## TASK A



1. Opened up Statistics, capture file properties to see 184 total and displaying all. Also located on bottom of first Wireshark pane. 184 packets in total and all 184 are being displayed because I did not apply a filter.

	🕎 Attacker Kali - External Workstation on CV301-JALI004 - Virtual Machine Connection		N - D X
<u>e</u>	File Action Media Clipboard View Help		
Recycle Bin	84 (0 🗩 🛛 🔍 💷 🕪 🦣 5 🖳 📸		
	Applications 👻 Places 👻 🛄 Wireshark 👻	Sat 20:10	1 4 / 40 0 -
~	"eth0	- 0	
2	Eile Edit View Go Capture Analyze Statistics Telephony Wirele	ss Tools Help	
Nmap – Zenman GUI	🖌 🖬 🦪 🕲 🛅 🎇 🖉 🔍 + + .2 (+ +) 🥅		
		Wireshark - Capture Fi	le Properties - etho
~	R icmp	Details	Y
a 📀	No. Time Source Destination	The second se	
Autania 558	+ 10 5.921930300 192.168.10.10 192.168.217.3	Interfaces	
	11 6.916221200 192.168.217.3 192.168.10.10 12 6.020020500 102.168.10.10 12 102.168.217.3	Interface Dropped Capture fil	ter Link type Packet size
	13 7.918144200 192.168.217.3 192.168.10.10	ath0 0 (0 %) none	Limit Ethernet 262144 bytes
Wiresbark	1 14 7 921835668 102 188 18 18 19 192 188 217 1	e cono o to ny mone	Lucinci Iblivi bjici
	Frame 9: 98 bytes on wire (784 bits), 98 bytes captures	d Statistics	11. 14. Alexand 10.
	<ul> <li>Internet Protocol Version 4, Src: 192.168.217.3, Dst:</li> </ul>	Measurement Captured Di	splayed Marked
	Internet Control Message Protocol	Packets 184 96 Time span c 100.093 47	(52.2%)
Weiself		Average pps 1.8 2.0	0 -
Login info	<b>1</b>	Average packet 83 98	· _
	0000 00 15 5d 40 57 1f 00 15 5d 40 57 05 08 00 45 00	size, B	00.001.7001 0
	0010 00 54 25 5f 40 60 46 01 b0 eb c0 a8 d9 03 c0 a8	Average bytes/s 152 19	-0
VMware	0030 98 08 08 08 08 00 21 80 07 40 98 01 58 01 07 63 98 89	Average bits/s 1,218 1,5	597 —
Workstation	0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25		
	0060 36 37	Capture file comments	
		- 1	
	Internet CoI: Protocol Packets: 184 · Displayed: 96 (52.2%) · Dro	0	
		☐Help	oard Sclose DiSave Comments
		August and a second sec	Helo Det
			Ju.edu
• 0 H 1	🛛 Honer, V. Mananer 💦 nFrense - Frenzell f 👘 Attacker Kale - Eder 🧖 Uburbu fal det	nn E-	o 51 de <sup>810</sup>

2. Apply "ICMP" as a display filter in Wireshark. Then repeat the previous question (Q1). After applying the filter icmp (internet control message protocol), WireShark will display 96 of the original 194 packets.



	🖳 Attacker Kali - External Workstatio	n on CV301-IALI004 - Virtual Machine Connection				- 🗆 ×	►.
0	File Action Media Clipboar	d View Help					
Recycle Bin	B 0 🗩 🛛 🕛 🖬 🕩 🧕	2 豆 種					
	Applications - Places -	🧱 Wireshark 🕶	Sat 20:16		1 4	: / **) () *	
~			*eth0			- 0 -	
	File Edit View Go	Capture Analyze Statistics Tele	shony Wireless Tools Help				1
Nmap -	1 = 1.0/					v.	
Zenmap GUI			Wireshark · Packet 10 · eth0		000	L.	ION
61	I icmp	[Checksum Status: Good]			-	Expression	V
	No. Time	Îdentifier (BE): 1869 (8×	074d)				
Nutania 558	9 5.9145	Identifier (LE): 19719 (6 Sequence number (BE): 1 (	x4d07)			4d, seq=1	
	11 6.9162	Sequence number (LE): 256	(8×9180)			4d, seq=2	
	12 6.9398	[Request frame: 9]				4d, seq=2	
	13 7.9181	Timestamp from icmp data:	Feb 4, 2023 20:07:38,0000	00008 EST		4d, seq=3	
Wiresbark	15 8.9191	Trimestamp from ionp data	(relative): 0.231473700 se	conds]		4d, seq=4	
	16 8.9268	Data (48 bytes)	e1112131415161718191ath1c16	itetf		4d, seq=4	
	17 5.5212	[Length: 48]			*	4d, seq=5	
	M	•)			(F)	10	
VM-sali	+ Frame 10: 98	0000 60 15 50 46 57 05 60 15 0010 60 54 c0 16 60 00 3f 65	50 40 57 17 08 00 45 00 57 3a c0 a8 0a 0a c0 a8	_]@W _]@W E T ? W:			
Logininto	Internet II,	0020 d9 03 00 00 29 0d 07 40	00 01 5a 01 df 63 00 00	····) ··· M ··· Z··· c···			
	Internet Cont	0030 60 66 64 60 60 60 80 0040 16 17 18 19 1a 1b 1c 10	10 80 10 11 12 13 14 15 1e 1f 20 21 22 23 24 25	**************************************			
		0050 25 27 28 29 2a 20 2c 2c	2e 2f 30 31 32 33 34 35	å° <u>()*+,/012345</u>			
VMware		0060 36 37		27			
Workstation	60						
	<b>100</b>						a defende
	P						A CONTRACTOR OF THE OWNER OF THE
	0000 00 15 5d						
	0028 d9 03 00						
	8030 88 68 d4						NA STA
	HI 0050 26 27 28	BHelp			≭ <u>C</u> lose		Help Desk:
	0060 36 37					5	lu.edu
							-
📲 🔎 🛤 📑	Hyper-V Manager 📃 👰 pFsens	e - Firewall 6	Ubuntu 64-bit on C			~	2/4/2023

3. Selected echo message from link using the icmp (internet control message protocol) filter, double clicked, information can be found in bottom of pane but also in Internet Protocol dropdown. Information is as follows:

Source IP is 192.168.10.10, Dst IP is 192.168.217.3; sequence number is 1; size of data is 48 bytes; response time is located at bottom of first pane 5.92... ms.

