OLD DOMINION UNIVERSITY

CYSE 301 Cybersecurity Techniques and Operations

Assignment #2: Lab 2-Traffic Tracing and Sniffing

Antonio Shields

TASK A: GET STARTED WITH WIRESHARK (5 POINT EACH X 6 QUESTIONS = 30 POINTS)

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



Figure 1 Screenshot of Wireshark in Attacker Linux for Task A.1

The above screenshot is the Wireshark results from pinging Ubuntu VM for 5-10 seconds. In the screenshot, it shows at the bottom that 113 packets were captured during listening on eth0 and also 113 packets are currently being displayed (highlighted in yellow at bottom).

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



Figure 2 Screenshot of Wireshark with "ICMP" filter in Attacker Linux for Task A.2

The above screenshot is the Wireshark results after applying the "ICMP" filter from the previously captured information. In the screenshot, it shows at the bottom that 113 packets were captured during listening on eth0 and only 80 packets are currently being displayed that have "ICMP" protocol (highlighted in yellow at bottom).

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?



Figure 3 Screenshot of Echo reply message from Packet 30 in Wireshark on Attacker Linux for Task A.3

The above screenshot is from Echo reply Packet 30. The source IP is 192.168.10.10 and the destination IP is 192.168.217.3. The sequence numbers are 1 for BE and 256 for LE. The data size is 48 bytes and the response time is 4.027 ms. (Information highlighted in yellow to bring attention to it).

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



Figure 4 Screenshot of Wireshark with "DNS" filter in Attacker Linux for Task A.4

The above screenshot shows the "DNS" filter being applied. Out of the 113 packets available, only 14 packets are being displayed under the "DNS" filter (highlighted in yellow).

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? Please express in the format: **IP:port**.



Figure 5 Screenshot of DNS query packet from Packet 3 in Wireshark on Attacker Linux for Task A.5

The above screenshot is from the DNS query Packet 3. The domain name that the host is trying to resolve is 3.debian.pool.ntp.org. The source IP and port number are 192.168.217.3:47434 and the destination IP and port number are 192.168.217.2:53 (Information highlighted in yellow to bring attention to it).

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?



Figure 6 Screenshot of corresponding DNS response from Packet 5 in Wireshark on Attacker Linux for Task A.6

The above screenshot is from the corresponding DNS response from Question 5 as Packet 5. The source IP and port number are 192.168.217.2:53 and the destination IP and port number are 192.168.217.3:47434. The standard query response was Refused and the response says "Message is a response". (Information highlighted in yellow to bring attention to it).

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.



Figure 7 Screenshot of Wireshark on Internal Kali sniffing traffic between External Kali and Ubuntu VM. This show the "ICMP" filter being used for Task B.1a

The above screenshot shows the "ICMP" filter being applied and showing the active ICMP traffic.

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.Display your current directory in a terminal.

