### ****Step 1: Set Up Your Virtual Lab****

Ensure you have a controlled environment where you can safely test phishing attacks.

* Install **Kali Linux** on a **Virtual Machine (VM)** (e.g., using VirtualBox or VMware). for this, I’m using a VMware with gnome extension
* Ensure you have internet access within your VM.

Update your system: sudo apt update && sudo apt upgrade -y

### ****Step 2: Install Social-Engineer Toolkit (SET)****

SET is a powerful tool for social engineering attacks like phishing, credential harvesting, and fake login pages.

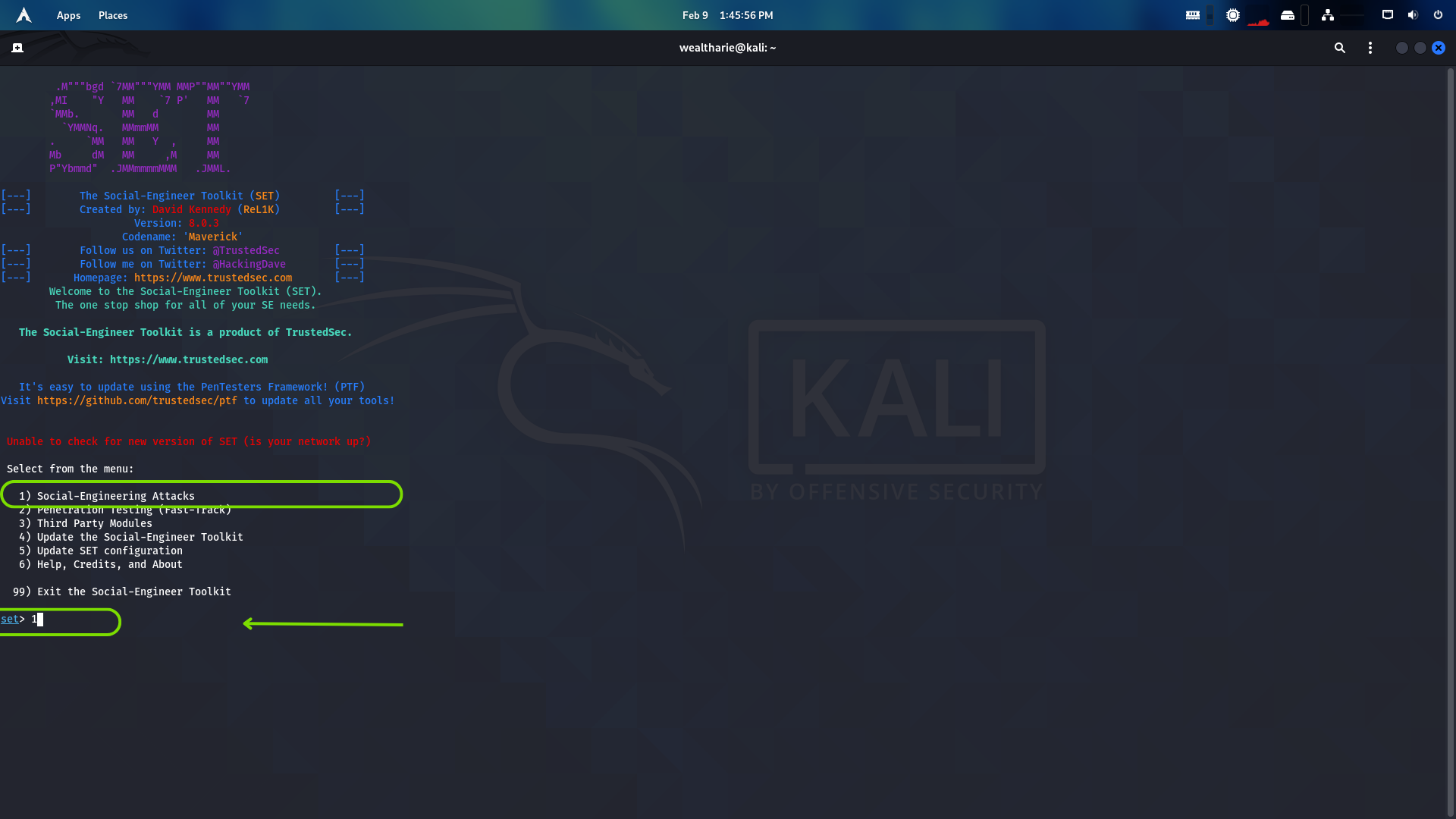
Install SET if it’s not already installed: sudo apt install setoolkit -y

