**CSE3501-Information security analysis and audit**

Name: O G RAGAVI

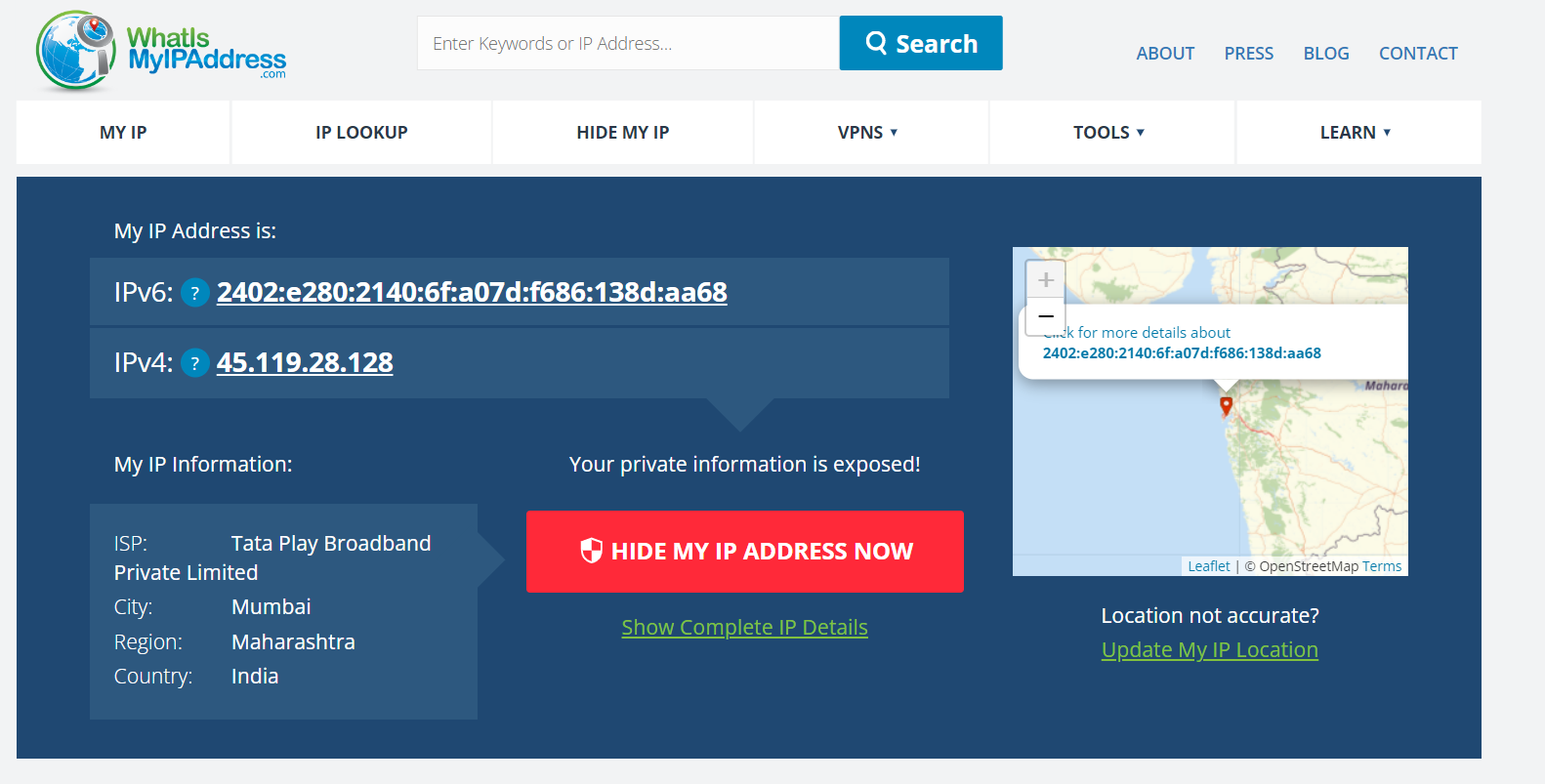
Reg No: 20BCE1988

Lab Ex: 8

Title: Tools, Setoolkit, the harvester lazybox

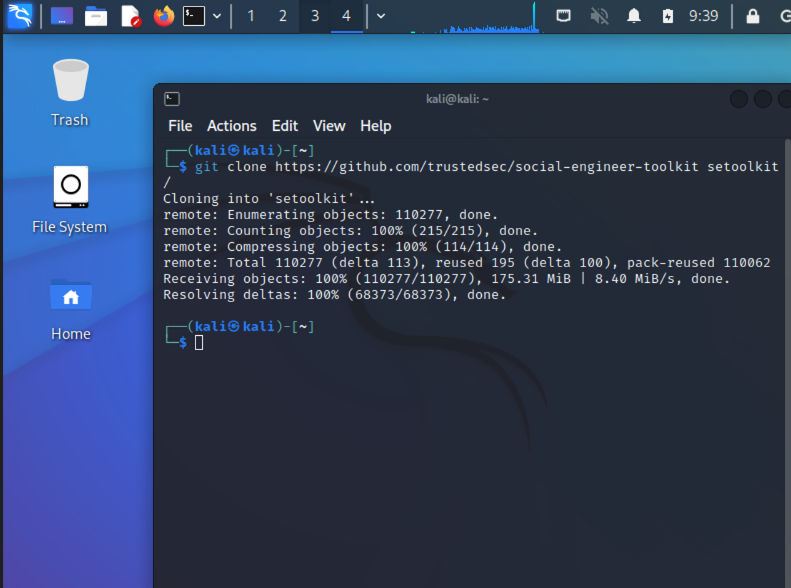
**Pre-requisite:**

Find your ip address using <http://whatismyipaddress.com/>

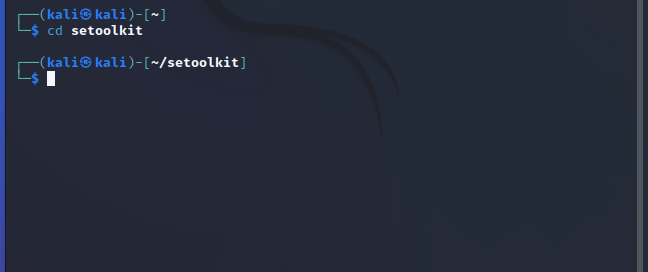
****

**Step1:** Open kali linux terminal and type the following command

**git clone** [**https://github.com/trustedsec/social-engineer-toolkit**](https://github.com/trustedsec/social-engineer-toolkit)