	🕎 Attacker Kali - External Workstation on CV301-JAL1004 - Virtual Machine Connection	- 0	×
0	File Action Media Clipboard View Help		
Recycle Bin	1a 0 € <b>0 0 11 1</b>		
	Applications - Places - 🔛 Wireshark -	Sat 20:18 🚺 😼 🖌 🐗	0 -
		*eth0	p
	File Edit View Go Canture Analyze Statistics Telephony Wireles	es Tads Help	ender werden eine eine eine eine eine eine eine e
Minapie	The For Yew So Subject Supple Supple Supple	a Toole Tech	
Zenmap GUI		Wireshark - Capture File Properties - eth0 🔘	
11	d dns	Datala	
	No Time Source Destination	Libbarana	Y .
Nutaria 558	18.00000000 192.168.217.3 192.168.217.2	Interfaces	
	2 8.000006900 192.168.217.3 192.168.217.2 3 8.002227100 192.168.217.3 192.168.217.3	NAMES AND A DESCRIPTION OF A DESCRIPTION	
	4 8.062288200 192.168.217.2 192.168.217.3	nterrace Dropped Capture filter Link type Packet size	
	5 5.004574300 192.168.217.3 192.168.217.2	eth0 0 (0 %) none Ethernet 262144 byte	50
Wrethark	6 5.004582300 192.168.217.3 192.168.217.2 7 5.017316800 192.168.217.2 192.168.217.3	Statistics	
	4 5.017385260 192.108.217.2 197.168.217.3	statistics	
	19 10.010405800 192.168.217.3 192.168.217.2	Measurement Captured Displayed Marked	
	N 1	Packets 184 84 (45.7%) -	
VIL- OF	+ Frame 8: 54 bytes on wire (432 bits), 54 bytes captured	Average pps 1.8 0.8 -	
Login info	Ethernet II, Src: Microsof_40:57:1f (00:15:5d:40:57:1f)	Average packet 83 68 -	
terms the second second	<ul> <li>Internet Protocol Version 4, Src: 192.108.217.2, DSL: 1</li> <li>User Datagram Protocol, Src Port: 53, Dst Port: 39122</li> </ul>	size, B	
	Domain Name System (response)	Bytes 15246 5670 (37.2%) 0	
-		Average bytes/s 152 56 -	
Workstati	8	Avelage only's 1,220 Has	
		Capture file comments.	176
	- <b>F</b> .		
	1 3000 00 15 5d 40 57 05 00 15 5d 40 57 1f 08 00 45 00	1	100 million (1990)
	0020 d9 03 06 35 98 d2 06 14 e2 03 d0 5d 81 05 06 00	Bliefe Befrech Corry To Clinhoard * Clore Di Save Corry	ments
		arrent a copy to capopare a 2mse at save come	initia j
	•••		Help Desk:
			du actor
			10.000
			and the second second
📲 🔎 🖽 闄	🙀 Hyper V Manager 👘 🧶 pFsense - Firewall 6 🧶 Attacker Kali - Exter 🧶 Ubuntu 64-bit c	an Ciu	∧ ₩ 4 818 PM 2/4/2023

4. Applied DNS (domain name system) display filter in Wireshark, 84 of the original 184 are displayed.



5. Found a DNS query packet by looking at the description "query" to located the correct packet. The domain name the host is trying to resolve is debian.pool.ntp.org and can be found within the message as shown above. The source IP and port number is **192.168.217.3**: **43905** and destination IP and port number is **192.168.217.2**: **53**.

6. Found the corresponding DNS response by looking at the listing description as I am following the flipped IP address. Source is now destination and vice versa. Also, Wireshark also has information of response and request, which can be found by expanding DNS row within listing. The source IP and port number is 192.168.217.2: 53 and the destination source IP and port number is 192.168.217.3: 43905. The response is "refused" meaning DNS refuses to preform operations. This is because the VM is not connected to the internet.

