## OLD DOMINION UNIVERSITY

### CYSE 301 Cybersecurity Techniques and Operations

## Assignment #3 Assignment 3: Sword vs. Shield

Stuart N. Howard 01241576

#### Task A: Sword - Network Scanning (20+ 20 = 40 points)

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.

Task A.1

Use namp to scan the subnet using the Nmap 192.168.10.0/24

😴 Attacker Kali - External Workstation on SHOWA006 - Vintual Machine Connection - 🗆 X	Uburts 66-bit on PHOWADD8 - Virtual Machine Connection     -
File Action Media Clipboard View Help tha 10 • • • • • • • • • • • • • • • • • •	File Action Media Clipboard View Help
Applications • Places • D Terminal • Sat 01:01	Ib     (0)     (0)     (1)     (1)     (1)       Capturing from eth0     → 12     (1)     (1)     (1)
root@CS2APenTest:~ © © Ø	
File Edit View Search Terminal Help	Apply a display filter <cut></cut> Expression +
Starting Mmap 7.70 ( https://mmap.org ) at 2023-07-15 00:57 E01 Nmap scan report for 192.168.10.11	No. Time Source Destination Protocol Length Info
Host 1s up (0.004/s latency). Not shown: 994 filtered ports	r 1 0.000000000 192.168.10.2 192.168.10.10 TCP 66 53 - 46898 [FIN, ACK] Seq=1 Ack=1 Win=51
Image: 100     Verwa Sacricia Interminati Herpinati A       Startica Herpinati Farminati Herpinati A     1 at 2623-67-15 60:57 EDF       Image: Came respect for 153:100.10.11       Herpinati Farminati Herpinati A       Void Starting Herpinati Farminati Herpinati A       Void Starting Herpinati Farminati Herpinati A       Void Starting Herpinati Farminati Herpinati Farminati Herpinati Farminati Fa	2 3 0.89344888 123 218 128 18 123 128 184 1 175 66 4698 − 53 [FF, AC] 1921 AC1
2 80/tcp open http 135/tcp open msrpc	5 0.003472000 132.100.10 192.105.10.10 192.105.10.10 TCP 74.53 - 40900 [3Vn, ACK] Seque Acks1 Min=05 6 0.003499100 192.105.10.10 192.105.10.2 TCP 66.40900 - 53 ACK] Seque Acks1 Min=29312 L
445/tcp open microsoft-ds 3389/tcp open ms-wbt-server	2 0 000412690 102:00:10:10 10 192:00:10:12 10 10 10 10 10 10 10 10 10 10 10 10 10
<ul> <li>49154/tcp open unknown</li> </ul>	9 8:33743780 1392 484:38.2 10 8:339743780 1392 484:38.2 10 8:3399100 1392 484:38.2 10 8:3399100 1392 484:38.10 19 192 484:30.2 10 8:3399100 1392 484:30.10 19 192 484:30.2 TCP 74 46982 - 53 [571] 5640 411:72208 [40:0] H.
Nnap done: 1 IP address (1 host up) scanned in 5.73 seconds	• 110.331033000 192.106.10.2 192.106.10.2 10F 24.0062 - 33 [318] Sec. 4 81-29201 Letter 1 -
Implementation         None 182,248,380,074           Starting Mugarity 7,761         Nigstrumpert 507,781,180,810,074           Implementation         Nigstrumpert 507,182,180,180,074           Implementation         Nigstrumpert 507,182,180,180,2	Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (538 bits) on interface 0 (1015) (1015) (1015) (1015) (1015) (1015) (1015) (1015) (1015) (1015) (1016) (1015) (1016) (1015) (1016) (1015) (1016) (1015) (1016) (1015) (1016) (1015) (1016) (1015) (1016) (1015) (1016) (1015) (1016) (1015) (1016) (1015) (1016) (1015) (1016) (1015) (1016) (1015) (1016) (1015) (1016) (
Nmap scan report for 192.168.10.2 Nmap scan report for 192.168.10.2 Nmap scan report for 192.168.10.2	<ul> <li>Internet Protocol Version 4, Src: 192.108.10.2, DSI: 192.168.30</li> <li>Transmission Control Protocol, Src Port: SJ, DSI: Port: 46998, Seq: 1, Ack: 1, Len: 0</li> </ul>
