

# Herwerkt tussentijds verslag P&O3 individuele opdracht

Willem Hendig (r0995944)

November 2024

# 1 Aircrack

The first step in the project is acquiring the WEP key, as it ~~'s~~ is a key component for all the following steps. Aircrack-ng is used to find this key.

## 1.1 Overview of Aircrack

Aircrack-ng, further referred to as Aircrack, is a suite of network security tools used for monitoring, attacking, and cracking WEP and WPA encrypted networks [Devine, 2022]. It ~~'s~~ is commonly used to assess network security. In this project, Aircrack will ~~crack a WEP-encrypted network to retrieve~~ acquire the WEP key ~~using flaws of the WEP-encryption algorithm.~~

## 1.1 Cracking the WEP access point

WEP encryption uses a combination of a shared key and ~~an~~ a Initialization Vector (IV) to encrypt network traffic. However, due to the weak IV implementation, it is possible to recover the shared key after capturing enough packets. ~~Aircrack-ng~~ Aircrack exploits this vulnerability by analyzing captured data and IVs to reconstruct the WEP key.

### 1.1.1 Structure of a WEP-encrypted packet

The inherent vulnerability of WEP encryption lies in its packet structure. To encrypt a packet, a key is used, which consists of:

- A 24-bit Initialization Vector (IV)
- A WEP key consisting of either 40 bits (for 64-bit encryption) or 104 bits (for 128-bit encryption)

This key is used in an RC4 algorithm to encrypt the packet. However, as the IV is randomly generated for every packet, this causes a problem for the receiver. To enable decryption, the IV is appended to the front of the encrypted packet. This ~~feature~~ is the core weakness of WEP encryption, as it creates two critical vulnerabilities:

1. The IV's limited size (24 bits) leads to the inevitable reuse
2. The transmission of the IV enables attackers to collect and analyze IV patterns

When two packets share the same IV, also known as IV Collision [Barken, 2003], cryptanalysis can be used to determine the static WEP key, allowing for all subsequent packets to be decrypted.

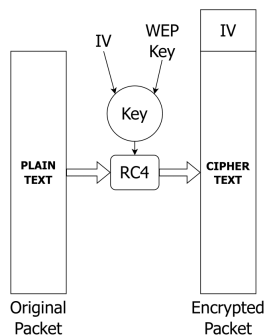


Figure 1: ~~The structure of a~~ WEP-encrypted packet

## 1.2 ~~Aircrack-commands~~Executing the attack

~~Aircrack-ng~~ ~~Aircrack~~ consists of several tools, each performing a specific function in ~~the process of cracking WEP encryption~~. The key tools used in this project are explained in the following paragraphs. ~~WEP password cracking~~. The following paragraphs aim to provide a high-level overview of the attack and the commands used during it. This attack largely follows the one detailed in [darkAudax, 2010]. The specific commands used are detailed in Appendix 7.1.

