

TASK C:

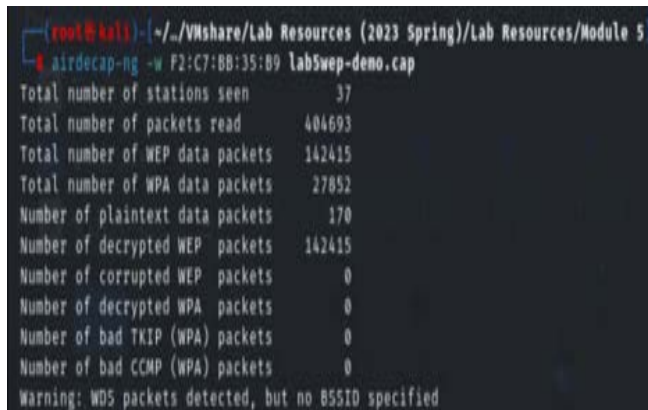
1. Decrypt the lab5wep-demo.cap file.



Find the Key (F2:C7:BB:35:B9)



Decrypt files using Key



Analysis shows abnormal ARP count
Could be because of network scanner or
Malware or another network issue.



Find the Key

```
(root@kali) [~/./VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
# aircrack-ng lab5wpa2-demo.cap -w rockyou.txt
Reading packets, please wait ...
Opening lab5wpa2-demo.cap
Read 10074 packets.
```

#	BSSID	ESSID	Encryption
1	00:16:86:DA:CF:32	ccni-test	WEP (0 IVs)
2	58:BF:EA:FA:3B:B0		Unknown
3	58:BF:EA:FA:3B:A0		Unknown
4	98:FC:11:7C:D0:C7	CCNI	WPA (1 handshake)
5	F4:7F:35:04:7D:E0		Unknown
6	F4:7F:35:39:0A:A0	AccessODU	Unknown
7	F4:7F:35:39:0A:A1		Unknown
8	F4:7F:35:39:0A:A2	MonarchODU	Unknown
9	F4:7F:35:39:0A:A4	eduroam	Unknown

```
Aircrack-ng 1.7

[00:00:00] 32/14344392 keys tested (182.46 k/s)

Time left: 21 hours, 50 minutes, 18 seconds      0.00%

KEY FOUND: [ password ]

Master Key      : 20 64 DE 6A 2E 73 86 96 81 91 BE 8C 1E 32 49 FC
                  3B C9 0A 44 BC 2B 6E 94 43 4B BF 8F B9 79 FC 3B

Transient Key   : 48 5D 7F 5E F5 AA 69 76 D8 85 83 31 FA 2A 65 A4
                  C0 A0 D1 4A 96 BC C5 96 65 7A FC A2 44 94 14 51
                  EC 9C 42 51 E1 EA BF AE 3F BB 64 11 0D 60 70 24
                  77 81 71 A3 2C 1B 0C D1 0A 1C BF 1C EC 00 00 00

EAPOL HMAC     : 49 94 2C 92 12 84 BA 66 ED DB 40 0F 10 A5 19 47
```

Use key to decrypt

```
(root@kali) [~/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
# airdecap-ng -p password lab5wpa2-demo.cap -e CCNI
Total number of stations seen      13
Total number of packets read      10074
Total number of WEP data packets   19
Total number of WPA data packets  2284
Number of plaintext data packets   7
Number of decrypted WEP packets    0
Number of corrupted WEP packets    0
Number of decrypted WPA packets    2228
Number of bad TKIP (WPA) packets  0
Number of bad CCMP (WPA) packets  0
Warning: WDS packets detected, but no BSSID specified
```

Analyze Traffic

No.	Time	Source	Destination	Protocol	Length	Info
-----	------	--------	-------------	----------	--------	------

No.	Time	Source	Destination	Protocol	Length	Info
-----	------	--------	-------------	----------	--------	------

[illegible]

