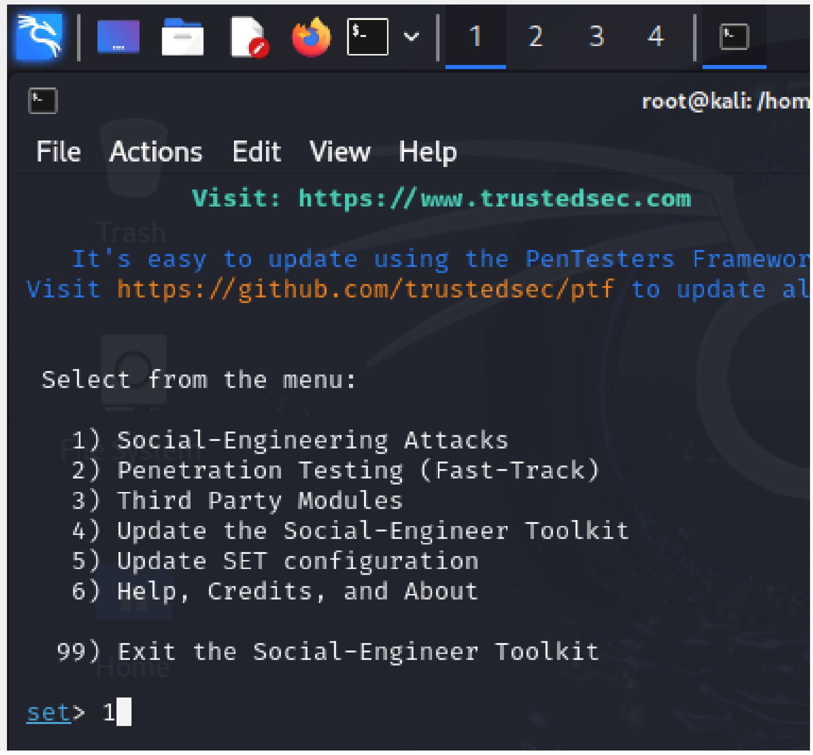
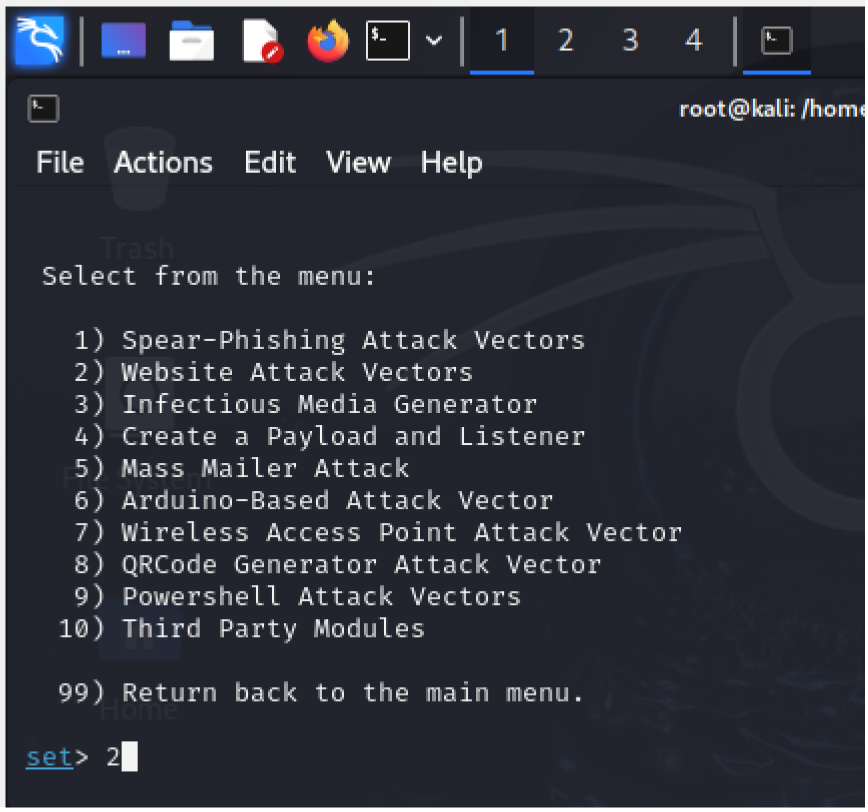
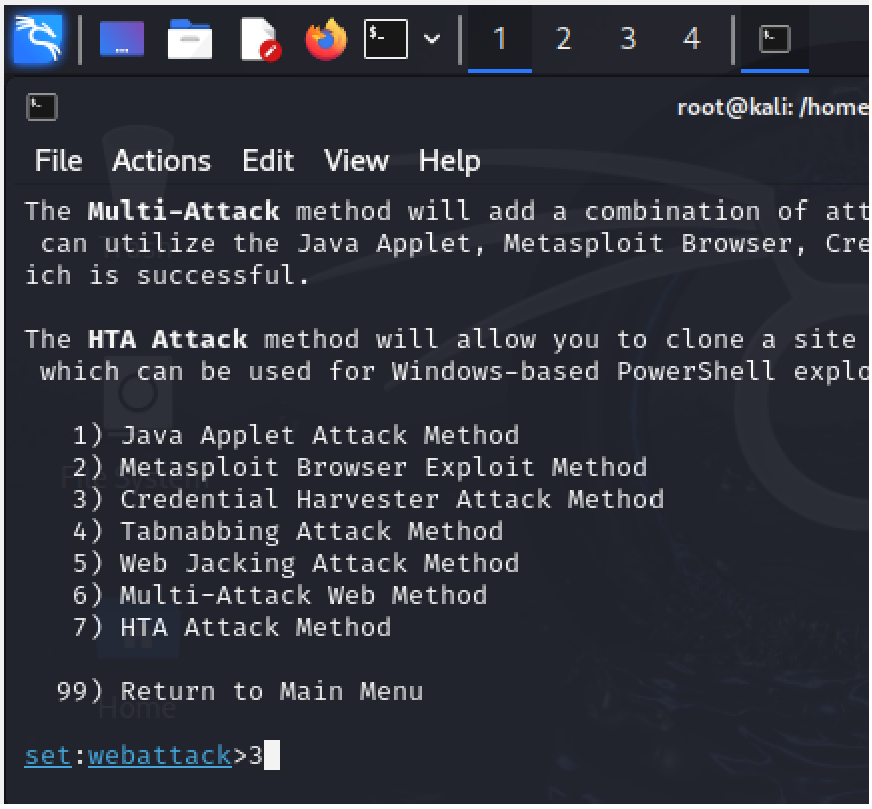


