Old Dominion University

CYSE 301 Cybersecurity Techniques and Operation

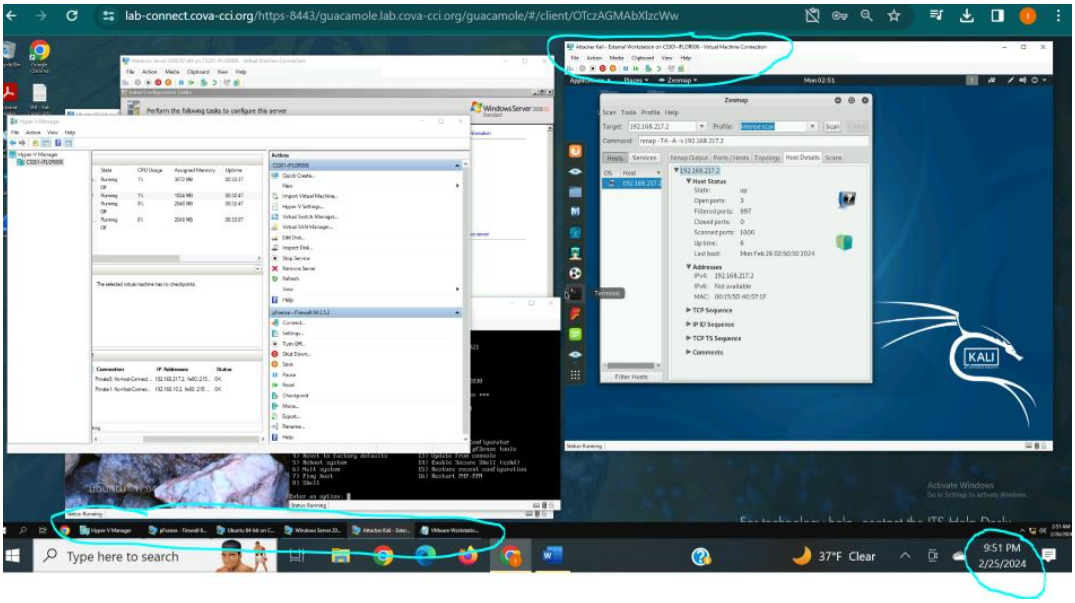
Assignment #3 Sword vs Shield

Isaac Flores

01270428

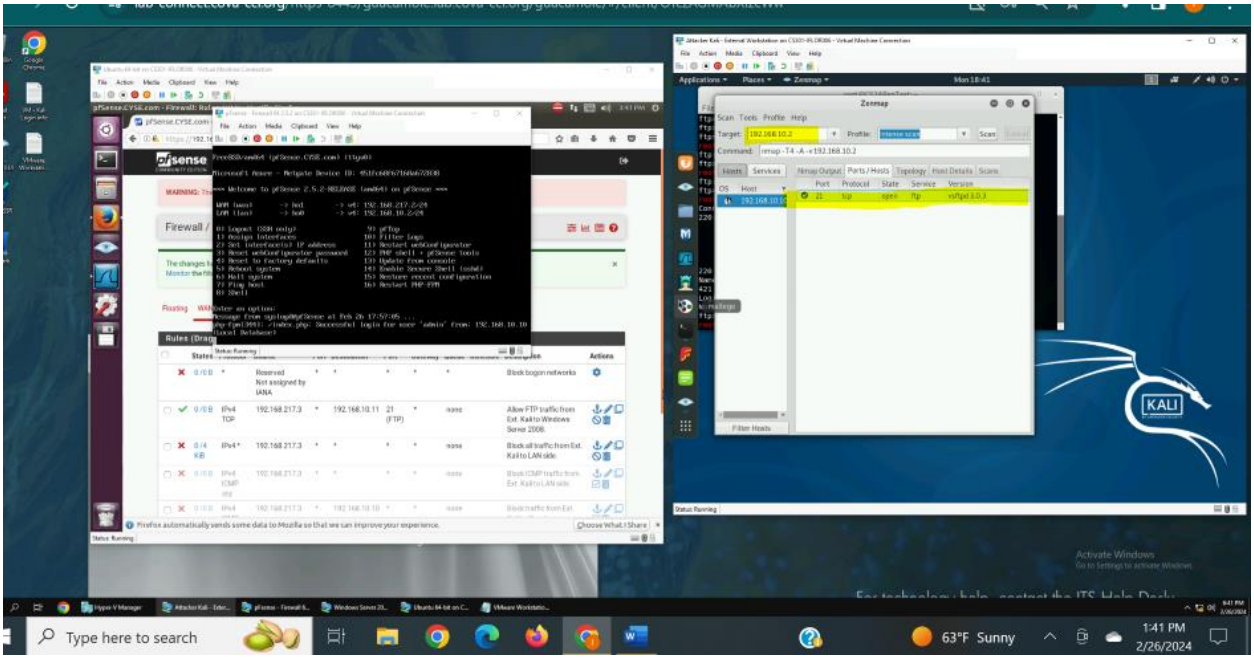
Task A: Sword – Networking Scanning

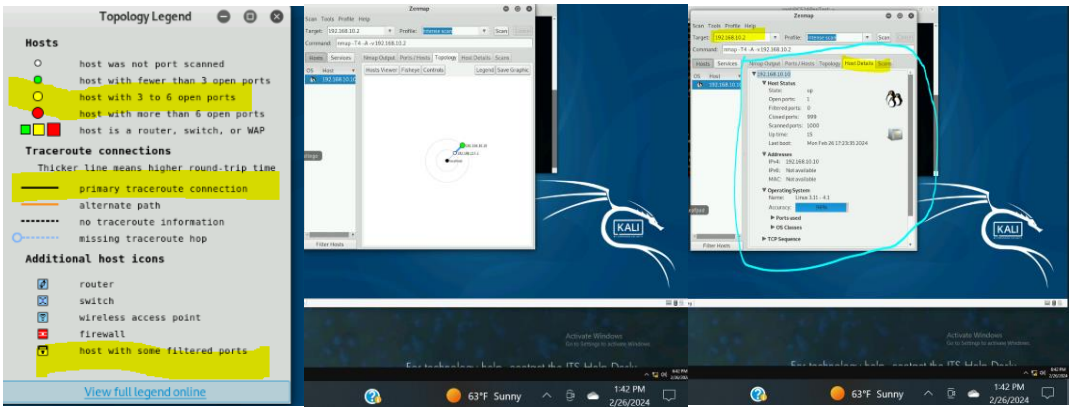
1. **Use Nmap to profile the basic information about the subnet topology (including open ports information, operation systems, etc.) You need to get the service and backend software information associated with each opening port in each VM.**



The image above shows the Attacker Kali, Windows Server 2008, pFsense, and Ubuntu as the running virtual machines. The timestamp is displayed in the bottom right corner, and the session information should be found on the session information should found in the Attacker Kali running virtual machine part of the image.

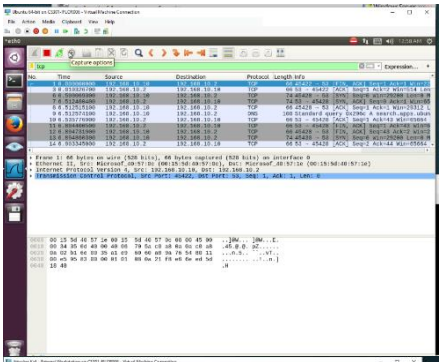
pFsense: The Zenmap scan was done by entering an Ip address in the Zenmap tool.



