**CYBER SECURITY WITH TECHSAMMY: EMAIL PHISHING (SOCIAL ENGINEERING)**

**Social Engineering Toolkit (SET) and Email Phishing on Kali Linux**

Email phishing is a common social engineering technique used to deceive individuals into providing sensitive information such as passwords, credit card numbers, or personal identification numbers. Tools like the Social Engineering Toolkit (SET) on Kali Linux provide a structured approach to creating and deploying phishing attacks. Here’s a step-by-step guide to conducting an email phishing attack using SET and measures to mitigate such threats.



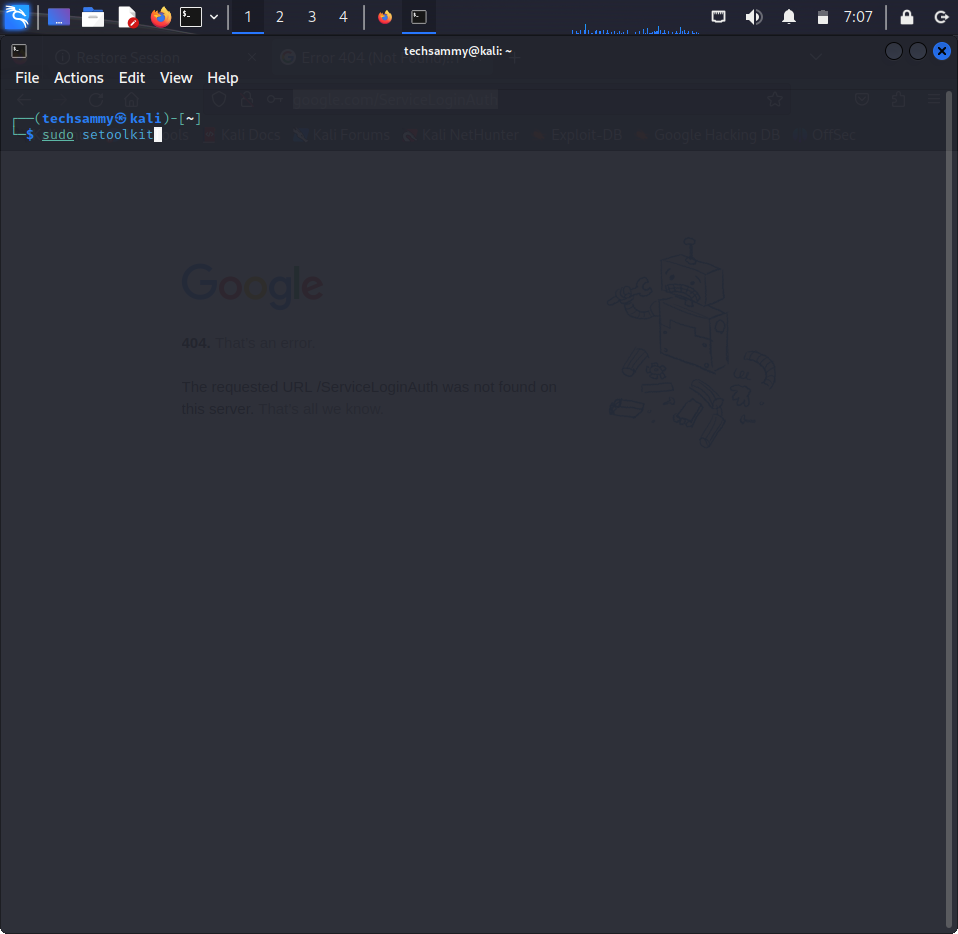
**Step-by-Step Guide to Email Phishing Using SET**

**Setup and Launch SET:**

1. **Install Kali Linux:** Ensure you have a Kali Linux environment ready, either on a physical machine or a virtual machine.

