#### OLD DOMINION UNIVERSITY

### CYSE 301 Cybersecurity Techniques and Operations

## Assignment #3: Sword vs. Shield

Antonio Shields

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.



Figure 1 Screenshot of TaskA1.txt being created in Attacker Linux for using the nmap command for Task A.1

The above screenshot shows the .txt file "TaskA1" being created with the following four IP addresses: 192.168.217.3 (attacker kali), 192.168.10.2 (pfSense), 192.168.10.10 (Ubuntu), 192.168.10.11 (Windows Server 2008). This file will be used to search these ip addresses using the nmap command at one time instead of using the nmap command separately for each ip address.



Figure 2 Screenshot of nmap command being used and the results returned in Attacker Linux for Task A.1

The above screenshot shows the nmap command being used to retrieve the subnet topology, service and backend software information from the open ports required for this Task. In the nmap command -O is used for OS detection, -sV is used to determine the service and version running on the port, and -iL allows me to scan from the ip addresses listed in the TaskA1.txt file in the previous screenshot. These are the results from 192.168.217.3 (Attacker Kali) which is the device currently on and initiating nmap.



Figure 3 Screenshot of nmap command results for 192.168.10.2 (pfSense) returned in Attacker Linux for Task A.1

The above screenshot shows the nmap command results for 192.168.10.2 (pfSense) and shows the open port information, the service and version. OS version came back with no match.



Figure 4 Screenshot of nmap command results for 192.168.10.10 (Ubuntu) returned in Attacker Linux for Task A.1

The above screenshot shows the nmap command results for 192.168.10.10 (Ubuntu) and shows the open port information, the service and version. OS version came back as Unix.



Figure 5 Screenshot of nmap command results for 192.168.10.11 (Windows Server 2008) returned in Attacker Linux for Task A.1

The above screenshot shows the nmap command results for 192.168.10.11 (Windows Server 2008) and shows the open port information, the service and version. OS version came back as Microsoft Windows Server 2008 R2.

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>

In running Wireshark in Ubuntu VM while External Kali scanned the network using the nmap command, the results that came back, which can be seen in figures 6, 7, 8, 9, and 10 below were as follows: In Figure 6 it shows, the TCP protocols and DNS protocols that were conducted multiple times between 192.168.10.10 (Ubuntu) and 192.168.10.2 (pfSense) with the three-way handshake between the two ip addresses for TCP and a DNS query sent for DNS. Near the bottom of Figure 6, it shows where 192.168.217.3 (Attacker Kali) and 192.168.10.10 begin TCP protocol. Figure 7 shows the protocol hierarchy statistics during the capture, where 2452 packets total were captured with 5 packets being UDP protocol, 2422 being TCP protocol with 1 of those 2422 being FTP and 31 being DNS, the remaining 25 of the total 2452 came from ICMP protocol. In figure 8 when scrolling further down in the captured packets, it was discovered that interactions between 192.168.217.3 (Attacker Kali) and 192.168.10.10 (Ubuntu) started appearing red in color and "RST" began appearing in the three-way handshake during the TCP protocol. It looks like the connection kept resetting or forcing the connection to terminate multiple times. In figure 9, it shows RST between 192.168.10.10 (Ubuntu) and 192.168.10.2 (pfSense) where the connection is being forcefully terminated and reset and can also be seen are black TCP Retransmission responses from the firewall back to Ubuntu. Figure 10 shows TCP, ICMP, and UDP protocols being used with some RST messages or indicators that ports are being reused or are unreachable. These errors can indicate possible suspicious activity like an outside actor scanning for open ports.

): 			Ution is the weath	REMO	- 1 × 1	😑 📭 🛅 🐠 438PM	¢
4	E 2 0 a	> P O X C	>> = = = =	000	12		
	puly a display filter	+Ctr5-/+				E · Expression	
	Play a despart state -		2222110222	12000		Contraction of the	
Nr.	* Time	Source	Destination	Protocol L	ength info		-
100	1 0.00000000	102 108 10 2	192 108 10.10	109	00 53 - 12840 [F]	N, ACK) Seg=1 Ack=1 H1	
	2 0.000010500	192.168.18.16	192.100.19.2	TCP	00 32840 - 53 AC	K] Seg-I Ack-2 Min-229	
	3 9,2444143999	192.100.10.10	182,100,30,2	TOP	90 37274 - D3 [P1	N ACKI Sedel ACKOI MS	
	5 0 3455 70300	102.100.10.10	100 100 10 10	166	00 53 - 32924 140	A Sector Action Level	
	3 0.245579200	192.100.10.2	197.100.10.10	TOP	22 55 - 51254 100	W ACE Same Acked M	
-	7.0.745601498	102 100 10 10	192 168 18 2	TCP	00 51464 - 53 40	AL Segura Ackat Migar201	
	0.0.245644000	102,168,10,10	192,168,18,2	DNS	100 Standard query	0x6317 A oto ubuntu c	
	8 0.240994300	192.168.10.2	197,100,10,10	TCF	00 53 - 51404 TAC	X1 Seg-1 Ack+25 Winsets	
	15 5 494413099	182 108 10.10	192 166 10.2	TOP	60 51484 - 53 (FI	N. ACK1 Seg=35 Ack=1 b	
48 C	11 5,494451500	192.108.10.18	192,168,10.7	TCP	74 39334 - 53 (5)	N] Seg=0 Win=20200 Len	
	12 5.405750000	192,160,16,2	192,168 10,18	TCP	74 53 - 20134 (5)	N. ACKI SOUND ACREL MS	
	13 5,495781288	192.160.10.10	192.168.18.2	TCP	66 39134 - 53 AC	x) Seg=1 Ack=1 Win=203	
	14 5,495753688	192,168,10.2	192.168.30.30	TCP	66 53 - 51484 (Ad	K) Seg=1 Ack=36 Win=65	
	15 5.495822386	192.108.10.10	192.168.10.2	DNS	199 Standard query	8x6317 A ntp.ubuntu.c	
	16 5,4564889988	192.108.18.2	192,168,18,18	TCP	06 53 - 39134 [AC	K] Seg=1 Ack=30 Win=65	
	17.7.218341500	102.108.217.3	192.108.10.18	TCP	58 37429 - 443 [5	NN) Segro Wire1024 Len	
11	rame 1: 66 bytes	on wire (528 bits).	65 bytes captured (5)	28 bits) on 10	nterface 0 48:57:0c (88:15:5d)	40:57:0c)	
• 1	nternet Protocol	Version 4, Src: 19	2.168.10.2, Dat: 192.10	68.18.18	and the fact and the		
1000	ANUBLASION CONC.	ul Protocol, Src P	ort 53. Ost Port 328	16. Seu: 1. A	N I Lett 0		
1000	50 15 Ed 40 ET	Ar 20 45 54 40 5	7 1.0 00 00 15 00 14	a 100 c			
1.0.1	00 13 20 40 57	00 40 45 50 40 5	1 10 00 00 00 00	W 18WE.			
0.01	0 00 04 00 00 40	00 40 00 85 67 0	0 80 08 82 00 80 .4.	- 환수환수 수업+ + + + +			
9992	u ua ua	40 01 00 41 10 0		a the second second			
00.0	12 12 43 MI 00	00 01 01 00 04 0	0 20 86 00 00 42	a a sea a sea la sel la sel la	1 ( )	- Arettinghe	Wirelesser.
	0 10 m						Contraction of the local division of the loc
							Compare window

