Kali Linux: Social Engineering Toolkit

Os humanos são o melhor recurso e ponto final de vulnerabilidades de segurança de todos os tempos. A Engenharia Social é um tipo de ataque que visa o comportamento humano manipulando e brincando com sua confiança, com o objetivo de obter informações confidenciais, como conta bancária, mídia social, e-mail e até acesso ao computador de destino. Nenhum sistema é seguro, porque o sistema é feito por humanos. O vetor de ataque mais comum usando ataques de engenharia social é o phishing espalhado por meio de spam por e-mail. Eles têm como alvo uma vítima que possui uma conta financeira, como informações bancárias ou de cartão de crédito.

Os ataques de engenharia social não estão invadindo um sistema diretamente, em vez disso, estão usando a interação social humana e o invasor está lidando diretamente com a vítima.

Kevin Mitnick, a lenda da Engenharia Social da era antiga. Na maioria de seus métodos de ataque, ele costumava enganar as vítimas fazendo-as acreditar que ele detém a autoridade do sistema.

Ataque de engenharia social para obter acesso a e-mail

- **Objetivo**: Testar a segurança do ambiente, visando conscientizar os usuários a não realizar acessos com informações confidenciais em qualquer ambiente
- **Agressor**: Teste na máquina virtual
- Alvo: Teste na máquina virtual ou celular pessoal
- **Dispositivo**: Computador ou laptop rodando Kali Linux e meu celular!
- **Ambiente** : Máquina Virtual
- **Ferramenta** : Kit de ferramentas de engenharia social

Nesse caso, primeiro vamos configurar a página de login da conta do Gmail de phishing no meu Kali Linux e usar meu telefone como um dispositivo de disparo.

Outras opções são mais restritas, a SET tem uma página de phising pré-formatada de sites populares, como Google, Twitter e Java.

```
The Social-Engineer Toolkit (SET)

[-] Created by: David Kennedy (ReLIK)

Version: 8.0.3

Codename: 'Maverick'

[-] Follow us on Twitter: MTrustedSec

[-] Follow me on Twitter: MTackingDave

[-] Homepage: https://www.trustedsec.com

Welcome to the Social-Engineer Toolkit (SET).

The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)

Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:

1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit
```

Sim, claro, vamos realizar ataques de engenharia social, então escolha o número 1 e pressione ENTER.

E então serão exibidas as próximas opções, e escolha o número 2. **Vetores de Ataque ao Site**.

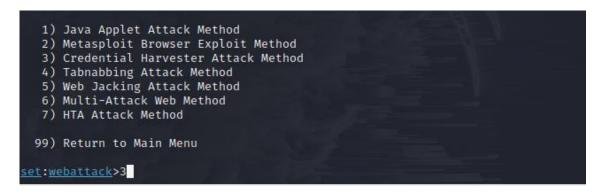
Aperte ENTER.

```
Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.
```

Em seguida, escolhemos o **número 3. Método de ataque do Harvester de credenciais**. Aperte Enter.



Outras opções são mais restritas, a SET tem uma página de phising pré-formatada de sites populares, como Google, Yahoo, Twitter e Facebook. Agora escolha **o número 1.**

Web Templates.

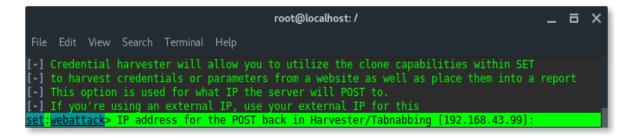
```
1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>1
```

Então basta inserir o endereço IP local do invasor (meu PC). E aperte ENTER.

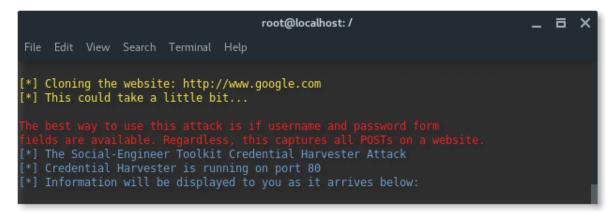
PS: Para verificar o endereço IP do seu dispositivo, digite: 'ifconfig'



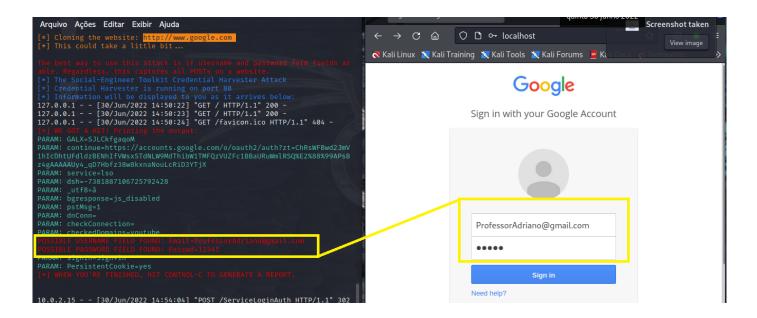
Tudo bem, até agora, definimos nosso método e o endereço IP do ouvinte. Nestas opções estão listados modelos pré-definidos de phising na web, como mencionei acima. Porque visamos a página da conta do Google, então escolhemos o **número 2. Google . Aperte ENTER .**

```
    Java Required
    Google
    Twitter

set:webattack
Select a template:2
```



Agora, SET inicia meu Kali Linux Webserver na porta 80, com a página de login da conta do Google falsa. Nossa configuração está feita.



Pronto sucesso no exercício!!