Start SET: sudo setoolkit

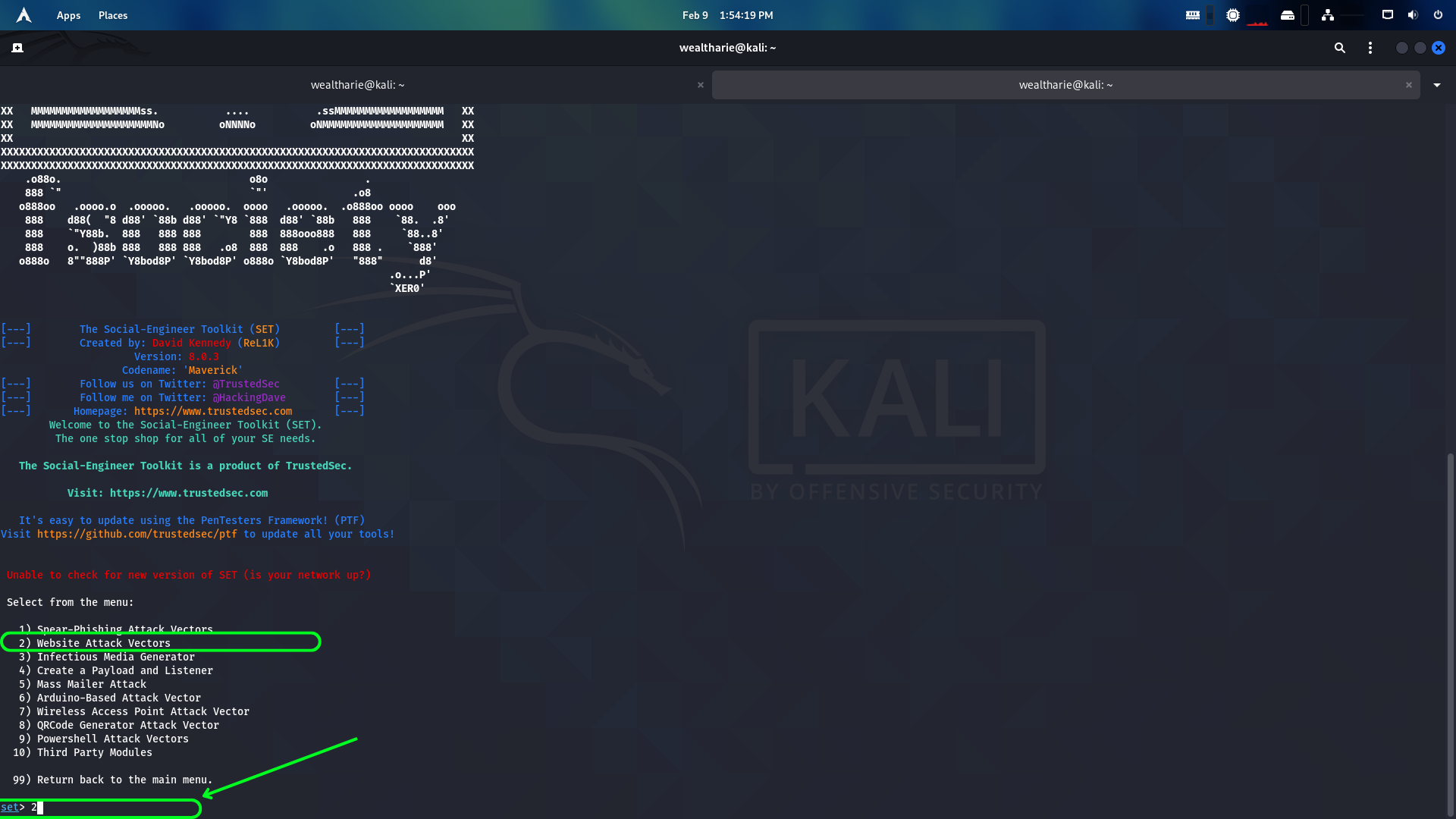
Accept the disclaimer when prompted.

