Task A: 40 points

Follow the steps in the lab manual, and decrypt WEP and WPA/WPA2 protected traffic. Requirements:

• Decrypt the lab4wep.cap file (10 points) and perform a detailed traffic analysis (10 points)

• Decrypt the lab4wpa2.cap file (10 points) and perform a detailed traffic analysis (10 points)



root@CS2APenTest: ~/CYS	E301/Module V-Wireless Security 🕒 回
File Edit View Search Terminal Help	
1 9/10 C7(24064) 71(23808) 5C(23552) 20(232 2 0/ 1 BB(30208) AB(25344) BE(25344) D0(248	296) 2A(23296) 52(23296) 84(23296) 99(23040)
3 = 8/ 12 FC(24064) 25(23808) 2A(23808) A9(238	308) BD(23808) 00(23552) 42(23552) 3F(23296)
941.02.0/88 1 B9(30720) 33(26624) 2E(25344) C4(253 8 0.017930 Apple_28:d8:50 Cisco-Li_7cid	844) 64(25088) ED(25088) 55(24832) 77(24832) FN=0, Fl 0:c5
7 0.014858 Apple_KEYdFOUND! [ F2:C7:BB:35:B9	]c5 802.11 146 QoS Data, SN=2831, FN=0, Flags=
6 0.0 Decrypted correctly: 100% Apple_28:d8:5	
50.002571 Apple_28:d8:50 Cisco-Li_7c:d	
4 0.000522 Cisco-Li_7c:d	
<pre>root@CS2APenTest:~/CYSE301/Module V-Wireless Security</pre>	<b># airdecap-ng -h</b> 150 QoS Data, SN=2829, FN=0, Flags=
airdecap-ng:Linvalid option_H-chh'c9 ( Cisco_fa:3b:a	
"airdecaping)help" for help. cl Broadcast	
<pre>root@CS2APenTest:~/CYSE301/Module V-Wireless Security</pre>	/# airdecap-ng -w F2:C7:BB:35:B9 lab4wep.cap
Total number of stations seen 37	
Total nümber/of packets read 4 bits)404693bytes captu	
Total number of WEP data packets 142415	
Total number of WPA data packets 27852	
Number of plaintext data packets 170	
Number of decrypted WEP packets 142415	
Number of corrupted WEP packets 0	
Number of decrypted WPA packets 0	
Number of bad TKIP (WPA) packets 0	
Number of bad CCMP (WPA) packets 0	
<pre>root@CS2APenTest:~/CYSE301/Module V-Wireless Security</pre>	#

	lab4v	vep-dec.cap					
<u>F</u> ile <u>E</u> dit <u>V</u>	iew <u>G</u> o <u>C</u> apture <u>A</u> nalyze <u>S</u> tatistics Telephon <u>y W</u> ireless	<u>T</u> ools <u>H</u> elp					
	Wireshark · Protocol Hierard	chy Statistics · lab4v	vep-dec.cap		•	• •	
Apply a dis	Protocol -	Percent Packets	Packets	Percent Bytes		Bytes ^	Ex
No Tir	<ul> <li>User Datagram Protocol</li> </ul>	0.1	198	0.0	1	1584	1
1220 20	NetBIOS Name Service	0.0	20	0.0	1	1102	÷
1400 30	<ul> <li>NetBIOS Datagram Service</li> </ul>	0.0	3	0.0	!	549	
1400 30	<ul> <li>SMB (Server Message Block Protocol)</li> </ul>	0.0	3	0.0	:	303	
1409 30	<ul> <li>SMB MailSlot Protocol</li> </ul>	0.0	3	0.0		75	
1412	Microsoft Windows Browser Protocol	0.0	3	0.0		45	
31.	Multicast Domain Name System	0.0	30	0.0		4542	1:
105 7.	Dropbox LAN sync Discovery Protocol	0.0	20	0.0		2300	
197 37	Domain Name System	0.1	80	0.0		6069	1.
198 37	Bootstrap Protocol	0.0	2	0.0	1	1500	
199 38	<ul> <li>Transmission Control Protocol</li> </ul>	13.6	19342	73.4	:	16399	1.
4	Secure Sockets Layer	0.6	788	2.7		5930	
▶ Frame 198	Malformed Packet	0.0	12	0.0		0	
- Ethernet	<ul> <li>Hypertext Transfer Protocol</li> </ul>	0.9	1296	7.7	1	17153	
👻 Destina	MIME Multipart Media Encapsulation	0.0	2	0.0	1	1767	
Addr	Media Type	0.0	18	0.0		4538	
	Line-based text data	0.0	11	0.0		7573	
	JPEG File Interchange Format	0.0	3	0.1	1	12178	
- Source	JavaScript Object Notation	0.0	1	0.0	1	12	
Addr	HTML Form URL Encoded	0.0	14	0.1	:	17314	
	Compuserve GIF	0.0	9	0.0		2734	
 Typo:	FTP Data	0.0	7	0.0		9464	
Addross	File Transfer Protocol (FTP)	0.0	22	0.0		656	
F Auuress r	Internet Group Management Protocol	0.0	7	0.0	!	56	
0000 ff f	Internet Control Message Protocol	0.0	3	0.0	1	120	
0010 08 0	Data	1.2	1730	9.7	:	21753	
0020 00 0	Address Resolution Protocol	86.2	122691	15.4	:	3435	
	4					• •	
	No display filter.						
				Conv		Close	
	e neth			Сору		close	

