A Research Report on
Social Engineering Toolkit

Prepared by
Siva Krishna Siripurapu

Report on

Social Engineering Toolkit

4.SET TOOL KIT (SOCIAL ENGINEERING TOOLKIT):

The Social Engineering Toolkit (SET) is a powerful tool for penetration testers and security professionals to perform social engineering attacks, including phishing. Below is a detailed report on how to use the SET toolkit for automation tasks related to phishing, including an attack simulation and recommendations for protection against social engineering attacks.

Report on Phishing Attack Using SET Toolkit

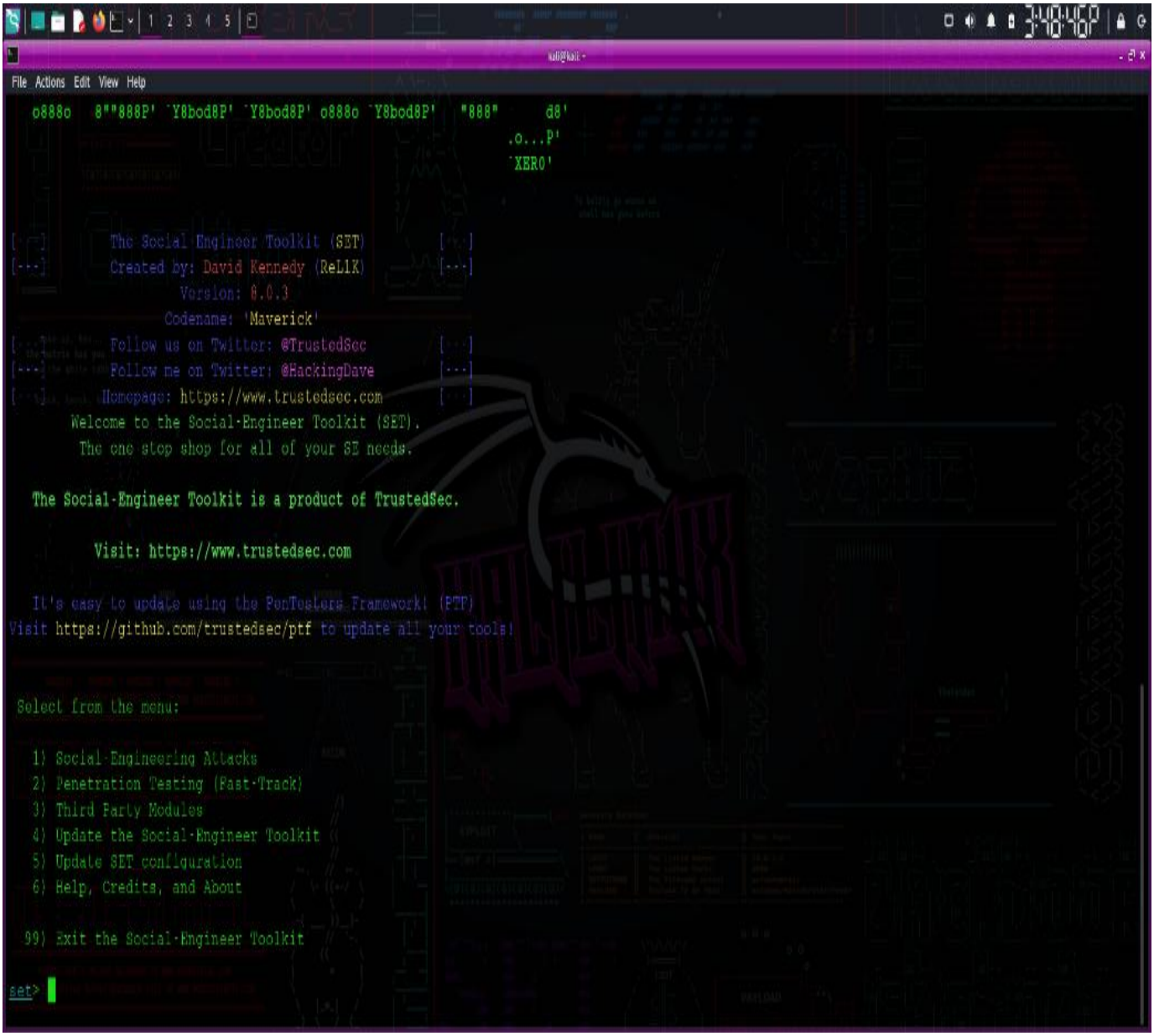
1. Overview of the Social Engineering Toolkit (SET)