### 1.2.1 ~~airmon-ng~~

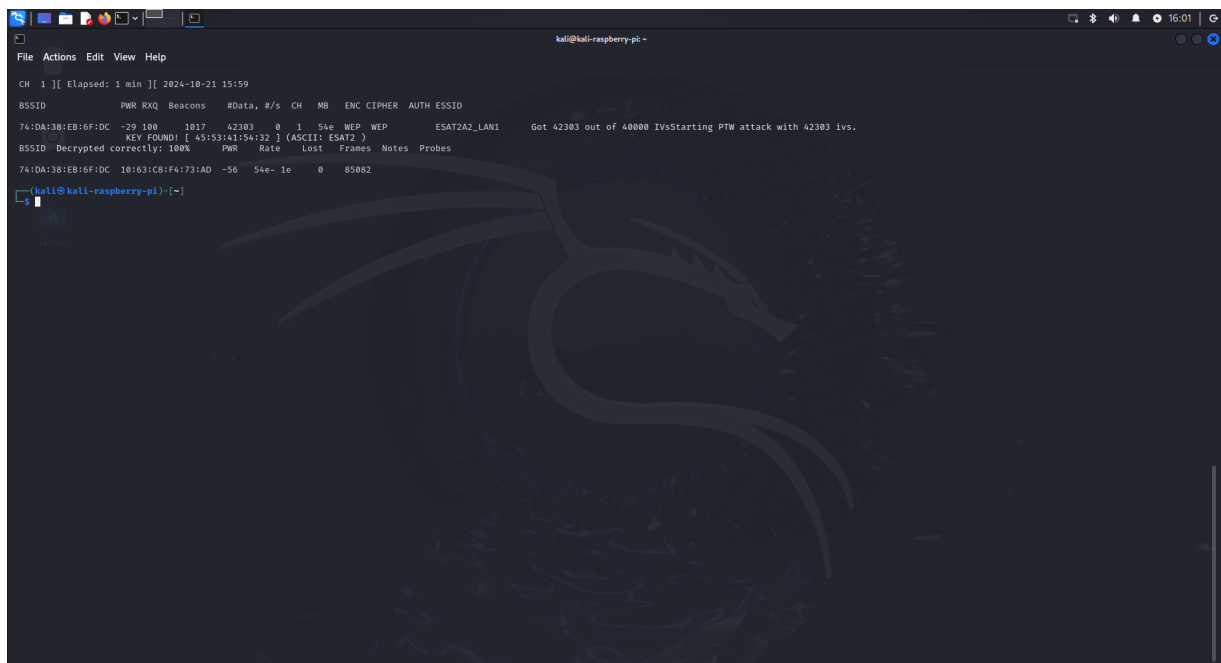
The main goal of the attack is to capture lots of packets sent on the WEP network in order to find cases of IV Collision. This process consists of a few steps. First, there is the matter of detecting the correct packets. Typically, a Raspberry Pi can only receive packets addressed to itself. This ~~problem~~ necessitates the use of the ~~"airmon-ng"~~ ~~airmon-ng~~ command. This command enables monitor mode on the Raspberry Pi, allowing it to listen to all packets in the air, thus enabling it to intercept WEP network traffic.

### 1.2.1 ~~airodump-ng~~

~~"airodump-ng"~~ captures the Now that the Raspberry Pi can detect traffic, ~~airodump-ng~~ is used to capture the data that the Raspberry Pi detects. By specifying a channel and BSSID, it ~~can be is~~ configured to exclusively capture data from ~~a specific network~~. This is how data from the WEP network is gathered. ~~the WEP-encrypted router~~. Aircrack will now capture all traffic on the network while keeping track of the IVs and the encrypted data.

### 1.2.1 ~~aircrack-ng~~

This command makes use of the weakness of WEP encryption. Once a sufficient amount of packets have been captured by ~~"airodump-ng"~~, ~~"aircrack-ng"~~ ~~airodump-ng~~, ~~aircrack-ng~~ is employed to crack the WEP key. This command makes use of the weaknesses of WEP encryption detailed in 2.1.1. Using packets with a shared IV, ~~Aircrack-ng~~ ~~aircrack-ng~~ utilizes cryptanalysis to determine the WEP key. A more detailed explanation of the RC4 algorithm can be found in Section 2.2.



```
kali@kali-raspberry-pi-~  
File Actions Edit View Help  
CH 1 ][ Elapsed: 1 min ][ 2024-10-21 15:59  
BSSID PWR RXQ Beacons #Data, #/s Ch MB ENC CIPHER AUTH ESSID  
74:DA:3B:EB:6F:DC -29 100 1037 42303 0 1 Sae WEP WEP ESAT2A2_LAN1 Got 42303 out of 40000 IVsStarting PTW attack with 42303 ivs.  
KEY FOUND! [ 45:53:41:54:32 ] (ASCII: ESA72 )  
BSSID Decrypted correctly: 100% PWR Rate Lost Frames Notes Probes  
74:DA:3B:EB:6F:DC 10:63:CB:FA:73:AD -56 54e- 1e 0 85002  
kali@kali-raspberry-pi-~
```

Figure 2: A WEP key that has been found by Aircrack

## 2 Aircrack

The first step in the project is acquiring the WEP key, as it is a key component for all the following steps. Aircrack-ng is used to find this key. Aircrack-ng, further referred to as Aircrack, is a suite of network security tools used for monitoring, attacking, and cracking WEP and WPA encrypted networks [Devine, 2022]. It is commonly used to assess network security. In this project, Aircrack will acquire the WEP key using flaws of the WEP-encryption algorithm.