**Open Terminal:** Launch the terminal in Kali Linux.

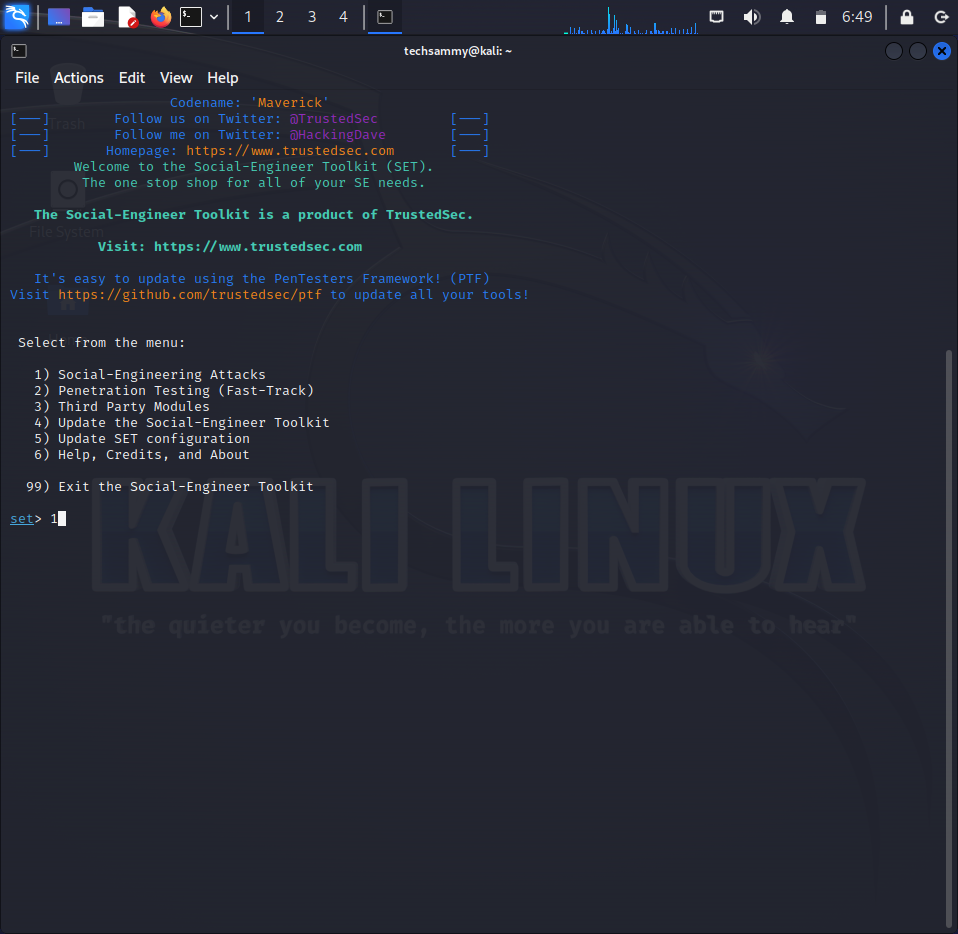
**Start SET:** Type setoolkit in the terminal and press Enter. This command starts the Social Engineering Toolkit.



