## CYSE 301: Cybersecurity Technique and Operations

Assignment 3: Sword vs. Shield

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
- pfSense
- Ubuntu
- Windows Server 2022

## 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.





2. Run Wireshark in Internal Kali VM while External Kali is scanning the network. Discuss the traffic pattern you observed. What do you find? <u>Please write a 200-word essay to discuss your findings.</u>

To begin gathering information about the network, I used Nmap from the External Kali machine to scan the subnet and identify any live devices. I first scanned the subnet 192.168.217.3/24 and found two active hosts, including the pfSense virtual machine at 192.168.217.2. This helped me confirm that pfSense was operating on the network. I then ran another scan on a different subnet, 192.168.10.13/24, which revealed additional hosts, including IP addresses like 192.168.10.2, .13, .18, and .19. These are likely the other virtual machines in the network, such as the Ubuntu and Windows Server 2022 systems.

While the External Kali machine was scanning, I used Wireshark on the Internal Kali machine to observe the network traffic. During the scan, Wireshark captured traffic related to the devices trying to communicate with each other, specifically using ARP (Address Resolution Protocol). This traffic showed that devices were asking for each other's physical (MAC) addresses so they could communicate. There were also some DNS queries related to local network service discovery. Overall, the pattern of traffic showed devices learning each other's presence on the network as I conducted the scan.

## Task B: Shield – Protect your network with a 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 appliable)
2	LAN	Block	192.168.10.18	192.168.217.3	IPv4   ICMP:any

[Add the screenshot here]

Rttacker Kali - External Workstation on CY301-MBROW096 - Virtual Machine Co	🖳 🖳 Ub	untu 220	04-64	-bit on	CY301-	MBROV	V096	- Virtual N	Aachine Co	nnection							-	- 0	) ×
File Action Media View Help	File	Action	n M	Media	Clipb	oard	View	v Help											
🖦 💿 💿 🕲 💷 🕨 🛼 5 ) 🕎 🚵	₽   (		0 (	0   11	₽	B 5	18	2 🚮											
😫 🔲 🖻 🍃 🍪 🕒 v 🛛 1 2 3 4 🕒	Act	ivities		🗐 F	refox	Web B	Вгоч	vser				Oct 12 19:27	Û					6 <b>?</b> 8	ڻ
	6		•	ø	ofSen	se.CYS	SE.co	om - Fire	•••× +								~	-	•
			$\leftarrow$	$\rightarrow$	С		0		1ttps://19	92.168.10.2/fire	ewall_	rules.php?if=la	n			☆	$\bigtriangledown$	۲	ර ≡
File Actions Edit View Help						Float	ting	WAN	LAN										
-V: Print version number -h: Print this help summary page.																			
EXAMPLES:	0					Ru	les	(Drag	to Chan	ge Order)									
nmap -v -sn 192.168.0.0/16 10.0.0.0/8 nmap -v -in 192.168.0.0/16 10.0.0.0/8								States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Action	IS
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR M ES 	?						~	1/1.22 MiB	*	*	*	LAN Address	443 80	*	*		Anti- Lockout Rule	٥	
La ifconfig eth0: flags=4163 <up, broadcast,="" multicast="" running,=""> mtu i inet 192.168.217.3 netmask 255.255.255.0 inet6 fe80::cf016444:5507f.6654 prefixlen 64 ether 00:15154/40:5727 txqueuelen 1000 (Eth RX packets 27 bytes 1594 (1.5 KiB)</up,>	>-						×	0/0 B	IPv4 ICMP any	192.168.10.18	*	192.168.217.3	*	*	none		Block ICMP from Kali External	€ 00 10	<b>\$</b>
RX errors 0 dropped 0 overruns 0 frame 0 TX packets 85 bytes 24083 (23.5 KiB) TX errors 0 dropped 0 overruns 0 carrier 0 d eth1: flags=4163 <up,broadcast,running,multicast> mtu 1</up,broadcast,running,multicast>							~	0/46 KiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	€ 00 10×	» )
inet 169.254.44.123 netmask 255.255.0.0 broat inet 6 fe80::c574:146:13580:5380 prefixlen 64 ether 00:15:5d:40:57:28 txqueuelen 1000 (Eth RX packets 176 bytes 63006 (61.5 KiB) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 241 bytes 52058 (50.8 KiB)							~	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	҈₩ ©© ā×	» )
VMSharter	0									1 Add	L Ado	d <u>前</u> Delete	🛇 То	ggle	Сору	🕄 Save 🗧	Separator		
						0													
file1.txt						_			· · ·										

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	LAN	Block	192.168.10.18	LAN network	IPv4   ICMP:any

[Add the screenshot here]



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 Ubuntu.

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
2	LAN	Block	192.168.10.18	LAN network	IPv4   ALL TRAFFIC



[Add the screenshot here]

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

Extra credit (15 points): Use NESSUS to enumerate the security vulnerabilities of Microsoft Windows Server 2022 VM in the CCIA network.