### ****Step 3: Choose the Attack Type****

Inside SET, select “**Social Engineering Attacks”** by typing: 1



Then, choose “**Website Attack Vectors”**:



Now, select “**Credential Harvester Attack Method”**: by pressing 3, and press 1 for **“Web Templates”**



This method clones a website and captures login credentials entered on the fake page.

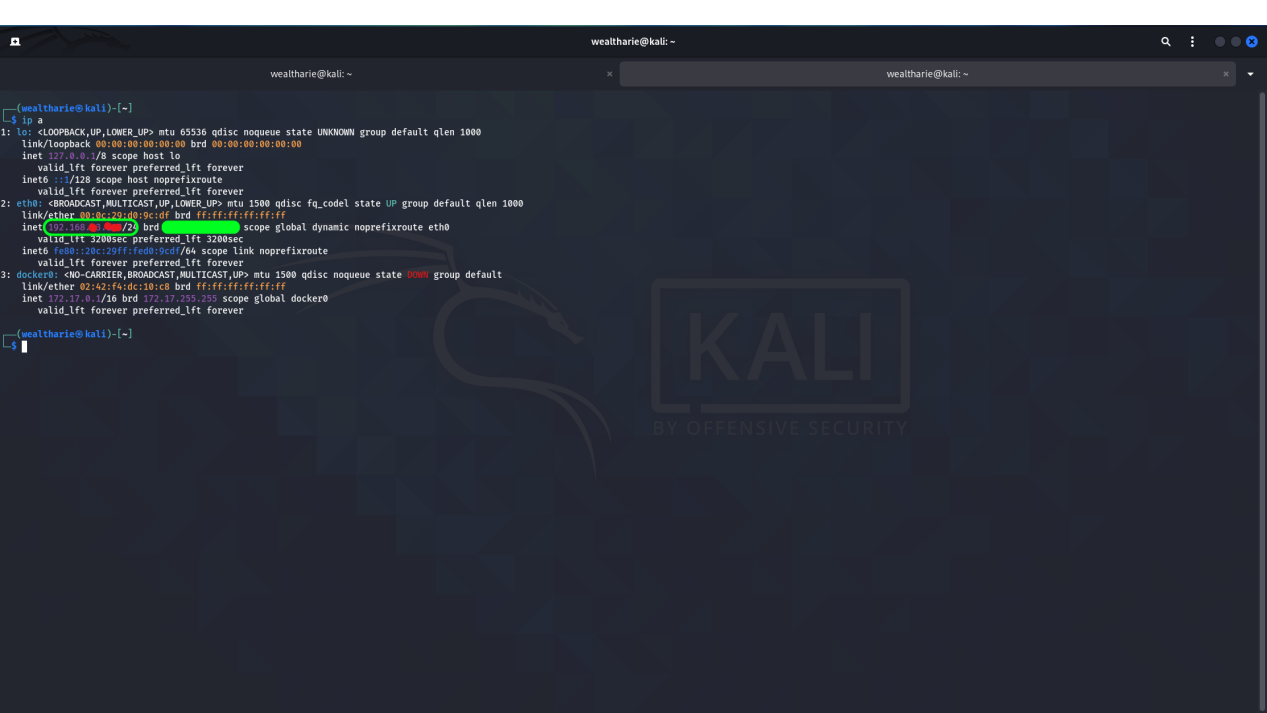
### ****Step 4: Select a Website to Clone****

SET allows you to clone a legitimate website for educational purposes, but for this case I wil be using the google web template or when prompted for the URL to clone, enter a test login page (e.g., a dummy site, not real websites like Facebook or Gmail). Example: plaintexthttps://testphp.vulnweb.com/login.php  
please do not try this ona website that you haven’t been authorized to hack!

