CYSE 301: Cybersecurity Technique and Operations

Assignment 1: Traffic Tracing and Sniffing

Jason Rivers

01236524

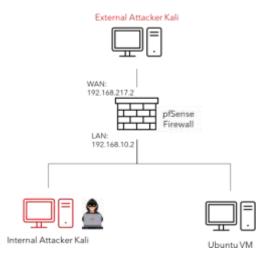
Each student needs to login into the CCIA virtual environment to complete this assignment.

Students use tshark will receive extra points.

Task B: Sniff LAN traffic

In this task, you will be acting as an **ATTACKER** who sniffs the regular communications between peers (External Attacker Kali and Ubuntu) by using either Wireshark or tshark on **Internal Attacker Kali VM**.

I would recommend you keeping the Wireshark/tshark running on Internal Kali all the time.



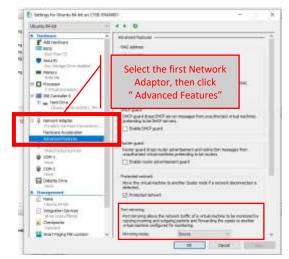


Figure 1 Required VMs for this assignment

Figure 2 How to configure port mirroring in Hyper-V

IMPORTANT NOTES!

* Because the current Hyper-V setting does not "broadcast" the communication between hosts in the same network, we need to <u>enable port mirroring</u> to allow Internal Kali to "see" other's communication. To be specific, you need to put the sniffer (Internal Kali) as the <u>mirroring Destination</u>, and the target VMs are <u>mirroring Source</u> (Figure 2). Since each VM has two network adapters, one for regular connection and the other is sharing with the CCIA server. We need to configure port mirroring on the first adapter. To be specific,

- Internal Kali: Set Miorroing mode to "*Destination*" in the "Port Mirroiring"
- Ubuntu Kali: Set Miorroing mode to "<u>Source</u>" in the "Port Mirroiring"
- External Kali: Set Miorroing mode to "Source" in the "Port Mirroiring"

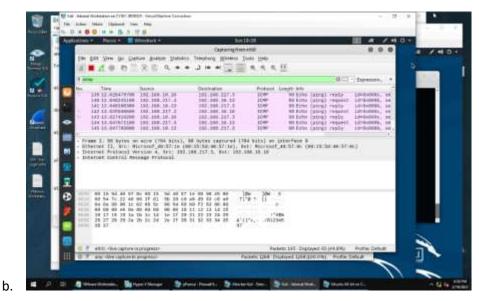
** Since each Windows 10 Host Machine has 20G memory. We need to adjust the assigned Memory for Internal Kali and External Kali from **8192** to **4096** MB to support 4 VM running simultaneously.

Attacker Kali - External Workstat	ion 🗸	ৰ ▶ ।ত					
 Hardware Add Hardware BIOS Boot from CD Security Key Storage Drive disabled 	^	Memory — Specify the amount of <u>R</u> AM: Dynamic Memory	fmemory that this v 4096	irtual machine can use. MB			
Memory 4096 MB		You can allow the a dynamically within	amount of memory a the range you set.	va gble to this virtual ma	chine to c	:hange	

1. Sniff ICMP traffic (10 + 10 = 20 points)

<u>Open two terminals on External Kali VM</u>. 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.



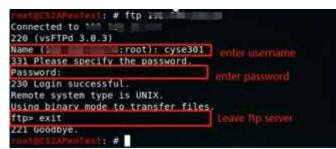
c. Apply proper display or capture filter on **Internal Kali VM** that ONLY displays **ICMP** request originated from <u>External Kali VM</u> and goes to <u>Ubuntu 64-bit VM</u>.