SET is an open-source framework designed to facilitate social engineering attacks, allowing security professionals to test and assess their organization's vulnerability to such attacks. The toolkit can simulate various social engineering scenarios, including phishing, credential harvesting, and more.

2. Launching SET:

Start the SET toolkit by running the following command in the terminal:

sudo setoolkit



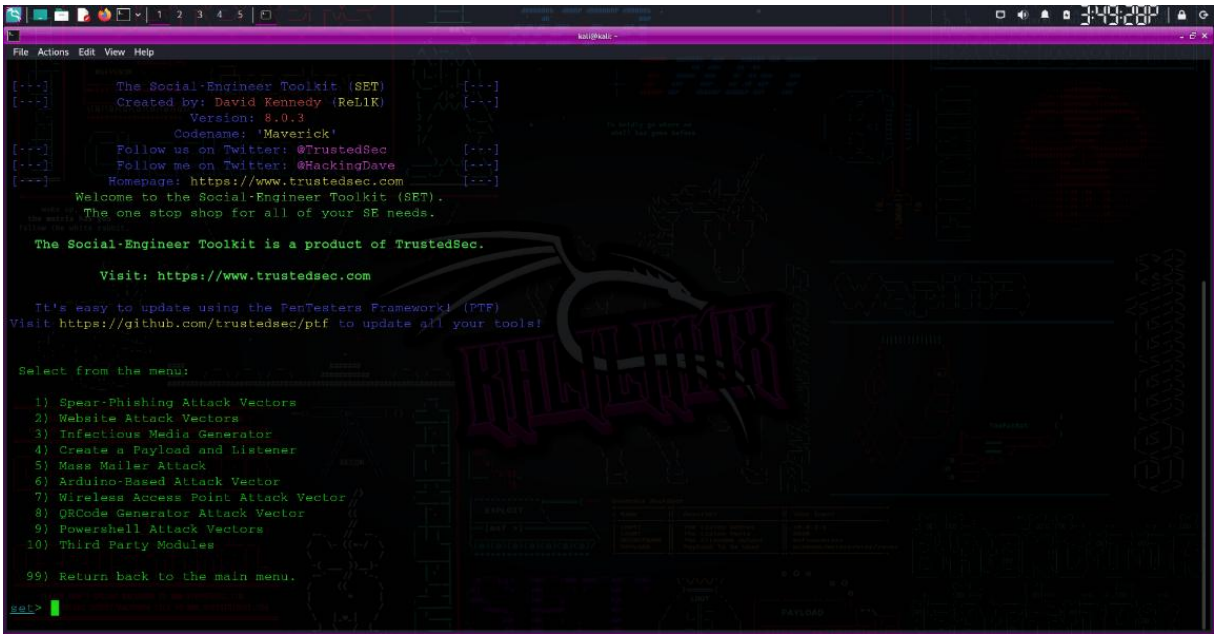
3. Performing a Phishing Attack

Here’s a step-by-step guide to performing a phishing attack using SET:

1. Select Attack Vector:

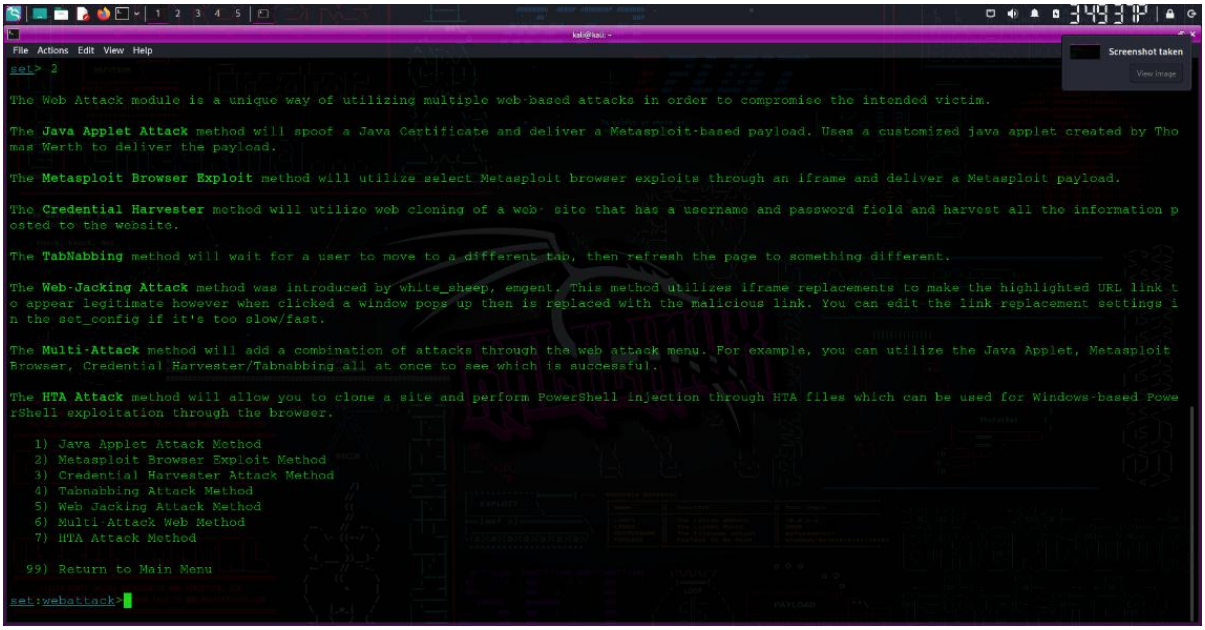
After launching SET, choose Social Engineering Attacks from the main menu.

