Hackers – As 7 ferramentas mais usadas por eles em toda a rede

David CHC

5 Min de leitura

1 Comentário

Cansado de ver por aí postagens falando coisas do tipo “As 10 músicas mais tocadas”, “Os 10 filmes do ano” ou “Os 10 cachorros mais feios do mundo”, resolvi inovar e trazer pra vocês “**As 7 ferramentas mais usadas pelos Hackers**”.

A ordem não representa necessariamente uma relação de importância entre as ferramentas. Procurei colocá-las em uma disposição lógica, dentro das possibilidades. E, como gosto sempre de deixar as coisas bem claras, para os que ainda tem dúvidas a respeito do termo Hacker e suas atribuições, recomendo a leitura do artigo Vamos Falar Sobre Hacking.

#1 – Google para Hackers

A primeira da lista talvez possa causar surpresa em alguns. Sim, o buscador do Google é **uma das principais ferramentas usadas pelos Hackers**.

Durante o processo de Hacking (ou Pentesting) passamos pela etapa de reconhecimento que objetiva coletar o máximo possível de informações a respeito de nosso alvo. Em face disso, não existe nada melhor do que contar com uma mãozinha do buscador na hora de obter informações.

É claro que as pesquisas realizadas não costumam ser muito triviais; fazemos uso das diretivas que o google oferece para realizar as buscas de uma maneira bem perspicaz.

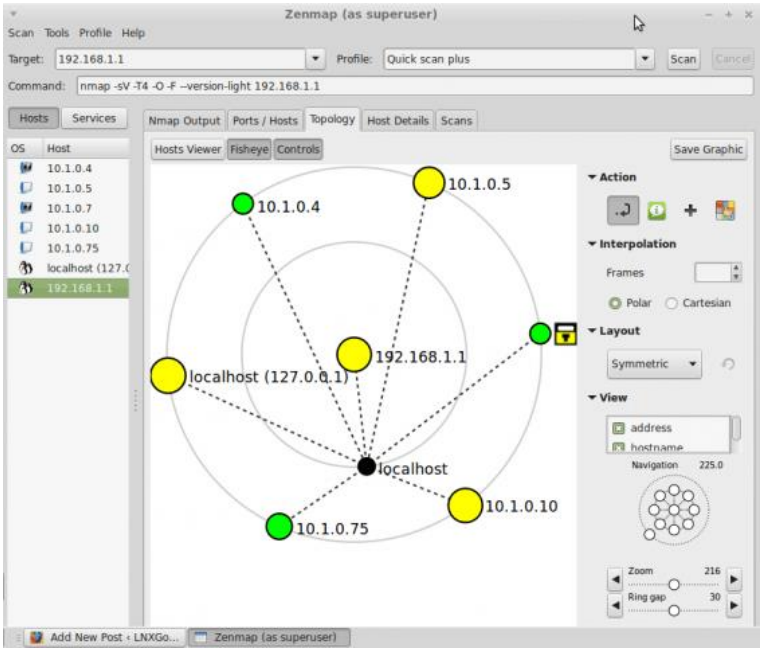
Falo sobre o Google Hacking no curso Hacking Sem Segredos.

#2 – Nmap/Zenmap

Um mapa do tesouro nos mostra o caminho para a fonte da riqueza. O Nmap, o Mapeador de Redes, nos permite criar um mapa de nossa rede a fim de compreender como os nós da rede estão interligados além de nos permitir encontrar as fragilidades dela – o tesouro do Hacker.

