OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

ASSIGNMENT #3: SWORD AND SHIELD

Peter MacMillan

01073897

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.

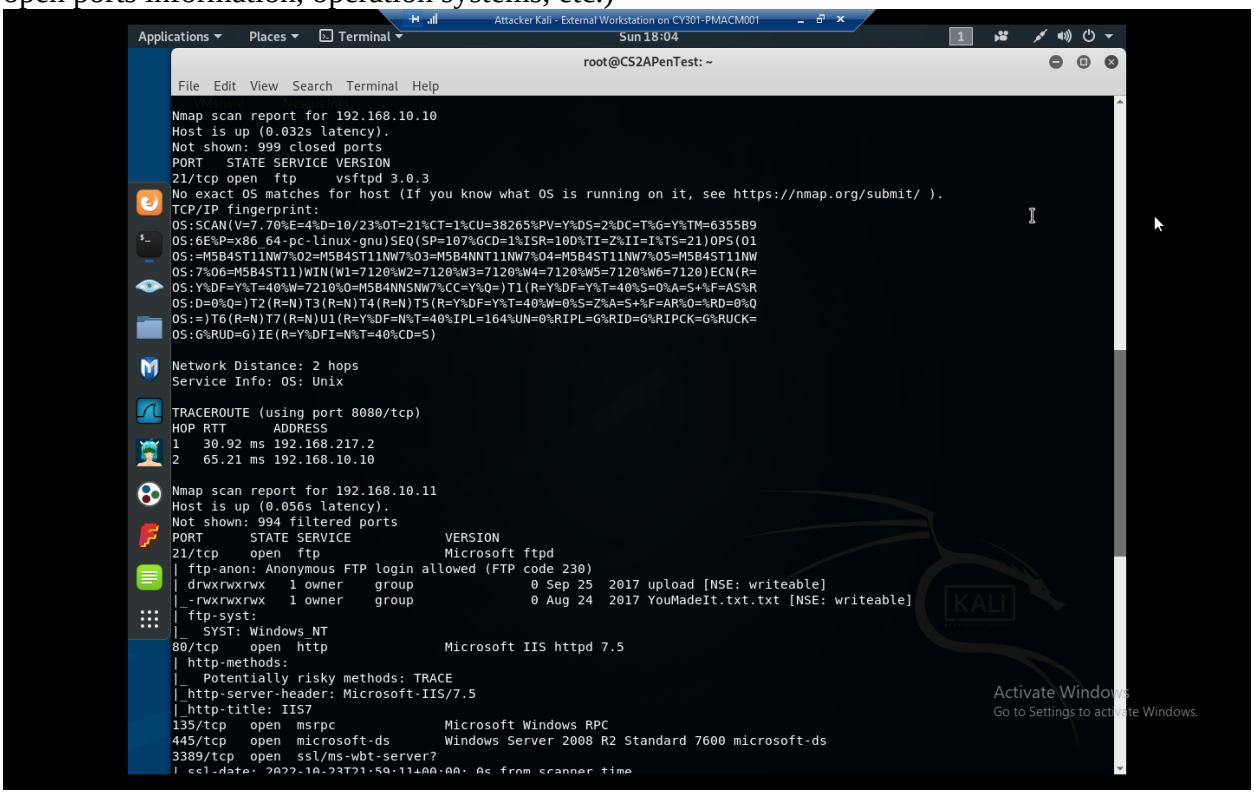
Task A: Sword - Network Scanning (10 + 10 + 20 = 40 points)

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)

