OLD DOMINION UNIVERSITY

CYSE 301 Cybersecurity Techniques and Operations

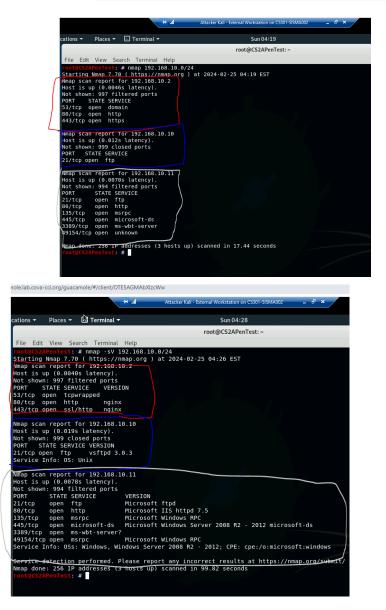
Assignment #3 Sword vs. Shield

Sahmer Ismael 01219271

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.



		tt al	Attacker Kali - External Workstation on CS301-SISMA002	- 8 × /
tions 👻	Places 🔻	🕞 Terminal 🕶	Sun 04:42	1
			root@CS2APenTest: ~	
File Edi	t View Se	arch Terminal Help		
		# nmap -0 192.168.1		
) at 2024-02-25 04:34 EST	
		for 192.168.10.2		
		3s latency).		
	STATE SER	ltered ports		
	open dom			
	open dom			
	open htt			
			able because we could not find at leas	t 1 open and 1 closed port
			sing a closed TCP port so results inco	
	tches for		sing a crosed for porc so resurce inco	mproco
map sca	n report	for 192.168.10.10		
ost is	up (0.007	0s latency).		
		osed ports		
	TATE SERV	ICE		
	pen ftp			
			know what OS is running on it, see htt	ps://nmap.org/submit/).
	ingerprin			
			CU=31240%PV=Y%DS=2%DC=I%G=Y%TM=65DB09B	
			%GCD=2%ISR=10C%TI=Z%II=I%TS=21)0PS(01=	
			NNT11NW7%04=M5B4ST11NW7%05=M5B4ST11NW7	
			3=7120%W4=7120%W5=7120%W6=7120)ECN(R=Y	
			Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+%F=AS%RD	
			DF=Y%T=40%W=0%S=Z%A=S+%F=AR%0=%RD=0%Q= 'L=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G	
) 01 (R=Y%DF=N%T=40%1P DFI=N%T=40%CD=S)	-104%UN-0%KIPL-0%KID=G%RIPCK=G%RUCK=G	
5:⊸RUD=	U)IE(R=1%	DF1-N-81-40%CD=5)		
etwork	Distance:	2 hons		



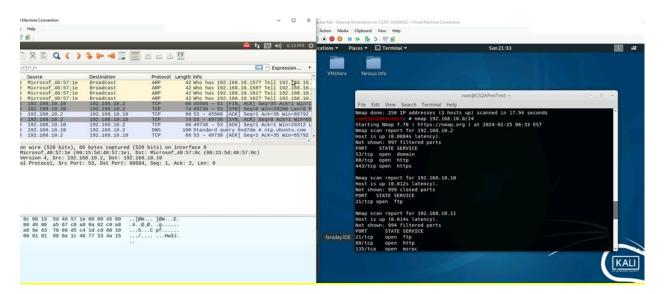
Description: Throughout using Nmap, I was able to locate the Subnet topology, such as the opens port information. The operating systems that the VMs where using, and as well as the services and the backend software's, with each opening port and each VM. Furthermore, I highlighted the different VMS data with different colors.

- Red 192.168.10.2 Pfsense
- Blue 192.168.10.10 Ubuntu

Grey - 192.168.10.11 Window Server 2008

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.

