Assignment 2 Report

Traffic Tracing and Sniffing

Each student needs to login into the CCIA virtual environment to complete this assignment. Please make sure to power on the pfsense VM at all times to keep the VMs connected.

Task A: Get started with Wireshark (5 point each x 6 questions = 30 points)

In this task, you will be using Wireshark on External Kali to monitor the traffic when External Kali and Ubuntu VM are talking to each other.



You should keep Wireshark running in the background while performing the following tasks.

1. Open Wireshark on External Kali and listen on interface "eth0".

2. Open a new terminal, then ping the Ubuntu VM for 5 – 10 seconds.

3. Open a new web browser tab in Kali Linux (even if no webpage will be displayed), and keep it for

a couple of seconds.

4. Stop capturing (the red button on the tool bar).

Now, answer the following questions. You need to provide a screenshot that contains the answers

to each question.

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



I was running for 1 minutes and captured 719 packets and displayed 719.

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

🖳 Kal	i - Internal Workstation on CY301-BNAJA001 - Virtual Machine Connection	-		×
File	Action Media View Help			
h C				
2	📰 🛅 🍃 🍏 🕒 🗸 📋 2 3 4 🛛 🌢 🕞 📶	15:43	₽	Ģ
۵.	🚄 •eth0 🔿 🖓 😵			0
	File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help			
÷	□ @ _ ⊑ 🗎 🔯 Q ← → ∩ ← → 📰 📃 🗖 🗖 🗖 🖬 🖬 🖬 🖬 🖬 🖬 🖬 🖬 🖬 🖬 🖬 👘 🖬 👘 👘 👘 👘 👘 👘 👘 👘 👘 👘 👘 👘 👘		ย	=
°⊂ K	🖪 lænp 🛛 🖾 🕤 + 🔤 Vessus Essentials / Fo 🖻 Home 🔀 Apache	2 Debian Del	fau	»
	No. Time Source Destination Protocol Length Info 112 5. 020954900 192.168.10.13 192.168.10.13 102.168.10.16 192.168.10.13 192.168.10.13 17 6.010801700 192.168.10.13 192.168.10.13 192.168.10.13 104.10 18 6.011991100 192.168.10.13 192.168.10.13 ICMP 98 Echo (pi) 19 7.012553100 192.168.10.13 192.168.10.13 ICMP 98 Echo (pi) 20 7.012553100 192.168.10.13 192.168.10.13 ICMP 98 Echo (pi) 130 131.917470400 192.168.10.13 192.168.10.2 ICMP 125 Destinat 131 131.917495600 192.168.10.2 ICMP 115 Destinat 132.131.917455600 192.168.10.2 ICMP 115 Destinat 133 131.917455600 192.168.10.2 ICMP 125 Destinat 132.131.917455600 192.168.10.2 ICMP 125 Destinat 133 131.917455600 192.168.10.2 ICMP 1			
	134 341.917551200 192.168.10.13 192.106.10.2 ICMP 116 Destinat			
	 Frame 133: 123 bytes on wire (984 bits), 12: 000 00 15 5d 40 57 29 00 15 5d 40 57 24 08 Ethernet II, Src: Microsoft_40:57:24 (00:15 0010 00 6d c0 05 00 00 40 01 24 6b c0 a8 0a Internet Protocol Version 4, Src: 192.168.1(00:26 0a 02 03 03 92 ab 00 00 60 06 04 50 00 Internet Control Message Protocol 00 00 40 11 bc ff c0 a8 0a 02 c0 a8 0a Domain Name System (response) 00 00 40 13 63 6f e 74 65 6e 74 2d 73 69 00 00 00 41 15 61 00 3d df 84 b5 78 18 20 00 10 00 			
	Activate Wind Go to Settings to			
⊟÷	💿 🎼 Hyper-V Manager 🛛 💩 Kali - Internal Work 💩 Ubuntu 2204-64-bit	^ 『	<u>ふ</u> (10)	3:43 PM 7/4/2024

When I applied ICMP displayed packet changed to 22 and packets still the same 719.

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?

