

Computação Forense Aplicada a Engenharia Social utilizando Kali Linux



Matheus M. Ferreira



Hacker x Cracker

Whitehad x Blackhad

Na prática, os dois termos servem para conotar pessoas que têm habilidades com computadores, porém, cada um dos "grupos" usam essas habilidades de formas bem diferentes. Os hackers utilizam todo o seu conhecimento para melhorar softwares de forma legal e nunca invadem um sistema com o intuito de causar danos. No entanto, os crackers têm como prática a quebra da segurança de um software e usam seu conhecimento de forma ilegal, portanto, são vistos como criminosos.



Computação Forense

A Computação Forense visa obter informações por meio da análise de dados de um computador ou sistema, rede ou qualquer dispositivo de armazenamento que seja alvo de investigação por crimes cibernéticos.[2]

Engenharia Social



O que é?

Engenharia Social é a arte de induzir pessoas para obtenção de um dado ou informação, explora a curiosidade da pessoa, em vez de invadir um sistema.[1]

Sobre

Os crimes de engenharia social são mais comuns do que qualquer outro, envolvem 70% dos ataques cibernéticos no mundo, outros tipos de ataque também usam ele como método para prover outros ataques, visto que ele explora o elo mais fraco da segurança da informação que são as pessoas.[1]

Kali Linux

- Distribuição baseada no debian-testing (arm, x86, adm64), foco em computação forense, segurança e análise de dados e de redes.
- Conhecida com “Distro do Hackers” por conta da maioria do seus usuários.

Kali Linux

Ficando popular logo após o lançamento da serie Mr. Robot



Fonte:<https://presleyson.com.br/2019/02/14/mr-robot-seguranca-da-informacao/>

Kali Linux

Site para download



<https://www.kali.org/downloads/>



Prática

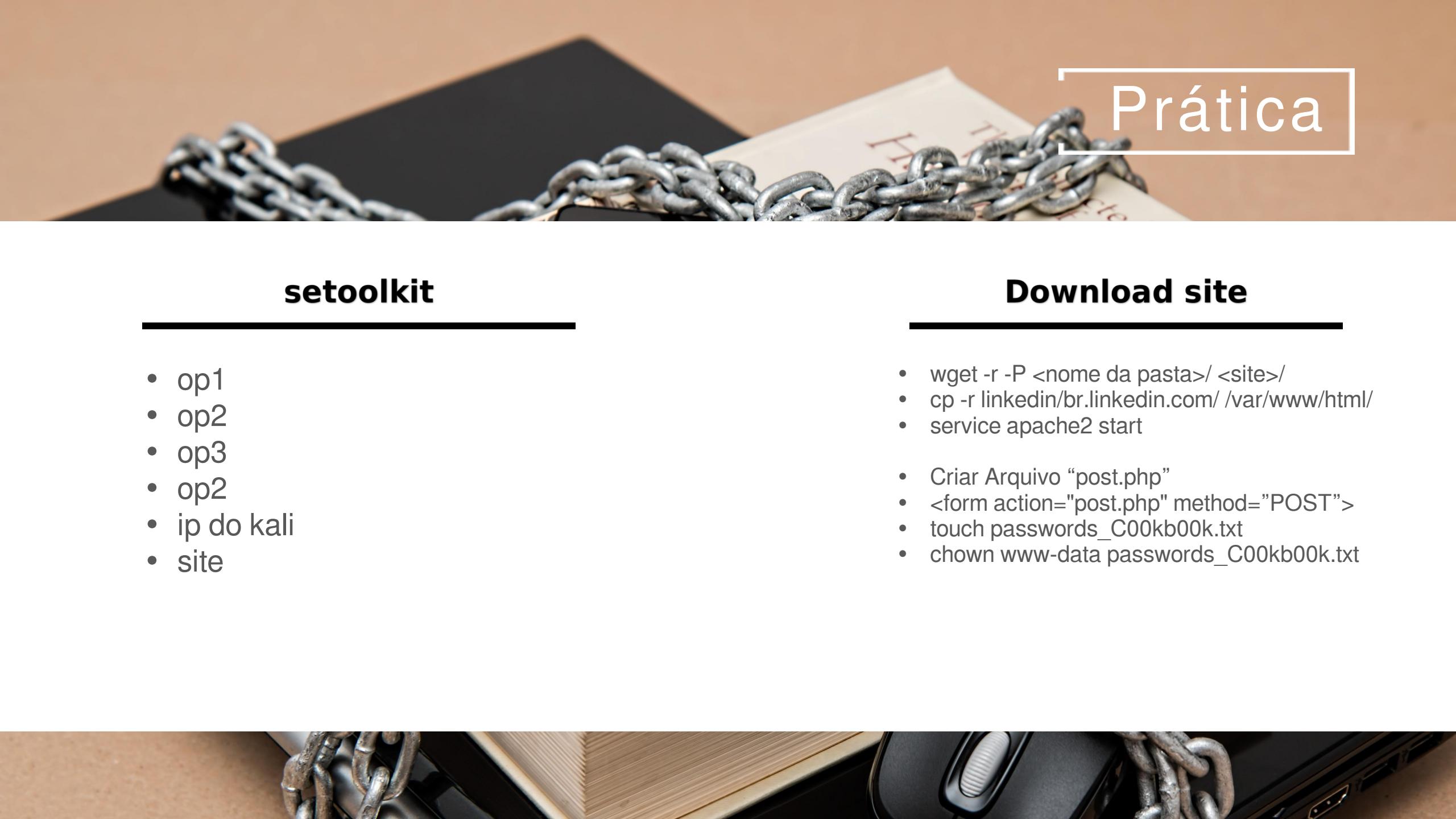
Phishing

Primeiramente a vítima é investigada para coleta de informações básicas necessárias, como :

- nome ;
- endereço de e-mail ;
- número de celular ;
- hobbies ;
- animal de estimação ; e
- possíveis pontos de entrada e fracos protocolos de segurança.

Social-Engineer Toolkit

É um conjunto de ferramentas projetadas para realizar ataques contra o elemento humano.



Prática

setoolkit

- op1
- op2
- op3
- op2
- ip do kali
- site

Download site

- wget -r -P <nome da pasta>/ <site>/
- cp -r linkedin/br.linkedin.com/ /var/www/html/
- service apache2 start
- Criar Arquivo “post.php”
- <form action="post.php" method="POST">
- touch passwords_C00kb00k.txt
- chown www-data passwords_C00kb00k.txt

Referências

- [1]<https://www.academiadeforensedigital.com.br/forense-aplicada-a-engenharia-social/>
- [2]<https://blog.ipog.edu.br/tecnologia/mercado-em-ascenso-computacao-forense/>



Matheus Moreira Ferreira

matheusf.2016@alunos.utfpr.edu.br 

OBRIGADO PELA
ATENÇÃO

