Phishing Campaign For ABC Company

Nadeesha Liyanage

Introduction

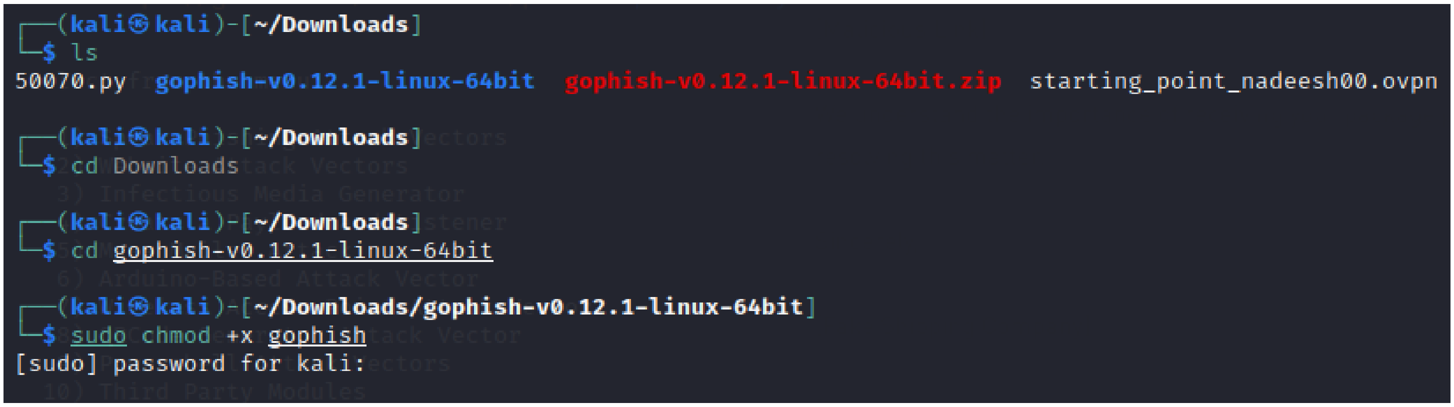
In this report I mentioned what are the steps I followed for perform the phishing simulation campaign to evaluate ABC company's employee security awareness with Gopish. The company is using Google workspace, so I created phishing templates for google.

Used tools Technologies:

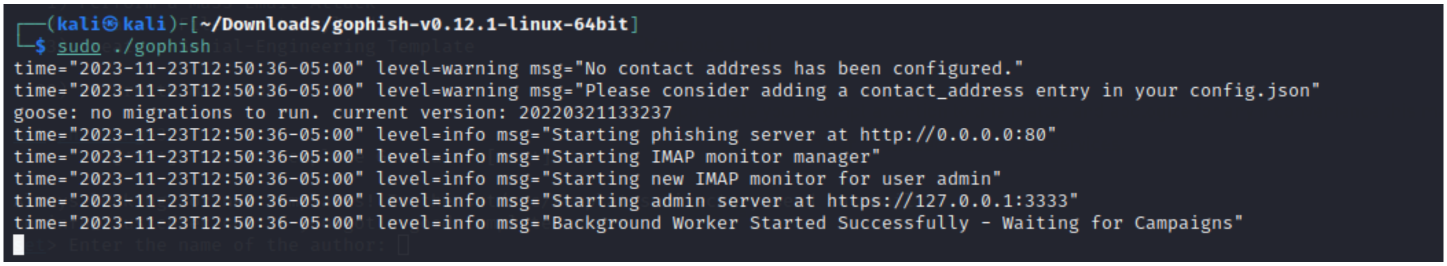
- Kali Linux OS
- Gopish
- SET
- Google SMTP