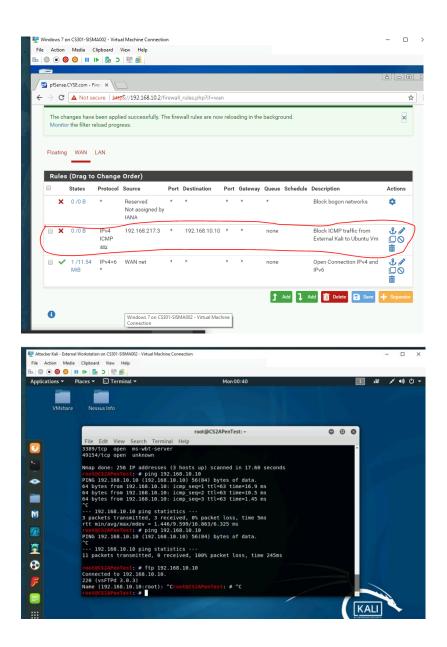


Description: From what I have gathered from the screenshot, is that after running the scan from the External Kali VM, using the command of 192.168.10.0/24 to scan the whole subnet. I was able to locate, the traffic from the Ubuntu VM, and was able to Identify that the Nmap scan was trying to communicate with different ports within the Subnet, and it was displaying a bunch of different source packets, that were running in the background of the scan. One of the protocols that the screenshot, displayed from the scan, is the ARP protocol, which is used to determine which IP addresses are in use within the local network. This message was broadcasted throughout the server, to display who has the 192.168.10.157, and to tell the designated Ip address, which was in this case, IP address 192.168.10.2, about it. Furthermore, the screenshot, displays that Nmap was completing the TCP handshake process, which it was trying to find out about the TCP ports that where in the network, to communicate with. I also examined the protocol Hierarchy statistics tool in Wireshark, and was able to identify, the different types of packets that where going, through the Wireshark tool, and the percentage of the packets being successful.

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

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)
	WAN	Block	192.168.217.3	192.168.10.10	ICMP
1					



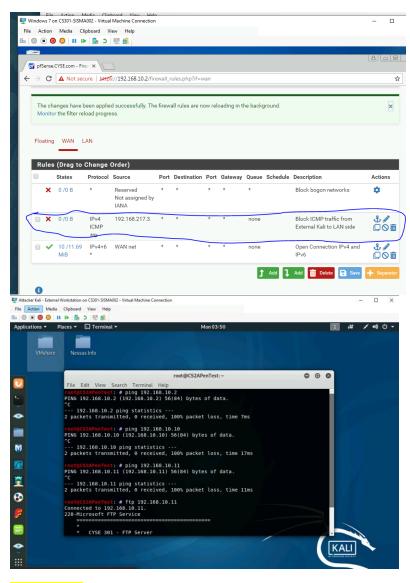
Description: from the screenshots above, I blocked the ICMP traffic, from external Kali to Ubuntu Vm. I showed, before the rule, they were connected, and then after, I showed the ICMP traffic being blocked, after the rule was set. I also accessed FTP packets, to make certain that the rule only blocked ICMP traffic.

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)

1 WAN Block	192.168.217.3	LAN Side	ICMP
-------------	---------------	----------	------



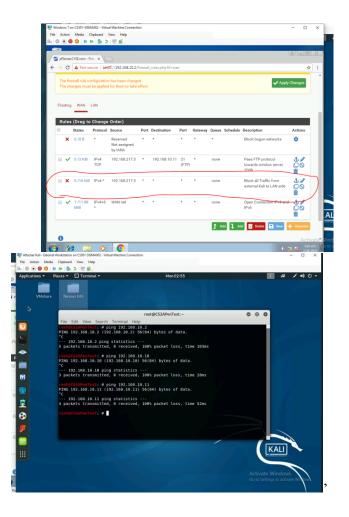
Description: I displayed, me blocking the ICMP traffic, from external Kali to the LAN side, and tested it. Furthermore I also tested the firewall rule, by using FTP, to show only ICMP was blocked.

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.