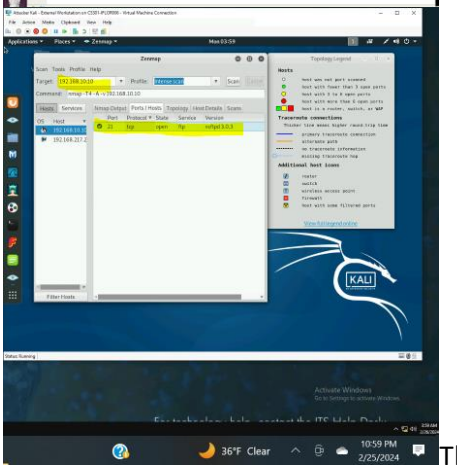


The first image should a Zenmap scan of the 192.168.10.2 Ip address for the pFsense virtual machine and the open port 21. The third image should show the topology information. The fourth image should show the Host details information about the Ip address. The images reveal that the host is up, 3 ports are open, port 433 is open, port 53 is open, and port 80 is open. Other information can be analyzed using the images such as ipv4 address, 999 closed ports, 1,000 total ports scanned, 0 filtered ports, and other information. The second and third images should show that the virtual machine has less than 3 ports open in the topology information.

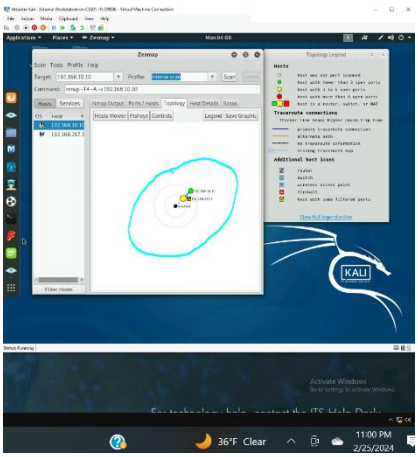
Ubuntu: The Zenmap scan was done by entering an Ip address in the Zenmap tool.



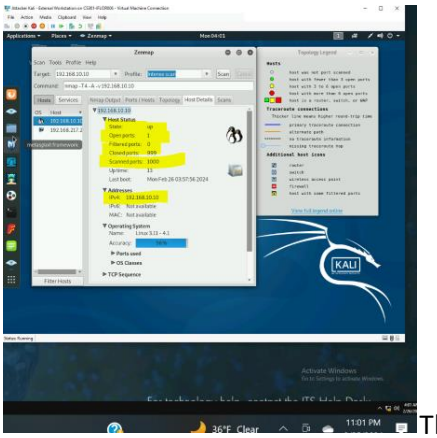
The image should show Wireshark while there is an Zenmap scan.



The second image should show that port 21 is open.

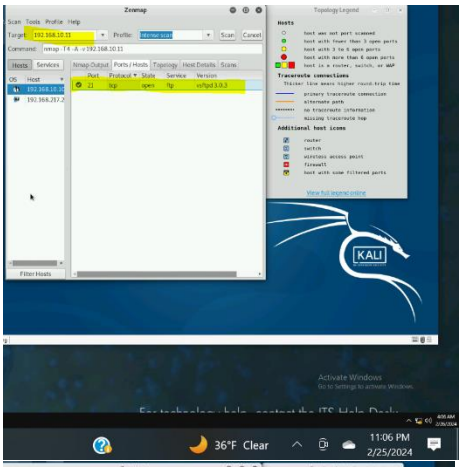


The third image should show that the virtual machine has less than 3 ports.

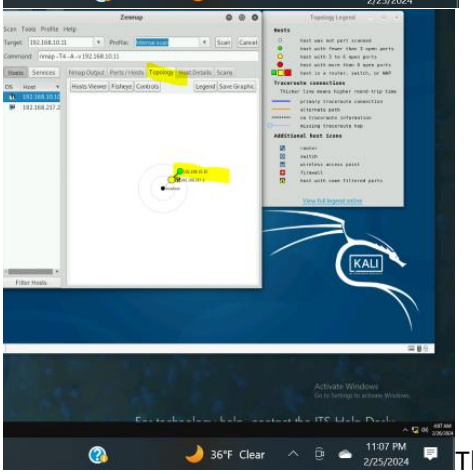


The fourth image should show that the host is up, 1 port is open, and 1000 ports were scanned.