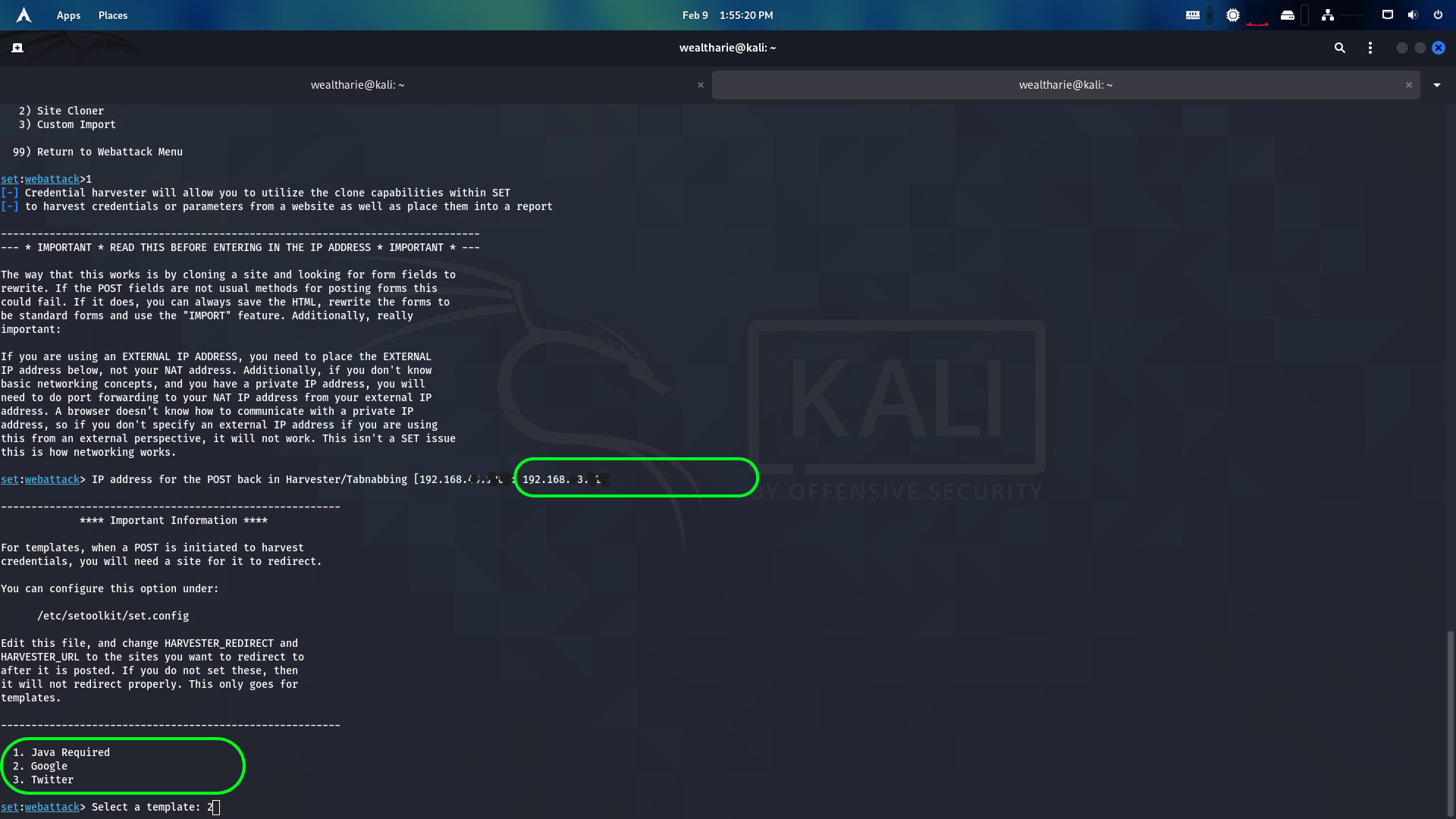
### ****Step 5: Set Up the Phishing Link****