1. **Navigate SET Menu:**

**Select Social-Engineering Attacks:** In the SET main menu, choose option 1 for Social-Engineering Attacks.

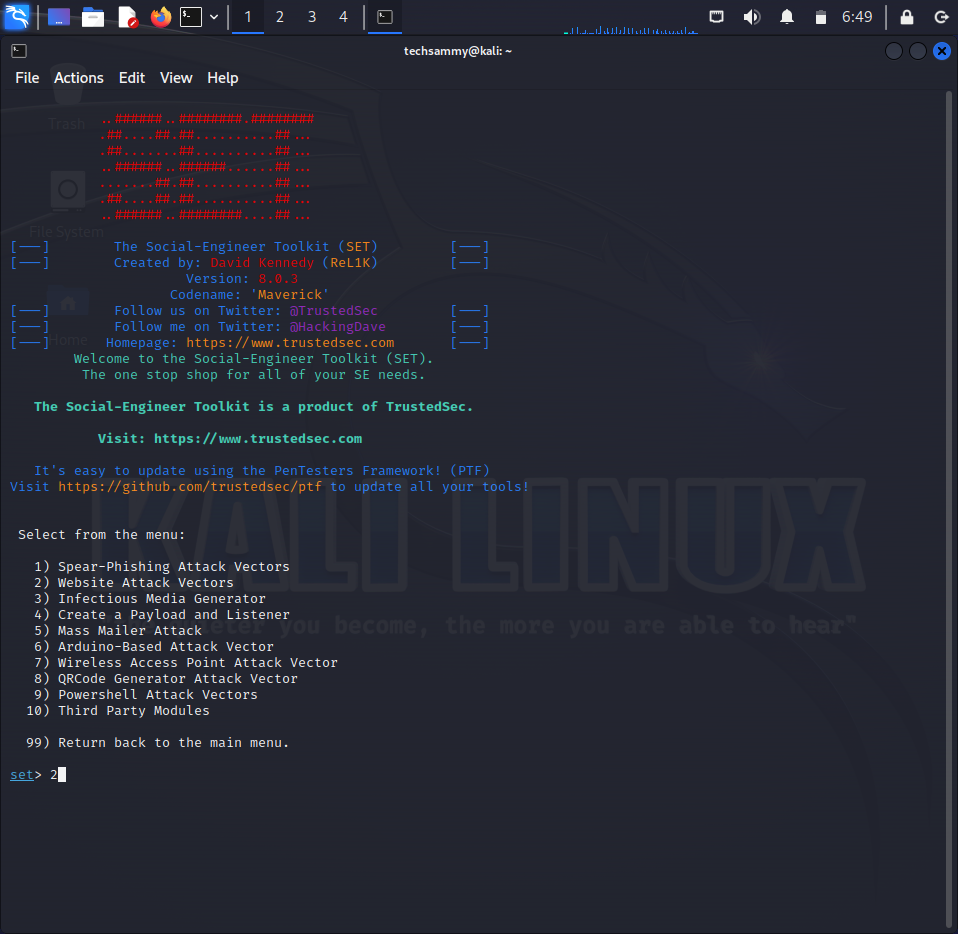
Choose the Type of Attack: Next, select 1 for Spear-Phishing Attack Vectors