Host is up (0.0029s latency). Not shown: 997 filtered ports	💯
PORT STATE SERVICE 3/rcp epen domain 80/rcp epen http	
80/tcp open http ¥43/tcp open https	
- Near scan report for 192 168 18 18	
Not shown: 999 closed ports	0000         00         15         5d         6d         07         18         06         1004
Port STATE SERVICE	0010 00 34 00 00 40 00 40 06 a5 67 c0 a8 0a 02 c0 a8 .4.,0,0.,0, 0020 0a 0a 09 35 b7 32 48 8c a5 b4 a1 b5 7 c 6f 80 115.2Hvo
	0030 02 02 fc 5f 00 00 01 01 08 0a c6 4c 5d fc ac ebL] 0040 52 fb
the scar report for 192,100,10,11     the scar report for 192,100,11     the scar report for 19	
Not shown: 994 Tiltered ports	
21/tcp open ftp 80/tcp open http	
135/tcp open msrpc 445/tcp open microsoft-ds	
3389/tcp open ins-wbt-server 49154/tcp open unknown	
Nmap done: 256 IP addresses (3 hosts up) scanned in 18.64 seconds root(C522PenTest:	Packets: 27253 - Disolaved: 27253 (100.0%) Profile: Default
Status Running 🗐 🗍	State
Generation: 1 Note: Madrine V/20092	
Notices 1WW WX00002 YS 103 0.11 Login Adventuation Premised 2 Paraseq12.0	Activate Windows
	Ge to Settings to activate Windows.
Summary Memory Networking	
🔎 🛱 🏮 🎁 Hyper V Manager 💩 Attacker Kill - Extern. 😓 pFzonse - Firewall 6 📚 Uburtu 64-bit on S 💩 Windows Server 20	ትርጉ የ 2 ቀባ 101 አለተ የ የ 2 ቀባ 2015 አለተ የ 101
Mostly sunny Q Search D	🖬 💭 💿 🖬 🥙 😋 🏣 🚳 🏪
rootQCS2APenTest - # nnap sV 192.168.10.9	52252 3011 5232718. 192.166.10.2 192.166.10.10 TCP 66 53 - 51356 [ACK] Seg-1 Ack-35 Win-65
<pre></pre>	1         1
Note: Host seems down. If it is really up, but blocking our ping probes, try -Ph Nmap done: I IP address (0 hosts up) scanned in 13.29 seconds	
rootQCS2APenTest: # nmap -0 192.168.10.7 192.168.10.11 192.168.10.2 Starting Nmap 7.70 ( https://nmap.org ) at 2023-07-15 01:32 EDT	52257 3046.7728821.102.166.10.10         102.186.10.2         1CP         66.41656         53.46K.5         Sec1.46K.16K.16K.16K.16K.16K.16K.16K.16K.16K.1
Nmap scan report for 192.168.10.11 Host is up (0.0036s latency).	
Host is up (0,0036s latency). Not shown: MP4 filtered ports PMF - SIATE SEMVICE	
21/tcp open ftp 80/tcp open http	Frame S1512: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0 Ethernet II, Src: Microsof.40:57:8c (00:15564:40:57:0c), Dat: Microsof.40:57:1e (00:15:561:40:57:1e) A date of the state o
445/tcp open microsoft-ds	* Internet Proceed Version 4, ord: 192.100.10.2
445/tCp Open microsoft-05 3389/tCp Open ms-whit-server	0100 = Version: 4           0010 = Model (cent): 20 bytes (5)           > Differentiated Services Field: 8:000 (DSCP: CS0, ECN: Not-ECT)           Total Length: 22
3189/tcp open ms-whi-server 49154/tcp open unknown Morning: DSCan results may be unreliable because we could not find at least 1 open and 1 closed port I	Identification: 0x6c8e (27662)
	Tuenti Italiani, okolee (2002)
Device type: general purpose specialized phone	Flags: 0x02 (Don't Fragment) Fragment offset: 0
Device type: general purpose specialized phone	Flags: 00x2 (Don't Fragment) Fragment offset: 0 Time to live: 64
Device type: general purpose specialized phone	Flags: 002 (On't Fragment)     Flags: 002 (On't Fragment)     August 102 (On't Fragment)
Device type: general purpose specialized phone	Flags: 002 (On't Fragment)     Flags: 002 (On't Fragment)     August 102 (On't Fragment)