Enter your local IP address for the listener (your **Kali VM’s IP**).  
Find your IP with:

ip a | grep inet



Example: If your IP is 192.168.1.100, enter it when prompted.



The type in the number to select your desired template, as for this case I will be using the google login page

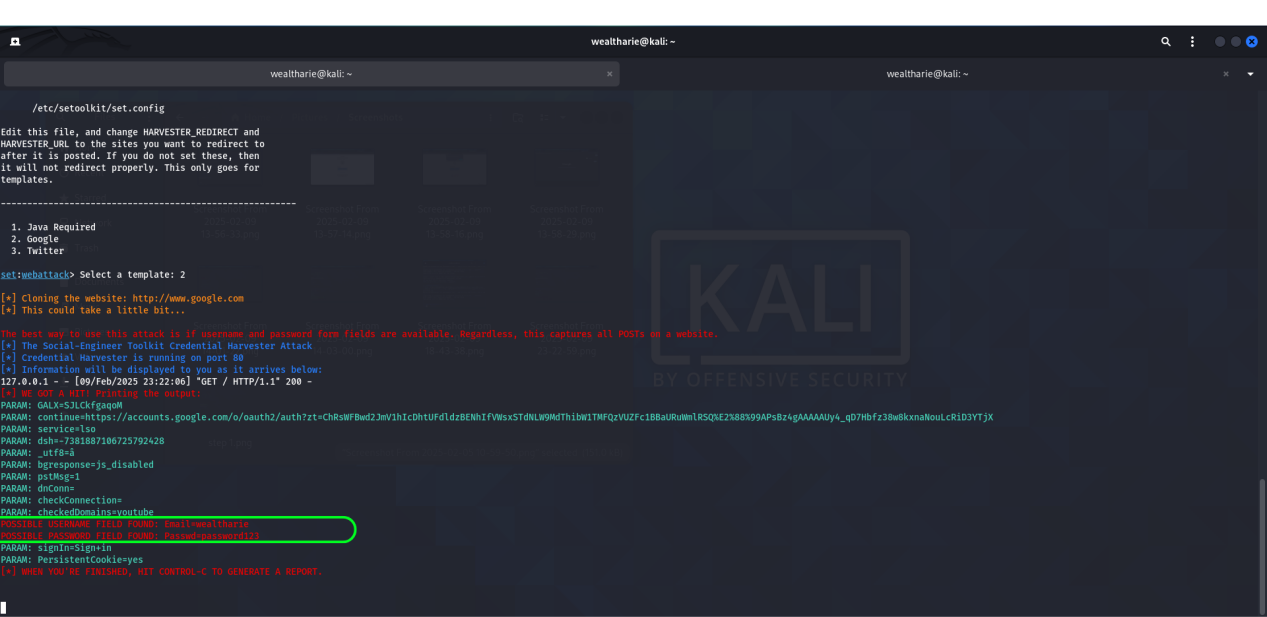
SET will now generate a fake login page that looks like the real one.

The link for the phishing page will be something like:

<http://192.168.1.100> be sure to chaange the ip address to that of your VMware or type in localhost in your browser.

### ****Step 6: Test the Phishing Page (Locally in Lab)****

* Open a browser inside your VM and visit the generated phishing link.
* Enter test credentials to see if SET captures them.



As you can see the login credentials have been successfully capture.

****Do not** deploy this outside your lab; real-world phishing without authorization is illegal**.