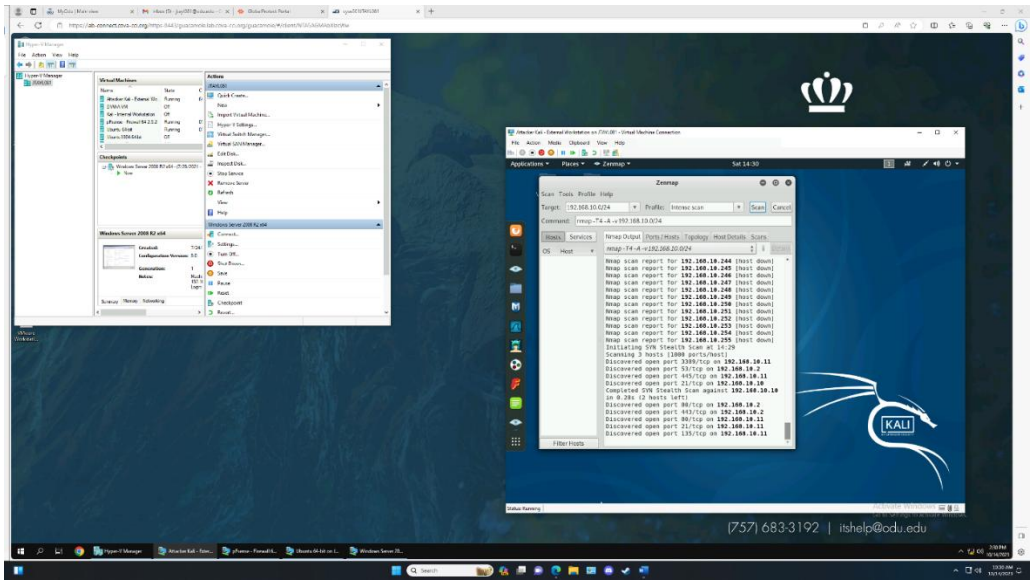
Power on the listed VMs and complete the following steps from the **External Kali** (you can use either nmap or zenmap to complete the assignment)

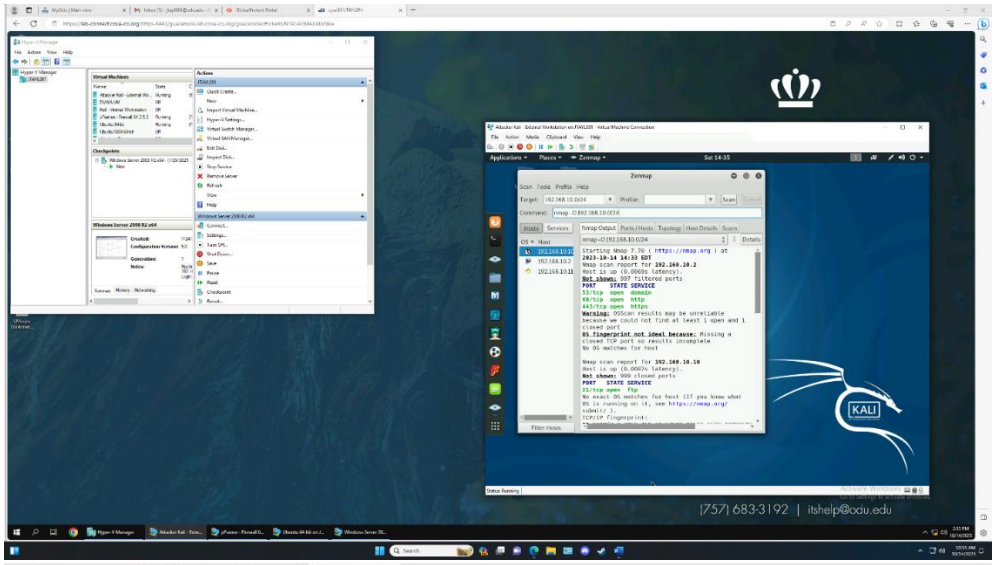
- External Kali
- pfSense
- Ubuntu
- Windows Server 2008