Device type: general purpose ipactalized phone device type: general purpose ipactalized phone of CHC (ser/initicosoft Luddow, server 2008)r2 (ger/omicrosoft ukindow, 8.3 ger/omicrosoft ukindow, 7 ger/omicrosoft ukindow, ger/omicrosoft ukindow, server 2008 r2 ger/omicrosoft ukindow, 5.3 ger/omicrosoft do device in recent Ukindow, server 2008 r2 ger/omicrosoft ukindow, 5.3 ger/omicrosoft Windows 7 SPL, or Windows Server 2008 r2 ger/omicrosoft ukindow Windows 7 SPL, or Windows Server 2008	Flags: 0x2 (0m): Fragment) Fragment offset: 0 Time to live: 64 Header Checksum: 0x3099 (validation disabled)
Device type: general purpose ipactalized phone device type: general purpose ipactalized phone of CHC (ser/initicosoft Luddow, server 2008)r2 (ger/omicrosoft ukindow, 8.3 ger/omicrosoft ukindow, 7 ger/omicrosoft ukindow, ger/omicrosoft ukindow, server 2008 r2 ger/omicrosoft ukindow, 5.3 ger/omicrosoft do device in recent Ukindow, server 2008 r2 ger/omicrosoft ukindow, 5.3 ger/omicrosoft Windows 7 SPL, or Windows Server 2008 r2 ger/omicrosoft ukindow Windows 7 SPL, or Windows Server 2008	11         + Flags: 0005 (Con't Fragment)           The top in the state of t
Device type: general purpose specialized phone (Construction) (Constr	11         + Flags: 0005 (Con't Fragment)           The top in the state of t
Device type: period purpose iperclaitized prove the second secon	11         + Flags: 0005 (Con't Fragment)           The top in the state of t
Device type: period purpose iperclaitized prove the second secon	11         + Flags: 0005 (Con't Fragment)           The top in the state of t
Device type: general purpose specialized phone (Construction) (Constr	11         + Flags: 0005 (Con't Fragment)           The top in the state of t
Device type: general purpose iperclaitized phone of CPU (gen/interced)truindow, prior 2008 (C gen/interced)truindow, 5.1 Gen/interceditruindow, 7 Gen/interced (window, gen/interced)truindow, prior 2008 (C gen/interced)truindow, vitis:spl details: Microsoft Microsoft Microsoft Microsoft All (G gen/interced)truindow, prior details: Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft States, prior 2008 (C gen/interced)truindow, vitis:spl microsoft Microsoft Mic	11         + Flags: 0005 (Con't Fragment)           The top in the state of t
Device type: general purpose ipectalized plowers 0.000 (FG (Gen/Charles) (FG)) (FG)) (FG)) (FG)) (FG)) (FG)) 0.01000 (FG) (FG))(FG))(FG)) (FG)) (FG)) 0.01000 (FG)) (FG))(FG)) (FG)) (FG)) 0.01000 (FG)) (FG)) 0.01000 (FG)) (FG)) 0.01000 (FG)) (FG)) 0.0100 (FG)) (FG)) 0.0100 (FG)) (FG)) 0.0100 (FG)) 0.	Image: 1000 (Cont f Fragment)
Device type: general personal particulated phone Device type: general personal particulated phone Device type: personal persona	* 1.02:00:00 for fragment)           * 1.02:00 for for fragment)           * 1.02:00 for for for fragment)           * 1.02:00 for
Decide type: general purposes inscribilized plots (Config Cape/InstructionSoft Linksey provide State	Image: 1000 (Cont f Fragment)
