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 2008

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 Ubuntu 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>



Wuturu 44 de m (S30)-05/L400 - Virtuul Machine Connection Ne de la fiele Maria							O							⊜ lai	b-con	nect.co	wa-cci.o	g				d	5									٩
Image: Antion Marke Organization (Market Market		🖳 Ubuntu	u 64-bit or	n CS301	-DSCA	R005 - V	firtual N	lachine	Connec	tion		_		_				_			_			_			_		_		>	
	DV	File Ad	ction N	Aedia	Clipbo	bard	View	Help																								
	40	B 0	. 0 (•	B 3	188	ai																								
Image: Solution of the	1	*eth0																									t ₁		()) 6:1	18 PM	
Image: Section of the sectin of the section of the section		-	1		1 6				8	0	1	\$	2	ki-			1 =			10												
Image: Control of the standard grant of the standard gran	3	Q)			9 G					~				-	-					2 11												
No. Imme Source Destination Protocol Length info 42 16.0004511800 122.168.10.10 132.168.1217.3 112.168.10.10 110.16.10 112.168.10.10 1		+	Ap	ply a d	lisplay	filter	<0	:trl-/>																			-	3 -	Exp	ressio	on	
41 16.666418000 192.168.217.3 192.168.19.10 ICMP 42 Echo (ping) request id=0x17fe, seq=0 43 17.321995700 192.168.10.10 192.168.10.10 ICMP 42 Echo (ping) request id=0x17fe, seq=0 43 17.321995700 192.168.10.10 192.168.10.1 ICMP 42 Echo (ping) request id=0x15fe, seq=0 45 17.794180300 Microsof.40:57:00 Bradcast ARP 42 Who has 192.168.10.27 Fell 192.168.10 47 21.001094900 192.168.10.1 192.168.10.2 TCP 66 58132 - 53 [Fin, AcK] Seq=35 Ack=1 Win 49 21.005931100 192.168.10.1 192.168.10.2 TCP 66 58134 - 53 [KM] Seq=0 Win=29200 Len- 49 21.005931100 192.168.10.1 192.168.10.2 TCP 66 58134 - 53 [KM] Seq=0 Win=29200 Len- 49 21.005931100 192.168.10.1 192.168.10.2 TCP 66 58134 - 53 [KM] Seq=0 Ack=1 Win 49 21.005931100 192.168.10.1 192.168.10.2 TCP 66 58134 - 53 [KM] Seq=1 Ack=3 Win=2933 51 21.000007100 192.168.10.1 192.168.10.2 TCP 66 58134 - 53 [KM] Seq=0 Ack=1 Win 49 21.005931100 192.168.10.1 192.168.10.2 TCP 66 58134 - 53 [KM] Seq=1 Ack=3 Win=2933 51 21.000007100 192.168.10.1 192.168.10.2 TCP 66 58134 - 53 [KM] Seq=1 Ack=3 Win- 51 21.000007100 192.168.10.1 192.168.10.2 TCP 66 58134 - 53 [KM] Seq=1 Ack=3 Win- 51 21.000007100 192.168.10.2 UN 100 Sig 100 S			No.	T	Time			Sourc	e				De	stin	atio	۱.			Protocol	Len	gth Ir	nfo										
417.321996700 192.168.12.7.3 192.168.10.10 107 42 Echo (ping) reply idextid sector, sequence 417.321996700 192.168.10.10 192.168.10.2 109 42 Echo (ping) reply idextid sequence 417.321996700 192.168.10.10 192.168.10.2 109 42 Echo (ping) reply idextid sequence 417.321996700 192.168.10.10 192.168.10.2 109 66 Stal2 - S3 [FN] Sequence Sequence 42.1.001047100 192.168.10.10 192.168.10.2 109 166 Stal2 - S3 [FN] Sequence Sequence 42.1.001047100 192.168.10.10 192.168.10.2 109 168.10.2 109 74 Stal4 - S3 [SN] Sequence Sequence 42.1.001047100 192.168.10.10 192.168.10.2 109 168.10.2 109 74 Stal4 - S3 [SN] Sequence Ack13 kmines57 50.21.0050871200 192.168.10.10 192.168.10.2 109 168.10.2 109 168.10.2 109 168.10.2 109 168.10.2 109 169.15.50:40:57:10: 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100				41 1	16.00	0418	000	192.	168.2	217.	3		19	2.1	.68.	10.1	.0		ICMP		42 E	cho	(pin	g)	requ	est	10	1=0x1	17fe	e, se	eq=0	