	Edit Yorw Edit Yorw M d. € CompE£ip.dst= Time 5792 256 6598 259.4 6698 261.4 6698 201.4	<u>So</u> Captur D 1 192,168,10,1 So 1000559900 1	• Analyze 8 C Q 10 ource	Statistics	Telephony	*eth0 Wireless	Tools Help	a, II			0	0 0		
	Edit View Edit View Edit CompESip.dst= Time System S	Go Captur D 110 =192,168,101 50 116659980 1	e Analyze C C Q 10 ource	Statistics	Telephony	Weeless	Icols Help	a, <u>II</u>						
	III 2 C	0 11 50 192,168,101 50	aurce	(+ +				9、旺						
VMs	CompESip.dst= Time 6598-259.4 6624-260.4 66562-261.4	=192.168.10.1 Se 167.2.100.51 16659990 1	10 ource											
VMs	Time 6598 259.4 6624 200.4 6626 261.4	Se 116659980 1	ource 92 168,21	1. Contraction (1. Contraction	dia anti-					0.03	Express	ion		
VM-	6598 259.4 6624 260.4 6658 201.4	16659988 1	92,168.21		Destinate	n	Proto	tol Lengt	th Info	12.11		_		
- ¥M6	0624 200.4 0650 201.4	100599900 1	00 000 04	7.1	192,168	10.10	1040	and the second se	BB Eche	(0109)	request	10701	<u> </u>	
	0650 261.4	the second se	92.199.21	7.8	192,198	10.10	1000		an Febr	(ping)	request	10-000		
	4000 367	18682468 1	92.168 21	7.9	192.168	10.10	TOMP		88 Echo	Ininal	request	id=Rv	а-	
		26692280 1	02.168.21	7.9	102.168	10.10	TCMP		HE Echo	(otno)	request	10=0x		
	6786 263.4	23320000 1	92.168.21	7.3	192.168	.10.10	ICMP		98 Echo	(pino)	request	id=0x	a l	
	6732 264.4	36877888 1	92.168.21	7.3	192.168	.18.18	TOMP		98 Echo	(ping)	request	id=800	e	
	6758 265.4	27067000 1	92.168.21	7.0	192.168	.10.10	ICMP		00 Echo	(ping)	request	1.0=000	0	
	6784 266 4	29447388 1	92.168.21	7.3	192.168	.18.19	LCMP		98 Eche	(ping)	request	1d=6x	e	
	6812 267.4	131758380 1	92.168.21	7.3	192.168	.18.10	ICMP		BB Echo	(ping)	request	1d=8x	0	
	6838.268.4	139386860 1	92.168.21	7.3	192.168	.10.10	ICMP		s8 Echo	(brud)	request	.id=8x	0.	
: :	Frame 6572: Ethernet II,	98 bytes o Src: Micr	on wire (7 rosof_40:5	84 bits) 7:1# (00	98 bytes 15:5d:46:	captur 57:1e),	ed (784 bit Dat: Micro	s) on in sof_40:5	sterface 57:00 (0	0 0:15:5	1:46:57:1	ec)		
1 1	Internet Pro Internet Co	otocol Vers otrol Messa	sion 4, 5r age Protoc	c: 192.1 ol	58.217.3,	Dst: 19	2.168.18.18							
2														
346	00 15 5	d 48 57 8c	00 15 50	0 40 57 1	e 00 00 4	5 00	30M 30	E					-	
101	10 00 54 0	a 4b 40 80	37 01 04	c ff c0 a	8 d9 03 c	0 80	T KB-7							
.402	04 89 0	8 88 c3 35	07 7a 00	0 01 20 7	9 85 65 6	0 00	-5-2	b-e						
10	16 17 1	3 a7 01 86 8 19 1a 1b	10 10 10	e 1f 28 2	1 12 13 1 1 22 23 2	4 15		1"#\$%						
0	₹ wireshari	_eth0_20230	0920181611	2Fkifii.pcap	ng Pad	kets: 9275	- Displayed: 11	(0.1%) D	ropped: 0	(0.0%)	Profile: 0	efault		
		1.1		111	110	1					U.S. HI			
	AND POST OFFICE ADDRESS OF	-		-	- 0	-		1000	-	1	and or	0		3-10.0

Figure 8 Screenshot of Wireshark on Internal Kali sniffing traffic between External Kali and Ubuntu VM. This show the "ICMP" and "ip destination of ubuntu" filter being used for Task B.1b

The above screenshot shows the filter being used to show only ICMP request that originated from External Kali (192.168.217.3) to Ubuntu VM (192.168.10.10). This was achieved by using the filter icmp&&ip.dst = = 192.168.10.10.

- 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.



Figure 9 Screenshot of accessing the Ubuntu FTP Server using External Kali. This shows the ftp command in the External Kali terminal to access the FTP server in Ubuntu for Task B.2a

The above screenshot shows External Kali accessing the FTP server on Ubuntu VM using the command: "ftp 192.168.10.10" (ip address of Ubuntu VM). After entering the proper username (cyse301) and password (password) the login will display as successful and file transfer can commence. Exit command was given because no file transfer at this time.

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.



Figure 10 Screenshot of Wireshark from Internal Kali showing the "FTP" traffic by using the "FTP" filter for Task B.2b

The above screenshot shows that when you filter just the FTP traffic in Wireshark on the Internal Kali, you are able to see the entire FTP interaction between External Kali and Ubuntu. This screenshot shows that the username used was "cyse301" and the password that was used was "password" followed by the response of login successful, so that you know it works.

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.



Figure 11 Screenshot of accessing the Ubuntu FTP Server again using External Kali. This shows the ftp command in the External Kali terminal to access the FTP server in Ubuntu for Task B.2c

The above screenshot shows the FTP Server on Ubuntu being access via External Kali this time using my MIDAS ID as the username and my UIN as the password. This time the login was incorrect and failed, but the traffic was captured and the "exit" command was entered.