Device type: general personal spectral tracked been for CHC cape/choicesoftiudioms envery 2000 r2 (per/onlicesoftivindows 8.1 cpe/onlicesoftivindows 7. dpe/onlicesoft undows cpe/onlicesoftiudioms cuttain: eps/onlicesoftivindows 8.1 cpe/onlicesoftivindows 7. dpe/onlicesoft undows cpe/onlicesoftivindows cuttain: eps/onlicesoftivindows 7.1 cpe/onlicesoftivindows 7. dpe/onlicesoft undows 2.3 ar 6.8, dresset Fieldsows Cuttains 2.0, and 3.0,	<ul> <li> <b>F</b> [Jags: 1002 (One 'f Fragment) <b>F</b> [Jags: 1002 (One 'f Framatheteeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee</li></ul>
Decide type: general purposes inscribilized plots (Config Cape/InstructionSoft Linksey provide State	* 1.02:00:00 for fragment)           * 1.02:00 for for fragment)           * 1.02:00 for for for fragment)           * 1.02:00 for
Device type: general personal spectral tracked been for CHC caper/ordersoft tuidney every 2000 r2 (per/ordersoft tuidneys, 5.1 cpe /ordersoft tuidney, 7 cpe /ordersoft undney cpr / Brickowst tuidney, stita : per /ordersoft tuidneys, vita ::s). Device type: context tuidney server 2000 r2 (per /ordersoft tuidneys, vita ::s). Device type: context tuidney server 2000 r2 (per /ordersoft tuidneys, vita ::s). Device type: context tuidney server 2000 r2 (per /ordersoft tuidneys, vita ::s). Device type: context tuidney server 2000 r2 (per /ordersoft tuidneys, vita ::s). Device type: context tuidney server 2000 r2 (per /ordersoft tuidneys, vita ::s). Device type: context tuidney server 2000 r2 (per /ordersoft tuidneys, vita ::s). Device type: context tuidney server 2000 r2 (per /ordersoft tuidneys, vita ::s). Device type: context tuidney server 2000 r2 (per /ordersoft tuidneys, vita ::s). Device type: context tuidney server 2000 r2 (per /ordersoft tuidneys, vita ::s). Device type: context tuidney server 2000 r2 (per /ordersoft tuidneys, vita ::s). Device type: context tuidney server 2000 r2 (per /ordersoft tuidneys, vita ::s). Device type: context tuidney server 2000 r2 (per /ordersoft tuidneys). Device type: context tuidney server 2000 r2 (per /ordersoft tuidneys). Device type: context tuidney server 2000 r2 (per /ordersoft tuidneys). Device type: context tuidney server 2000 r2 (per /ordersoft tuidneys). Device type: context tuidneys server 2000 r2 (per /ordersoft tuidneys). Device type: context tuidneys server 2000 r2 (per /ordersoft tuidneys). Device type: context tuidneys server 2000 r2 (per /ordersoft tuidneys). Device type: context tuidneys server 2000 r2 (per /ordersoft tuidneys). Device type: context tuidneys server 2000 r2 (per /ordersoft tuidneys). Device type: context tuidneys server 2000 r2 (per /ordersoft tuidneys). Device type: context tuidneys server 2000 r2 (per /ordersoft tuidneys). Device type: context tuidneys server 2000 r2 (per /ordersoft tuidneys). Device type: context tuid	*         F. F. Jaga: 1005 (Obt * F. Fragment).           *         *           *         *           *         *           *         *           *         *           *         *           *         *           *
Device type: general personal partial tree phone (Construction of the construction of	P Ligs: 1025 (005 ft regiment)     P Ligs: 102
Device type: general purposes juectilize(p)Device (C) (C) (C) (C) (C) (C) (C) (C) (C) (C)	P 1.43:: 002 (000'; f Project)     Project 100 (00) (00'; f Project)     Project 100 (00; f Project)     Proj
<pre>Device type: general purposes juscillatelyDevice Content of the content of t</pre>	P Ligs: 1025 (005 ft regiment)     P Ligs: 102

