

Bryant Watkins

4/9/26

Wi-Fi Password Cracking LAB REPORT

CYSE 601

Relevant Systems

- pfSense firewall VM (IP: 192.168.10.2)
- Internal Kali Linux machine (IP: 192.168.10.13)

WEP Password Cracking

```
root@kali: ~/Desktop
File Actions Edit View Help
6 18:9C:5D:EF:46:70 Unknown
7 18:9C:5D:EF:48:50 Unknown
8 18:9C:5D:EF:4D:A0 Unknown
9 58:BF:EA:0F:F9:00 Unknown
10 58:BF:EA:0F:F9:01 Unknown
11 58:BF:EA:24:98:91 WPA (0 handshake)
12 58:BF:EA:FA:16:10 Unknown
13 58:BF:EA:FA:38:B0 Unknown
14 58:BF:EA:FA:38:A0 Unknown
15 58:BF:EA:FA:38:A2 MonarchODU WPA (0 handshake)
16 5C:50:15:E7:FE:42 MonarchODU EAPOL-WPA (0 handshake)
17 98:FC:11:7C:CE:63 dd-wrt Unknown
18 98:FC:11:7C:D0:C7 CCNI WPA (0 handshake)
19 F4:7F:35:04:01:A0 Unknown
20 F4:7F:35:04:08:20 Unknown
21 F4:7F:35:04:65:A0 Unknown
22 F4:7F:35:04:7D:E0 AccessODU Unknown
23 F4:7F:35:04:7D:E1 Unknown
24 F4:7F:35:04:7D:E2 MonarchODU WPA (0 handshake)
25 F4:7F:35:04:7D:E4 eduroam Unknown
26 F4:7F:35:39:0A:A0 Unknown
27 F4:7F:35:42:0E:C2 Unknown

Index number of target network ? 1
Reading packets, please wait...
Opening lab5wep-demo.cap
Read 404693 packets.

1 potential targets
Attack will be restarted every 5000 captured ivs.

Aircrack-ng 1.7
[00:00:02] Tested 231 keys (got 19772 IVs)

KB depth byte(vote)
0 0/ 2 F2(28928) 7A(27136) 30(26112) 21(24832) 27(24832) 03(24576) F8(24576) 05(24320) 38(24064) 84(24064) 9A(24064) B6(24064) 29(23552) 3E(23552) 47(23552)
1 9/ 10 C7(24064) 71(23808) 5C(23552) 20(23296) 2A(23296) 52(23296) 84(23296) 99(23040) DE(23040) 5B(22784) 62(22784) 8A(22784) E8(22784) 49(22528) 6A(22528) 8D(22528)
2 0/ 1 B8(30208) AB(25344) BF(25344) D0(24832) 08(24576) 93(24576) CC(24320) D3(24064) 09(23808) 1C(23552) 4E(23552) ED(23552) 98(23296) 9B(23296) A5(23296)
3 8/ 12 FC(24064) 25(23808) 2A(23808) A9(23808) B0(23808) 00(23552) 42(23552) 3F(23296) 62(23296) 2C(23040) 3C(23040) 3E(23040) BA(23040) 41(22784) 48(22784)
4 0/ 1 B9(30720) 33(26624) 2E(25344) C4(25344) 64(25088) ED(25088) 55(24832) 77(24832) 9C(24576) FF(24576) 69(24064) 6D(24064) 49(23552) B1(23552) CA(23552)

KEY FOUND! [ F2:C7:BB:35:B9 ]
```

Aircrack-ng Command

```
root@kali: ~/Desktop
File Actions Edit View Help

(root@kali)~[~/Desktop]
# airdecap-ng -w F2:C7:BB:35:B9 lab5wep-demo.cap
Total number of stations seen 37
Total number of packets read 404693
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
Warning: WDS packets detected, but no BSSID specified
```