Select Website Attack Vectors to proceed

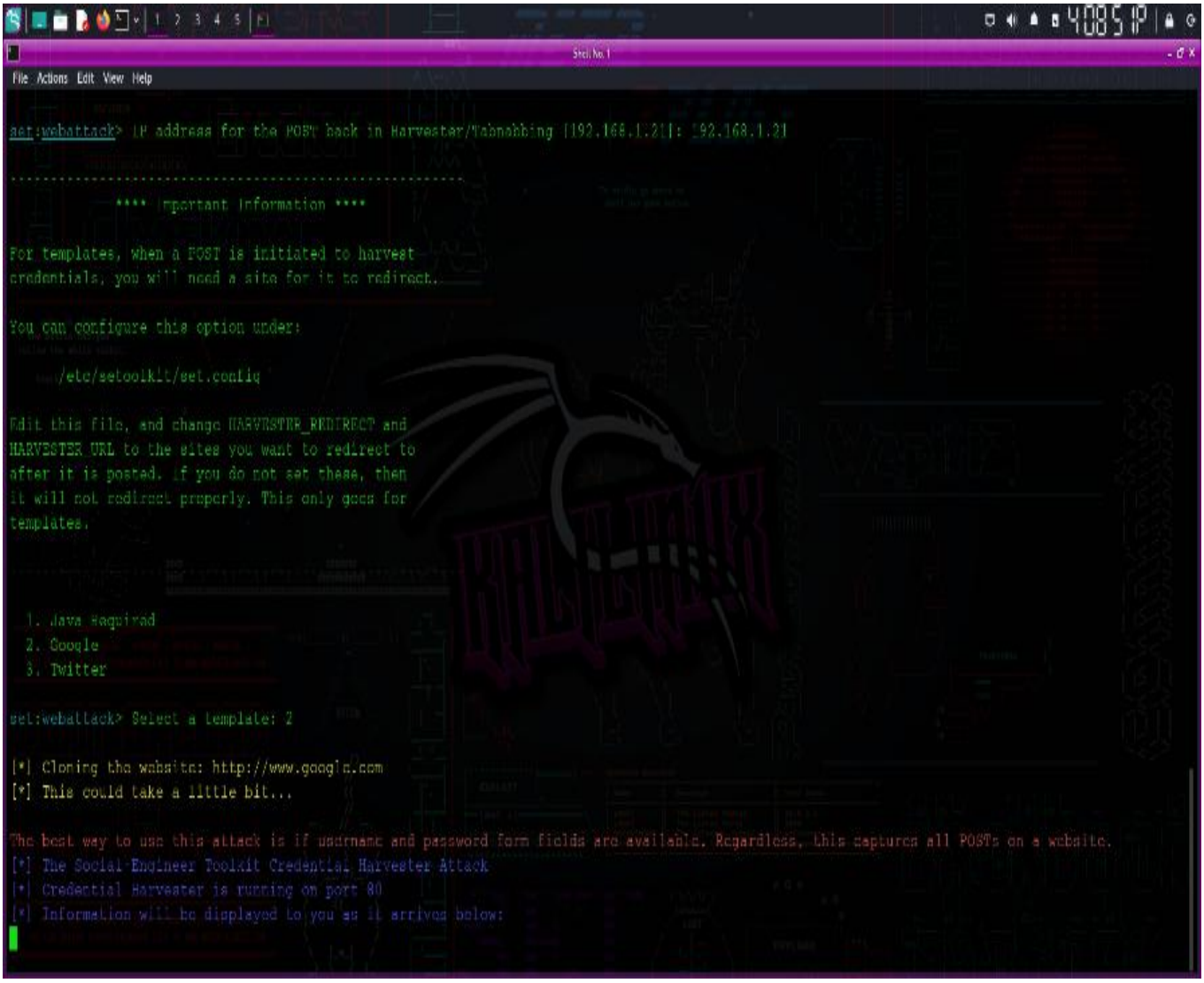


2. Choose the Phishing Method:

Select Credential Harvester Attack Method.



SET will ask for the URL of the legitimate site to clone (a Gmail login page for a service).



3. Setting Up the Attack:

SET will prompt you for the IP address (use your local IP) where the phishing page will be hosted.

Choose the option to use the built-in web server.

4. Customization:

Optionally, customize the phishing page using HTML to make it more convincing.

You can provide the text or any visual elements that mimic the original site.

