Old Dominion University

CYSE 301 Cybersecurity Techniques and Operations

Assignment #3 – Sword Vs. Shield

Ned Smith 01200384 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.

		🕎 Ubuntu 64-bit on ESMIT049 - Virtual Ma	achine Connection		
	Attacker Kali - External Workstation on E	5MIT049 - Virtual Machine Connection			- 🗆
Recycle Bin	File Action Media Clipboard Vi	iew Help			
		Zenman 🛪	Man 22:30	1 .2	1 11 ()
	Application -	Zemnap -	10122:33		1 - 40 0
Acrobat			Zenmap	0	0 0
Reader	Scan Tools Profile	Help			
	Target: 192.168.10.0	v/24 *	Profile: Quick scan	v Scan	Cancel
	Command: nmap -T4	4 -F 192.168.10.0/24		11 () () () () () () () () () (
Zenmap GUI	2	Newso Output Deute (Haste Transform)	Unit Datally Court		
	Hosts Services	nmap Output Ports / Hosts Topology	Host Details Scans	A =	Detaile
	OS Host V	Stasting Magn 7 70 (https://		• =	Details
Nutanix SSR		Nmap scan report for 192.168.	10.2		
	192.168.10.11	Host is up (0.0043s latency). Not shown: 97 filtered ports			
		PORT STATE SERVICE			
Wireshark	M	80/tcp open http			
		443/tcp open https			
	π	Nmap scan report for 192.168.	10.10		
		Not shown: 99 closed ports			
Chrome		PORT STATE SERVICE			
	2	zivec open vep			
	~	Nmap scan report for 192.168 . Host is up (0.0065s latency).	10.11		
VM - Kalii Leoin infe	F	Not shown: 94 filtered ports			
		21/tcp open ftp			
		80/tcp open http 135/tcp open msrpc			
VMware	•	445/tcp open microsoft-ds			
Workstati	-	49154/tcp open unknown			
	Filter Hosts				•
					1
= ア 日 💿 🎥 Hyper-V Manager 🤱	🖢 pFsense - Firewall 6 😥 Attacker	Kali - Exter 🧶 Ubuntu 64-bit on E 👲	Windows Server 20		
📕 🔎 Type here to search 🛛 🗮 🖽		0 0 0 0			

Explanation: The scan of all available networks shows the different ports, as well as their status and service. For the IP Address of 192.168.10.2, we can see that the 53, 80, and 443 ports are open and are all TCP ports. Port 53 deals with domain services (DNS), port 80 deals with HTTP protocol, and port 443 deals with HTTPS protocol, the more secure version of HTTP. For the IP Address of 192.168.10.10, or the

Ubuntu VM, we can see that just port 21 is open, which is a TCP port that deals with FTP protocol. The final IP Address we can see is 192.168.10.11, or the Windows Server 2008 R2 VM, which has the most ports. All of its ports are TCP ports and port 21 still deals with FTP protocol, while port 80 still deals with HTTP protocol as we mentioned before. Port 135 deals with MSRPC service, port 445 deals with microsoft-ds service, port 3389 deals with ms-wbt-server service, and 49154 deals with a service titled "unknown".

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>
 <u>Screenshots:</u>





200-word essay:

When the scan begins, Wireshark shows multiple ARP packet broadcasts being sent, each one asking who has certain IP addresses beginning with 192.168.10.1 and ranging to the end of the subnet. We see this for most addresses, but 192.168.10.10 instead shows an ICMP echo (ping) request followed by an ICMP reply. This is the address for the Ubuntu VM, so it seems that External Kali's Nmap Intense Scan is able to locate this IP Address because it is one of the only ones that is actually running, allowing it to send a ping request and receive a response. After External Kali continues to scan, we can see on Wireshark that External Kali is now attempting to establish the TCP three-way handshake with various ports on the Ubuntu VM by sending TCP SYN packets, but cannot because

none of the ports it is attempting to connect with are open. It then comes across Ubuntu VM port 21, and it continuously sends a TCP SYN packet from various External Kali ports to check if port 21 is open. Port 21 responds to almost all of them with TCP SYN packets of its own, showing that it is open. Near the end of the scan, we see the TCP SYN packets from both sides halt and we see a few more ICMP packets get sent from External Kali, which Ubuntu responds to as anticipated with an ICMP reply.