Airdecap-ng Command

The image shows a Wireshark capture of network traffic. The top pane displays a list of packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The bottom pane shows the raw packet bytes in hexadecimal and ASCII. The traffic includes IEEE 802.11 Beacon frames and QoS Data frames, all of which are encrypted, appearing as random hexadecimal data.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco_04:7d:e1	Broadcast	802.11	263	263 Beacon frame, SN=513, FN=0, Flags=....., BI=102, SSID=00
2	-0.000017	Intel_3b:c8:c9 (fc:..)	Cisco_fa:3b:a2 (58:..)	802.11	28	802.11 Block Ack, Flags=.....
3	0.000523	Apple_28:d8:50	CiscoLinksys_7c:d0:..	802.11	150	QoS Data, SN=2829, FN=0, Flags=p..R..T
4	0.000522		CiscoLinksys_7c:d0:..	802.11	10	Acknowledgement, Flags=.....
5	0.002571	Apple_28:d8:50	CiscoLinksys_7c:d0:..	802.11	457	QoS Data, SN=2830, FN=0, Flags=p.....T
6	0.002591		Apple_28:d8:50 (30:..)	802.11	10	Acknowledgement, Flags=.....
7	0.014858	Apple_28:d8:50	CiscoLinksys_7c:d0:..	802.11	146	QoS Data, SN=2831, FN=0, Flags=p.....T
8	0.017930	Apple_28:d8:50	CiscoLinksys_7c:d0:..	802.11	146	QoS Data, SN=2831, FN=0, Flags=p..R..T
9	0.024088	CiscoLinksys_7c:ce:..	Broadcast	802.11	112	Beacon frame, SN=2018, FN=0, Flags=....., BI=100, SSID="dd-wrt"
10	0.024056	CiscoLinksys_da:cf:..	Broadcast	802.11	115	Beacon frame, SN=1058, FN=0, Flags=....., BI=100, SSID="ccni-test"
11	0.029194	Apple_28:d8:50	CiscoLinksys_7c:d0:..	802.11	145	QoS Data, SN=2832, FN=0, Flags=p.....T
12	0.031754		CiscoLinksys_7c:d0:..	802.11	10	Acknowledgement, Flags=.....
13	0.032799		Apple_28:d8:50 (30:..)	802.11	10	Acknowledgement, Flags=.....
14	0.033280	Cisco_04:7d:e0	Broadcast	802.11	249	Beacon frame, SN=514, FN=0, Flags=....., BI=102, SSID="Access00U"
15	0.046080	Cisco_04:7d:e4	Broadcast	802.11	269	Beacon frame, SN=515, FN=0, Flags=....., BI=102, SSID="eduroam"
16	0.067103	CiscoLinksys_7c:d0:..	Broadcast	802.11	132	Beacon frame, SN=2767, FN=0, Flags=....., BI=100, SSID=00000000
17	0.067594	Apple_28:d8:50	CiscoLinksys_7c:d0:..	802.11	132	QoS Data, SN=2835, FN=0, Flags=p..R..T
18	0.067615		Apple_28:d8:50 (30:..)	802.11	10	Acknowledgement, Flags=.....
19	0.070687	Apple_28:d8:50	Apple_28:d8:50 (30:..)	802.11	10	Acknowledgement, Flags=.....
20	0.093194	Apple_28:d8:50	CiscoLinksys_7c:d0:..	802.11	145	QoS Data, SN=2837, FN=0, Flags=p.....T
21	0.103434	Apple_28:d8:50	CiscoLinksys_7c:d0:..	802.11	148	QoS Data, SN=2838, FN=0, Flags=p.....T
22	0.110602	Apple_28:d8:50	CiscoLinksys_7c:d0:..	802.11	518	QoS Data, SN=2839, FN=0, Flags=p.....T
23	0.110623		Apple_28:d8:50 (30:..)	802.11	10	Acknowledgement, Flags=.....
24	0.134154	Apple_28:d8:50	CiscoLinksys_7c:d0:..	802.11	143	QoS Data, SN=2840, FN=0, Flags=p.....T
25	0.141834	Apple_28:d8:50	CiscoLinksys_7c:d0:..	802.11	306	QoS Data, SN=2841, FN=0, Flags=p.....T

Frame 1: 263 bytes on wire (2104 bits), 263 bytes captured (2104 bits) on interface 0
 IEEE 802.11 Beacon frame, Flags:

Frame 10: 115 bytes on wire (920 bits), 115 bytes captured (920 bits) on interface 0
 IEEE 802.11 Wireless Management

lab5wep-demo.cap | Packets: 404693 - Displayed: 404693 (100.0%) | Profile: Default

