OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

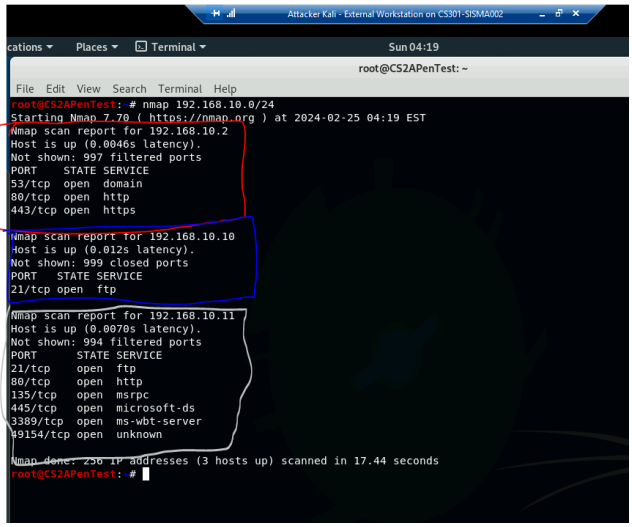
Assignment #3 Sword vs. Shield

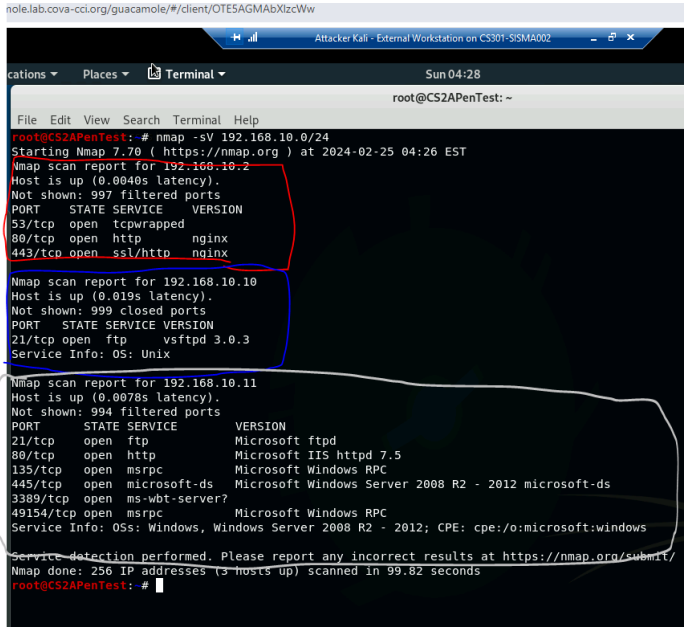
Sahmer Ismael

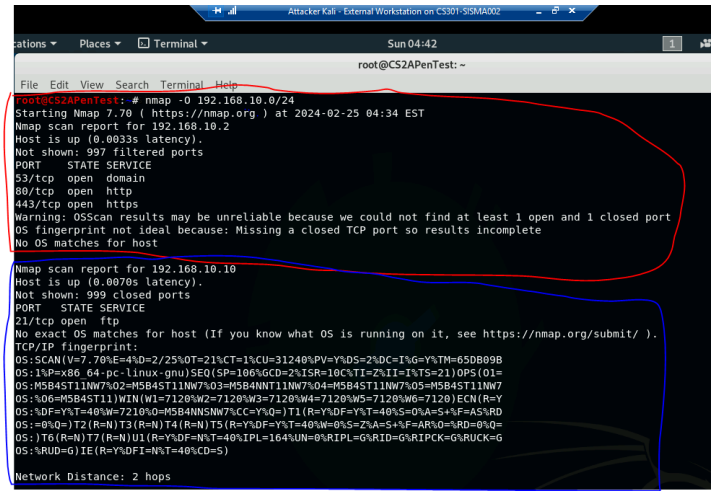
01219271

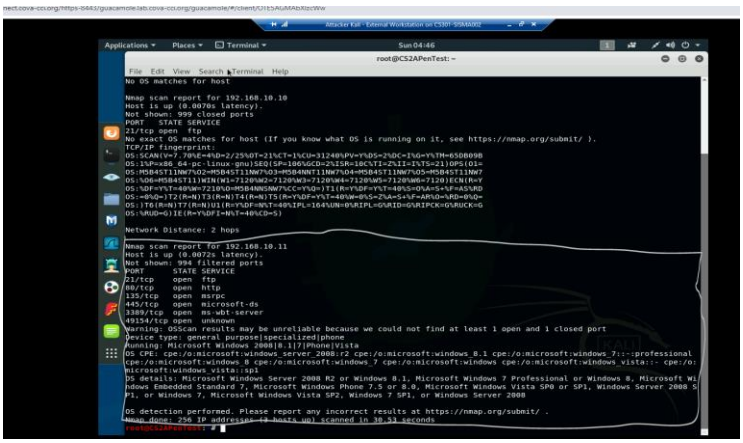
TASK A

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.









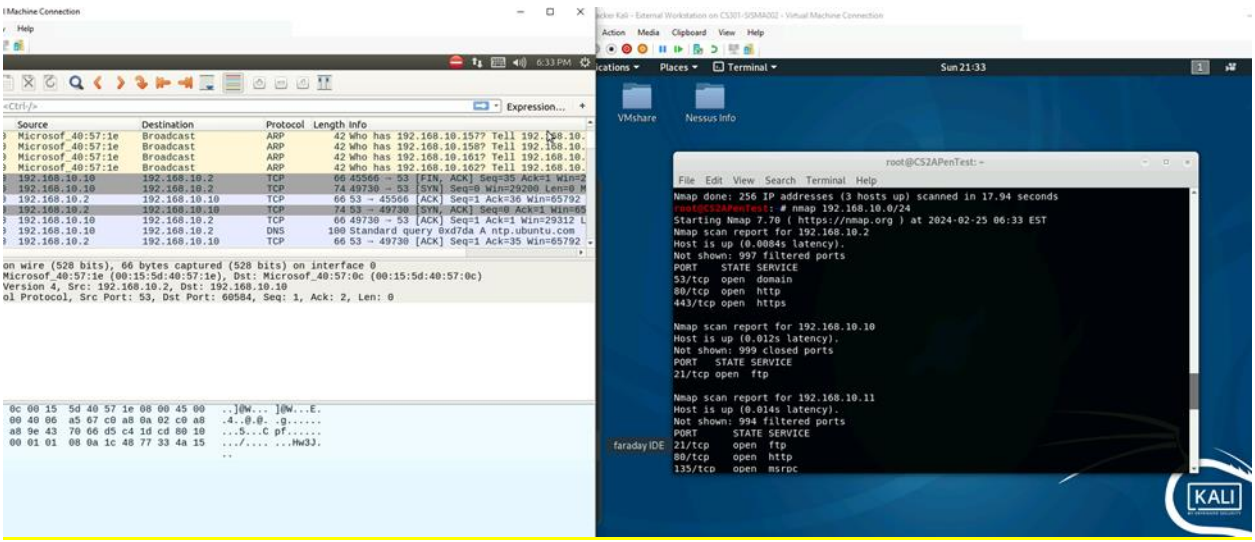
Description: Throughout using Nmap, I was able to locate the Subnet topology, such as the opens port information. The operating systems that the VMs where using, and as well as the services and the backend software's, with each opening port and each VM. Furthermore, I highlighted the different VMS data with different colors.

Red – 192.168.10.2 Pfsense

Blue - 192.168.10.10 Ubuntu

Grey – 192.168.10.11 Window Server 2008

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.