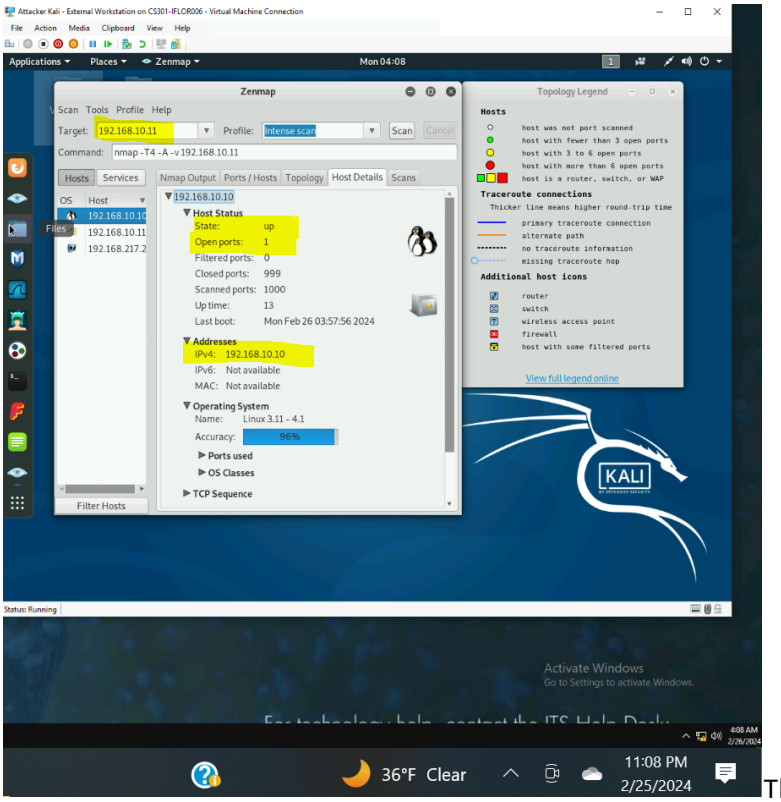
Windows Server 2008: The Zenmap scan was done by entering an Ip address in the Zenmap tool.



The image should show a Zenmap scan of the Windows Server 2008 virtual machine. Port 21 is open.



The image second image should show that virtual machine has less than 3 open ports.



The third image should show information regarding the virtual machine. The host is up, ftp port 1 is up, and the up time is 13.

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.

As the Zenmap scan was being done, I tried to observe certain patterns, unique occurrences, and packet meanings. Information such as open ports, closed ports, ports scanned, host up status, the topology configuration an information, Ip information, operating system information, up time, and accuracy was meant to be scanned using Zenmap. In this case, the target virtual machine being scanned was the Ubuntu 64-bit virtual machine on the Computer & Communications Industry Association tool interface. Wireshark was used to observe the packets sent and received.

