

MAJOR – SEP

Name – Anjali Kuamri

Email – anjalirajwar101@gmail.com

College Name – BIT Sindri

Cyber Security Major Project

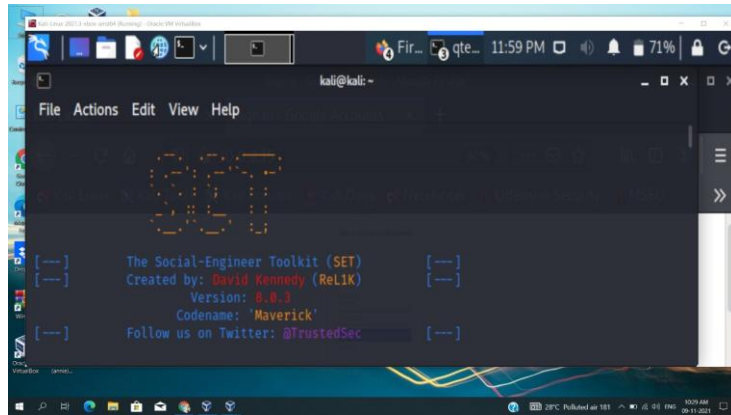
3. Use SET Tool and create a fake Gmail page and try to capture the credentials in command line and

Hacker Machine : Kali Linux

Victim machine : Windows XP / Windows 7 / Windows 10

Social Engineering Toolkit:-

Social engineering toolkit is the most powerful tool for performing social engineering attacks. It is the metasploit of social engineering in a way. It provides a very easy user interface to perform attacks like phishing, browser exploitation etc.



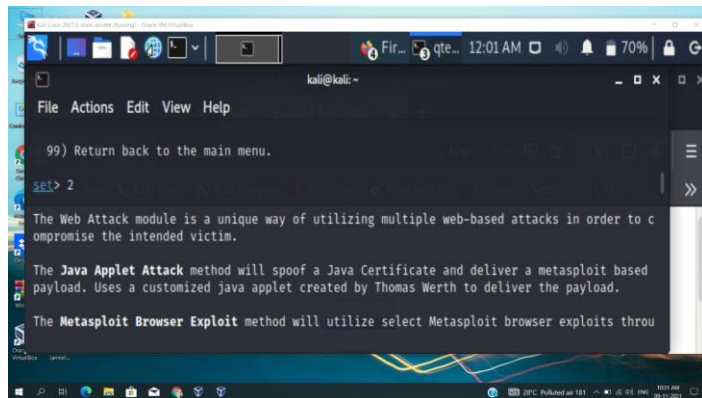
Credential Harvester Attack:-

Credential Harvester attack is one of the options available inside SET, that can create phishing pages and start a server to serve the pages and catch any user login data

steps:-

1. select "Social-Engineering Attacks" <1>
2. select "Website Attack Vectors" <2>

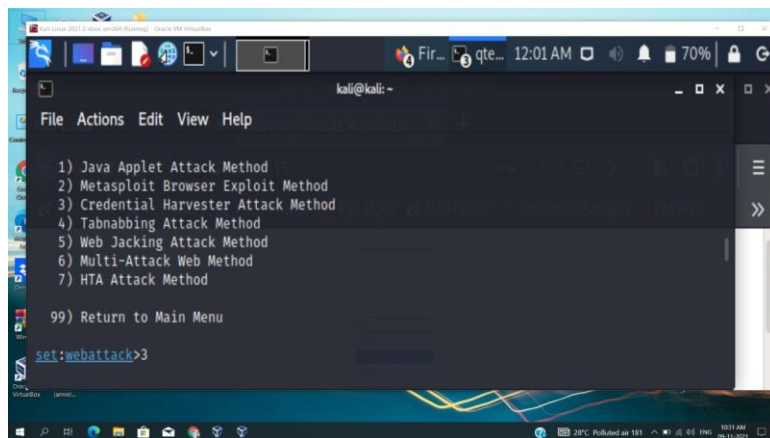




A screenshot of a Kali Linux terminal window. The terminal shows the output of the 'set' command, which lists several attack methods. The first option is '99) Return back to the main menu.' followed by 'set> 2'. Below this, there are three paragraphs of text describing different attack methods: 'The 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.', and 'The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through...'

```
kali@kali:~$ set
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 c
ompromise 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 throu
```

