

OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #3 Sword vs. Shield

Niko Florido

01227364

TASK A

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.

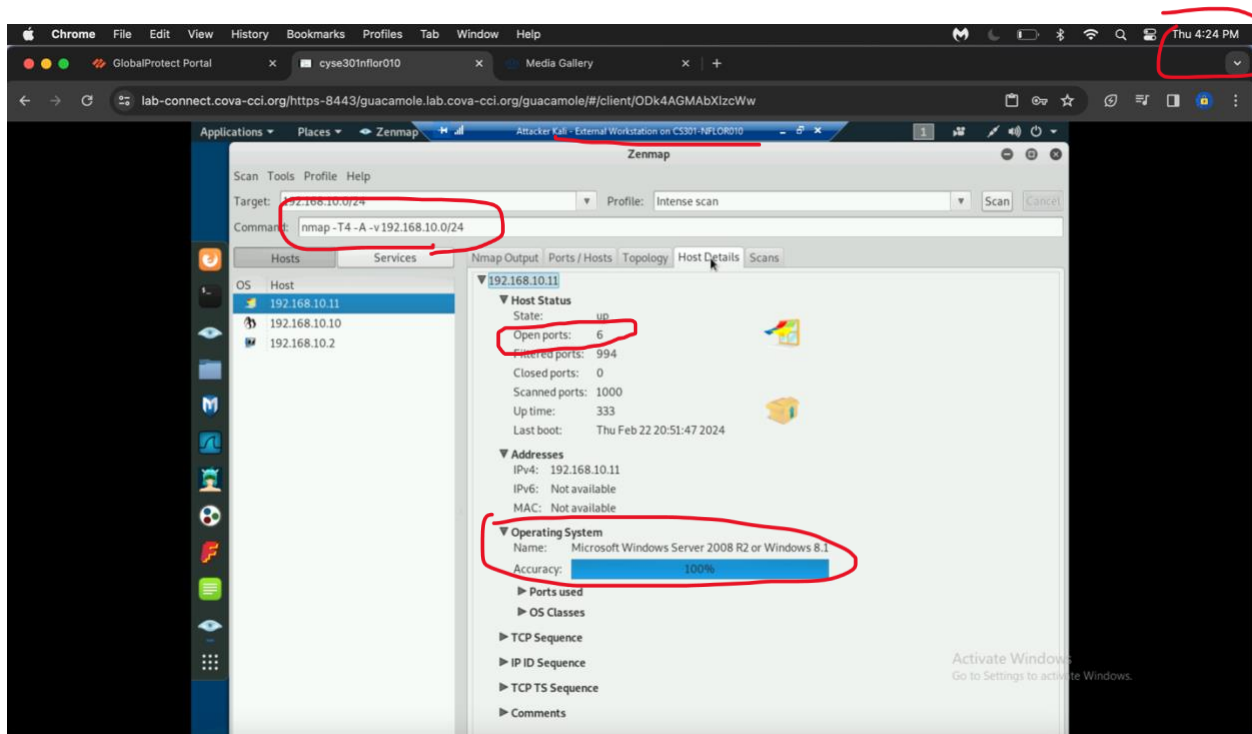
Task A: Sword - Network Scanning (20+ 20 = 40 points)

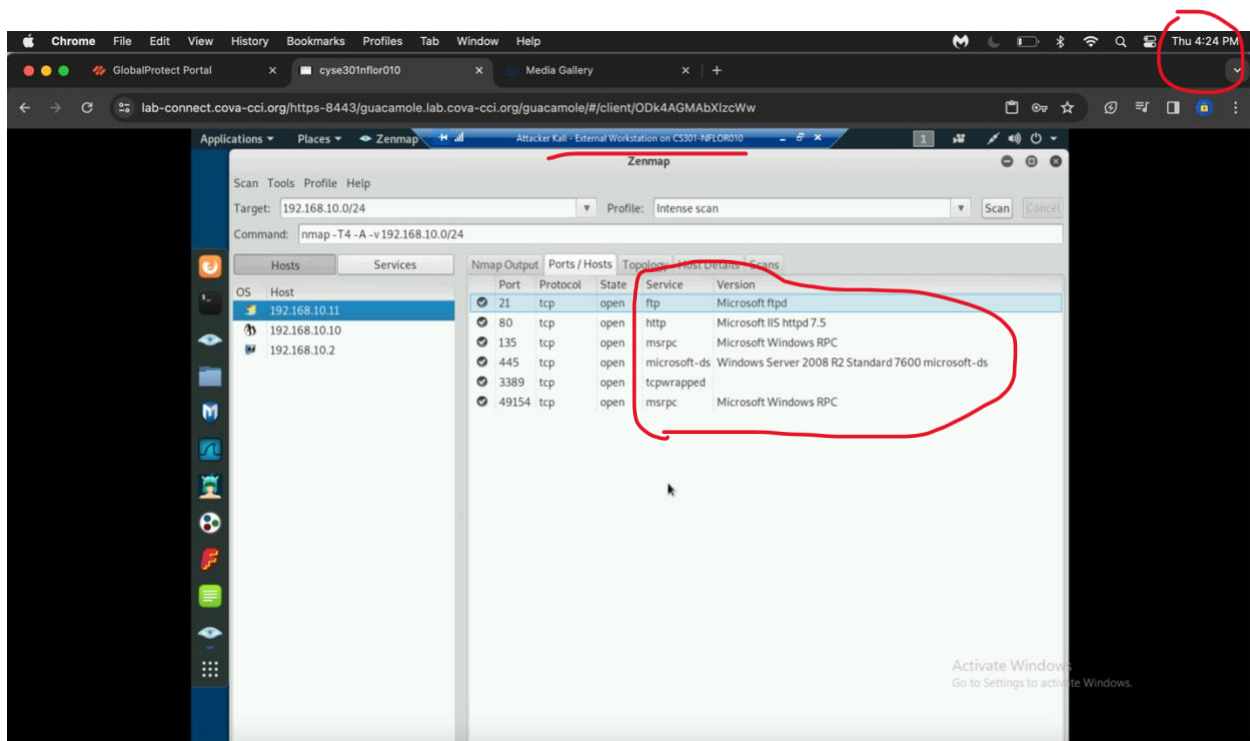
Power on the listed VMs and complete the following steps from the **External Kali** (you can use either nmap or zenmap to complete the assignment)

