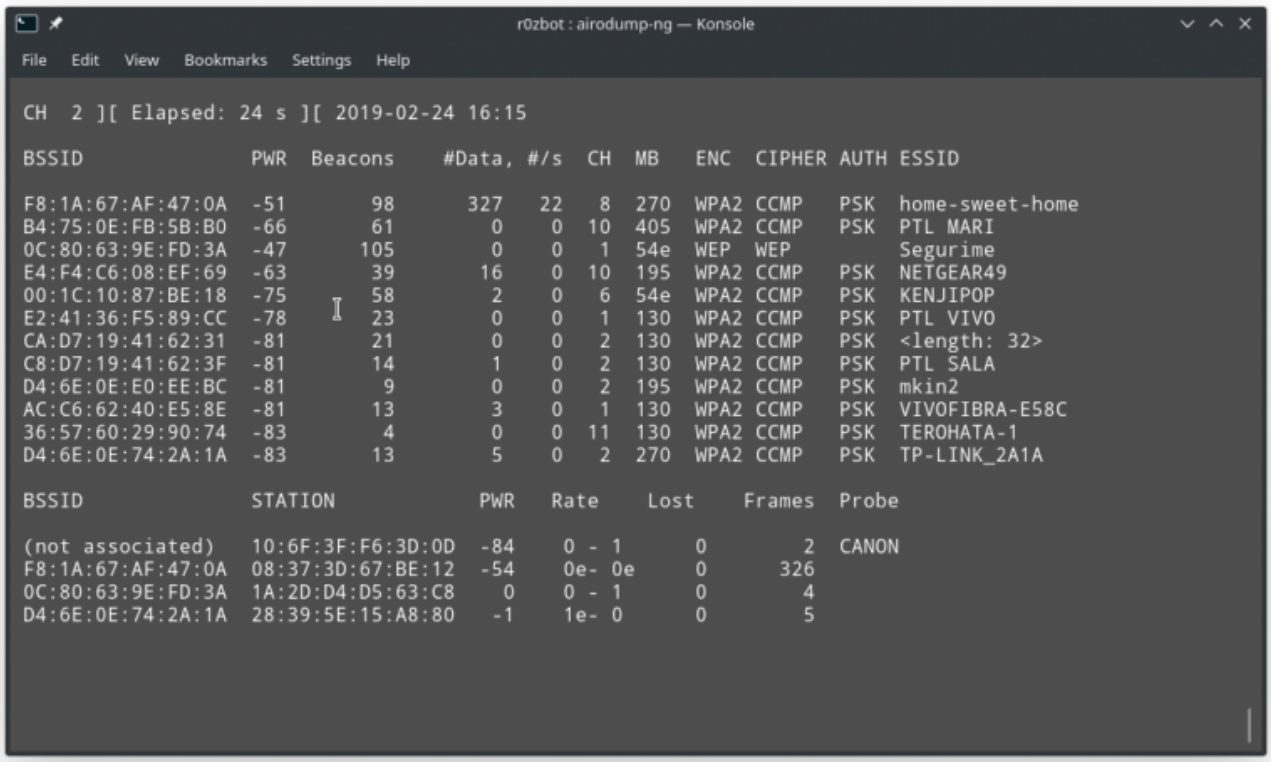
Crackeando WEP

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.