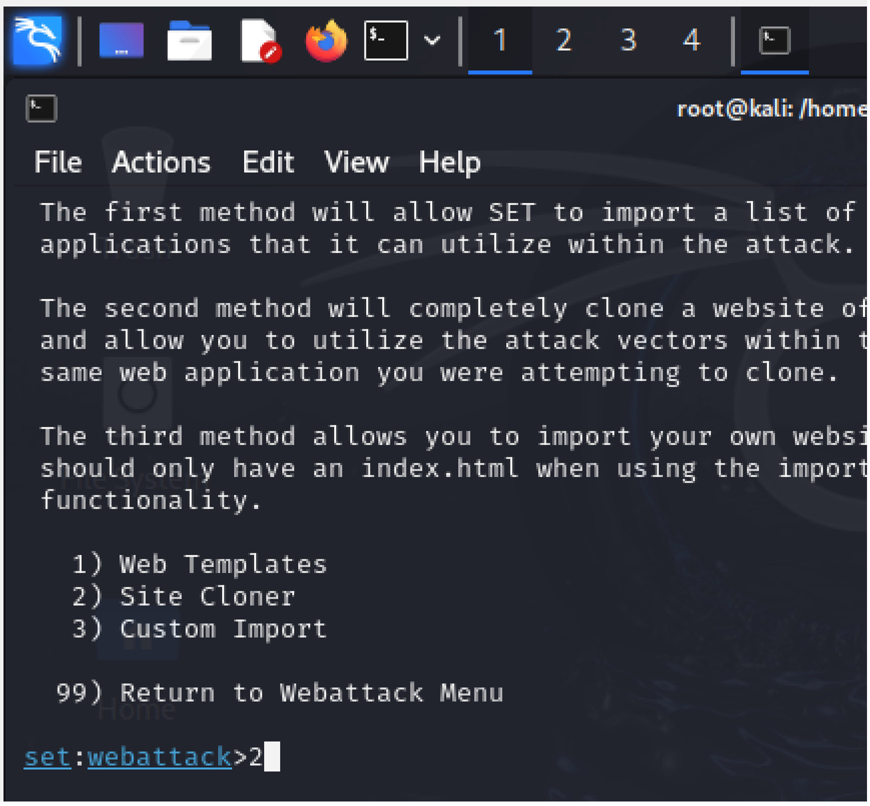
```
              Visit: https://www.trustedsec.com

    It's easy to update using the PenTesters Framewor
 Visit https://github.com/trustedsec/ptf to update al


  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> 1
```