- External Kali (192.168.217.3)
- pfSense (192.156.10.2)
- Ubuntu (192.168.10.10)
- Windows Server 2008 (192.168.10.11)

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.



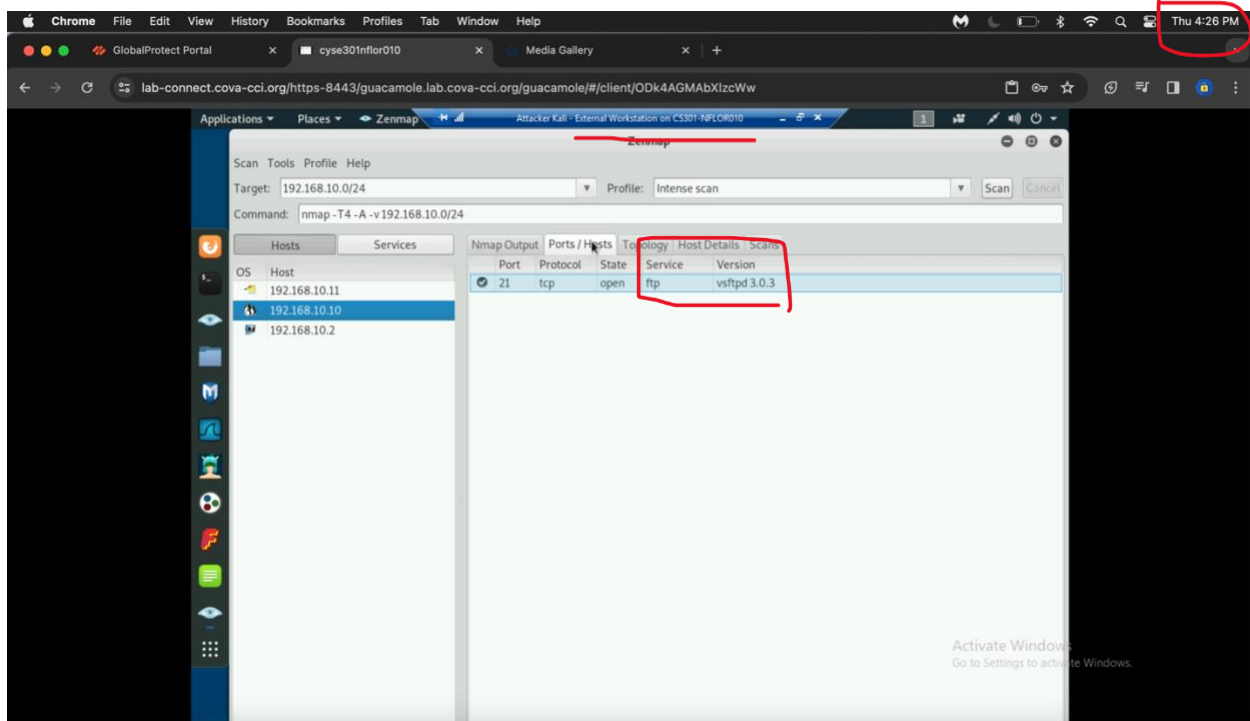
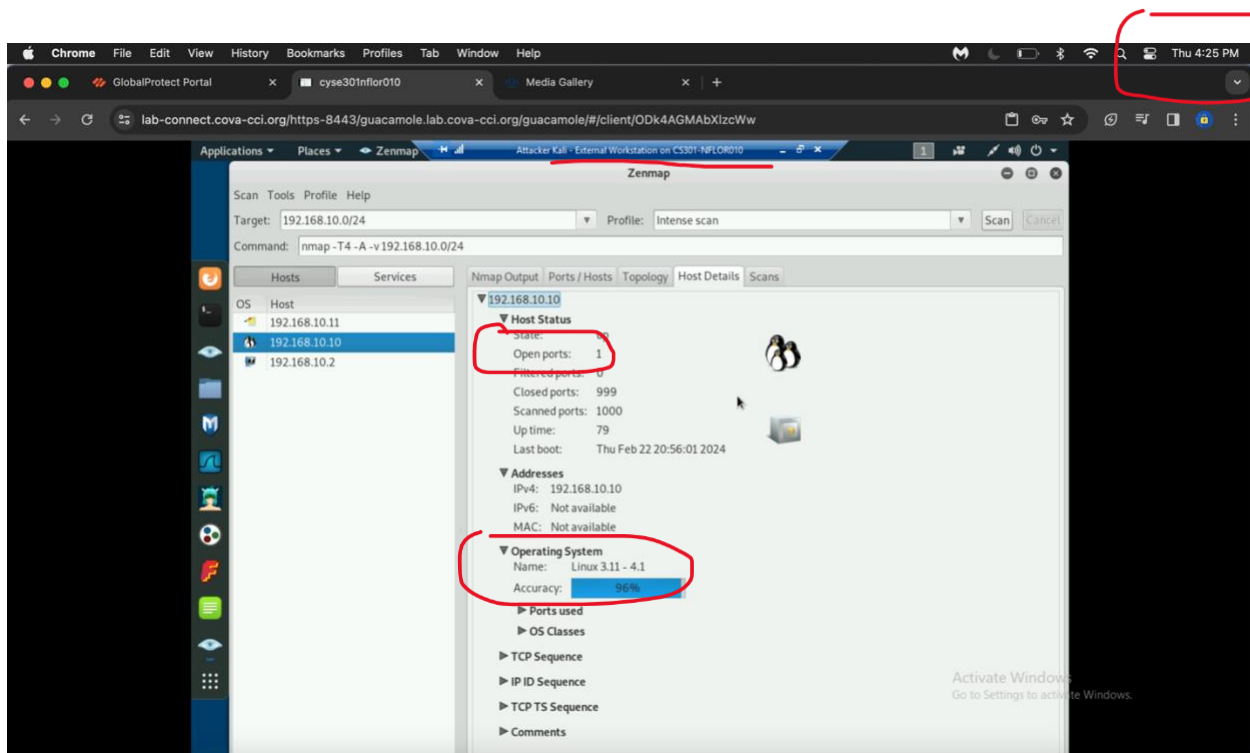