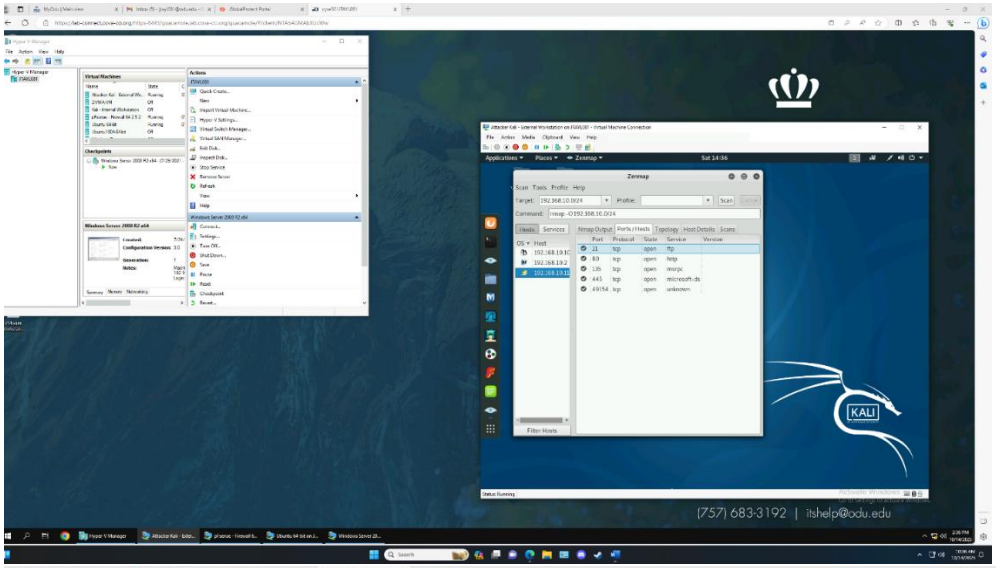
Make sure you didn't add/delete any firewall policy before continuing.

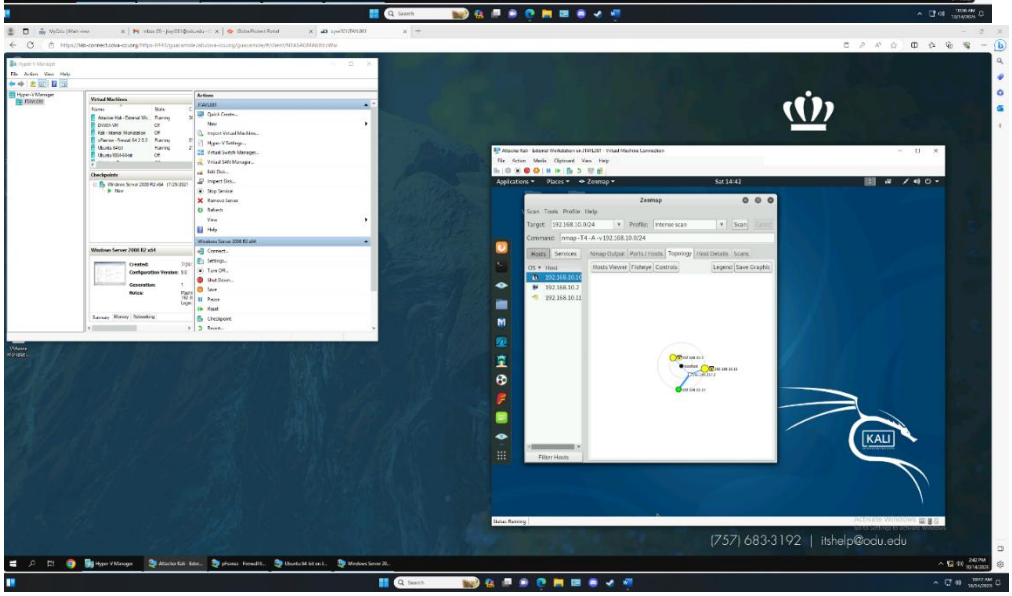
1. Use Nmap to profile the basic information about the **subnet** topology (including open ports information, operation systems, etc.) You need to get the **service** and **backend software** information associated with each opening port in each VM.

