Android Hacking: Explorando redes WiFi com zANTI

21 DE AGOSTO DE 2015

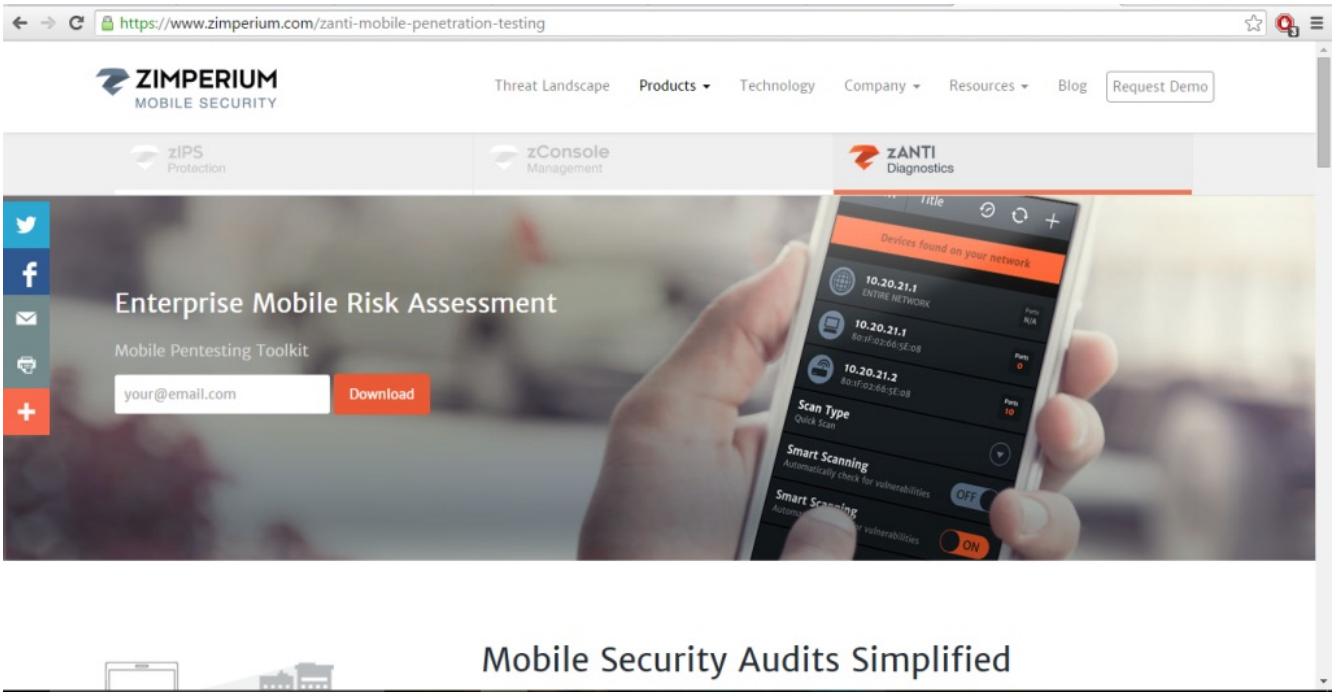
Todos nós estamos acostumados a usar ferramentas sofisticadas para pegar logins e senhas em redes WiFi que só poderiam ser usadas em computadores potentes e com sistemas feitos para isso. E se a partir de um simples celular você tivesse acesso a ferramentas tão poderosas quanto? Isso é possível. E vamos aprender a usar uma delas agora.

Pré-requisito

O único requisito é o celular ter ROOT (permissões de super usuário).

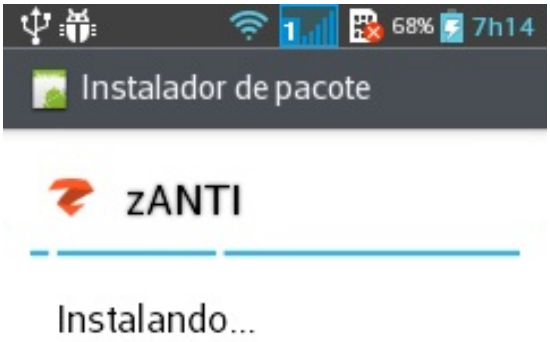
Vamos lá

Para começarmos, vamos baixar o zANTI que vai ser a ferramenta que usaremos hoje. Eu vou baixar no meu computador e passar para o celular. Esse é o site zANTI. Para baixar você vai ter que colocar seu email e clicar em download para receber o link de download em sua caixa de entrada.