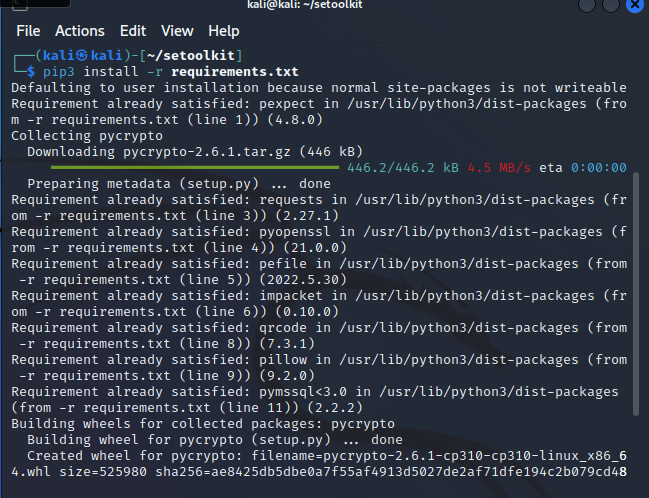
****

**cd toolkit**

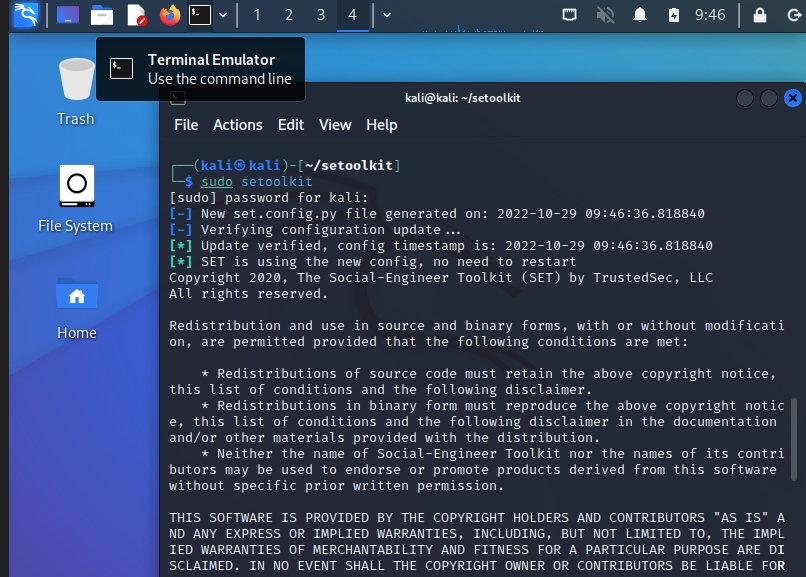
****

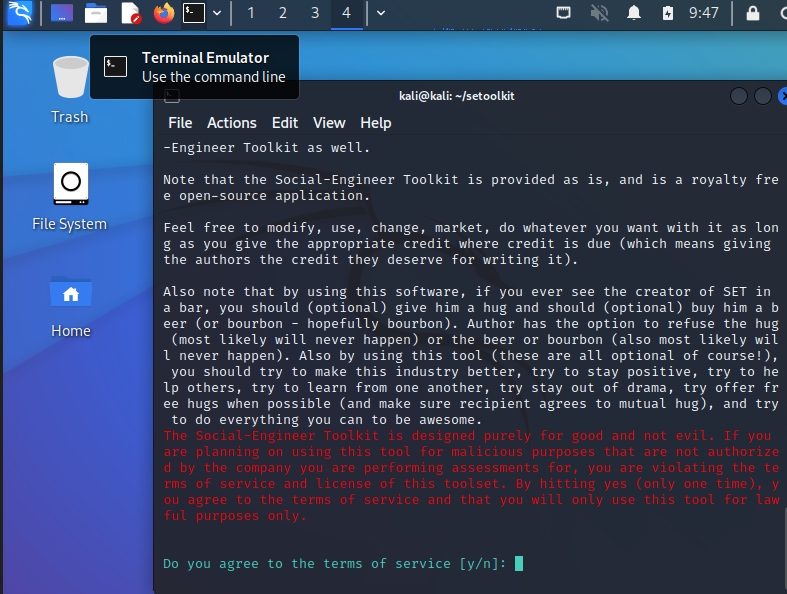
