hackeando WiFi

como roubar um
sinal de internet sem fio

Não parece totalmente ineficiente e dispendioso que cada pessoa que usa internet tenha que possuir seu próprio modem, roteador e contrato com um provedor? Não parece ridículo que cada pessoa pense que o acesso à internet é um privilégio seu, sendo que a web é uma criação coletiva, dinâmica e participativa?

A maioria trata a internet como sua, como um bem privado que tem que ser defendido contra hackers malvadxs e todo tipo de malware que diminua a velocidade da conexão.

Não é apenas ridículo, mas também um pensamento burro, pois não há muita proteção nisto. As informações que as pessoas tentam esconder, na verdade, são dadas espontaneamente quando elas acessam sites, alimentam redes sociais, usam e-mail de coorporações privadas, falam ao telefone, compram com cartão de crédito, etc.

A internet é uma via. E como todas as vias, sua melhor característica é estar livre. Então libere sua conexão, convide as pessoas a usá-la, compartilhe seu sinal!

Por fim, se queres proteção, pesquisa o que realmente faz diferença (GPG, TOR, *V*PN, sei lá) e tenha clareza de que o seu principal inimigo não é x vizinhx e sim o GO*V*ERNO!

Em 2006, a empresa dona da marca WiFi desenvolveu um protocolo para facilitar a configuração da rede sem fio para usuárixs comuns, chamado WiFi Protected Setup (WPS). Dizem que o WPS é bem vulnerável a ataques de força bruta, mas não é esse o nosso interesse agora. O que nos importa é que a maioria dos roteadores vem configurada de fábrica com um método de autenticação chamado Pre-Shared Key (PSK). Este método se mostrou incrivelmente falho e, em dezembro de 2011, um grupo de hackers desenvolveu o Reaver, um software de código aberto para recuperar o PIN do roteador e com isso obter sua senha.

Então é isso o que nós vamos fazer aqui: preparar nosso adaptador de rede para monitoramento de sinal, reconhecer um roteador perto o suficiente para conectarmos a ele, rodar o Reaver durante algumas horas e conseguir a senha!

O que a gente vai precisar:

* Uma distribuição LINUX
* Um adaptador de rede
* Aircrack-ng
* Reaver
* entre 4 a 10 horas

Caso alguém coloque senha na sua internet sem fio (o que não muda nada para a espionagem que o governo faz sobre nós), existe comumente 3 modos de encriptação: WEP, WPA, WPA2. É fácil encontrar tutoriais explicando como hackear a WEP, o que é bom saber, pois tem vários lugares que ainda usam, como no México.

No caso do Brasil, a imensa maioria dos roteadores já vem configurada com encriptação WPA2, que é a mais foda. Antigamente (há uns 2 anos) era muito difícil (pra mim foi impossível) quebrar esse padrão, então fiquei muito decepcionado, até descobrirem aquele problema do PIN. Agora podemos nos conectar em diversos roteadores, despistar nosso sinal, abrir as redes, ou até mesmo conseguir algum tipo de informação sensível na rede de alguma empresa ou prefeitura lazarenta.

A primeira coisa que tu precisa é uma distribuição LINUX, qualquer uma. Se não quiseres instalar, basta baixar a imagem (.ISO), por exemplo, do Debian, queimar num CD ou colocar num pendrive e usá-lo no modo Live. Caso tu use apenas window$ ou mac, sinto muito.

Uma vez no ambiente Linux, baixe e instale os programas:
- Aircrack-ng: www.aircrack-ng.org
(algumas distros já vêm com aircrack-ng instalado)
- Reaver: code.google.com/p/reaver-wps/

Caso tenhas dificuldades nas instalações, procure a solução em algum fórum.