 4 17.321995706 192.165.16.16 4 221.001027709 192.165.10.10 4 7 21.001094909 192.165.10.10 4 7 21.001094909 192.165.10.10 4 7 21.005931100 192.165.10.10 4 9 21.005931100 192.165.10.10 4 9 21.005931100 192.165.10.10 4 9 21.005931100 192.165.10.10 5 12.1096067100 192.165.10.10 5 12.1090667100 192.165.10 5 1 2 1000567100 192.165.10 5 1 2 100057100 10 5 1 2 10005 5 1 2 1 0 1 1 2 1 0 1 2 1				42 1	17.32	21960	000	192.	168.2	217.	3		19	2.1	68.	10.1	0		ICMP		42 E	cho	(pin	(g)	requ	y est	10	1=0x1	:510	1. Se	eq=0	E
45 17,794180309 Microsof_49:57:8a Broadcast APP 42 Who has 192.168.10.27 Tell 192.168.10. 47 21.001094900 192.168.10.10 192.168.10.2 TCP 74 58134 - 53 [SVN] Seq=9 Win=29200 Len- 49 21.005931309 49 21.005931309 192.168.10.2 192.168.10.2 TCP 74 58134 - 53 [SVN] Seq=9 Win=29200 Len- 49 21.005931209 192.168.10.2 192.168.10.10 TCP 74 58134 - 53 [SVN] Seq=9 Ack=1 Win 49 21.005931209 192.168.10.2 192.168.10.10 TCP 66 58134 - 53 [ACK] Seq=1 Ack=1 Win=2931 50 21.005874209 192.168.10.2 192.168.10.10 TCP 66 58134 - 53 [ACK] Seq=1 Ack=3 & Win=657 109 Standard query 0x2198 A ntp.ubuntu.co * Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 9 * Ethernet II, Src: Microsof_40:57:0c (00:15:5d:40:57:0c), Dst: Microsof_40:57:1e (00:15:5d:40:57:1e) * Transmission Control Protocol, Src Port: 58124, Dst Port: 53, Seg: 1, Ack: 1, Len: 0 * * * Activate Windows 60 e 59 58 30 00 00 01 01 08 00 a c c d a8				44 1	17.32	21995	700	192.	168.3	10.1	Θ		19	2.1	68.	217.	3		ICMP		42 E	cho	(pin	g)	repl	у	id	l=0xc	:510	i, se	eq=0	E
10 21:00102/100 192:100:10:1 102				45 1	17.79	4180	300	Micr	0S01	40:	57:0	a	Br	oad	cas	t 10 2			ARP		42 W	ho h	has 1	92.	168.	10.2	27 1	ell	192	2.168	8.10	
48 21.065873300 192.168.10.2 192.168.10.10 192.168.10.2 TCP 74 53 - 58134 CKX Seq=0 Ack=1 Win 59 21.065874200 192.168.10.2 192.168.10.10 TCP 76 53 - 58134 CKX Seq=1 Ack=30 Win-657 51 21.060607100 192.168.10.10 192.168.10.2 DV 66 53 - 58132 AcK1 Seq=4 Ack=1 Win 6 55 1 21.060607100 192.168.10.10 192.168.10.2 DV 160 Standard query 9x2198 A ntp.ubuntu.co 1 Ffmen 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0 Ethernet 1I, Src: Microsof (40:57:10:) Dist: Microsof 40:57:10: (00:15:5d:40:57:10:) 1 Internet Protocol Version 4, Src: 192.168.10.10, Dst: 192.168.10.2 Dist: Microsof 40:57:10: (00:15:5d:40:57:10:) 1 Internet Protocol, Src Port: S8124, Dst Port: 53, Seq: 1, Ack: 1, Len: 0 0 00 34 86 5c 40 00 40 66 17 6b cc 88 60 46 c6 88](W				47 2	21.00	1094	900	192.	168.3	10.1	0		19	2.1	.68.	10.2			TCP		74 5	8134	1 → 5	3	SYN]	Seq	1=0	Win=	=292	200 L	Len=	
49 21.089393100 192.108.10.0 192.108.10.2 192.108.10.2 100 100 66 53134 - 53 102K Seq=1 Ack=3 Win=2931 5 21.080507100 192.168.10.10 192.168.10.2 DNS 100 Standard query 9x2198 A ntp.ubuntu.co 1 Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0 100 Standard query 9x2198 A ntp.ubuntu.co 2 Frame 1: 1, Src: Microsof 40:57:0c (00:15:5d:40:57:0c), Dst: Microsof 40:57:1e (00:15:5d:40:57:1e) 100 Standard query 9x2198 A ntp.ubuntu.co 1 Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0 100 Standard query 9x2198 A ntp.ubuntu.co 2 Transmission Control Protocol, A; Src: 192:168.10.0, Dst: 192:068.10.2 110 Standard query 9x2198 A ntp.ubuntu.co 0000 00 15 5d 40 57 1e 00 15 5d 40 57 0c 08 00 45 00				48 2	21.00	5873	300	192.	168.3	10.2			19	2.1	.68.	10.1	63		TCP		74 5	3 -	5813	4 [SYN,	ACK	(] 5	seq=6	A G	:k=1	Win	