Após baixar o zANTI, passe para o seu celular. E instale como se fosse um aplicativo qualquer.

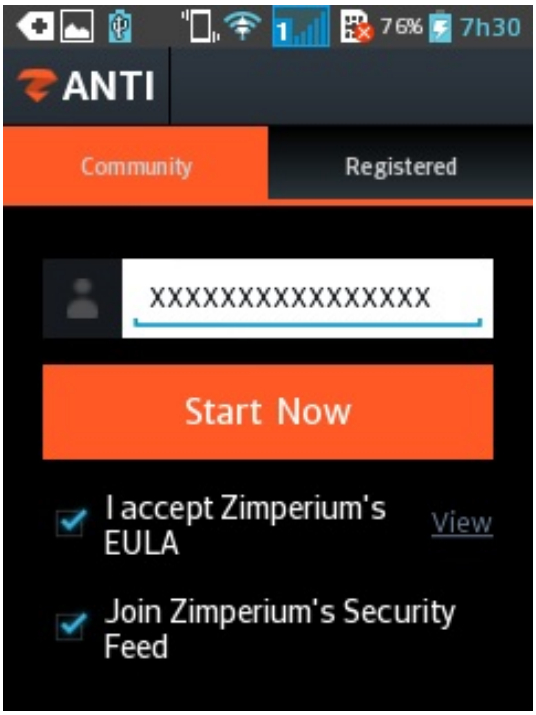
(quando eu disse que o celular podia ser simples eu estava falando sério).
Bem, agora é só clicar em instalar e esperar.



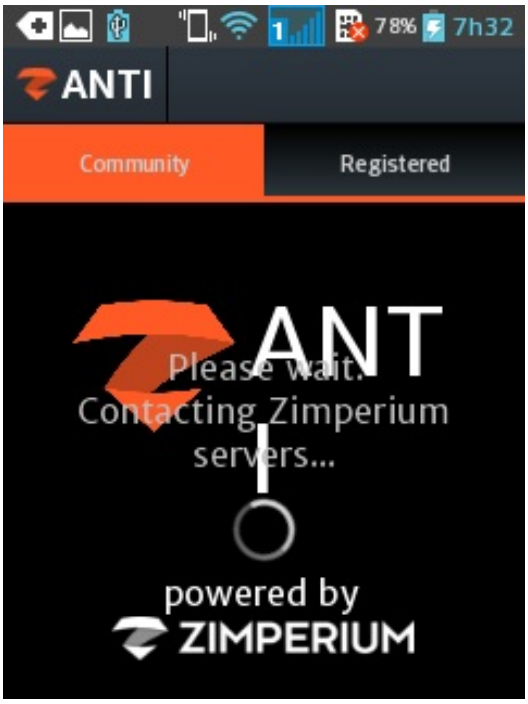
Após instalar, volte para a tela inicial do seu celular e inicie o zANTI. Aqui eu vou arrasta-lo para a tela inicial.

Agora vamos executa-lo.

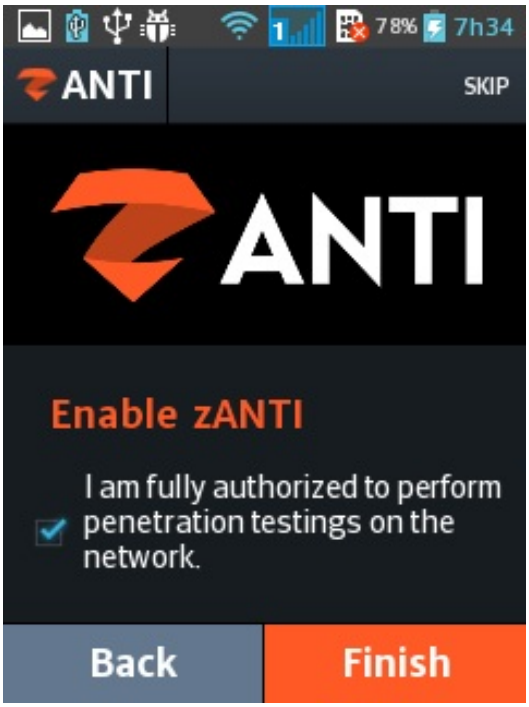
Aqui vamos permitir o acesso ROOT para o aplicativo.