Uma vez no ambiente Linux, acesse o terminal. Ative a função de SuperUsuárix com o comando:

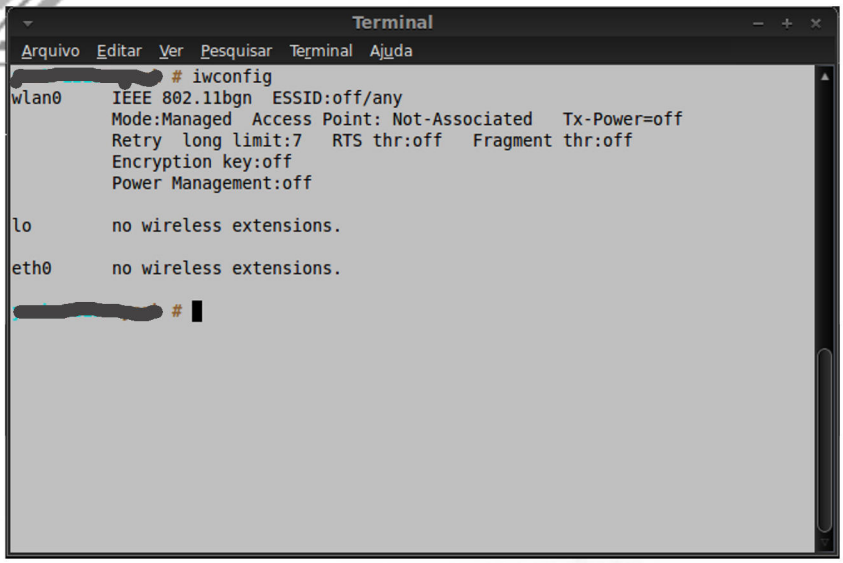
> su

em seguida, coloque a tua senha. Agora já podes executar comandos de administração. Verifique qual o nome do teu adaptador de rede sem fio:

> iwconfig

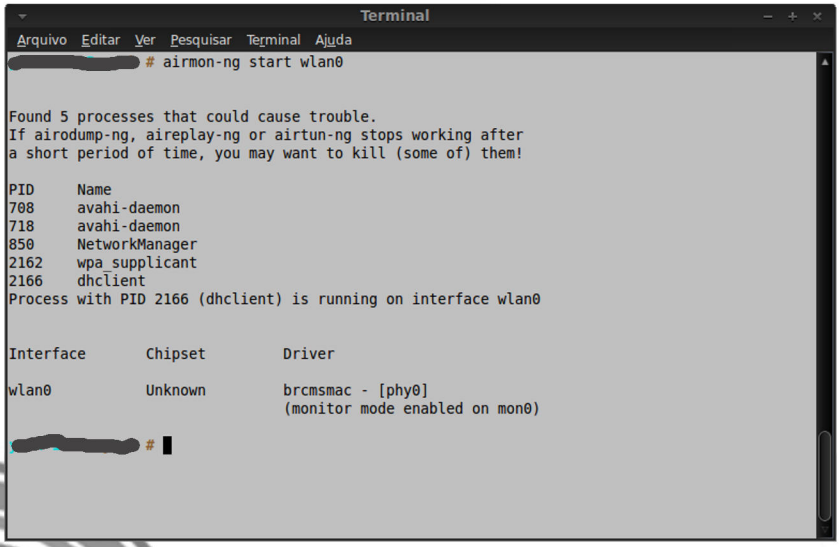
Geralmente está com nome "wlan0" e será aquele dispositivo com alguma descrição (o nome eth0 é para rede cabeada).

Veja a imagem da página 4



Tendo identificado o adaptador de rede sem fio, vamos colocá-lo no modo de "Monitoramento":