I powered on External Kali, pfSense, Ubuntu, and Windows Server 2008. I opened up External Kali and used Zenmap to gather basic information about the subnet topology. I used the command, “nmap -T4-A-v192.168.10.0/24”

The `-T4` option sets the timing to aggressive. `-A`: This is an option that enables aggressive detection. It enables OS detection, version detection, script scanning, and traceroute. `-v`: This is an option that enables verbose output. `192.168.10.0/24`: `nmap` to scan all IP addresses in the range `192.168.10.0` to `192.168.10.255`. The `/24` indicates that it should scan all addresses in the subnet, using CIDR notation.

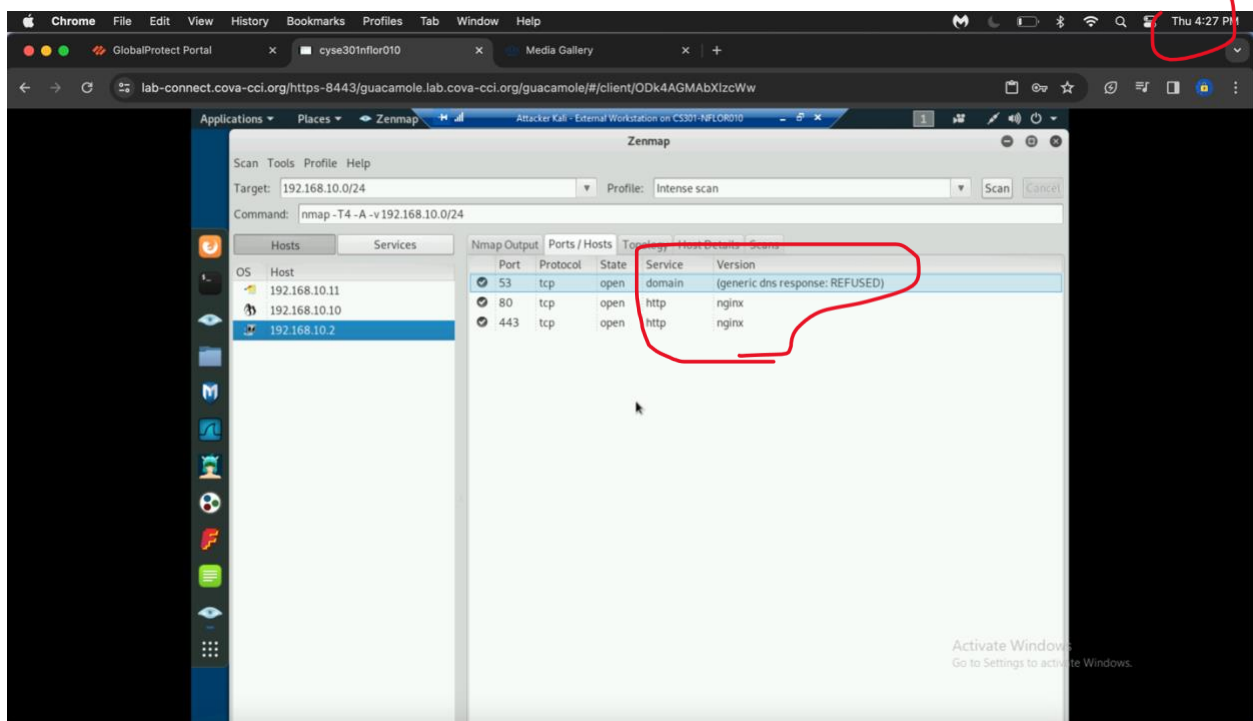
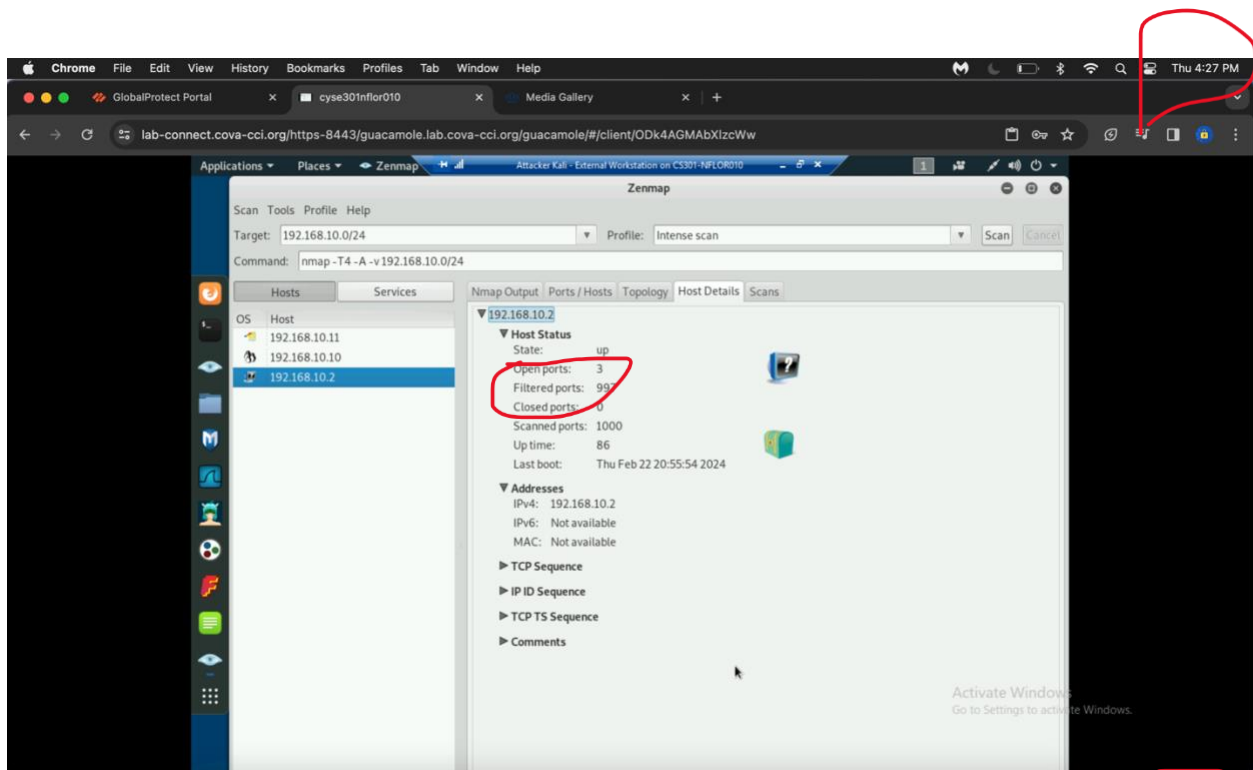
From the first screenshot, you can see the number of open ports and the operating system. The number of open ports is 6, and the operating system is Windows.

From the second screenshot, you can see the service and backend software information associated with each opening port in Windows Server 2008. The services include ftp, http, msrpc, Microsoft-ds, and tcpwrapped. The backend software is showed above.



From the third screenshot, you can see the number of open ports and the operating system. The number of ports is 1 and the operating system is Linux 3.11-4.1