root@CS2APenTest:~/CYSE301/Module V-Wireless Security# cp /usr/share/wordlists/rockyou.txt.gz /Cyse301, e V-Wireless Security . cp: cannot stat '/Cyse301/Module': No such file or directory cp: cannot stat 'V-Wireless': No such file or directory cp: cannot stat 'Security': No such file or directory root@CS2APenTest:~/CYSE301/Module V-Wireless Security# ls lab4wep.cap lab4wep-dec.cap lab4wpa2.cap rockyou.txt.gz root@CS2APenTest:~/CYSE301/Module V-Wireless Security# gunzip rockyou.txt.gz root@CS2APenTest:~/CYSE301/Module V-Wireless Security# ls lab4wep.cap lab4wep-dec.cap lab4wpa2.cap rockyou.txt root@CS2APenTest:~/CYSE301/Module V-Wireless Security# ls lab4wep.cap lab4wep-dec.cap lab4wpa2.cap rockyou.txt

🖳 Kali - Internal Workstation on BPEAR003 - Virtual Machine Connection	n	- 🗆 ×
File Action Media Clipboard View Help		
Applications - Places - E Terminal -	Thu 09:43	1 🗯 💉 🕬 🛈 🔻
r	oot@CS2APenTest: ~/CYSE301/Module V-Wireless Security	000
utils_ File Edit View Search Terminal He	lp	
Air	crack-ng 1.5.2	
[00:00:00] 720/9822768 keys	tested (1391.75 k/s)	
Time left: 1 hour, 57 minut	es, 41 seconds 0.01%	
KEY FO	UND! [ password ]	
Master Key : D9 61 39 7 AD 79 07 0	C CF 7F 65 50 70 B0 84 49 5C 80 F4 14 5 27 AF 6B A4 6B 53 E5 E3 90 B7 D7 A3	
Transient Key         : BD A0 CD 9           5C 5A 30 C         2F E3 52 2           CE E4 E3 7         CE E4 E3 7	4 EE 75 BA E7 2C 12 E3 39 C2 D3 68 21 9 FF 98 1F 73 56 31 41 FF F5 CD 0F 80 F 4A C5 ED 84 B5 A8 2D 48 34 3C 42 B6 6 EE 53 5C 90 F6 16 82 28 5C AB FA F8	
EAPOL HMAC : 33 04 CE 5 root@CS2APenTest:~/CYSE301/Module	2 33 89 5E A2 5B CE 3F DF C0 4B CE E0 V-Wireless Security#	
•		
<b>F</b> 些		
Q		KALI
		IFFENSIVE SECURITY

	1		lab4wp	a2-dec.cap				- • ×	
	<u>F</u> ile	Edit V	Wireshark · Protocol Hierarch	/ Statistics · lab4wpa	2-dec.cap		•••		
		ß	Protocol	Percent Packets	Packets	Percent Bytes	Bytes		
		1	▼ Frame	100.0	2228	100.0	4602		1.37
		oty a dis	<ul> <li>Ethernet</li> </ul>	100.0	2228	6.8	3119:	:xpression +	
	No.	Tir	<ul> <li>Internet Protocol Version 6</li> </ul>	0.1	3	0.0	120		<b>^</b>
9		10.	<ul> <li>User Datagram Protocol</li> </ul>	0.0	1	0.0	8	192.168	
		20.	Multicast Domain Name System	0.0	1	0.1	278	ple.com	
\$_		30.	Internet Control Message Protocol v6	0.1	2	0.0	40	deMacBo	
<u> </u>		40.	<ul> <li>Internet Protocol Version 4</li> </ul>	99.7	2221	9.7	4442		
_		50.	<ul> <li>User Datagram Protocol</li> </ul>	1.5	33	0.1	264	)::a65e:	
		60.	Network Time Protocol	0.0	1	0.0	48	portt	
		70.	Multicast Domain Name System	0.0	1	0.0	114	192.168	<b>1</b>
		80.	GQUIC (Google Quick UDP Internet Connections	) 0.1	2	0.3	1387	Win=409	
		91.	Domain Name System	1.0	22	0.2	939	192.168	Let - The
	4	10 1.	Data	0.3	7	0.3	1374	uredj 5	*
1	- Ere	mo 1.	<ul> <li>Transmission Control Protocol</li> </ul>	98.2	2188	82.6	3799		
	Fra	ernet	Secure Sockets Layer	5.7	127	8.5	3928		
1	Add	roce E	<ul> <li>Hypertext Transfer Protocol</li> </ul>	2.8	63	14.5	6680		
	, Aug	1035 1	Portable Network Graphics	0.0	1	0.2	1060	-	
<b>~</b>			Data	0.0	1	0.1	343		
			Address Resolution Protocol	0.2	4	0.0	112		
									1
•									
_									10 - APA
<b>7</b>									
		_						L	a beat h
	0000	ff f							
	0010	08 0							
	0020	00 0	4				Þ		
			No dienlaw filter						
-			No display meet.						
			Help			Сору	× <u>C</u> lose		
								1	