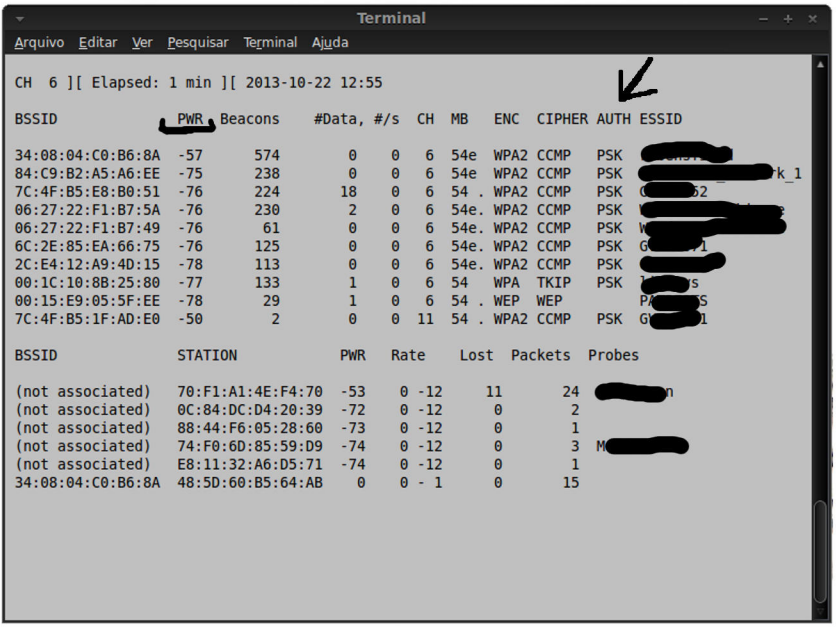
> airmon-ng start wlan0



Agora, dê uma olhada em todos os sinais que chegam até o teu computador com o comando:

> airodump-ng mon0

Se tu tais num centro urbano ou num condomínio, poderão ser dezenas de roteadores emitindo sinal de rádio (eita desperdício!). Temos que buscar aquele com maior potência (coluna PWR: quanto menor, melhor) e com modo de autenticação (coluna AUTH) tipo PSK.



Depois de um tempo, pare o monitoramento apertando ctrl+C. Geralmente, o primeiro sinal da lista costuma ser o melhor para hackear.

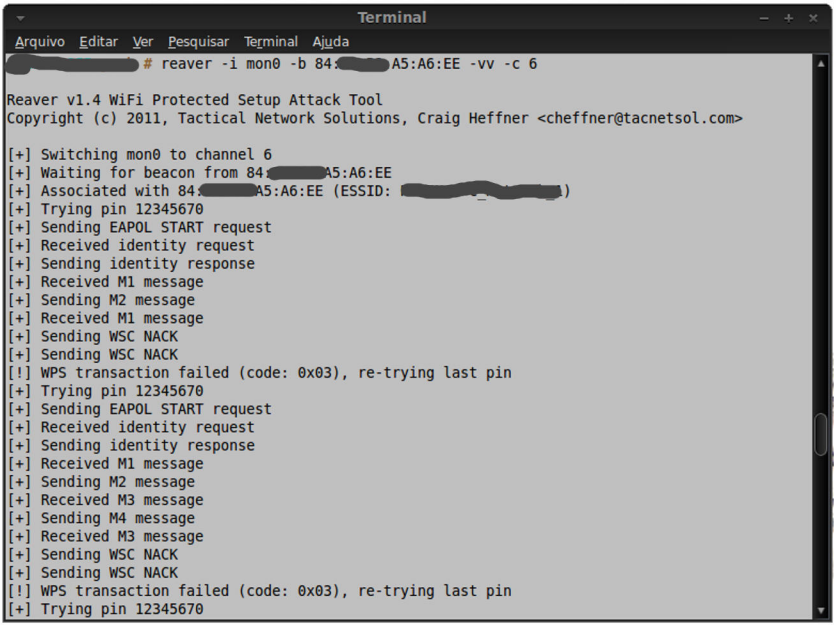
Anote o número BSSID e vamos rodar o Reaver.

O que o reaver faz é um ataque de força bruta refinado, tentando encontrar o PIN do roteador. Não sei como ele consegue recuperar a própria senha depois, mas funciona! Às vezes, mesmo com um sinal bom, a coisa não anda. Então, tenta o segundo da lista e por aí vai, até dar certo.