Encrypted Traffic

The image shows a Wireshark capture of network traffic where the traffic has been decrypted. The top pane displays a list of packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The bottom pane shows the raw packet bytes in hexadecimal and ASCII, revealing the actual content of the frames.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	CiscoLinksys_da:cf:..	Spanning-tree-(for-..)	0x0000	52	Ethernet II
2	0.281158	70.186.28.24	192.168.2.10	TCP	66	443 -> 63745 [ACK] Seq=1 Ack=1 Win=260 Len=0 TSval=1002332331 TSecr=1102367625
3	1.434778	Apple_d3:93:65	CiscoLinksys_da:cf:..	ARP	42	192.168.2.10 is at a4:5e:00:d3:93:65
4	1.945724	CiscoLinksys_da:cf:..	Spanning-tree-(for-..)	0x0000	52	Ethernet II
5	2.133124	70.186.30.27	192.168.2.10	TCP	66	443 -> 63613 [ACK] Seq=1 Ack=1 Win=470 Len=0 TSval=1008078397 TSecr=1102504918
6	2.138756	70.186.30.27	192.168.2.10	TLSv1.2	112	Application Data
7	2.175108	70.186.30.27	192.168.2.10	TLSv1.2	164	Application Data, Application Data
8	2.175108	70.186.30.27	192.168.2.10	TLSv1.2	168	Application Data, Application Data
9	2.232451	70.186.30.27	192.168.2.10	TCP	78	443 -> 63613 [ACK] Seq=749 Ack=47 Win=470 Len=0 TSval=1008078496 TSecr=1102505016 SL...
10	3.175102	192.168.2.39	192.168.2.255	NBNS	92	Name query NB CCNI_LAB<00>
11	3.176677	192.168.2.10	192.168.2.255	BROWSER	216	Get Backup List Request
12	3.179198	192.168.2.10	192.168.2.255	BROWSER	216	Get Backup List Request
13	3.994366	192.168.2.39	192.168.2.255	NBNS	92	Name query NB CCNI_LAB<00>
14	3.994878	CiscoLinksys_da:cf:..	Spanning-tree-(for-..)	0x0000	52	Ethernet II
15	4.710718	192.168.2.39	192.168.2.255	NBNS	92	Name query NB CCNI_LAB<00>
16	4.733275	192.168.2.10	70.186.30.26	TCP	54	63753 -> 443 [ACK] Seq=1 Ack=1 Win=4092 Len=0
17	4.733275	192.168.2.10	70.186.30.27	TCP	54	63752 -> 443 [ACK] Seq=1 Ack=1 Win=4083 Len=0
18	14.850800	70.186.30.27	192.168.2.10	TCP	60	110 -> 443 [ACK] Seq=1 Ack=1 Win=4092 Len=0 TSval=1008078444 TSecr=1102508206 [Seq=1 Ack=2 Win=243 Len=0 TSval=918936
19	15.262240	192.168.2.10	70.186.28.23	TCP	54	63755 -> 443 [ACK] Seq=1 Ack=1 Win=4083 Len=0
20	15.262748	192.168.2.10	70.186.28.21	TCP	54	63754 -> 443 [ACK] Seq=1 Ack=1 Win=4083 Len=0
21	15.427101	192.168.2.10	164.106.251.250	TCP	66	63776 -> 80 [FIN, ACK] Seq=1 Ack=1 Win=4104 Len=0 TSval=1102508206 TSecr=1872767129
22	15.427101	192.168.2.10	164.106.251.250	TCP	66	63777 -> 80 [FIN, ACK] Seq=1 Ack=1 Win=4104 Len=0 TSval=1102508206 TSecr=1872767923
23	15.427101	192.168.2.10	164.106.251.250	TCP	66	63779 -> 80 [FIN, ACK] Seq=1 Ack=1 Win=4104 Len=0 TSval=1102508206 TSecr=1872766944
24	15.427612	192.168.2.10	164.106.251.250	TCP	66	63778 -> 80 [FIN, ACK] Seq=1 Ack=1 Win=4104 Len=0 TSval=1102508206 TSecr=1872767725
25	15.427612	192.168.2.10	164.106.251.250	TCP	66	63780 -> 80 [FIN, ACK] Seq=1 Ack=1 Win=4104 Len=0 TSval=1102508206 TSecr=1872767328

Frame 1: 52 bytes on wire (416 bits), 52 bytes captured (416 bits) on interface 0
 Ethernet II, Src: CiscoLinksys_da:cf:32 (00:16:b6:da:cf:32), Dst: Spanning-tree-(for-..)