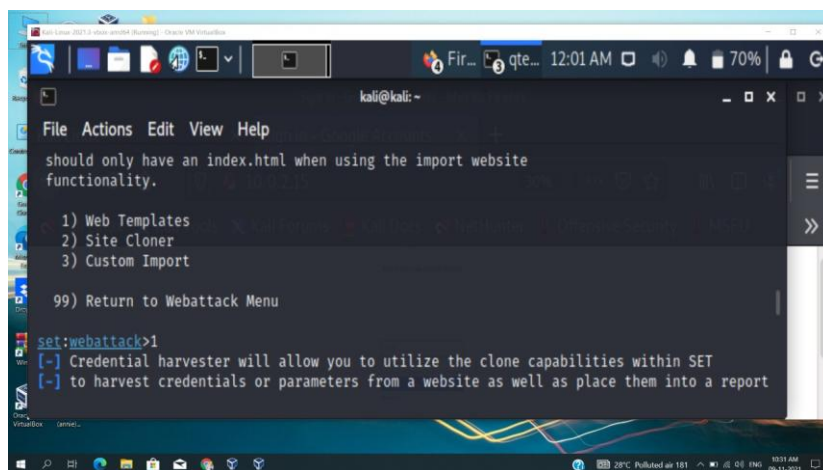
3. select "Credential Harvester Attack" <3>



A screenshot of a Kali Linux terminal window. The terminal shows the output of the 'set:webattack' command, which lists seven attack methods. The first option is '1) Java Applet Attack Method', followed by '2) Metasploit Browser Exploit Method', '3) Credential Harvester Attack Method', '4) Tabnabbing Attack Method', '5) Web Jacking Attack Method', '6) Multi-Attack Web Method', and '7) HTA Attack Method'. Below this, there is an option '99) Return to Main Menu' and the command 'set:webattack>3' is entered.

```
kali@kali:~$ set:webattack
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
```