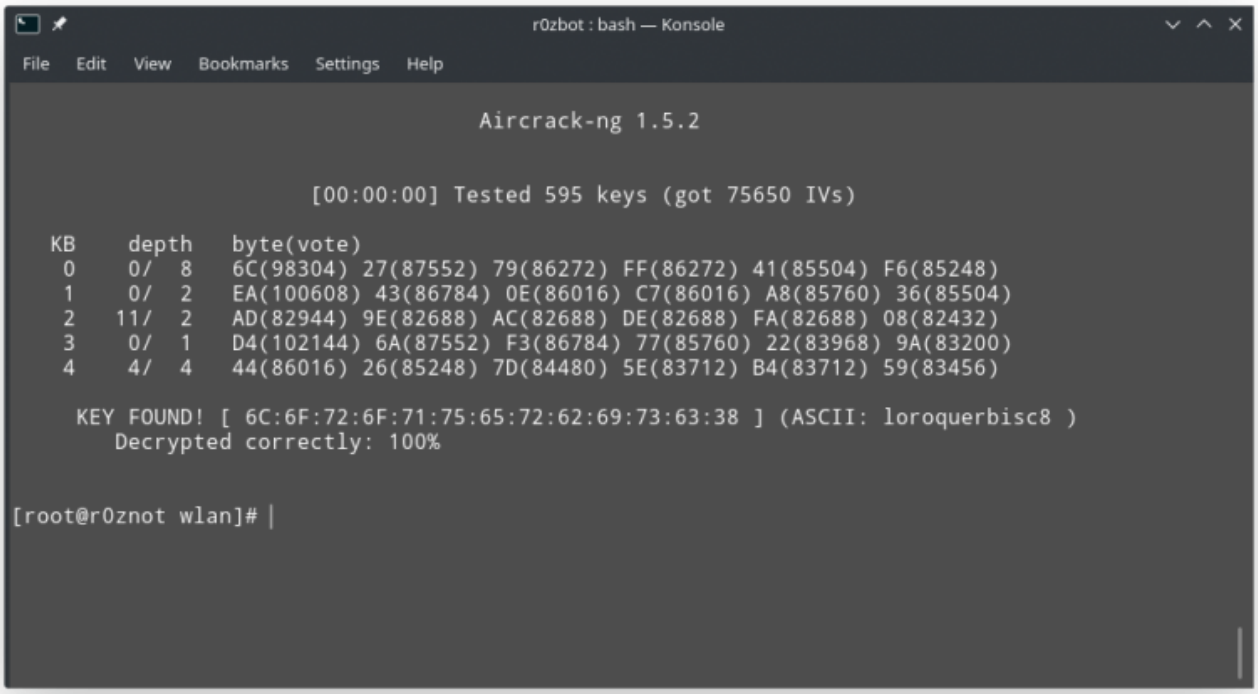


Você pode simplesmente esperar que o tráfego natural da rede gere-os pra você, ou você pode injetar pacotes na rede para aumentar a velocidade da coleção de pacotes de dados.