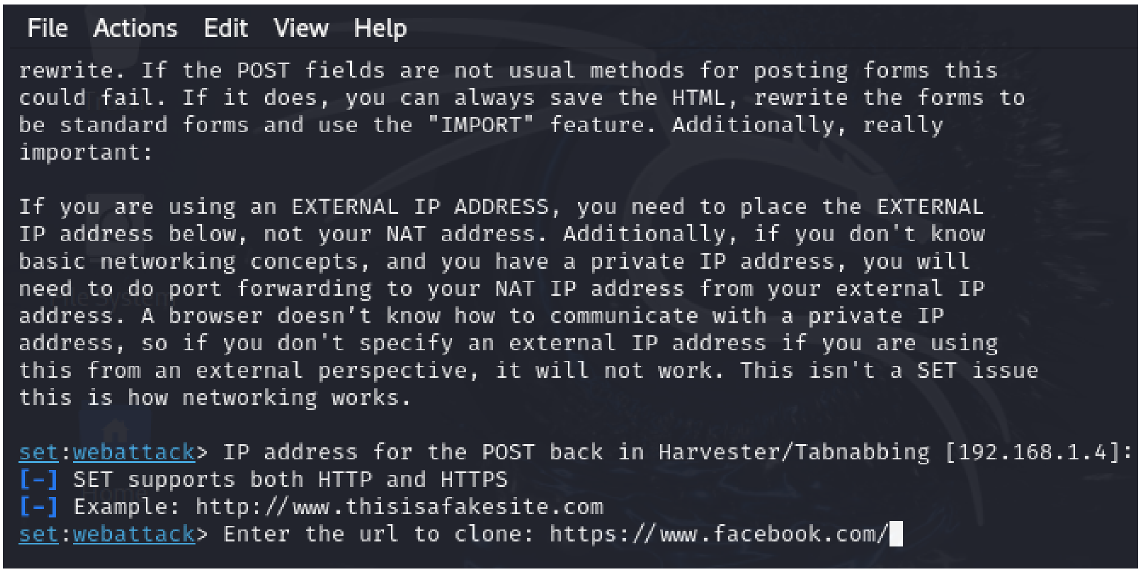
```
  Select from the menu:

    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
```



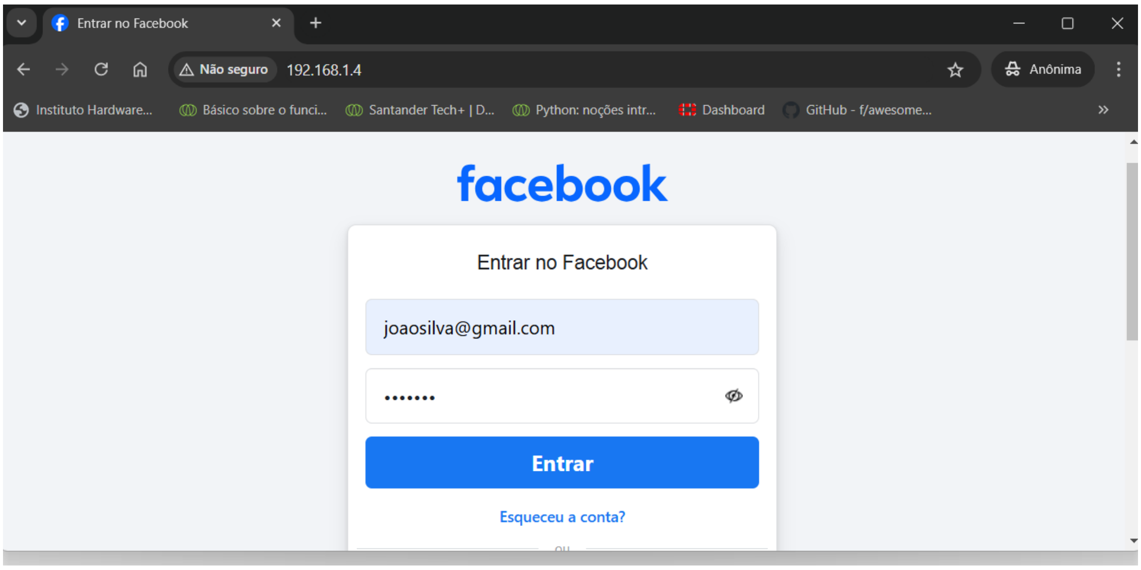
```
The Multi-Attack method will add a combination of att
 can utilize the Java Applet, Metasploit Browser, Cre
ich is successful.

The HTA Attack method will allow you to clone a site
 which can be used for Windows-based PowerShell explo

   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
```