   - For this excersize I scanned the network using zenmap from the external Kali. I scanned the subnet of 192.168.10.0/24 to get a broad overview of the subnet. It provided me with a image of the topology and showed that ther were 3 other machines powered on on the subnet (Ubuntu, pfsense, and Windows 2008.) When I did the intense scan of just the subnet, it showed that there were a few ports open on various systems such as port 80, 3389, 21, and 49154. However, when I conducted an operating system scan (nmap -O 192.168.10.0/24) it again showed 3 other systems, however it showed other ports open such as port 443 and 53. It also showed that windows 2008 was an operating system that was on one of the scanned machines. The scan was unable to determine what pfsense and the ubuntu OS were.



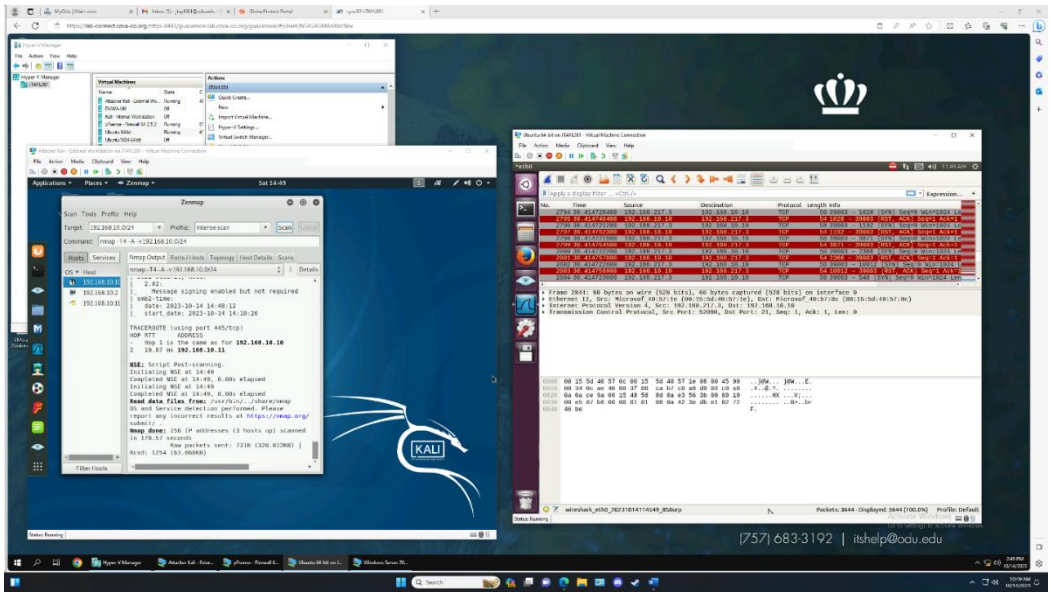

(757) 683-3192 | itshelp@odu.edu

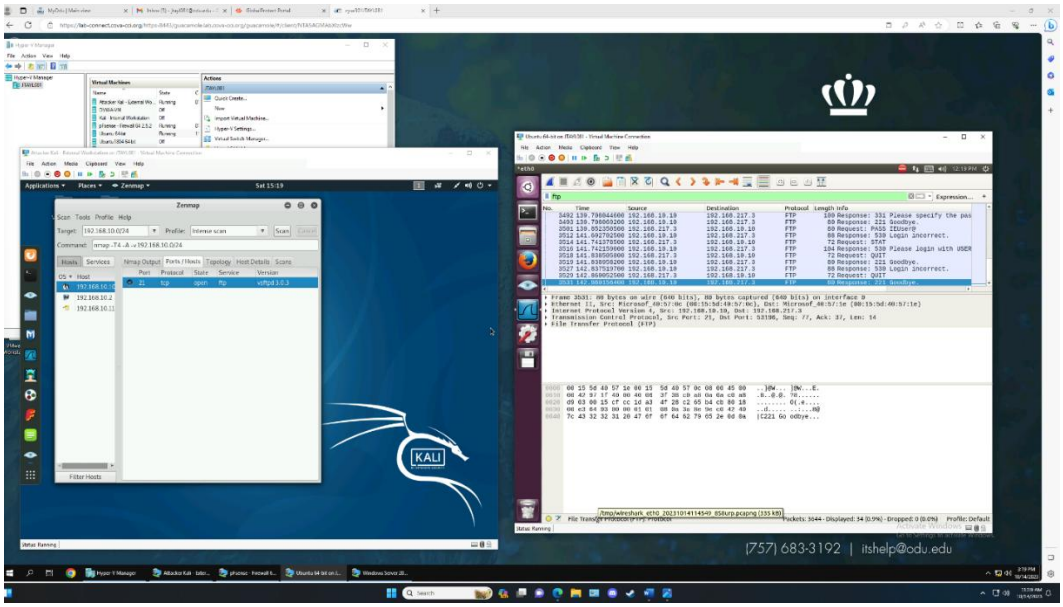

(757) 683-3192 | itshelp@odu.edu


(757) 683-3192 | itshelp@odu.edu

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.**

- Initially when I ran wireshark on the Ubuntu machine, It showed various arp requests and connections to the DNS server. However, once I began scanning on the external Kali machine, the