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

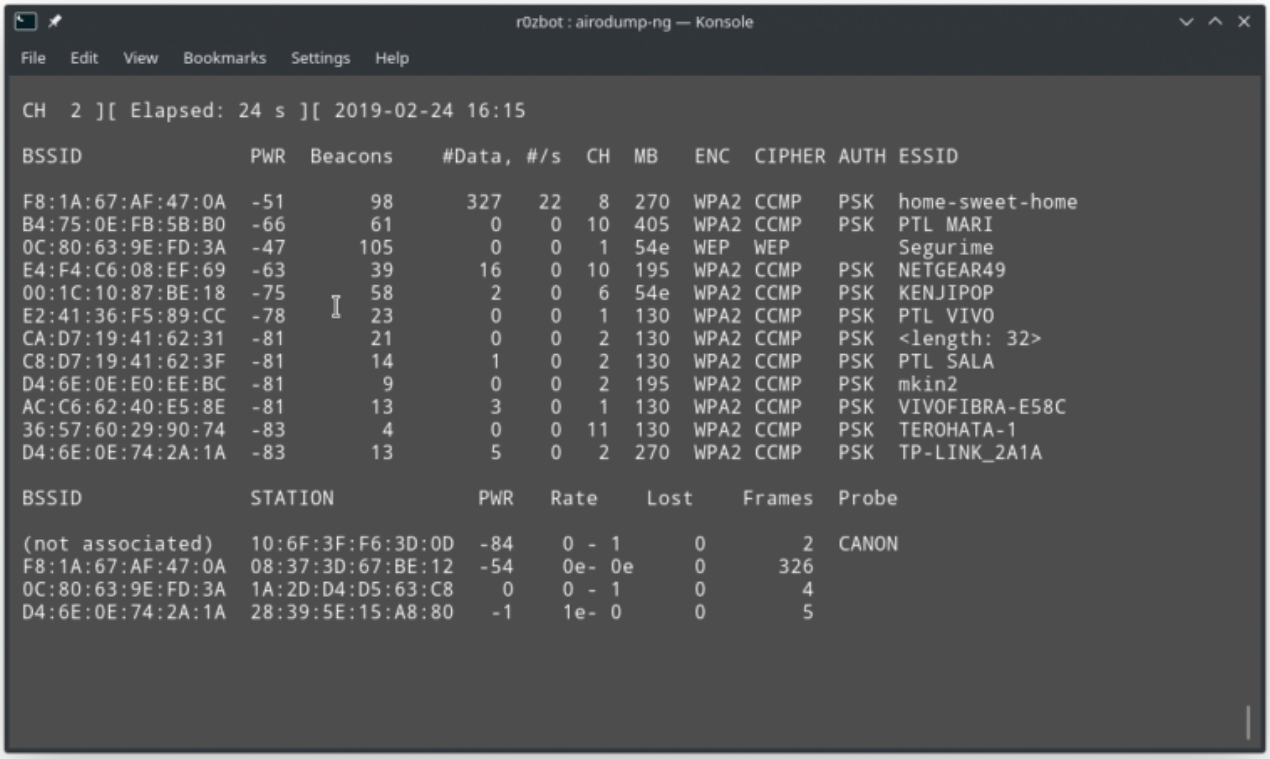
Em seguida, você vai precisar colocar sua placa de rede no modo monitor. (o `airodump-ng` que vamos ver mais pra frente faz isso pra você, mas só se tudo ja estiver certo). Use o comando `iwconfig` para visualizar quais são as interfaces de rede Wi-Fi disponíveis no seu computador. Anote o nome dela,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

Revision #12
Created Sun, Feb 24, 2019 6:21 PM by Daniel
Updated Sat, Mar 2, 2019 12:02 AM by Daniel