Task B: 60 points

Each student will be assigned a new WPA2 traffic file for analysis. You need to refer to the table below

and find the file assigned to you based on the LAST digit of the MD5 of your MIDAS ID. For example, the

last digit of the hash for pjiang is e. Thus, I should pick up file "WPA2-P5-01.cap."

MD5 of pjiang is 5a618cdc3edffd8b4c661e7e9b70ce1e

You can find an online MD5 hash generator or the following command to get the hash of a text string

root@CS2APenTest:~/CYSE301/Module V-Wireless Security# echo -n bpear003 | md5sum b8d1c2eb538b0cb05cf8ad4229250380 -

Last digit of your MD5 Filename

## 0~3 WPA2-P1-01.cap

4~5 WPA2-P2-01.cap

6~8 WPA2-P3-01.cap

9~B WPA2-P4-01.cap

C~F WPA2-P5-01.cap

The above files are zipped in a folder named "Lab Resources." You can locate the zipped folder in the Windows 10 Host Machine under C:/VMShare. Then, unzip the following zipped file in the Kali Linux VM,find the assigned WPA file under sub-folder "Module 5".

Then complete the following steps:

## 1. Implement a dictionary attack and find the password. - 30 points

## 2. Decrypt the encrypted traffic and write a detailed summary to describe what you have explored from this encrypted traffic file. -30 points

In order to ge the password/ key for the 0~3 WPA2-P1-01.cap document. I came across many confusing parts so I am not sure if I did it the way that was entended. I had to make sure that a rockyou.txt was inside the lab resource folder and that I was in the correct directory before doing any commands.

## The first command I did was aircrack-ng WPA2-P1-01.cap



I got this screen above. Usually, you would type 1 or the number that went with the encryption you wanted but it didn't let me. My solution was to use the command aircrack-ng -w rockyou.txt WPA2-P!-01.cap

This worked and gave me key found screen PASSWORD

20 0.087043	ADDIE D9:94:TA (/0:	802.11 10 Clear-to-send. Flads=	
	root@CS2APenTest: ~/Desktop/Lab Resourc	es (2023 Spring)/Lab Resources/Module 5	
File Edit View Search	Terminal Help		
24 0.108547	Apple b9:94:fa (70:		A
25 0.116219 Cisco	-Li_da:cfAircrack-ng 1.5.2		=0, Flags=
26 0.116739 Xiaom	iCo_72:56:1e (. Apple_b9:94:fa (70:. 1/7120712 kovs tostod (2141 62 k/s)		
	1//120/12 Reys tested (2141.62 K/s)		
Time left: 55 m	inutes, 15 seconds	0.32%	
Frame 1: 130 bytes on wire			
<ul> <li>IEEE 802.11 Probe Response</li> <li>IEEE 802.11 wireless LAN</li> </ul>	, FlagKEY FOUND! [ PASSWORD ]		
Master Key	: D0 CF 0D 1E 7F F2 3C 7D 9B 52 39 E 33 AE E6 A3 1E BA 4E 9A 2E 43 41 2	E8 9D B0 B7 81 23 5B 30 90 22	
Transient Key	: 11 B5 8E DC C6 96 01 01 84 41 6D 2	2A AF 8E 23 79	
- <u>-</u> -	EF A0 D6 6E F8 DB 3D 10 74 04 3C 9	96 55 EC FE 28	
-	A8 FD 03 DE F5 FC E0 1F 9E 30 69 E	EA EF 7C 96 4B	
	30 AC 43 /F FB ED /C 39 49 /E 3C 3	3E E2 01 11 97	
EAPOL HMAC	: 0E E5 34 4B B1 58 41 53 6F DC 73 C	CF 46 A8 FD BB	
<pre>interfect: content in the conte</pre>		ab Resources/Module 5# aircrack-ng -w ro	ckyou.txt WPA
0020 <b>2-P1-01.cap</b> 00 08 43			
0030 B2 84 8b 96 24 30 48			
			<b>V</b>
0060 10 18 02 00 f0 00 00	dd 18 00 50 f2 02 01 01	· · · · P · · · ·	
	A 00 00 40 40 Eo 00 60 00	L DOA bo	