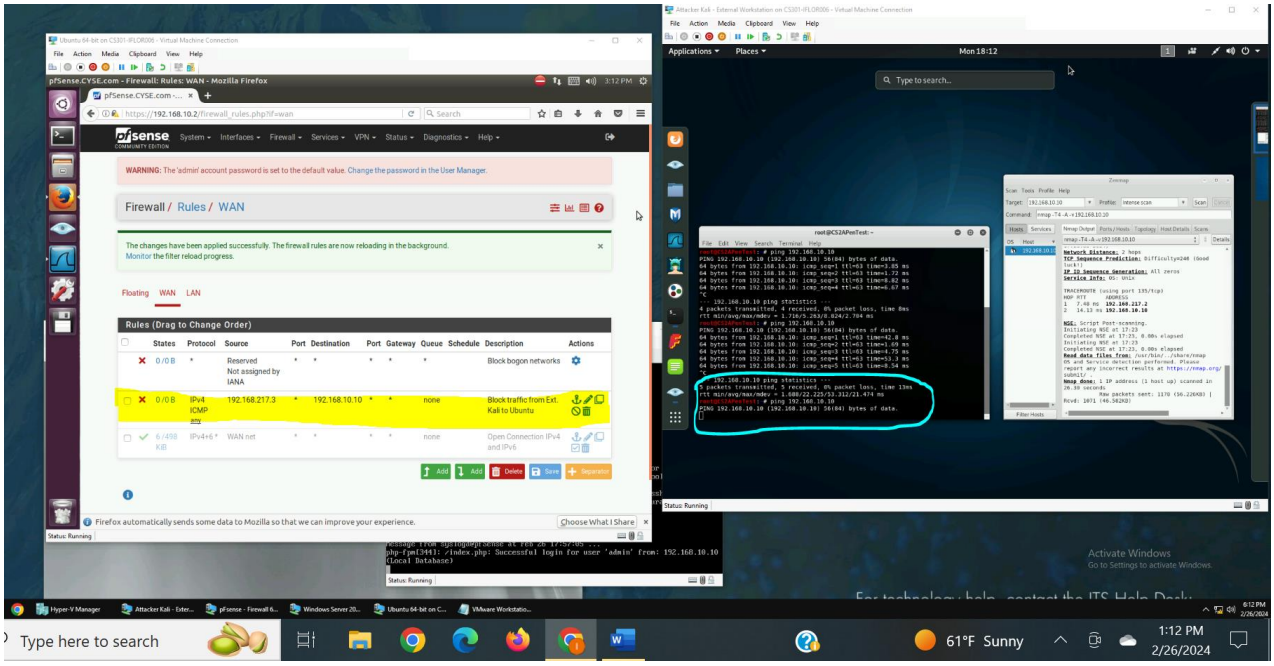
I noticed the use of trying to make a 3-way handshake. Furthermore, the protocol being used was transmission control protocol. Furthermore, the use of the Internet Control Message Protocol was used to ping the Ubuntu virtual machine and was successful as a ping request as received by the target machine, and a reply was sent back to the scanning machine. In addition, requests for Transport Layer Security were made by the attacking machine to the target machine. I also found it interesting that a request for statistics was made by the attacking machine.

I find it interesting that Zenmap provides so much information about port scanning. However, I have now learned of Wireshark's usefulness in providing more detail-oriented information about packets sent and received.

Task B: Shield – Protect your network with firewall

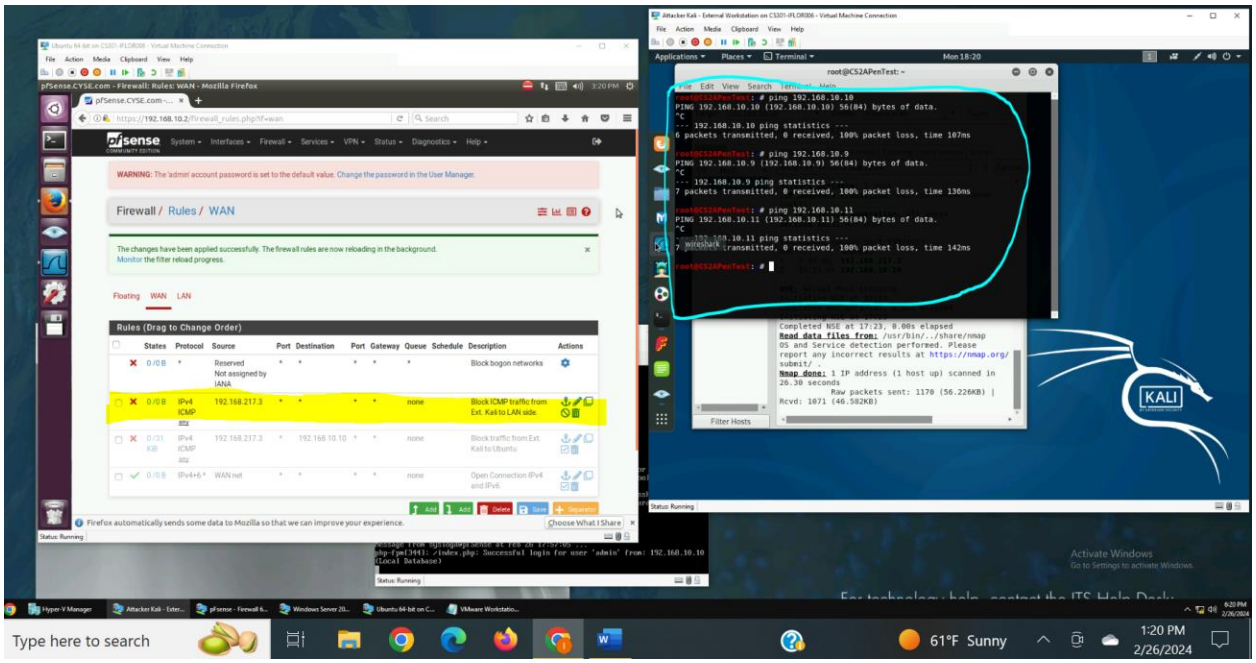
1. Configure the pfSense firewall rule to block the ICMP traffic from External Kali to Ubuntu VM.

