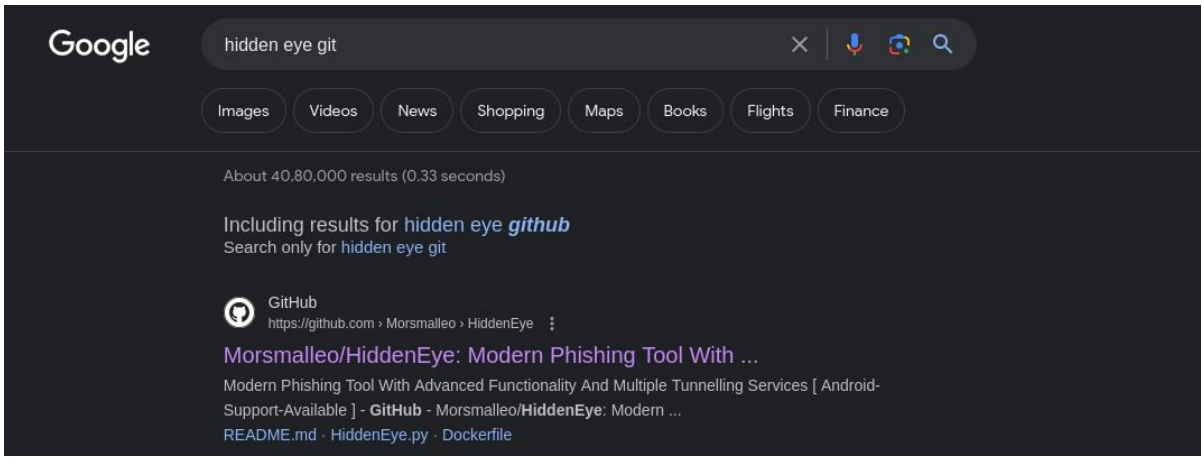
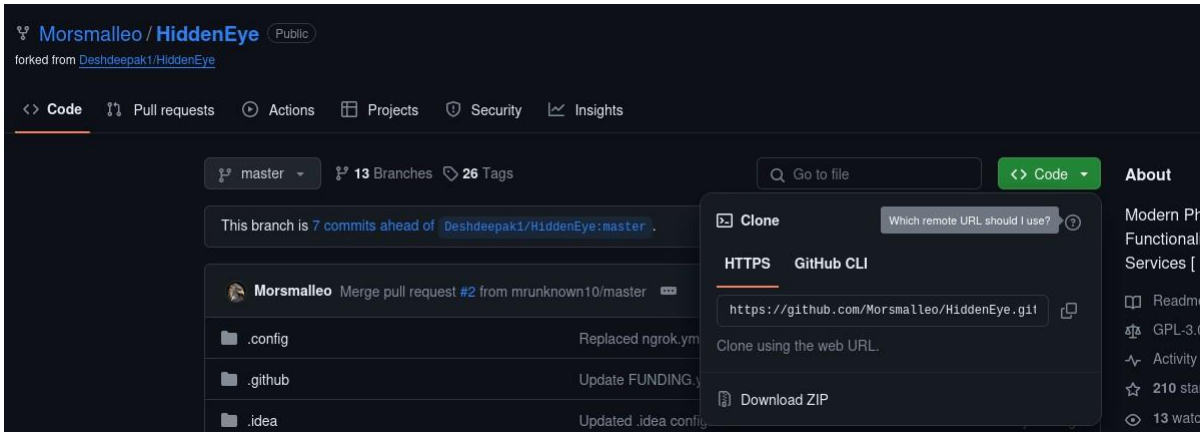
Phishing attack using Hidden eye tool

Introduction:

In ethical hacking, a keylogger is a tool that records keystrokes on a computer. Ethical hackers use keyloggers to identify security vulnerabilities, such as weak passwords or unauthorized access points. They only deploy keyloggers with the user's permission, adhering strictly to ethical guidelines to ensure legality and privacy.

Step 1: Search Hidden eye git to copy the link of clone to install in linux.