Contents

Setup Gophish

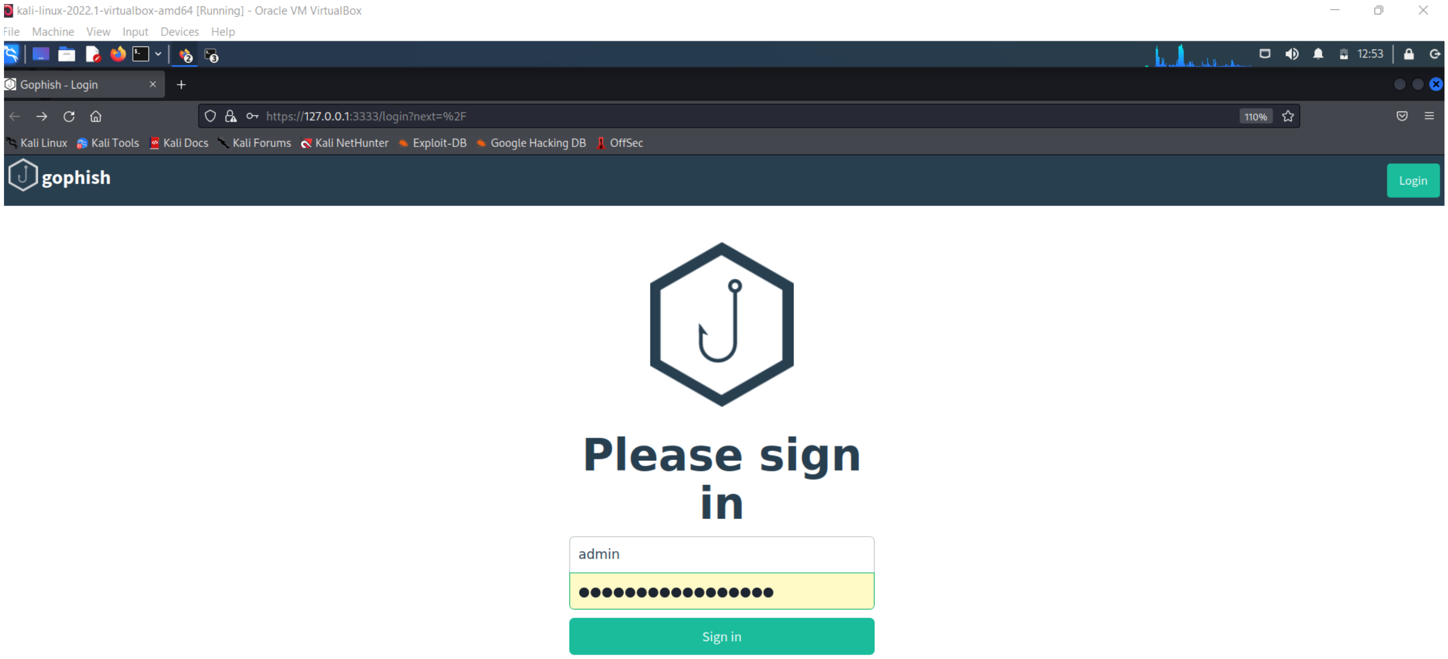


```
┌──(kali㉿kali)-[~/Downloads]
└─$ ls
50070.py  gophish-v0.12.1-linux-64bit  gophish-v0.12.1-linux-64bit.zip  starting_point_nadeesh00.ovpn

┌──(kali㉿kali)-[~/Downloads]
└─$ cd Downloads

┌──(kali㉿kali)-[~/Downloads]
└─$ cd gophish-v0.12.1-linux-64bit

┌──(kali㉿kali)-[~/Downloads/gophish-v0.12.1-linux-64bit]
└─$ sudo chmod +x gophish
[sudo] password for kali:
```



```
┌──(kali㉿kali)-[~/Downloads/gophish-v0.12.1-linux-64bit]
└─$ sudo ./gophish
time="2023-11-23T12:50:36-05:00" level=warning msg="No contact address has been configured."
time="2023-11-23T12:50:36-05:00" level=warning msg="Please consider adding a contact_address entry in your config.json"
goose: no migrations to run. current version: 20220321133237
time="2023-11-23T12:50:36-05:00" level=info msg="Starting phishing server at http://0.0.0.0:80"
time="2023-11-23T12:50:36-05:00" level=info msg="Starting IMAP monitor manager"
time="2023-11-23T12:50:36-05:00" level=info msg="Starting new IMAP monitor for user admin"
time="2023-11-23T12:50:36-05:00" level=info msg="Starting admin server at https://127.0.0.1:3333"
time="2023-11-23T12:50:36-05:00" level=info msg="Background Worker Started Successfully - Waiting for Campaigns"
█
```