🖳 Ka	i - Internal	Workstation on CY30	1-BNAJA00	1 - Virtual Mac	hine Connect	ion											-		×	
File	Action	Media View H	elp																	
Ba C		0 🛛 🖬 🕨 🔂	5 1																	
2		🗖 🌛 😂 🔚	- 1		· 🐸 (o 4 0								(genmon)XX	x 🔹 🇯		16:06	♠	G	
-						*eth0														
<u> </u>	File	Edit View Go	Capture	e Analyze	Statistics	Telephony	Wireless Too	ols <u>H</u> elp												
←	1		1 🕋 🕅		2 4 -	• ∩ • €	→ • 📃 📕		0 192					1				്		
*4 K							Wires	shark - Packet	18 - eth0				🗙 Fo	Nome 🔁	Here Apach	e2 Deb	ian Def	au		
	No. + + + + Eti No.	Time 7 3.005532 8 3.007708 9 4.007251 10 4.009722 11 5.009212 12 5.020544 17 6.010921 18 0.011921 19 7.012553 20 7.015658 20 7.01568 20 7.015688 20 7.0156888 20 7.0156888 20 7.015688 20	Sc 300 11 300 12 300 12 300 12 100 12 10	ource 92.168.5 92.168.6 92.168.1 92.168.1 92.168.3 92.168.3 92.168.3 92.168.3 92.168.3 92.168.4 92.168.4 92.168.4 92.168.4 92.168.4 92.168.4 92.168.5 92.169.5 92.169.5 92.169.5 92.169.5 92.169.5 92.169	<pre>> Inte > Inte > Inte > Inte > Inte - Inte - Inte</pre>	rnet Proto rnet Contr pe: 0 (Ech de: 0 ecksum: 0x hecksum 3 extentifier (entifier (quence Num quence Num quence Num quence Num quence Num quence Num duestamp fr imestamp fr imestamp fr imestamp fr de 5d 5d 6 05 5d 5f 8 sec. 60199100- opacket bytes s: 719- Displat	col Version ol Message P io (ping) rep 2:2666 [correc atus: Good] BE): 39596 (LE): 4186 (ber (BE): 7 ber (LE): 4186 (ber (SE): 7 ber (LE): 4186 (ber (LE): 4	4, Src: : Protocol Ply) ct] (0x9aac) (0xac9a) (0xa	192.168.10.11 00) , 2024 15:25 ive): 0.0012 57 32 08 00 . Co a8 0a 12 reply id=0x9aac, sec (0.0%) Profile	8, Dst: 192 :54.2431176 25800 secon : c0 a8 =7/1792 ttl=64 (n x Clos e: Default	2.168.10 900 EDT nds] .]@W\$.]@w:] MHelp	ess th gain	ie						
														Activ Go to	/ate Wir Settings t					

The Source is 192.163.10.18 and destination is 192.168.10.13. the sequence number (BE) is 7 and (LE) is 1792 and size of the data is 40 bytes. The respond time 1.189 millisecond.

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

File	Action	Media	View H	elp																				
b C	0	0 1	1	5																				
۲			🍅 도 ·	- 1	2	3	4	۵	Co 🚄	4														
•	4								*eth0														8	
	<u>F</u> ile	<u>E</u> dit <u>V</u> i	ew <u>G</u> o	<u>C</u> apt	ure <u>/</u>	Analyz	ze <u>S</u> ta	atistic	s Telep	hony	<u>W</u> irel	ess	Too	ols	<u>H</u> el	р								
÷	11		© .		X	6	۹	~ -	⇒ ∩	• + +	•			÷	-			1						
™ Ka				-	_	_															_	- -		Vessus Es
	No	۹ Tim		_	Course				Da	stinatio					Drot	acel	1.0	n ath	Inf		-			
	INO.	21 11	ie 7.69881	6200	192.	.e 168.	10.13	3	19	2.168	л .10.2	2			DNS	.000	Le	ngth 88	St	o and	ard			
		22 117	7.69883	4300	192.	168.	10.13	3	19	2.168	.10.2	2			DNS			88	St	and	ard			
		23 117	7.87055	5300	192.	168.	10.13	3	19	2.168	.10.2	2			DNS	2		79	St	and	ard			
		24 11	96626	5400	192.	168	10.13	\$	19	2.108	10.2	2			DNS			95	St	and	ard			
		26 118	3.96628	4100	192.	168.	10.13	3	19	2.168	.10.2	2			DNS			95	St	and	ard			
		27 120	9.04021	4000	192.	168.	10.13	3	19	2.168	.10.2	2			DNS			87	St	and	ard			
		28 120	9.04024	1300	192.	168.	10.13	3	19	2.168	.10.2	2			DNS	5		87	St	and	ard			
		29 120	9.70786	9500	192.	168.	10.13	3	19	2.168	.10.2	2			DNS			85	St	and	ard			
		31 12	1.19115	5200	192.	168.	10.13	3	19	2.168	.10.2	2			DNS			97	St	and	ard			
	- Erec		00 hu			17	704 h	ita)	00 bi		00	15	Ed	40	57	20	00	15	Ed	40	57	24	00	
	> Ft	hernet	TT Sr	es of es Mi	crose	e (/	10:57	:24	(00:15	0000		15 4a	5u 6e	40 d2	40	00	40	10	36	71	0	24 a8	00 0a	
	Int	ternet	Protoco	ol Ve	rsior	1 4,	Src:	192	.168.10	0020) 0a	02	b1	eb	00	35	00	36	95	a7	02	cc	01	
	▶ Use	er Data	gram Pi	rotoc	ol, §	SrcF	Port:	4554	17, Ds1		00	00	00	00	00	00	07	63	6f	6e	74	69	6c	
	 Dor 	nain Na	me Syst	tem (query	()				0040	65	72	76	69	63	65	73	07	6d	6f	7a	69	6C	
										0050	63	61	6d	00	00	01	00	01						r pormit
																								is permit
	_																							
	02	Domai	in Name	Systen	n: Prot	tocol	Pa	ackets	: 719 - Di	splaye	d: 124	(17.2	%) -	Dro	ppe	d: 0 (0.09	6)	Pro	file: I	Defa	ult		