## TASK B

## 1. Sniff ICMP Traffic



Therese	tions - Places -	📃 Wireshark 🕶	Wed	12:52			1 4	1	<b>*(i)</b> (i) <b>*</b>	.12	1 10 0	<u>е</u> .
			*eth0				00	0	4			
2	File Edit View Go	Capture Analyze Statisti	lcs Telephony Wireless ]	Tools <u>H</u> elp								
	🖌 🔳 🧷 💿 🔈	* P 🖏 🕅	+ + + 🛄 🚍		17							
8	icmp					8 ·	Expression	+				
N	lo. Time	Source	Destination	Protocol L	ength Info		1					
2	• 299 76.259171	300 192.168.217.3	192.168.10.10	ICKP	D8 Echd (p1)	g) request	10=0×0					
-	308 76.260151	/08 192.168.10.10	192.168.217.3	ICMP	98 Echo (pi	ng) reply	id=6x8					
-	301 77.264239	400 192.168.217.3	192.168.10.10	ICMP	98 Echo (pi	ng) request	id=8x0					
	302 77.265139	500 192.168.10.10	192.168.217.3	ICMP	98 Echo (pin	ng) reply	id=8×8					
~	307 78.275885	300 192.168.217.3	192.168.10.10	ICMP	98 Echo (p1)	ng) request	1d=0×0					
•	308 /8,2/0304	200 192,108,10,10	187, 188, 717, 3	11 11 12	108 FCD0 (01)	HII FROIV	10-0×0					4
	210 70 007755	C 710 991 991 991	100 100 10 10	TOND	no Fabo (ale	at contract	14-0-0					
	310 79.267755 311 70 274022 Frame 299: 98 by Ethernet II, Src Internet Protoco Internet Control	700 192.168.217.3 748 102.168 18 18 tes on wire (784 bits : Microsof_40:57:16 ( l Version 4, Src: 192 Message Protocol	192.188.10.10 102.188.217.3 ), 98 bytes captured 00:15:5d:40:57:10), D 2.168.217.3, Dst: 192.1	ICMP TCMP (784 bits) on Ost: Microsof_ 158.10.10	98 Echo (pi 98 Echo (pi 98 Echo (ni 10 Ech	g) request a) reals 5:5d:40:57:	id=0x0i id=8x8i id=8x8i id=8x8i					
	310 79.267755 311 70.274922 Frame 299: 98 by Ethernet II, Src Internet Protoco Internet Control	780 192.168.217.3 780 102.168.217.3 tes on wire (784 bits : Microsof.40:57:1e ( l Version 4, Src: 192 Message Protocol	192.168.10.10 103.188.217.3 1), 98 bytes captured 00:15:5d:40:57:10), D 2.168.217.3, Dst: 192.	ICMP TrMp (784 bits) on Sst: Microsof 160.10.10	98 Echo (pir 98 Echo (nir 108 Echo (nir 101 Echo (00:1) 10:57:00 (00:1)	g) request	ld=0x0 id=0x0					
	310 79.267755 S11 70.274922 Frame 299: 98 by Ethernet II, Src Internet Protoco Internet Control	700 192.108.217.3 704 103 108 14 10 tes on wire (784 bits : Microsof_40:57:10 ( l Version 4, Src: 192 Message Protocol 57 0c 00 15 5d 40 5	192 168 10.10 103 168 217 3 1), 96 bytes captured 00:15:54:40:57:10), D 2.168.217.3, Dst: 192. 7 1c 08 68 45 69	(784 bits) on Dst: Microsof. 168.10.10	98 Echo (pir 98 Echo (nir interface 0 40:57:0c (00:1	g) request	1d=0x0 id=8x0 id=8x0 9					-
	310 79.267755 511 70.274922 Frame 299: 98 by Ethernet II, Src Internet Protoco Internet Control	700 192.108.217.3 700 103 108 10 10 tes on wire (784 bits : Microsof.40:57:12 ( l Version 4, Src: 192 Message Protocol 57 0c 00 15 5d 40 5 56 00 3f 01 f0 f2 ci	192.168.10.10 103.168.217.3 (), 98 bytes captured (00:15:5d:40:57:10), D (.168.217.3, Dst: 192.) 7 1c 08 00 45 60] 7 1c 08 00 45 60] 7 1c 08 00 45 60]	10MP TrMD (784 bits) on 581: Microsof. 168.10.10 10W 18W E M0.7	98 Echo (pir 98 Febo (nu interface 0 40:57:00 (00:1)	g) request m) renu	1d=0x0: id=8x0:					
	310 79.267755 311 70.274872 Frame 299: 98 by Ethernet II, Src Internet Protoco Internet Control 0010 00 54 dc 57 0010 00 54 dc 57 0020 04 06 09	700 192.108.217.3 704 102.108.217.3 704 102.108.10 10 tes on wire (784 bits : Microsof.40:57.10 ( l Version 4, src: 192 Message Protocol 57 0c 00 15 5d 40 5 40 00 3f 01 f0 f2 c 84 99 06 00 00 10	192.168.10.10 103.188.217.3 5), 90 bytes captured (00:15:5445:7:10), D t.168.217.3, Dst: 192. 7 1e 00 00 45 00 1 2 a8 d9 03 c0 a8 T 5 1b ed 63 00 00	1000 1000 7700 (784 bits) on 551 Nicrosof_ 158.10.10 1000 1000 000 0 000 0 000 0 0 0	98 Echo (pi as r-ha fri interface 0 10:57:00 (00:1	g) request	1d=0x0 id=8x0 id=8x0 9C)					
	310 79.267755 311 70.274822 Frame 29: 98 by Ethernet II, Src Internet Protoco Internet Control 00 54 c6 57 020 60 60 80 60 032 60 60 60 60 033 60 60 60 60 040 60 10 10 040 60 10 10 040 60 10 040 60 10 040 60 10 040 60 10 040 60 10 040 60 60 040 60 60 040 60 60 040 60 040 040 60 040 60 040 60 040 60 040 60 040 60	700 192.108.217.3 704 102.108.217.3 704 102.108.14.10 tes on wire (784 bits : Microsof_40:57:10 ( l Version 4, Src: 192 Wessage Protocol 57 0c 00 15 5d 40 5 40 00 3f 01 f0 f2 ct 84 99 06 00 00 10 53 00 00 00 00 00 01 53 00 00 00 00 00 01	192 168 10.10 193 168 217 3 b), 96 bytes captured (0:15:56:40:57:10), D 1.168.217.3, Dst: 192. 7 1e 08 60 45 60 1 1e 03 c6 a6 1 1e 12 13 14 1e	1000 Trime (784 bits) on St: Nicrosof. 166.10.10 10W 10W E W0 ? 0 C	98 Echo (pi as Echo (ni interface 0 10:57:00 (60:1)	g) request nl reniv	1d=0x0 id=8x0 0c)					-
	310 79.267755 311 70.274822 Frame 299: 98 by Ethernet II, Src Internet Protoco Internet Control 0010 00 54 c6 57 0020 00 46 86 80 0030 00 66 53 3046 16 17 10 19 0050 26 27 28 29	700 192.108.217.3 700 102.108.217.3 tes on wire (784 bits : Microsof.40:57:10 ( l Version 4, Src: 192 Message Protocol 57 0c 00 15 5d 40 5 40 00 3f 01 f0 f2 ci 84 99 06 06 00 01 0 59 00 00 06 00 01 0 59 00 00 06 00 01 1 10 15 1c 1d 1e 1f 2 2 2 25 20.2 2 2 f 3	192.168.10.10 193.168.217.3 s), 96 bytes captured (00:15:5d:40:57:10), D 2.168.217.3, Dst: 192. 7 1c 06 00 45 00 1 2 a6 d9 03 c0 a6 T 5 1b cd 63 00 00 11 12 13 14 15 21 22 23 24 25 31 52 33 34 35	1000 1000 1000 (784 bits) on 581 Nicrosof, 168.10.10 1000 - 100 000 - 0 000	98 Echo (pi as prha fri interface 0 40:57:00 (00:1)	g) request n) rentv 5:5d:40:57:	1d=0x0 id=0x0; id=0x0; 0c)			ľ		