Access to the gopish


kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
12:53
Gophish - Login
https://127.0.0.1:3333/login?next=%2F
110%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
gophish
Login
Sign in

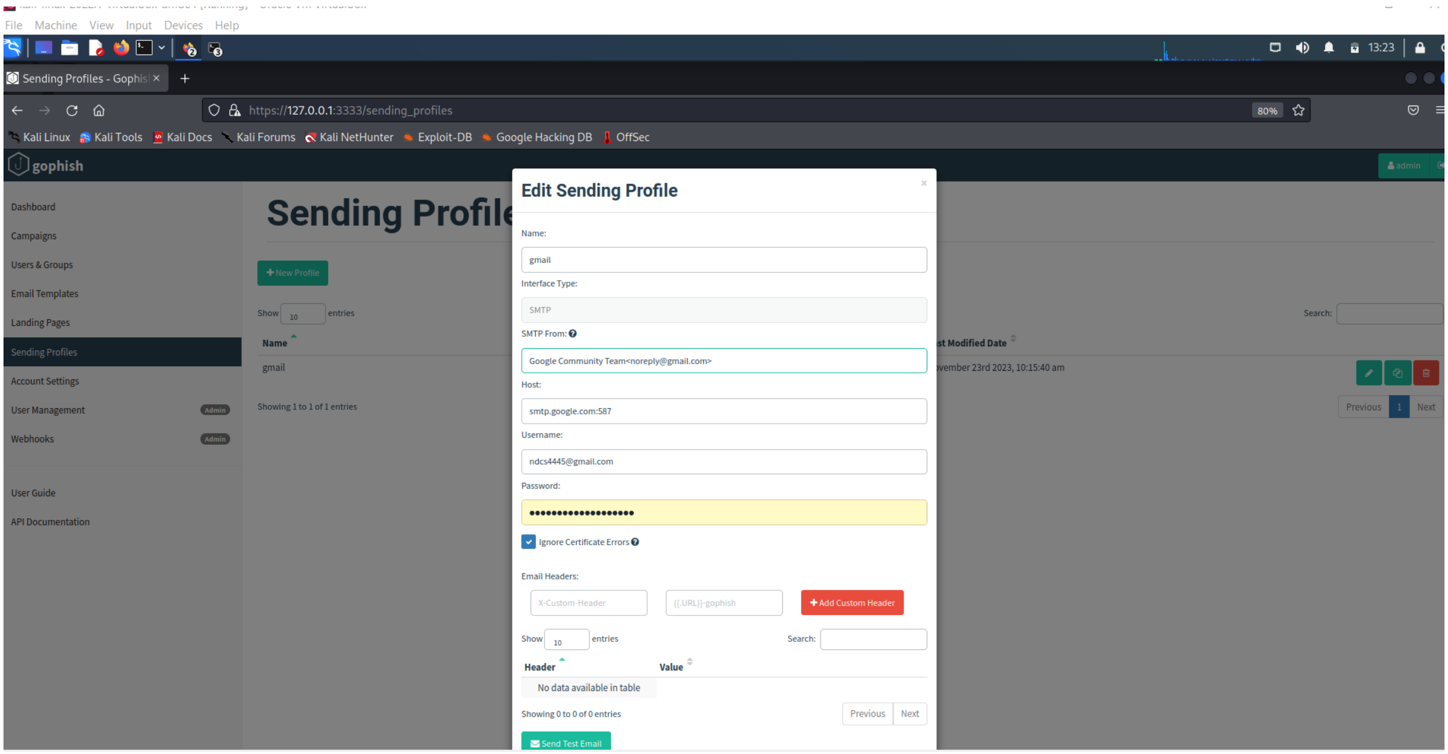
Please sign in

admin

●●●●●●●●●●●●●●●●●

Create Sending Profile

- In second step we have to create the sending profile as follows,



Edit Sending Profile

Name: gmail

Interface Type: SMTP