*Figure 6 Screenshot of wireshark results ran on 192.168.10.10 (Ubuntu) while 192.168.217.3 (Attacker Linux) scanned the network for Task A.2* 

reshark	1000	diamont pro-	ni ASTETICO		diam'r	😑 'i 🖾	(1) 454 PM 6	0
Appty a display filter No. • Time C. 0.00001.0000 C. 0.2453.0500 C. 0.245571200 C. 0.24557120 C. 0.24557120 C. 0.24557120 C. 0.24557120 C. 0.24557	Vulreshark - Pro Protocol • Fatte • Ethernet • User Datagra Data • Transmisske file Trans Domain N Intermet Com	ol Version 4 im Protocol i Control Protocol fer Protocol (FTP) ame System Irral Message Protocol	00000000000000000000000000000000000000	etho_202311 Packets 2452 2452 2452 5 5 5 2422 1 31 25	Percent Bytes 23.1 33.0 0.0 1.0 39.9 0.0 0.7 3.1	0,48758 148758 34328 49040 49040 49040 1500 55340 20 1054 4540	Bity/s 9191 2120 3029 2 92 3665 7 65 280	
0010 00 15 5d 40 57 0010 00 34 00 00 40 0020 8a 6a 00 23 00 0020 72 02 02 45 at 00 0020 70 61	÷-						Activity M	/indows

*Figure 7 Continued screenshot of wireshark results ran on 192.168.10.10 (Ubuntu) while 192.168.217.3 (Attacker Linux) scanned the network for Task A.2* 

100		1.4 March 1.	Shorts 64	her on ASI Plane		😑 🖬 🖽 🖛 🗐	шрм 😋
41	1 2 0 🔒	> P S X M	ンダモーニー		<u>EX</u>		
ALAPP	ily a display filter					CI - Expressio	in +
12	Source	Destination	Protoco	Length Info		and the second sec	-
12000-1	182.168.217	3 102,160,10.	10. TCP	58 37429 - 11	35 [SYN] Seque Minut	824 Lennik #55=1469	
5466	192.168.18.	10 192.168.217	10 TCP	54 135 - 374	29. [RST, ACK] 5eq=1	Ack=1 W1N=0 Len=0	
ISHOO	192.108.19.	10 192,368,237	.1 TCP	58 21 - 37425	9 [SYN, ACK] Sec-8 /	ck=1 Win=29290 Lenn8	and the second s
7188	192.188.217	.2 103.16B.18.	ter rcp	5E 37429 - 21	56 [SYN] Seq=# Win=1	1824 Lon=8 MSB=1468	
19006	192.168.10.	30 192,100,237	10 TOP	54 256 H d74	29 [RST, ACK] Seg-1	Ackel Wines Lunes	Contraction of the local division of the loc
1100	100.168.21	3 192.108.18	10 TCP	58 57429 - 1	U SYN SUCCE WIND	4024 Loneo 808-1460	
\$3280	192.168.18	10 102-100-217	a tur	54 113 - 374	28 [RST, ACK] Begs1	Ack=1 Win=8 Len=0	
1700	192.166.217	18 182.168.18.	10 TEP	58-37429 5	54 [SYN] Beg=0 Win=1	1824 Len:8 M58=5468	
17700	192.168.18.	10 102.168.217		24 354 - 374	29 [KS1, ACK] Segel	Act-1 Winter Lunte	
8408	192 168 18	18 1924108 217	13 TOP	54 1720 - 87	429 NST. ACK1 Beg-1	Actes Wines Lenet	
50.00	192:358.217	13 102,168.18.	10 TCF	58 37429 - 54	07 (SYN) Segra Mines	624 Laura M55-1460	
3780	192,168.10.	10 102.160.217	.3 TCP	54 567 - 274	29 [RST, ACK] Seg=1	Ack*1 Win=9 Len=0	
10201	103 155 10	10 102 169 217	10 100	54 000 - 174		Actual Winter Land	
	11000						
> Era	me 1: 66 byte	s on wire (528 bits),	66 bytes captur	ed (520 bits) on	interface 0	0.8332-201	
> Eth	ernet II, Sro	: Microsof_48:57:1e (	88:15:5d:48:57:1	ie), Dst: Microsof	_48:57:00 (00:15:5d:	:48:57:8c)	
• 4000	nemission Con	tre: Protucol Mrc Ro	rt: Mil Unt Hort	221148 Sent 1.	Artho L. Lenr &		
	00 15 5d 40	57 0c 00 15 5d 40 57	1e 86 00 45 00	]@/]@/]	E,		
		40 08 40 06 45 67 60	a8 8a 02 c8 a8	.4	**		
0010	00 34 00 00	CONTRACTOR AND ADDRESS OF TAXABLE AND ADDRESS OF TAXABLE ADDRESS OF TA	States and a second state of the second states and the				
0010 0020 0030	00 34 00 00 0a 6a 20 15	00 4# 6f c# 41 75 bb	47 5C FA 80 11				and the second se
0010 0020 0030 0040	00 34 00 00 0a 0a 20 05 22 02243 00	00 40 61 68 41 76 66 00 80 61 81 88 88 56	1 47 50 fa 80 11 29 at #4 46 42	C	re		vinte Wir daws
0010 0020 0030 0040	00 34 00 00 0a 0a 20 05 02 02 43 00 70 62	00 40 87 68 41 75 00 00 88 01 81 88 88 50	1 47 50 74 80 51 29 84 84 46 42	C P].1	FB		onte Windows Setterge ta activate Window
0010 0020 0030 0040	00 34 00 00 9a 6a 20 05 82 02243 an 76 45	00 40 6f c0 41 75 05 00 80 01 01 80 08 50	1 47 50 TA 80 15 29 04 ## 46 42	5 N. ALG C P] I	FB.		onte Windows Settinge to activate Window
0010 0020 0030 0040	00 34 00 00 9a 9a 20 05 12202245 an 76 45	60 AN AT CH 41 75 66 00 AN AT CH 48 AN AN A	1 47 50 74 88 35 29 44 44 48 42	25. N AN. ON. C			onte Wir dows Getinge te activate Window
0010 0020 0030 0040	00 34 00 00 0a 8a 20 05 17 62 45 an 76 45	60 AN AT CH AI 75 66 00 AN AI DI AN AN AN A	1 47 50 74 80 35 20 44 44 48 42	22 5 N. AH.O. C. P3.1			onte Windows Settinge to activite Window

