Social Engineering Toolkit

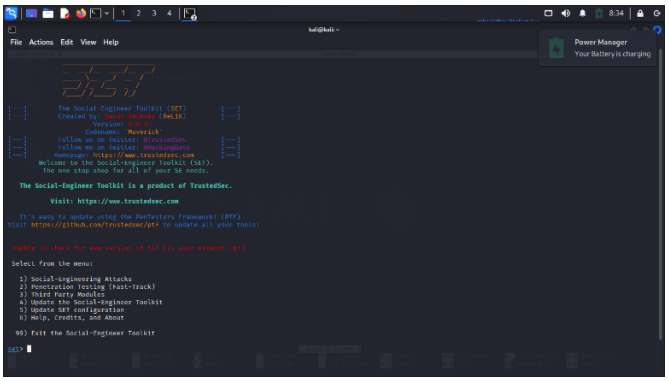
Objective :

Use setoolkit to get the credentials of user by cloning a website.

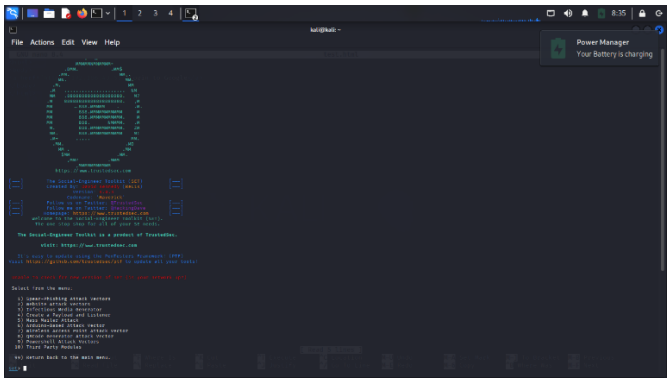
Steps To Clone A Website :

1.Open a terminal and create a new file test.html by using : “nano test.html” & save the file.

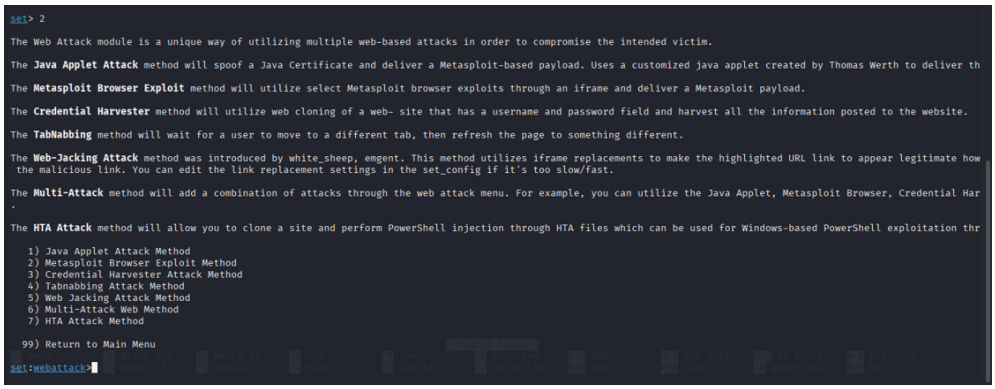
2.Open a new terminal and type the command “sudo setoolkit”. You can see the following :



3.Now enter the option 1 i.e., “Social-Engineering Attacks”. You can see another 10 options :

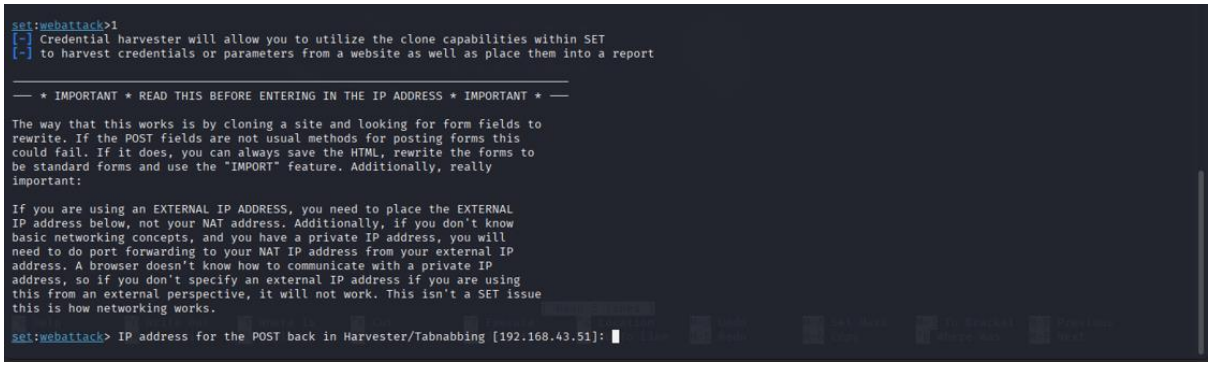


4.Select 2nd option which is “Website Attack Vectors”. You can observe 7 options :