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>

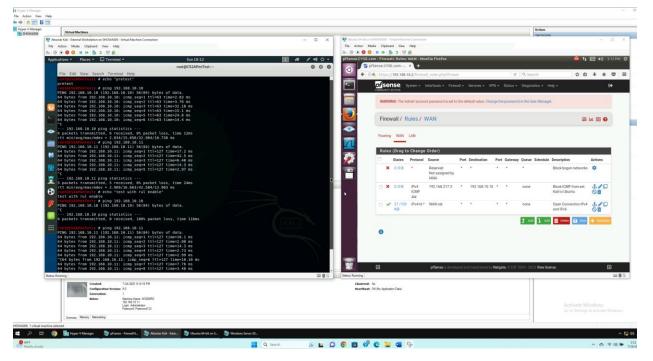
By analyzing the captured network traffic, we aim to gain insights into the traffic patterns, identify potential vulnerabilities, and understand the impact of the network scan on the LAN environment. The network scan caused an increase in ARP traffic. The Kali sent ARP requests to discover the MAC addresses of various IP addresses on the network, and the ARP replies containing their respective MAC addresses. Wireshark captured TCP and UDP packets showing port scanning activities probing different ports from the Nmap port scan. During the network scan, we observed ICMP traffic in the echo requests and responses (ping). The network traffic analysis during the External Kali network scan provided effective insights into the impact of the scanning activities. I was able to ARP traffic, port scanning activities, ICMP, and requests and responses for source and destination IPs. These findings aided in the verification of the Nmap process and the need for effectiveness. We can identify and mitigate potential security risks by analyzing the captured traffic patterns, such as open ports, to strengthen the overall network security posture.