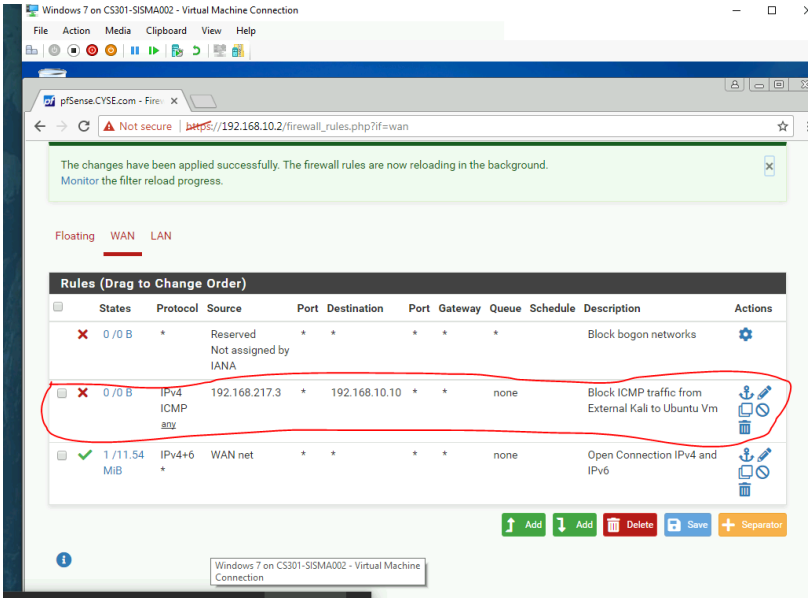


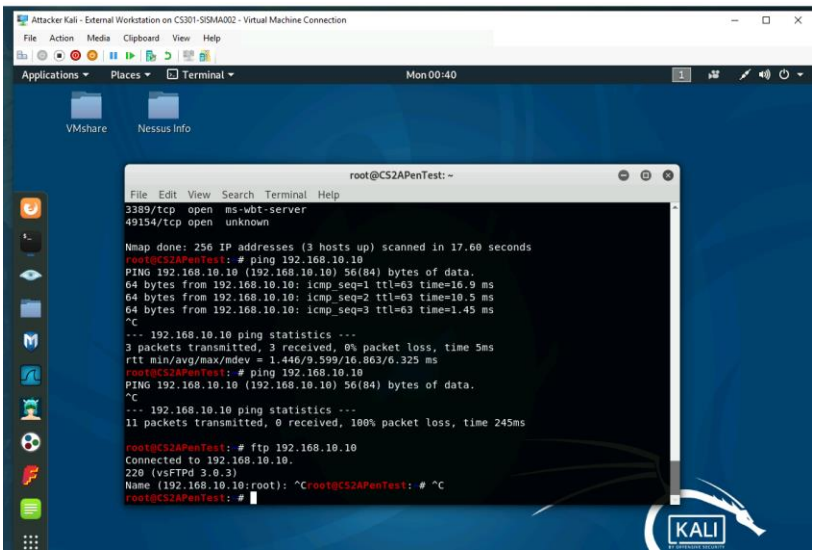
Description: From what I have gathered from the screenshot, is that after running the scan from the External Kali VM, using the command of 192.168.10.0/24 to scan the whole subnet. I was able to locate, the traffic from the Ubuntu VM, and was able to Identify that the Nmap scan was trying to communicate with different ports within the Subnet, and it was displaying a bunch of different source packets, that were running in the background of the scan. One of the protocols that the screenshot, displayed from the scan, is the ARP protocol, which is used to determine which IP addresses are in use within the local network. This message was broadcasted throughout the server, to display who has the 192.168.10.157, and to tell the designated Ip address, which was in this case, IP address 192.168.10.2, about it. Furthermore, the screenshot, displays that Nmap was completing the TCP handshake process, which it was trying to find out about the TCP ports that where in the network, to communicate with. I also examined the protocol Hierarchy statistics tool in Wireshark, and was able to identify, the different types of packets that where going, through the Wireshark tool, and the percentage of the packets being successful.

