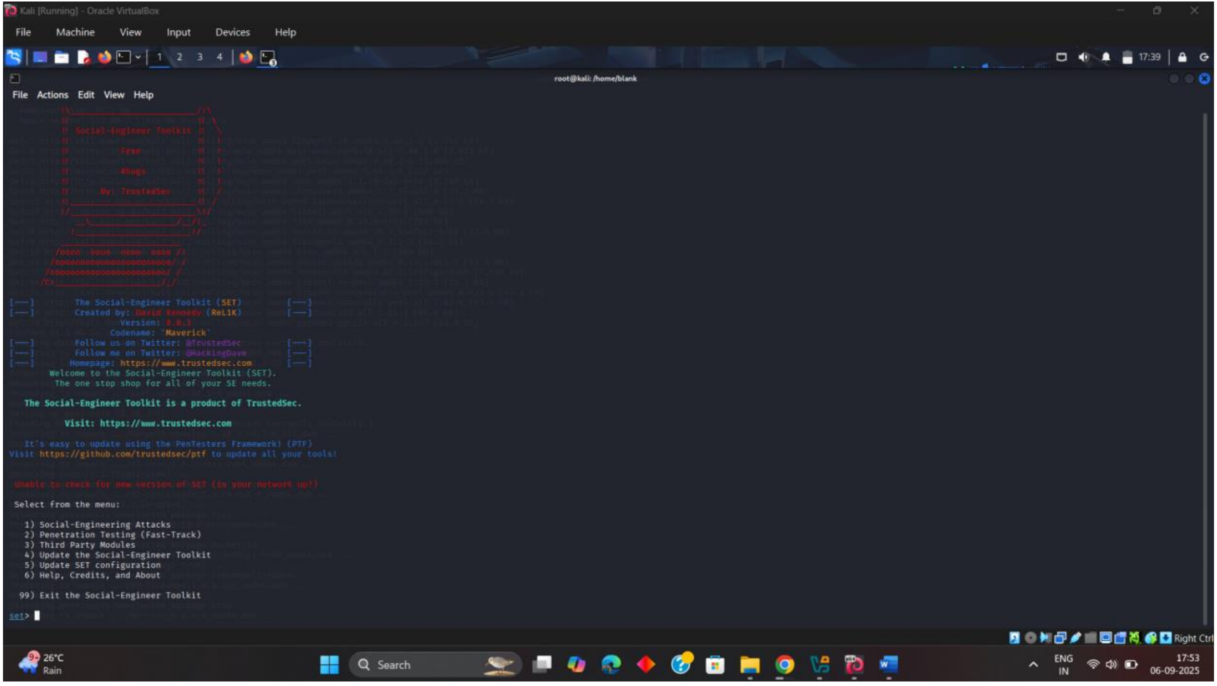
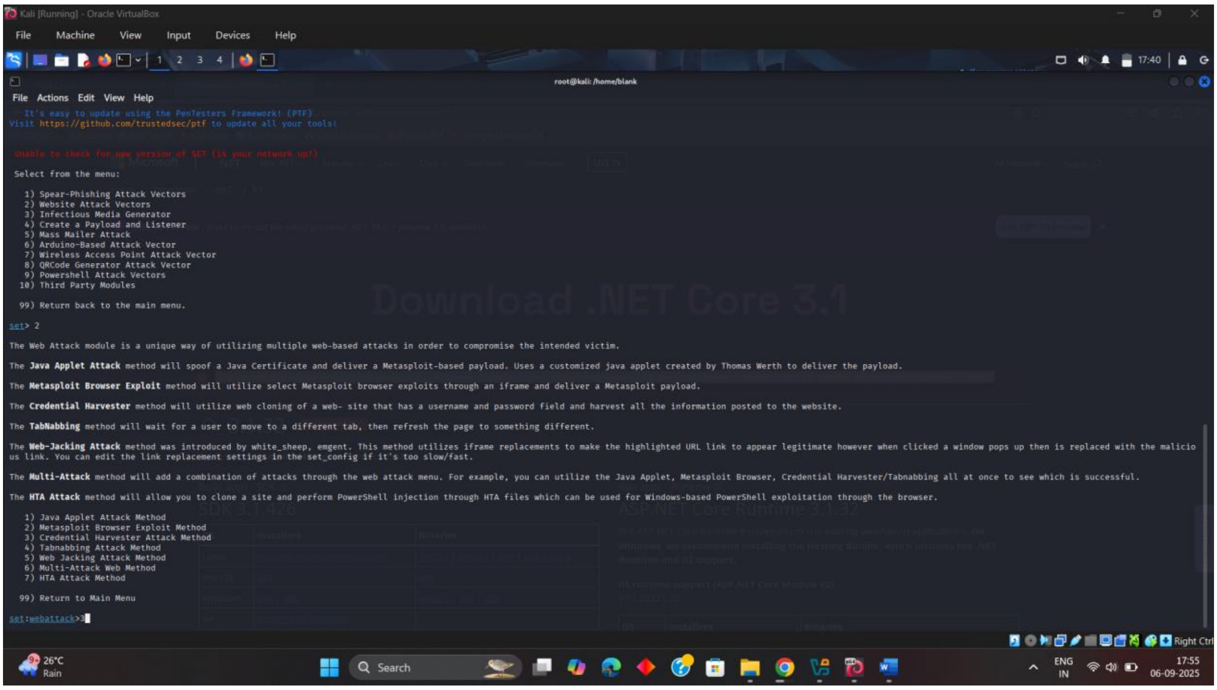
5. Social Engineering Lab