**pip3 install -r requirements.txt**

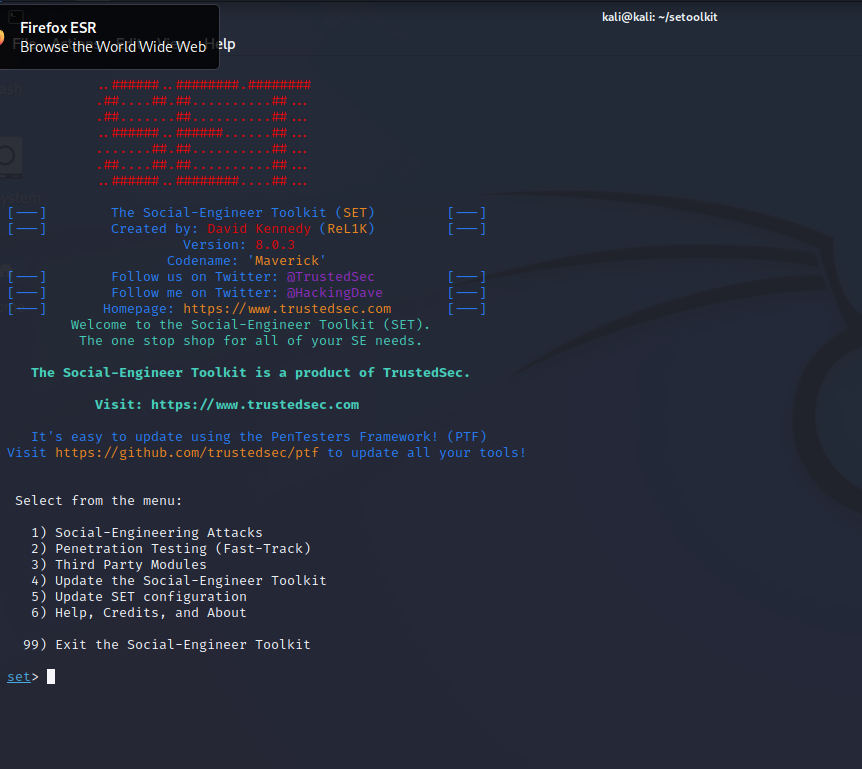
**python setup.py**

****

**sudo setoolkit**

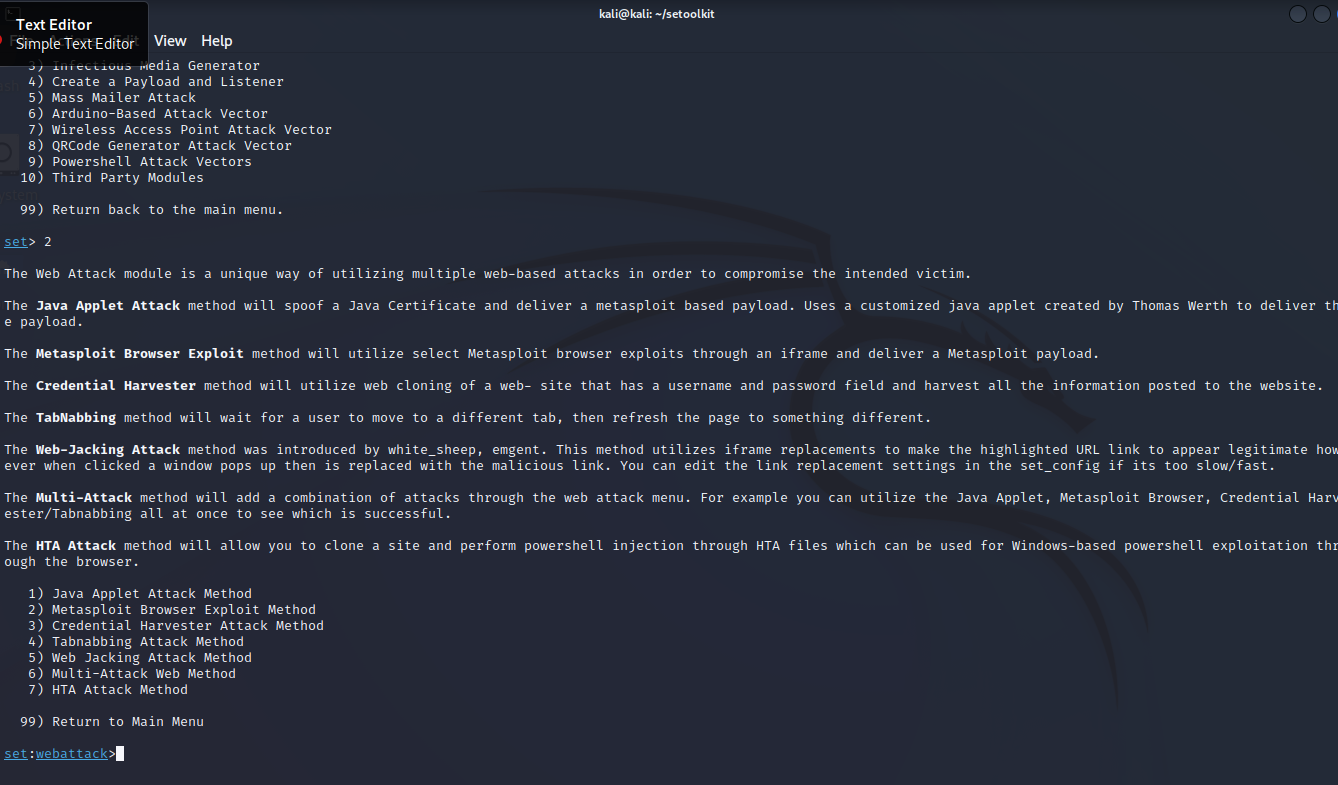