SMTP From: Google Community Team<noreply@gmail.com>

Host: smtp.google.com:587

Username: ndcs4445@gmail.com

Password: ••••••••••••••••••

☑ Ignore Certificate Errors

Email Headers: X-Custom-Header {{.URL}}-gophish

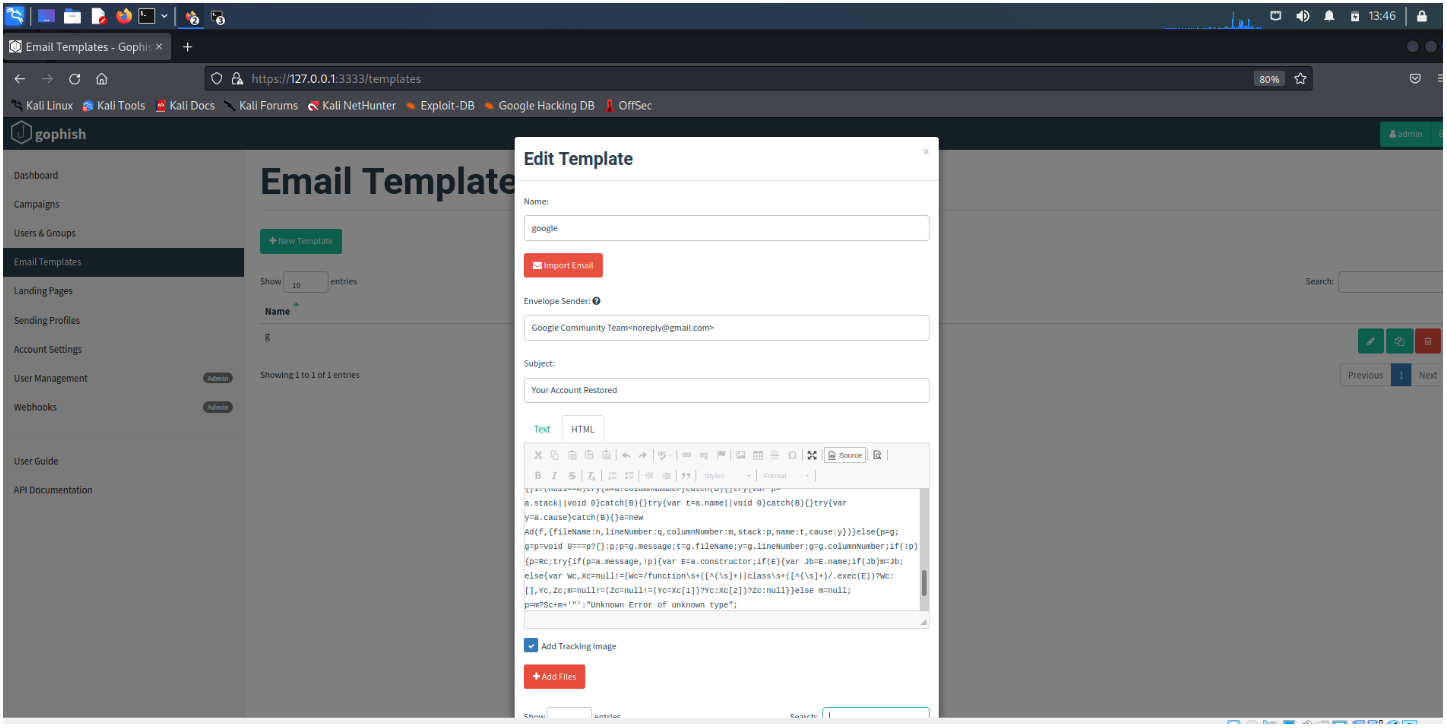
No data available in table

Showing 0 to 0 of 0 entries

- Fist we have to setup a SMTP server, I did with the google.
- In this step we have to fill sending profile name, Interface, host , username and password for authenticate for SMTP server.