1000	tant + - Paris + - 🖬 Wrestant, 1		Gei3838		1 4 / 4	10-1
		a da an	94		0 0 0	# 1
	De Dit Ven in jatur fri	us Salata leastary more	a Jose Des			
			101 A A A A A	1000	Devicin. +	1000
	These are pairing that the second				Lagreener.	
100	DITE DIT. ADADDEAU DAY	Cantination (Cartination)	Protect Length	Error Lainel TreamyL	10-8w800. pr	
	2028 204 V26210089 287.754			sufm thing) request	1dTRabilit, 10	
	bils for atstrikes 197, 188			Film 101rd) repair	all-dubbers, an	
	2047 and appendiums and 200			solut (mirg) request		
	2013 401.024505400 152.150			Enter (ping) rement	10-Eulifide. an	
•	205.5 and arring 182.384			Rotes (prod) technol.	10-808001, 84	
	2012 AND ROADLINES 232.254	1.217.8. 292.286.27.38	10me au	Exempting) vesionst.	10-6906411.14**	
	Daternet Gentrol Hessage Are					
2						
0	101 04 15 50 45 57 ft 10 15	No 44 117 (or 301 64 48, 101	284 - 384 - 8			
100	THEF. BR 64 TO 22 49 20 3T 61	No 28 (8 all # 61 (# all	T(10 P 12			
100	AN UN UN DO DO 21 U2 00 01	NV 54 99 85 F2 01 HE 00 80 80 18 11 13 13 13 15	AND ALC: SPECIME			
	28 17 18 29 18 18 10 10 28		·····			
	38 27 26 29 38 38 30 30 38	De 17 36 31 22 33 54 35	BTERS, 1 WHERE			
	10.0 18.32		67			
_						×.
	7 withink and JULBINES	RDL.703EDApagerig	Fadette 347	Distance and charge	Porte Dred	
and the second s	7 and the right is management	Net Have Department	Robette M.M. Dissigned	SCHALLER PAGE WORKS D	STATUTE OF STREET, STR	

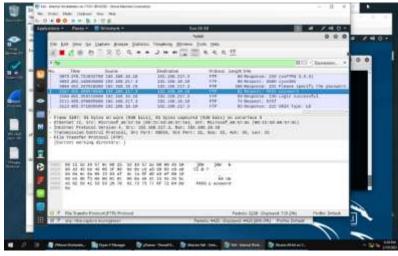
2. Sniff FTP traffic (10 + 15 + 15 = 40 pts points)

d.

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.

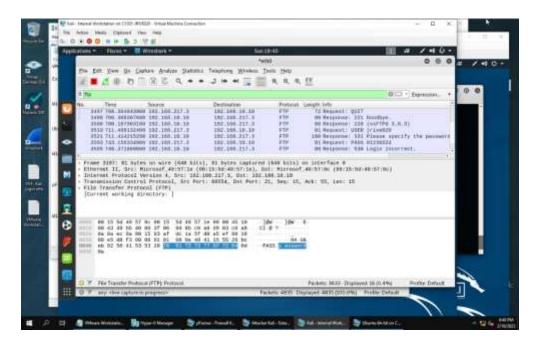


b. Unfortunately, Internal Kali, the attacker, is also sniffing to the communication. Therefore, all of your communication is exposed to the attacker. Now, you need to find out the password used by External Kali to access the FTP server from the intercepted traffic on Internal Kali. You need to screenshot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



I typed FTP into the Wireshark search bar, and saw the Username and password under info. Not very secure honestly.

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.



Task C – Extra credit: Steal files with Wireshark (15 points)

Login to Ubuntu VM, and create a file in your home directory, named "YOUR_MIDAS.txt". Put the current timestamp and your name in the file. You can use the following command in the example below to do the job.



Once you have the file ready in Ubuntu, switch back to **External Kali**. Get the file you just created with FTP protocol remotely. Below is an example.