🕎 Kali - Internal Workstation on CY301-BNAJA001 - Virtual Machine Connection

Above I highlighted Pckets:719 and Displayed: 124

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.

🖳 Kali	- Interna	Workst	ation on	CY301-	BNAJAO	/01 - Virt	rtual Ma	chine	e Conn	ection												
File	Action	Media	a Viev	w Help	p																	
h O		0	II IÞ	1 🎰 🙏	5 🖳																	
1		- 6	. 🍅	۶ ۷	1	2	3	4	۵	5	4											
6											eth0											
	<u>F</u> ile	<u>E</u> dit	View	<u>G</u> o	<u>C</u> aptur	re <u>A</u> r	nalyze	e <u>S</u> t	tatisti	ics T	elepho	ony <u>v</u>	Vireles	s <u>T</u> ool	ls <u>H</u> elp	b						
÷			10) 🖬	1110	8	3	۹	÷	→	Ĥ ••	÷ →•				0						
™s Ka	I dr	ıs												Wiresh	hark • Paci	ket 24 · eth0)					🙁 Fo.
	No. Fr Et Jn Uso V	21 2 22 2 23 2 24 2 25 2 26 2 27 2 28 2 29 2 30 3 31 2 30 3 31 2 4 berne terne er Da main Trans Flags 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.	Ime 117.6 117.6 117.8 117.8 117.8 117.8 120.0 120.0 120.0 120.0 120.0 120.0 120.7 120.7 121.1 4: 79 t II, t A: 79 t II, t A: 79 t II, * agra sactic * 00.0 * 00.0 * 00.0 * 00.0 * 00.0 * 00.0 * 00.0 * 00.0 * 00.0 * 00.0 * 00.0 * 00.0 * 00.0 * 00.0 * 00.0 * 00.0 * 00.0 * 00.0	98816 98834 70555 66265 66284 40214 40214 40214 907868 91155 9 byte Src: ptocol am Pro Syste on ID 9100 : 0 0 0 Jame S	S 200 1 300 1 300 1 400 1 100 100 1 100 100 1 100 100 1 100 100 100 100 100 100 100 100 100 100	in the second se	<pre>168.1 1</pre>	Na V	 Fracket Fracket Fracket Fracket 	ame 2 herne serne Sour Desti Leng Checi [Stri [Time IStri [Time 1 0. .0 00 <i>Time</i> : 1 w pac	24: 79 it II, it Pro atagra ce Pool inatio th: 48 Ksum: cksum iestam paylo Name sacti s: 0x 00 0. 15 5 117.8706 ket byt	<pre>9 bytt , Src btoco am Pr rt: 4 0 0 95 0 x95 5 Stat ndex: ps] ad (3 Syst 0 100 0 100 0 ad 40 34600 ces</pre>	es on : Mic l Ver otoco 17105 i9e [u : U : 1] : 7 byt em (q): 0xa Stand 	wire rosoff sion 4 1, Sro 3 nveri nveri es) uery) d82 lard q = 9 00 1 192.168.1 192.168.1	(632 t_40:5 4, Src ; Port fied] fied] uery Respor Opcode 5 5d 0.139	bits), 7:24 (0 : 192.1 : 47105 : 47105 : Stand : 0 (0.0%	79 byt 0:15:5 68.10. , Dst ssage i iard qu 24 08 6 <i>ard query</i>) Prof	es cap d:40:5 13, Ds Port: is a qu Jery (6 00 45 6 0xad82 AA 0xad82 AA	tured 7:24), t: 192 53 53 53 90 90 90 90 90 90 90 90 90 90 90 90 90	(632 DSt: .168. .168.	bits) Micro 10.2	o ≥ss gai