Activities:

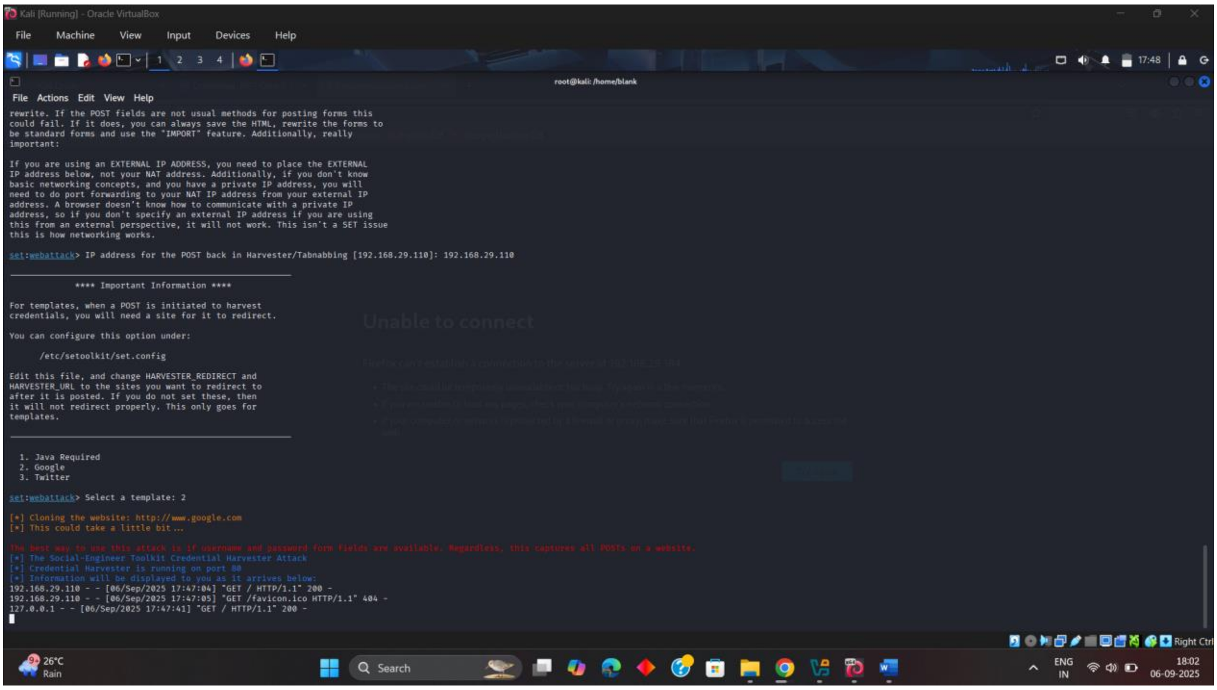
- **Tools:** SET, PhoneInfoga, Maltego.
- **Tasks:** Simulate a vishing or pretexting scenario, gather target intel.
- **Brief:**
- Intel Gathering: Use PhoneInfoga to collect target phone data; map relationships in Maltego.


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
17:39
root@kali: /home/blank
File Actions Edit View Help
26°C
Rain
Search
ENG
IN
17:53
06-09-2025