****

****

****

**Step2: choose 1(Social engineering attack)**

**Choose 2(web attack)**

****

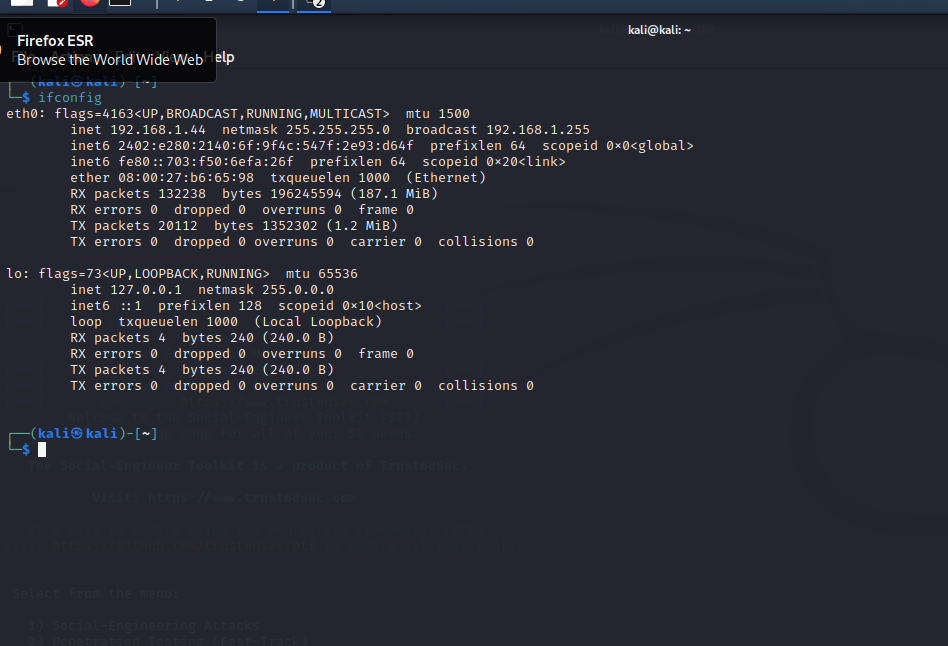
**Choose 3( credential harvester attack method)**