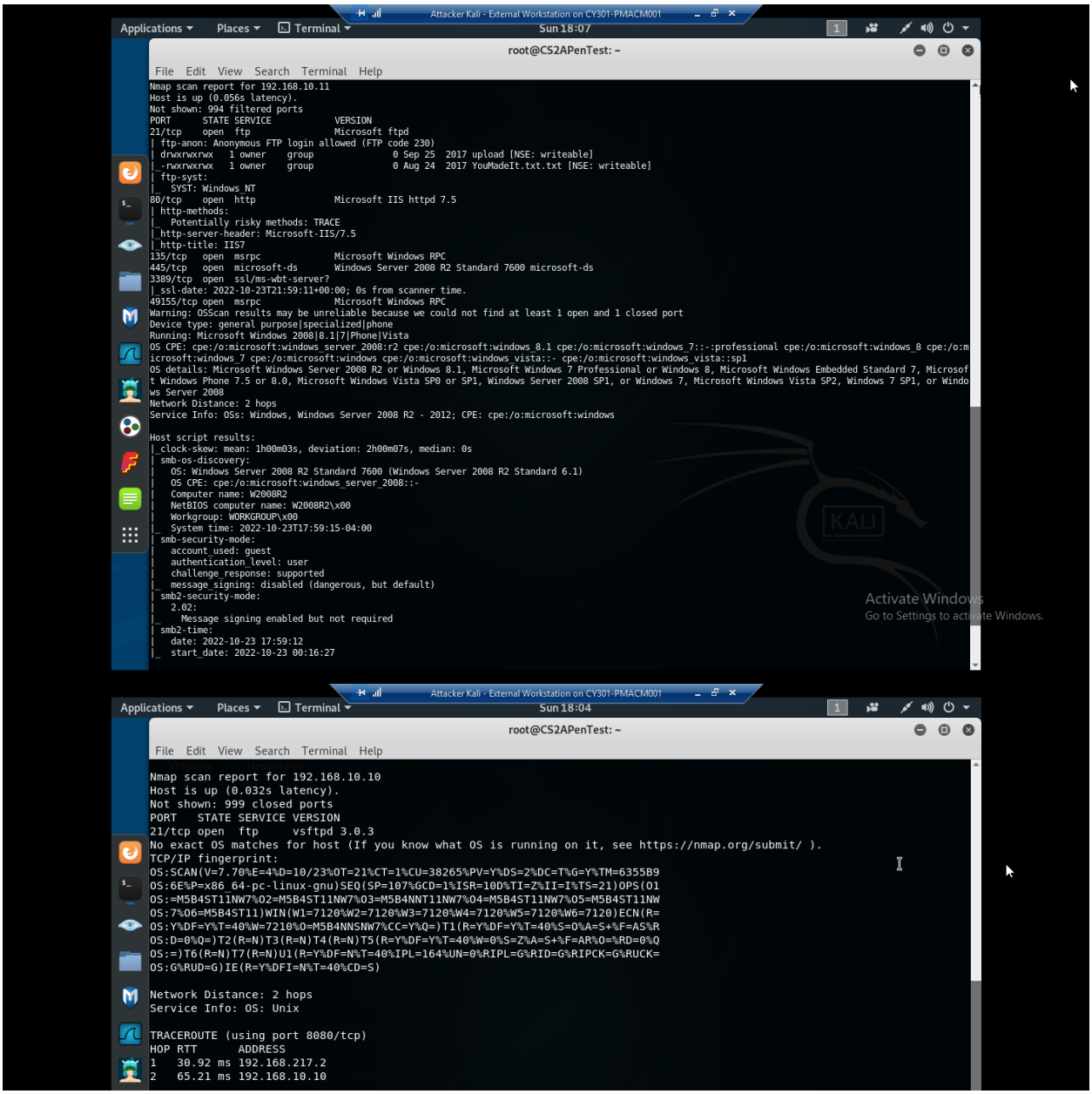
- External Kali
- pfSense
- Ubuntu
- Windows Server 2008

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

1. Run a simple scan to obtain the basic information about the subnet topology (including open ports information, operation systems, etc.)



2. Run an intensive scan to obtain detailed information about the subnet topology. Get the service and backend software information associated with each opening port in each VM.



3. 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. When running Wireshark in the Ubuntu VM, you can see the standard traffic that you would expect to see when running a ping command. You can see many TCP, DNS, ICMP, and one ARP packet that was found during the capture. For my nmap command, I also carried out a port scan so you can also see the TCP packets that are queries, replies, and acknowledging of the port scan. It scanned all of the open ports in the Ubuntu VM and listed them as packets. The TCP packets are easy to spot in the listing of the packets in Wireshark as they have been grouped together. Each query and response were grouped together in Wireshark, but you could attach a display filter to see them all individually. You can see the VMs and firewall communicating with one another to complete the network scan and list all of the packets that went across the network. The ICMP packets that were captured were ping requests and replies that made it to the network