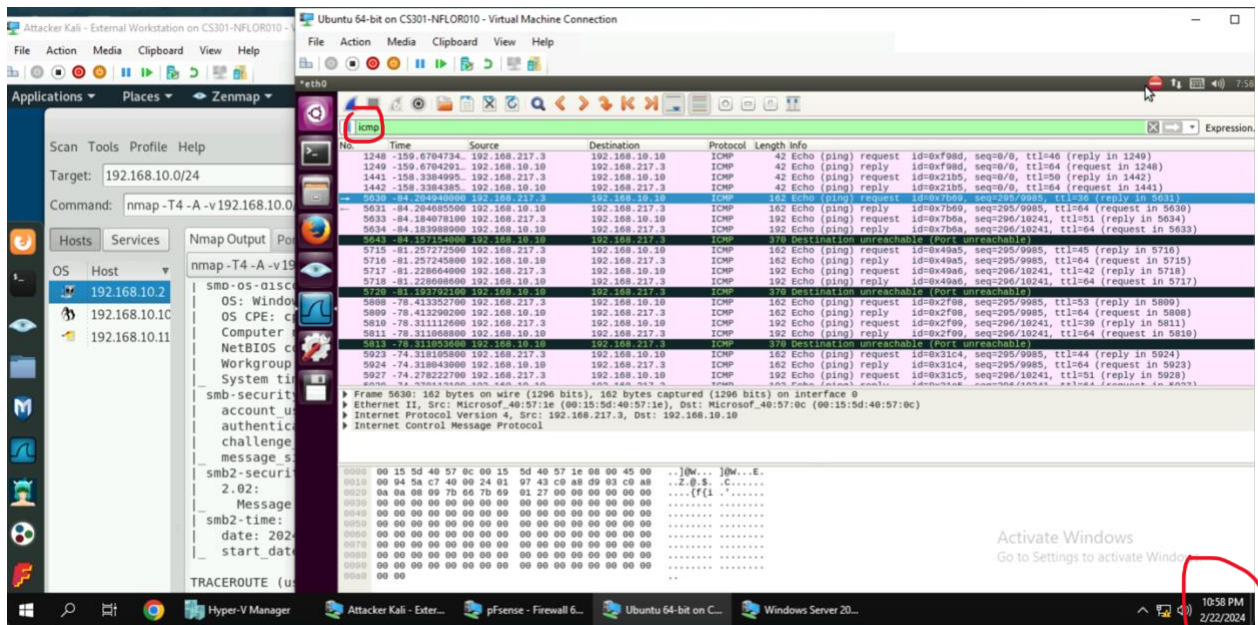
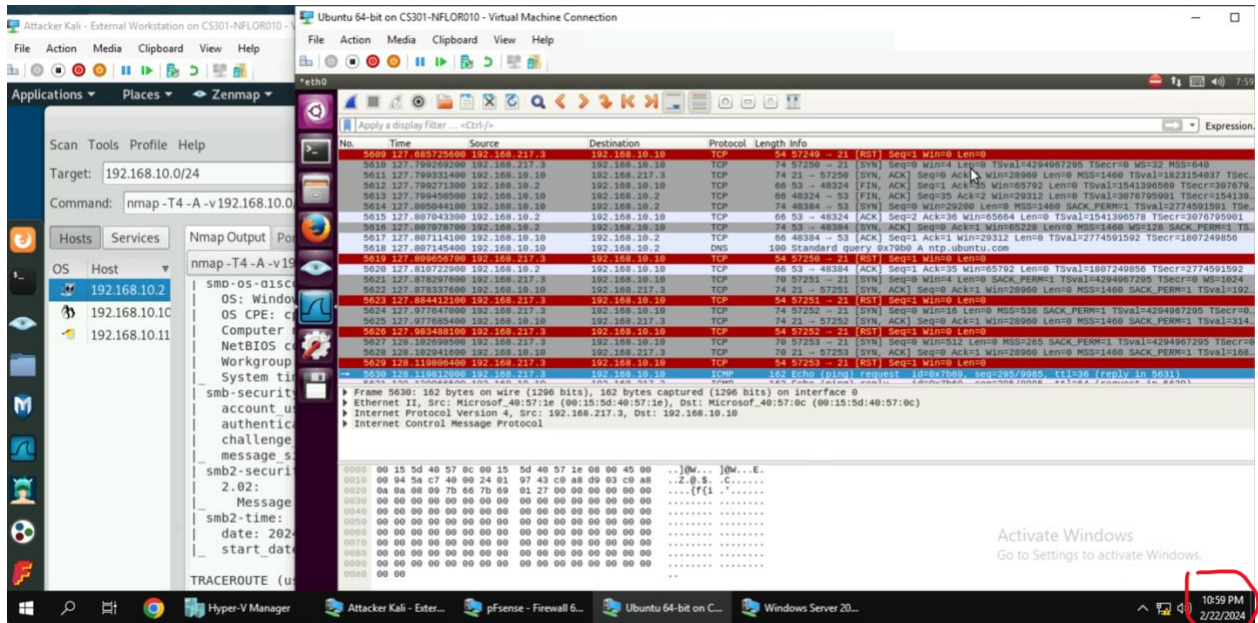
From the fourth screenshot, you can see the service and backend software information associated with each opening port in Ubuntu. The service is ftp and the backend software is vsftpd 3.0.3



From the fifth screenshot, you can see the number of open ports and the operating system. The number of open ports is 3 and the operating system is not listed.

From the sixth screenshot, you can see the service and backend software information associated with each opening port in pfSense. The services are domain and http. The backend software is nginx.

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.



So, I provided two images to show. Firstly, while I started my initial Nmap scan on External Kali, I changed my VM to Ubuntu to run Wireshark. I immediately noticed the huge amounts of packets I was receiving at a short time. I let wire shark run for about 30 seconds, and at the very end, I received almost 6000 packets. There are three-way handshake connections when you run Nmap, and it shows on Wireshark. The red highlighted packets on Wireshark are the Nmap connections. As you can see from the screenshots above, a TCP segment with the SYN (synchronize) flag set to External Kali. Upon receiving the SYN segment, Windows Server 2008 responds with a TCP segment that has both the SYN and ACK (acknowledge) flags set. Finally, the client, External Kali, responds to the Windows Server 2008's SYN-ACK segment by sending a TCP segment with the ACK flag set. At this point, the TCP connection is established. For the second screenshot, I applied an ICMP display filter to show all of the ICMP packets. ICMP can be utilized to troubleshoot TCP/IP and for managing network flow and function. As you can see from the source and destination IP's, External Kali and Ubuntu are the hosts that are communicating with each other.