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 appliable)
1	WAN	block	192.168.217.3	192.168.10.10	N/A

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

		Sense.CYSE.com 1	okmarksizitootsiriHelp				- TI [2:26 Al	M Q	
	() () () () () () () () () ()	https://192.168.10	.2/firewall_rules.php?if-	wan	C Q	Search	1 1 4 A V	=	
	▶-	COMMUNITY EDITION	stem + Interfaces + Fi	rewall - Services -	VPN - Status - Diag	nostics + Help +	400 🗘		
		WARNING: The adm	nin' account password is se	t to the default value. C	hange the password in the	User Manager.			
		Firewall / Ru	les / WAN				± ₩ 8 8		
		The changes have b Monitor the filter rel	een applied successfully. T oad progress.	he firewall rules are now	reloading in the backgrou	ind.	×		
		Election WAN I	-						
		Produing Triver L	~						
		Rules (Drag to	Protocol Source	Port Destinati	on Port Gateway Queu	e Schedule Description	Actions		
		× 0/0B	 Reserved Not assigned IANA 	• • Iby		Block bogor	networks 🌣		
		🗆 🗙 0/504 B	IPv4 192.168.217 ICMP	.3 • LANnet	• • none		\$/D 01		
		O ✔ 1/11.38 MB	any IPv4+6 * WAN net		• • none	Open Conne and IPv6	ction IPv4		
					t	Add 🕽 Add 💼 Delete	Save + Separator		
	-	0						Activate Windows	
	*							Go to Settings to activate windows.	
				_				. 106.44	
🗄 🔎 Type here to search 🛛 🔍 🏹 🛱	<u> </u>) 🖻 🚺 🤇		Attacker Kall - External We	rlatation on ESMITORY	. 6 × /		54°F Mostly cloudy ^ @ =	Q
	Applications w	News - Tree							
	appacations -	Places - El Term	ninal -	Tu	e 05:26		II # / +0 (Ф -	
	b.		ninat -	Tu	e 05:26		I # / •0 (ن -	
	Þ	Nessus Info	vMshare	Tu	e 05:26		I # / 4 (• •	
	₽	Nessus Info	vinal • VMshare	root@CS	2APenTest: ~	0	● ● ● ●	o -	
	b	Nessus Info	Edit View Search 1 (524/2007/2012 - 0 Jin 122.168.10.10 (122	Tu root@CS [erminal Help g 192.168.10.10 .168.10.10 56(8	2APenTest: - 4) bytes of data.	0	• •	• •	
	2 2 2	Nessus Info	Maat • VMshare Edit View Search 1 192,168,10,10 (192 192,168,10,10 ping kets transitted.	Tu root@CS ferminal Help g 192.168.10.10 .168.10.10) 56(8 statistics	2APenTest:- 4) bytes of data. packet loss, time	© (0 0 ∖	o •	
		Nessus Info	Maat • Wishare Edit View Search 1 1923-168-38-18 (132) 1922-168-10-10 (132) 1922-168-10-10 ping kets transmitted, ************************************	root@CS ferminal Help g 192.168.10.10 168.10.10) 56(8 statistics 0 received, 100% g 192.168.10.11 156.10.11) 56(7	2APenTest:- 4) bytes of data. packet loss, time	© (9725	■ A2 / 40 0	0.	
		Nessus Info	Edt View Search 1 (192,166,10,10) 192,166,10,10 (192) 192,166,10,10 (192) 192,166,10,11 (192) 192,166,10,11 (192) 192,166,10,11 (192)	root@CS ferminal Help g 192.168.10.10 J.668.10.10) 56(8 statistics g received, 100% g 192.168.10.11) 56(8 statistics	2APenTest:- 4) bytes of data. packet loss, time 4) bytes of data.	© (■ A2 / 40 0	o -	
		Netsus Info	Ede Wew Search 1 Control of the search 1 Con	root@CS ferminal Heip g 192.168.10.10 g 192.168.10.10 g received, 1004 (192.168.10.11) 56(8 statistics g received, 1004 g 192.168.10.2	2APenTest:- 4) bytes of data. packet loss, time 4) bytes of data.	© 1 87as 86as		o •	