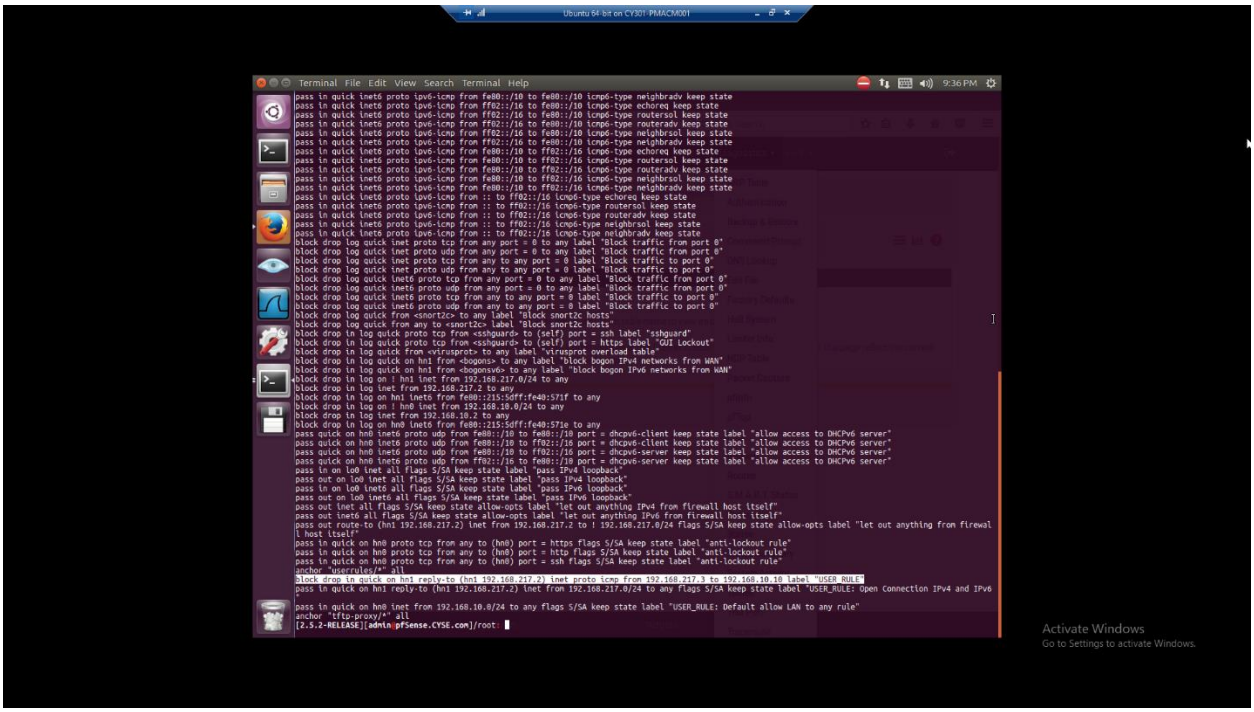
that was being scanned. The ARP packet that was captured was the VM trying to reach and communicate with its neighboring VMs.

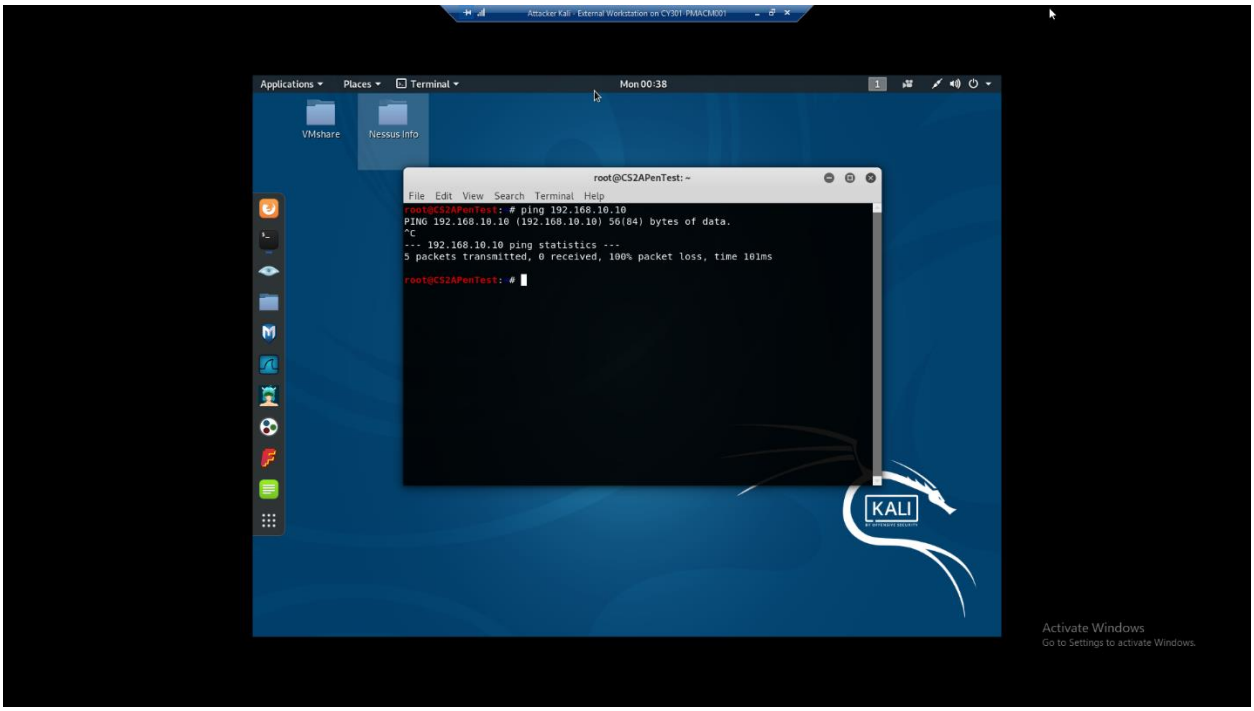
Task B: Shield – Protect your network with firewall (10 + 10+ 20 + 20 = 60 points)