wireshark on the Ubuntu machine was inundated with Syn/Ack requests from the Kali machine. After combing through various packets on Wireshark, it appears that the Kali machine was sending requests to various ports on the Ubuntu Machine (I also expect it was happening on the other powered on machines on the network) to see if it got a response indicating it was open. The packets were destined for all kinds of ports, not just the commonly used ports like 443, 53, etc. The Kali source port was always 39003. Primarily it appears that Kali was utilizing TCP packets, it did however also ping various systems with ICMP packets. One thing of note that I found was that Kali linux had attempts to access the FTP server, and attempted multiple times to input usernames and password. All of which appear to have been unsuccessful. What I gatherd from this excersize is that zenmap will show what ports are open, the topology of the network that it can detect, operating systems, etc. Wireshark showed how zenmap achieves this, by sending out packets looking for responses, attempting to log in to systems, etc.





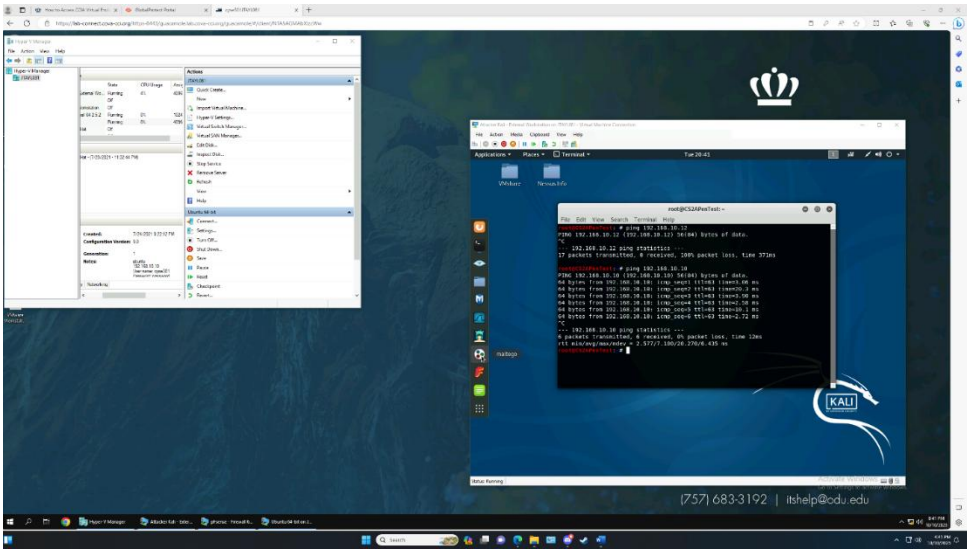
Task B: Shield – Protect your network with firewall (10 + 10+ 20 + 20 = 60 points)