TASK B

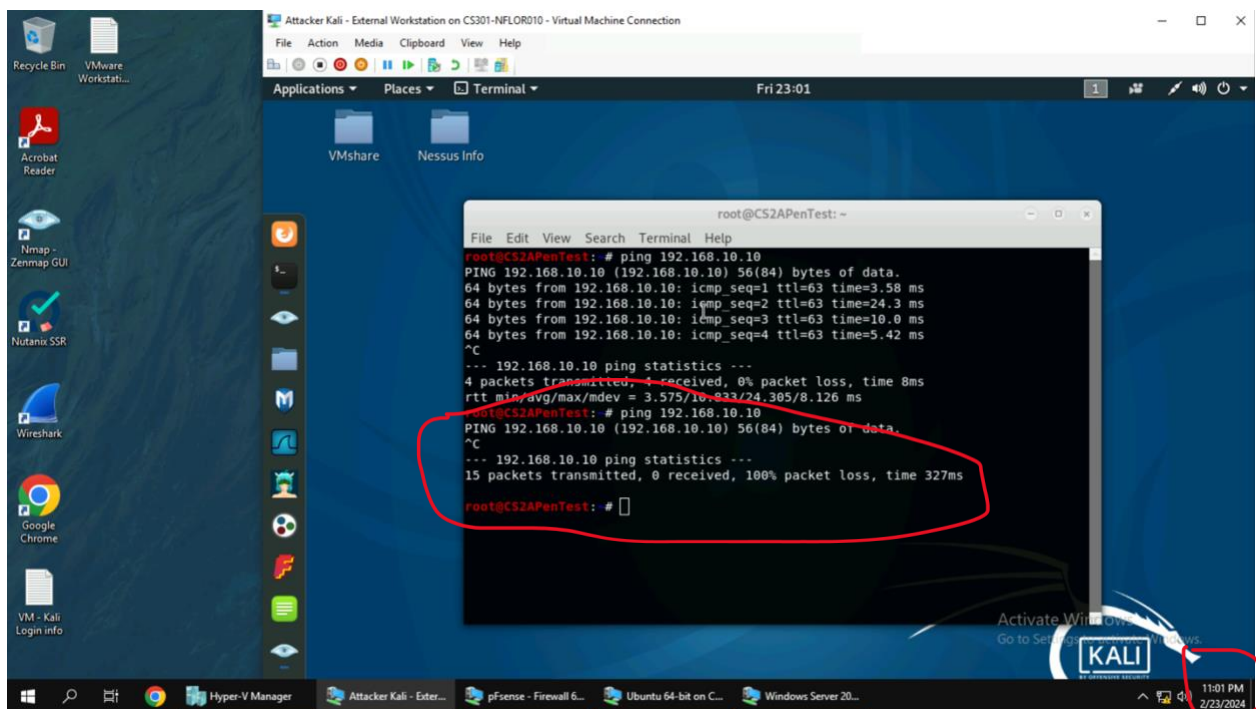
Task B: Shield – Protect your network with firewall (10 + 10+ 20 + 20 = 60 points)

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 applicable)	Direction
1	WAN	Block	192.168.217.3	192.168.10.10	ICMP	Inbound

Rules (Drag to Change Order)											
☐	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☒	0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
☐	☒ 0/0 B	IPv4 ICMP any	192.168.217.3	*	192.168.10.10	*	*	none		icmp block from external kali to ubuntu	
☐	☒ 1/10.26 MiB	IPv4+6 *	WAN net	*	*	*	*	none		Open Connection IPv4 and IPv6	