	310 79.267755 311 70.274822 Frame 299: 98 by Ethernet II, Src Internet Protoco Internet Control 0010 00 54 c6 57 0040 16 71 18 19 0050 00 90 90 30 0040 16 71 18 19 0050 26 27 28 29 0066 30 37	700 192.108.217.3 700 102.108.217.3 700 102.108.10.10 tes on wire (784 bits : Microsof.49:57:10 ( 1 Version 4, Src: 192 Message Protocol 57 0c 00 15 5d 40 5 40 00 3f 01 f0 f2 ct 84 99 06 00 01 f0 f2 ct 35 00 00 00 00 01 10 f0 f2 ct 35 00 00 00 00 00 01 10 1b 1c 1d 10 f1 f2 20 2b 2c 2d 2c 2f at	192 168 10.10 192 168 217 3 •), 96 bytes captured (00:15:5d:40:57:10), D 100:217.3, Dst: 192. 7 1c 08 00 45 00 1 0 a8 d9 03 c0 a8 T 5 1b cd 63 00 60 11 12 13 14 15 5 1b cd 63 00 60 11 12 13 14 15 5 12 22 24 25 5 31 52 53 54 35	1000 1000 1000 (784 bits) on 551 Nicrosof_ 158.10.10 1000 100 1000 1000 1000 1000 10000 1000 1000 1000 1000 1000	98 Echo (pi 98 Echo (ni interface 9 10:57:00 (09:1	9) request	id=0x0i id=nvni 0c)					-
	310 79.267755 311 70.274822 Frame 29: 98 by Ethernet II, Src Internet Protoco Internet Control 00 54 e6 57 026 0a 68 08 0938 09 69 26 33 0404 16 17 18 19 0550 26 27 28 29 0660 36 37	700 192.108.217.3 704 102.108.217.3 704 102.108.14.10 tes on wire (784 bits : Microsof_40:57:10 ( l Version 4, Src: 192 Wessage Protocol 57 0c 00 15 5d 40 5 40 00 3f 01 f0 f2 ct 84 99 06 00 00 10 93 00 00 00 00 00 11 a 1b ct 10 i = 1f 2 20 2b 2c 2d 2c 2f 30	192       168       10       10         193       168       217       3         5)       96       bytes       captured         60:15:53:40:57:10)       D       10       10         7.168.217.3       Dst: 192       192         7       16.08       60       11         0       36       90       30       66       66         11       12       13       14       16       14         21       22       22       24       25       13       13       15         31       32       33       34       35       64       67	1000 Trime (784 bits) on St: Nicrosof. 168.10.10 10W 10W E W0 ? ? 8 C X3 1'st ()**, ./01234	98 Echo (pi as Echo (ni interface 0 10:57:00 (00:1)	g) requést	14=9x0i id=8x0i id=8x0i					-
	310 79.267755 311 70.274822 Frame 299: 98 by Ethernet II, Src Internet Protoco Internet Control 0010 00 54 c6 57 0020 00 46 56 33 0040 16 17 18 19 0055 26 27 28 29 0050 36 37	700 192.108.217.3 700 102.108.217.3 700 102.108.10.13 tes on wire (784 bits : Microsof.40:57:12 ( l Version 4, Src: 192 Message Protocol 57 0c 00 15 5d 40 5 40 00 3f 01 f0 f2 ci 84 00 03 f01 f0 f2 ci 84 00 06 00 00 10 59 00 00 00 00 01 0 59 00 00 00 00 11 in 15 ic 1d 1e 1f 2 2a 2b 2c 2d 2e 2f 30	192.168.10.10 193.168.217.3 s), 96 bytes captured (00:15:5d:40:57:10), D 2.168.217.3, Dst: 192. 7 1c 06 09 45 09 0 a6 d9 03 c0 a6 T 5 1b ed 63 00 09 0 11 12 13 14 15 2 12 22 23 24 25 5 11 52 33 34 35 4 (07	1000 1000 1000 (784 bits) on 581 Nicrosof, 168.10.10 1000 - 100 000 - 100 000 0	98 Echo (pi as Frha fri interface 0 40:57:00 (00:1)	99) requést	14=9x0i id=8x0i 0					
	310 79.267755 311 70.274822 Frame 299: 98 by Ethernet II, Src Internet Protoco Internet Control 0015 00 54 c5 40 00 54 c5 457 002 00 64 56 36 004 06 36 36 004 06 36 36 004 06 36 36 004 06 36 37 005 00 30 005 00 37 005 00 30 005 000000000000000000000000000000000	700 192.108.217.3 700 102.108.217.3 700 102.108.10.10 tes on wire (784 bits : Microsof.49:57:10 ( l Version 4, Src: 192 Message Protocol 57 0c 00 15 5d 40 5 40 00 37 01 fo 12 ci 84 99 00 co 00 31 01 fo 12 ci 84 99 00 co 00 01 10 11 fo 12 10 10 10 10 11 fo 17 2 2a 2b 2c 2d 2c 2f 3	192 166 10.10 192 168 217 3 a), 96 bytes captured (00:15:5d:40:57:10), D 2.108.217.3, Dst: 192. 7 1c 08 00 45 60 0 a6 45 03 c0 a8 7 1c 08 00 45 60 11 12 13 14 15 15 1b ed 63 00 60 11 12 13 14 15 12 12 24 25 5 31 32 33 34 35 07	1000 1000 1000 1000 1000 1000 1000 100	98 Echo (pi 98 Echo (ni interface 9 10:57:00 (09:1	ig) requést	14=9x0i id=8x9;					
	310 79.267755 311 70.274822 Frame 29: 98 by Ethernet II, Src Internet Protoco Internet Control 0054 e6 57 026 0a 68 08 0938 09 09 06 36 37 026 36 37 027 Internet Control	700 192.108.217.3 700 102.108.217.3 700 102.108.10.10 1 tes on wire (784 bits : Microsof_40:57:10 ( l Version 4, Src: 192 Wessage Protocol 57 0c 00 15 5d 40 5 40 00 37 01 f0 f2 ct 84 99 06 00 00 10 53 00 20 00 00 00 10 53 00 20 00 00 00 11 10 15 ct 10 10 17 2 20 2b 2c 2d 2c 2f 33 Message Protocot: Protoco	192_168_10.10 193_168_217_3 a), 96 bytes captured (00:15:54:40:57:10), D 2.168.217.3, Dst: 192. 7 1e 08 60 45 00 0 a6 49 63 c6 a6 7 1b ed 63 06 00 11 12 13 14 15 12 12 24 425 3 1 32 33 34 35 1 Packets: 14	1000 1000 1000 (784 bits) on 551: Nicrosof 166:10:10 100	98 Echo (pi as Echo (ni interface 9 10:57:0c (09:1)	ig) requést s:51:40:57: 5:5(1:40:57:	1d=0x0i id=0x0i d=0x0i oc)			Ē/		