plications +	Paces * 👩 W	ireshe.	H 18	to:	Preside With	de com Aprileo	6	- 7	-	1	E 4	1	e 0 -	
						*eth0						0	00	
Ele Edt	View Go Capt	ire Alaty	te Statistics	Telephon	<u>w</u> ireles	s Tools Het	6							
4	10 m	5 2	0 + +	7.14	-			E.						
A	85. 9 0. U	(C) (M)	nessoan e	0.000	0.000	= ~ ~	- m - II	4.11						
II ftp://											13 CD -	Express	sion +	
No.	Time	Source		Destin	ition:	Prot	ocol Les	ngth Info						-
2228	88.431421209	192.168	10.10	192.1	88.217.3	FTP	1.10.001+12.2	BB Respon	nse: 22	1 Goodbye	2.V			
14752	588,582158598	192.168	.18.10	192.1	68.217.3	FTP		86 Respo	nse: 221	8 (vsFTPd	3.8.3)			
14886	586,819289708	192,168	217.3	192.1	68.10.10	FTP		81 Reque	st: USE	R ashie00	5			
14888	585.821436998	192.168	.18.10	192.1	68.217.3	FTP		188 Respo	nse: 33	t Please	specify	the p	issword	
100133-142	590.20000408	102,100	217.3	102.1	60.10.10			B1 Reque	HEL PASS	5 01240g0			1	
15217	599.162812108	192.168	.10.10	192.1	68.217.3	FTP		88 Respo	nset 53	B Login 1	ncorrec	C		
15219	599.164180108	192.168	.217.3	192.1	68.10.10	FTP		72 Reque	st: SYS	T.				
15221	599.165226998	192.166	.10,10	192.1	68.217.3	FTP		184 Respo	nse: 53	6 Please	login w	ith USE	ER and I	
15703	618.706669708	192.168	.217.3	192.1	68.10.10	FTP		72 Reque	st: QUI	r	20210-01			
15784	618.767972998	192.168	.10.10	192.1	68.217.3	FTP		88 Respo	nse: 22	1 Goodbye				2
· · · · · · · · · · · · · · · · · · ·											-			
 Etherns Interns Transm File T PASS Re Re [Curre] 	Net 11, SrC: Mil Wet Protocol Ver Hission Control Transfer Protoco 5 822484955/riu equest command: equest arg: 812 mt working dire	Protoco Protoco ol (FTP) PASS 40495 sctory:	8:57:10 (00 Src: 192.: 1, Src Port	9:15:50:4 160:217:3 1: 42378,	8:57:10) , Dst: 11 Dst Port	, Det: Mick 92.160.19.1 1: 21, Seq:	0507_40 0 16, Ac	157186 (8	e:15:54	140:57:80	,		ate Wir	
8006 00 0010 00 0520 0e 0530 0e	0 15 5d 40 57 0 0 43 db 35 40 0 a 0a a5 8a 60 1 0 45 12 85 80 0	c 00 15 0 3f 06 5 5f 06 0 01 01	5d 40 57 fc 10 c0 d0 88 9d 85 8a 45	1e 88 88 a8 d9 83 f3 b6 2f e8 bd 58	10 c6 a5 50 18 36 a0	16M 10 C 58 7	N 3 / P6				1			
	Q Search				<u>a</u> 0			9 🔤 י	·	67 6	· ·	-		P 41 10 1/20

Figure 12 Screenshot of Wireshark from Internal Kali showing the "FTP" traffic by using the "FTP" filter for Task B.2c

The above screenshot shows the Wireshark information from Internal Kali using the "FTP" filter again. This time it shows the username as my MIDAS ID and my UIN as my username. It also shows that the login was incorrect as well.

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.



Figure 13 Screenshot of the terminal in Ubuntu VM and creating a file and inputting the required information for Task EC

The above screenshot shows creating a file using the touch command using my MIDAS ID as the title and also entering the current timestamp and name in the file. The ls command was used to ensure the file existed in the directory and the cat command was used to verify the information in the .txt file.

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



Figure 14 Screenshot of the "FTP" command being used in External Kali to access the FTP server in Ubuntu VM and the created file being transferred to Ubuntu for Task EC.

The above screenshot shows the "FTP" command being used in the External Kali terminal to connect to the FTP server in Ubuntu using the correct credentials. Once successfully logged in, the created file that made in the previous step was transferred and shows that the transfer was completed.

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.



Figure 15 Screenshot of Wireshark from Internal Kali showing the "FTP-data" traffic by using the "FTP-data" filter for Task EC-1

The above screenshot shows the "FTP-DATA" filter being applied to retrieve the packets between External Kali and Ubuntu VM.

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



Figure 16 Screenshot of Wireshark from Internal Kali showing the TCP stream of the FTP-data packet and the contents of the file Task EC-2

The above screenshot shows that by going to "Analyze" on the menu bar, then go to "Follow" and then select "TCP Stream" the contents of the file selected will appear as shown. Using the "Save As" button at the bottom will allow you to save the contents as a .txt file in the place of your choice.



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

Figure 17 Screenshot of the .txt file opened in text editor to view the content for Task EC-3

The above screenshot shows the results of saving the tcp stream content as a .txt file and opening it up using text editor to verify successful saving and execution.