Above on the screenshot I highlighted the source IP and port number, destination IP and port number.

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?



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.

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

🕎 Attacker Kali - Ex	ternal Workstation on CY301-BNAJA001 - Virtual Machine Connection	
File Action	Kali - Internal Workstation on CY301-BNAJA001 - Virtual Machine Connection	
🖿 🕘 🖲 🧕 F	File Action Media View Help	
3		
	🖏 📖 🚞 🍃 🍪 🕒 🗸 🕇 1 2 3 4 🛛 🗆 🧟	a line
	*eth0	
\leftarrow \rightarrow (File <u>E</u> dit <u>V</u> iew <u>Go</u> <u>C</u> apture <u>A</u> nalyze <u>S</u> tatistics Telephony <u>W</u> ireless <u>T</u> ools <u>H</u> elp	
🛰 Kali Linux	← 📶 📕 🔏 @ 🕞 📾 🕅 🞯 🔍 ← → ቡ ← → 💻 📰 🖬 🖬 🖬 🖬	
		Nessus I
Burnet	M Ip.addr== 192.168.10.13&&icmp	
Otenable	No. Time Source Destination Protocol Length into 142 225.866607200 192.168.217.3 192.168.10.13 ICMP 98 Echo (p	ing) r
FOLDERE	← 143 225.866659100 192.168.10.13 192.168.217.3 ICMP 98 Echo (p 145 226 866698200 192 168 217 3 192 168 10 13 ICMP 98 Echo (p	ing) r
FOLDERS	146 226.866736600 192.168.10.13 192.168.217.3 ICMP 98 Echo (p	ing) r
My Scan	148 227.868734400 192.168.217.3 192.168.10.13 ICMP 98 Echo (p 149 227.868776000 192.168.10.13 192.168.217.3 ICMP 98 Echo (p	ing) r jing) r
All Scan:	150 228.874042200 192.168.217.3 192.168.10.13 ICMP 98 Echo (p	ing) r
🔟 Trash	151 220.874964400 192.160.10.13 192.168.217.3 1CMP 98 Echo (p 152 229.875732000 192.168.217.3 192.168.10.13 ICMP 98 Echo (p	ping) r
RESOURCES	153 229.875772800 192.168.10.13 192.168.217.3 ICMP 98 Echo (p 154 230.891809600 192.168.217.3 192.168.10.13 ICMP 98 Echo (p	ning) r
Policies	Frame 142: 08 bytes on wire (784 bits) 08 1 0000 00 15 5d 40 57 24 00 15 5d 40 57	7 20 69
Plugin P	Ethernet II, Src: Microsoft_40:57:29 (00:15) 0010 00 54 aa 18 40 00 3f 01 2d 2f cd	0 a8 d9
Tarrage	Internet Protocol Version 4, Src: 192.168.2: 0020 0a 0d 08 00 86 5a 96 a7 00 01 53 Internet Control Message Protocol 0030 00 00 37 69 0a 00 00 00 00 10	3 5a 87 9 11 12
(e) Terrasca	0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20	9 21 22
	0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 0060 36 37	9 31 32 is permi
	Dackate: 210. Displayed: 14 (4 5%) . Drafile: De	foult
🧿 👪 Hyper	r-V Manager 🛛 🧶 Attacker Kali - Exter 🐙 Kali - Internal Work 🌷 Ubuntu 2204-64-bit	

To see the traffic from the internal kali and the attacker, I used command (ip.addr==192.168.10.13&&icmp), to display the traffic.

b. Apply a proper display or capture filter on the internal Kali VM that ONLY displays the ICMP request that originated from the external Kali VM and goes to the Ubuntu 64-bit

VM.

