# Assignment 2.1 Traffic Tracing and Sniffing

# 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.

Tip: Please power on the pfsense VM and DO NOT revert to a previous checkpoint.

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 Ubuntu VM for 5 - 10 seoends.

3. 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

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

## There are a total of 120 captures, and 120 are displayed.

- 2. Apply "ICMP" as a display filter in Wireshark. Then repeat the previous question. **There are 56 ICMP captures.**
- 3. 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?

Source ip: 192.168.10.10 Destination ip: 192.168.217.3 Sequence number: 8 Size: 48 Bytes Response time: 170.730 ms

- 4. Apply "DNS" as a display filter in Wireshark. How many packets are displayed? There are 52 DNS captures. The query selected is trying to resolve wpad.mshome.net.
- 5. 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?

## Source ip: 192.168.217.3:50426 Destination: 192.168.217.2:53

6. 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?

Source ip: 192.168.217.2:53 Destination: 192.168.217.3:50426. The message from the server says refused.

## Assignment 2.2

## 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. IMPORTANT NOTES!

\* Because the current Hyper-V setting does not "broadcast" the communication between hosts in the same network, we need to enable port mirroring to allow Internal Kali to "see" other's communication. To be specific, you need to put the sniffer (Internal Kali) as the mirroring Destination, and the target VMs are mirroring Source (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 Mirroring mode to "Destination" in the "Port Mirroring"
- Ubuntu Kali: Set Mirroring mode to "Source" in the "Port Mirroring"
- External Kali: Set Mirroring mode to "Source" in the "Port Mirroring"

\*\* 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. Figure 1 Required VMs for this assignment Figure 2 How to configure port mirroring in Hyper-V Select the first Network Adaptor, then click "Advanced Features"

### 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.

R.								*eth0								•	•	8
<u>F</u> ile	<u>E</u> dit <u>V</u> iew	<u>G</u> o <u>C</u> a	pture <u>A</u> r	nalyze g	<u>S</u> tatistics	Telep	ohon <u>y</u>	<u>W</u> ireless	<u>T</u> ools	<u>H</u> elp								
		0	) 🖹 🕻	<u>ି</u>   ୧	+ +	<b>ن</b>	<b>H</b>		۹	Q	Q	3 8						
📕 ic	Expression +																	
No.	Time		Source			De	stinati	on		Proto	col	Length	Info					-
7*	10.000	000000	192.1	.68.217	.3	19	2.168	10.10		ICMP		98	Echo	(ping)	request	id		
+	2 0.000	010900	192.1	.68.10.	10	19	2.168	1.217.3		ICMP		98	Echo	(ping)	reply	10	3	
	11 0.420	226900	192.1	68 10	.3	19	2.100	217 2		TCMP		98	Echo	(ping)	request	10	1	
	29 1.014	828700	192.1	68.217	-3	19	2.168	10.10		TCMP		90	Echo	(ping)	request	id	]	
	30 1.017	958200	192.1	.68.10.	10	19	2.168	.217.3		ICMP		98	Echo	(ping)	reply	id	-	
	39 1.426	240100	192.1	.68.217	.3	19	2.168	10.13		ICMP		98	Echo	(ping)	request	id	-	
	40 1.426	276900	192.1	68.10.	13	19	2.168	.217.3		ICMP		98	Echo	(ping)	reply	id	=	
	50 2.038	318000	192.1	.68.217	.3	19	2.168	10.10		ICMP		98	Echo	(ping)	request	id	=	
	51 2.040	486000	192.1	.68.10.	10	19	2.168	3.217.3		ICMP		98	Echo	(ping)	reply	id	=	-
> Et	hernet II, hternet Pro hternet Com	Src: M otocol V otrol Me	licrosof Version Ssage F	40:57 4, Src Protoco	(0) 192.1	10:15:5	00 4	5.00	Dst: M 2.168.2	4icro 10.10	sof.	_40:57	:0c (	00:15:5	5d:40:57:	0c)		
000 001 002 003 004 005 006	0 00 15 5 0 00 54 32 0 00 00 34 0 00 00 34 0 16 17 14 0 26 27 28 0 36 37	1 40 57 2 46 40 8 00 4c 1 26 07 8 19 1a 8 29 2a	0C 00 3 00 3 e7 07 00 00 1b 1c 2b 2c	15 50 01 a5 09 00 00 00 1d 1e 2d 2e	40 57 04 c0 69 db 00 10 1f 20 2f 30	1e 08 a8 d9 47 c5 11 12 21 22 31 32	00 4 03 c 65 0 13 1 23 2 33 3	5 00 - 0 08 - 0 00 - 4 15 - 4 25 - 4 35 & 6	- ]@W T2F@ - ? - L    	- j@w i /0	G e	E ·  \$%% 445						
0	/ Internet C	ontrol Me	essage Pro	otocol: P	rotocol		Pac	kets: 1290	· Displa	yed: 14	14 (1	1.2%) · I	Droppe	d: 0 (0.0	%) Profil	e: De	fault	

