OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #3 Sword vs. Shield

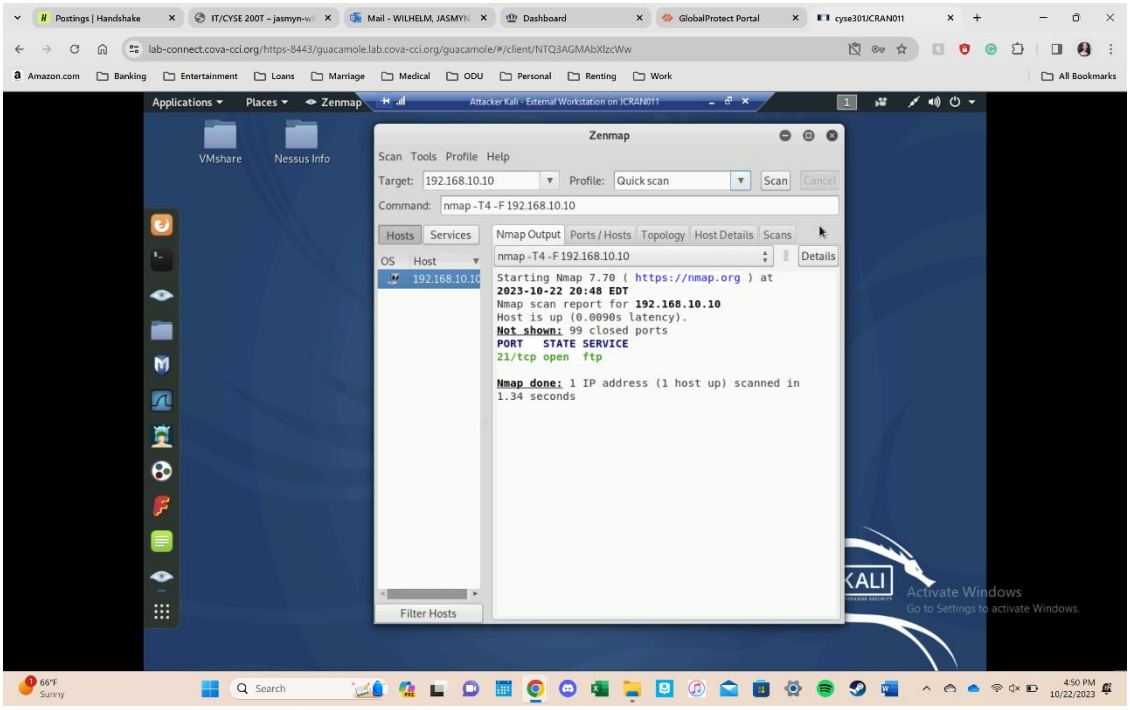
Jasmyn Wilhelm

01155323

Task A: Sword – Network Scanning

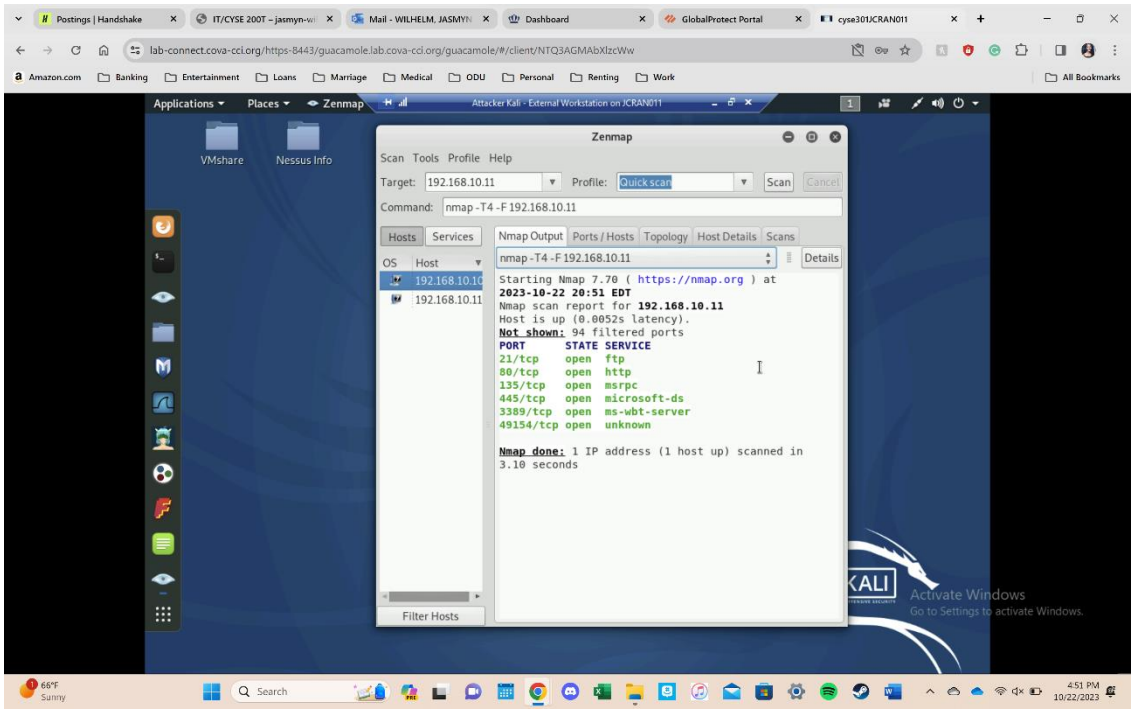
Question 1 Part 1:

Attached is a screenshot of the open ports or a quick scan of the Ubuntu VM. I accomplished this by opening Zenmap and typing in the Ubuntu IP address for a quick scan.



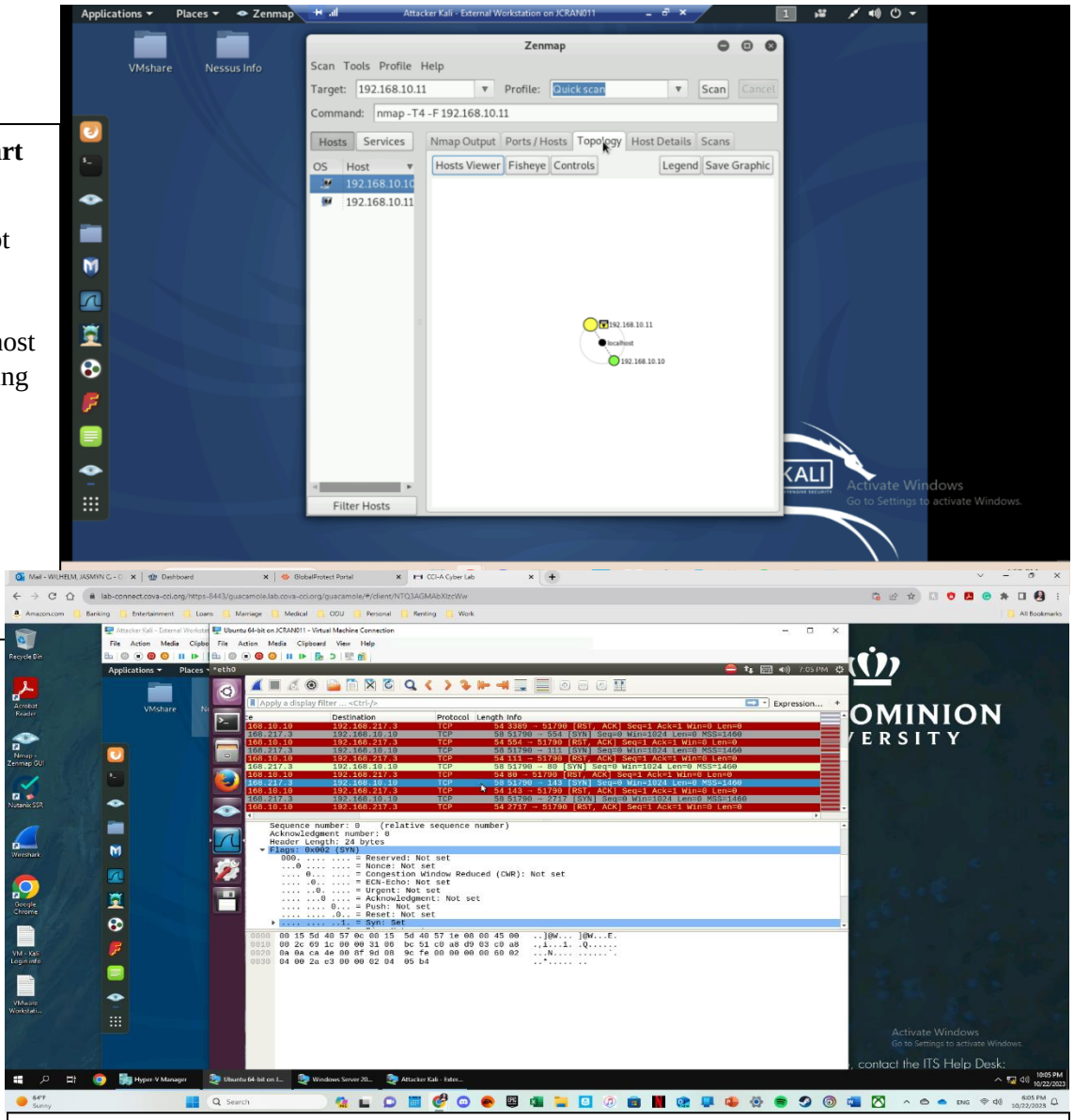
Question 1 Part 2:

This picture shows the quick scan for Windows Server 2008 using the same method for Ubuntu.



Question 1 Part 3:

This screenshot shows the topology including the host and 2 VMs being used.



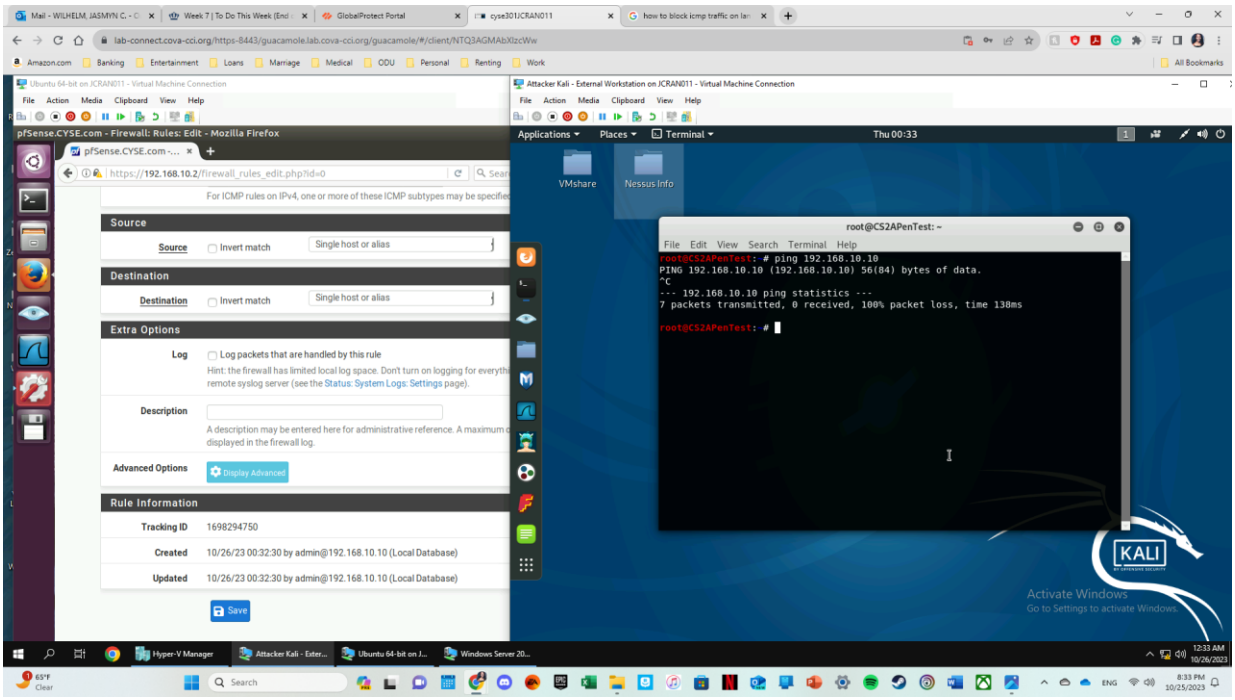
Question 2:

In the screenshot above, the sequence of Attacker Kali reaching the Ubuntu server is shown. The whole time Attacker Kali was scanning the Ubuntu server it appeared in Wireshark as red. The yellow frame is a warning sign. The red frames indicate and potential problem or that a problem is happening. These colors are set by the administrator to best help them differentiate the packets. It can also show these frames at the top when viewing logs. The grey frames indicate the messages that are sent from Attacker Kali to Ubuntu. The red frames show where Ubuntu responds to Attacker Kali's message. The yellow frame shows the open port http receiving a message from Attacker Kali. The Windows 2008 VM was still operating at the time of the scan and therefore showed the ports for that virtual machine as well. The messages in the frame show 'RST". This means the receiver (Ubuntu) should reset the connection or even delete it. The interesting thing in these findings is the fact that port 80 is the only port to have a warning packet for it. The other open ports do not have a warning for them and are hidden in the other packets.

Task B: Shield – Protect your network with firewall

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)
1698286209	**WAN**	**Block**	**192.168.217.3**	**192.168.10.10**	**ICMP**



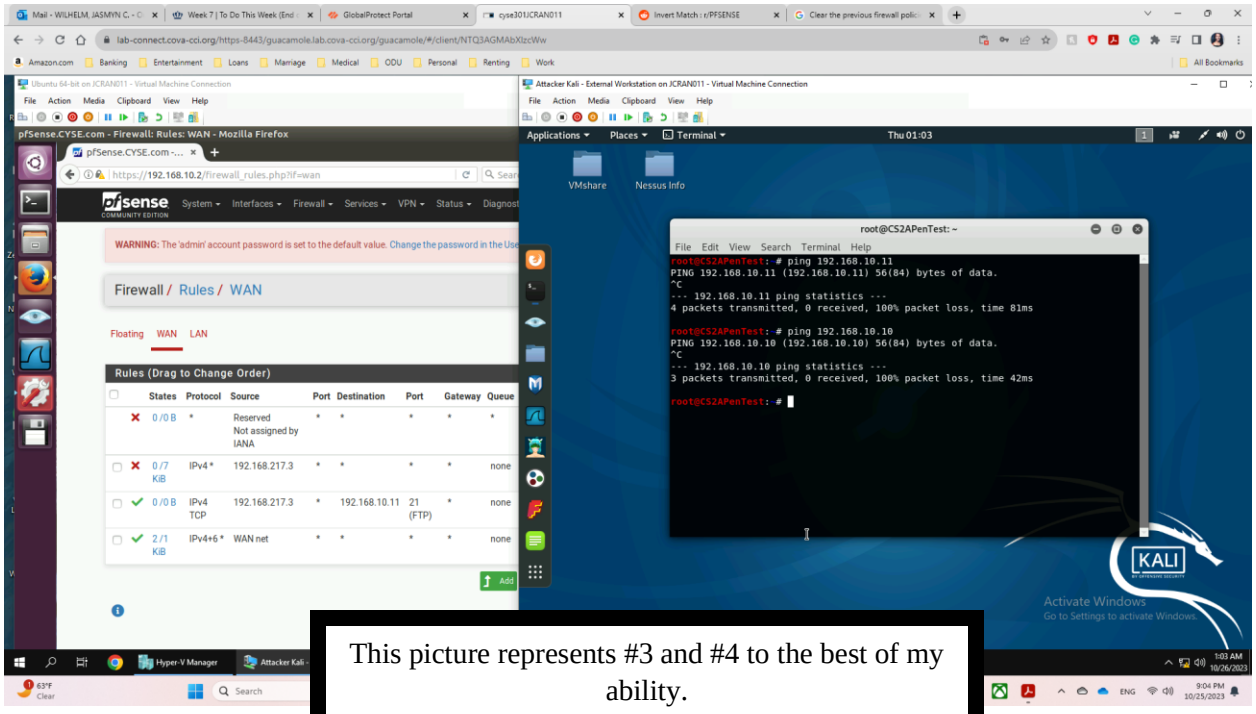
2. Clear the previous firewall policies and configure the pfSense firewall to block all ICMP traffic from External Kali to the LAN side.

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
1698294447	**WAN**	**Block**	**192.168.217.3**		**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)
1698295239	**WAN**	**Allow**	**192.168.217.3**	**192.168.10.11(FTP)**	**TCP**
1698295011	**WAN**	**Block**	**192.168.217.3**		**Any**

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



This picture represents #3 and #4 to the best of my ability.

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