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

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	ICMP



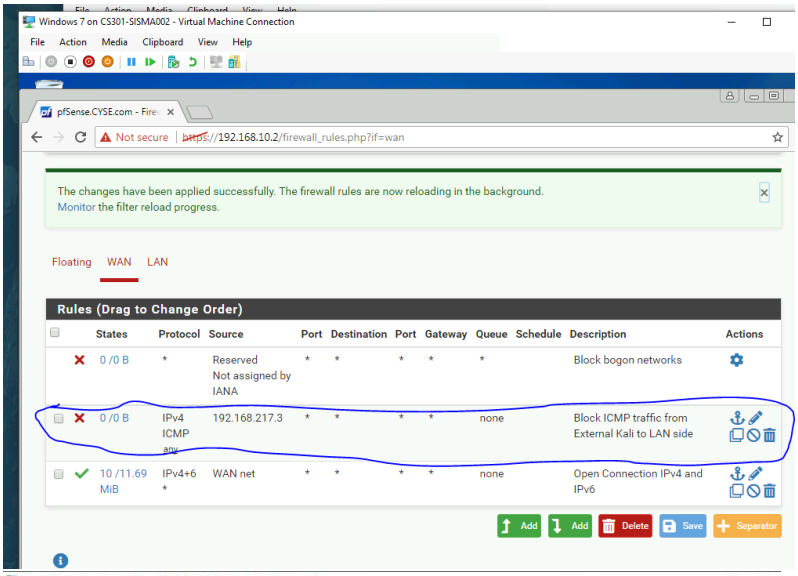


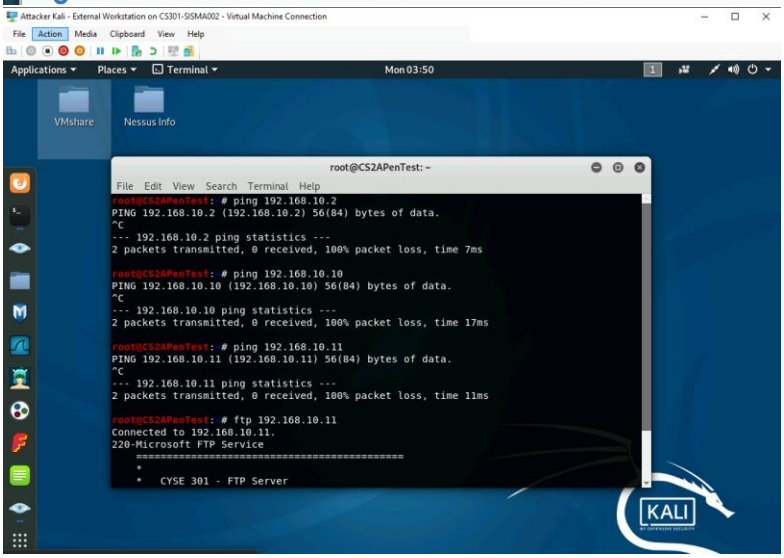
Description: from the screenshots above, I blocked the ICMP traffic, from external Kali to Ubuntu Vm. I showed, before the rule, they were connected, and then after, I showed the ICMP traffic being blocked, after the rule was set. I also accessed FTP packets, to make certain that the rule only blocked ICMP traffic.