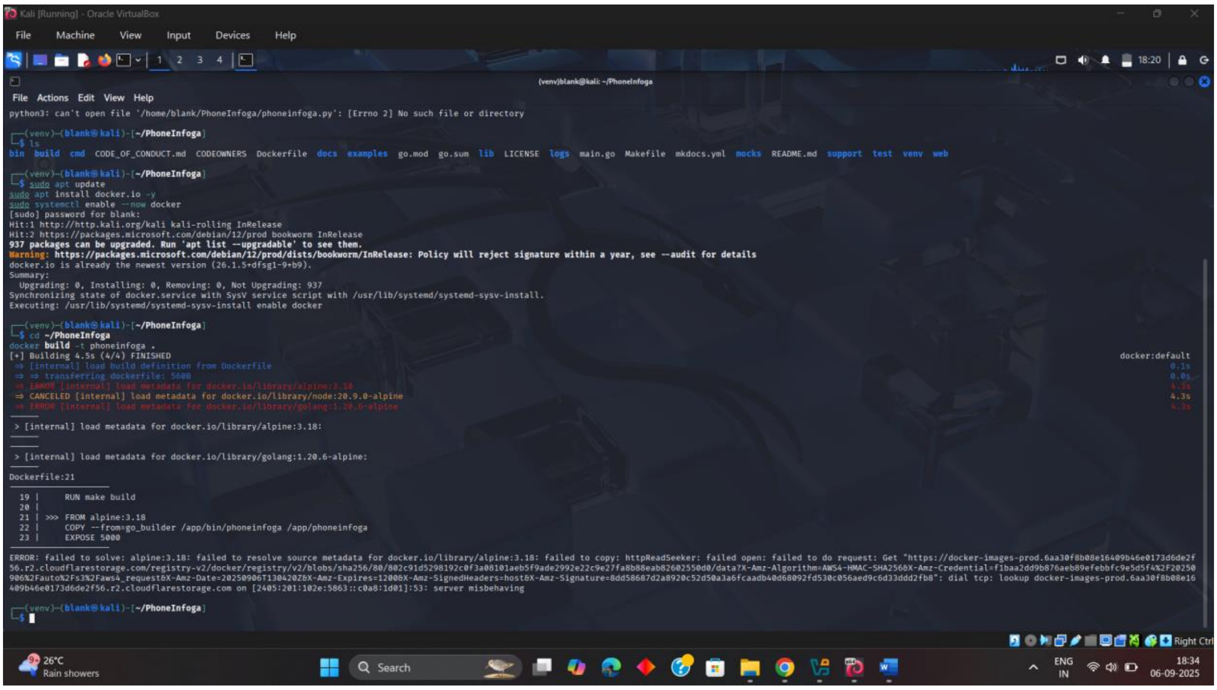
```
              Social-Engineer Toolkit

                      Free

                      #hugs

                 By: TrustedSec

[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                      Version: 8.0.3
                    Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       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!


 Unable to check for new version of SET (is your network up?)

 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> 
```


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
17:40
root@kali: /home/blank
File Actions Edit View Help
26°C
Rain
Search
ENG
IN
17:55
06-09-2025

```
   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Unable to check for new version of SET (is your network up?)

 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

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.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicio
us link. You can edit the link replacement settings in the set_config if it's 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
```


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@kali: /home/blank
File Actions Edit View Help
Unable to connect
26°C
Rain
Search
ENG
IN
18:02
06-09-2025
Right Ctrl

```
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 [192.168.29.110]: 192.168.29.110

 ─────────────────────────────────────────────────────────
             **** 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:
192.168.29.110 - - [06/Sep/2025 17:47:04] "GET / HTTP/1.1" 200 -
192.168.29.110 - - [06/Sep/2025 17:47:05] "GET /favicon.ico HTTP/1.1" 404 -
127.0.0.1 - - [06/Sep/2025 17:47:41] "GET / HTTP/1.1" 200 -
█
```