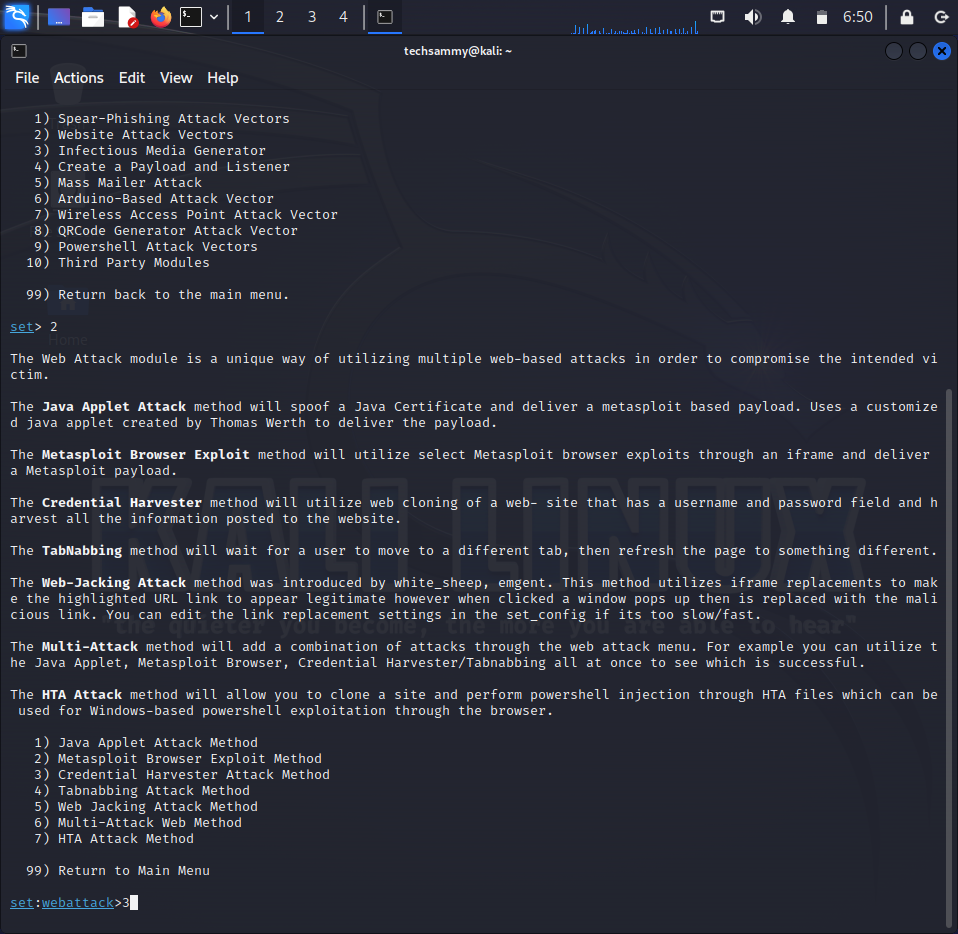


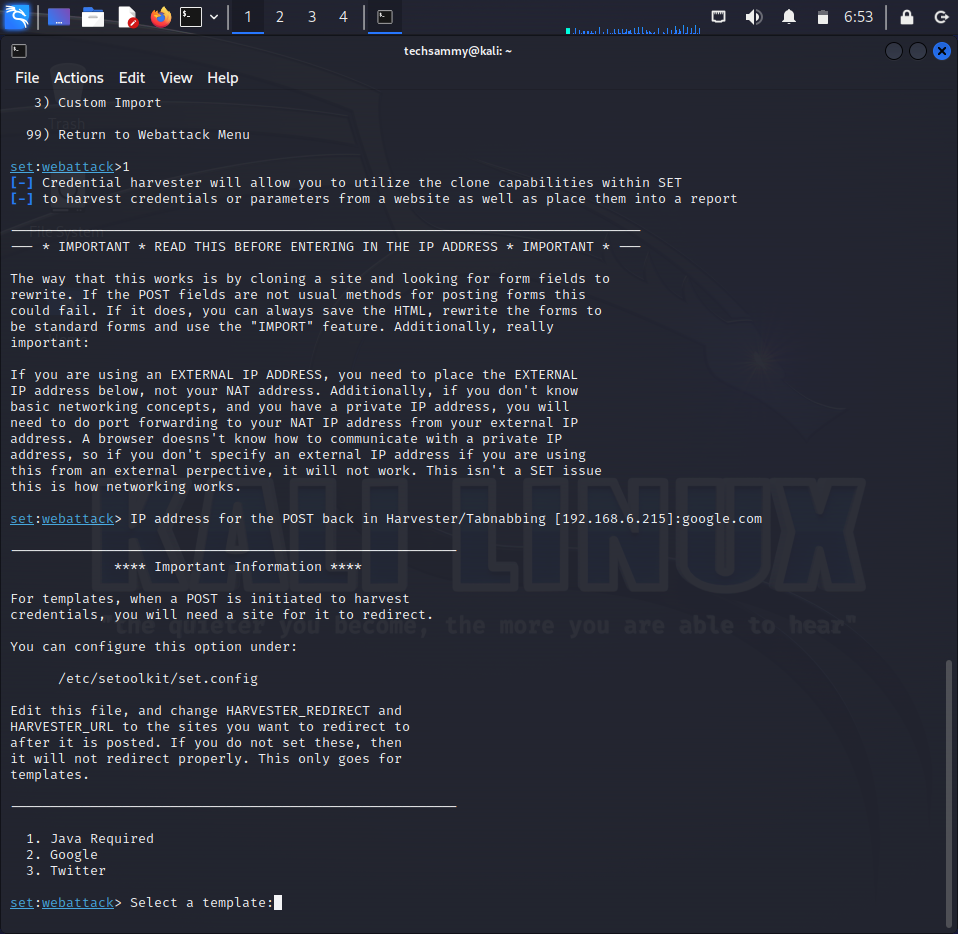
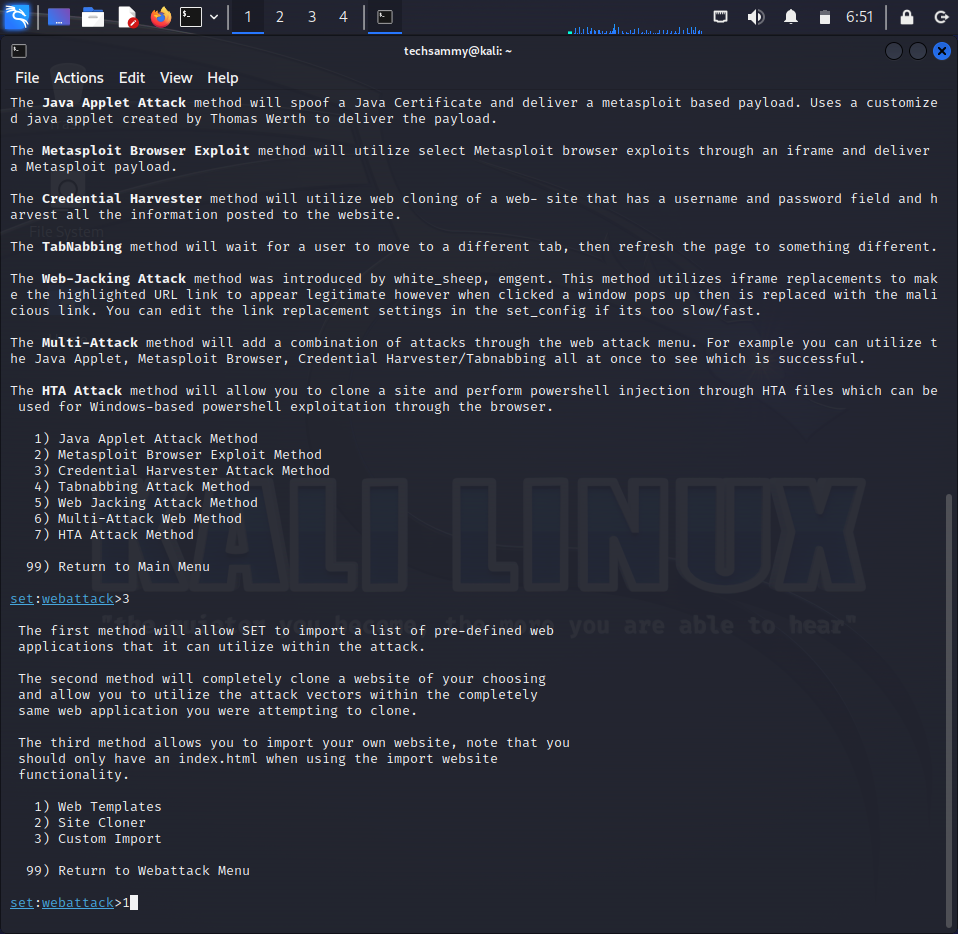
1. **Setup the Email Attack:**

Website attack vector: Choose option for Perform an Email Attack.

Choose an Email Template: SET provides several templates. Select a relevant phishing email template. For example, choose 1 for the Credential Harvester Attack method.