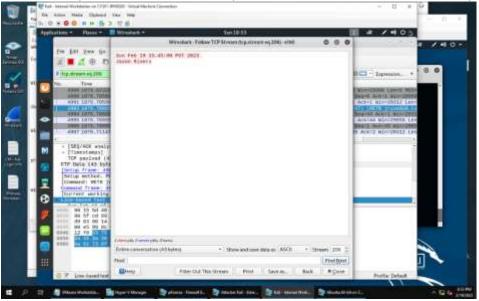
🕞 Attacker Kali - External W 🛛	pfsense - Firewall 64-bit	Kali - Internal Workstation	Windows 7 Workstation	× Windows Server 2
Applications * Places *	🖪 Terminal 🕶			Mon 15:01
		root@CS2	2APenTest: ~	
File Edit View Se	earch Terminal Help			
226 Director	and the second sec			
ftp> get pji				
	g.txt remote:			
	mand successfu			
		ita connection	for pjiang.txt	(41 bytes)
ZZO Transfer				
41 bytes rec	eived in 0.00	secs (63.4534	kB/s)	

As an attacker, you need to complete the following tasks in Internal Kali:

1. Apply a proper display filter to display the **FTP-DATA** packets between External Kali and Ubuntu VM.

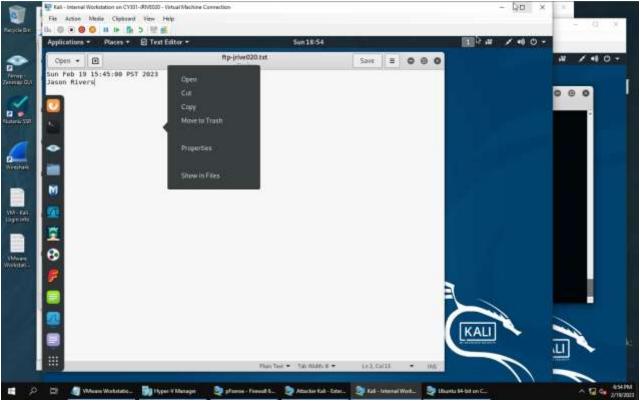
Here Here Particular Person Particular Person<	Replations - Name - Withdate -		Sec.18-49			
Comparing a problem (at bytes) The problem (at bytes) Problem (at bytes) TOP problem (at bytes) The problem (at bytes) Problem (at bytes) TOP problem (at bytes) The problem (at bytes) Problem (at bytes) TOP problem (at bytes) The problem (at bytes) Problem (at bytes) TOP problem (at bytes) The problem (at bytes) Problem (at bytes) TOP problem (at bytes) The problem (at bytes) Problem (at bytes) TOP problem (at bytes) The problem (at bytes) Problem (at bytes) TOP problem (at bytes) The problem (at bytes) Problem (at bytes) TOP problem (at bytes) The problem (at bytes) Problem (at bytes) TOP problem (at bytes) The problem (at bytes) Problem (at bytes) TOP problem (at bytes) The problem (at bytes) Problem (at bytes) TOP problem (at bytes) The problem (at bytes) Problem (at bytes) TOP problem (at bytes) The problem (at bytes) Problem (at bytes) TOP problem (at bytes) The problem (at bytes) Problem (at bytes) TOP problem (at bytes) Top (at bytes) Problem (at bytes) TOP problem (at bytes) Top (at bytes) Problem (at	Charles and the second of the					
Implement There Sparse Destination Produces Sparse Courteent Produces Sparse	Fie Fill View So Captore Audyor St	distics Telephong Works	n Tank Help			
Mile Data Time Destruction Protocol Land 10 MVV Data 10 MVV Mile All TDP prophese 43 bytes TDD '10 All 10 MVV Data 10 MVV Data 10 MVV Data 10 MVV Mile TDP prophese 43 bytes TDP 'non-los 146 bytes TDP 'non-los 146 bytes TDP 'non-los 146 bytes Mile TDP 'non-los 146 bytes TDP 'non-los 146 bytes TDP 'non-los 146 bytes TDP 'non-los 146 bytes Mile TDP 'non-los 14 bytes TDP 'non-los 146 bytes TDP 'non-los 146 bytes TDP 'non-los 146 bytes Mile TDP 'non-los 14 bytes TDP 'non-los 14 bytes TDP 'non-los 14 bytes TDP 'non-los 14 bytes Mile TDP 'non-los 14 bytes TDP 'non-los 14 bytes TDP 'non-los 14 bytes TDP 'non-los 14 bytes Mile TDP 'non-los 14 bytes TDP 'non-los 14 bytes TDP 'non-los 14 bytes TDP 'non-los 14 bytes Mile TDP 'non-los 14 bytes TDP 'non-los 14 bytes TDP 'non-los 14 bytes TDP 'non-los 14 bytes TDP 'non-los 14 bytes TDP 'non-los 14 bytes TDP 'non-los 14 bytes TDP 'non-los 14 bytes TDP 'non-los 14 bytes TDP 'non-los 14 bytes TDP 'non-los 14 bytes TDP 'non-los 14 bytes TDP 'non-los 14 bytes TDP 'non-los 15 bytes </th <th>1 1 1 2 8 0 1 2 2 Q</th> <th></th> <th></th> <th></th> <th></th> <th></th>	1 1 1 2 8 0 1 2 2 Q					