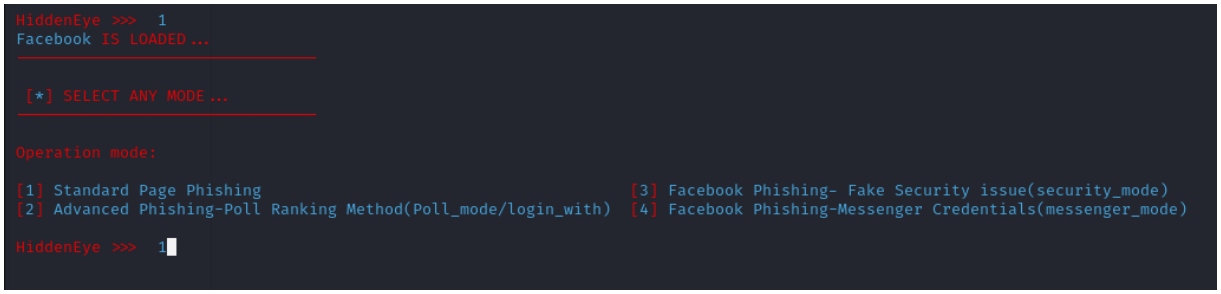




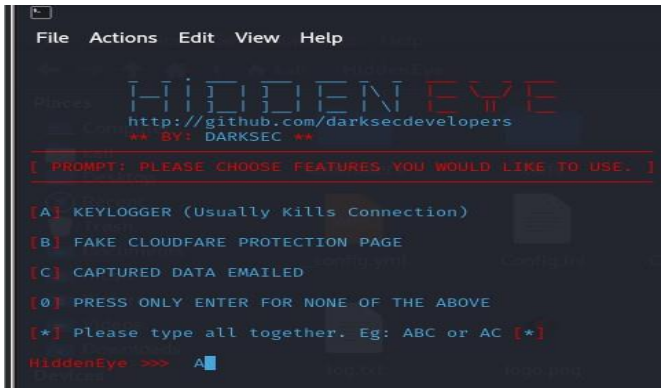
Step 2: use git clone and paste the link that copied from the git and install it
Then change the directory to HiddenEye folder and to access HiddenEye use ./HiddenEye.py command