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	End Packets	End Bytes	End Bytes
- IPsec	506.0	2228	506.0	440,293	142.4	0	0
- Ethernet	506.0	2228	4.8	2162	9,674	0	0
- Internet Protocol Version 6	4.1	3	0.0	120	37	0	0
- User Datagram Protocol	0.0	1	0.0	4	2	0	0
- Multicast Domain Name System	0.0	1	0.1	278	86	1	278
- Internet Control Message Protocol v6	0.1	2	0.0	40	12	3	40
- Internet Protocol Version 4	99.9	2226	9.7	444,30	116	0	0
- User Datagram Protocol	1.3	33	0.0	444	33	0	0
- Network Time Protocol	0.0	1	0.0	48	14	1	48
- Multicast Domain Name System	0.0	1	0.0	194	39	1	194
- GIGOC (Google Cloud) UDP Internet Connectivity	0.1	2	0.3	1287	430	3	1287
- Domain Name System	1.6	33	0.2	939	281	32	939
- Data	0.3	7	0.3	3274	426	7	1218
- Transmission Control Protocol	98.3	2198	82.6	378997	717.4	7688	305797
- Transport Layer Security	9.7	197	6.5	36188	12.6	127	36188
- Hypertext Transfer Protocol	2.6	62	14.2	63337	20.4	97	64332
- Portmap Network Graphics	0.0	1	0.2	1090	328	1	1090
- Data	0.0	1	0.0	140	14	1	140
- Address Resolution Protocol	0.2	4	0.0	72	16	4	12

The traffic displays normal, secure traffic primarily utilizing TCP protocol. Unlike the previous results, there is a much lower percentage of ARP requests. Traffic is consistent with HTTP/HTTPS use.

TASK D: swood041 -> 6b351b67f8512748fb4d4d44b12bab7c (WPA2-P5-01.cap)

1. Implement a dictionary attack and decrypt the traffic. (Key: messenger)

```
(root@kali) ~/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5
# aircrack-ng WPA2-P5-01.cap -w rockyou.txt
Reading packets, please wait...
Opening WPA2-P5-01.cap
Read 7675 packets.

# BSSID      ESSID      Encryption
1 00:16:B6:DA:CF:2F  CyberPHY   WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening WPA2-P5-01.cap
Read 7675 packets.

1 potential targets
```

```
Aircrack-ng 1.7
[00:00:01] 1988/10303727 keys tested (2315.64 k/s)
Time left: 1 hour, 14 minutes, 8 seconds 0.02%

KEY FOUND! [ messenger ]

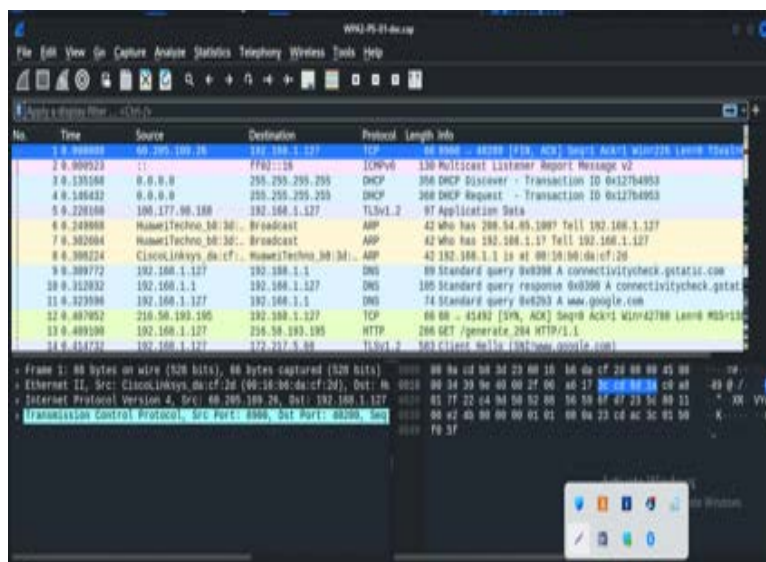
Master Key   : 16 3E A6 91 E3 3C 93 35 91 D1 8B CC 78 88 A6 1D
              8D FB 9D 22 B6 72 FF 9D 71 1A E3 92 36 EF D2 29

Transient Key : 18 A2 CC E8 B5 4A 5F C6 50 74 DE 6E FB 86 21 D6
              9F B6 D2 88 D7 7C EB 31 E3 7F DB 56 36 91 E0 F0
              AD 1A 45 77 26 ED 20 D0 E7 C0 2E F7 2D 00 92 00
              00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC   : 1D E7 D1 39 D3 96 98 0F 5C FB 90 7A 89 32 25 2B
```

```
(root@kali) ~/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5
# aircrack-ng -p messenger WPA2-P5-01.cap -e CyberPHY
Total number of stations seen      7
Total number of packets read      7675
Total number of WEP data packets   0
Total number of WPA data packets  1793
Number of plaintext data packets   0
Number of decrypted WEP packets    0
Number of corrupted WEP packets    0
Number of decrypted WPA packets    1668
Number of bad TKIP (WPA) packets   0
Number of bad CCMP (WPA) packets   0
```

