MAJOR – SEP

Name – Anjali Kuamri

Email – [anjalirajwar101@gmail.com](mailto:anjalirajwar101@gmail.com)

College Name – BIT Sindri

**Cyber Security Major Project**

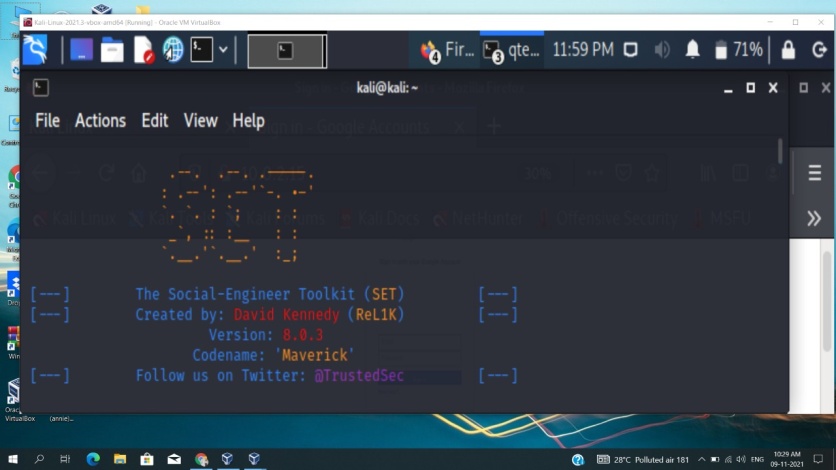
3. Use SET Tool and create a fake Gmail page and try to capture the credentials in command line and

Hacker Machine : Kali Linux

Victim machine : Windows XP / Windows 7 / Windows 10

Social Engineering Toolkit:-

Social engineering toolkit is the most powerful tool for performing social engineering attacks. It is the metasploit of social engineering in a way. It provides a very easy user interface to perform attacks like phishing, browser exploitation etc.



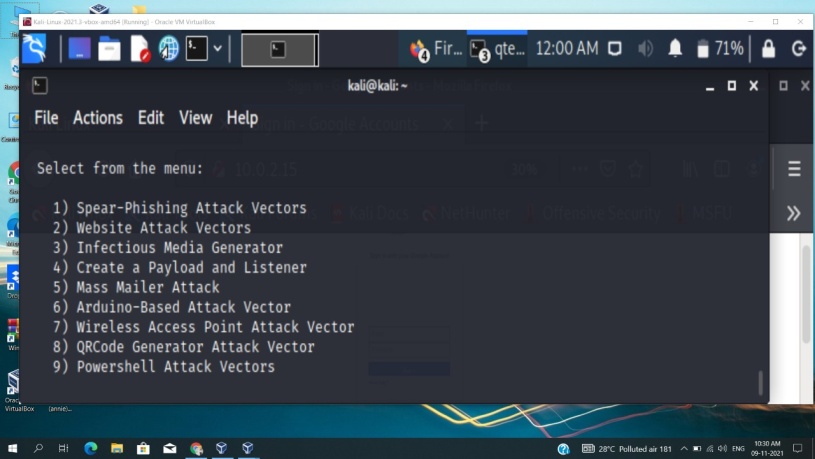
Credential Harvester Attack:-

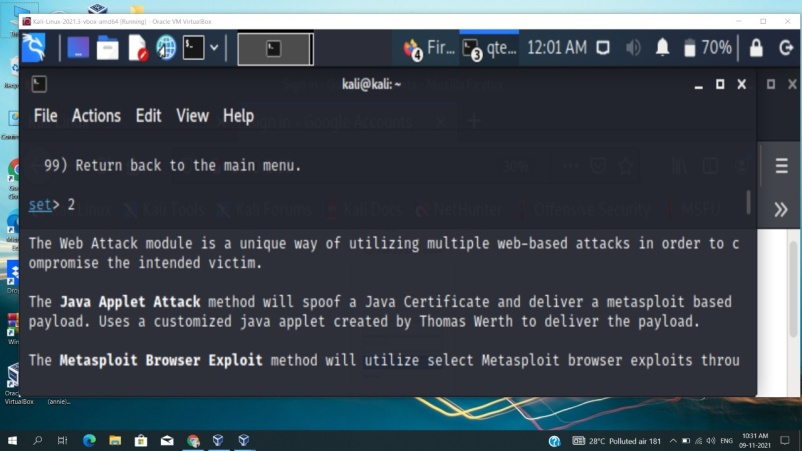
Credential Harvester attack is one of the options available inside SET, that can create phishing pages and start a server to serve the pages and catch any user login data