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

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

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

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
```



```
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 [192.168.1.4]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://www.facebook.com/
```

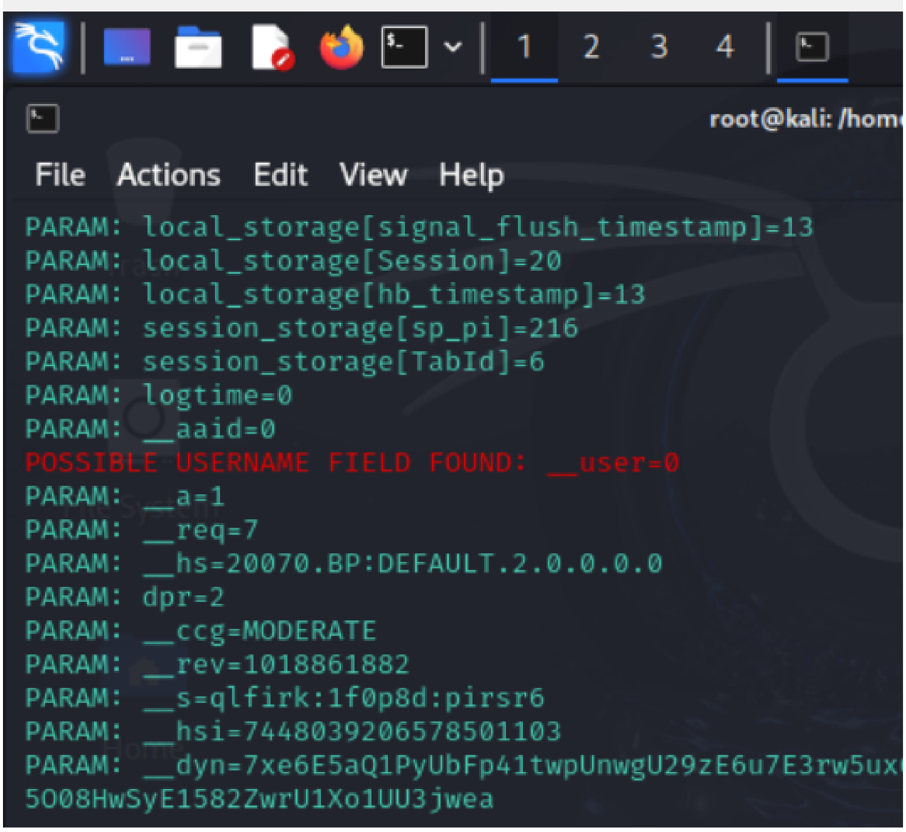


Entrar no Facebook

joaosilva@gmail.com

•••••••

Após seguir todos os passos corretamente e refazer mais de 5 vezes, o retorno sempre foi o abaixo, mesmo desativando o antivírus.



```
PARAM: local_storage[signal_flush_timestamp]=13
PARAM: local_storage[Session]=20
PARAM: local_storage[hb_timestamp]=13
PARAM: session_storage[sp_pi]=216
PARAM: session_storage[TabId]=6
PARAM: logtime=0
PARAM: __aaid=0
POSSIBLE USERNAME FIELD FOUND: __user=0
PARAM: __a=1
PARAM: __req=7
PARAM: __hs=20070.BP:DEFAULT.2.0.0.0.0
PARAM: dpr=2
PARAM: __ccg=MODERATE
PARAM: __rev=1018861882
PARAM: __s=qlfirk:1f0p8d:pirsr6
PARAM: __hsi=7448039206578501103
PARAM: __dyn=7xe6E5aQ1PyUbFp41twpUnwgU29zE6u7E3rw5ux
5O08HwSyE1582ZwrU1Xo1UU3jwea
```