In order to receive full credits, you need to fill the table (add more rows if needed), implement the policy, 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.

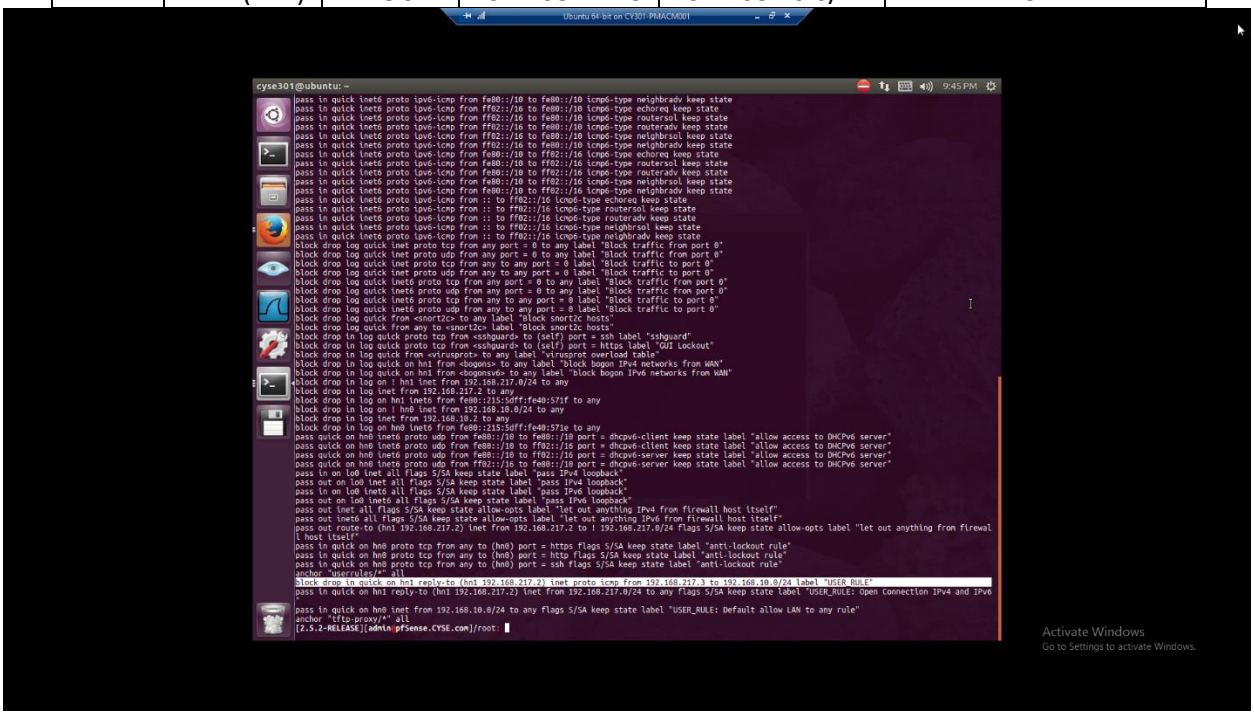
Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
1	WAN(hn1)	BLOCK	192.168.217.3	192.168.10.10	ICMP