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 Side	ICMP



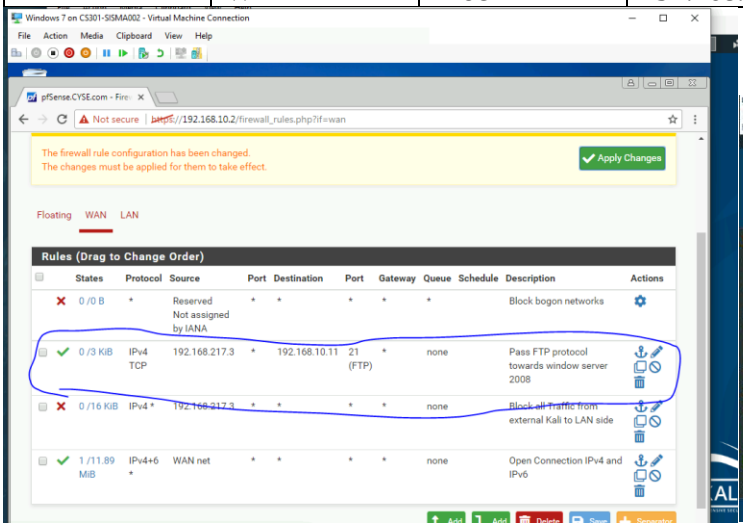


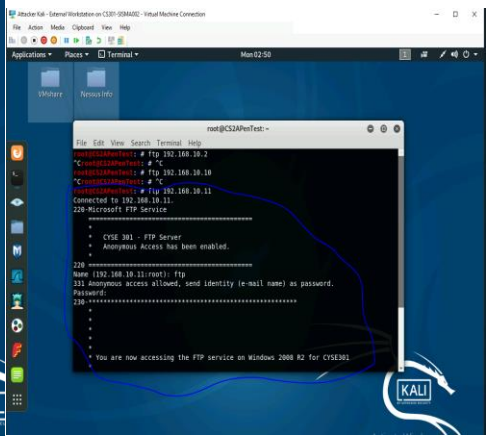
Description: I displayed, me blocking the ICMP traffic, from external Kali to the LAN side, and tested it. Furthermore I also tested the firewall rule, by using FTP, to show only ICMP was blocked.

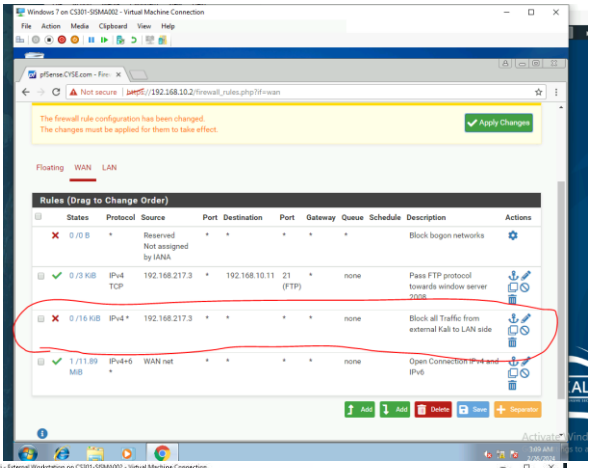
3. Clear the previous firewall policies and configure the pfSense firewall to block ALL traffic from External Kali to the LAN side, except for the FTP protocol towards Windows Server 2008.

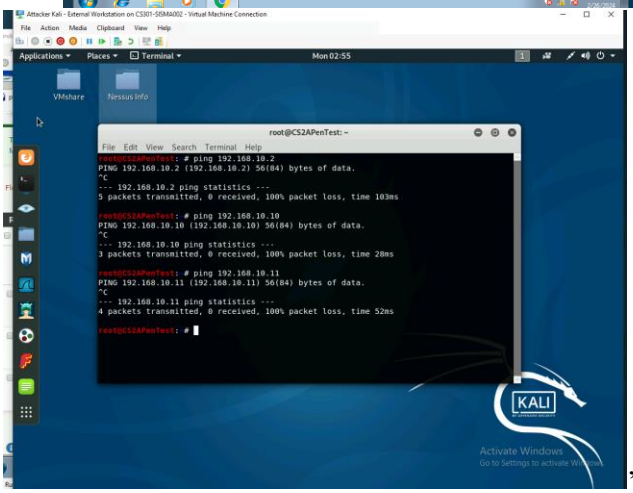
Rule#	Interface	Action	Source IP	Destination IP	Protocol
1	WAN	pass	192.168.217.3	192.168.10.11	TCP