TOP providence (48 bytes) Top (48.0)	A Nor-Arts				Dia - Egenne.	. 0 0
TDP invilence (43. bytes) TDP invilence (43. bytes) State frame: 4463) Sotap fram: 4463) Correct working directory: Correct working directory: Sotap fram: 4463 Sotap fram: 4463 Sotap fram: 4463 Sotap fram: 4463 Correct working directory: Correct working directory: Sotap fram: 4463 Sot for directory: Sotap fram: 4463 Sot for directory: Sotap fram: 4415 Sot for directory: Sotap fram: 4415 Sot for directory: Sotap fram: 4415 Sot for directory: Sotap fram: Sotap fram					COMMENSAL STREET	
PTW Backs (43 Myres Mats) PTW Backs (43 Myres Mats) Sortap sentual F0001 Sortap sentual F0001 Command F1mm Dering Sentual F0001 Dering F00000 Dering F100000 Dering F100000 Dering F100000 Dering F1000000 Dering F10000000 Dering F1000000000000000000000000000000000000	100 100 100 100 100 10 10	1 141 164 217 1	KTP-DA	Lite FTF Balai, 45 Bitter	(root)-perk proved	85
P Prime Handar (128 Aprimes Handa) [Settap transmit 4888] [Settap transmit 48888] [Settap transmit 4888] [Settap transmit 4888] [Settap transmi	1					
P Prime Handar (128 Aprimes Handa) [Settap transmit 4888] [Settap transmit 48888] [Settap transmit 4888] [Settap transmit 4888] [Settap transmi						
P Prime Handar (128 Aprimes Handa) [Settap transmit 4888] [Settap transmit 48888] [Settap transmit 4888] [Settap transmit 4888] [Settap transmi	•					
P Prime Handar (128 Aprimes Handa) [Settap transmit 4888] [Settap transmit 48888] [Settap transmit 4888] [Settap transmit 4888] [Settap transmi						
P Prime Handar (128 Aprimes Handa) [Settap transmit 4888] [Settap transmit 48888] [Settap transmit 4888] [Settap transmit 4888] [Settap transmi	1					
P Sottop Trane: 4805) [Command: StTR Privet001.5k] [Command: StTR Privet001.5k] [Sottop Trane: 4805] [Sottop Trane: 4805] [-6
Image: Second Process, Herric Second Process, Herric Second Process, Herric Image: Second Process, Herric Second Process, Herric Second Process, Herric Image: Second Process, Herric Second Process, Herric Second Process, Herric Image: Second Process, Herric Second Process, Herric Second Process, Herric Image: Second Process, Herric Second Process, Herric Second Process, Herric Image: Second Process, Herric Second Process, Herric Second Process, Herric Image: Second Process, Herric Second Process, Herric Second Process, Herric Image: Second Process, Herric Second Process, Herric Second Process, Herric Image: Second Process, Herric Second Process, Herric Second Process, Herric Image: Second Process, Herric Second Process, Herric Second Process, Herric Image: Second Process, Herric Second Process, Herric Second Process, Herric Image: Second Process, Herric Second Process, Herric Second Process, Herric Image: Second Process, Herric Second Process, Herric Second Process, Herric Second Process, Herric Image: Second Process, Herri Second Process, Herric <td< td=""><td>(Setup Frame: 4905)</td><td></td><td></td><td></td><td></td><td></td></td<>	(Setup Frame: 4905)					
