Old Dominion University <u>CYSE 301 Cybersecurity Techniques and Operations</u>

Assignment #2 Traffic Tracing and Sniffing

Ned Smith 01200384

Preface: I had to run the ping command for 2-3 minutes in order to get some DNS traffic, the TA's had mentioned doing this if you weren't getting any DNS traffic so I just wanted to explain why I had so many packets.

Task A

Question 1:



Explanation: There are a total of 420 packets have been captured and 420 packets have also been displayed.

Question 2:



Explanation: There are a total of 420 packets have been captured, but there are only 390 packets being displayed due to the ICMP filter.

Question 3:



Explanation: The source IP is 192.168.10.10 and the destination IP is 192.168.217.3. The sequence number of this packet was 1/256 and the total size was 84 bytes. The response time is 6.067 ms (milliseconds).

Question 4:



Explanation: The total number of packets captured was 420, but only four packets were displayed due to the DNS filter.

Question 5:

Explanation: I'm not sure if I did something wrong but this was the only DNS traffic I captured, the domain name it was trying to resolve was 3.debian.pool.ntp.org. The source IP/port and destination IP/port are displayed below:

Source: 192.168.217.3/55610

Destination: 192.168.217.2/53

Question 6:



Explanation: The message replied from the server is "Refused" and the source IP/port and destination IP/port are displayed below:

Source: 192.168.217.2/53

Destination: 192.168.217.3/55610

Task B

Question 1a:

	🕎 Abarian Kali - Estamal Worldstatio <u>n on FS</u>	MT040 - Viewel Machine Conception		- 0 X		
0	File Action Media Clipsoar 🕎 Kal	i - Internal Workstation on ESMIT049 - Virtual Machine Connection			- 0 ×	
Recycle Bin	ba 🗇 💌 🙆 😂 🖬 🕩 隆 File	Action Media Clipbeard New Help				
	Applications * Places * Ball	0 🖲 🕲 🖬 🕪 🎥 Þ 🔣 📓				
	Appli	ications 🔹 Places 🕶 👩 Wiresbark 🕶	Tue 18:23		1 # / •• 0 -	
1						
Arailter	File Edil View Se		toth0		0 0 0	- <u>^</u>
Respec	64 bytes from 192	P. P. R. R. A.		•		N
	64 bytes from 192	File Edit View Go Capture Bharyze Statistics	Telephony Wreess Tools Help			• I N
	64 bytes from 192 🍞	🛯 📶 📕 🙋 💿 🛅 🖹 🖉 🔍 🔶 🔶	.) 🖛 🖬 📮 🔍 🔍 Q. Q. Q.	12	Mat	hine
1	64 bytes from 192	Ismo			El Ta Evenueiro de St.	
Zenmap GU	64 bytes from 192	(H schip)			talian expression. * Ma	iget.
7.53	64 bytes from 192	No. Time Source	Destination Protocol	Length Info	ica:	et
	64 bytes from 192	153 31.101292600 192.155.10.13	192.166.217.3 ICMP	98 Echo (ping) reply	1d=9x9b99, seq=20/51	
2 .	64 bytes from 192	155 31, 384634666 192, 168, 19, 16	192,168,217.3 ICMP	98 Echo (ping) regluire	id=9x9b91, seg=19/48	
Nutarie SSR	_ 64 bytes from 192	156 32.100554806 192.168.217.3	192.168.10.13 ICMP	98 Echo (ping) request	id=9x9b99, seq=21/53	
	🗢 64 bytes from 192 💻	157 32.100591266 192.168.10.13	192.168.217.3 ICMP	98 Echo (ping) reply	id=0x0b90, seq=21/53	
	64 bytes from 192	158 32.390273500 192.168.217.3	192.168.10.10 ICMP	98 Echo (ping) request	1d=8x8b91, seq=28/51	
2	64 bytes from 197		102 108 10 13 TCMP	98 Echo (ping) request	id=5x5551, s0q-26/51	
2	64 bytes from 192	101 33.102931900 192.168.10.13	192.168.217.3 ICMP	98 Echo (ping) reply	1d=0x0b90, seg=22/56	•
with an	M 64 bytes from 192 📶	162 33.387692100 192.168.217.3	192.168.10.10 ICMP	98 Echo (ping) request	1d=0x0b91, seq=21/53	
and the second second	64 bytes from 192	163 33.368320800 192.168.10.10	192.168.217.3 ICMP	98 Echo (ping) reply	id=0x0b91, seq=21/53	
	64 bytes from 192	166 34.10343/566 192.165.21/.3	192.166.16.13 ICMP	98 Echo (ping) request	1d=0x0b00, seq=23/58	
	64 bytes from 192	168 34.399243298 192.158.217.3	192.168.10.10 ICMP	98 Echo (ping) repry	id=9x9b90, seq=23/38	
Georgie	🗮 👘 🖓	169 34.391226600 192.168.10.10	192.168.217.3 ICMP	98 Echo (ping) reply	id=0x0b01, scq=22/56	
Chiome	1	L 176 35.109773766 192.168.217.3	192.158.10.13 ICMP	98 Echo (ping) request	id=8x8b98, scq=24/61	
		L 171 35.100884400 192.168.10.13	192.168.217.3 ICMP	98 Echo (ping) reply	1d=8x8b98, seq=24/61	
	1 🐨 🖉	172 35.391892766 192.168.217.3	192.168.10.10 ICMP	98 Echo (ping) request	10=9x9091, 500=23/58	
100.00		110 00.000140100 102.100.10.10	101.100.111.0	oo cono (pring) repry	10 00001, 100 10,000	
Luginiste	F 🗉	Farme Of the business of these (704 busines)				
100 C		Frame 34: 90 bytes on uire (764 bits), 1 Ethernet TT, Src: Microsof 48:57:1e (68)	15:5d:40:57:1e) Dat: Microsof	48:57:83 (89:15:5d:48:57:	831	
		Internet Protocol Version 4, Src: 192.16	8.217.3, Dst: 192.168.19.13			
	-	 Internet Control Message Protocol 			-	
Witnesse		00000 00 15 5d 40 57 03 00 15 5d 40 57 1	e 08 00 45 66 j@w _]@w -	· E ·		
WERE STOL		0010 00 54 C5 dT 40 00 3T 01 11 68 C0 a	9 13 65 66 66			
	101	0030 00 00 51 56 0e 00 00 00 00 00 10 1	1 12 13 14 15 OV	5000 C		
		8849 16 17 18 19 1a 1b 1c 1d 1c 1f 28 2	1 22 23 24 25	u ŝ N		
		0050 26 27 28 29 28 26 20 20 20 27 39 3 0060 36 37	1 32 33 34 35 8 ()*+,7012	345		
			can		1.	Go to Settings to activate Windows
					sib	, condenne no neip Desk:
. D H-	🙃 🖬 Harer-V Manazer 🤊	Attacher Kali - Extern 🧖 Kili - Internal Work 🔍 💷 al fence - Ein	wal 6. 🦻 Uhuntu 61-bit on F			M4658 10 E7 01
						9/26/102
🗎 🔎 Type t	iere to search 🛛 🧾 🖽					🐣 70'T Cloudy 🔿 🎢 👄 🖡 🖉 926/2023 💀

Explanation: I applied the capture filter "ICMP" to capture all current ICMP packets being transmitted between all sources and destinations.

Question 1b.