Frame 2: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
 TCP, Src: 70.186.28.24, Dst: 192.168.2.10, Seq: 1, Win: 260, Len: 0

Frame 3: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
 ARP, Src: Apple_d3:93:65, Dst: 192.168.2.10

Frame 5: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
 TCP, Src: 70.186.30.27, Dst: 192.168.2.10, Seq: 1, Win: 470, Len: 0

Frame 6: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface 0
 TLSv1.2, Src: 70.186.30.27, Dst: 192.168.2.10

Frame 7: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits) on interface 0
 TLSv1.2, Src: 70.186.30.27, Dst: 192.168.2.10

Frame 9: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
 TCP, Src: 70.186.30.27, Dst: 192.168.2.10, Seq: 749, Win: 470, Len: 0

Frame 10: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0
 NBNS, Src: 192.168.2.39, Dst: 192.168.2.255

Frame 11: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface 0
 BROWSER, Src: 192.168.2.10, Dst: 192.168.2.255

Frame 12: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface 0
 BROWSER, Src: 192.168.2.10, Dst: 192.168.2.255

Frame 13: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0
 NBNS, Src: 192.168.2.39, Dst: 192.168.2.255

Frame 15: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0
 NBNS, Src: 192.168.2.39, Dst: 192.168.2.255

Frame 16: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
 TCP, Src: 192.168.2.10, Dst: 70.186.30.26, Seq: 1, Win: 4092, Len: 0

Frame 17: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
 TCP, Src: 192.168.2.10, Dst: 70.186.30.27, Seq: 1, Win: 4083, Len: 0

Frame 18: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
 TCP, Src: 70.186.30.27, Dst: 192.168.2.10, Seq: 1, Win: 4092, Len: 0

Frame 19: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
 TCP, Src: 192.168.2.10, Dst: 70.186.28.23, Seq: 1, Win: 4083, Len: 0

Frame 20: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
 TCP, Src: 192.168.2.10, Dst: 70.186.28.21, Seq: 1, Win: 4083, Len: 0

Frame 21: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
 TCP, Src: 192.168.2.10, Dst: 164.106.251.250, Seq: 1, Win: 4104, Len: 0

Frame 22: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
 TCP, Src: 192.168.2.10, Dst: 164.106.251.250, Seq: 1, Win: 4104, Len: 0

Frame 23: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
 TCP, Src: 192.168.2.10, Dst: 164.106.251.250, Seq: 1, Win: 4104, Len: 0

Frame 24: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
 TCP, Src: 192.168.2.10, Dst: 164.106.251.250, Seq: 1, Win: 4104, Len: 0

Frame 25: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
 TCP, Src: 192.168.2.10, Dst: 164.106.251.250, Seq: 1, Win: 4104, Len: 0

lab5wep-demo-dec.cap | Packets: 142415 - Displayed: 142415 (100.0%) | Profile: Default

Decrypted Traffic

Analysis

The first step in the WEP Wi-Fi password cracking process entails changing the current working directory to the location of the encrypted Wireshark traffic data. The command to examine this traffic is *aircrack-ng "file name"*, this command will display any Wi-Fi networks within the captured packet traffic file. The administrator will then be prompted to select the "index number of target network", this simply requires the administrator to enter the number corresponding to the desired Wi-Fi network, which is *WEP* in this case. The *aircrack-ng* command will then produce an output displaying a 64-bit WEP key, which will be used for the next command.

The next applicable command in the process is *airdecap-ng* to further decrypt the traffic file, and this command will require the inclusion of the newly acquired 64-bit WEP key along with file name. This will then produce a new decrypted packet file available for further analysis. Upon opening the newly created decrypted packet file, there will be a plethora of data fields to assess. Upon assessing the data, the administrator will be able to observe any distinctive patterns in traffic.

