

# 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 phishing pré-formatada de sites populares, como Google, Twitter e Java.

```

[—] The Social-Engineer Toolkit (SET) [—]
[—] Created by: David Kennedy (ReL1K) [—]
      Version: 8.0.3
      Codename: 'Maverick'
[—] Follow us on Twitter: @TrustedSec [—]
[—] Follow me on Twitter: @HackingDave [—]
[—] Homepage: https://www.trustedsec.com [—]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

Inicio
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.

set>

```

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

```
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>3
```

Outras opções são mais restritas, a SET tem uma página de phishing 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'**

```
root@localhost: /
File Edit View Search Terminal Help
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.43.99]:
```

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

```
1. Java Required
2. Google
3. Twitter

set:webattack> Select a template:2
```

```
root@localhost: /
File Edit View Search Terminal Help

[*] Cloning the website: http://www.google.com
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

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

The image shows a Kali Linux terminal window on the left and a web browser window on the right. The terminal window displays the output of the SET (Social-Engineer Toolkit) command to clone the Google website. It shows the cloning process, the attack running on port 80, and the capture of a POST request from a user. The user's email address, ProfessorAdriano@gmail.com, and a password, 12345, are captured and displayed in the terminal. The web browser window on the right shows the cloned Google login page, which is a replica of the real Google login page. The email field is filled with ProfessorAdriano@gmail.com and the password field is filled with 12345. A yellow box highlights the email and password fields in the browser, and another yellow box highlights the captured email and password in the terminal. A yellow arrow points from the browser's email field to the terminal's output, indicating the successful capture of the user's credentials.

```
Arquivo Ações Editar Exibir Ajuda
[*] Cloning the website: http://www.google.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are
able. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
127.0.0.1 - - [30/Jun/2022 14:50:22] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [30/Jun/2022 14:50:23] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [30/Jun/2022 14:50:24] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLckfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV
1hIcDhtUf0ldz8ENhIFVwsxSTdNLW9MdThibW1TMFQzVUZFc1B8aURUwmlRSQxE2%88%99APsB
z4gAAAAUy4_qd7Hbfz38w8kxnaNouLcRID3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=a
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtu.be
POSSIBLE USERNAME FIELD FOUND: Email=ProfessorAdriano@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=12345
PARAM: sign-in=sign-in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
10.0.2.15 - - [30/Jun/2022 14:54:04] "POST /ServiceLoginAuth HTTP/1.1" 302
```

Pronto sucesso no exercício!!