		Passes - 2 - 144 Nessus Info - 2100 	Edt Vew Scarch 11 VM/share 192.168.0.10 (52) 202.168.10.10 (52) 202.168.10.10 (52) 202.168.10.11 (52) 202.168.10.11 (52) 202.168.10.11 (52) 202.168.10.11 (52) 202.168.10.2 (52	roct@CS [erminal Help [072.168.10.10 [102.168.10.10] 50(6 [102.168.10.10] 50(6 [102.168.10.11] 50(0 statistics [0 received, 1004 g 192.168.10.2 108.10.2) 50(104) g 192.168.10.2 108.10.2) 50(104)	2APenTest:- 4) bytes of data. packet loss, time packet loss, time bytes of data.	© (87as 86as		o •	
		Nersous Info Nersous Info PTMG 	Long	roct@CS (cmt0al Hep (1972.163.10.10 (160.10.10) 50(0 (160.10.10) 50(0 (160.10.10) 50(0 (160.10.11) 50(0 (160.10.11) 50(0 (160.10.11) 50(0 (160.10.21) 50(04) (160.10.21) 50(04) (160.10.	2APenTest:- 4) bytes of data. packet loss, time 4) bytes of data. packet loss, time bytes of data. packet loss, time	© 1 87as 86as	■ .42 / 40 (■	o •	
		Netsus Info	And I CHAPTER CHAPT	rect@CS erminal Hep 0 192-148.10.10 .108.10.10) 56(8 statistics 0 received, 100% g 192.108.10.11) 56(8).10.11) 56(10 g 192.108.10.2) 0 received, 100% g 192.168.10.2) 56(8).10.2) 56(8) tatistics 0 received, 100%	2APenTest:- 4) bytes of data. packet loss, time 4) bytes of data. packet loss, time bytes of data. packet loss, time	© 1 87as 86as 98as		o •	
		Nessos Info Nessos Info PIMG C C C C C C C C C C C C C C C C C C C	Edt Vew Search 1 (1)224847441; e pin 192,168,10.10 (192 92.168,10.10 (192 92.168,10.10 (192 192,168,10.11 (192 92,168,10.11 ping kets transmitted, ping2,168,10.11 ping kets transmitted, ping2,168,10.11 ping kets transmitted, ping2,168,10.10 (192, 192,168,10.10,2 ping sets transmitted, ping2,168,10.10,2 ping sets transmitted, ping2,168,10.10,2 ping sets transmitted, ping2,168,10.10,2 ping sets transmitted, ping2,168,10.10,2 ping sets transmitted, ping2,168,10,2 ping sets transmitted, ping2,168,10,10,2 ping2,10,00,00,00,00,00,00,00,00,00,00,00,00,	root@CS erminal Heip 9 192.168.10.10 .168.10.10 56(8 erceived, 100% 9 192.168.0.11) 56(8 statistics 6 received, 100% statistics 6 received, 100%	ZAPenTest:- 4) bytes of data. packet loss, time 4) bytes of data. packet loss, time bytes of data. packet loss, time	© 1 87ms 86ms 90ms			
		Nessus Info Nessus Info Pillo C C S Pillo C C S Pillo C C S Pillo C C S Pillo C C S Pillo C C S Pillo C S S Pillo C S S Pillo C S S Pillo C S S S S S S S S S S S S S S S S S S	And - Control	root@CS erminal Help g 192.168.10.10 1.66.10.10 50(6) statistics 0 received, 100% g 192.168.10.11 56(8 statistics 0 received, 100% tatistics 0 received, 100%	20528 2APenTest:- 4) bytes of data. packet loss, time bytes of data. packet loss, time	© 1 87%5 86%5			
		Nessus Info Nessus Info P100 C	Edt Wew Search 1 Control of the search 1 Con	root@CS (erminal Help () 192-106.10.10 () 182.106.10.10 () 186.10.10 () 186.10.10 () 186.10.10 () 186.10.10 () 186.10.10 () 192.106.10.2 () 186.10.2 () 192.106.10.2 () 186.10.2 () 186.10.10 () 186.10 () 186.10.10 () 186.10 () 18	2APenTest:- 4) bytes of data. packet loss, time 4) bytes of data. packet loss, time bytes of data. packet loss, time	© 0 8745 8645 9085			