Image: Contrent working directory: Image: Contrent working: Image: Contrent working: Image: Contrentworking: Image: Contrent workin: <td>[Command: #ETH jrivelo0.tat]</td> <td></td> <td></td> <td></td> <td></td> <td></td>	[Command: #ETH jrivelo0.tat]					
Imper tensed texts (string (fr. Lines)) Linese Rithers(M) Imper tensed texts (string (fr. Lines)) Linese Rithers(M) PP OB 5 Mol 48 57 12 823 \u03e9 \u03e9 09 56 cd 19 40 80 71 2823 \u03e9 \u03e9 09 56 cd 19 40 80 71 28 825 \u03e9 \u03e9 00 86 48 50 0 86 \u03e9 11 48 0 48 57 88 31 09 81 80 14 118 cd 11 16 77 28 86 114 80 44 57 89 31 09 81 80 14 118 cd 11 16 77 28 86 114 80 44 57 89 31 12 76 33 77 06 27 34 60 0 12 80 72 33 31 32 30 30 40 16 17 5 7 28 82 12 76 33 77 06 27 34 60 0 16 23 31 17 93 31 32 30 30 30 16 17 5 7 28 83 12 40 81 73 87 68 20 55 20 56 53 14 20 51 23 53 32 32 32 30 80 40 189 F5 7 2823 Jammer H1 sers Ser 76 4 45 10 31 16 7 28 82 40 189 F5 7 2823 Jammer H1 sers	Connatal Franci 4007.					
Product Product <t< td=""><td> Line based text data (2 lines) </td><td></td><td></td><td></td><td></td><td>- 1</td></t<>	 Line based text data (2 lines) 					- 1
00 15 50 45 57 50 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80 80<	Con Feb 58 15:45:00 PST 2023 Ve Zanas RiversVe					
00 57 cd 10 40 00 10 04 00 40 00 60 00 60 00 60 00 60 00 60 00 60 00 60 00 60 00 60 00 60 00 60 00 60 00 60 00 60 00 60 00 60 00 60 00 60 00 60 00 60 00 60 00 60 00 60 00 60 00 60 40 67 00 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60 60<	and the second s		100 100 1			
60 e5 02 60 e5 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02<	00 of cd 80 40 00 40 00 40 00 cd	9 10 85 00 56 05 88	10.0			
54 25 54 15 54 15 54 15 54 15 54 15 54 15 54 15 54 15 54 15 54 15 54 15 54 15 15 15 15 15 15 15 15 15 15 15 15 15	0 H0 211 23 H1 00 38 00 28 00 2111 0		and the second second second			
and the term of the 20 N2 00 10 42 72 73 Na Danset NL overs						100
	ta 41 73 87 64 28 52 00 76 4	0 72 72 84				
	44 41 73 87 54 29 38 53 54 2 44 41 73 87 64 29 52 00 76 0	0 52 36 32 38 29 8w	45:00 PS T 2023			

2. Follow the tcp steam of the **FTP-DATA** packet, and view the content of the file just transferred.



3. Export (Save) the transferred file as a text file in Internal Kali, and view the content. Below is the example.

plications - Place	s 👻 🗐 Text Editor 👻	Thu 23:14		1	1 1 0 .
	Open +	transferred_data.txt	Save	=	
File Edit Yie	hu Feb 10 20:09:10 PST 2022 eng Jiang	content of the fi	le transferre	d wi	th FTP



The right click would not go away, but I got the FTP file exported to the desktop properly.