B. Apply proper display or capture filter on Internal Kali VM that ONLY displays ICMP request originated from External Kali VM and goes to Ubuntu 64-bit VM

		0																						_
ſ											*(	eth0										•	•	8
<u>F</u> ile	<u>E</u> dit <u>V</u> iew	Go	<u>C</u> aptur	е <u>А</u>	nalyze	<u>S</u> ta	tistic	s T	elepł	hon <u>y</u>	w	/irele	ss <u>T</u> o	ols	<u>H</u> elp									
		Ō	01010 01010	X	6	۹ ۹		▶ .	ı ډ	+	<b>*</b>			€	Q	Q								
(ip.src == 192.168.217.3) && (ip.dst == 192.168.10.10)										+														
No.	▼ Time		S	ource	9				Des	tinat	tion				Proto	col	Lenath	Info					_	-
_+	10.000	00000	0 1	92.1	168.2	17.3			192	2.16	8.1	0.10			ICMP		98	B Echo	(ping)	req	uest	id		
	29 1.014	82870	00 1	92.1	168.2	17.3			192	2.16	8.1	0.10			ICMP		98	B Echo	(ping)	req	uest	id	-	
	50 2.038	31800	00 1	92.1	168.2	17.3			192	2.16	8.1	0.10			ICMP		98	B Echo	(ping)	req	uest	id	1	
	78 3.019	80880	00 1	92.1	168.2	17.3			192	2.16	8.1	0.10			ICMP		98	B Echo	(ping)	req	uest	id	1	
	106 4.016	81350	00 1	92.1	168.2	17.3			192	2.16	8.1	0.10			ICMP		98	B Echo	(ping)	req	uest	id	1	
	136 5.034	31060	00 1	92.1	168.2	17.3			192	2.16	8.1	0.10			ICMP		98	B Echo	(ping)	req	uest	id	1	
	164 6.028	47280	00 1	92.1	168.2	17.3			192	2.16	8.1	0.10			ICMP		98	Echo	(ping)	req	uest	10:	1	
	192 7.032	40080	1001	92.1	168.2	17.3			192	2.16	8.1	0.10			1CMP		98	Echo	(ping)	req	uest	10:	1	
	220 8.063	48000	10 1	92.1	168.2	17.3			192	1.10	8.1	0.10			TCMP		98	ECNO	(ping)	req	uest	10:	1	
	249 9.049	19320	10 1	92.1	108.2	17.3			192	2.10	8.1	0.10			ICMP		98	ECHO	(ping)	req	uest	10	-	
				.90																				
0000 0010 0020 0030 0040 0050 0060	00 15 5   00 54 3   0a 0a 0 0   00 00 3 16 17 1   26 27 2 36 37	40 2 46 8 00 d 26 8 19 8 29	57 0c 40 00 4c e7 07 00 1a 1b 2a 2b	00 3f 07 00 1c 2c	15 5 01 a 09 ( 00 ( 1d 2 2d 2	5d 40 a5 04 90 69 90 00 1e 1f 2e 2f	57 c0 db 10 20 30	1e a8 47 11 21 31	08 d9 c5 12 22 32	00 4 03 0 13 1 23 2 33 1	45 ( c0 a 00 ( 14 2 34 3	90 a8 90 15 25 35	••]@ •T2F ••=& &'() 67	W @ - ? L * +,	- ]@\ /(	√ G e !"# 9123	E -     - - - - - - - - -							
0 2	wireshark	_eth0	_20240	208	16300	3_TcF	ZDM	1.pca	png		Pack	ets: 1	l290 · I	Disp	layed:	37 (	2.9%)·	Droppe	ed: 0 (0.0	%)	Profile	e: Def	ault	