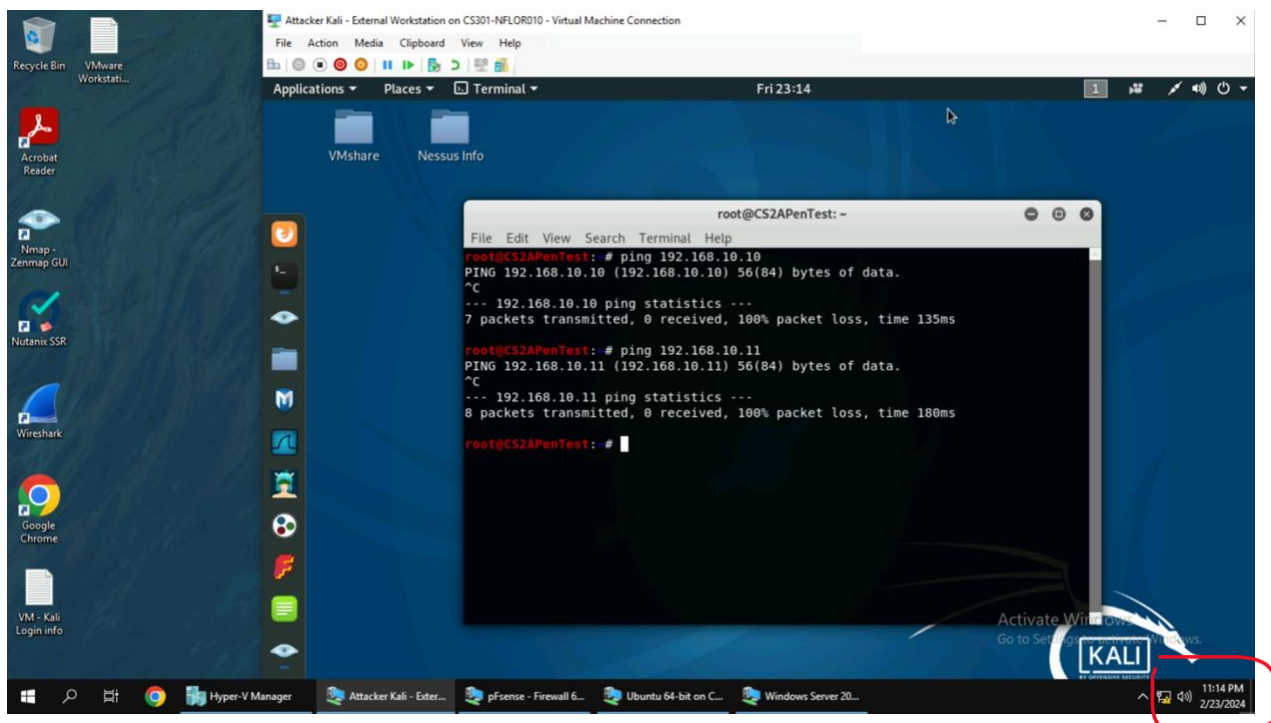


ICMP traffic is blocked from External Kali to Ubuntu. I used to ping command to verify. Zero packets were received.

- 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 applicable)
1	WAN	Block	192.168.217.3	ALL (*)	ICMP

Rules (Drag to Change Order)											
☐	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☒	0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
☒	0/0 B	IPv4 ICMP any	192.168.217.3	*	192.168.10.10	*	*	none		icmp block from external kali to ubuntu	
☒	0/0 B	IPv4 ICMP any	192.168.217.3	*	LAN net	*	*	none		icmp block from external kali to the lan side	
☒	1/10.31 MiB	IPv4+6 *	WAN net	*	*	*	*	none		Open Connection IPv4 and IPv6	

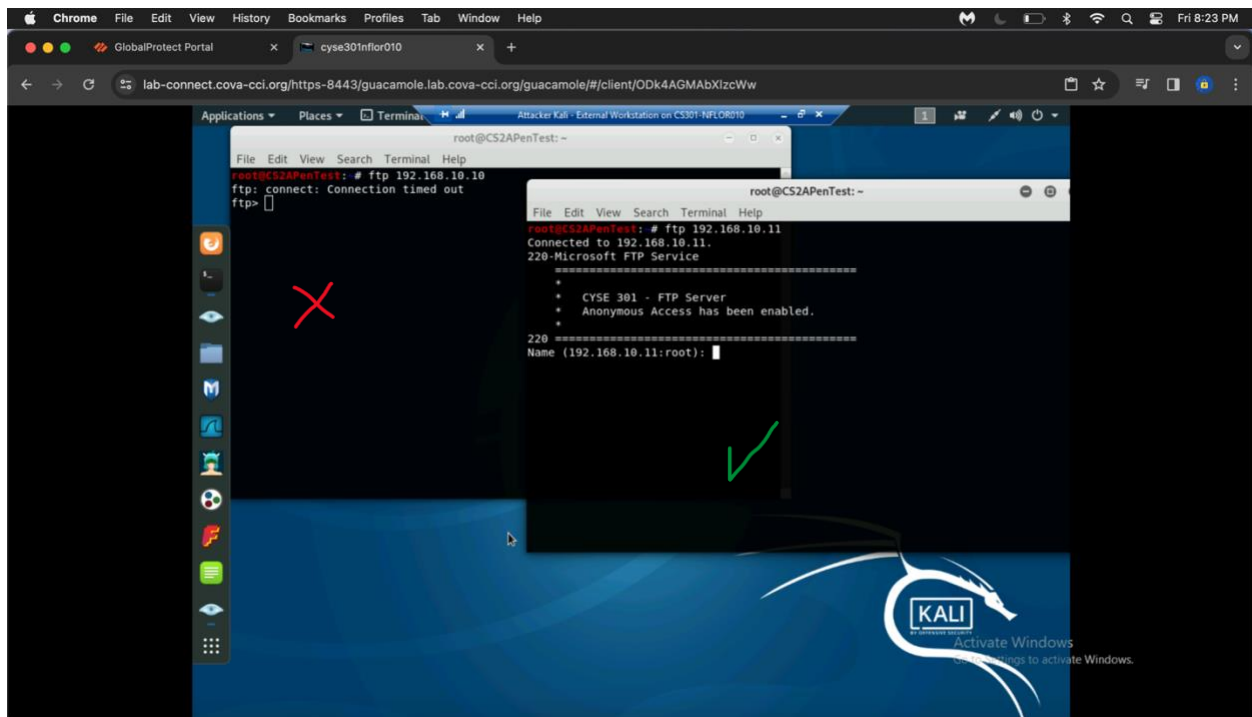


I blocked all ICMP traffic from external Kali to every host in the LAN. This type of direction is inbound because an outside source is trying to penetrate inside a network. As you can see from the terminal above, both Ubuntu and Windows Server 2008 are not receiving traffic.