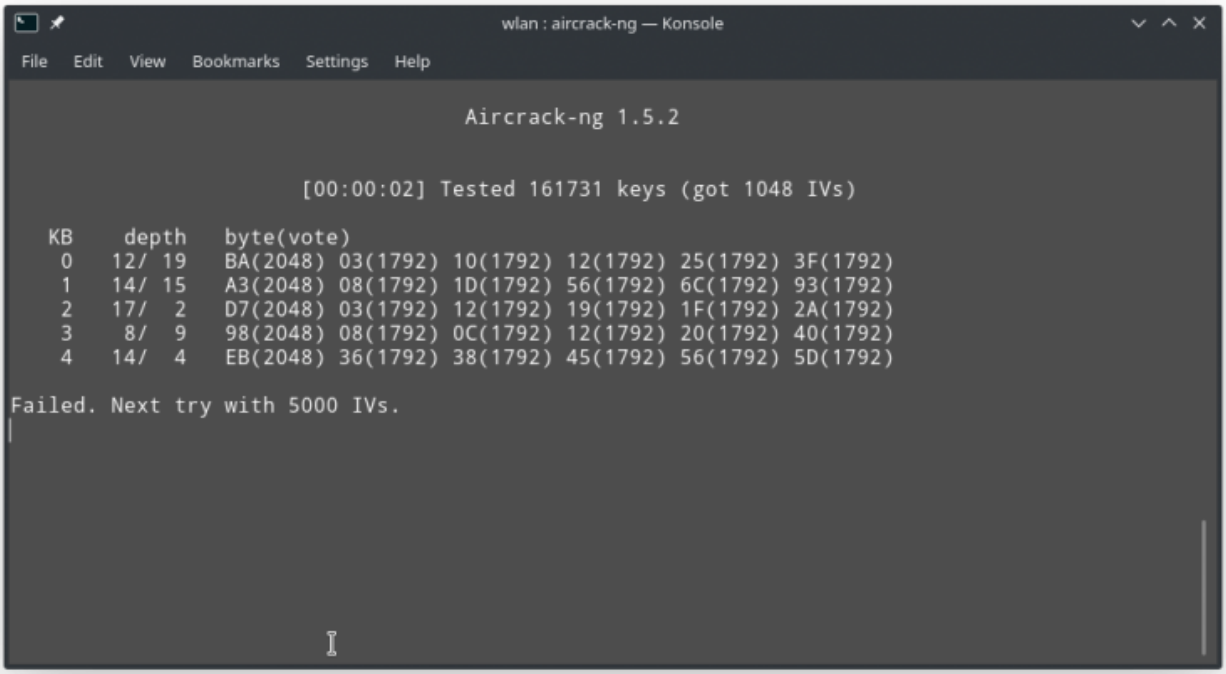
Quebrando a chave

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`

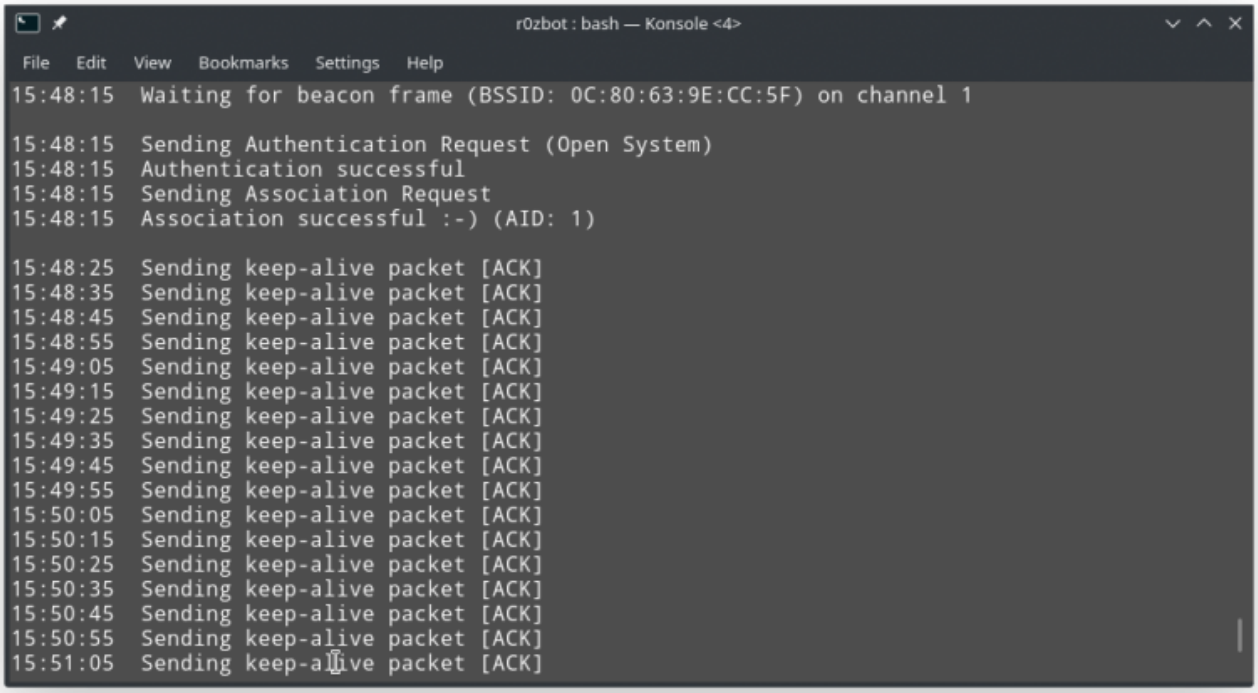
Note que os argumentos entre chaves devem ser substituidos pelos seus valores, então o comando acima fica assim no nosso exemplo:
`aireplay-ng -9 -e Segurime -a 0C:80:63:9E:FD:3A wlp8s0`

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.

Revision #2

Created Sun, Feb 24, 2019 6:21 PM by Daniel

Updated Tue, Feb 26, 2019 2:27 PM by Daniel