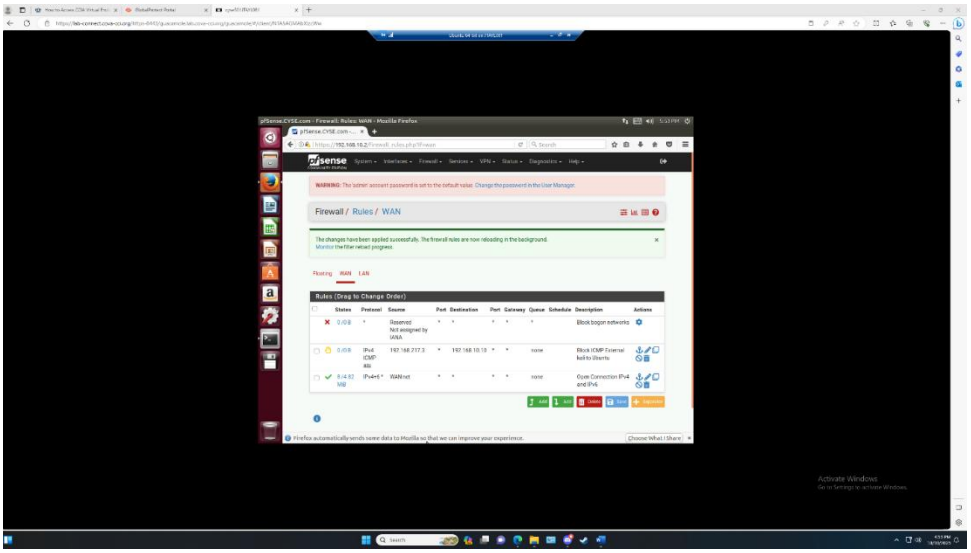
In order to receive full credits, you need to fill the table (add more rows if needed), implement the firewall rule(s), show me the screenshot of your firewall table, and verify the results.

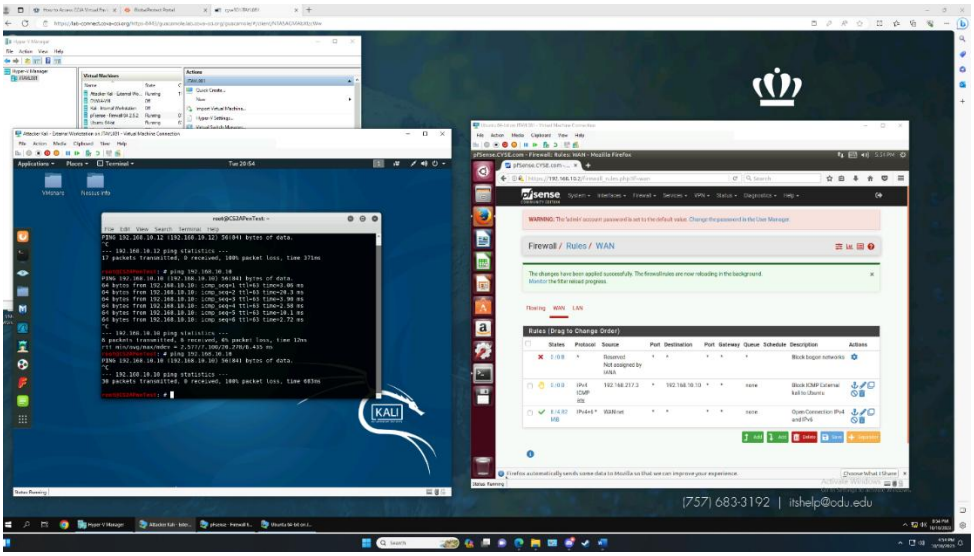
1. Configure the pfSense firewall rule to block the ICMP traffic from External Kali to Ubuntu VM.