Create E mail Templete.

In this step we must create our own realistic email template.



Edit Template

Name: google

Import Email

Envelope Sender: Google Community Team<noreply@gmail.com>

Subject: Your Account Restored

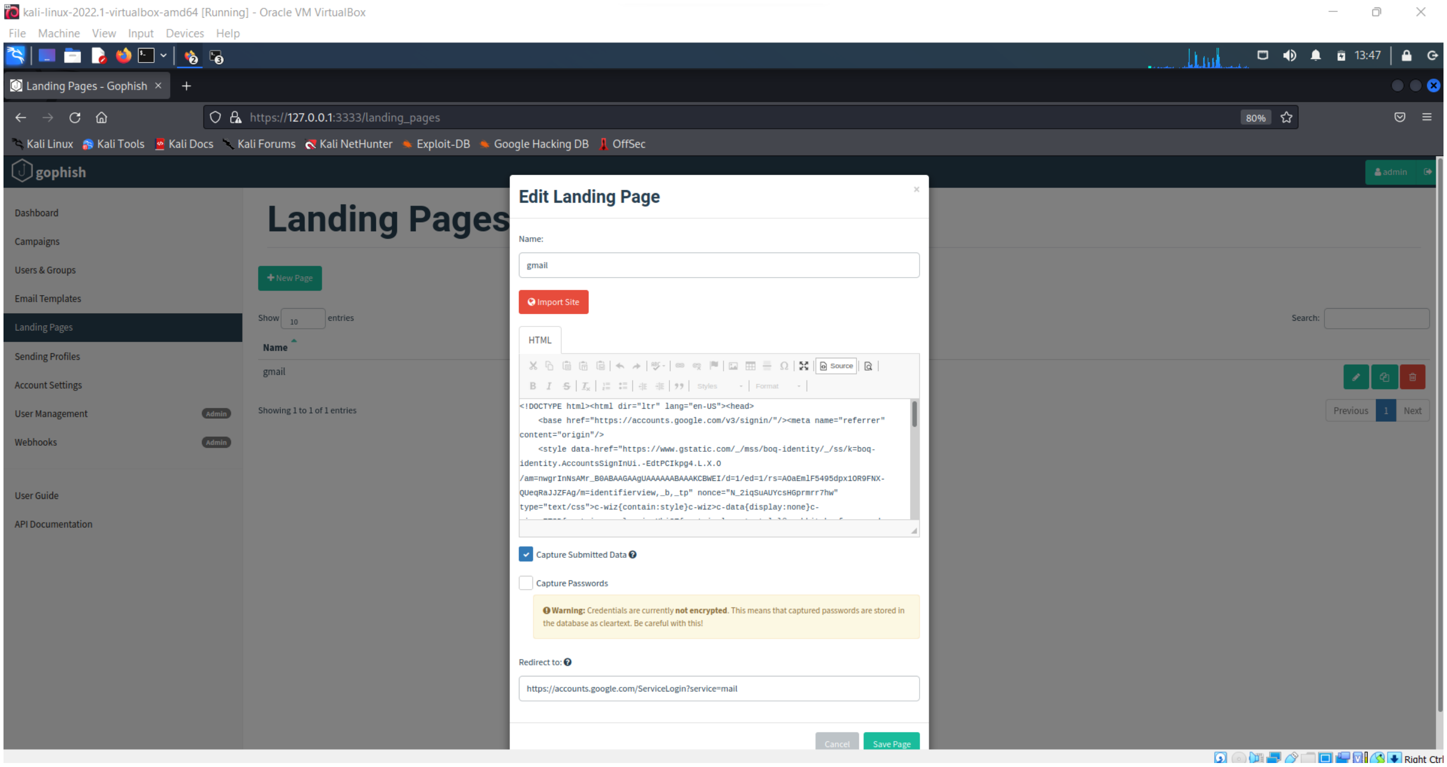
Text | HTML

```
a.stack||void 0}catch(B){}try{var t=a.name||void 0}catch(B){}try{var
y=a.cause}catch(B){}a=new
Ad(f,{fileName:n,lineNumber:q,columnNumber:m,stack:p,name:t,cause:y})}else{p=g;
g=p=void 0===p?{}:p;p=g.message;t=g.fileName;y=g.lineNumber;g=g.columnNumber;if(!p)
{p=Rc;try{if(p=a.message,!p){var E=a.constructor;if(E){var Jb=E.name;if(Jb)m=Jb;
else{var Wc,Xc=null!=(Wc=/function\s+([^(\s]+)|class\s+([^{\s]+)/.exec(E))?Wc:
[],Yc,Zc;m=null!=(Zc=null!=(Yc=Xc[1])?Yc:Xc[2])?Zc:null}}else m=null;
p=m?Sc+m+'"':"Unknown Error of unknown type";
```