The decrypted Wi-Fi Wireshark traffic obtained provides us with a few data points of particular note. The packets' protocols are now visible, as they were initially illustrated as "802.11" initially. Critically, the newly decrypted traffic also now displays source and destination internet protocol addresses previously concealed, providing further information for potential escalatory attacks if desired. An incredibly high volume of ARP protocol packets is visible as well, indicating the immense scanning efforts taken in the decryption process. Analyzing data points such as these are critical in the understanding of the Wi-Fi password cracking process and can assist in exploring options for future incursions and vulnerability exploitation.

WPA2 Password Cracking

```
root@kali: ~/Desktop
└─(root@kali)─[~/Desktop]
# aircrack-ng -w rockyou.txt lab5wpa2-demo.cap
Reading packets, please wait...
Opening lab5wpa2-demo.cap
Read 10074 packets.

# BSSID      ESSID      Encryption
1 00:16:B6:DA:CF:32 ccni-test  WEP (0 IVs)
2 58:BF:EA:FA:38:B0          Unknown
3 58:BF:EA:FA:38:A0          Unknown
4 98:FC:11:7C:00:C7          WPA (1 handshake)
5 F4:7F:35:39:04:7D: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

Index number of target network ? 4

Reading packets, please wait...
Opening lab5wpa2-demo.cap
Read 10074 packets.

1 potential targets

Aircrack-ng 1.7

[00:00:00] 16/14344392 keys tested (78.50 k/s)

Time left: 2 days, 2 hours, 45 minutes, 40 seconds      0.00%

KEY FOUND! [ password ]

Master Key   : 20 64 DE 6A 2E 73 86 96 81 91 8E 8C 1E 32 49 FC
              3B C9 0A 44 BC 2B 6E 94 45 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 5F BB 64 11 0D 60 70 24
                77 81 71 A3 2C 1B BC D1 0A 1C BF 1C EC 00 00 00

EAPOL HMAC   : 49 94 2C 92 12 04 BA 66 ED D8 40 8F 10 A5 19 47
```

Aircrack-ng Command

```
root@kali: ~/Desktop
└─(root@kali)─[~/Desktop]
# 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
```