51 21.006006700 192.168.10.10 192.168.10.2 DK 100 Standard query 9x2198 A ntp.ubuntu.co Image: Standard query 9x2198 A ntp.ubuntu.co Image: Standard query 9x2198 A ntp.ubuntu.co Image: Standard query 9x2198 A ntp.				49 2	21.00	5931	200	192.	168.	10.1	Θ		19	2.1	68.	10.2	Θ		TCP		66 5	8134	5813	2 1	ACK]	Seq	1=1	ACK=	=1 V =36	Win=2	2931	
 Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 9 Ethernet II, Src: Microsof 40:57:0c (00:15:5d:40:57:0c), Dst: Microsof 40:57:1e (00:15:5d:40:57:1e) Internet Protocol Version 4, Src: 192.168.10, Dst: 192.168.10.2 Transmission Control Protocol, Src Port: 58124, Dst Port: 53, Seq: 1, Ack: 1, Len: 0 0000 00 15 5d 40 57 1e 00 15 5d 40 57 0c 08 00 45 00 0010 00 34 86 5c 40 00 40 06 17 0b ce a8 0a 0a ce a8 0010 00 34 86 5c 40 00 40 06 17 0b ce a8 0a 0a ce a8 0020 0a 22 83 0c 00 35 0d bc ec be 4d 47 35 b8 80 11 0030 0a es 95 83 80 00 00 10 10 80 0a eb fd 97 80 82 ba 0040 0a 55 0d 40 57 1e 00 15 10 00 0a eb fd 97 80 82 ba 0040 0a 55 0d 40 57 1e 00 10 10 80 0a eb fd 97 80 82 ba 0040 0a 50 00 01 01 00 0a a eb fd 97 80 82 ba 0040 0a 50 00 01 01 00 0a a eb fd 97 80 82 ba 0040 0a 50 00 01 01 00 0a a eb fd 97 80 82 ba 0040 0a 50 00 01 01 00 0a a eb fd 97 80 82 ba 0040 0a 50 00 01 01 00 0a a eb fd 97 80 82 ba 0040 0a 50 00 01 01 00 0a a eb fd 97 80 82 ba 0040 0a 50 00 01 01 00 0a a eb fd 97 80 82 ba 0040 0a 50 00 01 01 00 0a a eb fd 97 80 82 ba 0040 0a 50 00 01 01 00 0a a eb fd 97 80 82 ba 0040 0a 50 00 01 01 00 0a a eb fd 97 80 82 ba 0040 0a 50 00 01 01 00 0a a eb fd 97 80 82 ba 0040 0a 50 00 01 01 00 0a a eb fd 97 80 82 ba 0040 0a 50 00 00 01 01 00 0a a eb fd 97 80 82 ba 0040 0a 50 00 00 01 01 00 0a a eb fd 97 80 82 ba 0040 0a 50 00 00 01 01 00 0a a eb fd 97 80 82 ba 0040 0a 50 00 00 01 01 00 0a a eb fd 97 80 82 ba 0040 0a 50 00 00 01 01 00 0a a eb fd 97 80 82 ba 0040 0a 50 00 00 01 01 0a 0a a ba fd 97 80 82 ba 				51 2	21.00	6067	100	192.	168.3	10.1	Θ		19	2.1	68.	10.2			DNS	1	100 S	tand	lard	que	ry 0	x219	8 A	h ntp	p.ut	ountu	u.co	
 Prime 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 6 Ethernet II, Src: Microsof 40:57:00 (00:15:5d:40:57:10 (00:15:5d:40:57:10) Internet Protocol Version 4, Src: 192.168.10.10, Dst: 192.168.10.2 Transmission Control Protocol, Src Port: 58124, Dst Port: 53, Seq: 1, Ack: 1, Len: 6 0000 00 15 5d 40 57 10 00 15 5d 40 57 00 08 00 45 00 001 00 34 86 5c 40 00 40 66 17 9b c0 88 0a 6a c0 88 0020 6a 02 c3 0c 00 35 0d bc cc be 4d 47 35 b8 80 11 0020 6a 02 c3 0c 00 35 0d bc cc be 4d 47 35 b8 80 11 0020 6a 02 c3 0c 00 35 0d bc cc be 4d 47 35 b8 80 11 0020 6a 02 c3 0c 00 35 0d bc cc be 4d 47 35 b8 80 11 0020 6a 02 c3 0c 00 35 0d bc cc be 4d 47 35 b8 80 11 0020 6a 02 c3 0c 00 35 0d bc ec be 4d 47 35 b8 80 11 0020 6a 02 c3 0c 00 35 0d bc ec be 4d 47 35 b8 80 11 0020 6a 59 58 30 00 00 16 1 08 0a ab fd 97 80 82 ba 0020 6a 59 58 30 00 00 16 1 08 0a ab fd 97 80 82 ba 0020 6a 59 58 30 00 00 16 1 08 0a ab fd 97 80 82 ba 0020 6a 59 58 30 00 00 16 1 08 0a ab fd 97 80 82 ba 0020 6a 59 58 30 00 00 16 1 08 0a ab fd 97 80 82 ba 0020 6a 59 58 30 00 00 16 1 08 0a ab fd 97 80 82 ba 0020 6a 59 58 30 00 00 16 1 08 0a ab fd 97 80 82 ba 0020 6a 59 58 30 00 00 16 1 08 0a ab fd 97 80 82 ba 0020 6a 59 58 30 00 00 16 1 08 0a ab fd 97 80 82 ba 0020 6a 59 58 30 00 00 16 1 08 0a ab fd 97 80 82 ba 0020 6a 59 58 30 00 00 16 1 08 0a ab fd 97 80 82 ba 0020 6a 59 58 30 00 00 16 1 08 0a ab fd 97 80 82 ba 0020 6a 59 58 30 00 00 16 1 08 0a ab fd 97 80 82 ba 0020 6a 59 58 6a 6a 50 6			4						1.0.0																							