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

- For this rule, I started up the External Kali, Ubuntu, and pfsense VMs. I checked before applying a rule that ICMP traffic was flowing between the external kali and Ubuntu VMs. After establishing that the machines could talk to each other I applied the rule to the pfsense firewall by logging into the firewall via the Ubuntu machine and using the GUI. After setting the rule on the machine I retested the ICMP traffic to ensure the rule worked, and after seeing that ICMP traffic from the external Kali machine no longer made it through to the Ubuntu machine I verified using the Windows 7 VM that ICMP traffic was still making to other machines. The windows 7 machine was receiving traffic from the External Kali machine, indicating to me that the rule worked as intended.


(757) 683-3192 | itshelp@odu.edu

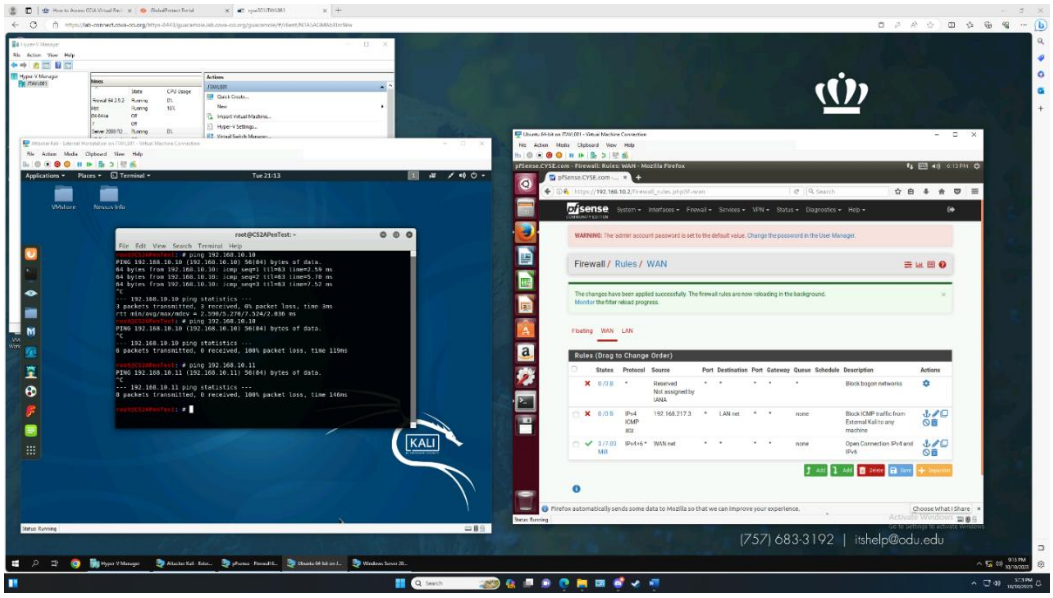

pfSense.CYSE.com - Firewall: Rules: WAN - Mozilla Firefox
Firewall / Rules / WAN


(757) 683-3192 | itshelp@odu.edu

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	WAN	Block/Reject	192.168.217.3	LAN Net	ICMP

- After erasing the previous steps rule, I retested ICMP traffic from External Kali to Ubuntu to ensure it was working properly again; it was. After that I entered the new policy blocking all ICMP traffic from the external Kali VM to any LAN VM. After setting the rule, I verified the validity of the rule on both the Ubuntu VM and the Windows Server 2008 VM; both of which did not receive ICMP traffic from the external Kali.