Airdecap-ng Command

The screenshot shows a Wireshark capture of network traffic. The main pane displays a list of packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The selected packet (No. 1) is an IEEE 802.11 Request-to-send frame from Cisco_39:0a:a0 to LiteonTechno_c8:c4:802.11. The packet details pane shows the frame structure, including the MAC addresses and the IEEE 802.11 header. The packet bytes pane shows the raw hex and ASCII data.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco_39:0a:a0 (f4:...	LiteonTechno_c8:c4:802.11	802.11	16	Request-to-send, Flags=.....
2	0.000001	Cisco_39:0a:a0 (f4:...	LiteonTechno_c8:c4:802.11	802.11	16	Request-to-send, Flags=.....
3	0.000000	Cisco_39:0a:a0 (f4:...	LiteonTechno_c8:c4:802.11	802.11	28	802.11 Block Ack, Flags=.....
4	0.006144	Cisco_39:0a:a0 (f4:...	LiteonTechno_c8:c4:802.11	802.11	16	Acknowledgement, Flags=.....
5	0.015382	CiscoLinksys_da:cf:...	Broadcast	802.11	115	Beacon frame, SN=69, FN=0, Flags=....., BI=100, SSID="ccni-test"
6	0.020480	Cisco_39:0a:a0 (f4:...	LiteonTechno_c8:c4:802.11	802.11	16	Request-to-send, Flags=.....
7	0.025000	Cisco_39:0a:a0 (f4:...	LiteonTechno_c8:c4:802.11	802.11	16	Request-to-send, Flags=.....
8	0.040469	CiscoLinksys_da:cf:...	Spanning-tree-for-...	802.11	78	Data, SN=69, FN=0, Flags=p....F.
9	0.040448	Cisco_39:0a:a0 (f4:...	LiteonTechno_c8:c4:802.11	802.11	16	Request-to-send, Flags=.....
10	0.040448	Cisco_39:0a:a0 (f4:...	LiteonTechno_c8:c4:802.11	802.11	16	Request-to-send, Flags=.....
11	0.040449	Cisco_39:0a:a0 (f4:...	LiteonTechno_c8:c4:802.11	802.11	16	Request-to-send, Flags=.....
12	0.047105	Cisco_39:0a:a0 (f4:...	LiteonTechno_c8:c4:802.11	802.11	16	Request-to-send, Flags=.....
13	0.047104	Cisco_39:0a:a0 (f4:...	LiteonTechno_c8:c4:802.11	802.11	16	Request-to-send, Flags=.....
14	0.048129	Cisco_39:0a:a0 (f4:...	LiteonTechno_c8:c4:802.11	802.11	28	802.11 Block Ack, Flags=.....
15	0.070176	CiscoLinksys_7c:d0:...	Broadcast	802.11	132	Beacon frame, SN=3453, FN=0, Flags=....., BI=100, SSID="00000000"
16	0.135679	Apple_8f:58:79	Broadcast	802.11	123	Probe Request, SN=1012, FN=0, Flags=....., SSID="MonarchODU"
17	0.166913	Cisco_39:0a:a2	Broadcast	802.11	272	Beacon frame, SN=3442, FN=0, Flags=....., BI=102, SSID="MonarchODU"
18	0.206008	Cisco_39:0a:a4	Broadcast	802.11	269	Beacon frame, SN=3445, FN=0, Flags=....., BI=102, SSID="eduroam"
19	0.275000	CiscoLinksys_49:f4:...	CiscoLinksys_49:f4:...	802.11	10	Acknowledgement, Flags=.....
20	0.276400	CiscoLinksys_49:f4:...	CiscoLinksys_49:f4:...	802.11	26	Deauthentication, SN=3447, FN=0, Flags=.....
21	0.286715	CiscoLinksys_49:f4:...	CiscoLinksys_49:f4:...	802.11	10	Acknowledgement, Flags=.....
22	0.287744	LiteonTechno_c8:c4:...	LiteonTechno_c8:c4:...	802.11	10	Acknowledgement, Flags=.....
23	0.295424	Intel_38:ea:05 (ac:...	Intel_38:ea:05 (ac:...	802.11	10	Clear-to-send, Flags=.....
24	0.295424	Intel_38:ea:05 (ac:...	Intel_38:ea:05 (ac:...	802.11	10	Acknowledgement, Flags=.....
25	0.305664	LiteonTechno_c8:c4:...	LiteonTechno_c8:c4:...	802.11	10	Acknowledgement, Flags=.....