and the second second second	liew Help										
• • • • • • • • • • • • • • • • • • •	12 d										
ations = 🛛 Places = 🗧	Wireshark -	Wed	13:11			·*	1	*0 0 -		# /	10 0
		*eth0			h	00	0		100		
File Edit View Go C	apture Analyze Statisti	cs Telephony Wireless 1	Tools Help								
1 = 1 @ b		💻 🖂 بد ما د 🐛		Ŧ							
		*	444	<u>E</u>			_				
ip.src == 192.168.217.3	&& icmp && ip.dst == 192	168.10.10			8 = - ·	Expression_	+				
No. Time	Source	Destination	Protocol Lei	info			-				
9 0.165631400	192.168.217.3	192,166,10.10	ICMP	98 Echo (ping	) request	1d=0x0					
37 1.167797800	192.168.217.3	192.168.10.10	ICMP	98 Echo (ping	) request	id=0x0					
67 2.170531800	192.168.217.3	192.168.10.10	ICMP	98 Echo (ping	) request	id=0x0					
95 3.173007300	192.168.217.3	192.168.10.10	ICNP	98 Echo (ping	) request	id=0x0					
123 4.171241600	192.168.217.3	192.168.10.10	ICMP	98 Echo (ping	) request	id=0x0					
158 5.175763000	192.168.217.3	192.168.10.18	ICMP	98 Echo (ping	) request	1d=0x0				- 6	
187 6.178825100	192.168.217.3	192.168.10.10	ICMP	98 Echo (ping	) request	id=0x0					
210 7 1707952AA	192 168 217 7	192 168 18 16	TOMP	og Frhn Ininn	) request	id=8v8	-				
<ul> <li>Frame 9: 98 bytes</li> <li>Ethernet II, Src:</li> <li>Internet Protocol</li> <li>Internet Control M</li> </ul>	on wire (784 bits), Microsof_40:57:1e ( Version 4, Src: 192 Wessage Protocol	98 bytes captured (7 09:15:5d:40:57:1e), D .168.217.3, Dst: 192.	84 bits) on int st: Microsof_40 168.10.10	terface G 0:57:0c (00:15:	5d:40:57:	θς)			5 5 5 5		
<ul> <li>Frame 9: 98 bytes</li> <li>Ethernet II, Src:</li> <li>Internet Protocol</li> <li>Internet Control M</li> </ul>	on wire (784 bits), Microsof_40:57:1e ( Version 4, Src: 192 Wessage Protocol	98 bytes captured (7 00:15:5d:40:57:1e), D .168.217.3, Dst: 192.	84 bits) on int st: Microsof_40 168.10.10	terface © 0:57:0c (00:15:	5d:40:57:	θc)			5 5 5 5 5 5 5		
• • Frame 9: 98 bytes • Ethernet II, Src: • Internet Protocol • Internet Control M	on wire (784 bits), Nicrosof_40:57:1e ( Version 4, Src: 192 Wessage Protocol	98 bytes captured (7 00:15:5d:40:57:10), D .168.217.3, Dst: 192.	84 bits) on int st: Microsof_46 168.10.10	terface 0 0:57:0c (00:15:	50:40:57:	θc)			* * * * * * * * * *		
<ul> <li>Frame 9: 98 bytes</li> <li>Ethernet II, Src:</li> <li>Internet Protocol</li> <li>Internet Control M</li> </ul>	on wire (784 bits), Microsof_40:57:1e ( Version 4, Src: 192 Wessage Protocol	98 bytes captured (7 00:15:5d:40:57:1e), D .168.217.3, Dst: 192.	84 bits) on int st: Microsof_48 168.10.10 ]8W ]8W E	terface 0 0:57:0c (00:15:	5d:40:57:	ec)			* * * * * * * * * *		
<ul> <li>Frame 9: 98 bytes</li> <li>Ethernet II, Src:</li> <li>Internet Protocol</li> <li>Internet Control M</li> <li>0800</li> <li>60 15 5d 46 5</li> <li>060 64 58 66 40</li> </ul>	on wire (784 bits), Microsof_40:57:1e ( Version 4, Src: 192 essage Protocol 7 0c 00 15 5d 40 55 3 00 3f 01 de db co	98 bytes captured (7 09:15:5d:40:57:1e), D .168.217.3, Dst: 192. 7 1e 08 00 45 00 - 1 9 a6 d9 03 c0 a8 - T	84 bits) on int st: Microsof_46 168.10.10 18W ]0W E n@ ?	terface 0 0:57:0c (00:15:	5d:40:57:	8c)			* * * * * * * * * * *		
• • Frame 9: 98 bytes • Ethernet II, Src: • Internet Protocol • Internet Control M 0000 00 15 5d 40 5 0010 00 54 78 6e 40 0010 00 54 78 6e 40	on wire (784 bits), Microsof_40:57:1e ( Version 4, Src: 192 lessage Protocol 7 0c 00 15 5d 40 55 3 00 37 01 de db c5 3 7b 06 e0 04 4e bi	98 bytes captured (7 09:15:5d:48:57:1e), D .168.217.3, Dst: 192. 7 1e 08 00 45 00 - ] 0 88 d9 03 C0 88 - T 1 1e d6 3 00 00	84 bits) on int st: Microsof_40 168.10.10  0W  0W -E n0 ? 9{ N c	terface 0 0:57:9c (00:15:	5d:40:57:	8c)			* * * * * * * * * * * * *		
<ul> <li>Frame 9: 98 bytes</li> <li>Ethernet II, Src:</li> <li>Internet Protocol</li> <li>Internet Control M</li> <li>0000 00 15 5d 40 5</li> <li>0054 78 66 4</li> <li>0000 00 64 78 66 4</li> <li>0000 00 66 4 c0 60</li> <li>0000 00 66 4 c0 60</li> </ul>	on wire (784 bits), Microsof_40:57:1e ( Version 4, Src: 192 essage Protocol 7 0c 00 15 5d 40 53 3 00 37 01 de db c6 3 7b 66 e0 04 4e bb 7 09 00 00 01	98 bytes captured (7 09:15:56:44:57:1e), D .168.217.3, Dst: 192. 7 1e 08 00 45 00 - ] 9 a8 d9 03 c0 a8 -T 1 1f ed 63 00 00 11 12 13 14 15 - 1	84 bits) on int st: Microsof_46 168.10.10 [8W ] 8W E n@ ? _9{ N C	terface 0 0:57:0c (00:15:	:5d:49:57::	8c)			* * * * * * * * * * * * * *		