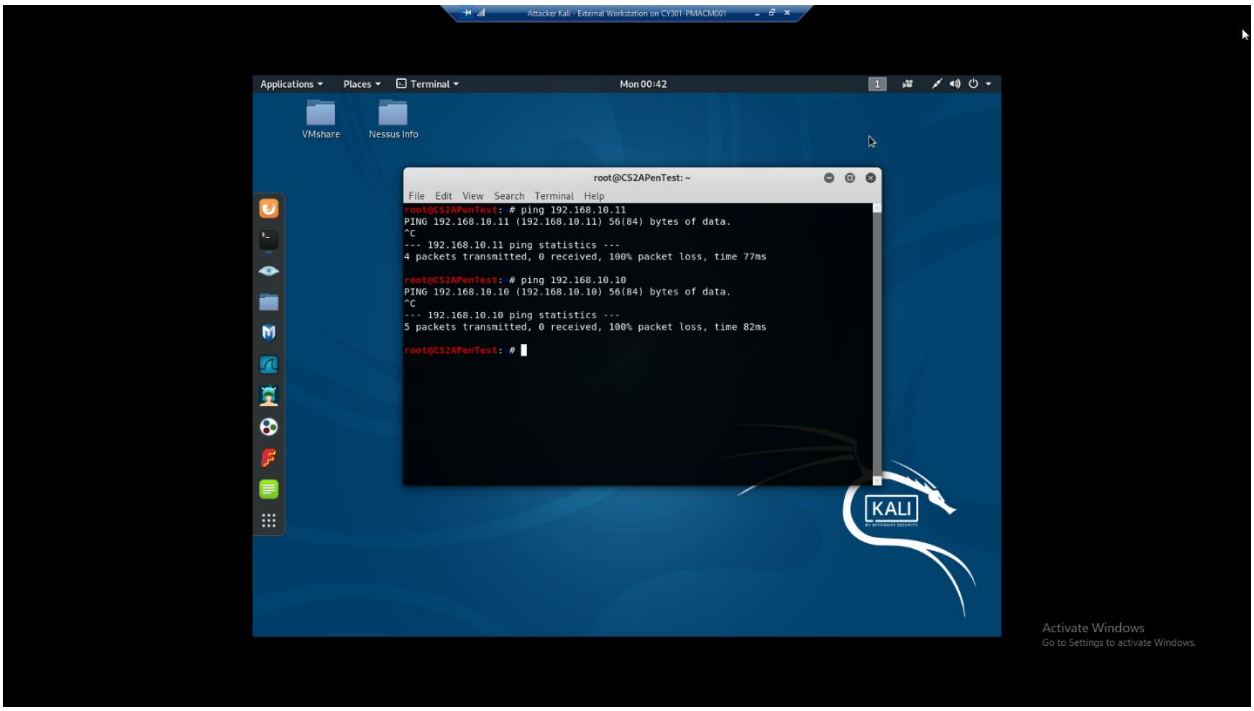




2. Clear the previous firewall policies and configure the pfSense firewall to block all ICMP traffic from External Kali to the LAN side.