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
Inbound	WAN	Block	192.192.217.3	192.168.10.10	



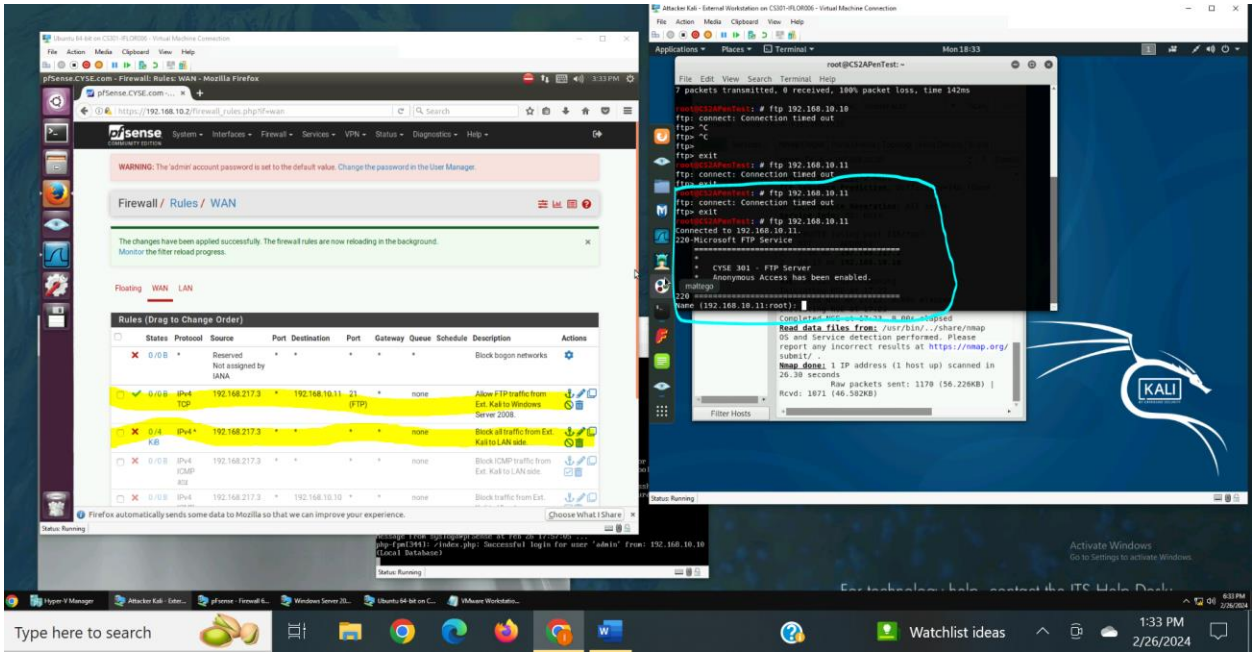
2. Clear the previous firewall policies and configure the pfSense firewall to block all ICMP traffic from External Kali to the LAN side.

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
Inbound	Wan	Block	192.168.217.3	any	



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)
Inbound	Wan	Block	192.168.217.3	all	
Inbound	Wan	Pass	192.168.217.3	192.168.10.11	21



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

The rule in task B.3 allowed only a specific protocol to be allowed from one virtual machine to another. Task A.1 is different as it uses Nmap to scan ports on virtual machines.