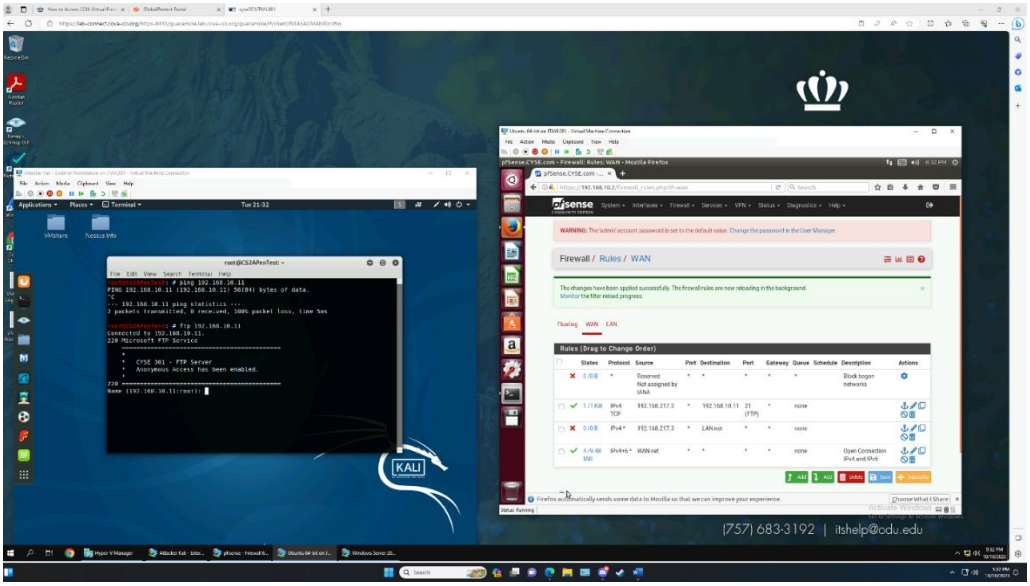


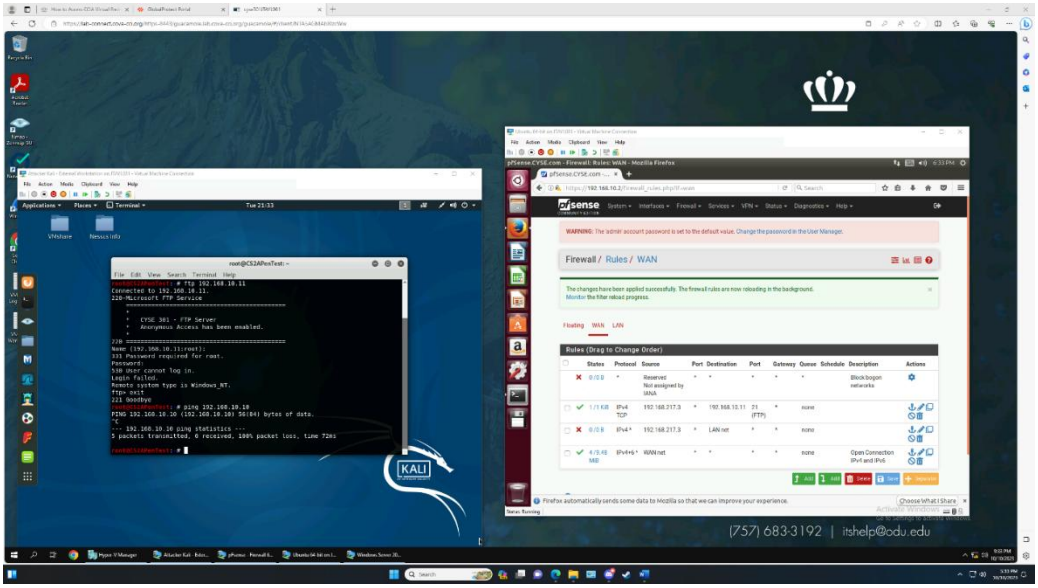
3. Clear the previous firewall policies and configure the pfSense firewall to block ALL traffic from External Kali to the LAN side, except for the FTP protocol towards Windows Server 2008.

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
3	WAN	Pass	192.168.217.3	192.168.10.11	21
4	WAN	Block/Reject	192.168.217.3	LAN Net	*

- After resetting the firewall rules, I entered the rules listed above. I verified that the rules worked appropriately by first pinging the windows server 2008 VM; no packets received. I then attempted to connect to the FTP server on the same machine; I was connected and prompted for the login