🕎 Kali - Internal Workstation on CY301-BNAJA001 - Virtual Machine Co	nnection	
File Action Media View Help		
🖦 🔘 💿 🔘 🔰 💵 🕨 🔂 5 🕎 👬		
📉 🔲 🗖 🍃 🍪 🖭 v 🛛 1 2 3 4 🛛 🗉		
🔞 🖉	*eth0	
<u>File E</u> dit <u>View Go</u> Capture <u>Analyze Statis</u>	stics Telephon <u>y W</u> ireless <u>T</u> ools <u>H</u> elp)
* A Solution A Solu	→ ∩ ·← →· 📑 🔳 🖬 🖬	
Ka icmp&&ip.dst==192.168.10.18		Nessus Esse
Time Source 38 78.056472800 192.168.217.3	Destination Protocol Le 192.168.10.18 ICMP	ngth Info 98 Echo (ping) request
40 79.071588000 192.168.217.3	192.168.10.18 ICMP	98 Echo (ping) request
44 81.082553300 192.168.217.3	192.168.10.18 ICMP	98 Echo (ping) request
46 82.066447100 192.168.217.3	192.168.10.18 ICMP	98 Echo (ping) request
52 84.092154100 192.168.217.3	192.168.10.18 ICMP	98 Echo (ping) request
54 85.084274000 192.168.217.3	192.168.10.18 ICMP	98 Echo (ping) request
56 86.082526100 192.168.217.3	192.168.10.18 ICMP	98 Echo (ping) request
56 67.061200200 192.106.217.5	192.100.10.10 ICMP	so Echo (ping) request
 Frame 58: 98 bytes on wire (784 bit Ethernet II, Src: Microsoft_40:57:2 Internet Protocol Version 4, Src: 1 Internet Control Message Protocol 	s), 98 by 0000 00 15 5d 40 57 9 (00:15 0010 00 54 5f 45 40 92.168.2: 0020 0a 12 08 00 4c 0030 00 00 f2 84 0d 0040 16 17 18 19 1a 0050 26 27 28 29 2a 0060 36 37	32 00 15 5d 40 57 29 08 00 3f 01 77 fd c0 a8 d9 c8 9d 15 00 0a c8 59 87 00 00 00 00 00 10 11 12 1b 1c 1d 1e 1f 20 21 22 2b 2c 2d 2e 2f 30 31 32 is permitted
Bytes 58-97: Data (data data)	Dackets: 807 - Displayed	· 10 (1 2%) È Profile: Default
	The second	
😏 📷 Hyper-V Manager 🛛 🛬 Attacker Kali - Exter	🣚 Kali - Internal Work 🚬 Ubuntu 2204-64	-Dit

The screenshot shows on display filter Wireshark the exact command that ONLY displays the ICMP request that originated from the external Kali VM

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 ubuntu VM]. The username for the FTP server is cyse301, and the password is password. You can follow the steps below to access the FTP server.



I don't know, if I open the wrong terminal but every time I tried it, it says incorrect login, I can't move forward, see the screenshot above.

b. Unfortunately, Internal Kali, the attacker, is also sniffing into the communication. Therefore, all of 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 take a screenshot and explain how you found the password.

🖳 Kali	- Internal Workstation on CY301-BNAJA001 - Virtual Machine Connection														
File	ile Action Media View Help														
h 6	🖲 🞯 ڬ 💵 🕨 🖄 🖄														
Š	📰 🚞 🍃 ڬ 🖳 🗸 📘 2 3 4 🛛 🧆 📶														
1	*eth0	3													
	<u>File E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture <u>A</u> nalyze <u>S</u> tatistics Telephony <u>W</u> ireless <u>T</u> ools <u>H</u> elp														
4	📶 🔲 🗟 🎯 🖪 🛅 📓 🙆 오 < → Դ < ↔ 🜉 📃 🛛 🖬 🖽 🎬														
The Ka	I ftp +	- N													
	Source Destination Protocol Length Info														
	192.168.217.3 192.168.10.18 FTP 81 Request: PASS password														
	192.168.10.18 192.168.217.3 FTP 88 Response: 530 Login incorrect														
	192.168.10.18 192.168.217.3 FTP 80 Response: 221 Goodbye.														
	192.168.10.18 192.168.217.3 FTP 86 Response: 220 (vsFTPd 3.0.5)														
	192.108.217.3 192.108.10.18 FTP 80 Request: USER Cyse301 192.168.10.18 192.168.217.3 FTP 100 Response: 331 Please specify 1														
	192.168.217.3 192.168.10.18 FTP 81 Request: PASS password														
	192.168.10.18 192.168.217.3 FTP 88 Response: 530 Login incorrect														
	192.168.217.3 192.168.10.18 FTP 72 Request: QUIT														
	Frame 1218: 81 bytes on wire (648 bits), 81 0000 00 15 5d 40 57 32 00 15 5d 40 57 29 0 Frame 1218: 81 bytes on wire (648 bits), 81 0000 00 15 5d 40 57 32 00 15 5d 40 57 29 0	8													
	▶ Internet Protocol Version 4. Src: 192.168.21 0020 0a 12 bb 38 00 15 29 7a 1e 00 3a a5 c	9 e													
	> Transmission Control Protocol, Src Port: 47! 0030 7f e5 23 c6 00 00 01 01 08 0a d5 1f a	1													
	File Transfer Protocol (FTP) 0040 45 16 50 41 53 53 20 70 61 73 73 77 6	f													
	[current working directory:] 0050 0a	is													
	File Transfer Pro. 1 (FTP): Protocol Packets: 1998 · Displayed: 35 (1.8%) · Dropped: 0 (0.0%) Profile: Default														