Step 3 : Select any Attack Vector template

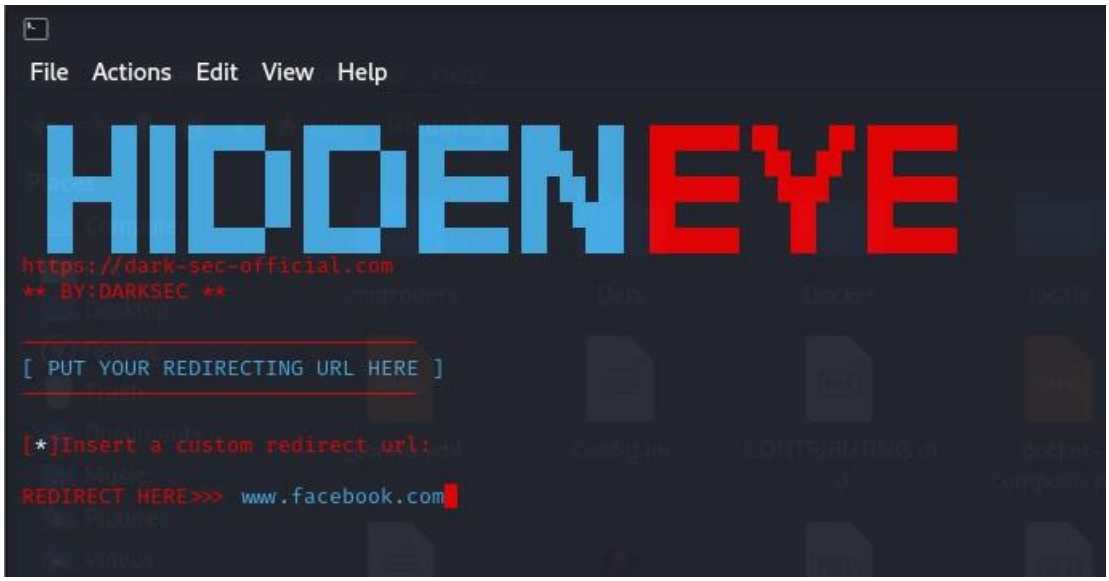
Step 3: Select the operation



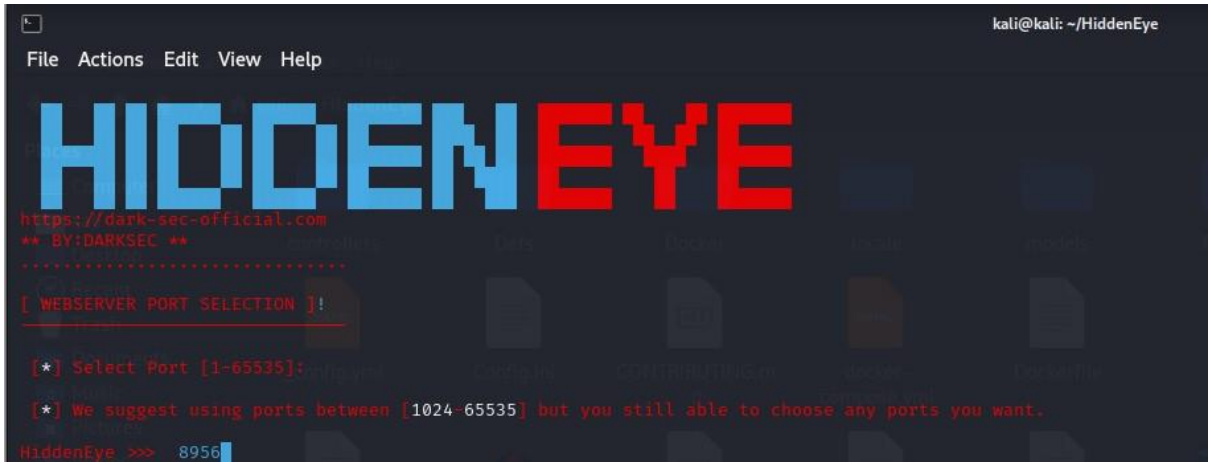
Step 4: Select any feature you would like to do



Step 5: Put your redirecting url of page here

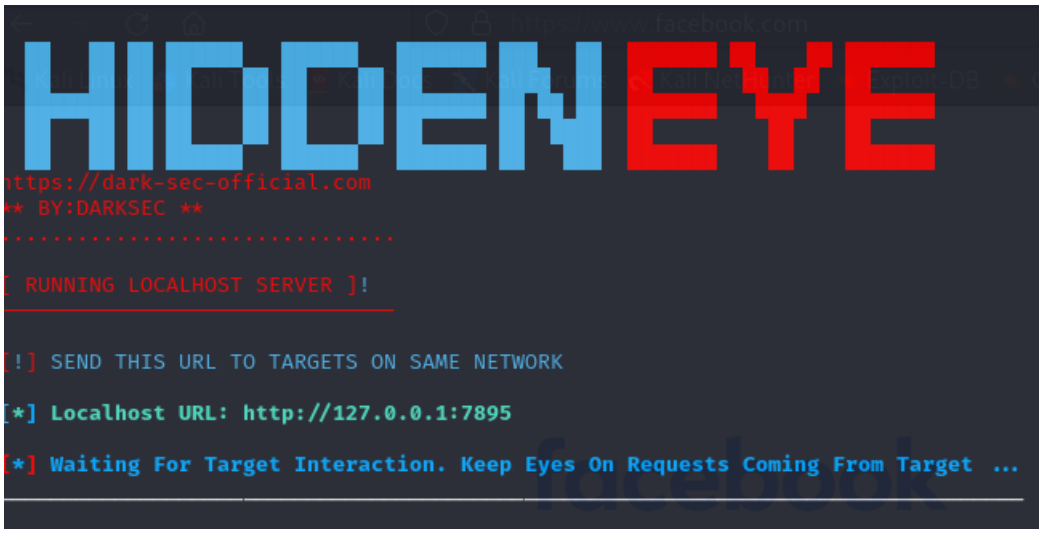


Step 6: Select the port number.