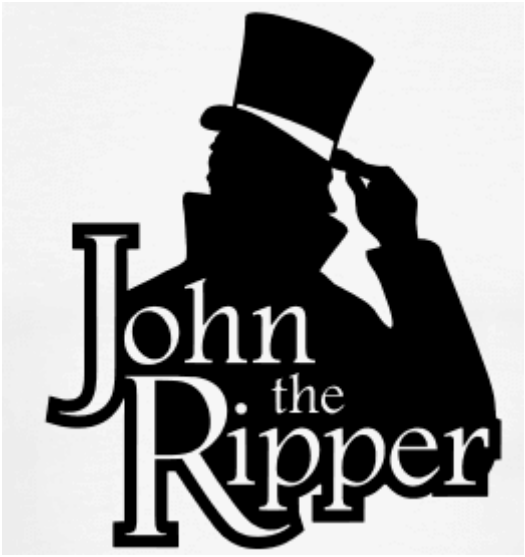
O Nmap é uma ferramenta em modo terminal e possui uma versão em janelas, chamada de Zenmap que, em essência, são a mesma coisa. Mostro como instalar no artigo Tutorial: Instalando o Nmap e o Zenmap.

Em outros artigos eu ensino como dar os Primeiros Passos com o Nmap e Como Mapear redes com o Zenmap. Para um conhecimento mais profundo recomendo o Curso de Nmap ou o Curso de Zenmap.



Zenmap

#3 – John the Ripper



Pensou em quebra de senhas, pensou em John the Ripper. Essa ferramenta é simplesmente fenomenal. **Nos permite realizar a quebra de diversos tipos de hashes de senha seja por força bruta ou por ataques baseado em dicionários.**

Mostro como quebrar senhas Linux, Windows e de arquivos zip, rar, libreoffice, pdf etc. no Curso Password Hacking.

#4 – Metasploit/Armitage

Tenho certeza que a parte mais empolgante em um Pentest é quando conseguimos obter acesso remoto ao alvo. A partir de então, assumimos o controle do host invadido. **É possível executar programas, fazer upload de arquivos, visualizar o que o alvo está fazendo, tirar o controle do alvo** e etc. Embora isso seja bem divertido, não é uma prática comum para o profissional do Hacking Ético :).

Nessas horas, contamos com a imensa ajuda do Metasploit. Mas há quem prefira o Armitage, uma versão gráfica para a mesma ferramenta.

Falo sobre o Metasploit e o Armitage no Curso Hacking Sem Segredos.

#5 – Setoolkit

Quando tudo está difícil ou quando não parece haver uma solução, eis que surge uma luz no fim do túnel.

Há quem imagine que todo o processo de Hacking se dá somente pela força das ferramentas. Em parte isso é verdade, mas como falei no artigo Engenharia Social: a arte de Hacker Pessoas **é necessário que o Hacker tenha habilidades para persuadir as pessoas envolvidas com seus alvos.**

Nem sempre encontramos vulnerabilidades no sistema alvo, o que nos força a apelar por técnicas contra as pessoas do alvo (a luz no fim do túnel). Nesse caso, a ferramenta Setoolkit cai como uma luva. Ela contém uma enxurrada de técnicas com ênfase no ataque a pessoas.

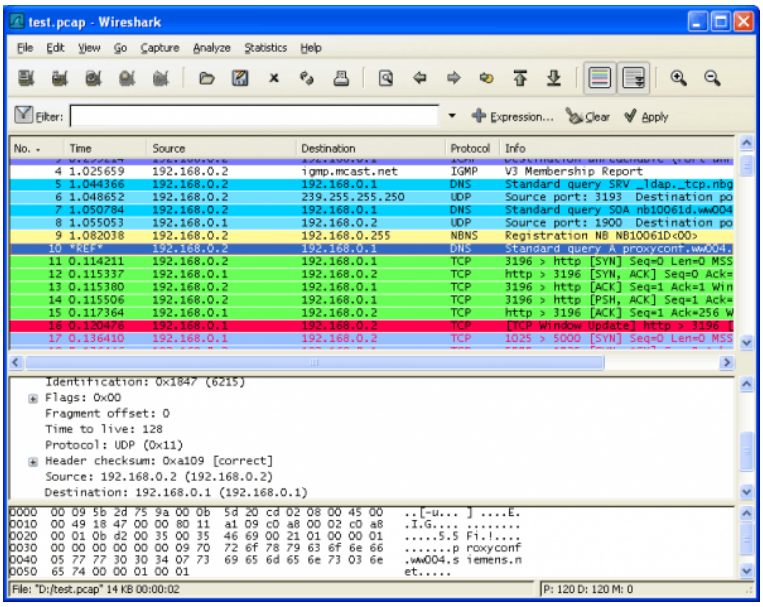
Disseco a ferramenta no Curso Social Hacking.