	File Edit View Se								
	64 bytes from 192			*et	h0 k		0		
	64 bytes from 192	File Edit View Go	Capture Analyze Statist	ics Telephony Wireless I	ools <u>H</u> elp				
	64 bytes from 192	1 📕 🧟 🔍 🦻		*) I# #I 🛄 🧮	@ Q Q !	*		Machine.	· · · · · · · · · · · · · · · · · · ·
	64 bytes from 192	licmp and ip.dst == :	92.168.10.10 and ip.src == 1	192 168 217.3			Express	ion + 95	
2	64 bytes from 192	No. Time	Source	Destination	Protocol La	ngth Info		-	
	64 bytes from 192	734 98.498384	890 192.168.217.3	192.168.16.10	ICMP	98 Echo (ping) request	id=6x0b91, se	q=86/22	
	64 bytes from 192 🚭	738 99.498222	000 192.168.217.3	192.168.10.10	ICMP	98 Echo (ping) request	id=6x0b91, se	a=87/22	
	64 bytes from 192	742 160.49986	0700 192.168.217.3	192.168.10.10	ICMP	98 Echo (ping) request	id=6x0b91, se	22/88=p	
	64 bytes from 192	748 101.50376	8100 192.168.217.3	192.168.10.10	ICMP	98 Echo (ping) request	id=Gx0b91, se	1=89/22	
	64 bytes from 192	759 102.50370	4400 192.100.217.3	192.100.10.10	TOMP	98 Echo (ping) request	10-0x0031, se	-90/23	
	64 bytes from 192	763 163.0006	4506 102 168 217 3	192.168.10.10	TOMP	98 Echo (ping) request	idedvohot se	1-91/23	
	64 bytes from 192	777 165,5141	7300 192.168.217.3	192,168,16,10	ICMP	98 Echo (ping) request	id=6x0b91, se	=93/23	
	64 bytes from 192	783 166.51573	4100 192.168.217.3	192.168.10.10	ICMP	96 Echo (ping) request	id=6x0b91, se	=94/24	
M	64 bytes from 192	798 167.51749	7800 192.168.217.3	192.168.16.18	ICMP	98 Echo (ping) request	id=6x0b91, se	=95/24	
	64 bytes from 192	B02 168.51384	6100 192.168.217.3	192.168.10.10	ICMP	98 Echo (ping) request	id=0x0b91, se	96/24	
	64 bytes from 192 🎽	806 169.51585	2300 192.168.217.3	192,168.16.10	ICMP	98 Echo (ping) request	id=6x0b91, se	q=97/24	
2 C	64 bytes from 192 🎿	816 110.5181	1996 192.168.217.3	192.168.16.18	TCMP	98 Echo (ping) request	id=Gx9b91, se	1=98/25	
-	64 bytes from 192	827 112 5292	2600 102 100 217 3	192.169.10.10	TOWP	98 Echo (ping) request	id-Gyobal, se	-100/2	
	ē	831 113 5229	1288 192 168 217 3	192 168 16 16	TCMP	98 Echo (ping) request	id=0x0001, sc	=100/2	
		835 114.52640	1800 192.168.217.3	192.168.16.10	ICMP	98 Echo (ping) request	id=6x0b91, se	-192/2	
Po		839 115.52490	4900 192.168.217.3	192.168.10.10	ICMP	98 Echo (ping) request	id=6x0b91, se	=193/2	
		L 854 116.52883	3400 192.168.217.3	192.168.10.10	ICMP	98 Echo (ping) request	id=6x0b91, se	q=104/2	
F		•							
_		+ Ethernet II. Sr	es on wire (784 bits : Microsof 40:57:1e), 98 bytes captured () (00:15:5d:40:57:1e), Ds	st: Microsof 4	nterrace 0 8:57:0c (00:15:5d:40:57:	Bc)	1	
		 Internet Protoco 	l Version 4, Src: 19	2.168.217.3, Dst: 192.1	168.19.10			-	
	No.	+ Internet Contro.	Message Protocol					-	
		8000 00 15 5d 46	57 BC 00 15 5d 49 5	7 1e 88 98 45 09 ···]	(W · · ·] (W · · · E ·				12
		ugin 00 54 d4 23	40 00 3T 01 03 27 c	0 88 09 03 C0 88 -T-	eg.7				~
	100	0030 00 00 00000	01 00 00 01 00 01 0	0 10 13 03 08 09	Y E				
	<u>×</u>	0040 16 17 10 19	1a 1b 1c 1d 1e 1f 2	0 21 22 23 24 25					
		0050 26 27 28 29		0 31 32 33 34 35 4'(
		8669 36 37		67					
									entect the ITS Help Dec

Explanation: I applied a capture filter that specified the packet must be an ICMP packet as well as have a source IP of 192.168.217.3 (the IP address of External Kali) and a destination IP of 192.168.10.10 (the IP address of the Ubuntu VM). This showed only ICMP request packets from External Kali and to Ubuntu VM.

Question 2a:



Explanation: This screenshot shows both the normal login for the Ubuntu VM and the login I was instructed to use for question 2c. One is username "cyse301" and password "password" and the other is my MIDAS and UIN.