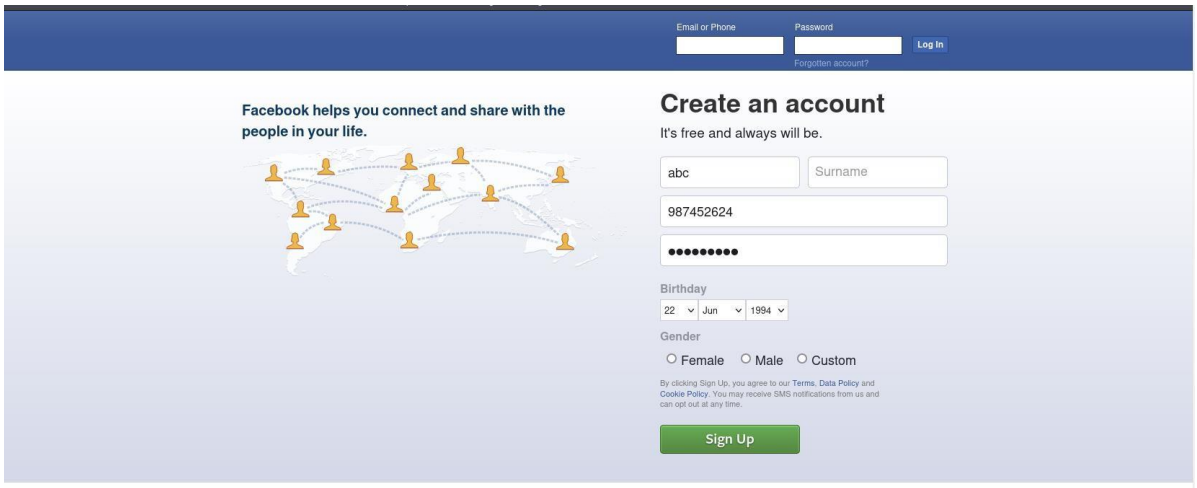


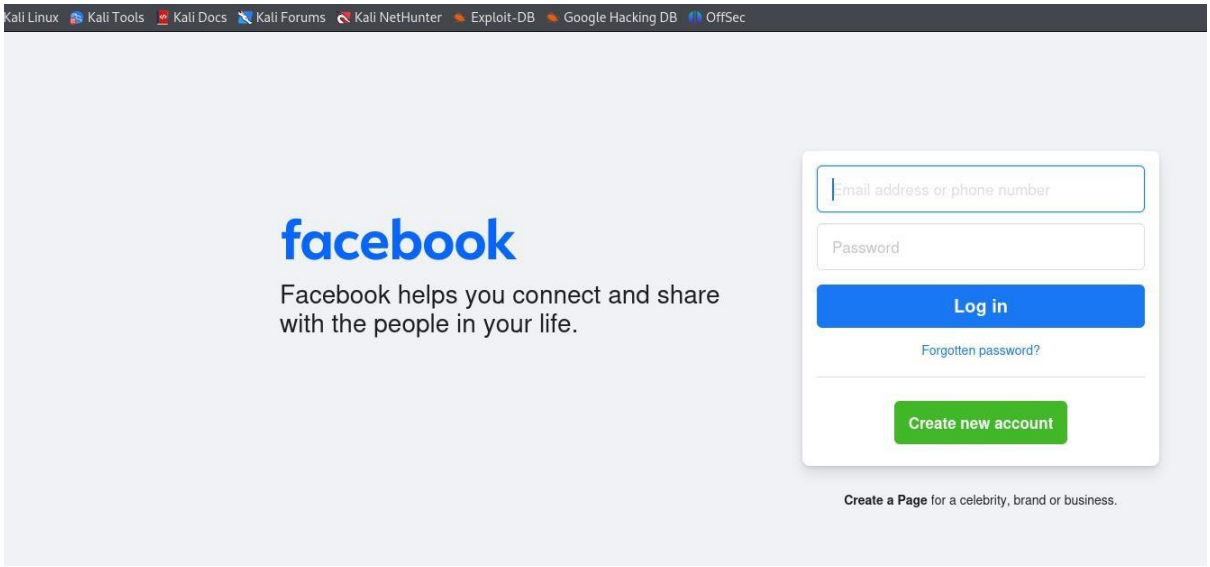
Step 7: Select the Available Server

Step 8 : Localhost URL: http://127.0.0.1:7895 send this to victim

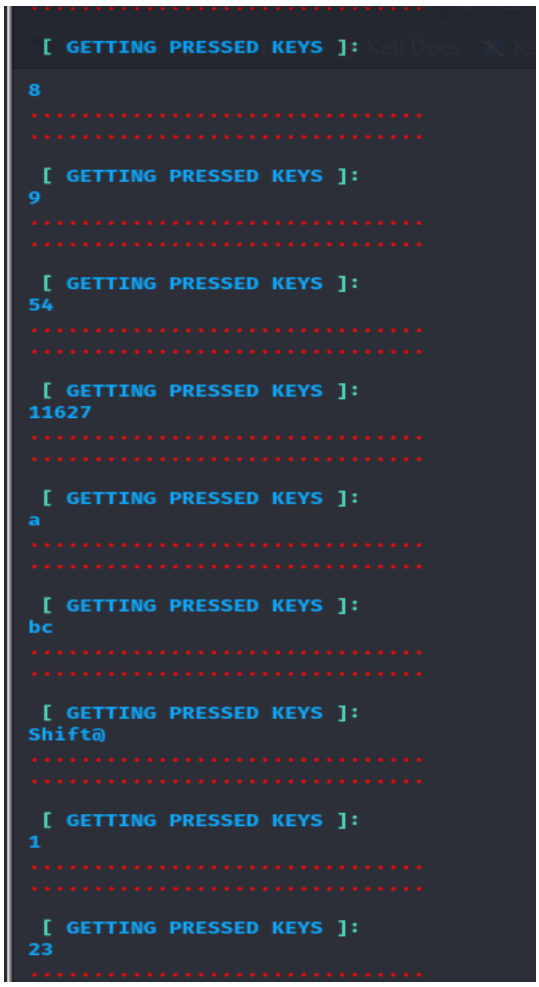


Step 9: After clicking Victim will enter his/her details in the page

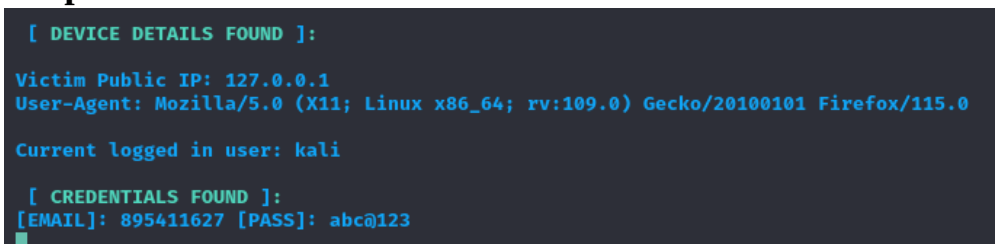




Step 10: Once the victim start entering the detail all the details will display on Hackers cmd



Step 11: Details of victim found.



Conclusion:

The Phishing Attack using Hidden Eye demonstrates how attackers can manipulate user trust through social engineering tactics. Ethical hackers use such tools to raise awareness about phishing threats and train organizations to recognize and defend against similar attacks. The key is to use these insights to enhance cybersecurity measures and promote user education.