*Figure 8 Continued screenshot of wireshark results ran on 192.168.10.10 (Ubuntu) while 192.168.217.3 (Attacker Linux) scanned the network for Task A.2* 

	Ringel	y a ritigilay filter							Expressio	0R	•
	- N:	Source	Destination	Protocal	Length info		- AND REAL PROPERTY.	LINE SHIT	Contrastice.		-
	67899	1021168.10.2	192,368,18,18	TOP	100 TEP Netra	nselsstel) 53	- 31426 IAIN	PSH,	ACK 5	eur	
-	135500	192.165.10.10	192,108,10,2	100	24 37420 - 23	ficarl ned-se	with-0 Cout-0	and services.	ALC: NO.		
	39399	192,168,18,10	192,160,10,2	TCP	54 52994 - 53	IRSTITUTE: 30	Mintel Lenne	dense ord	and a second second		
	966699	102.168.10.2	102-108-10.20		100 DCF Actru	minutention (HBS	- 42004 [FIN	L PBH	ACK 1 1	en	80
-	16500	152.168.18.10	102.108.10.2	TOP	54 52054 - 53	[RST] 9eq=30	Winto Lento				
	01500	182/201-10/2	182-169-18-28	TOP	100 HIGH Retro	or out the party of the party o		ç enarç	NACK 1 1	-	
	11499	192.108.19.19	192.308.10.2	THE	160 FYC9 Bobra	restanted 45	atui-a reu-a	Distant.	APRIL D		
	87500	192,168,18,19	192.168.10.2	TCP	54 37426 - 53	Rott Segras	Win-B Len-D	1.11	Contractor of		
	65899	192-160-18-2	192,468,49710		160 EXCR Retra	ninitiasia on hida	DH 52894 FEN	N PSH	ACK S	ett.	
	87999	192.108.18.18	102.155.18.2	TCP	54 52094 53	[RST]=5eq=38	WIN+8 Len+8				
-	576488	192,368,10,20	- 102.108.10.10	TCP	100 PTCP Retra	newseepen mess	52094H[EIN	, PSH,	ACK] B	1011	
7 1	0700	195-100-10-10	192,198,1972	TUP	.04 02014 → 0J	THEAT BEAGING	WIN-0 Lenvo	and second	COMPANY OF	1.0	
4	01100	192 168 18 10	192,168,16.2	TCP	54 37426 - 53	INSTI-Section	Minch Lence	un rong	in the second	eur .	
	06500	102/108/10/2	102/108/10/10	ITCP	100 LTCH Retru	INTERNAL STATEMENT	TADB FETN	L PRINT	AOCH 1	0.00	
6	· Fran	e 2002: 66 bytes on	wire (528 hits), 6	6 bytes capt	tured (528 bits) o	n interface 0	15-54-45-57-2	101			
	• Fram • Ethe • Inte	e 2002: 66 bytes un rmet II, Src: Micros rmet Protocol Versio mitteson Control Pro	wire (520 bits), 6 of 40(57)1# (0011 n 4, 5rc: 192.108 recolmente for for the	6 bytes capt 15d:40:57;1e 10.2, Dst: 1	tured (520 hits) o ), Dat: Microsof_ 162.100.10.10	n interface ( 40:57:0c (00) Ackt 2, Lent	15:5d:40:57:8	ic)		•	
	• Fram • Ethe • Inte	e 2092: 06 bytes on rmet II, Src: Micros rmet Protocol Versio	Mire (520 hits), f of 40:57:14 (00:11 n 4, Src: 192.108	6 bytes capt 15d(40:57)1e 10.2, Dst: 1	tured (520 bits) o ), Dat: Microsof (52.100.10.10 57544, Bog: 20,	n interface 0 40:57:0c (00) Ack: 1, Len:	15:5d:40:57:0	ic)			
	<ul> <li>Fram</li> <li>Ethe</li> <li>Inte</li> </ul>	e 2092: 66 bytes un rmet II, Src: Microso rmet Protocol Versio rmet Protocol Versio rmet State Contemported 00 15 5d 40 57 0c 00 00 34 00 00 40 00 40	Mire (520 hits), f of 40:57:1e (00:11 n 4, Src: 192 108 10001, frc Forti 15 5d 40 57 1e ( 06 a5 67 cp a8	6 bytes capt 155(.40:57.1e 10.2, Dst: 1	Lured (520 hits) o ), Dat Microsof 192.100.10.10 	n interface () 40:57:0c ()0 ACK1 2, 1991	15:5d:40:57:8	ic)		•	
	• Fram • Ethe • Inte	e 2002: 66 bytes on rrest II, Src: Nicros rrest Protocol Versio rest Protocol Versio 00 15 54 40 57 0c 00 00 34 00 00 40 00 40 80 80 00 34 00 00 40	Mire (520 bits), f of d015718 (6013 n d, Brc: 192 108 100 bits 192 108 15 5d 40 57 18 0 06 a5 67 c0 a8	8 bytes capt 15d 40:57 10 10.2, Ost: 1 10.2, Ost: 1 00 00 45 00 10 02 c0 a8	Lured (520 bits) o ), Dat: Microsof (92.100.10.10 57544, Seq. 55 	n interface ( 40:57:9c (00)	15:5d:40:57:8	ic)		•	
	<ul> <li>Fram</li> <li>Ethe</li> <li>Inte</li> <li>6000</li> <li>6028</li> <li>6838</li> </ul>	e 2002: 66 bytes on freet II, Src: Micros freet Fractocol Versio entres for Goldania (1997) 00 15 5d 40 57 0c 90 06 34 00 00 46 06 40 88 6 50 jenuto 13	Mire (520 bits), 4 of 40 57 1e (00:11 n 4, Srci 192 108 tocol, Hrc Porti 15 5d 40 57 1e ( 06 a5 57 CD a0 01 bit 20 50 55 cd	6 bytes capt 15d 40:57 10 10.2, Dst: 1 10.2, Dst: 1 00 00 45 00 10 02 c0 a0 10 50 11 10 11	Lured (52% bits) o ), Det Microsof 192 100 10 10 192 100 10 10 193 44, Ben 34, 10W. 10W. 10 4.0 0 0 0	n interface ( 40:57:0c (00) Active Lent	15:5d:40:57:8	ic)		•	