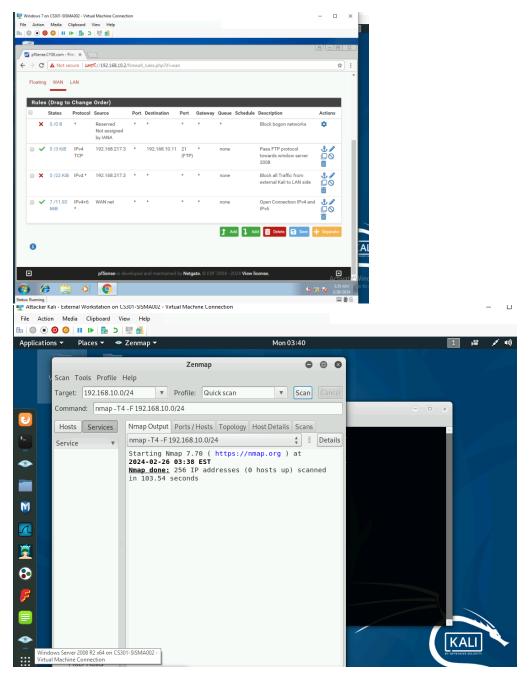
Rule#	Interface	Action	Source IP	Destination IP	Protocol
1	WAN	pass	192.168.217.3	192.168.10.11	ТСР

