OLD DOMINION UNIVERSITY

CYSE 301 Cybersecurity Techniques and Operations

Assignment #2 Traffic Tracing and Sniffing

Sahmer Ismael 01219271

Q1. How many packets are captured in total? How many packets are displayed?



Description- The total number of packets that have been captured are 46, and the total number of packets displayed are 46.

Q2. Apply "ICMP" as a display filter in Wireshark. Then repeat the previous question (Q1).



Description: After applying the ICMP filter, in Wireshark the amount of the packets captured stayed the same. However, the amount of the packets that where displayed have changed.

Q3. Select an Echo (replay) message from the list. What are the source and destination IPs of this

packet? What are the sequence number and the size of the data? What is the response time?

🖳 Atta	🐙 Attacker Kali - External Workstation on CS301-SISMA002 - Virtual Machine Connection —														>	<					
File	Action	Media Clipb	ooard	View	Help																
Appli	cations :			M/ir	osbark v					c	05.42						1	•• . <i>4</i>	((the `	(1)	
Арри		• Places			esnark •					S <mark>u</mark>	lius.45							- /			
	File	Edit View	Ga	Cantur	o Apoly	To Ctati	ation	Tolonho	ny Mir	olocc	Tools	Halp							•	9	-
	<u>File</u>		<u> </u>		e <u>A</u> naty		sucs		<u>ny vv</u> ii			<u>n</u> etp				×.					
			Ū	0303 0310 0333	×	4	*	⊫اله.			۹	Q	۵ 🛉								
	📕 icm	р															\times \rightarrow	* Expr	essior	ı	+
	Т	ïme	S	ource			Des	ination			Protoc	ol L	ength Inf	ō							F.
	21 2	0.5189989	00 1	92.1	58.217.	2	192	.168.2	17.3		ICMP		118 Re	dir	ect		(Redirect	for ho	st)		4
\$	22 2	1.3296062		92.1	08.217.	3	192	169 2	17 2		TCMP		98 EC	no:	(ping)	request	id=0x07fe,	seq=4	/1024		
	24 2	2.3446478	00	92.1	58.217.	3	2192	.168.1	0.10	ر	TCMP		98 Ec	tho	(ping)	request	id=0x07fe.	seq=4	/1280		
_	25 2	2.3618784	00 1	92.1	58.10.1	0	192	.168.2	17.3		ICMP		98 Ec	ho	(ping)	reply	id=0x07fe,	seq=5	/1280		2
	26 2	3.3461582	00 1	92.1	58.217.	3	192	.168.1	0.10		ICMP		98 Ec	ho	(ping)	request	id=0x07fe,	seq=6	/153		
	27 2	3.3614215	00 1	92.1	58.10.1	0	192	.168.2	17.3		ICMP		98 Ec	ho	(ping)	reply	id=0x07fe,	seq=6	/1530		
	28 2	4.3496693	00 1	92.1	68.217.	3	192	.168.1	0.10		ICMP		98 Ec	ho	(ping)	request	id=0x07fe,	seq=7	/1792		
	29 2	4.3675800	00 1	92.1	58.10.1	Θ	192	.168.2	17.3		ICMP		98 Ec	:ho	(ping)	reply	id=0x07fe,	seq=7	/1792		
	30 2	5.3516691	.00 1	.92.1	68.217.	3	192	.168.1	0.10		ICMP		98 Ec	ho	(ping)	request	id=0x07fe,	seq=8	/2048		4
M	31 2	5.4290908	00 1	92.1	58.10.1	Θ	192	.168.2	17.3		ICMP		98 Ec	ho	(ping)	reply	id=0x07fe,	seq=8	/2048		ł.
	4	0500004	~ ^	~ *	~ ~ ~ ~	^	100		~		TAUE		00 F	· .	, , ,			^	()		
	C	hecksum:	0xbcb)2 [c	orrect]																Τ.
	[Checksum	Statu	is: Go	ood]																
**		dentifier	(BE)	: 204	16 (0x0	7†e)															
			(LE)	: 050) 4 (0x	x0004)															
	S	equence n	umber	(LE	1024	(0x040	0)														٩.
	l ī	Request f	rame:	22]																	
	ו ו	Response	time:	12.3	30 <mark>0 ms</mark>]																
	Т	imestamp	from	icmp	data:	Feb 11,	2024	02:25	:14.00	00000	00 EST										
.		Timestamp	from	1 icm	o data	(relati	.ve):	0.1179	67300	secon	ids]										
		ata (40 D	ytes,																		
	0000	00 15 5d	40 5	57 05	00 15	5d 40	57 1f	08 00	45 00) .]@W···]@\	V···E·								
	0010	00 54 39	adu	00 00	3T 01	aa 9a	C⊍ a8	0a 0a	a c⊍ aa	5 - 1	19		74.0.								
	0030	00 00 58	90 (01 00	00 00	00 00	10 11	12 13	3 14 15		x										
-	0040	16 17 18	19 :	la 1b	1c 1d	1e 1f	20 21	22 23	3 24 25				!"#\$%								
:::	0050	26 27 28	3 29 2	2a 2b	2c 2d	2e 2f	30 31	32 33	3 34 35	5 &	()*+,-	./0	012345								
••••	0060	36 37								67	7										