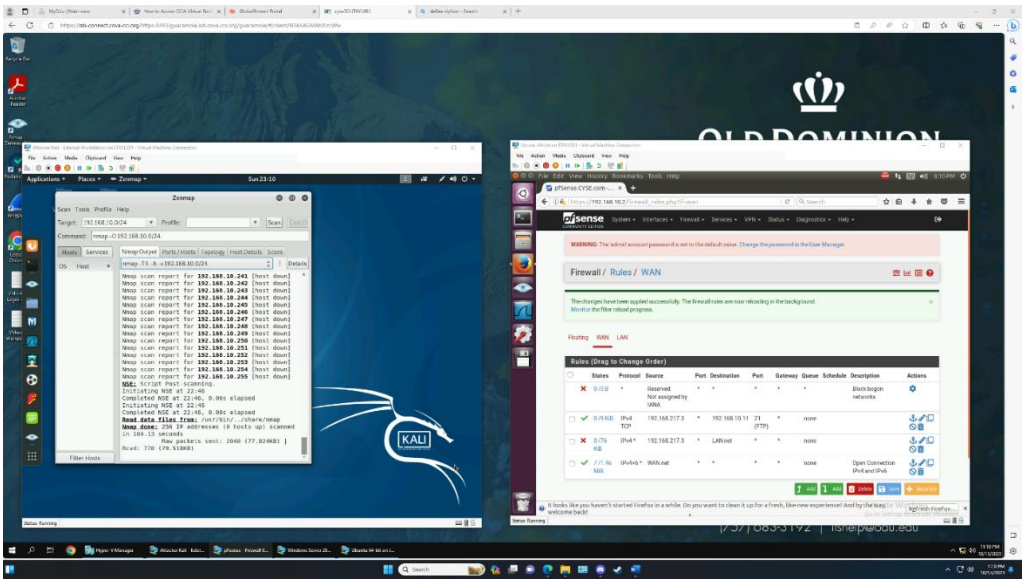
credentials. I then verified that ICMP traffic could not make it to other machines by pinging the Ubuntu VM; no packets received.

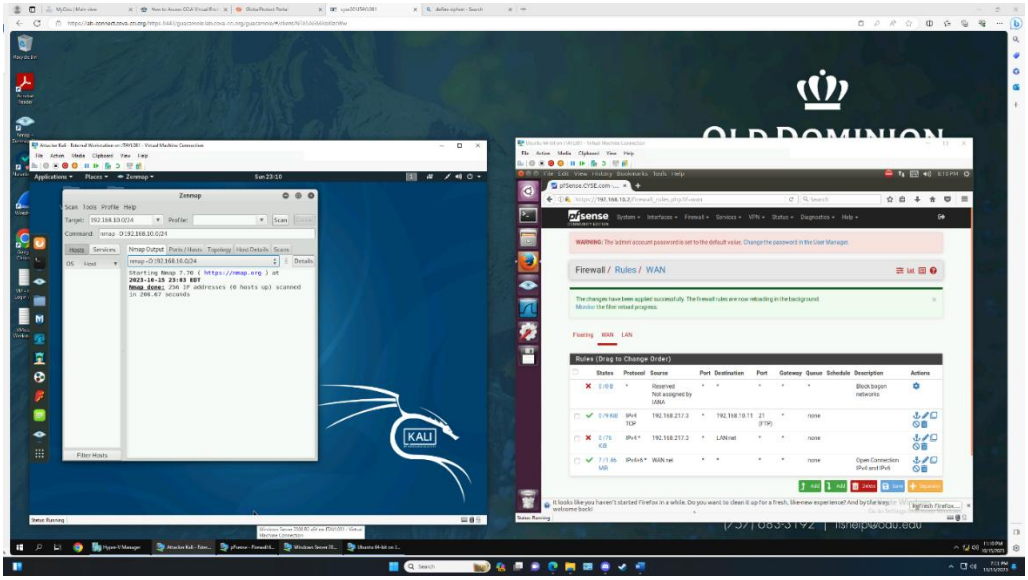




4. Keep the firewall policies you created in Task B.3 and repeat Task A.1. What's the difference?

- When I conducted the same scans on zenmap as I did in task A.1, the results differed from the original. With the firewall rule changes implemented in task B.3 in place, no hosts could be pinged and no operating systems could be identified when I conducted an OS scan on zenmap. That differs from the original scan in that originally I was able to determine the topology, OS system for Windows Server 2008, open ports, and was able to ping and identify the ubuntu systems, windows system, and the pfsense firewall.





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