<ul> <li>Frame 9: 98 bytes</li> <li>Ethernet II, Src:</li> <li>Internet Protocol</li> <li>Internet Control M</li> <li>0000 00 15 5d 46 5</li> <li>0010 00 54 78 56 44</li> <li>0020 06 54 78 66 44</li> <li>0020 06 42 06 6</li> <li>0040 16 17 18 19 14</li> <li>0050 16 77 28 29 27 28 29</li> </ul>	on wire (784 bits), Microsof_40:57:1e ( Version 4, Src: 192 lessage Protocol 7 0c 00 15 5d 40 57 3 00 37 61 de db c5 3 7b 06 e0 04 4e bi 7 06 00 00 00 01 a 1b 1c 1d 1e 1f 20 a 2b 2c 2f 2c 2f 36	98 bytes captured (7 09:15:56:48:57:1e), D .168.217.3, Dst: 192. 7 1e 08 00 45 06 1 9 88 09 03 c0 88 1 1 16 46 3 00 09 11 12 13 41 5 - 1 21 22 23 24 25 31 32 23 34 35 8'	84 bits) on int st: Microsof_46 168.10.10  @w _ ]@w _ E n@ ? 9{ N c !"#5%	terface 0 0:57:0c (00:15:	5d:40:57:	0c)			* * * * * * * * * * * * * * * * * * *		
<ul> <li>Frame 9: 98 bytes</li> <li>Ethernet II, Src:</li> <li>Internet Protocol</li> <li>Internet Control M</li> <li>0000</li> <li>00 15 5d 46 57</li> <li>0010</li> <li>00 54 78 56 40</li> <li>0000</li> <li>00 60 64 c0 66</li> <li>0000</li> <li>17 18 19 11</li> <li>015 26 27 28 29 26</li> </ul>	on wire (784 bits), Microsof_40:57:1e ( Version 4, Src: 192 Lessage Protocol 7 0c 00 15 5d 40 57 3 00 37 01 de db c5 3 7b 06 00 04 4e b4 7 00 00 00 00 16 a 1b 1c 1d 1e 17 22 a 2b 2c 2d 2e 2f 36	98 bytes captured (7 09:15:56:40:57:1e), D .168.217.3, Dst: 192. 7 1e 08 06 45 06 · ] 88 09 03 c0 a8 · · 11 12 13 14 15 · L 9 12 12 23 34 35 & ( 9 31 32 33 34 35 & ( 07	84 bits) on int st: Microsof_46 168.10.10 ]@W n@ ? 9 { N 9 { N !"#5% ()*+,/012345	terface 0 0:57:0c (00:15:	5d:40:57:	ec)			* * * * * * * * * * * * * * *		
<ul> <li>Frame 9: 98 bytes</li> <li>Ethernet II, Src:</li> <li>Internet Protocol</li> <li>Internet Control M</li> <li>Internet Control M</li> <li>0000 00 15 5d 40 5</li> <li>0010 00 54 78 66 44</li> <li>0020 6a 6a 68 06 33</li> <li>0030 00 66 4c 06 67</li> <li>0040 16 17 18 19 11</li> <li>0050 26 27 28 29 24</li> <li>0060 36 37</li> </ul>	on wire (784 bits), Microsof_40:57:1e ( Version 4, Src: 192 essage Protocol 7 0c 00 15 5d 40 57 3 00 37 01 de db c6 3 7b 66 e0 04 de bb 7 00 00 00 00 16 a 1b 1c 1d 1e 1f 26 a 2b 2c 2d 2e 2f 36	98 bytes captured (7 09:15:5d:48:57:1e), D .168.217.3, Dst: 192. 7 1e 08 00 45 00 - 1 9 a8 d9 03 c0 a8 -T 1 1f ed 63 00 00 0 11 12 13 14 15 - 1 9 21 22 23 24 25 - 1 9 31 32 33 34 35 & 1 67	84 bits) on int st: Microsof_46 168.10.10 168.10.10 168.7 9{ N C 1"#5% ()*+,/012345	terface 0 0:57:0c (00:15: 5 5	5d:40:57:	8c)					
• • Frame 9: 98 bytes • Ethernet II, Src: • Internet Protocol • Internet Control M 0050 00 54 78 56 44 0050 60 54 78 59 20 0060 15 17 18 19 11 0055 26 27 28 29 20	on wire (784 bits), Microsof_40:57:1e ( Version 4, Src: 192 lessage Protocol 7 0c 00 15 5d 40 57 3 00 37 01 de db c5 3 7b 06 e0 04 de bi 7 00 06 00 00 16 a 1b 1c 1d 1e 1f 26 a 2b 2c 2d 2e 2f 36	90 bytes captured (7 00:15:5d:40:57:1e), D .160.217.3, Dst: 192. 7 1e 08 00 45 00 - 1 8 A8 09 03 C0 A8 - 1 1 1f ed 63 00 00 - 1 11 12 13 14 15 - 1 2 21 22 22 42 25 - 1 3 13 22 33 34 35 & () 67	84 bits) on int st: Microsof_46 168.10.10 168.10.10 168.10.10 168.10.10 168.10.10 168.10.10 168.10.10 168.10.10 168.10.10	terface 0 0:57:0c (00:15: 5	5d:40:57:	8c)					
<ul> <li>Frame 9: 98 bytes</li> <li>Ethernet II, Src:</li> <li>Internet Protocol</li> <li>Internet Control M</li> <li>00 54 78 56 40</li> <li>00 54 78 56 43</li> <li>00 68 68 06 33</li> <li>00 69 64 cc 66 6</li> <li>00 69 17 18 19 11</li> <li>00 56 26 27 28 29 24</li> <li>00 60 36 37</li> </ul>	on wire (784 bits), Microsof_40:57:1e ( Version 4, Src: 192 Lessage Protocol 7 0c 00 15 5d 40 57 3 00 37 01 de db c5 3 7b 06 00 04 4e b4 7 00 00 00 09 01 16 a 1b 1c 1d 1e 1f 26 a 2b 2c 2d 2e 2f 36	98 bytes captured (7 09:15:56:40:57:1e), D .168.217.3, Dst: 192. 7 1e 08 00 45 00 - ] 0 88 09 03 C0 88 1 11 21 31 44 15 - L 0 12 12 23 34 35 & ' 0 31 32 33 34 35 & ' 67	84 bits) on int st: Microsof_46 168.10.10  BW  CW E n@:7 9 N C !*#S% ()*+,/012345	terface 0 0:57:0c (00:15:	:5d:40:57::	0c)			* * * * * * * * * * * * * * * * * * * *		