Description: The source IP, for this reply packet is 192.168.10.10, which I circled in blue. The destination IP for this certain packet, is 192.168.217.3, which I circled with red above, in the photo. The sequence number is 4 (0x0004) for big Endian (BE), which I highlighted. And the sequence number for Little Endian (LE) is 1024 (0x0400), which I highlighted. The size of the data is currently (48 bytes), and the response time is, 12.300 ms, which I highlighted both in the above diagram.

Q4. Apply "DNS" as a display filter in Wireshark. How many packets are displayed?



Description: There a total of 16 DNS packets, that are displayed currently.

Q5. Find a DNS query packet. What is the domain name this host is trying to resolve? What is the source IP and port number, destination IP and port number? Please express in the format: IP:port.



		*eth0		000
File Edit View	o <u>Capture</u> <u>Analyze</u> <u>Stat</u>	tistics Telephony	<u>W</u> ireless <u>T</u> ools <u>H</u> elp	
🧉 🔳 🧖	to 🛅 🖹 🙆 🔍 🖣	* * .2 !* *	Q Q Q Q	R 🎹
dns			× =	Expression +
Protocol	Length Info			
DNS	81 Standard guery	0x026f A 0.debi	an.pool.ntp.org	
DNS	81 Standard query	0xd279 AAAA 0.d	ebian.pool.ntp.org	
DNS	54 Standard guery	response 0x026f	Refused	
DNS	54 Standard query	response 0xd279	Refused	
DNS	81 Standard guery	0xb43a A 1.debi	an.pool.ntp.org	
DNS	81 Standard query	0xc24b AAAA 1.d	ebian.pool.ntp.org	
DNS	54 Standard query	response 0xb43a	Refused	
DNS	54 Standard query	response 0xc24b	Refused	
				•
Erame 558 81	hytes on wire (648 h	its) 81 hytes (antured (648 hits)	on interface*
Ethernet II.	rc: Microsof 40:57:0	5 (00:15:5d:40:5	7:05). Dst: Microso	of 40:57:1f (
Internet Prot	col Version 4.	92 100 217 3	st: 192,168,217,2	
User Datagram	Protocol, See Port	19431, Dst Port	53	
Source Port	49434			
Destination	Port: 53			
Destination				
Length: 47				
Length: 47 Checksum: 0	3398 [unverified]			

Description: The domain name, this is host is trying to resolve,

1.debian.pool.ntp.org: Type A, class IN, which is displayed in green. The source IP and Port number is highlighted in purple, 192.168.217.3:49434. The destination Ip and Port number is highlighted in orange, 192.168.217.2:53.

Q6. Find the corresponding DNS response to the query you selected at the previous step, and what is the source IP and port number, destination IP and port number? What is the message replied from the DNS server?