	<ul> <li>Fram</li> <li>Ethe</li> <li>Inte</li> <li>Inte</li> <li>0028</li> <li>0028</li> <li>0040</li> </ul>	e 2002: 66 bytes on rrest II, Src: Micros rrest Fractocol Versio 00 15 5d 40 57 0c 00 00 34 00 00 40 00 00 88 80 10 0 00 00 00 10 88 00 11 54 00 00	Mire (520 bits), 4 of 40157 1e (6013 14, Srci 192 108 150 5d 40 57 1e ( 06 a5 67 C0 a8 10 b2 76 20 55 11 m 05 m 56	8 bytes capt 15d 40 57 10 10 2, 0st 1 10 01 00 0 1 0 00 45 80 0 02 c0 a8 1 50 0 1 1 50 0 0 1 1 50 0 0 0 0 1 50 0 0 0 1 50 0 0 0 1 50 0	ured (520 bits) o ), Dat Microsof (52 100 10 10 	n interface ( 40:57:6c (00) Acti 1, 1441	15:5d:40:57:8	ic)	Acto	• exte V	Virdaws.
	<ul> <li>Fram</li> <li>Ethe</li> <li>Inte</li> <li>Inte</li> <li>6000</li> <li< td=""><td>e 2002: 66 bytes on rreet II, Src: Mirros rreet Fractocol Versio 00 15 5d 40 57 0c 00 00 34 00 00 40 00 40 80 80 90 54 00 00 16 80 91 54 00 00 42</td><td>Mire (520 bits), 4 of 40157 1e (0011 n 4, Src 192 108, 50001, Fre Port 15 5d 40 57 1e ( 06 05 67 c0 05 01 08 66 50 55</td><td>6 bytes capt 155(40:57)16 19.2, Dst: 1 19.2, Dst: 1 05 00 45 00 10 02 c6 48 30 14 7</td><td>Lured (520 bits) o ), Dat: Microsof (92.300.10.10 57544, Reg. 50 .](W</td><td>n interface ( 40:57:60 (00) ACUT 1, Lent</td><td>15:5d:40:57:8</td><td>ic)</td><td>Ac0 (0.1</td><td>ewter V</td><td>Vir daws</td></li<></ul>	e 2002: 66 bytes on rreet II, Src: Mirros rreet Fractocol Versio 00 15 5d 40 57 0c 00 00 34 00 00 40 00 40 80 80 90 54 00 00 16 80 91 54 00 00 42	Mire (520 bits), 4 of 40157 1e (0011 n 4, Src 192 108, 50001, Fre Port 15 5d 40 57 1e ( 06 05 67 c0 05 01 08 66 50 55	6 bytes capt 155(40:57)16 19.2, Dst: 1 19.2, Dst: 1 05 00 45 00 10 02 c6 48 30 14 7	Lured (520 bits) o ), Dat: Microsof (92.300.10.10 57544, Reg. 50 .](W	n interface ( 40:57:60 (00) ACUT 1, Lent	15:5d:40:57:8	ic)	Ac0 (0.1	ewter V	Vir daws
	+ Fram + Ethe + Inte + I	e 2002: 66 bytes on freet II, Src: Micros renet Fractocol Versio mission Goltrati Ven 00 15 56 40 57 0c 90 00 34 00 00 40 00 40 00 34 00 00 40 co 40 00 34 00 00 40 co 40 00 34 00 00 40 co 40 00 40 50 m 00 51 m 00 41 54 6m 00 57 m 55	Mire (520 bits), 4 of 40:57 1# (00:11 n 4, Src:192 108 tocol, inc Perti 15 0d 40 57 1# ( 06 a5 67 C0 a8 ( 01 ba 76 28 55 ( 01 m 04 61 55 )	8 bytes capt 154 40 57 14 19 2, Det 1 1, Det Wrtt 10 00 45 00 10 00 45 00 10 00 45 00 10 00 45 00	Lured (520 bits) o ), Dat Microsof 197.100.10.20 5.544, Hou 34, 	n interface ( 40:57:00 (00) ACU 1 L Lenn	15:54:40:57:1	ic)	Ac0 012	vate V	Vir daws - 1- scheite Wikas
2	<ul> <li>Frame</li> <li>Ethe</li> <li>Inte</li> <l< td=""><td>e 2092: 66 bytes on rrest 11, Src: Micros rrest 71, Src: Micros rest Fractocol Versio 00 15 5d 40 57 0c 00 00 34 00 00 40 00 40 8n 8n 90 40 40 40 40 40 40 40 40 8n 8n 90 40 40 40 40 40 40 40 40 40 8n 8n 90 40 40 40 40 40 40 40 40 40 40 8n 8n 90 40 40 40 40 40 40 40 40 40 40 40 8n 8n 90 40 40 40 40 40 40 40 40 40 40 40 40 40</td><td>Mire (520 bits), 6 of 40157 1e (6013 n 4, Srci 192 108 tool, nrc 193 108 tool, nrc 1</td><td>8 bytes capt 194 40 5714 197 20 5714 197 20055000000000000000000000000000000000</td><td>Ured (520 bits) o ), Dat: Microsof (52 100 10 10 5/544, Neu: 30 .](W](WE 4.00 0 </td><td>m interface ( 40:57:66 (00) ACE: 1, 1997</td><td>15:54:40:57:8</td><td>ic)</td><td>Acti (015)</td><td>varia V Senog</td><td>Vir daws.</td></l<></ul>	e 2092: 66 bytes on rrest 11, Src: Micros rrest 71, Src: Micros rest Fractocol Versio 00 15 5d 40 57 0c 00 00 34 00 00 40 00 40 8n 8n 90 40 40 40 40 40 40 40 40 8n 8n 90 40 40 40 40 40 40 40 40 40 8n 8n 90 40 40 40 40 40 40 40 40 40 40 8n 8n 90 40 40 40 40 40 40 40 40 40 40 40 8n 8n 90 40 40 40 40 40 40 40 40 40 40 40 40 40	Mire (520 bits), 6 of 40157 1e (6013 n 4, Srci 192 108 tool, nrc 193 108 tool, nrc 1	8 bytes capt 194 40 5714 197 20 5714 197 20055000000000000000000000000000000000	Ured (520 bits) o ), Dat: Microsof (52 100 10 10 5/544, Neu: 30 .](W](WE 4.00 0 	m interface ( 40:57:66 (00) ACE: 1, 1997	15:54:40:57:8	ic)	Acti (015)	varia V Senog	Vir daws.