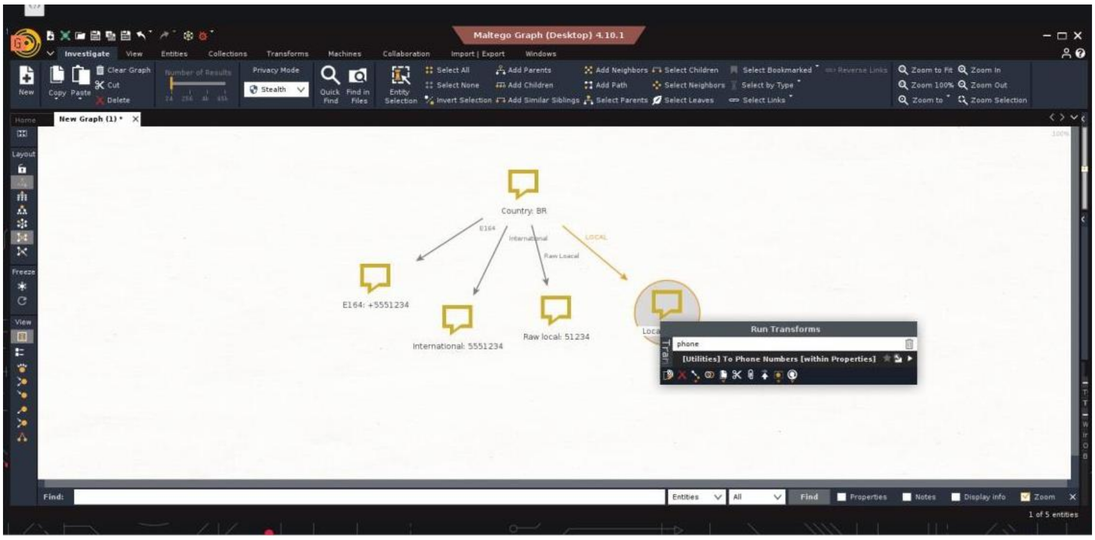

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
(venv)blank@kali: ~/PhoneInfoga
File Actions Edit View Help
26°C
Rain showers
Search
ENG
IN
18:34
06-09-2025
Right Ctrl

```
python3: can't open file '/home/blank/PhoneInfoga/phoneinfoga.py': [Errno 2] No such file or directory

┌──(venv)─(blank㉿kali)-[~/PhoneInfoga]
└─$ ls
bin  build  cmd  CODE_OF_CONDUCT.md  CODEOWNERS  Dockerfile  docs  examples  go.mod  go.sum  lib  LICENSE  logs  main.go  Makefile  mkdocs.yml  mocks  README.md  support  test  venv  web

┌──(venv)─(blank㉿kali)-[~/PhoneInfoga]
└─$ sudo apt update
sudo apt install docker.io -y
sudo systemctl enable --now docker
[sudo] password for blank:
Hit:1 http://http.kali.org/kali kali-rolling InRelease
Hit:2 https://packages.microsoft.com/debian/12/prod bookworm InRelease
937 packages can be upgraded. Run 'apt list --upgradable' to see them.
Warning: https://packages.microsoft.com/debian/12/prod/dists/bookworm/InRelease: Policy will reject signature within a year, see --audit for details
docker.io is already the newest version (26.1.5+dfsg1-9+b9).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 937
Synchronizing state of docker.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable docker

┌──(venv)─(blank㉿kali)-[~/PhoneInfoga]
└─$ cd ~/PhoneInfoga
docker build -t phoneinfoga .
[+] Building 4.5s (4/4) FINISHED                                                                                                  docker:default
 => [internal] load build definition from Dockerfile                                                                                         0.1s
 => => transferring dockerfile: 560B                                                                                                         0.0s
 => ERROR [internal] load metadata for docker.io/library/alpine:3.18                                                                         4.3s
 => CANCELED [internal] load metadata for docker.io/library/node:20.9.0-alpine                                                               4.3s
 => ERROR [internal] load metadata for docker.io/library/golang:1.20.6-alpine                                                                4.3s
──────
 > [internal] load metadata for docker.io/library/alpine:3.18:
──────
──────
 > [internal] load metadata for docker.io/library/golang:1.20.6-alpine:
──────
Dockerfile:21
────────────────────
  19 |       RUN make build
  20 |
  21 | >>> FROM alpine:3.18
  22 |       COPY --from=go_builder /app/bin/phoneinfoga /app/phoneinfoga
  23 |       EXPOSE 5000
────────────────────
ERROR: failed to solve: alpine:3.18: failed to resolve source metadata for docker.io/library/alpine:3.18: failed to copy: httpReadSeeker: failed open: failed to do request: Get "https://docker-images-prod.6aa30f8b08e16409b46e0173d6de2f
56.r2.cloudflarestorage.com/registry-v2/docker/registry/v2/blobs/sha256/80/802c91d5298192c0f3a08101aeb5f9ade2992e22c9e27fa8b88eab82602550d0/data?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=f1baa2dd9b876aeb89efebbfc9e5d5f4%2F20250
906%2Fauto%2Fs3%2Faws4_request&X-Amz-Date=20250906T130420Z&X-Amz-Expires=1200&X-Amz-SignedHeaders=host&X-Amz-Signature=8dd58687d2a8920c52d50a3a6fcaadb40d68092fd530c056aed9c6d33ddd2fb8": dial tcp: lookup docker-images-prod.6aa30f8b08e16
409b46e0173d6de2f56.r2.cloudflarestorage.com on [2405:201:102e:5863::c0a8:1d01]:53: server misbehaving

┌──(venv)─(blank㉿kali)-[~/PhoneInfoga]
└─$ █
```

- Vishing Simulation: Craft a script for a mock vishing call; test in a controlled environment. Log:

Target ID	Data Source	Information	Notes
TID001	PhoneInfoga	Phone +123456789	failed

- **Summary**: Write a 50-word vishing scenario summary.



A caller posing as an IT support technician contacts an employee, claiming urgent suspicious activity on their account. They request the employee's username and password to "resolve the issue." The call pressures quick action and exploits trust in internal departments, aiming to steal credentials through a convincing but fraudulent phone interaction.