			V	VAI	Ν			Block		192.	.168	.217.3	Any	Any	
ndows 7 or	n CS301-SISM	1A002 - Virtu	al Machine Connecti	on							×				
Action	Media C	lipboard	View Help												
0	0 0 11 1	l 🔂 5	분 👸												
-										8	~				
pfSense.0	CYSE.com - Fi	irev × \										🐺 Jitador Koli - Esternel Norkstete	n on CS301-95M4002 - Vietual Machine Connection		- D X
→ c	A Not se	cure bit	5 ://192.168.10.2/	firewall_ru	ules.php?if=wai	n				☆	:	File Action Media Clipboa			
				-						_		Applications • Places •		Mon 02:50	1 # /40-
			n has been chang						🗸 Apply 0	hanges					
The cha	anges must	be applied	for them to take	errect.								Whitere Ne	susirio		
Floating	WAN	LAN											root@CS2AJ	PerTest:- O (9 0
												File	Edit View Search Terminal Help		
Rules	(Drag to	Change	Order)									C .	CS1AFeeTest: # ftp 192.168.10.2 dgC17AFeeTest: # ^C g57AFeeTest: # ftp 192.168.10.10		
		Change Protocol		Port D	estination	Port	Gateway	Queue Schedule	Description	Actions			CC1ARenText: # ftp 192.168.10.2 http://www.Text: # ftp 192.168.10.10 cc12/ArenText: # ftp 192.168.10.10 cc22ArenText: # ftp 192.168.20.11		100
	States			Port D		Port		Queue Schedule *				Conn 228- 228- 228-	Coldensity::= ftp 192.168.10.2 http://www.tet: = ftp 192.168.10.10 http://www.tet: = ftp 192.168.10.10 http://www.tet.i = ftp 192.168.10.11 http://www.tet.ii.ii.ii.ii.ii.ii.ii.ii.ii.ii.ii.ii.ii		
		Protocol	Source Reserved Not assigned						Description Block bogon networks	Actions Image: Action series		Cone 220-	CLIANCTINT: # ftp 192.108.10.2 ACCIMPTNT: # ft 192.108.10.10 ACCIMPTNT: # ftp 192.108.10.10 ACCIMPTNT: # ftp 192.108.10.11 ACCIMPTNT: ftp 192.108.10.11 ACCIMPTNT: ftp 192.108.10.11 ACCIMPTNT: ACCIMPTNT: ACCIMPTN: ACCIMPT	-	8
	States	Protocol	Source Reserved									Cone 220-	Coldensity::= ftp 192.168.10.2 http://www.tet: = ftp 192.168.10.10 http://www.tet: = ftp 192.168.10.10 http://www.tet.i = ftp 192.168.10.11 http://www.tet.i = ftp 192.168.10.11 http://www.tet.ice.inter.int	-	8
×	States	Protocol *	Source Reserved Not assigned		•	* 21			Block bogon networks Pass FTP protocol	*		Connormality 220	Schladerberg # trp 192,043.04.2 (Schladerberg # trp 192,043.04.0 Schladerberg # trp 192,043.04.0 Schladerberg # trp 192,043.04.01 Schladerberg # trp 192,043.04.01 Schladerberg # trp 192,043.04.01 Cross # 10 12,240.04.01.0 Cross # 201 - FTP Server Atomynous Access has been enabled.		F
×	States 0 /0 B	Protocol *	Source Reserved Not assigned by IANA		•	*	*	•	Block bogon networks	¢ ↓/		Conn 228- 229- 229- 229- 229- 229- 229- 229-	Exclusioner: # Tp 102.104.10.2 Exclusioner: # Tp 102.104.10.10 Exclusioner: # Tp 102.104.10.10 Exclusioner: Tp 102.104.10.11 Exclusion: Tp 202.104.10.11 Exclusion: Tp 202.104.10.11 Exclusion: Tp 202.104.10.11 Exclusion: Tp 202.104.10.11 Exclusion: Exclusioner: Tp 202.104.10 Exclusion: Tp 202.104.10 Exclusion: Tp 202.104.10 Exclusion: Tp 202.104.10 Exclusion: Tp 202.104.10 Exclusion: Tp 202.104.104 Exclusion:	e-mail name) as password.	5
×	States 0 /0 B 0 /3 KiB	Protocol * IPv4 TCP	Source Reserved Not assigned by IANA 192.168.217.3	* *	* 192.168.10.11	* 21 (FTP)	•	* none	Block bogon networks Pass FTP protocol towards window server 2008	¢ ↓/		Con 7000 700 7000 7	COMMUNITY: # TID 102.108.30. COMMUNITY: # TID 102.108.30.10 COMMUNITY: # TID 102.108.30.10 COMMUNITY: # TID 102.108.30.11 COMMUNITY: # TID 102.108.11 COMMUNITY: # TID 102.11 COMMUNITY:	e-mail name) as password.	1
×	States 0 /0 B	Protocol * IPv4 TCP	Source Reserved Not assigned by IANA	* *	* 192.168.10.11	* 21	•	•	Block bogon networks Pass FTP protocol towards window server 2008 Block ell Traffic from			Conn 228- 229- 229- 229- 229- 229- 229- 229-	COMMUNITY: # TID 102.108.30. COMMUNITY: # TID 102.108.30.10 COMMUNITY: # TID 102.108.30.10 COMMUNITY: # TID 102.108.30.11 COMMUNITY: # TID 102.108.11 COMMUNITY: # TID 102.11 COMMUNITY:	e-mail name) as password.	T
×	States 0 /0 B 0 /3 KiB	Protocol * IPv4 TCP	Source Reserved Not assigned by IANA 192.168.217.3	* *	* 192.168.10.11	* 21 (FTP)	•	* none	Block bogon networks Pass FTP protocol towards window server 2008	¢ ↓/		□ •	Relations: 4 To 102.108.02 Relations and 4 To 202.108.02 Relations and the second se	e abil name) as passurd.	ſ
×	States 0 /0 B 0 /3 KiB 0 /16 KiB	Protocol * IPv4 TCP IPv4 *	Source Reserved Not assigned by IANA 192.168.217.3	* *	* 192.168.10.11 *	* 21 (FTP)	*	* none	Block bogon networks Pass FTP protocol towards window server 2008 <u>Block ell traffic from</u> external Kali to LAN side			□ •	COMMUNITY: # TID 102.108.30. COMMUNITY: # TID 102.108.30.10 COMMUNITY: # TID 102.108.30.10 COMMUNITY: # TID 102.108.30.11 COMMUNITY: # TID 102.108.11 COMMUNITY: # TID 102.11 COMMUNITY:	e abil name) as passurd.	
×	States 0 /0 B 0 /3 KiB	Protocol * IPv4 TCP IPv4 *	Source Reserved Not assigned by IANA 192.168.217.3	* 1	* 192.168.10.11 *	* (FTP) *	*	* none	Block bogon networks Pass FTP protocol towards window server 2008 Block ell Traffic from				Relations: 4 To 102.108.02 Relations and 4 To 202.108.02 Relations and the second se	e abil name) as passurd.	KAUI
×	States 0 /0 B 0 /3 KiB 0 /16 KiB 1 /11.89	Protocol * IPv4 TCP IPv4 * IPv4 *	Source Reserved Not assigned by IANA 192.168.217.3	* 1	* 192.168.10.11 *	* (FTP) *	*	* none	Block bogon networks Pass FTP protocol towards window server 2008 Rlock-all-fraffic from external Kall to LAN side Open Connection IPv4 and			□ •	Relations: 4 To 102.108.02 Relations and 4 To 202.108.02 Relations and the second se	e abil name) as passurd.	