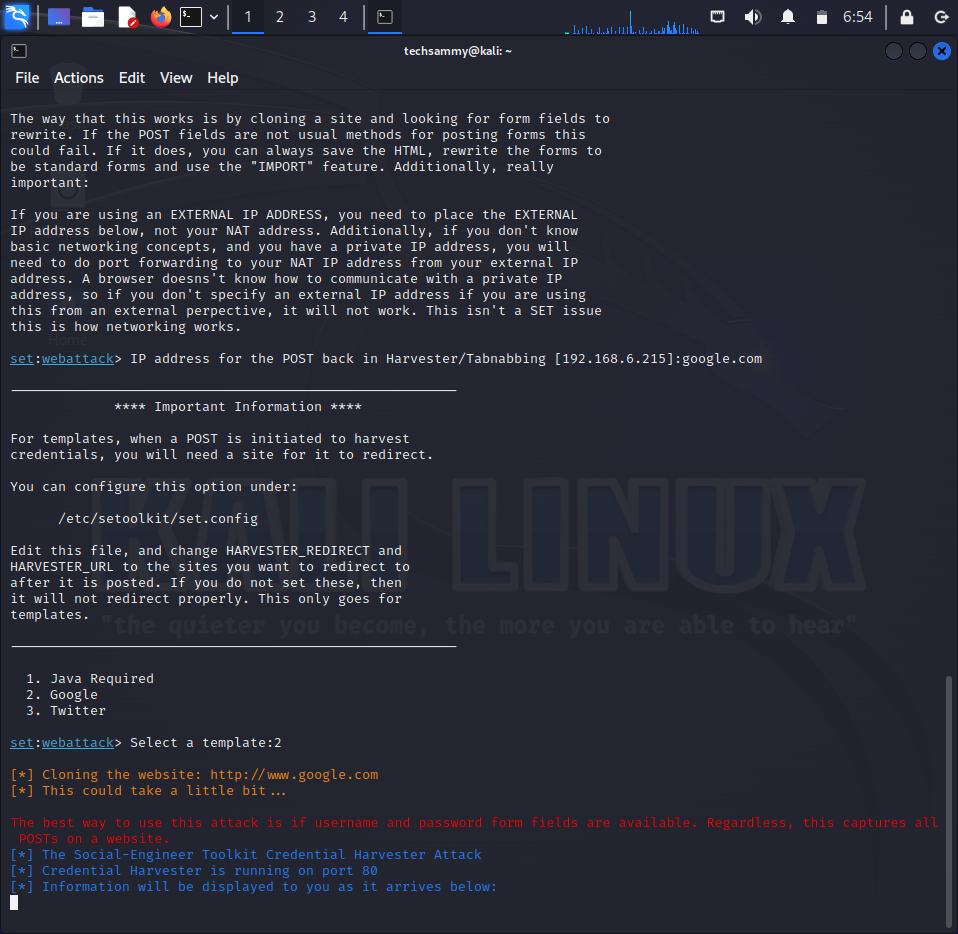


Credential harvesting is a common technique used in phishing attacks to capture usernames and passwords from unsuspecting users. The Social Engineering Toolkit (SET) in Kali Linux provides an easy-to-use framework to create and deploy such attacks. Below, we’ll explore how to use SET for credential harvesting and discuss steps to protect against such threats.