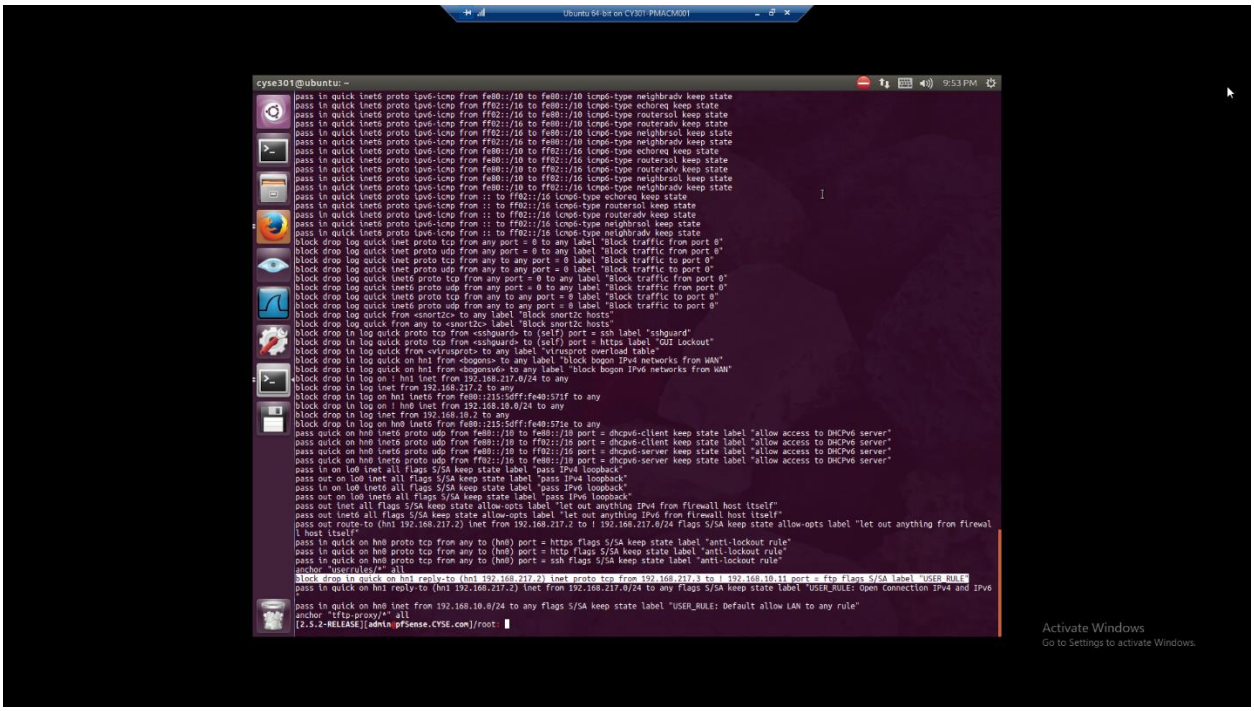
Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
2	WAN(hn1)	BLOCK	192.168.217.3	192.168.10.0/24	ICMP

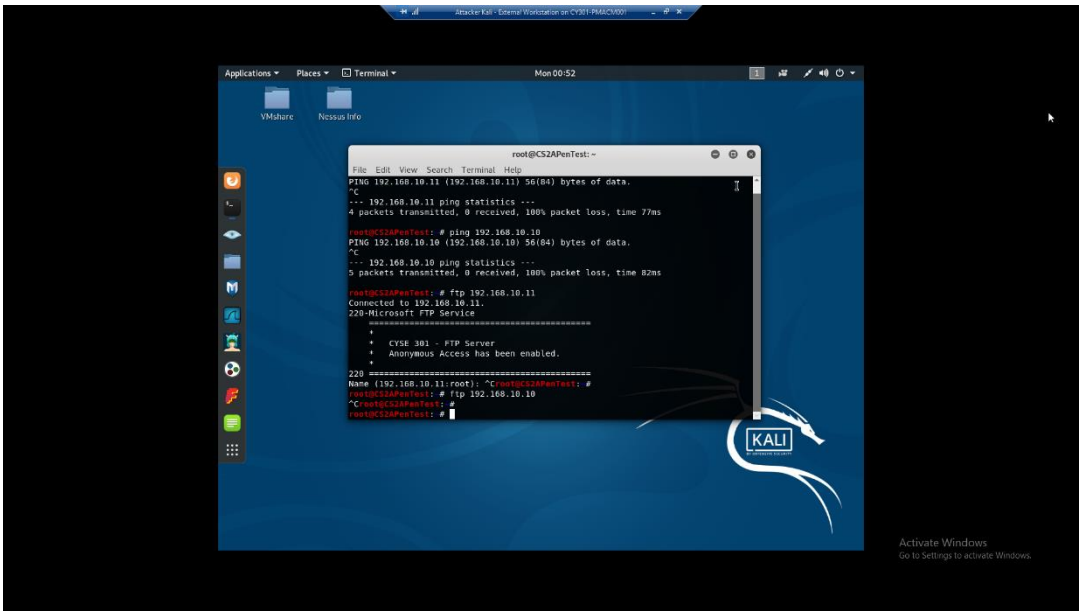




3. Clear the previous firewall policies and configure the pfSense firewall to block ALL traffic from External Kali to the LAN side, except for the FTP protocol towards Windows Server 2008.

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)	Invert Rule?
3	WAN	BLOCK	192.168.217.3	**!** 192.168.10.11	FTP (Port 21)	Yes





4. Keep the firewall policies you created in Task B.3 and repeat Task A.2. What's the difference? In this case, the nmap was successful and scanned 256 possible ip addresses but found no host that was up.

Extra credit (10 points): Use NESSUS to enumerate the security vulnerabilities of Microsoft Windows Server 2008 VM in the CCIA network.