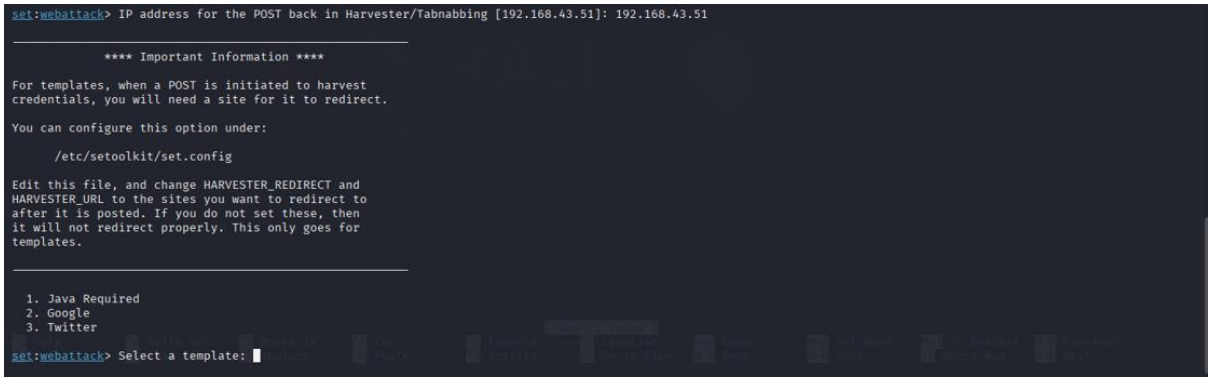


5.Now select the “Credential Harvester Attack Method” by entering 3 which shows you 3 different methods :

6.As we want to clone a website just select the “Web Template”. This method asks you to enter your IP Address :

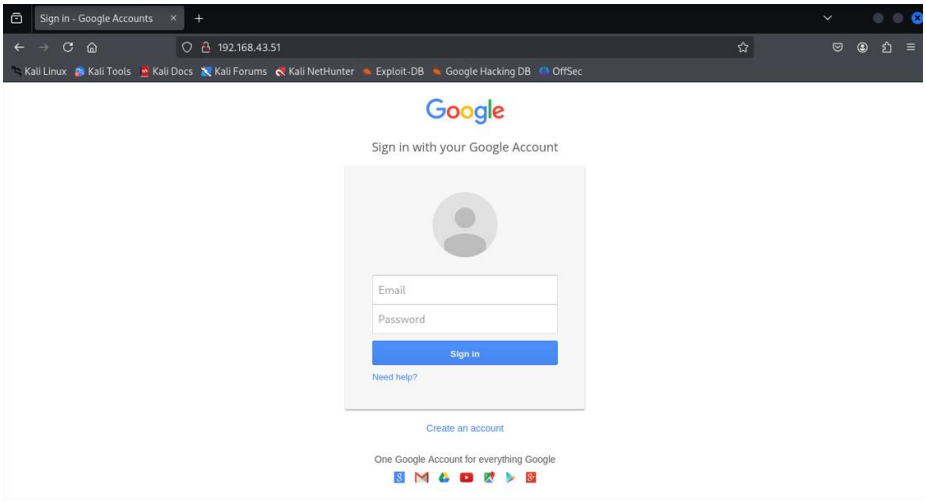


7.When you enter your IP Address, it asks you 3 types of templates :

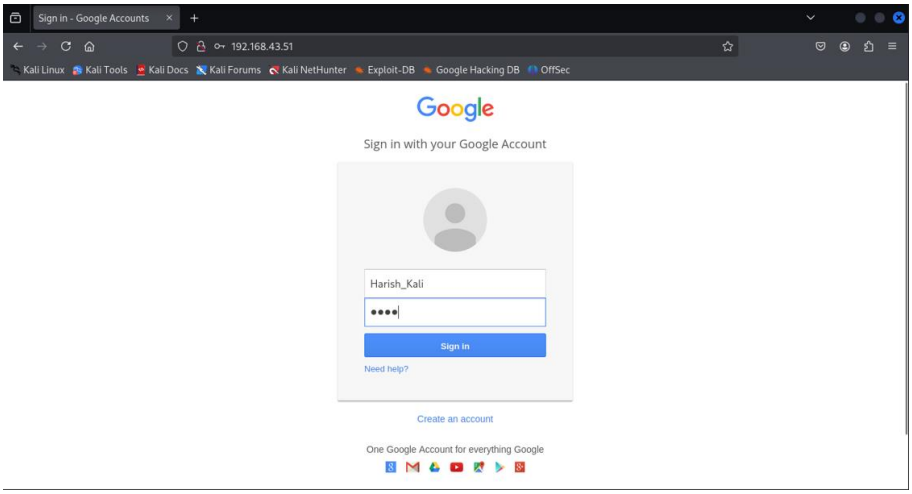


8.Select the “Google” template by entering 2. Now it starts to clone the template :

9.Open firefox and enter your IP Address :



10.Enter your “username & password” to sign in with google :



11.When you observe the terminal, you can get the “credentials of the user” who uses the clone template to sign in to google :

Conclusion :

The Social Engineering Toolkit is a real time credentials stealing tool. By this we can get the users details easily by sending a fake link by various methods.

In this experiment we cloned “Google sign in page” to get users details by using ‘Web Template’ method of ‘Credential Harvester Attack Method’ belongs to the ‘Website Attack Vectors’ in the ‘Social-Engineering Attacks’.