#### 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)
	WAN	Block/reject	192.168.217.2	192.168.10.10	ICMP

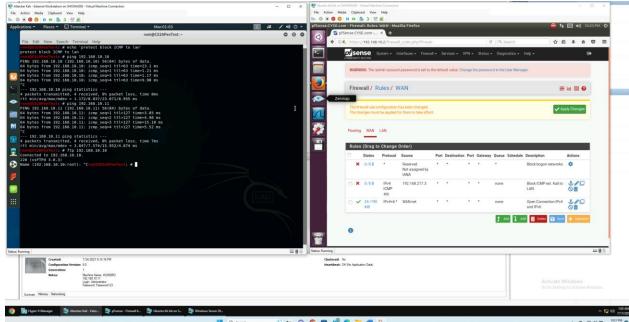


ker Kali - External Workstation on SHOWA006 - Virtual Machine Connection –	🕎 Übuntu 64-bit on SHOWA006 - Virtual Machine Connection
Action Media Clipboard View Help	File Action Media Clipboard View Help
🖲 🗮 📩 🗆 🗮 📠	in  0 ● ● ●  1  0   = 0
ations + Places + 🖸 Terminal + Sun 18:21 🔳 🗯 💉 📢 🔿	pfSense.CYSE.com - Firewall: Rules: WAN - Mozilla Firefox 😑 👣 💹 🐗 🕮 3:21 PM
root@CS2APenTest:~ O O	m pfsense.CYSE.com · × +
File Edit View Search Terminal Help	
exploit202404151:4 # ping 102.108.10.10 16 bytes from 102.108.10.10 (102.108.10.10 (104.108.108.108.108.108.108.108.108.108.108	Encirclence         System +         Interfaces +         Freesal +         Services +         VPN +         Status +         Deposition +         Help +         Get           Image: Services +         VPN +         Status +         Deposition +         Help +         Get           Image: Services +         VPN +         Status +         Deposition +         Help +         Get           Image: Services +         VPN +         Status +         Deposition +         Help +         Get
197.148.10.18 ping statistics packets transmitted, 4 received, 40 packet loss, time 9ms statistics transmitted, 4 received, 90 packet loss, time 9ms packets provide a scholar scholar packet packets provide a scholar scholar packet packets packets a scholar scholar packet packets packets a scholar scholar packet packets packets packets packets packets packets packets packets packets packets packets packets packets packets packets packets packets packets pa	Firewall / Rules / WAN 🗮 🖬 🛛
PERD 132, 108.10.19 (152.108.19.107.506) bpc of data 109 (150.108.10.19 (152.108.10.107.500) bpc sept t110.81 (109.27.60 ns 54 bytes from 152.108.10.107.1000 psept t110.81 (109.27.60 ns 54 bytes from 152.108.10.107.1000 psept t110.81 (109.27.60 ns 14 bytes from 152.108.10.107.1000 psept t110.81 (109.27.60 ns 14 bytes from 152.108.10.107.1000 psept t110.81 (109.27.60 ns) 15 bytes from 152.108.107.1000 psept t110.81 (109.27.60 ns) 15 bytes fr	The changes have been appled successfully. The freewall rules are now reloading in the background. X Monitor: the fifter reload progress.
94 bytes from 192.108.10.10: icmp_seq=4 ttl=63 time=1.95 ms ~ 202.108.10.10 ping statistics f packets framsitted, 4 received, 00 packet loss, time Bms	Pouting WAN LAN
rtt min/avg/max/mdev = 1.952/6.804/14.944/5.165 ms	Rules (Drag to Change Order)
oot@CS2APenTest:	
	States Protocol Source Port Destination Port Gateway Queue Schedule Description Actions
maltego	X 0/08 * Reserved * * * Block bogon networks Not assigned by MNA
	✓ 4/147 IPv4+6* WAN net * * * none Open Connection IPv4      ★/□     K8     And IPv6     S
	X         0 /504         PV4         192.168.217.3         192.168.10.10         *         none         BioditXMP form ext.         ↓ // □           8         ICMP         Kall to Ubuntu         © ■         Kall to Ubuntu         © ■
	J AN J AM DOM DOM TO THE
ning 🔤 🗌	
Counted 70,2021 51.51 M Counterful Winner 810 Generalizer 1 Notes March Neurer W20082 10,202 51 H1 March March Neurer W20082	Centered: ID Neutrise: Dr(Ru-lpitonin Dea) Activate Windows Go to Settings to activate Window
	do to settings to activate window
Summary Memory Memory Memory	

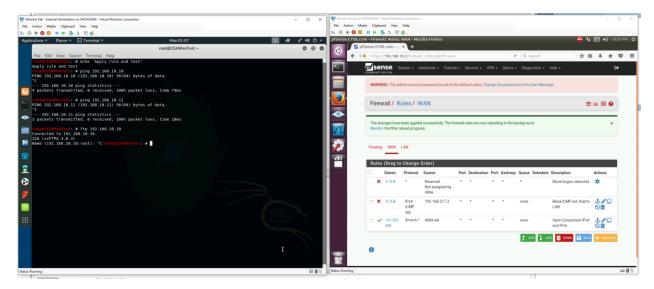
2. Clear the previous firewall policies and configure the pfSense firewall to block all ICMP traffic from External Kali to the LAN side.

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if appliable)
	LAN	Block	192.168.217.3	192.168.10.2	

- Pre-test
- ping to Ubuntu (PASS)
- ping to WS 2008 (PASS)
- FTP to Ubuntu (PASS)



- Apply the rule
- Test the rule
- ping to Ubuntu (No response/ blocked)
- ping to WS 2008 (No response/ blocked)
- FTP to Ubuntu/WS 2008 (PASS



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)
2	WAN	Block	192.168.217.3	LAN Address	ТСР

Pre-test

- ping to Ubuntu (PASS)
- ping to WS 2008 (PASS)
- FTP to Ubuntu (PASS)