<ul> <li>Frame 9: 98 bytes</li> <li>Ethernet II, Src:</li> <li>Internet Protocol</li> <li>Internet Control M</li> <li>Internet Control M</li> <li>0000 00 15 5d 40 5</li> <li>0010 00 54 78 5c 44</li> <li>0020 6a 6a 68 66 33</li> <li>0030 66 4c 66 6</li> <li>0040 16 17 18 19 11</li> <li>0050 26 27 28 29 24</li> <li>0060 36 37</li> </ul>	on wire (784 bits), Microsof_40:57:1e ( Version 4, Src: 192 lessage Protocol 7 0c 00 15 5d 40 57 3 00 3 01 de db c5 3 7b 06 e0 04 4e bi 7 06 00 00 00 00 10 a 1b 1c 1d 1e 1f 26 a 2b 2c 2d 2e 2f 36	96 bytes captured (7 09:15:56:46:57:1e), D .168.217.3, Dst: 192. 7 1e 08 00 45 06 1 9 a8 d9 03 c0 a8 1 1 1f c1 a6 3 00 06 1 1 11 21 14 15 1 2 12 22 32 42 5 3 1 32 33 34 35 87 07 00000000000000000000000000000000	84 bits) on int st: Microsof_46 168.10.10  0W E n0 ? 9{ N c !"#5% ()*+,/012345	terface 0 0:57:0c (00:15: 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	-5d:40:57::	BC }	dt	•	* * * * * * * * * * * * * * * * * * * *		
<ul> <li>Frame 9: 98 bytes</li> <li>Ethernet II, Src:</li> <li>Internet Protocol</li> <li>Internet Control M</li> <li>Internet Control M</li> <li>0050 60 15 5d 46 5;</li> <li>0050 60 34 78 5e 44</li> <li>0050 60 64 c0 6 6;</li> <li>0050 60 64 c0 6 6;</li> <li>0050 26 27 28 29 2;</li> <li>0060 36 37</li> <li>0 72 wireshark_eth0.;</li> </ul>	on wire (784 bits), Microsof_40:57:1e ( Version 4, Src: 192 lessage Protocol 7 0c 00 15 5d 40 5j 000 3f 01 de db cc 3 7b 06 e0 04 4e bi 7 06 06 00 00 16 a 1b 1c 1d 1e 1f 2c a 2b 2c 2d 2e 2f 36 20230215130852_ywe523	96 bytes captured (7 09:15:56:46:57:1e), D .168.217.3, Dst: 192. 7 16 08 00 45 00 - 1 0 88 09 03 c0 a8 - 7 1 1f ed 63 00 00 11 12 13 14 15 - 1 0 21 22 23 24 25 - 67 9 31 32 33 34 35 & 4'( 67 pcapng Packets:1	84 bits) on int st: Microsof_40 168.10.10  @W - E n@ ? 9{ N c !"#S% ()*+,/012345	terface 0 0:57:0c (00:15: 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	-5d:40:57:1 0 (0.0%) 8	Bc) Profile: Defau	alt		**************		
<ul> <li>Frame 9: 98 bytes</li> <li>Ethernet II, Src:</li> <li>Internet Protocol</li> <li>Internet Control M</li> <li>Internet Control M</li> <li>00 15 5d 40 57</li> <li>00 54 78 66 40</li> <li>00 66 4c 66 67</li> <li>00 66 4c 66 67</li> <li>00 66 4c 78 29 20</li> <li>06 63 37</li> <li>36 37</li> <li>wireshark_eth0_2</li> </ul>	on wire (784 bits), Microsof_40:57:1e ( Version 4, Src: 192 essage Protocol 7 0c 00 15 5d 40 57 3 00 3f 01 de db c6 3 7b 66 e0 04 4e bi 7 00 00 00 00 16 a 1b 1c 1d 1e 1f 22 a 2b 2c 2d 2e 2f 30 20230215130852_yxe523.	98 bytes captured (7 09:15:5d:46:57:1e), D .168.217.3, Dst: 192. 7 1e 08 00 45 00] 9 A8 09 03 c0 a8 -T 11 12 13 14 15 - L 9 13 22 23 24 25 9 31 32 33 34 35 & 'C 67 pcapng Packets:1	84 bits) on int st: Microsof_46 168.10.10  @W - E n@ ? 9 { N c !"#5% ()*+,/012345	terface 0 0:57:0c (00:15: 5 5 5(3.5%)-Dropped:	0 (0.0%) <b>f</b>	BC) Profile: Defau	alte		5 2 5 2 5 2 5 2 5 2 5 2 5 2 5 5 5 5 5 5		
<ul> <li>Frame 9: 98 bytes</li> <li>Ethernet II, Src:</li> <li>Internet Protocol</li> <li>Internet Control M</li> <li>Internet Control M</li> <li>0000 00 15 5d 46 5</li> <li>0010 00 54 78 56 44</li> <li>0020 0a 0a 08 00 33</li> <li>0030 00 54 78 56 44</li> <li>0020 0a 0a 08 00 33</li> <li>0030 0a 04 c0 06 97</li> <li>0030 16 17 18 19 11</li> <li>0050 26 27 28 29 24</li> <li>0060 36 37</li> <li>2 wireshark_eth0_2</li> </ul>	on wire (784 bits), Microsof_40:57:1e ( Version 4, Src: 192 lessage Protocol 7 0c 00 15 5d 40 57 3 00 3f 01 de db cc 3 7b 6d e0 04 4e bi 3 1b 1c 1d 1e 1f 26 a 2b 2c 2d 2e 2f 36 20230215130852_yxe523.	98 bytes captured (7 09:15:56:48:57:1e), D .168.217.3, Dst: 192. 7 1e 08 06 45 06 1 0 a8 d9 03 C0 a8 1 1 1f e6 3 00 06 1 0 11 12 13 14 15 1 0 21 22 23 24 25 1 3 1 32 33 34 35 & '( 67 pcapng Packets: 1	84 bits) on int st: Microsof_40 168.10.10 168.10.10 168.7 9{ N C 1°#5% ()'+,/012345	terface 0 0:57:0c (00:15: 5 5 (3.5%)-Dropped:	(5d:40:57:) 0 (0.0%) {	Bc) Profile: Defau	4		* * * * * * * * * * * * * * * * * * * *		