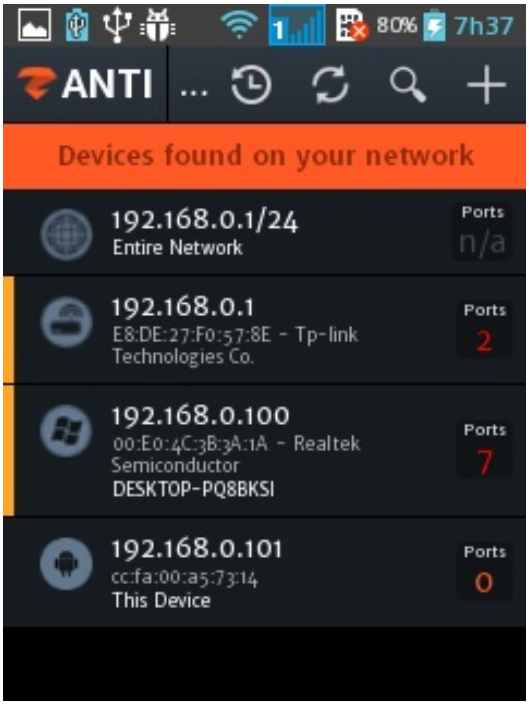
Marque as duas caixinhas e coloque xxxxxxxxx no campo acima e clique em Start Now.



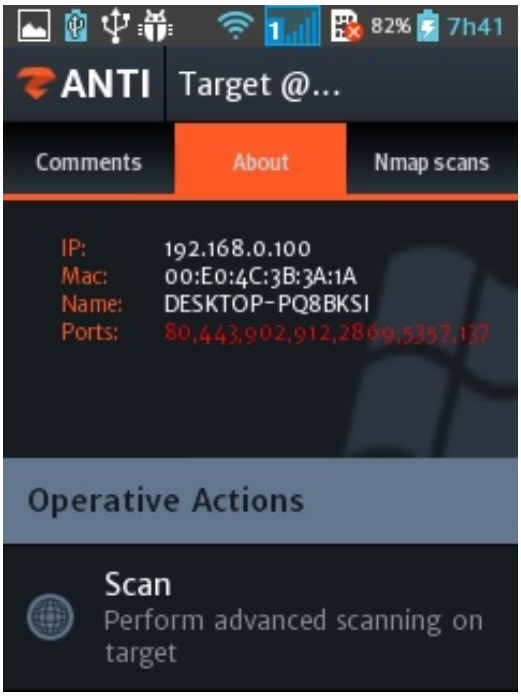
Apenas espere ele conectar aos servidores.



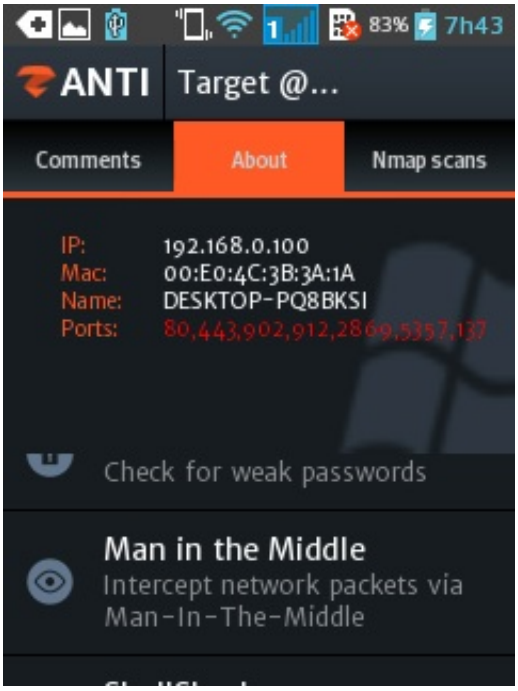
Marque a opção e clique em Finalizar.



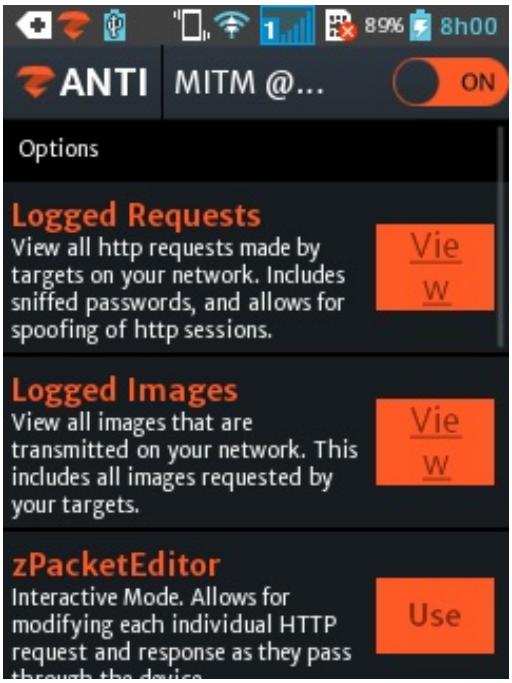
Aqui podemos ver que ele escaneou minha rede e me deu todos os dispositivos nela conectados. Podem ver que ele listou meu computador host, meu roteador e o celular android. Ele também lista as portas neles, vou explorar meu host, apenas clicando nele.