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



Wireshark - Protocol Hierarchy Statistics - WPA2-P5-01-decap.pcap

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End
Frame	100.0	1668	100.0	613627	140 k	0	0	0
Ethernet	100.0	1668	3.8	23352	5.35k	0	0	0
Internet Protocol Version 6	0.2	4	0.0	160	36	0	0	0
Internet Control Message Protocol v6	0.2	4	0.0	188	43	4	188	43
Internet Protocol Version 4	99.4	1658	5.4	32160	7.69k	0	0	0
User Datagram Protocol	55.5	926	1.2	7408	1.70k	0	0	0
Multicast Domain Name System	0.1	2	0.0	122	27	2	122	27
Internet Security Association and Key Management Protocol	0.1	1	0.1	488	111	1	488	111
QUIC (Google Quick UDP Internet Connections)	41.9	699	46.8	287090	65 k	699	287090	65 k
Dynamic Host Configuration Protocol	0.1	2	0.1	640	146	2	640	146
Domain Name System	2.3	39	0.3	1803	413	39	1803	413
Data	11.0	183	13.5	82617	18 k	183	82617	18 k
Transmission Control Protocol	43.8	731	28.7	175216	40 k	624	87839	20 k
X11	0.1	1	0.0	34	5	0	0	0
Malformed Packet	0.1	1	0.0	0	0	1	0	0
Transport Layer Security	2.9	48	2.1	12856	2.95k	48	12856	2.95k
MSN Messenger Service	1.9	31	7.3	44888	10 k	31	44888	10 k
Hypertext Transfer Protocol	1.5	25	4.4	27075	6.21k	25	27075	6.21k
Data	0.1	2	0.0	132	30	2	132	30
Internet Control Message Protocol	0.1	1	0.1	489	112	0	0	0
Internet Security Association and Key Management Protocol	0.1	1	0.1	453	103	1	453	103
Address Resolution Protocol	0.4	6	0.0	168	38	6	168	38

- For this part of the assignment, I was tasked with decrypting and analyzing the network traffic for WPA2-P5-01.cap. After running a dictionary attack against the CyberPHY network, I was able to reveal that the password was “messenger”. After decrypting the network traffic using the password, I was able to see all the different kinds of network traffic going across the network in this lab snippet. It appears as if UDP was the primary protocol used at 55.5% of packets. TCP was secondary to UDP coming in at 43.8% of packets. GQUIC at 41.9% of packets reveals that the network was being used for a form of UDP Google Service. mSN Messenger Service at 1.9% of packets reveals that a form of messaging service was also being used at the time.