☑ Add Tracking Image

Add Files

Creating the Landing Page



Edit Landing Page

Name: gmail

Import Site

HTML

```
<!DOCTYPE html><html dir="ltr" lang="en-US"><head>
    <base href="https://accounts.google.com/v3/signin/"/><meta name="referrer"
content="origin"/>
    <style data-href="https://www.gstatic.com/_/mss/boq-identity/_/ss/k=boq-
identity.AccountsSignInUi.-EdtPCIkpg4.L.X.O
/am=nwgrInNsAMr_B0ABAAGAAgUAAAAAABAAAKCBWEI/d=1/ed=1/rs=AOaEmlF5495dpx1OR9FNX-
QUeqRaJJZFAg/m=identifierview,_b,_tp" nonce="N_2iqSuAUYcsHGprmrr7hw"
type="text/css">c-wiz{contain:style}c-wiz>c-data{display:none}c-
```

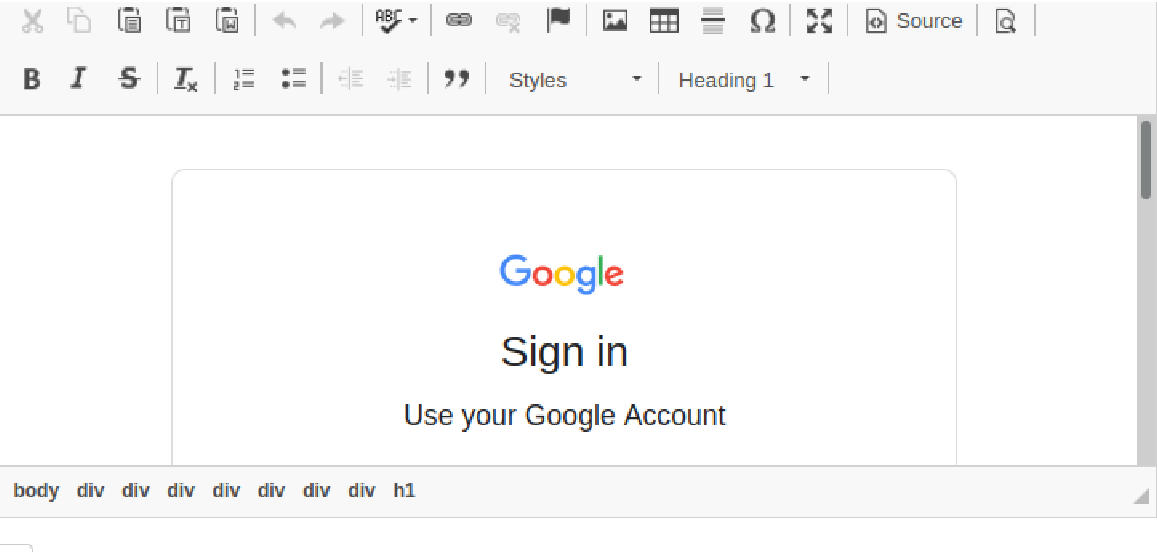
☑ Capture Submitted Data

□ Capture Passwords

Warning: Credentials are currently **not encrypted**. This means that captured passwords are stored in the database as cleartext. Be careful with this!