 Pinternet Prótocol Version 4, Src: 192.168.18.19, Dst: 192.168.18.2 Transmission Control Protocol, Src Port: 58124, Dst Port: 53, Seq: 1, Ack: 1, Len: 0 0000 00 15 5d 40 57 1e 00 15 5d 40 57 0c 08 00 45 00 0010 00 34 8e 5c 40 00 40 66 17 0b c0 a8 0a 6a c0 a8 0020 0a 62 95 83 00 00 01 61 08 0a eb fd 97 80 82 ba 0040 68 fd Activate Windows Go to Settings to activate Windows. 			Fra	ame 1 herne	: 66 t II	byte Sro	es on : Mi	crose	e (52 of 40	8 b1	ec (66 00:	by 15:	tes 5d:4	car 40:5	iture	ed (5 c). D	28 b: st: 1	ts) on licroso	1nte	erfa :57::	ce 0 1e (00:15	5:50	1:40:	57:1	1e)					
• Transmission Control Protocol, Src Port: 58124, Dst Port: 53, Seq: 1, Ack: 1, Len: 0 • O000 00 15 5d 40 57 1e 00 15 5d 40 57 0c 08 00 45 00]@w]@wE. • 010 00 34 8e 5c 40 00 40 06 17 0b c0 a8 0a 0a c0 a8]@w]		·L/U	> Int	erne	t Pr	otoco	ol Ve	rsio	n 4,	Src:	192	.16	8.1	9.10	Ð, [st:	192.	168.3	0.2								,					
0000 00 15 5d 40 57 1e 00 15 5d 40 57 0c 08 00 45 00			> Ira	ansmi	\$\$10	n Cor	itrol	Prot	10201	, Sr	CPO	rt:	58	124,	, Ds	E PO	ort:	53, 3	eq: 1,	ACK	: 1,	Len	: 0									
0000 00 15 5d 40 57 10 00 15 5d 40 57 0c 08 00 45 00]@w]@w @w]@wE. 0010 00 34 86 5c 40 00 40 06 17 0b c0 88 0a 0a c0 88]@w]@wE.		100																														
0000 00 15 5d 40 57 1e 00 15 5d 40 57 0c 08 00 45 00 .)0v .)0v 010 00 34 86 5c 40 00 40 06 17 0b c6 88 04 06 08 06 17 0b c6 88 04 06 08 08 020 0a 02 e3 0c 00 35 0d bc ec be 4d 47 35 b8 08 11 033 00 e5 95 83 00 00 01 01 08 0a eb fd 97 80 82 ba 0440 68 fd 0440 0440 0440 0440 0440 050 050 .																																
0000 00 15 5d 40 57 1e 00 15 5d 40 57 0c 08 00 45 00		The second second																														
0000 00 15 5d 40 57 1e 00 15 5d 40 57 0c 08 00 45 00]@w]																																
0000 00 15 5d 40 57 0c 08 04 60 17 0b c8 0a 0a 0c 0a <																																F
001 00 01 55 50 40 57 0c 68 00 45 06																																
001 001 34 86 52 64 64 66 17 90 68 <		1	0000	00	15 5	d 40	57 1	le 00	15	5d 4	10 57	7 Oc	08	00	45	00]	@W]@W	.E.												
Comparison of the second			0010	00	34 8	e 5c	40 6	00 40	06	17 6	b ce	a8	0a	0a	CO PO	a8	.4.	10.0.	MCE	• • •												
		(0020	00	e5 9	3 OC 5 83	00 0	00 01	01	08 G	a et	1 4/	30	80	80	ba			MG5													
Activate Windows Go to Settings to activate Windows.			0040	68	fd					55 S							h.							de ca								
Go to Settings to activate Windows.																							AC		ite v	vina		5				
🚛 🔿 📴 Hunger, V. Mananose 🦄 Attacher Kali - Frite 🔊 of conce - Firewall 🔅 Uburdu/ródubit on 🛸 Windows Server 20. 🔿 🖅 du)) 9:18 PM																																
💶 🔘 🖽 🖓 🔚 Honger V. Mananar 🔊 Attacker Kali - Erte 🔊 ofcence - Erevall 🧖 Ilburch 64-bit on 🔭 Windows Server 20 🔿 🖓 dtacker Kali - Erte		1.																														I.
			5 8	(0	See.	honer-V	Manaou		-	Attacke	e Kali	- Exte			nEsen	ce - Fire	wall	1 LIN	untu 64	l-hit or		1 N	Ninda	une See	ver 20		~ 5	1 c1m)	9:18	PM	