2	WAN	Block	192.168.217.3	Any	Any



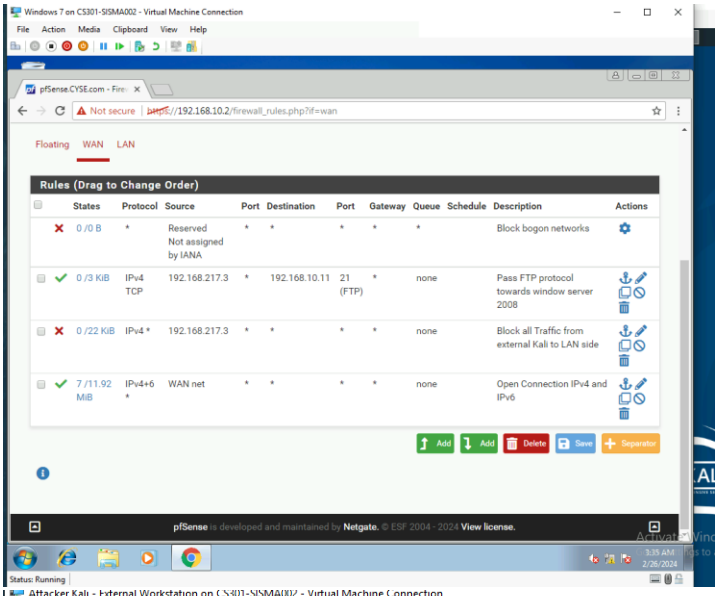


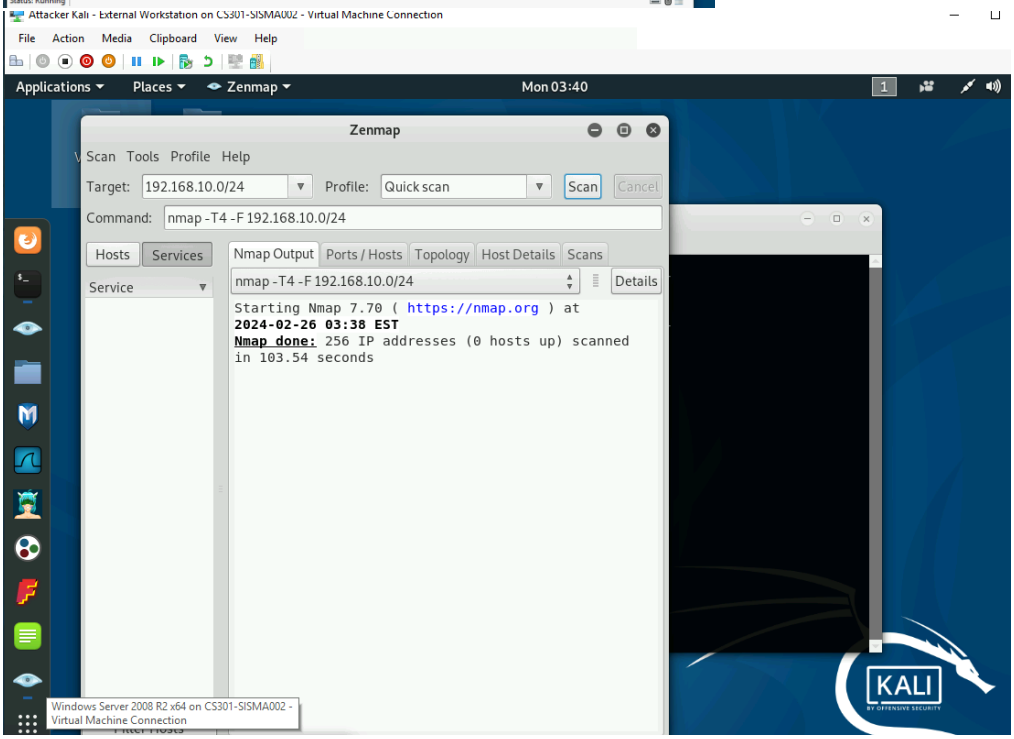




Description: The first set of screenshots, for question 3 display, FTP only passing, through the windows server 2008, and the firewall rule that was used. The second set of pictures for question 3, displays that all the VMS are completely blocked besides, the FTP on windows server.