### 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.A.



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 used wireshark on the internal kali which recorded the ftp connection from the exteranl kali workstation to capture the tcp connection that took place. I used the filter ip.src==192.168.217.3 in order to show traffic from that source ip and then selected the tcp that went to the 192.168.10.10 and selected follow tcp stream in order to show usernam and password that was used for connection.



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.



## Extra Credit: Steal files with Wireshark (15 points)

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

駻 Kali	Internal Workstation on CS301-BCOWD001 - Virtual Machine Connecti	- 🗆 X	
File	Action Media Clipboard View Help		
<b>B</b>   <b>C</b>	🖲 🞯 💴 🕩 🔂 1 🔡 🎆		
Appli	ations 🔻 🛛 Places 👻 🇖 Wireshark 👻	Thu 18:08	1 🗯 💉 🕪 🖯 🔫
		*eth0	000
	<u>File Edit View Go</u> Capture <u>Analyze Statistics</u>	Telephon <u>y W</u> ireless <u>T</u> ools <u>H</u> elp	
		🖛 🕈 🧮 🔳 🔍 Q 🛇	۹ 🏦
	📕 ftp-data		Expression +
	No. Time Source	Destination Protoco	l Length Info
9	80 26.542164700 192.168.217.3	192.168.10.10 FTP	80 Request: USER cyse301
	83 26.543262300 192.168.10.10	192.168.217.3 FTP	100 Response: 331 Please specify the passwo…
\$_	88 28.985465800 192.168.217.3	192.168.10.10 FTP	81 Request: PASS password
	90 29.037877000 192.168.10.10	192.168.217.3 FTP	89 Response: 230 Login successful.
	92 29.182266700 192.168.217.3	192.168.10.10 FIP	72 Request: SYST
~	94 29.180197300 192.108.10.10	192.108.217.3 FIP	74 Dequest: TYPE T
		192.100.10.10 FTF 192.168.217.3 ETP	97 Response: 200 Switching to Binary mode
		192.168.10.10 FTP	94 Request' PORT 192 168 217 3 223 123
_	109 33.469184200 192.168.10.10	192.168.217.3 FTP	117 Response: 200 PORT command successful
M	110 33.478977600 192.168.217.3	192.168.10.10 FTP	85 Request: RETR bcowd001.txt
- V	Frame 110: 85 bytes on wire (680 bits).	85 bytes captured (680 bits)	on interface 0
	Ethernet II, Src: Microsof 40:57:1e (00)	:15:5d:40:57:1e), Dst: Micros	of_40:57:0c (00:15:5d:40:57:0c)
	▹ Internet Protocol Version 4, Src: 192.1	68.217.3, Dst: 192.168.10.10	
	Transmission Control Protocol, Src Port	: 48770, Dst Port: 21, Seq: 72	2, Ack: 179, Len: 19
- X	File Transfer Protocol (FTP)		
_	[Current working directory: ]		
	[Command response frames: 1]		
•	[Command response bytes: 4/]		
_	[Command response last frame: 114]		
<b>7</b>	[Setup frame: 108]		
	0000 00 15 5d 40 57 0c 00 15 5d 40 57 1	A AR AA 45 10	
	0010 00 47 b7 36 40 00 3f 06 20 0c c0 a	8 d9 03 c0 a8 G 60 2	· · · ·
	0020 0a 0a be 82 00 15 a7 d0 50 b5 e8 1	b ed aa 80 18 · · · · · · P · · ·	
	0030 00 e5 b2 ff 00 00 01 01 08 0a e2 2	a 70 08 9b e3 💀	p · · ·
<u> </u>	0040 ed b1 52 45 54 52 20 62 63 6f 77 6	4 30 30 31 2e 🛛 RETR b cowd	1001.
l.≽	Show Applications od Oa	txt··	
			Activate Windows
			Go to Settings to activate Wind
			Go to settings to activate will

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.