*Figure 9 Continued screenshot of wireshark results ran on 192.168.10.10 (Ubuntu) while 192.168.217.3 (Attacker Linux) scanned the network for Task A.2* 



*Figure 10 Continued screenshot of wireshark results ran on 192.168.10.10 (Ubuntu) while 192.168.217.3 (Attacker Linux) scanned the network for Task A.2* 

# 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.

*Figure 11 Screenshot of ping of 192.168.10.10 (Ubuntu) on 192.168.217.3 (Attacker Linux) prior to firewall rule set for Task B.1* 

The above screenshot shows the ping command results for 192.168.10.10 (Ubuntu) on 192.168.217.3 (Attacker Kali) prior to the firewall rule below being applied in pfSense. All 7 packets received.

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
1	WAN	Block	192.168.217.3	192.168.10.10	ICMP

Figure 12 Table 1 for Firewall Rule for Task B.1

Ploense.CYSE.com - Firewalt: Rules: WAN - Modills Firefox       Image: CYSE.com - Firewalt: Rules: WAN - Modills Firefox         Image: ploense.CYSE.com - Firewalt: Rules: Branch - Disconsection       Image: Rules: Rule - Rules: Rules: Rules: Rule - Rules: Rule - Rules:	
Implience CYSE.com +F × +	0
Image: Index//192.158.10.2/Merewall_state_php?fr=xxin       Image: Comparison of the index	
D Nessus Home Kali Linux Kali Docs Kali Toola Exploit DB O Most Visited Result / Introducing Interturges name served appear backeting intertown methatemer relating on the background.          Montor the filter reloct progress.         Foatorg       WAN       LAN         Rules (Orag to Change Order)       Port Destination       Port Gateway Queue Schedule Description       Actions         X       0/0 II       Reserved Not assigned by IANA       *       *       Block bogon networks       *         X       0/0 II       Reserved Not assigned by IANA       *       *       none       Task B #1 External Kali ULMAP)       *         X       0/0 II       IPv4+6*       WAN het       *       *       none       Task B #1 External Kali ULMAP)       * <td>=</td>	=
Member the filter relace program.         Posting WAN LAN         Rules (Drag to Change Order)         States       Protocol       Source       Post Destination       Post Gateway Queue       Schedule       Description       Actions         ×       0/01       *       Reserved Not assigned by IANA       *       *       *       Block bogon networks       *         ×       0/01       *       Reserved Not assigned by IANA       *       *       *       *       Block bogon networks       *         ×       0/01       *       Reserved Not assigned by IANA       *       *       *       *       *       Block bogon networks       *         ×       0/01       *       Post Bit 1217.3       *       192.168.10.10       *	
Rules (Drag to Change Order)       Rules (Drag to Change Order)         States       Protocol       Source       Port       Destination       Port       Eateway       Queue       Schedule       Description       Actions         X       0/0.0       *       Reserved Not assigned by INNA       *       *       *       *       Block bogon networks       Intervention         X       0/0.0       IPv4       192.168.10.10       *       *       none       Task B #1 External Kait       Jule       Jule         X       0/0.0       IPv4+6*       WAN net       *       *       *       none       Task B #1 External Kait       Jule       Jule       Jule       Intervent	
Rules (Drag to Change Order)         States       Protocol Source       Part Destination       Port Gateway Queue Schedule Description       Actions         X       0/0 B       *       Reserved Not assigned by INNA       *       *       *       Blick bogon networks       ©         X       0/0 B       IPP44       192.168.217.3       *       192.168.30.10       *       *       none       Task B #1 External Kat to Ubantu (ICMP)       ©       ©         X       0/0 B       IPV4+6*       WAN net       *       *       *       none       Open Construction IPV4       U// C	
Rules (Drag to Change Order)       Post States       Post Destination       Post Eateway       Queue       Schedule       Description       Actions         X       0/0 B       *       Reserved Not assigned by IANA       *       *       *       *       Block togon networks       *         X       0/0 B       (Py-4) CAMP Block       192.168.30.10       *       none       Task B #1 External Kail to Ubuntu (ICMP)       *       *       *       none       Task B #1 External Kail       * </td <td></td>	