5. Execution:

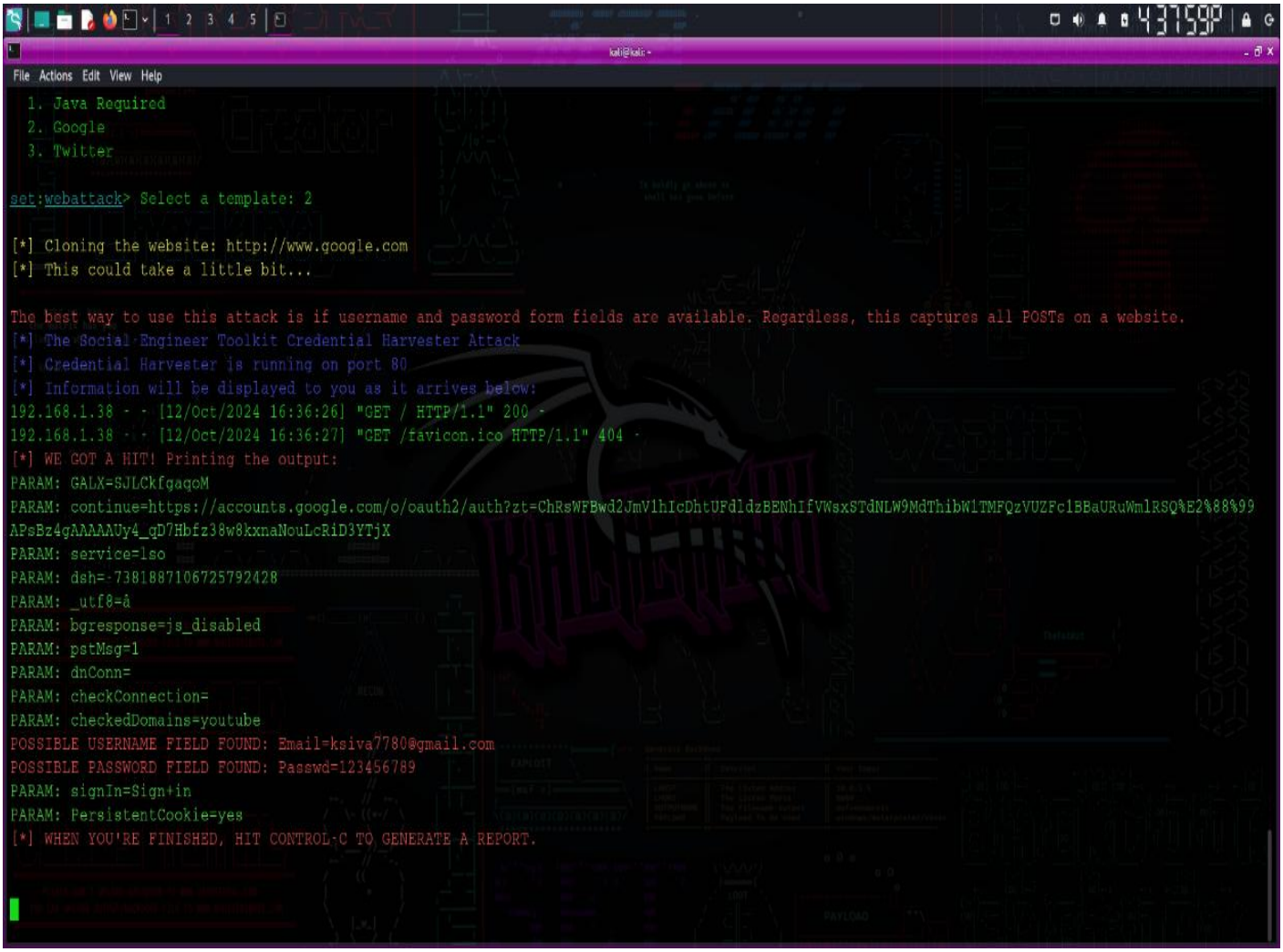
Once configured, SET will start the web server and provide you with the link to the phishing site.

Share the link with potential victims (via social engineering tactics like email or messaging).

6. Capturing Credentials:

When users enter their credentials on the phishing page, SET will log this information and display it in the terminal.

Monitor the terminal for captured usernames and passwords.



Reporting the Attack:

Details of the Attack:

12-10-2024 and4:37:59 PM of the attack

IP ADDRESS of the phishing site: 192.168.1.21

Number of credentials captured (including usernames and passwords): 1

Analysis:

Evaluate the effectiveness of the phishing attack.

Analyze how many users fell for the phishing attempt and any common patterns.

Protection from Social Engineering Attacks

To protect against social engineering attacks, including phishing, implement the following strategies:

1. User Education and Training:

Conduct regular training sessions for employees about recognizing phishing attempts and social engineering tactics.

Provide examples of phishing emails and suspicious links.

2. Email Filtering and Security Solutions:

Use email filtering solutions to detect and block phishing emails.

Implement multi-factor authentication (MFA) for all sensitive accounts.

3. Regular Security Audits:

Conduct periodic security audits and phishing simulations to assess employee readiness

Review and update security policies regularly.

4. Incident Response Plan:
Establish an incident response plan for reporting and responding to phishing attempts.
Encourage users to report suspicious emails or messages immediately.
5. Secure Browsing Practices:
Educate users on secure browsing practices, such as verifying URLs and avoiding clicking on unknown links.
6. Conclusion
The SET toolkit is an effective method for simulating phishing attacks and understanding the vulnerabilities within an organization. By actively testing and implementing protective measures against social engineering attacks, organizations can enhance their overall security posture and minimize the risks associated with these types of threats.
Appendices
Captured Credentials:
Username: ksiva7780@gmail.com
Password: 123456789