Several unusual traffic patterns were observed in the simulated scenario where Wireshark was operating in an Ubuntu Virtual Machine (VM) while an external Kali system was scanning the network. A network protocol analyzer called Wireshark provided an informative look at the dynamics of communication during the scanning process. A spike in ARP (Address Resolution Protocol) requests was instantly apparent after starting the Kali scan. The scanning system was making queries to map IP addresses to MAC addresses in an effort to find active hosts on the network. Then, a string of ICMP (Internet Control Message Protocol) echo requests—often indicative of a host scanning for live hosts—were noticed. In the reconnaissance stage of a network assault, this step is crucial. Port scanning activity were visible while the scan went on. There were a lot of TCP SYN packets, indicating an effort to connect to a variety of target machines' ports. A network's vulnerabilities or active services may be indicated by unusual or unexpected ports that are being probed. The Wireshark logs also showed an increase in HTTP requests, indicating that the scanning system was attempting to learn more about the web services available on the discovered hosts. This might entail determining web servers, versions, or even potential vulnerabilities in web applications.

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.





	WAN	Block/reject	192.168.10.10	192.168.217.3	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)
	WAN	Block	192.168.217.3	LAN net/ any	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.





(port # if appliable)

ľ	WAN	Block	192.168.217.3	Any	Any
	WAN	Pass	192.168.217.3	192.168.10.11	ТСР

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

The main goal of this project was to use pfSense firewall to develop appropriate countermeasures while acting as both an attacker and a defender to find vulnerabilities in a LAN network. Network scanning, Wireshark traffic pattern capture, and firewall rule configuration were among the duties.

Task A involved profiling the fundamental details of the subnet topology, including open ports, operating systems, and services connected to each VM in the LAN network, using Nmap or Zenmap from the External Kali VM. The Ubuntu VM was also used to run Wireshark in order to record network activity while scanning was being done.

Task B concentrated on configuring pfSense's firewall rules to secure the network. The four subtasks were to block all ICMP traffic to the LAN side, all ICMP communication from External Kali to Ubuntu VM, all LAN side traffic except for FTP to Windows Server 2008, and finally to rerun the network scan after configuring the firewall rules.

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