Rules (Drag to Change Order)       Part Destination       Port Eatency Queue Schedule Description       Actions         X       0/011       *       Reserved Not assigned by IANA       *       *       *       *       Block bogon networks       *         X       0/011       *       Reserved Not assigned by IANA       *       *       *       *       Block bogon networks       *         X       0/018       IPV4       192.168.30.10       *       *       none       Task B #1 External Kail to Ubuntu (ICMP)       *	
States     Protocol     Source     Port     Destination     Port     Eateway     Queue     Schedule     Description     Actions       ×     0/0 B     *     Reserved Not assigned by IANA     *     *     *     *     Block togon networks     ©       ×     0/0 B     IPv4     192.168.10.10     *     *     none     Task B #1 External Kall     ↓ ✔ ID       ∞     20/4.43     Bv4+6*     WAN net     *     *     none     Open Connection B*4     ↓ ✔ ID	
X         0/0 II         Reserved Not assigned by INNA         *         *         Block bogon networks         Q           Image: State of the stat	
★         0/0.8         IPv4 ICMP arg         192.168.217.3         192.168.30.10         none         Task B #1 External Kai to Ubumtu (ICMP)         ↓ / □	
🖂 🛩 20/4.43 IBV4+6* WAN net 🔹 🔹 none Open Connection IBV4 🕹 🖉 💭	
MB and IPv6 O D	
T ALC 1 ALL B LAND B LAND & MARCH	
	activate Wind
0	
	-

Figure 13 Screenshot of firewall rule from table 1 being created and set for Task B.1

The above screenshot shows the previous table being created and set in pfSense which will be tested below to ensure effectiveness.



*Figure 14 Screenshot of ping of 192.168.10.10 (Ubuntu) on 192.168.217.3 (Attacker Linux) after firewall rule from Table 1 was set and applied for Task B.1* 

The above screenshot shows the ping command results for 192.168.10.10 (Ubuntu) on 192.168.217.3 (Attacker Kali) after the firewall rule was applied in pfSense. All 16 packets were lost.

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



Figure 15 Screenshot of pinging of LAN Side, which consists of 192.168.10.2 (pfSense), 192.168.10.10 (Ubuntu), and 192.168.10.11 (Windows Server 2008) on 192.168.217.3 (Attacker Linux) prior to firewall rule set for Task B.2

The above screenshot shows the ping command results for the entire LAN side consisting of 192.168.10.2 (pfSense), 192.168.10.10 (Ubuntu), and 192.168.10.11 (Windows Server 2008) on 192.168.217.3 (Attacker Kali) prior to the firewall rule below being applied in pfSense. 4 packets on each LAN Side ip address were received.

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
1	WAN	Block	192.168.217.3	LAN Side	ICMP

Figure 16 Table 2 for Firewall Rule for Task B.2

optications +	Plac	m - 01	Firefax Li	+	International Academics	e Kali y Ditertigi	Worksta		a.x9			1.	# C	
			-	pfSett	ie.CYS	E.com - Firm	valt F	lutes: WA/	N-Mozilla Fir	efox		0	0	0
🕲 piSer	iei.CYS	E.Lung (Fill)	* +											
(e) 🕫	C 6	5	0.6.1	npi//192.168.10.7	bhiov	witz nation proj	ht:-n	án)		5 4		8/	D	=
O Ness	in Hom	e 🔨 Kali Li	na 🔨 Kal	Docs 🥆 Kali Too	dy . 💌	Exploit-DB	<b>0</b> M	ost Visited	D Nessus /	initializing				
	_				_	-	_					-		
2	The	ctionges have	been apple	d auccessfully. The f	frewait	rules are soon	retio	ding in the)	background.			ж		
	Mon	the near	mova brođu											
•	(inclusion)		-											
	1 104.0	ng wat	LAN											
	Rul	es (Drag te	o Change	Order)										
M		States	Protocol	Source	Part	Destination	Port	Gateway	Queue Sche	dule Description	Actions			
20		× 1/08		Reserved		*				Block bogon networks	٠			
				Not assigned by IANA										
1	0	K 0/08	1Pv4	192.168.217.3		LAN net	٠		none	Task 8 #2 External Kall to	211	0		
3			ICMP ICX							LAN Side (ICMP)	OB			
		227/1.40	IPv4+6*	WAN net	٠		٠		none	Open Connection IPv4	211			
		MB								and IPv%	OB			V daws
									1	1 and 🗿 Dene 🔒 Law	+	-		
	0													-
		(HING)	1			-		1.02	-			- 2		11 P A M 2
		- 26 DEDI					1							<b>6</b> PU

Figure 17 Screenshot of firewall rule from table 2 being created and set for Task B.2