Question 2b:

a	🐺 Kali - Internal Workstation on ESM(104) - Vi	tual Machine Connection		- 0 X	
Recycle Inn	File Action Media Clipboard View	Help			- a ×
	Ba © ● ◎ ◎ Ⅱ ▶ Ba ⊃ H	1 🛃	200N0X1		
L	Applications - Places - W	ireshark 👻 Tue	18:27	1 # / •0 0 -	
Annahar		Wireshark - Display	/ Filter Expression		- 🔶 🔶
Reider	File Edit View Go Cap	ture Analyze Statistics Telephony Wireless	Tools Help	996	N
•		S C Q + + J + +			Machine
P Nmin-				Expression +	gs
Zenmap GU	No. Time	Source Destination	Protocol Length Info		Managet
0	1188 207.752239288	9 192.168.18.18 192.168.217.3	FTP 86 Response:	220 (vsFTPd 3.0.3)	phager
	1203 215.295232400 1205 215.296585100	0 192.168.217.3 192.168.10.10 0 192.168.10.10 192.168.217.3	FTP 86 Request: FTP 106 Response:	USER cyse301 331 Please specify the password	
	1216 218.340215386	192.168.217.3 192.168.10.10	FTP 81 Request:	PASS password	
	1218 218.430353706 1220 218.433251000	0 192.168.10.10 192.168.217.3 0 192.168.217.3 192.168.10.10	FTP 89 Response: FTP 72 Request:	230 Login successful. SYST	
	1222 218.433992780	0 192.168.10.10 192.168.217.3	FTP 85 Response: CTP 72 Request:	215 UNIX Type: L8	
Wirshark	1383 233.91/464/06	9 192.168.18.18 192.168.217.3	FTP 88 Response:	221 Goodbye.	•
	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1				-
	*				
Google Chromir	8				
	<i></i>				6
VM - Kali Loginistro					
	Frame 1216: 81 bytes Ethernet II. Src: M	s on wire (648 bits), 81 bytes capture icrosof 48:57:1e (80:15:5d:48:57:1e).	d (648 bits) on interface 0 Dat: Microsof 40:57:8c (00:15	:5d:40:57:0c)	
	 Internet Protocol V 	ersion 4, Src: 192.168.217.3, Dst: 192	.168.10.10		
VMware	0000 00 15 5d 40 57	0c 00 15 5d 40 57 1e 08 00 45 10	21, Sed: 15, ACK: 55, Len: 1 	5	
	6610 08 43 bf 64 48	96 3f 96 18 42 c8 a8 d9 93 c8 a8	B		×
	0030 00 c5 05 11 00	00 01 01 08 0a a7 ac 45 ea ce 81			and the second se
	0040 d0 44 50 41 53 0050 0a	53 26 76 61 73 73 77 6f 72 64 6d 1	OPASS p assword		Activate Windows
					Go to Settings to activate Windows
					elp, contact the ITS Help Desk:
📑 🔎 🖽 🌍 🛼 Hype-V Manager	🧶 Attacker Kali - Exter 🤰 Kali - Inte	emal Work 🧶 pFsense - Firewall 6 💩 Ubuntu 61-t	it on E		▲ 41 627 PM 926/003
👖 🔎 Type here to search 🛛 🍂	1 H 🖬 👂 🔘 👘 (0 0			🜁 70°F Cloudy 🔨 🖧 🛥 🖡 🕬 22279M 星

Explanation: The password used on External Kali to access the FTP server was "password" as shown in the screenshot above. By applying the "FTP" filter to Wireshark, we can find the username and password that was used to access the FTP server as well as see that the login was successful.

Question 2c:



Explanation: This screenshot shows that Wireshark was able to again find out what was input for the username and password to the FTP server, this time being my MIDAS and UIN information. It was also able to see that the login was unsuccessful, similar to how it was able to see that the previous login was successful.

Task C (Extra Credit)

Question 1:



Explanation: This image shows me creating and saving the file that will soon be transferred over to the External Kali VM.



Explanation: This image shows me performing an FTP file transfer to transfer the file created in screenshot one over to the External Kali VM from the Ubuntu VM.



Explanation: This image shows that the FTP file transfer was captured by Wireshark on the Internal Kali VM.



Explanation: This image shows that the text file and its contents were properly saved to a text file on the Internal Kali VM from what was found during the Wireshark sniffing.