After this, I used the command Airdecap-ng -p PASSWORD WPA2-p1-01.cap -e CyberPHY

root@CS2APenTest:~/Desktop/Lab	Resources (2023	Spring)/Lab	Resources/Module	5# airdecap-ng	-p PASSWORD	WPA2-P1-01.cap	- e
CyberPHY							
Total number of stations seen	12						_ 1
Total number of packets read	2660						_ 1
Total number of WEP data packet	s 0						_ 1
Total number of WPA data packet	s 629						_ 1
Number of plaintext data packet	s 0						_ 1
Number of decrypted WEP packet	s 0					Ĩ	,
Number of corrupted WEP packet	s 0					2	,
Number of decrypted WPA packet	s <sub>df 19</sub> 6471 <sub>6 b6</sub>						
Number of bad TKIP (WPA) packet	s oo f3 02 oo						_ 1
Number of bad CCMP (WPA) packet	S62 65 72 90 48			_			
<pre>root@CS2APenTest:~/Desktop/Lab</pre>	Resources (2023	<pre>Spring)/Lab</pre>	Resources/Module	5#			
0040 00 30 14 01 00 00 0f ac	04 01 00 00 0f	ac 0/ 01			_		_

Wireshark WPA2-p1-01.dec.cap to view the new file that is deciphered

rippatations ra							
	WPA2-P1	-01-dec.cap				×	
<u>F</u> ile <u>E</u> dit <u>V</u>	Wireshark · Protocol Hierarchy S	tatistics · WPA2-P1	-01-dec.cap	•			
	Protocol	Percent Packets	Packets	Percent Bytes	Bytes		D
	<ul> <li>Frame</li> </ul>	100.0	471	100.0	1561		
Apply a dis	<ul> <li>Ethernet</li> </ul>	100.0	471	4.2	6594	xpression +	
No. Tir	Internet Protocol Version 6	7.9	37	0.9	1480	-	
3 - 10	User Datagram Protocol	5.9	28	0.1	224	0xd5b2	
2.0.	Multicast Domain Name System	0.6	3	0.1	120	168.1.1	
· 30.	Link-local Multicast Name Resolution	4.5	21	0.4	582	ftconne	
40.	DHCPv6	0.8	4	0.2	380	J<00>	
5 0.	Internet Control Message Protocol v6	1.9	9	0.2	292	/in=513	
60.	<ul> <li>Internet Protocol Version 4</li> </ul>	90.9	428	5.5	8588		
70.	<ul> <li>User Datagram Protocol</li> </ul>	18.9	89	0.5	712	.07 → 80	2
80.	Simple Service Discovery Protocol	0.8	4	0.4	692	.ve.wns.	
90.	NetBIOS Name Service	5.3	25	0.8	1322	. A skyd	
10 0.	Multicast Domain Name System	0.6	3	0.1	120	ured] 8 🚽 🔻	
M •	Link-local Multicast Name Resolution	3.4	16	0.3	446	b l	
→ Frame 1:	GOLIIC (Google Quick LIDP Internet Connections)	25	12	25	3981		
Ethernet	Domain Name System	4.5	21	11	1793		
Internet → Internet	Data	11	5	0.2	239		
User Data	Bootstran Protocol	0.6	3	0.6	954		
🛛 👔 🕨 Bootstrap	Transmission Control Protocol	64.2	303	0.0	1261		146
	Secure Seckets Laver	28.0	126	61.9	9657		
	- Humantaut Transfer Distance	20.9	130	1.7	2669		
	Line based text data	0.0	1	1.7	2008		
	eXtensible Markun Language	0.2	1	0.0	1116		
	Data	0.2	2	1.2	2025		
<b>F</b>	Data	0.0	3	1.5	2035		
	Internet Group Management Protocol	1.5	20	0.1	120		
0000 ff f	Address Desolution Drotocol	0.2	29	0.7	160	1	-
0010 01 5	Address Resolution Protocol	1.5	Ø	0.1	108		
					•		
	No dieplay filter						
0050 00 0	No uspay men						
0060 00 0	Help			Сору -	≭ <u>C</u> lose		
0070 00 0							
0.000 00 00							

This is the Protocol Hierarchy after decryption

After review, there are multiple different protocols that are used = Mostly TCP, ICMP, and NBNS Looks like Cisco and Microsoft