I use ftp to display the data that is store in external kali, as a result login is incorrect. I believe I am doing something wrong I don't know what it is.

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

reaccess 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.



File	Action	Media	View	Help															
B. C	0	0	I IÞ	2 2	🖳 🔒														
~		1	🝅 🛯] ~	1 2	3	4	۵ 🖉										Armahan and an an	🗂 (ge
6	4								*eth0								• *		
	File	Edit	<u>V</u> iew (<u>50 C</u> a	pture	Analyz	e <u>S</u> tat	istics	Telep	hony <u>V</u>	<u>/</u> ireless]	ools <u>F</u>	<u>H</u> elp						
÷			0	E I		6	<i>م</i>	- <i>></i>	ц,	• · ••		÷	•						
°≒ Ka	📕 ftp														×	D •]+	Nessus Essentials / F	Fo 📘
	rce			Des	tinatio	n		Prot	tocol	Length	Info						-		
	1.168.	217.3		192	2.168.	10.18		FTP		72	Request	: QUIT	Coodby		-				
	1.168.	10.18		19.	2.168.	217.3		FTP		86	Respons	e: 221	(vsFTF	7e. Pd 3.0).5)				
	2.168.	217.3		192	2.168.	10.18		FTP		81	Request	: USER	≀ bnaja0	001					
	1.168.	217 3		192	2.168.	217.3		FTP		100	Respons	 e: 331 • PASS 	Please	e spec	ify t	he pa	ISSWOI		
	1.168.	10.18		19:	2.168.	217.3		FTP		88	Respons	e: 530) Login	incor	rect.				
									12										
	 Fra Eth Int Tra Fi 	ame 19 hernet ternet ansmis le Tra urrent	: 81 II, Prot sion unsfer work	bytes Src: Dcol Contr Prot ing d	on wi Micros Versio ol Pro ocol (irecto	ire (6 soft_4 on 4, otocol (FTP) orv: 1	48 bit 0:57:2 Src: 2 , Src	ts), 8 29 (00 192.10 Port:	31 by 0:15 58.2: : 57]	0000 0010 0020 0030 0040 0050	00 15 5 00 43 a 0a 12 6 7f f6 2 52 19 5 0a	id 40 5 if 3a 4 1 7e (29 b2 (55 53 4	57 32 00 40 00 3 90 15 e0 90 00 0 45 52 20	0 15 f 06 6 0c 1 01 0 62	5d 40 28 04 a3 5f 08 0a 6e 6f	0 57 2 4 c0 a 5 <mark>14 3</mark> a d5 4 L 6a 6	29 08 a8 d9 <mark>3c d6</mark> 4b bb 61 30		
						.,,,,,												is permitted to acce	ss the Jain
	• 2	wire	shark_e	th0OC	GMQ2	.pcapng		Packets	s: 56 ·	Displaye	d: 7 (12.5%) · Drop	ped: 0 (0.	0%)	Profile	: Defau	ult _i		
																			A C
G		Hyper-\	/ Manage	r	😍 Atta	cker Kali	- Exter	🧶 к	ali - Int	ernal Work	퇒 u	buntu 220	4-64-bit						

🕎 Kali - Internal Workstation on CY301-BNAJA001 - Virtual Machine Connection

Same thing happened when I tried my MIDAS ID.