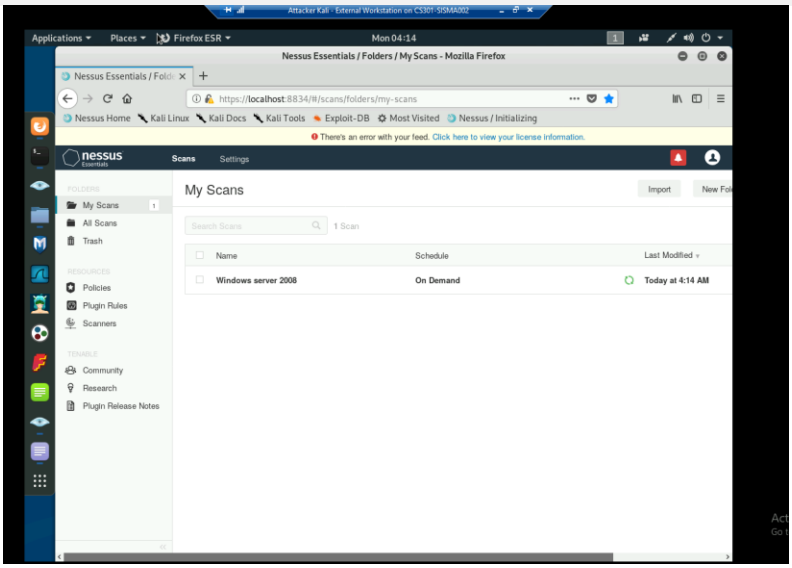
4. Keep the firewall policies you created in Task B.3 and repeat Task A.1. What's the difference?

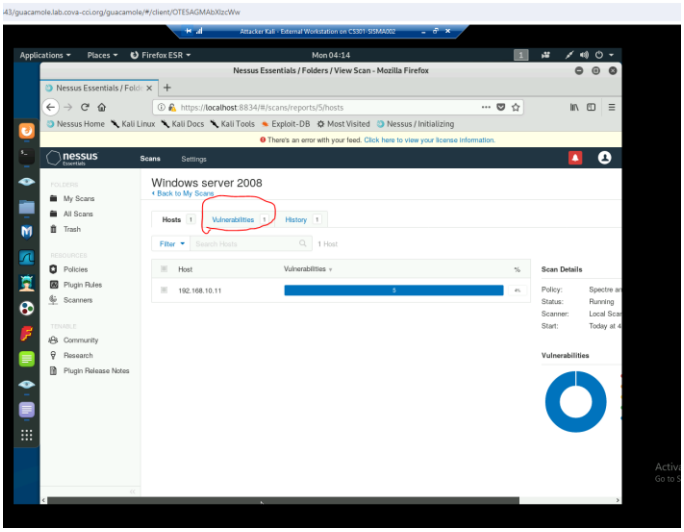




Description: After keeping the same rules on PF sense, from the previous step, and applying a quick scan to Zen map/Nmap, it seems that the subnet topology which include, the port information, operating system, and backend software where all down, due to the firewall rules blocking all traffic, and information from the kali VM.

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





Description: After going through Nessus from external Kali, I initated a scan to target windows server 2008, which I inputed the Ip address. After that, the website scanned the server, which it found 1

vulnerability in the system. I only scanned the system for a couple, mins and many vuilerabilites occurred.