The above screenshot shows the previous table being created and set in pfSense which will be tested below to ensure effectiveness.

polications =	Places +	🖾 Terminai 🗧	a standard generating working	un un Adentidate 🛛 🖉 🔺	. INI	# / 40-	
			root@CS2APe	inTest: -	100	000	
File Edit	Wew Se	tarch Terminal Hel	P.:				8
PING 192	.168.18.2	(192.168.18.2) 1	66(84) bytes of data.				
192.	165.10.2	ping statistics	ile 1. Mart Laudick Vices Street Marte				
13 packe	ts transm	utted, o received	1, 100% packet toss, time 242%	5			
PING 192	.168.16.1	# ping 192.168.1 0 (192.168.10.10)	(0,10 56(84) bytes of data.				
-C 192.	168.10.10	ping statistics					
12 packe	ts transm	ditted, 0 received	I, 100% packet loss, time 91ms				
PING 192	Mextert	# ping 192.168.1	0.11 56(84) bytes of data.				
°C 182	145 10 11	ning statistics					
15 packe	ts transe	itted, 0 receiver	1, 100% packet loss, time 63ms				
2							
						an Matanasan	Carlester.
						Go to Settings	ddws. Factivate Windows.
						1.1.1	
E.							
		- Guarth		15 II 18 III 18			9 0 8 SIST

*Figure 18 Screenshot of pinging of LAN Side, which consists of 192.168.10.2 (pfSense), 192.168.10.10 (Ubuntu), and 192.168.10.11 (Windows Server 2008) on 192.168.217.3 (Attacker Linux) after firewall rule from table 2 was set and applied for Task B.2* 

The above screenshot shows the ping command results for the entire LAN side consisting of 192.168.10.2 (pfSense), 192.168.10.10 (Ubuntu), and 192.168.10.11 (Windows Server 2008) on 192.168.217.3 (Attacker Kali) after the firewall rule was applied in pfSense. All packets sent to each LAN Side ip address were lost (12 packets to pfSense, 12 packets to Ubuntu, and 15 packets to Windows Server 2008).

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.



*Figure 19 Screenshot of pinging of LAN Side, which consists of 192.168.10.2 (pfSense), 192.168.10.10 (Ubuntu), and 192.168.10.11 (Windows Server 2008) and ftp command on 192.168.10.10 (Ubuntu) on 192.168.217.3 (Attacker Linux) prior to firewall rule set for Task B.3* 

The above screenshot shows the ping command results for the entire LAN side consisting of 192.168.10.2 (pfSense), 192.168.10.10 (Ubuntu), and 192.168.10.11 (Windows Server 2008) and the ftp command was used on 192.168.10.10 (Ubuntu) on 192.168.217.3 (Attacker Kali) prior to the firewall rule below being applied in pfSense. 2 packets on each LAN Side ip address were received and the ftp was logged in successfully.



*Figure 20 Screenshot of using the ftp command for 192.168.10.11 (Windows Server 2008) on 192.168.217.3 (Attacker Linux) prior to firewall rule set for Task B.3* 

The above screenshot shows the the ftp command results 192.168.10.11 (Windows Server 2008) on 192.168.217.3 (Attacker Kali) prior to the firewall rule below being applied in pfSense. This was unable to fit in previous screenshot. Connection was established with 192.168.10.11.

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
1	WAN	Pass	192.168.217.3	192.168.10.11	FTP/21
2	WAN	Block	192.168.217.3	All	All

Figure 21 Table 3 for Firewall Rule for Task B.3

Antantiona	Pla	ces.	- 0	Firefox E		NES.	ekin tahu tahuni b	metata	n thr Adress	1		107	-12	1.	0.0	
	_	_	_	_	ptSe	me.C	YSE.com - Firew	rafi: Rub	en WAN-	Mozilla F	irefax			0		
🖀 pisere	se.CYS	SE:0	om - Fill	× +												
$\leftarrow \rightarrow$	G.	ŵ		@ 🗛	https://192.168.1	0.2/10	ewall_rules.php	11famun				O 🕁		10	D =	
O Nesau	IN Hon	ne *	Kali Li nger niv the filter	intox 🔨 Ka v unter appr reliced prog	ali Doca 🥆 Kali T ani successi uny in press.	oots or men	<ul> <li>Exploit DB</li> <li>Exploit at a nuw</li> </ul>	Ø Moet	Visited ground use	> Nesaut xgrounu	(Initializi	ng		×		*
	Float	ting	WAN	LAN												
	Ru	les	(Drag t States	o Change Protocol	e Order) Source	Port	Destination	Port	Galeway	Queue	Schedule	Description	Actions			
		×	8 <i>1</i> 08		Reserved Not assigned by IANA	•	•	4	•	•		Block bogon networks	٥			
	0	~	0.70 8	IPv4 TCP	192.166.217.3	\$	192,168,10,11	21 (FTP)	•	none		Took B #3 External Kali to Windows Server 2008 (FTP)	00	Ø		
	0	×	0/0B	iP <sub>P</sub> 4*	192.168.217.3	3	LANinet	S.*		none		Task B #3 External Kali to LAN Side (ALL Traffic)	00	۵		
		4	14 /9.12 MB	iPv4+£ ₄	WAN net	×	39	54	•	hone		Open Connection (Py4 and (Py6	00	a ah		Hows Eacthate Window
											1.000		-	-		

Figure 22 Screenshot of firewall rule from table 3 being created and set for Task B.3

The above screenshot shows the previous table being created and set in pfSense which will be tested below to ensure effectiveness.