**Choose 1 ( web templates)**

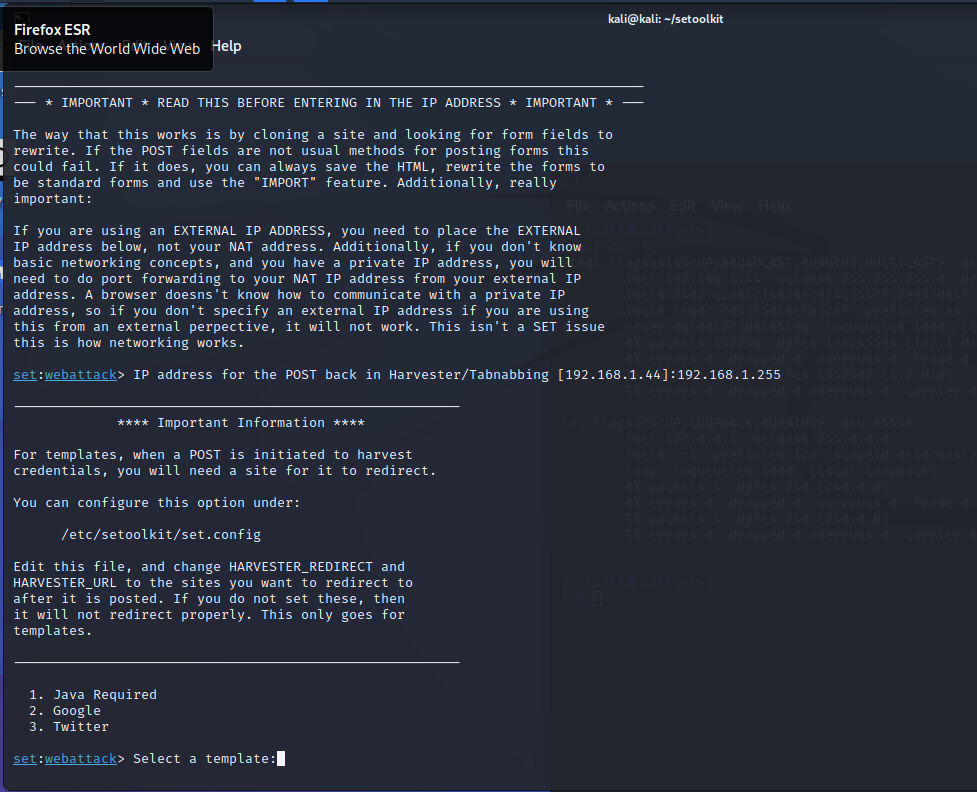
****

**Step 3: Open another terminal and find the ip address of the kali.**

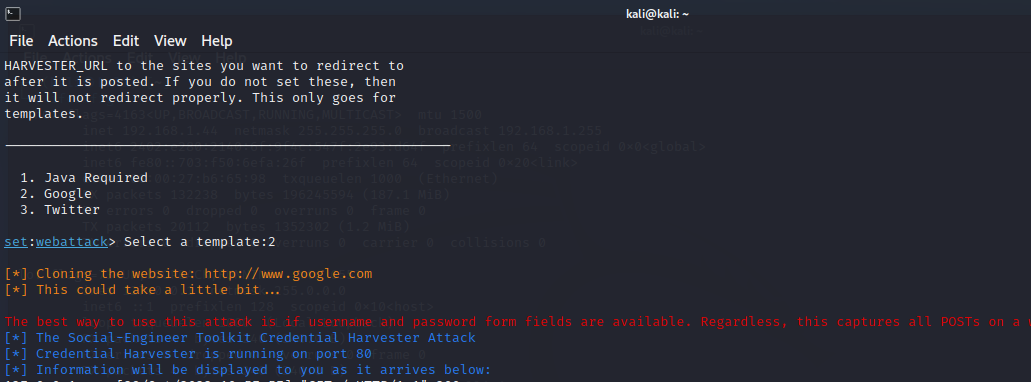