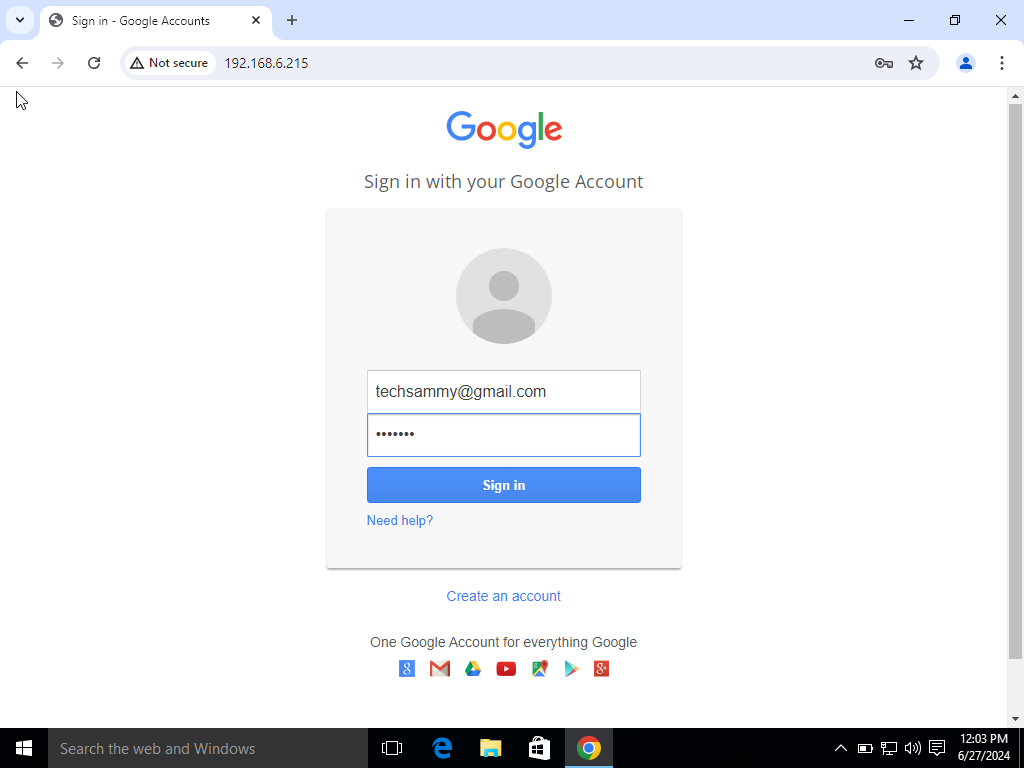
1. **Define the Recipients:**

Specify Target Email Addresses: Enter the target email addresses. You can send to multiple addresses by separating them with commas.