steps:-

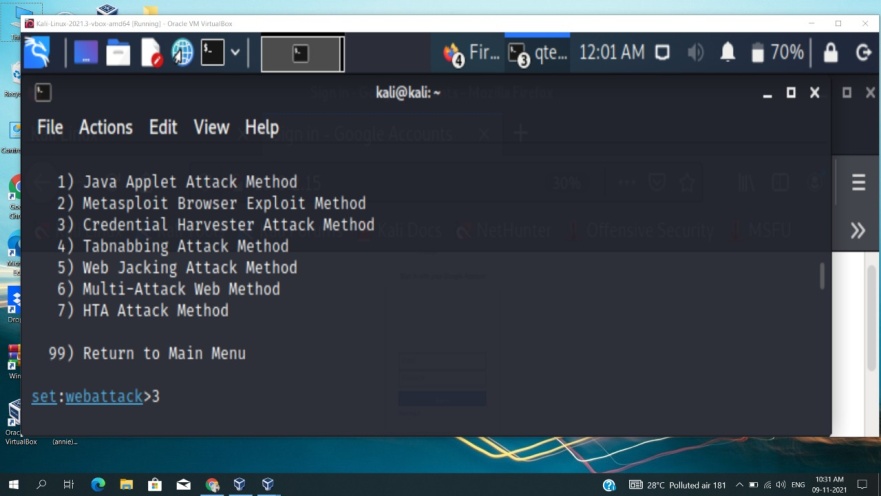
1. select "Social-Engineering Attacks" <1>

2. select "Website Attack Vectors" <2>

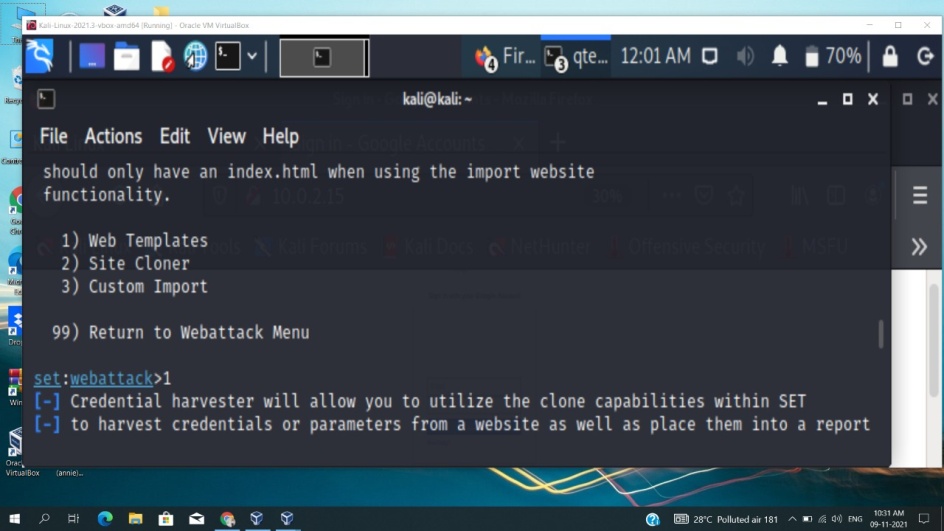




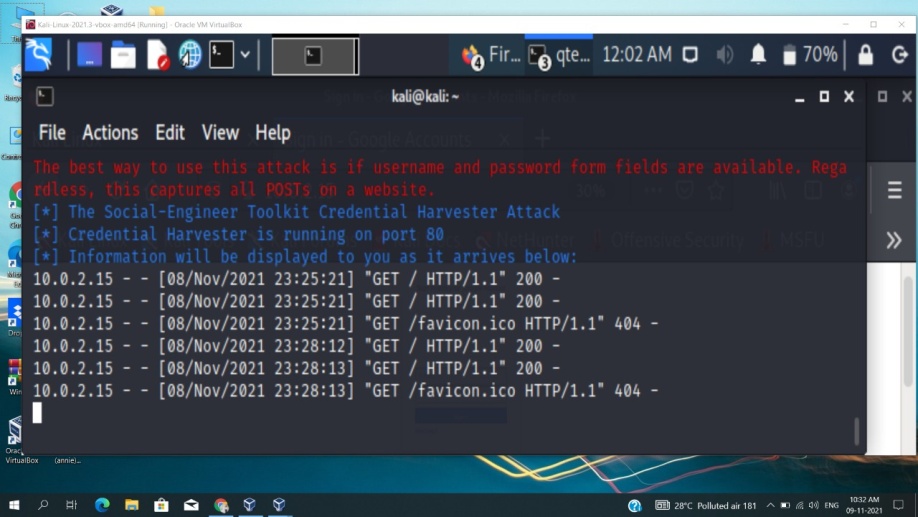
3. select "Credential Harvester Attack" <3>