**Type command ifconfig.**

****

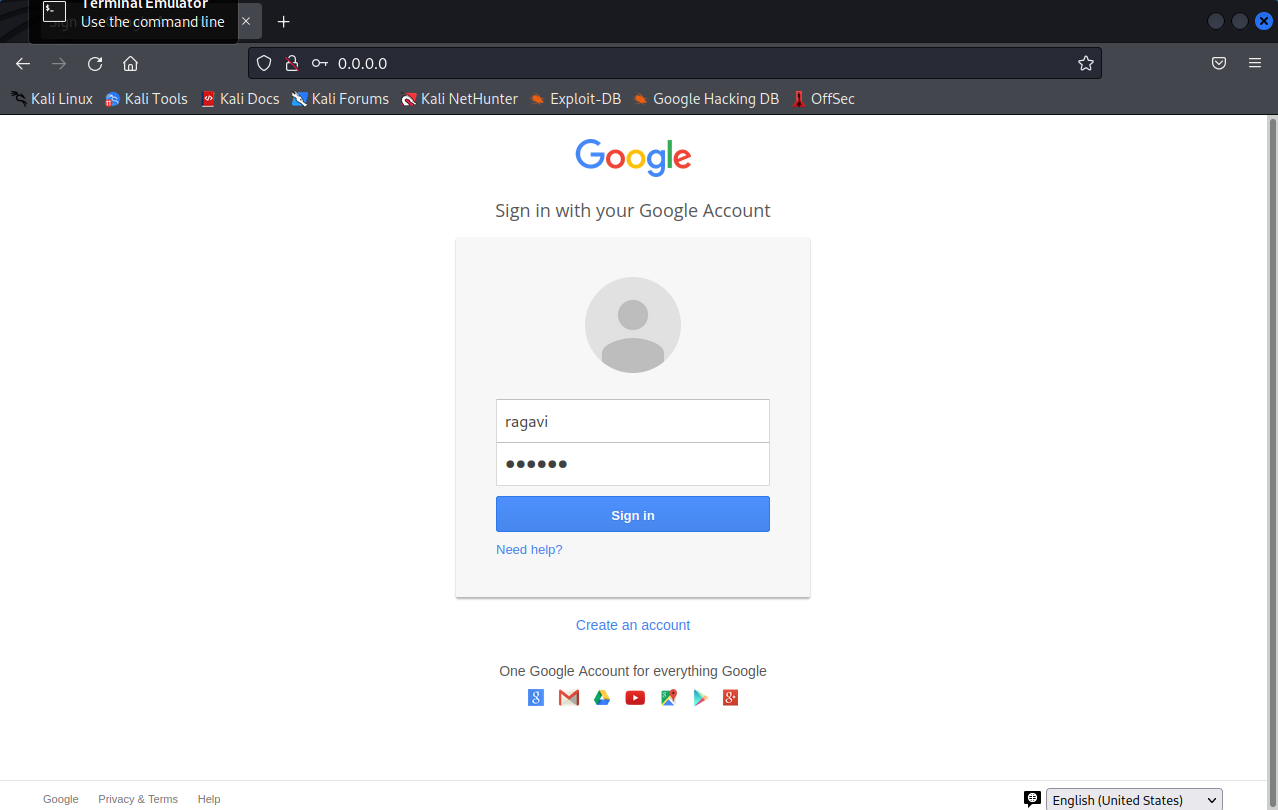
**Step 4: Now go to the previous terminal and type the ip address of kali .**