Encrypted Traffic

The screenshot shows a Wireshark capture of network traffic. The main pane displays a list of packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The selected packet (No. 1) is a Whois query from Apple_d3:93:65 to 192.168.2.23. The packet details pane shows the query structure, including the IP addresses and the query text. The packet bytes pane shows the raw hex and ASCII data.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Apple_d3:93:65	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.2.23
2	0.033280	192.168.2.23	8.8.8.8	DNS	73	Standard query 0xcb70 A www.apple.com
3	0.227328	192.168.2.23	224.0.0.251	MDNS	156	Standard query 0x0000 ANY PengdeMacBook-Pro.local, "qu" question ANY PengdeMacBook...
4	0.227328	192.168.2.23	192.168.2.1	UDP	46	58834 192 Len=1
5	0.480768	::	ff02::1:ff03:9365	ICMPv6	78	Neighbor solicitation for fe80::a65e:60ff:fed3:9365
6	0.606032	fe80::a65e:60ff:fed3:9365	ff02::fb	MDNS	340	Standard query 0x0000 PTR _airport._tcp.local, "QM" question PTR _raop._tcp.local, ...
7	0.842304	Apple_d3:93:65	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.2.23
8	0.883264	192.168.2.23	74.125.22.189	TCP	66	57368 - 443 [ACK] Seq=1 Ack=1 Win=4091 Len=0 TSval=499413164 TSecr=1482114238
9	1.208896	Apple_d3:93:65	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.2.23
10	1.216576	192.168.2.23	74.125.22.189	TCP	66	[TCP Previous segment not captured] 57368 - 443 [ACK] Seq=2325 Ack=343 Win=4085 Len=...
11	1.735808	192.168.2.23	17.172.232.82	TCP	66	57369 - 5223 [ACK] Seq=1 Ack=1 Win=4117 Len=6 TSval=499414011 TSecr=2178265941
12	0.000000	192.168.2.23	17.172.232.82	TLSv1.2	101	[TCP Previous segment not captured] . Application Data
13	2.232960	Apple_d3:93:65	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.23
14	3.004800	17.110.226.165	192.168.2.23	TLSv1.2	135	Application Data
15	3.429954	17.172.232.82	192.168.2.23	TLSv1.2	204	[TCP ACKed unseen segment] . Application Data, Application Data
16	3.441856	192.168.2.23	17.110.225.208	TCP	54	57356 - 5223 [RST] Seq=1 Win=0 Len=0
17	3.762944	fe80::a65e:60ff:fed3:9365	ff02::1	ICMPv6	78	Router Solicitation from a4:5e:60:d3:93:65
18	3.822336	17.172.232.82	192.168.2.23	TCP	66	[TCP ACKed unseen segment] [TCP Previous segment not captured] 5223 - 57369 [ACK] S...
19	3.849984	17.248.135.143	192.168.2.23	TLSv1.2	1514	Server Hello
20	3.859200	17.167.138.20	192.168.2.23	TCP	1514	443 - 57372 [PSH, ACK] Seq=1 Ack=1 Win=2568 Len=1460 [TCP segment of a reassembled ...
21	3.860224	192.168.2.23	17.167.138.20	TCP	54	[TCP ACKed unseen segment] 57372 - 443 [ACK] Seq=1 Ack=2682 Win=8110 Len=0
22	3.876095	17.248.135.143	192.168.2.23	TCP	66	[TCP Previous segment not captured] 443 - 57373 [ACK] Seq=3817 Ack=82 Win=122 Len=0
23	3.908864	17.167.138.20	192.168.2.23	TCP	54	[TCP ACKed unseen segment] [TCP Previous segment not captured] 443 - 57372 [ACK] Se...
24	3.910400	17.167.138.20	192.168.2.23	TCP	54	[TCP ACKed unseen segment] 443 - 57372 [ACK] Seq=2682 Ack=274 Win=3281 Len=0
25	3.911934	17.167.138.20	192.168.2.23	TLSv1.2	97	[TCP ACKed unseen segment] . Change Cipher Spec. Encrypted Handshake Message

Decrypted Traffic

Analysis

The first step in the WPA2 Wi-Fi password cracking process entails changing the current working directory to the location of the encrypted Wireshark traffic data file. The command to examine this traffic file is *aircrack-ng* "*file name*", this command will display any Wi-Fi networks within the captured packet traffic file. The administrator will then be prompted to select the "index number of target network", this simply requires the administrator to enter the number corresponding to the desired Wi-Fi network, which is *WPA* in this case. This is where the *WPA* password cracking process begins to differ from the *WEP* password cracking process. Not only are we looking for *WPA*, however, but we must also ensure the option selected has a four-way handshake. As opposed to the *aircrack-ng* command producing an output displaying a 64-bit WEP key, the output for *WPA* will further require the administrator to "Please specify a dictionary". After selecting the desired dictionary file, the administrator may now successfully obtain the password through a Dictionary attack (Syntax: *aircrack-ng* "*Traffic file name*" -w "*Dictionary file name*").

The next applicable command in the process is *airdecap-ng* to further decrypt the traffic file, and this command will require the inclusion of the newly acquired password along with file name and ESSID (which can be obtained from the initial *aircrack-ng* command output). This will then produce a new decrypted packet file available for further analysis. Upon opening the newly created decrypted packet file, there will be a plethora of data fields to assess. Upon assessing the data, the administrator will be able to observe any distinctive patterns in traffic.

The decrypted Wi-Fi Wireshark traffic obtained provides us with a few data points of particular note. The obtained unencrypted data shares a few similarities with the *WEP* unencrypted data. The packets' protocols are now visible, as they were initially illustrated as "802.11". Critically, the newly decrypted traffic also now displays source and destination internet protocol addresses previously concealed, providing further information for potential escalatory attacks if desired. As opposed to the patterns observed within the *WEP* traffic data, there is an incredibly high volume of TCP protocol packets that are visible. The high volume of TCP packets indicates a high level of network activity/traffic, which can also be indicated by the red TCP packet indicating network congestion and connection failure. As with *WEP traffic* data, analysis of data points such as these are integral in the understanding of the Wi-Fi password cracking process and could assist in exploring options for future incursions and vulnerability exploitation.