		Nessus Info Nessus Info Pila Pila Pila Pila Pila Pila Pila Pila	Edt View Search 1 Vidibare	roct@CS erminal Help (192-168-10-10 1-88-10-10) 30(6 (192-168-10-11 0) received, 100% (192-168-10-11) 30(8 statistics (0) received, 100% (192-168-10-2) (192-10-2) (192-10-	20526 2APenTest:- 4) bytes of data, packet loss, time 4) bytes of data, packet loss, time bytes of data, packet loss, time	© 1		o -	
		Nersons Info	And -	root@CS [0722.163.10.10 [0722.163.10.10 [165.10.10] 56(0 [0] 122.163.10.10 [0] 122.163.10.11 [0] 120.10.10 [0] 120.10.11 [0] 120.11 [0] 120.11 [0	200-200 200-200 4) bytes of data. packet loss, time bytes of data. packet loss, time	0 1 8723 8603 9805		O • Activate Windows Co to Seringa Io activate Windows.	
		Nessus Info Nessus Info Pilo C C C C S Pilo C C C C S Pilo C C C C S Pilo Pilo C C C C S Pilo Pilo C C C S S Pilo Pilo C C S S Pilo C S S S S S S S S S S S S S S S S S S	Edt View Search 1 (G12Aentratt: # pin 192.166.30.10 (192 S2.166.30.10 (192 S2.166.10.10 (192 S2.166.10.11 ping Acts transmitted), (G12Aentratt: # pin 192.166.10.11 ping Acts transmitted, (G12Aentratt: # pin 192.168.10.2 (192. 192.168.10.2 ping 192.168.10.2 (192. 192.168.10.2 (192.) (S12Aentratt: #)	root@CS erminal Help [9 192.168.10.10 .168.10.10 56(6 statistics 0 received, 100% statistics 0 received, 101 56(8.10.2) 56(84) tatistics 0 received, 100%	20528 2APenTest:- 4) bytes of data. packet loss, time bytes of data. packet loss, time	0 1 8785 9085		Activate Windows Go to Settings to activate Windows.	
11 🖉 Type here to search		Parks - C (1977) Nessous Info 7166 7166 7166 7166 7166 7166 7166 716	Edt Wew Search 1 Vidibare Edt Wew Search 1 192.166.10.10 [202 202.166.10.10 [202 202.166.10.11 [202 202.166.10.11 [202 202.166.10.11 [202 202.166.10.11 [202 202.166.10.11 [202 202.166.10.12 [202 202.166.10.21 [202 202 202.166.10.21 [202 202 202 202 202 202 202 202	root@CS erminal Help (0.122.168.10.10 1.08.10.10) 30(6 0.122.168.10.10 0.108.10.10) 30(6 0.122.168.10.21 0.108.10.21) 30(6 0.192.168.10.2 108.10.21) 30(64) 1.015115(5 0. received, 100Y	20526 2APenTest:- 4) bytes of data, packet loss, time 4) bytes of data, packet loss, time bytes of data, packet loss, time	0 a		Activate Windows Co to Settings to activate Windows.	

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
1	WAN	Block	192.168.217.3	LAN net	N/A

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 (port # if appliable)
1	WAN	pass	192.168.217.3	192.168.10.11	FTP (port 21)
2	WAN	Block	192.168.217.3	LAN net	N/A

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



Explanation: The Nmap scan is not picking up any hosts or open ports, including port 21 (FTP port) for IP Address 192.168.10.11 (Windows Server 2008 R2 VM).

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



Explanation: There were 28 total vulnerabilities found in the NESSUS Scan of Microsoft Windows Server 2008 R2 VM. Of the 28 found vulnerabilities, four were considered mixed severity, three were considered medium severity, one was considered low severity, and the other 20 were considered "info" severity, which seems to be a level under low severity.