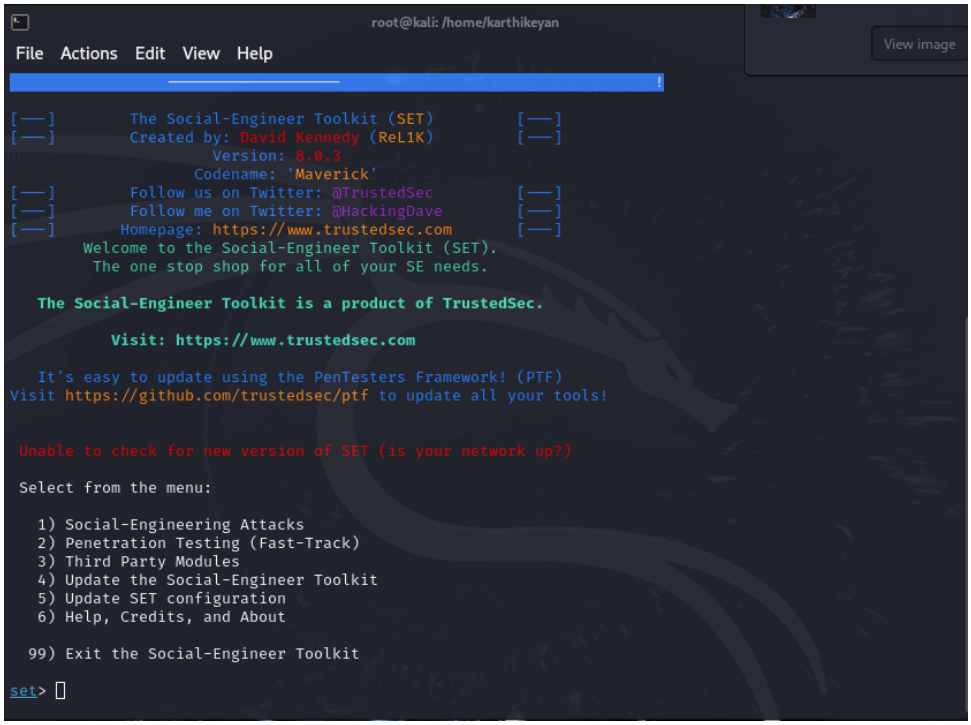
Assignment - 10

Karthikeyan G
Roll No: CB.SC.P2CYS24008

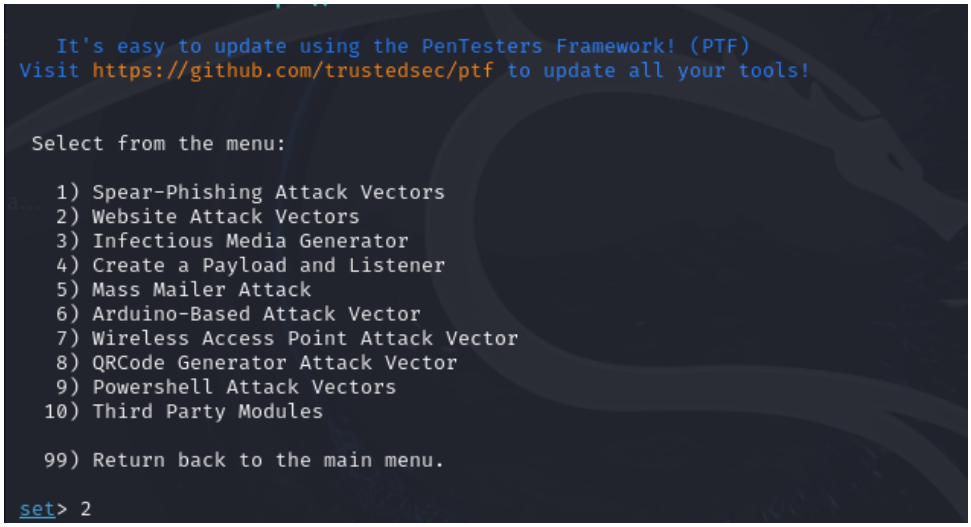
March 28, 2025

1 Exploring the SEToolkit for Social Engineering Attacks

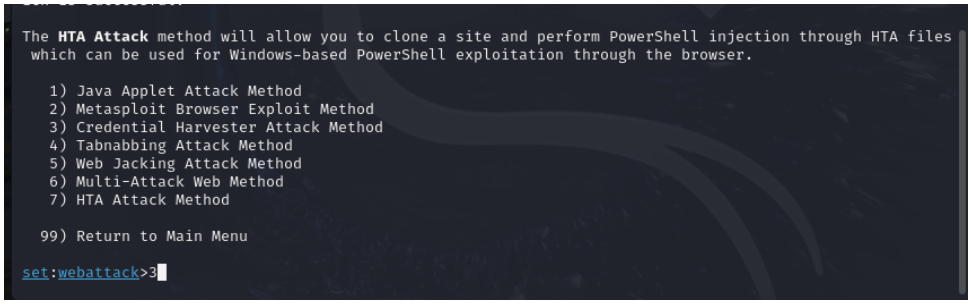
- Social-Engineering Attack is selected.



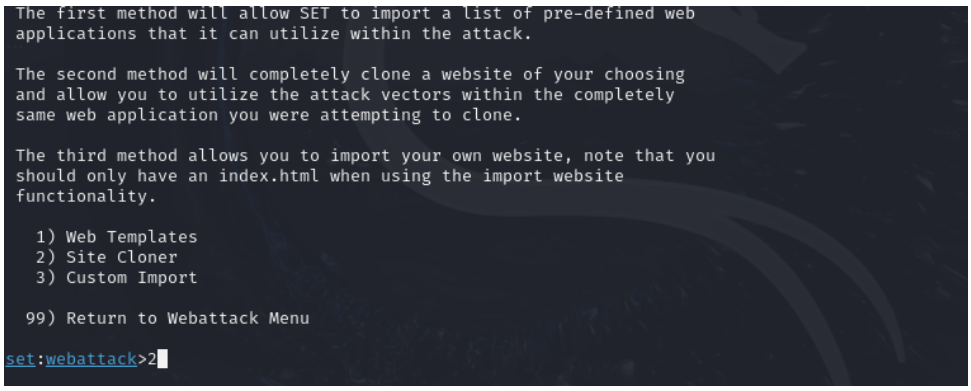
- Website Attack Vectors are chosen.



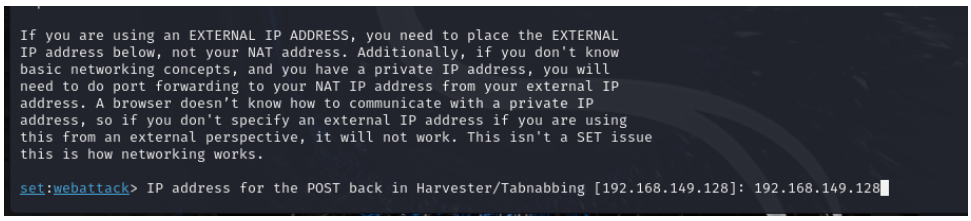
- Credential Harvester Attack is attempted.



- Site Cloner option is selected.



- IP address of the host system (for credential retrieval) is provided.



- Target credential site is specified.

- After this step, an attempt was made to clone the website using the SEToolkit's Credential Harvester Attack. The URL was provided correctly, and the cloning process was initiated. However, despite multiple attempts, the cloned website did not function as expected. Various troubleshooting methods were applied, including:
  - Checking for conflicting services such as Apache or NGINX running on port 80 and stopping them using 'sudo systemctl stop apache2' or 'sudo systemctl stop nginx'.
  - Attempting to bind the Credential Harvester to an alternative port, such as 8080, by setting 'set PORT 8080' in SEToolkit.
  - Verifying network connectivity by checking firewall settings and temporarily disabling 'ufw' using 'sudo ufw disable'.
  - Ensuring that the cloned website was accessible by trying to open it from a browser on the attacker's machine as well as a remote victim machine.
  - Reinstalling SEToolkit and its dependencies using 'sudo apt update sudo apt install set' to rule out missing packages or corrupted installations.

  Despite these efforts, the website cloning process failed, and the expected phishing page did not load correctly. The issue remains unresolved and may require further debugging or an alternative approach.