1. **Launch the Attack:**

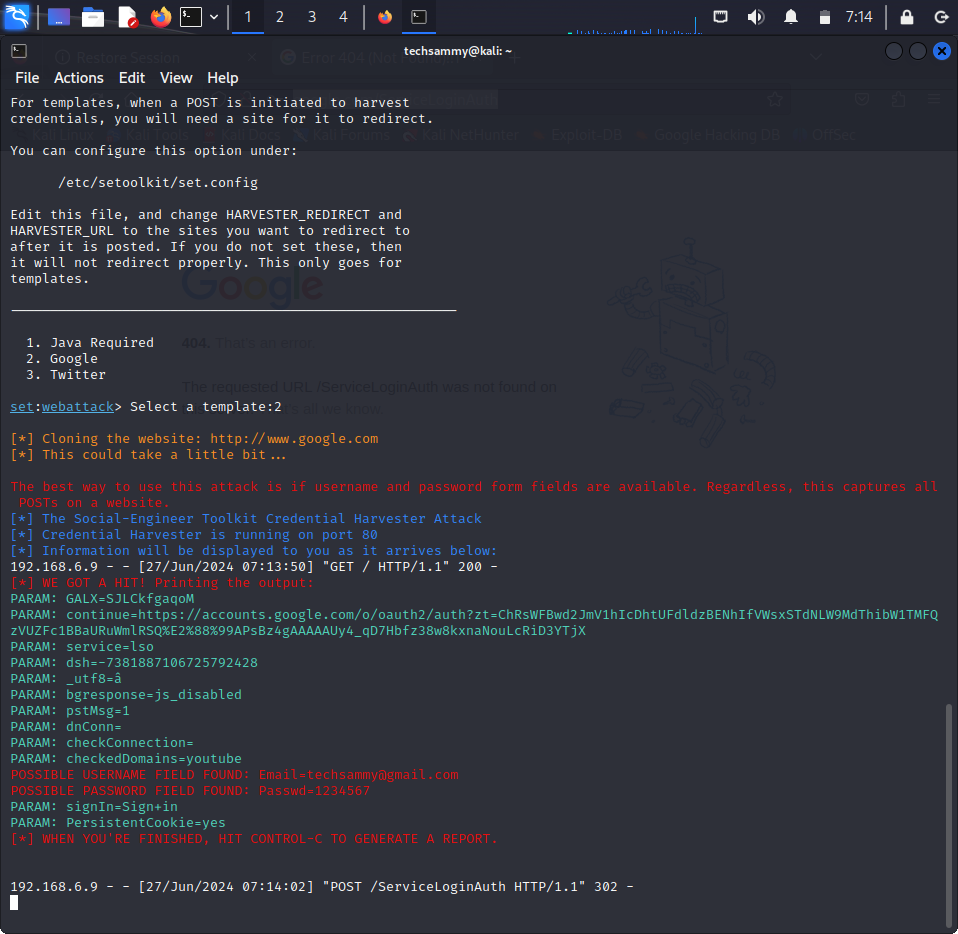
****

**Send the Phishing Email:** Once all configurations are done, SET will send the crafted email to the specified recipients.



To capture credentials using SET, clone the target website and host it on your Kali Linux IP. Send this IP link in a deceptive email. As victims enter their credentials, they’ll instantly appear in your Kali Linux terminal.

**Monitor the Results:** The email will contain a link to the malicious payload or a credential-harvesting page. When a recipient clicks the link and provides their information, SET will capture the credentials.



**Remediation and Employee Awareness**

Phishing attacks are prevalent, and organizations must take steps to protect themselves. Here are key measures to mitigate phishing threats and improve cybersecurity awareness among employees:

1. **Employee Training and Awareness:**

Regular Training Sessions: Conduct frequent cybersecurity training sessions to educate employees about the risks of phishing and how to identify suspicious emails.

Phishing Simulations: Perform regular phishing simulations to test employees' ability to recognize and report phishing attempts. This can reinforce training and highlight areas needing improvement.

1. **Email Filtering and Protection:**

Spam Filters: Implement advanced spam filters to detect and block phishing emails before they reach employees’ inboxes.

Email Authentication Protocols: Use protocols like SPF, DKIM, and DMARC to prevent spoofed emails from being delivered.

1. **Encouraging Vigilance and Reporting:**

Suspicious Email Protocol: Establish a clear protocol for employees to report suspicious emails. Encourage employees to forward such emails to the IT department for further analysis.

No Click Policy: Advise employees not to click on links or open attachments from unknown or unexpected sources

1. **Technical Measures:**

URL Filtering: Implement URL filtering to block access to known malicious websites.

Antivirus and Endpoint Protection: Ensure all devices have up-to-date antivirus and endpoint protection software to detect and block malware.

1. **Secure Password Practices:**

Password Policies: Enforce strong password policies requiring complex and unique passwords for different accounts.

Multi-Factor Authentication (MFA): Enable MFA wherever possible to provide an additional layer of security beyond just a password.

1. **Incident Response Plan:**

Establish Response Procedures: Develop and regularly update an incident response plan that outlines steps to take in the event of a phishing attack.

Regular Drills: Conduct drills to ensure that the response plan is effective and that employees know their roles during a phishing incident.

1. **Monitoring and Detection:**

Network Monitoring: Use network monitoring tools to detect unusual activity that may indicate a phishing attempt or compromised credentials.

Log Analysis: Regularly review system and security logs to identify any anomalies that could signify a security breach.

**Conclusion**

Phishing attacks continue to evolve, becoming more sophisticated and harder to detect. Tools like SET allow security professionals to understand and demonstrate these tactics for training and awareness purposes. By combining technical defenses, employee education, and vigilant monitoring, organizations can significantly reduce their risk of falling victim to phishing attacks. It's crucial to foster a security-conscious culture where every employee plays a part in protecting the organization's assets and data.

**Contact Information for Tech Support and Inquiries**

If you need assistance with technical issues, have any questions, or want to discuss collaboration opportunities, please feel free to reach out to me. You can contact me through any of the following channels:

Email: techsammy50@gmail.com

Phone: +2348060590922

Instagram: @techsamm\_y

Twitter: @samuel\_aigberua

Looking forward to connecting with you!