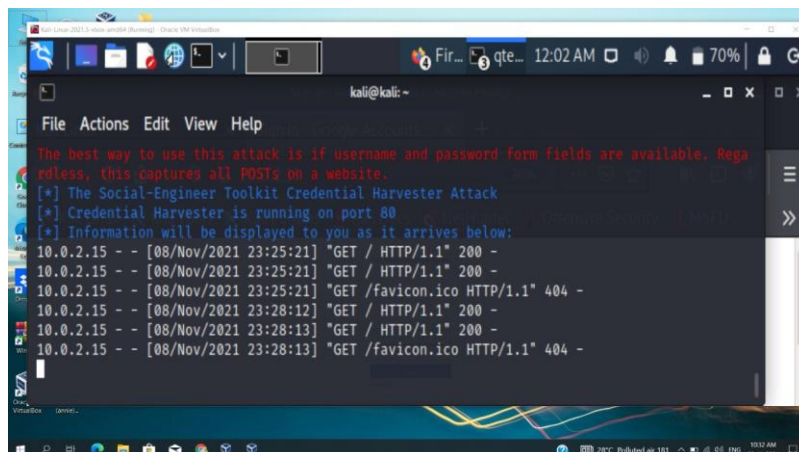
4. select "site cloner" <2>



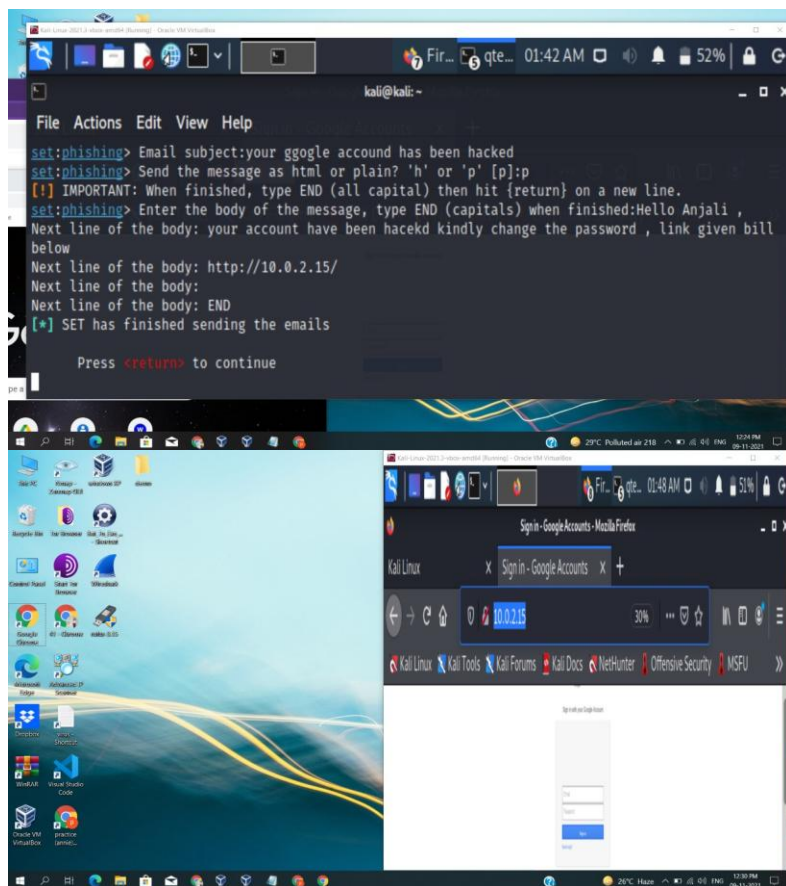
A screenshot of a Kali Linux terminal window. The terminal shows the output of the 'set:webattack' command, which lists three options: '1) Web Templates', '2) Site Cloner', and '3) Custom Import'. Below this, there is an option '99) Return to Webattack Menu' and the command 'set:webattack>1' is entered. Below the command, there are two lines of text: '[-] Credential harvester will allow you to utilize the clone capabilities within SET' and '[-] to harvest credentials or parameters from a website as well as place them into a report'.

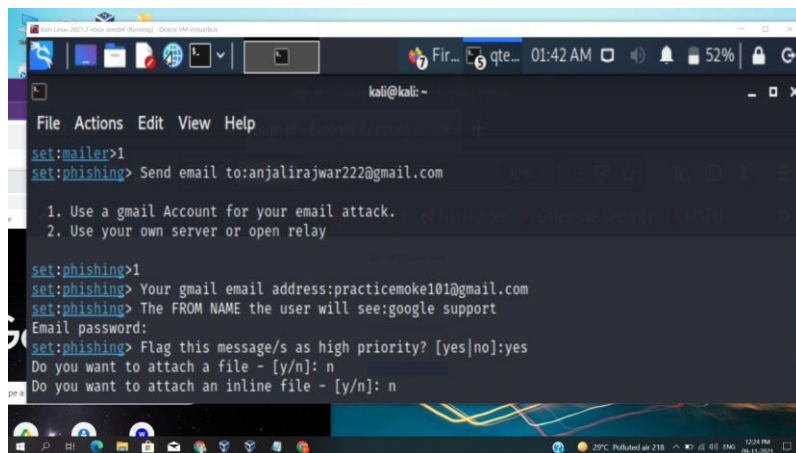
```
kali@kali:~$ set:webattack
should only have an index.html when using the import website
functionality.
1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu
set:webattack>1
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
```

5. it will ask for 2 important piece of information. The first is the ip address, to which it would submit the data and second is the url to clone which is in this case gmail.com



```
kali@kali: ~  
File Actions Edit View Help  
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:  
10.0.2.15 - - [08/Nov/2021 23:25:21] "GET / HTTP/1.1" 200 -  
10.0.2.15 - - [08/Nov/2021 23:25:21] "GET / HTTP/1.1" 200 -  
10.0.2.15 - - [08/Nov/2021 23:25:21] "GET /favicon.ico HTTP/1.1" 404 -  
10.0.2.15 - - [08/Nov/2021 23:28:12] "GET / HTTP/1.1" 200 -  
10.0.2.15 - - [08/Nov/2021 23:28:13] "GET / HTTP/1.1" 200 -  
10.0.2.15 - - [08/Nov/2021 23:28:13] "GET /favicon.ico HTTP/1.1" 404 -
```





Ways to Prevent Social Engineering Attacks:-

Some Quick Tips to Remember:-

1. Think before you click.
2. Research the sources
3. Email spoofing is ubiquitous.
4. Don't download files you don't know.
5. Offers and prizes are fake.

Five Ways to Protect Yourself:

1. Delete any request for personal information or passwords.
2. Reject requests for help or offers of help.
3. Set your spam filters to high.
4. Secure your devices.
5. Always be mindful of risks.

Thank You...