RESEARCH ON CREDENTIAL HARVESTING: SITE CLONING

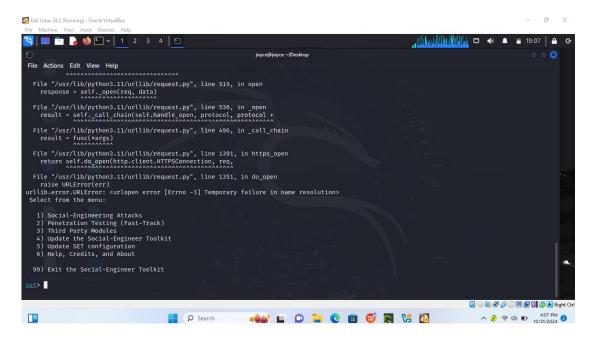
Project Objective: Learn how to harvest credentials using a cloned site, and discover events where threat actors clone site.

Project Tool: Kali Linux(sudo setoolkit)

Credential Harvesting is the process of gathering sensitive information on a target such as credit card details or passwords, without them knowing that such information is captured.

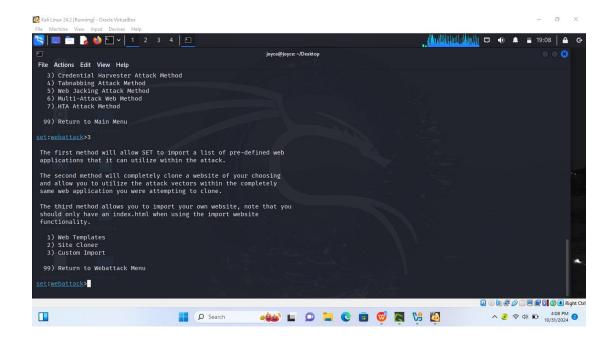
Sudo setoolkit(Social Engineering Tool Kit) 试 🔲 🛅 🍃 🝅 🕒 🗸 🗎 2 3 4 🕒 19:06 | 🖺 G 2 - I Right Ctr ^ ■ ③ ⑤ Φ Φ D 4:06 PM 2

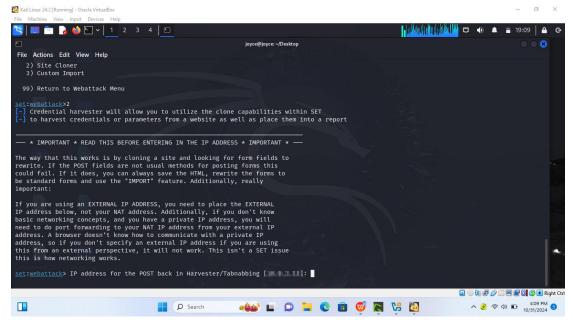
Setoolkit options



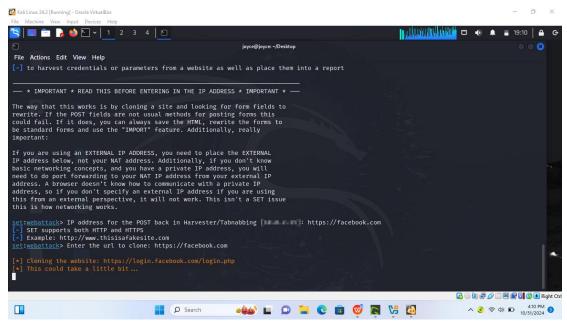


Credential Harvest will utilize web cloning of a web-site that has username and password field, and harvest all information on the website.

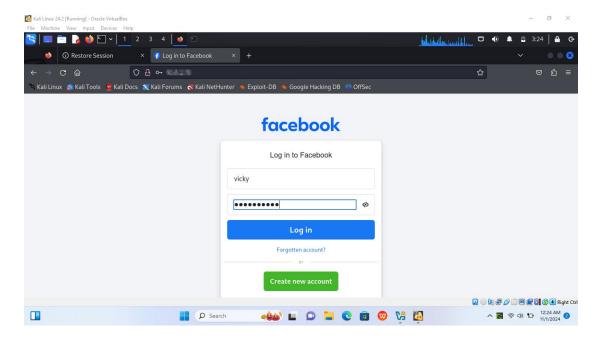




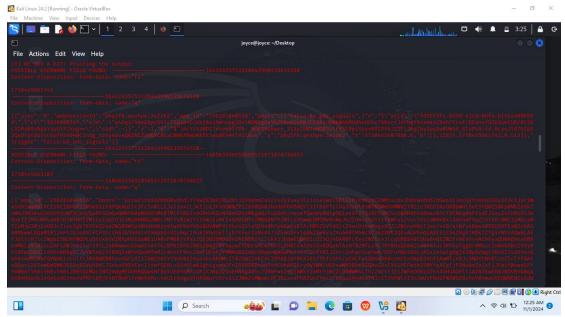
Using the Local IP address to access the clone site.



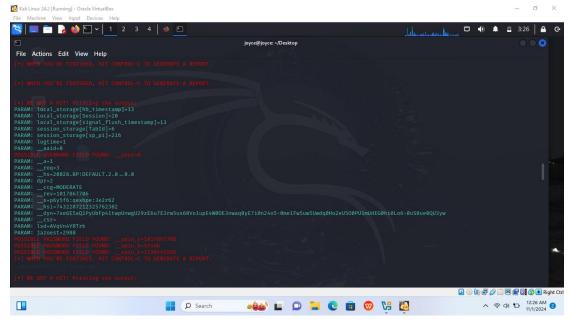
SET would clone the website, then ask of the URL to be cloned, it will display all the POST requests.



Using the local etho IP address to get to the Cloned site Enter random username and password and hit enter.



This displays the possible username and password , and other information inputted into the clone site.



This displays the information inputted into the cloned site