- 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 applicable)
1	WAN	PASS	192.168.217.3	192.168.10.11	ALL

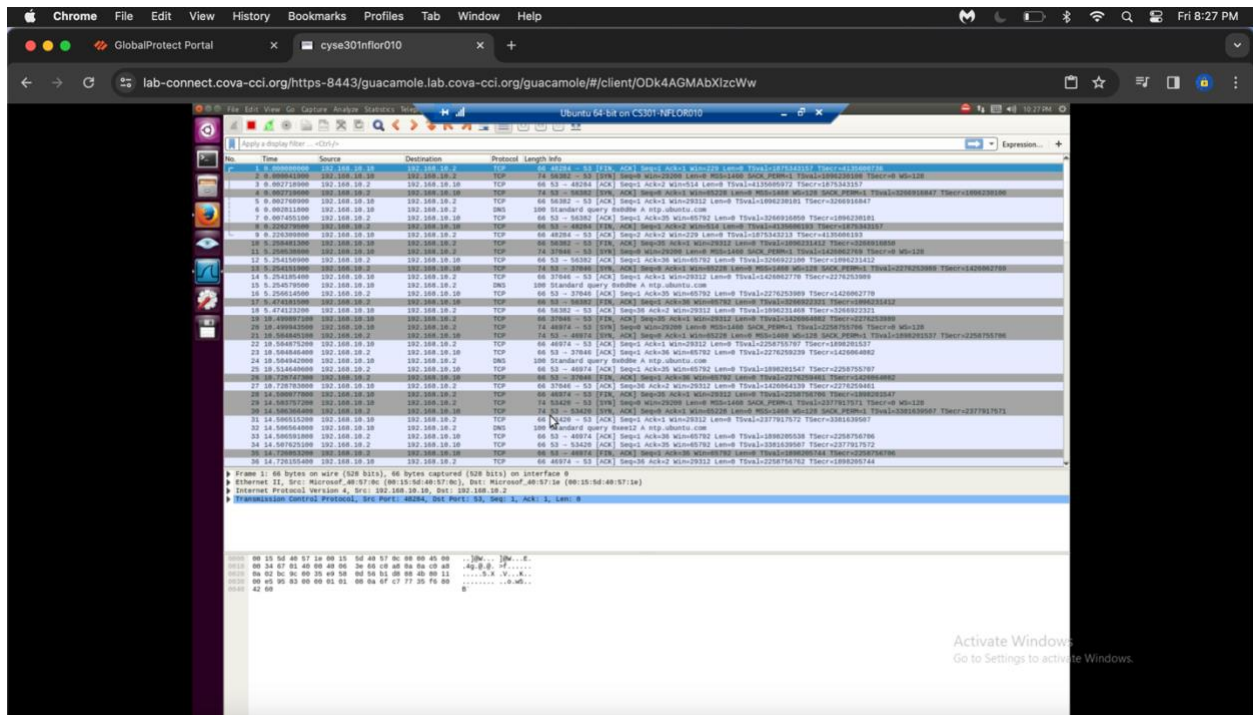
Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if applicable)
2	WAN	BLOCK	192.168.217.3	192.168.10.0/24	FTP (port 21)



Rules (Drag to Change Order)												
☐	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
☐	0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogus networks		
☐	0/0 B	IPv4 TCP	192.168.217.3	*	192.168.10.11	*	*	none	1	FTP protocol towards Windows Server 2008	 	
☐	0/0 B	IPv4 *	192.168.217.3	*	192.168.10.0/24	*	*	none	2	block all traffic from external kali to lan side	 	
☐	0/0 B	IPv4 ICMP any	192.168.217.3	*	192.168.10.10	*	*	none		icmp block from external kali to ubuntu	 	
☐	0/0 B	IPv4 ICMP any	192.168.217.3	*	LAN net	*	*	none		icmp block from external kali to the lan side	 	
☐	11 /10.92 MiB	IPv4+6 *	WAN net	*	*	*	*	none		Open Connection IPv4 and IPv6	 	

I only received TCP traffic when using the firewall policy. There are two rules that I implemented. Firstly, I only allowed FTP towards Windows to pass. Next, all other traffic from external kali to LAN side is blocked. The order of the rules is very important for this to work. The screenshot with the two terminals show's FTP. On the left is the IP address of Ubuntu. You can see that the connection is blocked. ON the right side is Windows Server 2008. This host is able to access the FTP server. For the first rule, I configured Windows Server 2008 to be the destination address.

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



I immediately noticed that I am not receiving that many packets. Next, I realized I only received TCP traffic when using the firewall policy. I only allowed FTP towards Windows Server 2008 to pass, all other traffic from external kali to LAN side is blocked.

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

192.168.10.9				
2	1	9	1	20
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities				Total: 33
SEVERITY	CVSS	PLUGIN	NAME	
CRITICAL	10.0	79638	MS14-060: Vulnerability in Schannel Could Allow Remote Code Execution (2692611) (unauthenticated check)	
CRITICAL	10.0	125313	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (unauthenticated check)	
HIGH	9.3	58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (unauthenticated check)	
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted	
MEDIUM	6.4	57582	SSL Self-Signed Certificate	
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection	
MEDIUM	5.1	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm	
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)	
MEDIUM	4.3	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	
MEDIUM	4.3	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only	
MEDIUM	4.3	57690	Terminal Services Encryption Level is Medium or Low	
LOW	2.6	30218	Terminal Services Encryption Level is not FIPS-140 Compliant	
INFO	N/A	45590	Common Platform Enumeration (CPE)	
INFO	N/A	54615	Device Type	

The above screenshot is the pdf info sheet. I used Nessuss and found a critical vulnerability called (CVE-2019-0708) also known as Blue Keep. This is a vulnerability that affects the Remote Desktop Services (RDS) in older versions of Microsoft Windows. This vulnerability allows an attacker to exploit the Remote Desktop Protocol (RDP) and execute arbitrary code on the target system without authentication. BlueKeep is considered highly dangerous because it can be used to propagate malware and create self-replicating worms, similar to the infamous WannaCry ransomware.