****

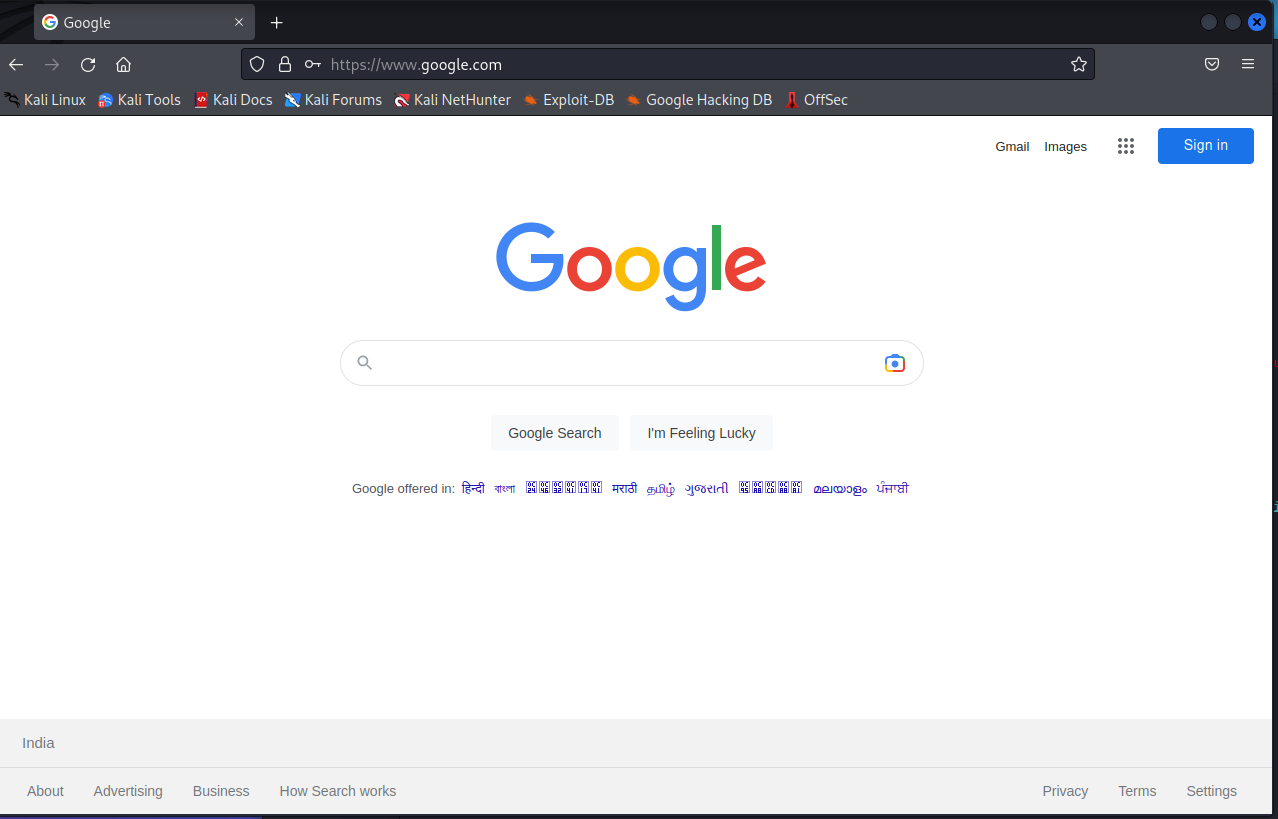
**select a template 2**

****

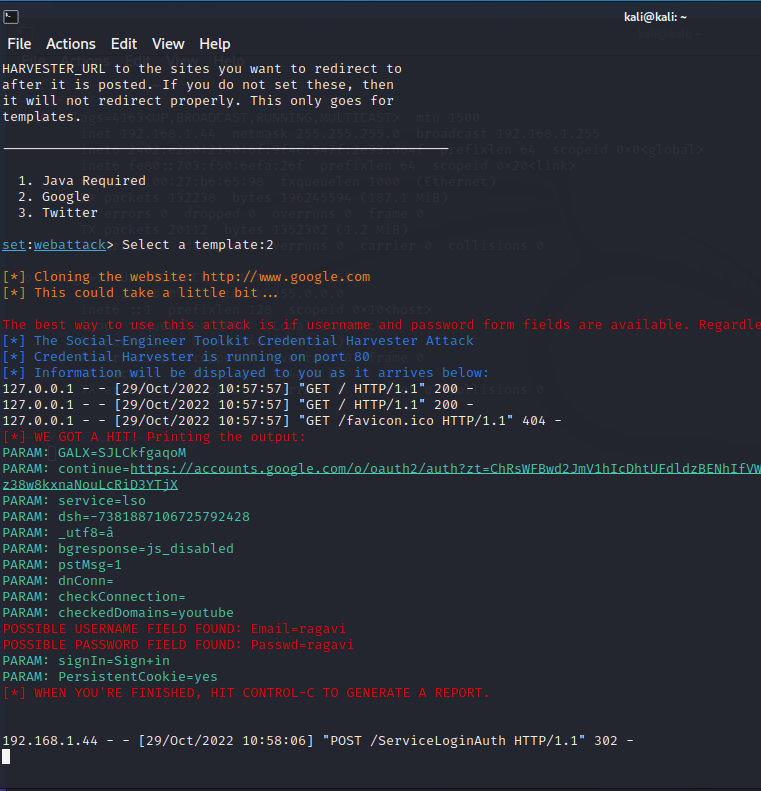
**Step 5: Now go to the browser in kali and type address 0.0.0.0:80 in the search bar and it will lead to the google sign in page.**

****

**Give some random username, password and sign in(which leads to google web page)**

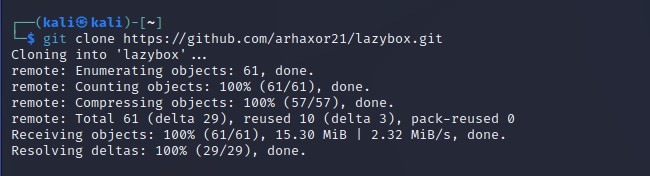
****

**Step 6: Now check terminal .**

****

**2.Installing lazybox:**

**Step1:** git clone <https://github.com/arhaxor21/lazybox.git>



**Step 2:** cd lazybox/

**Step 3:** chmod +x lazybox.sh

**Step 4:** ./lazybox.sh