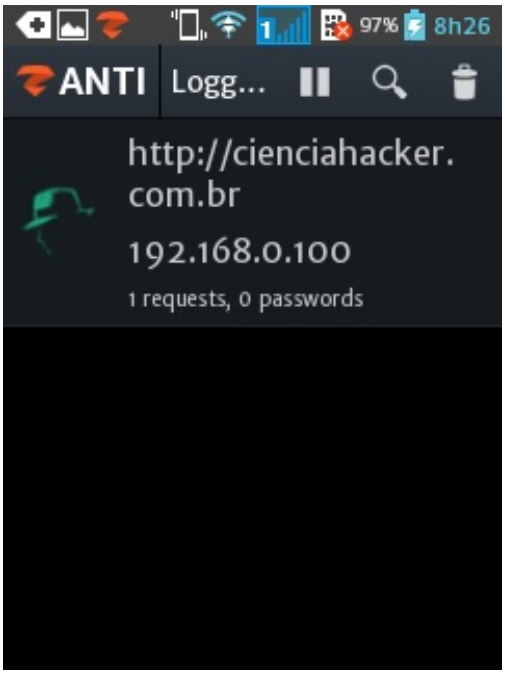
Veja que tenho várias portas abertas, eu poderia explora-las mas vou mostrar um ataque mais *interessante.* Em Operative Actions vá descendo até achar a opção Man in the Middle.



Selecione e veremos várias opções. Ative o MITM para usa-las

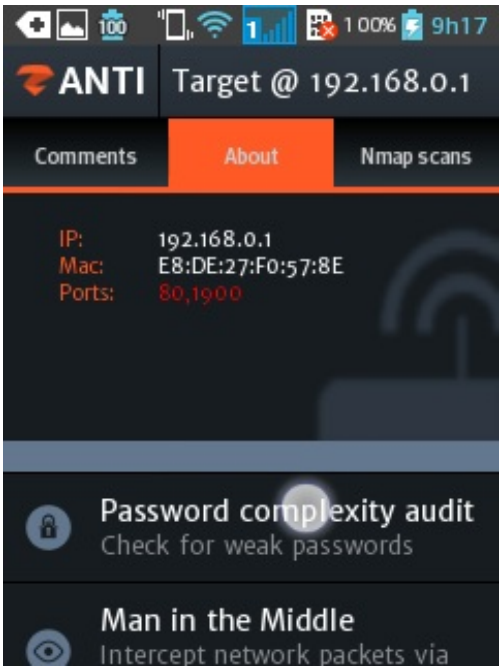


Aqui inicia-se a diversão. Só na primeira opção temos um sniffer muito bom, para testa-lo vou entrar em algum site qualquer no meu host ‘computador’.

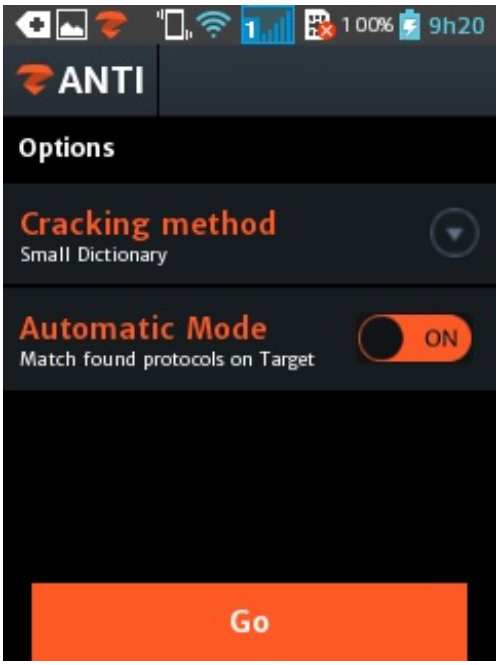


Como vocês podem ver ele pegou que estou mexendo no site do CH. Caso eu tivesse feito algum login e colocado senha iria me retornar as senhas digitadas.