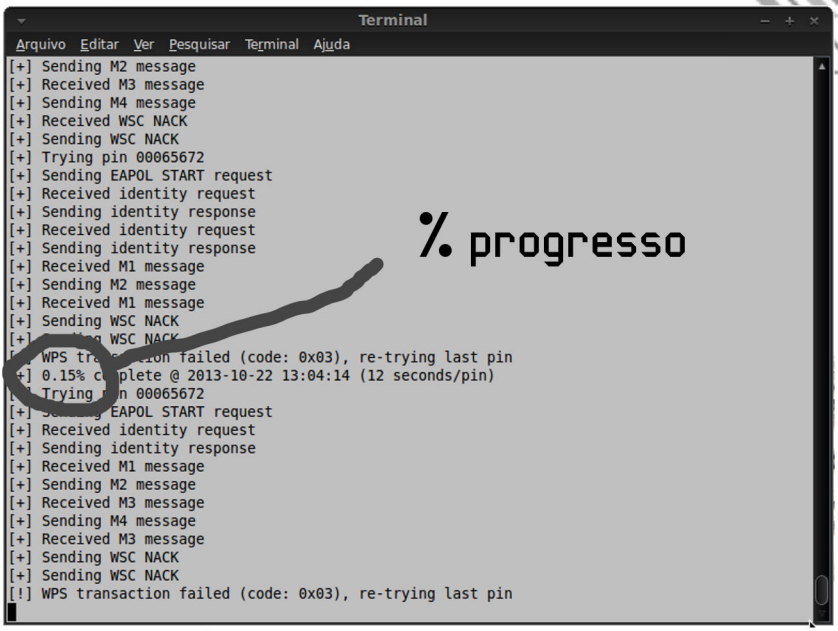
Execute o seguinte comando para começar:

>reaver -i mon0 -b BSSID -vv -c canal

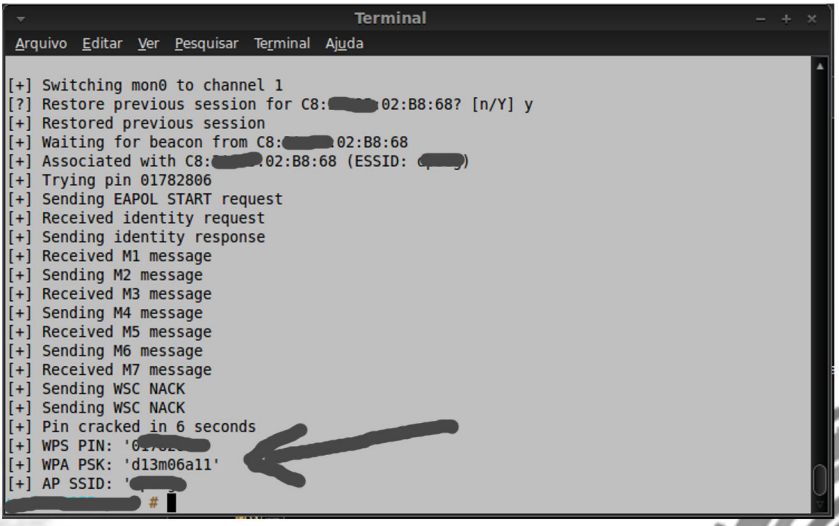
(BSSID é o endereço de MAC do roteador. Troque _BSSID_ pelo "número" que está na primeira coluna da lista e _canal_ pelo número da coluna CH correspondente)