•	Wireshar	+ 4	Attacker Kali - Er	ternal Workstation on CS	301-SISMA002 -	8 ×	1 ab-connect.co	wa-cci.org/https-8443/gu	acamole.lab.cova-cci.org/guacamole/#/cl	ent/OTE5AGMAbXIzcWw			Ľ
				*eth0		00	Sons	🝷 🔲 Wireshar 🗮	al Attacker Kali - External Worksta	tion on CS301-SISMA002 🔷 🗸 🗸	-	1	,2
No <u>File</u>	Edit Vie	w <u>G</u> o	Capture Analyze St	tatistics Telephony	Wireless Tools	Help		-					
		9 t	1 🗋 🗙 🏹 🤇	* *) !* :	🔿 📃 🔍	ର୍ ବ୍ 🚹			*eth	1	00	0	
Co. Lo							VMshare	No File Edit View G	<u>So</u> <u>Capture</u> <u>Analyze</u> <u>Statistics</u> Te	lephony Wireless Tools Help			
	ns					Expression		4 = <i>C</i> 0	to 🗋 🕅 🖉 🖓 🔍 + +) 🖛 🖬 🛄 📒 ଭ୍ର୍	0, 11		
	Proto	col Ler	ngth Info					(day				1.4	
	DNS		81 Standard query	y 0x026f A 0.del	bian.pool.ntp.o	rg		MOIIS		E local	J Expression		
	DNS		54 Standard query	y UX02/9 AAAA U	.debian.pool.nt	p.org		Protocol	Length Info	I A debies and also are			
	DNS		54 Standard quer	v response Avd2	79 Refused			DNS	81 Standard query 0x0201	A 0.debian.pool.ntp.org			
	DNS		81 Standard quer	v 0xb43a A 1.del	bian.pool.ntp.o	ra		DNS	54 Standard query respons	e 0x026f Refused			
	DNS		81 Standard quer	y 0xc24b AAAA 1	.debian.pool.nt	p.org		DNS	54 Standard query respons	e 0xd279 Refused			
	DNS		54 Standard guer	y response 0xb4	3a Refused			DNS	81 Standard query 0xb43a	A 1.debian.pool.ntp.org			
	DNS		54 Standard query	y response 0xc2	4b Refused			DNS	81 Standard query 0xc24b	AAAA 1.debian.pool.ntp.org	1		
								DNS	54 Standard guery respons	e 0xc24b Refused			
4													
	fstream	index	301				-	4					
	main Nam		em (response)					> Frame 560: 54	bytes on wire (432 bits), 54	bytes captured (432 bits) on interf	ace*	
	Transact	ion I	0: 0xb43a					Ethernet II, S	Src: Microsof_40:57:1f (00:1	:5d:40:57:1f), Dst: Micro	sof_40:57:0	15 (
	Flags: 6	x8105	Standard query re	esponse, Refused	L			Internet Proto	ocol Version 4, Src: 192.168	217.2, Dst: 192.168.217.3			
	Question	IS: 0						- User Datagram	· 53	POFT: 49434			
	Answer F	Rs: 0						Destination	Port: 49434				
	Authorit	y RRs	: 0					Length: 20					
	Addition	al RR	s: 0				Activate	Checksum: 0	xd5de [unverified]			Action	ate V
-	Lkequest	10:	008				Setti	[Checksum St	tatus: Unverified]			Golte	
	[lime: e	.0233	52400 seconds]					[stream inde	ex: 30]				

Description: the source IP and port number, is 192.168.217.2:53, displayed green. The destination IP and port number is 192.168.217.3:49434 and it is displayed in yellow.

Task B: Sniff LAN traffic

1. Sniff ICMP traffic (10 + 10 = 20 points) Open two terminals on External Kali VM. Use one ping Ubuntu VM and use the other ping Internal Kali.

 Apply proper display or capture filter on Internal Kali VM to show active ICMP traffic



Description: The screenshot displays, that I pinged, the ubuntu vm, and the second is external kali vm. Then after I used the icmp filter, to show the proper packets, that where being displayed.

2. Sniff FTP traffic (10 + 15 + 15 = 40 pts points)

a. Ubuntu VM is also serving as an FTP server inside the LAN network. Now, you need to use External Kali to access this FTP server by using the command: ftp [ip_addr of ubuntuVM]. The username for the FTP server is cyse301, and the password is password. You can follow the steps below to access the FTP server

b. Unfortunately, Internal Kali, the attacker, is also sniffing to the communication. Therefore, all your communication is exposed to the attacker. Now, you need to find out the password used by External Kali to access the FTP server from the intercepted traffic on Internal Kali. You need to screenshot and explain how you find the password.



Description: The way, that I was able to find the password, was by using the FTP, filter and then following the TCP stream.

c. After you successfully find the username & password from the FTP traffic, repeat the previous step (2.a), and use your MIDAS ID as the username and UIN as the password to reassess the FTP server from External Kali. Although External Kali may not access the

FTP server, you need to intercept the packets containing these "secrets" from the attacker VM, which is Internal Kali.



Description: I was able to locate my Midas Id and password, by using the FTP filter, and then after locating the packet, and following TCP stream.