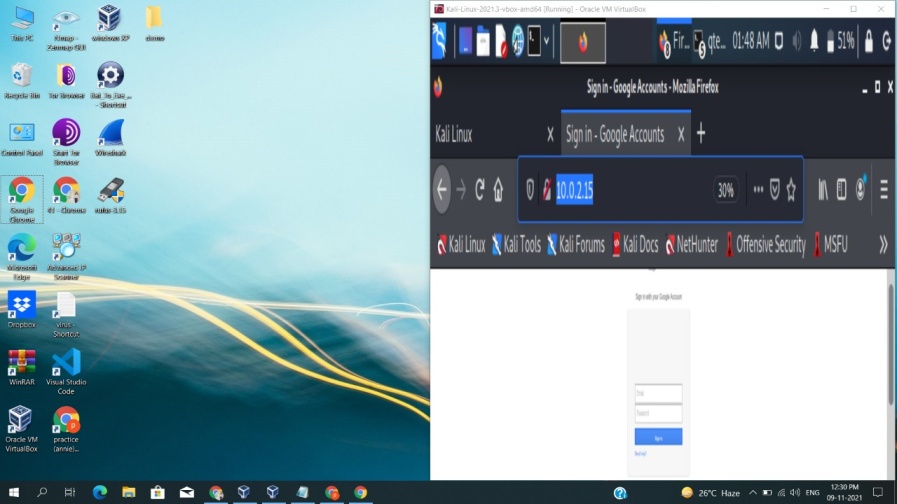
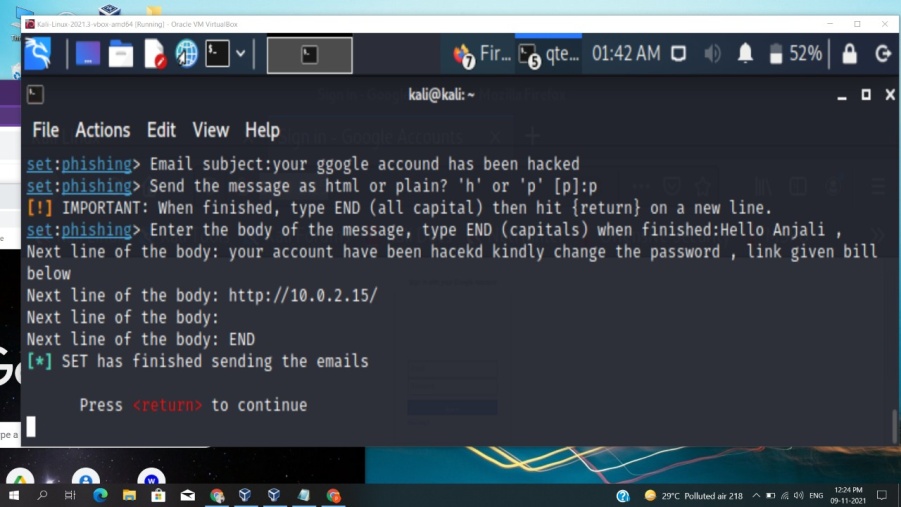


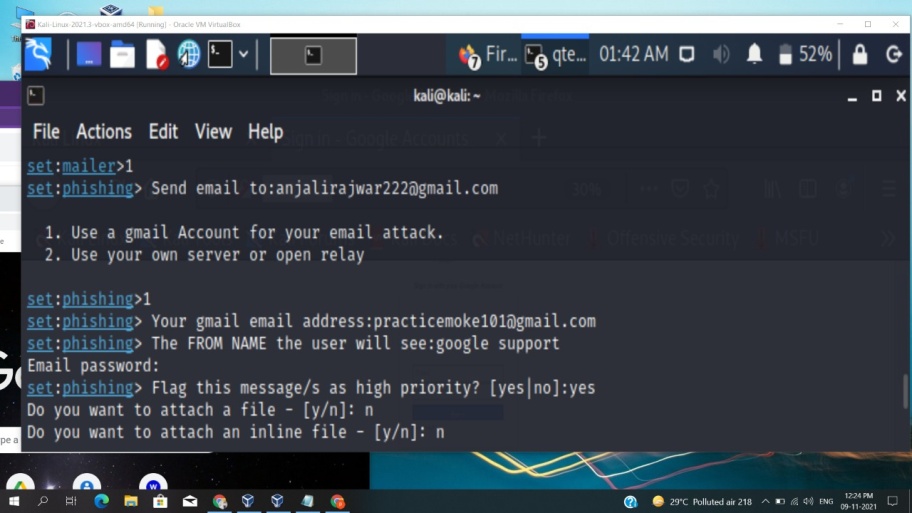
4. select " site cloner" <2>



5. it will ask for 2 important piece of information. The first is the ip address, to which it would submit the data and second is the url to clone which is in this case gmail.com







**Ways to Prevent Social Engineering Attacks:-**

**Some Quick Tips to Remember**:-

1. Think before you click.

2. Research the sources

3. Email spoofing is ubiquitous.

4. Don’t download files you don’t know.

5. Offers and prizes are fake.

**Five Ways to Protect Yourself**:

1. Delete any request for personal information or passwords.

2. Reject requests for help or offers of help.

3. Set your spam filters to high.

4. Secure your devices.

5. Always be mindful of risks.

**Thank You…**