Explanation: Opened two terminals on Ext. Kali VM and used "ping" command to create traffic for Ubuntu (192.168.10.10) and Int. Kali (192.168.19.13). Then applied "icmp" display filter on Int. Kali VM

to view ICMP traffic. Lastly, I applied proper display filter "ip.src = 192.168.217.3 && icmp && ip.dst. == 192.168.10.10" on Internal Kali VM that ONLY displays ICMP request originating from External Kali VM and going to Ubuntu 64-bit VM. The first part of the display filter specifies where the traffic came from while the second part defines the type of traffic, and the last or third part defines the destination. The operators && mean that all conditions must be met to display packet.

## 2. Sniff FTP Traffic

0	₽ Kal	- lietamä/ Viorist	tation an	CVIDI-JAL004 - Vetsal Machine Connection			- 🗆 ×	
Recyc	File	Action Media	Atta	acker Kali - External Workstation on CY301-JALI	04 - Virtual Machine Connection		- 1	I X D X
	Apoli	rations	File	Action Media Clipboard View Hel				
	rippe	Cathorns	B 0	) • 🛛 🔍 💷 🕨 🚺 b 🗮 👬				THE OWNER WATER OF THE OWNER OF
		File Edit	Appli	ications * Places * 🗈 Termin	5at 23:45		1 4 / 4	
Nm Zenm					Capturing from eth0	- 0 s		Sala a
				File Parts Contraction	root@CS2APenTest: ~	000		READ.
		Apply a c		File Edit View Search	Terminal, Help			
Nutar	1	No. 716		A contection to 102 168 1	p 192.168.10.10	Contraction of the local division of the loc		
	1965	717		No. 220 (vsFTPd 3.0.3)		Bankho, Lingui Ing.		
		719	-	Name (192.168.10.10:ro 331 Please specify the	ot): cyse301 password.	And Distant		1829 H
6	•	728		Password:		C 100		1.1
Wire		+ Frame 1		Remote system type is	UNIX.	24 2220		12.51
		Etherne	-	Using binary mode to t	ransfer files.	and the second		P.C.
	M	Transmi		221 Goodbye.		That was to an an an		
VM.				· Inconcentration www.		1997 B		
aagir	n	-	M	· Dokata Kine Sector (Antes				ALC: NO
	-	0090 00	120					53098
-	1	0010 00 0020 0a		4) 606				1988
Werk	8	0030 72	1	0010				2.53
	-			083		1 Sector		1000
	F			965				22
		@ ? eth	P					6.28
	-		-	0 7 eth0: <live capture="" in="" progr<="" td=""><td>ess&gt; Packets: 291 - Displayed: 291 (100.</td><td>0%) Profile: Default</td><td></td><td>645 A</td></live>	ess> Packets: 291 - Displayed: 291 (100.	0%) Profile: Default		645 A
	A							NS8 .
			0					sk:
			1					100
	م	Lt: 1	Hyper	-V Manager 💿 pFsense - Firewall 6	Dountu 64-bit on C 🛞 Attacker Kali - Ester	🕽 Kali - Internal Work		



Explanation:

a) Ubuntu VM is also serving as an FTP server inside the LAN network. I use External Kali to access this FTP server by using the command: ftp 192.168.10.10. The username for the FTP server is cyse301, and the password is password. I followed the steps in the photo to access the FTP server and also exited. I have created FTP traffic. While the password I typed did not show up in the terminal, it will in the traffic packets.

b)Unfortunately, Internal Kali, the attacker, is also sniffing to the communication. Therefore, all of my communication is exposed to the attacker. Now, I found out the password used by External Kali to access the FTP server from the intercepted traffic on Internal Kali by using Wireshark on Int. Kali and applying the filter "ftp && ip.addr. 192.168.10.10". Which means I am looking for ftp traffic originating from Ubuntu. The information I need is found the Info column.

c)I repeat this process from part b in the terminal on Ext. Kali. but the only thing that changes is my username (jali004) and password (01166237), and I also establish a connection again because I logged out. In the last screenshot we can see what the password is in the column labeled info.

TASK C

1. Extra Credit: Steal files with Wireshark





Explanation: Logged into to Ubuntu VM, and created a file in my home directory with the command "echo -e "\$(date) \nAli Jessica>jali.txt" and put the current timestamp and my name in the file. The first part is creating the contents while the second part of the command is naming/creating the actual file. I

also double checked that I had created it correctly with the "ls" command and called on the filled to check the contents with the "cat" command. I then switched back to Ext. Kali to see the file I just created with FTP protocol remotely. I did this connecting again with the command ftp 192.168.10.10 and logged into cyse301 with the password, password. Once the connection was established, I then used the "get jali.txt" command to successfully access the file, and waited for the code 226 transfer complete. Therefore creating ftp traffic. Lastly, using Wireshark on Int.Kali VM I applied the display filter (ftp-data) to display the FTP-DATA packets between External Kali and Ubuntu VM and followed the tcp steam of the FTP-DATA packet, viewed the content of the jali.txt and then exported the it as a text file in Int.Kali. Ultimately to view the content of my jali.txt file. I saved the file on Int. Kali's desktop so I could access it easier as illustrated in my last screenshot above.