			Ultranto 64 bit an SHOWA006 - 1											
cker Kali - External Workstation on SHOWA006 - Virtual Machine Connection Action Media Clipboard View Help			File Action Media Clipbo											
• • • • • • • •		a	0.00	5 D 18										
cations • Places • Terminal •	Mon 01:44	1 # / 40 · P	fSense.CYSE.com - Firew	ll: Rules:	WAN - M	zilla Firefox						🖨 ti	- 	10:44 PM
	root@CS2APenTest: -	000	pfSense.CYS	E.com	× +									
File Edit View Search Terminal Help			Q C Q https:	/192.168.1	10.2/firm	all rules.php?ifw	wan			1	9. Search	☆ [	1.4	* 5
<pre>netWithCollmanness: # echo.'pretest block all pretest block all traffice pass ftp to WS 'versecialAratimetr: # ping 192.108.10.10 PINO 192.108.10.10 (192.108.10.10) 56(84) by 64 bytes from 192.108.10.10: icomp_sequel ttl=4 64 bytes from 192.108.10: icomp_sequel</pre>	tes of data. 63 tine=2.23 ms 63 tine=0.931 ms		> <i>pf</i> set	<b>nse</b> s	lystem +	Interfaces + Fire	ewall •				Olisgnostics • and in the User Man	Нер •		64
<pre>C 192.168.10.10 ping statistics 3 packets transmitted, 3 received, 0% packet rtt min/avg/max/mdev = 0.931/2.487/4.328/1.46 pine 102.160.10.112</pre>	loss, time 5ms 80 ms		Firev	vall / R	ules /	WAN								0
PING 192.168.10.11 (192.168.10.11) 56(84) by 64 bytes from 192.168.10.11: icmp seq=1 ttl= 64 bytes from 192.168.10.11: icmp seq=2 ttl= 64 bytes from 192.168.10.11: icmp seq=3 ttl= 64 bytes from 192.168.10.11: icmp seq=4 ttl=	127 time=2.37 ms 127 time=6.79 ms 127 time=3.81 ms 127 time=5.98 ms	I				n has been change for them to take e						✓ <sup>∧</sup>	oply Chang	
<pre>^C64 bytes from 192.168.10.11: icmp_seq=5 tt' 64 bytes from 192.168.10.11: icmp_seq=6 ttl= 64 bytes from 192.168.10.11: icmp_seq=7 ttl= ^r</pre>	127 time=3.71 ms		Floating	WAN	LAN									
7 packets transmitted, 7 received, 0% packet	loss time 15mg		Rules	(Drag to	o Change	Order)								
rtt min/avg/max/mdev = 2.371/4.635/6.789/1.3	toss, time 15ms 86 ms		0	States	Protocol	Source	Port D	stination	Port	Gateway	Queue Schedule	Description	Action	6
<pre>root@CSZAPenTest: # ftp 192.168.10.10 Connected to 192.168.10.10. 220 (vsFTPd 3.0.3) Name (192.168.10.10:root): ^Crool@CSZAPenTest</pre>			×	0/08	•	Reserved Not assigned by IANA	• •		•	•	•	Block bogon networks	٥	
	-	C Local C	• ×	0/0B	IPv4 TCP	192.186.217.3			21 (FTP)	•	none	Block TCP from Ext Kali LAN except FTP to WIN2008		
	LIMAGE T	• •	67365 KiB	IPv4+6 *	WAN net	• •		•	•	none	Open Connection IPv4 a IPv6			
										1 440 1	Add 📋 Defeto 🕞 Seve	+ ~~	irahter	
			÷											
tunning			atus Running											= 0
Created: 7/24/2021 514 16 PM Configuration Version: 90 Generation: 190 Modroe Name: W20092 Notes: 192 (768 10.11			Chustered: No Heartbeat: OK (No Applica	tion Data)										
Logn: Administrator Password: Password123														
Surreary Menory Networking														

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 2008 VM in the CCIA network.