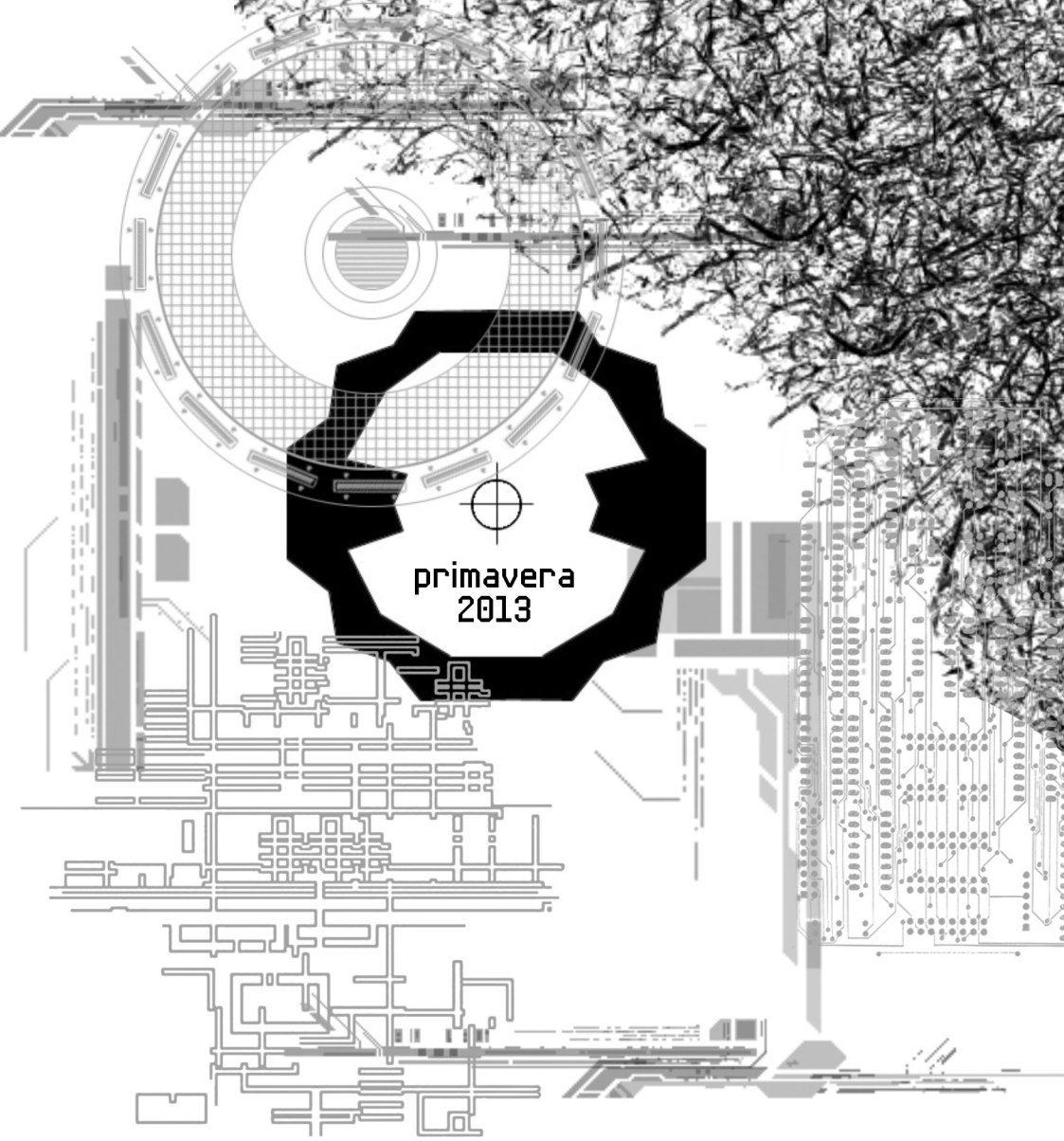


O programa vai começar a testar os PINs e é só aguardar entre 4 a 10 horas. De vez em quando vai aparecer um indicador em porcentagem mostrando o progresso. Caso precises parar, o Reaver salva até onde ele foi e depois continua a partir dali.



Ao final, teremos a senha:





Mais links:

- http://lifehacker.com/5873407/how-to-crack-a-wi+fi-networks-wpa-password-with-reaver
- http://www.tacnetsol.com/reaver/
- http://lifehacker.com/5305094/how-to-crack-a-wi+fi-networks-wep-password-with-backtrack
- www.wireshark.org
- www.backtrack-linux.org/