Description: The first set of screenshots, for question 3 display, FTP only passing, through the windows server 2008, and the firewall rule that was used. The second set of pictures for question 3, displays that all the VMS are completely blocked besides, the FTP on windows server.

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



Description: After keeping the same rules on PF sense, from the previous step, and applying a quick scan to Zen map/Nmap, it seems that the subnet topology which include, the port information, operating system, and backend software where all down, due to the firewall rules blocking all traffic, and information from the kali VM.

Extra credit (15 points): Use NESSUS to enumerate the security vulnerabilities of Microsoft Windows

Server 2008 VM in the CCIA network.

pplications 👻 Places 👻 😥		Mon 04:14	1	y≌ ≠ 40) O +
		ials / Folders / My Scans - Mozilla Firefox		000
Nessus Essentials / Fold	• × +			
(←) → 健 ŵ	🛈 🐔 https://localhost:8834/#/scan	s/folders/my-scans	🗢 ★	lii\ © ≡
🕥 Nessus Home 🥆 Kali I	.inux 🌂 Kali Docs 🌂 Kali Tools 🛸 Exp	loit-DB 🔅 Most Visited 🗿 Nessus / Initializing		
	There	's an error with your feed. Click here to view your licens	e information.	
nessus [®]	Scans Settings			1
FOLDERS	My Scans			Import New Fo
My Scans 1				
All Scans	Search Scans Q 1	Scan		
1 Trash	Name	Schedule		Last Modified v
RESOURCES	Windows server 2008	On Demand	0	Today at 4:14 AM
Policies	Windows server 2000	On Demand	ŭ	Today at 4.14 AM
Plugin Rules				
 Plugin Rules Scannes Community Research Plugin Rulesse Notes 				
TENABLE				
😂 Community				
Research				
Plugin Release Notes				
•				

olications - Places - 🖸	Firefox ESR 👻	Mon 04:14	1	,# <i>/</i>	40 0 -
		lessus Essentials / Folders / View Scan - Mozilla Firefox			000
Nessus Essentials / Fold	* × +				
€ → ୯ û	① 🐔 https://localhost:	8834/#/scans/reports/5/hosts	🖸 🏠	li i	\ ⊡ ≡
🕲 Nessus Home 🥆 Kali I	Linux 🥆 Kali Docs 🥆 Kali T	Tools 🛸 Exploit-DB 🔅 Most Visited 🥥 Nessus / Initializing			
		There's an error with your feed. Click here to view your license	information.		
C nessus	Scans Settings				3 🕗
FOLDERS	Windows server a	2008			
My Scans	Back to My Scans				
Al Scans	Hosts 1 Vulnerabl	lities 1 History 1			
1 Trash	6-				
RESOURCES	Filter Search Hosts	Q 1 Host			
Policies Policies Plugin Pules	III Host	Vulnerabilities v	5	Scan Deta	ils
Plugin Rules	192,168,10,11	5	-	Policy:	Spectre an
🐏 Scanners				Status:	Running
Scanners TEMABLE				Scanner: Start:	Local Scar Today at 4
AB Community					
				Vulnerabil	ities
Plugin Release Notes					
:					
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~					

Description: After going through Nessus from external Kali, I initated a scan to target windows server 2008, which I inputed the Ip address. After that, the website scanned the server, which it found 1

vulnerability in the system. I only scanned the system for a couple, mins and many vullerabilites occurred.