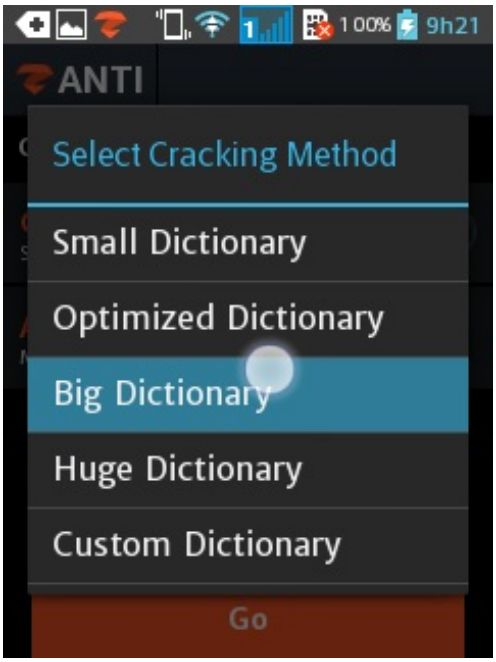
Outra ferramenta muito boa é a de quebra de senhas. Como visto anteriormente ele listou meu roteador e todo roteador tem um painel de configuração onde é configurada a senha e configurações da rede. Mas nem sempre o login e senhas são admin:admin, então essa ferramenta é extremamente útil. *Lembrando que não recomendo em hipótese alguma fazer isso em redes em que você não tem permissão.* Volte para o painel que lista os dispositivos e selecione o roteador.



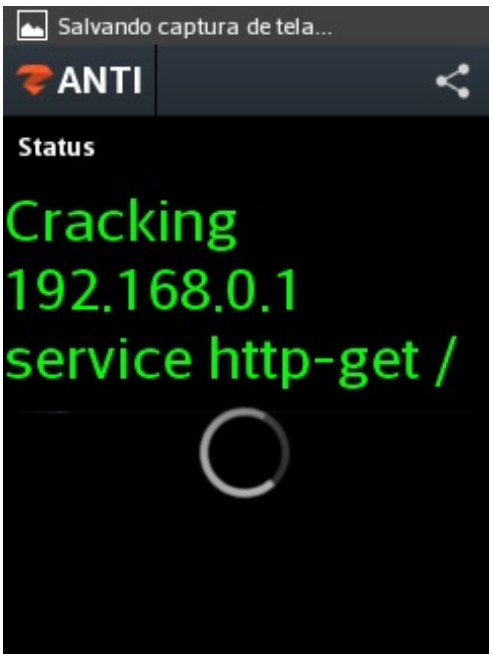
Selecione a opção mostrada na imagem.



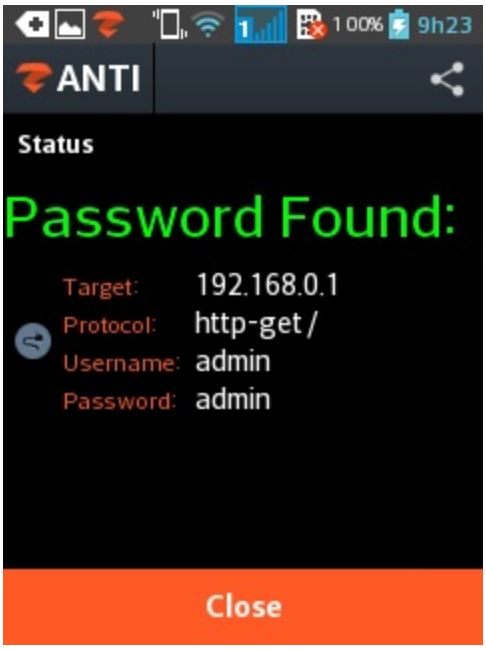
Clique na primeira opção.



Aqui vamos selecionar um grande dicionário. Após isso apenas de Go.



Ele está quebrando a senha e em alguns segundos me deu o resultado.



Claro a minha senha esta no padrão, mas se fosse outras senhas padrões que variam de acordo com a marca do roteador ele iria encontrar na mesma velocidade. Agora apenas digite no navegador do celular o IP do roteador e o usuário e senha adquiridos.

Existem várias ferramentas ótimas dentro do zANTI, mas se fosse mostrar todas iria ficar muito extenso. Por isso vou ficando por aqui espero que tenham gostado e até mais!

Cyber Segurança / Espionagem, Segurança da Informação

ANDROID HACKING DICIONÁRIO ESPIONAR QUEBRAR SENHAS SUPER USUÁRIO WIFI

,,