#6 – Wireshark

O Wireshark é uma daquelas ferramentas que assusta na primeira vez em que vamos usar. Muitos recursos e funcionalidades, além de ser necessário um conhecimento e uma boa bagagem de redes.

Esse é o mais famoso sniffer de rede da atualidade. **Com ele nos podemos capturar todos os pacotes que chegam até a nossa interface e analisarmos com detalhes**. No artigo Wireshark – Introdução e Tutorial de Instalação eu explico mais tecnicamente o que é a ferramenta e como você pode instalar em seu computador.

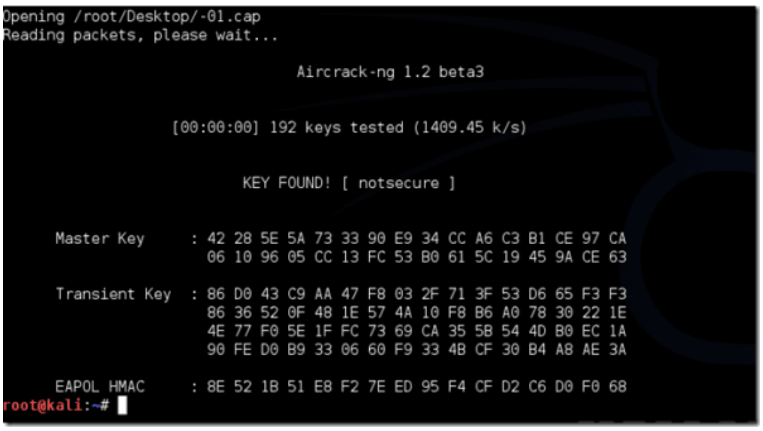
No Curso de Wireshark eu ensino tudo que você precisa saber sobre a ferramenta.



#7 – Aircrack-ng

Terminamos a lista da perfeição com a suíte Aircrack-ng, que na verdade é um pacote de ferramentas para quebra e análise de redes Wi-Fi. Esse kit **é usado direta ou indiretamente para a quebra de redes WEP e WPA/WAP2**. Talvez você até já tenha utilizado outra ferramenta, mas tenho quase certeza que o Aricrack-ng estava por trás dela.

Ensino tudo que você precisa saber no Curso Wi-Fi Hacking – Ataque à Infraestrutura e no Curso Wi-Fi Hacking – Ataque a Clientes.



Bônus – Kali

Eu disse que seriam 7 ferramentas, mas decidi trazer mais uma aqui de bônus pra você. A bem da verdade, o Kali não é exatamente uma ferramenta mas sim uma distro Linux contendo um arsenal que engloba um conjunto quase que ilimitado de ferramentas, inclusive as que citei acima.

O Kali figura a primeira posição entre as distros para Hacking e está ente as 15 distribuições mais baixadas segundo a fonte distrowath.com (no momento em que escrevo este artigo). **Um Hacker de verdade tem que ter um certo domínio sobre o Linux**; é praticamente um prerrequisito, motivo pelo qual decidi adicioná-la para a lista.

Abordo tudo que você precisa saber sobre o Kali no Curso de Kali Linux Fundamental. Se quiser uma ajudinha para dar o pontapé inicial confira o artigo Kali Linux – Tutorial de Instalação.

E você, conhece alguma outra ferramenta usada pelos hackers? Espero que vocês tenham gostado, até a próxima!