### 2.1 Cracking the WEP access point

WEP encryption uses a combination of a shared key and a Initialization Vector (IV) to encrypt network traffic. However, due to the weak IV implementation, it is possible to recover the shared key after capturing enough packets. Aircrack exploits this vulnerability by analyzing captured data and IVs to reconstruct the WEP key.

#### 2.1.1 Structure of a WEP-encrypted packet

The inherent vulnerability of WEP encryption lies in its packet structure. To encrypt a packet, a key is used, which consists of:

- A 24-bit Initialization Vector (IV)
- A WEP key consisting of either 40 bits (for 64-bit encryption) or 104 bits (for 128-bit encryption)

This key is used in an RC4 algorithm to encrypt the packet. However, as the IV is randomly generated for every packet, this causes a problem for the receiver. To enable decryption, the IV is appended to the front of the encrypted packet. This feature is the core weakness of WEP encryption, as it creates two critical vulnerabilities:

1. The IV's limited size (24 bits) leads to the inevitable reuse
2. The transmission of the IV enables attackers to collect and analyze IV patterns

When two packets share the same IV, also known as IV Collision [Barken, 2003], cryptanalysis can be used to determine the static WEP key, allowing for all subsequent packets to be decrypted.

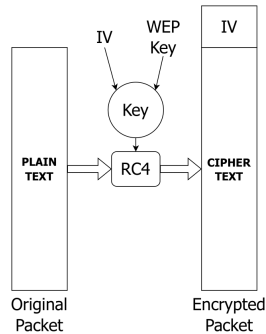


Figure 3: The structure of a WEP-encrypted packet

### 2.2 Executing the attack

Aircrack consists of several tools, each performing a specific function in WEP password cracking. The following paragraphs aim to provide a high-level overview of the attack and the commands used during it. This attack largely follows the one detailed in [darkAudax, 2010]. The specific commands used are detailed in Appendix 7.1.

The main goal of the attack is to capture lots of packets sent on the WEP network in order to find cases of IV Collision. This process consists of a few steps. First, there is the matter of detecting the correct packets. Typically, a Raspberry Pi can only receive packets addressed to itself. This problem necessitates the use of the *airmon-ng* command. This command enables monitor mode on the Raspberry Pi, allowing it to listen to all packets in the air, thus enabling it to intercept WEP network traffic.

Now that the Raspberry Pi can detect traffic, *airodump-ng* is used to capture the data that the Raspberry Pi detects. By specifying a channel and BSSID, it is configured to exclusively capture data from the WEP-encrypted router. Aircrack will now capture all traffic on the network while keeping track of the IVs and the encrypted data.

Once a sufficient amount of packets have been captured by *airodump-ng*, *aircrack-ng* is employed to crack the WEP key. This command makes use of the weaknesses of WEP encryption detailed in 2.1.1. Using packets with a shared IV, *aircrack-ng* utilizes cryptanalysis to determine the WEP key. A more detailed explanation of the RC4 algorithm can be found in Section 2.2.

```

kali@kali-raspberry-pi- ~
File Actions Edit View Help
CH 1 ][ Elapsed: 1 min ][ 2024-10-21 15:59
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
74:DA:38:EB:6F:DC -29 100 1017 42303 0 1 54e WEP WEP ESAT2A2_LAN1 Got 42303 out of 40000 IVsStarting PTW attack with 42303 ivs.
KEY FOUND! [ 45:53:41:54:32 ] (ASCII: ESAT2 )
BSSID Decrypted correctly: 100% PWR Rate Lost Frames Notes Probes
74:DA:38:EB:6F:DC 10:63:C8:FA:73:AD -56 54e 1e 0 85082
kali@kali-raspberry-pi- (~)
$

```

Figure 4: A WEP key that has been found by Aircrack

## References

- [Barken, 2003] Barken, L. (December 23, 2003). Wep vulnerabilities—wired equivalent privacy? <https://www.informit.com/articles/article.aspx?p=102230&seqNum=6>. [Online; accessed 14-October-2024].
- [darkAudax, 2010] darkAudax (January 11, 2010). Tutorial: Simple wep crack. [https://www.aircrack-ng.org/doku.php?id=simple\\_wep\\_crack](https://www.aircrack-ng.org/doku.php?id=simple_wep_crack).
- [Devine, 2022] Devine, C. (May 10, 2022). Aircrack-ng. <https://www.aircrack-ng.org/>.