*Figure 23 Screenshot of pinging of LAN Side, which consists of 192.168.10.2 (pfSense), 192.168.10.10 (Ubuntu), and 192.168.10.11 (Windows Server 2008) on 192.168.217.3 (Attacker Linux), also ftp command on 192.168.10.10 (Ubuntu) after firewall rule from table 3 was set and applied for Task B.3* 

The above screenshot shows the ping command results for the entire LAN side consisting of 192.168.10.2 (pfSense), 192.168.10.10 (Ubuntu), and 192.168.10.11 (Windows Server 2008) and the ftp command was used on 192.168.10.10 (Ubuntu) on 192.168.217.3 (Attacker Kali) after the firewall rule was applied in pfSense. All packets on each LAN Side ip address were lost (7 packets for pfSense, 5 packets for Ubuntu, and 5 packets for Windows Server 2008) and the ftp timed out connection.



*Figure 24 Screenshot of ftp command for 192.168.10.11 (Windows Server 2008) on 192.168.217.3 (Attacker Linux) after firewall rule from table 3 was set and applied for Task B.3* 

The above screenshot shows the the ftp command results 192.168.10.11 (Windows Server 2008) on 192.168.217.3 (Attacker Kali) after the firewall rule was applied in pfSense. The connection was still able to be established with 192.168.10.11.

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



Figure 25 Screenshot of nmap command from Task A.1 being used with firewall rules from Task B.3 still in place and the results returned in Attacker Linux for Task B.4

The above screenshot shows the nmap command that was used in Task A.1 but with the firewall rules applied from Task B.3. The results only showed information for 192.168.217.3 (Attacker Kali), which is the machine that is currently running. It shows that 4 IP addresses were checked but only the host is up. With this lack of information, nmap was ran again, but using the LAN side ip addresses separately below.



*Figure 26 Screenshot of nmap command from Task A.1 separately applied to each ip address being used with firewall rules from Task B.3 still in place and the results returned in Attacker Linux for Task B.4* 

The above screenshot shows the individual results of each LAN side ip addresses and gave more details than the previous screenshot. This time when the nmap was ran, the LAN side responded "Host seems down. If it is really up, but blocking our ping probes, try -Pn", so firewall rules blocked nmap from working on the LAN side ip addresses.

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

	Nessus Essen	hais / Folders / View Scan - Mod	INTE - ILLEGON				. <del>G</del> . G		
Nexus Essential	UFBUL X +								
+ - C @	A https://iocalhost#834/4/sta	is/reports/SNutterabilities		87%	0	Ŷ	IN D	=	
D Neslus Home	Kall Limix 🗙 Kall Docs 🥆 Kall Tools 🍝 Es	pipit-DB O Most Visited D M	lessus ( Init	Delizing					
	O Territo de arter	ett plat find. Die tere is vere plat here	e eduration.					-	
Dessus	Net Street						🚺 erre	0	
· Hylans	Extra Credit NESSUS Scan		Configure	Aust Ind	Lane	• Raper •	Due!		
<ul> <li>all States</li> <li>Texts</li> </ul>	Han 1. Westellins In Revision-	a han a hand a							
	Past +	and the							
O Police	I See . Note:	Family	Cart	0	Scan Details	-			
Physic Fisher	😳 🚺 💷 Manual Westari Multipe Incert	Windows			Putos	Sam Newsel, Sam			
in the second se	11 Territor (Matter Incom	Web Second	3		boever.	Local Suprem Takes at 12:25 PM			
B Connucty	Comment of the Margan Issues	General			End	Teday at 12:35 PM U wantee			
Plage Remain for	🗇 📰 🧃 jaj Manach Wednes (Matkie Incent	Max	18						
	O CO Museo Winasa Perse Dening P	Wridows	1		Yaheesakiitiin			- 51	
	ESS Gettigen Signal Links Wash Ha	German				• Cetta			
	1 TES Wester 1 & Process Deverses	Service advance	196				Activist	e Wie dow	
	C Sens beautroper law an.	1944	- i		-				
	DCE Senses Examples	Widews	1						

Figure 27 Screenshot from Nessus scanning of 192.168.10.11 (Windows Server 2008) to show vulnerabilities

The above screenshot shows the Nessus vulnerability scan on 192.168.10.11 (Windows Server 2008). The vulnerabilities came back 28 total and varies in the severity. The screenshot below shows one of the mixed serverities and how it is subdivided.

-	(D. D. Jatim (darality) and a state		Serence 1	10.00	in the second	e	10.00	
A CW	Kali Jana & Kali Dara & Kali Taris	Emist DB A Marthiated D	Nesson Thereid	interioria.			ы. Ш	-
Actus moute 2	Gibertaa	eter with your beal. Citic ferents also put item	Netsus / messe	ating.				
nessus	255US Scana Interimpe					1	atten (	8
My Buarry	Extra Credit NESSUS Scan / Mic	rosoft Windows (Multip	Datase	Auto	(Lane -	Bages *	Equit	~
Al Loans	mote i Vulverabilities is Hanacha	and a Mater 1 Hang 1						
1 her	(married and a strength							
O Puters	Contract Name +	Firsh: c	Gent -	0	Scen Denete			
Page Human     Samuela     Samuela     Connuclio     Page Human Na.	Mensue RDP HCE ICVE 2019-019	B (F. Without			Poler	Basil Newsyl Scan		
	META BALL Vyterskille in Salarise	Coul Wintere	÷.		Status: Camplete Scarreri Limat Sca	Campleonit Local Bolever		
	Transported Minister (1) preside	Winisten	1.1		Ent: Tomy of 10.35			
	MET2 (20) Vorwenziellers in Remain	Des Wooses	- H		Dquet	0 virune		
	C CONTRACTOR Second Update to Man	and Writes	÷.		Vaherstelle			_
	U COM MELSON MANAGEMENT	rif				1	i tigo.	and second
	Alternat Written Wijkkill Auto	ente. Writes				Here Call the Settings	Wiledows or the activate Windo	
	Will Hat Available	Written			-			

*Figure 28 Screenshot of one of the mixed-severity vulnerabilities from the Nessus scanning of 192.168.10.11 (Windows Server 2008).* 

The above screenshot shows the first mixed vulnerability in the previous screenshot and how it is subdivided. This vulnerability shows 3 critical issues, 2 high issues, and 1 medium issue as an example.