Redirect to: https://accounts.google.com/ServiceLogin?service=mail

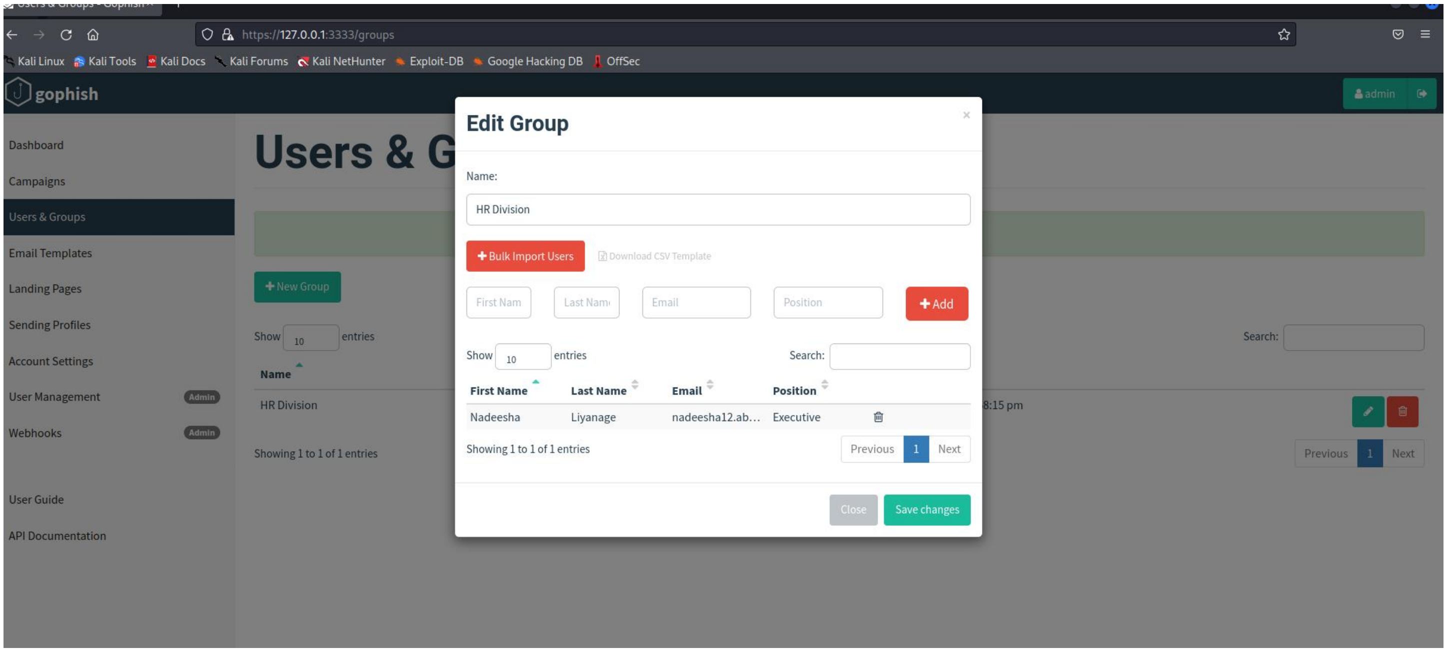
Cancel | Save Page



Sign in

Use your Google Account

Create Users And Groups



Edit Group

Name: HR Division

Show 10 entries Search:

First Name	Last Name	Email	Position
Nadeesha	Liyanage	nadeesha12.ab…	Executive

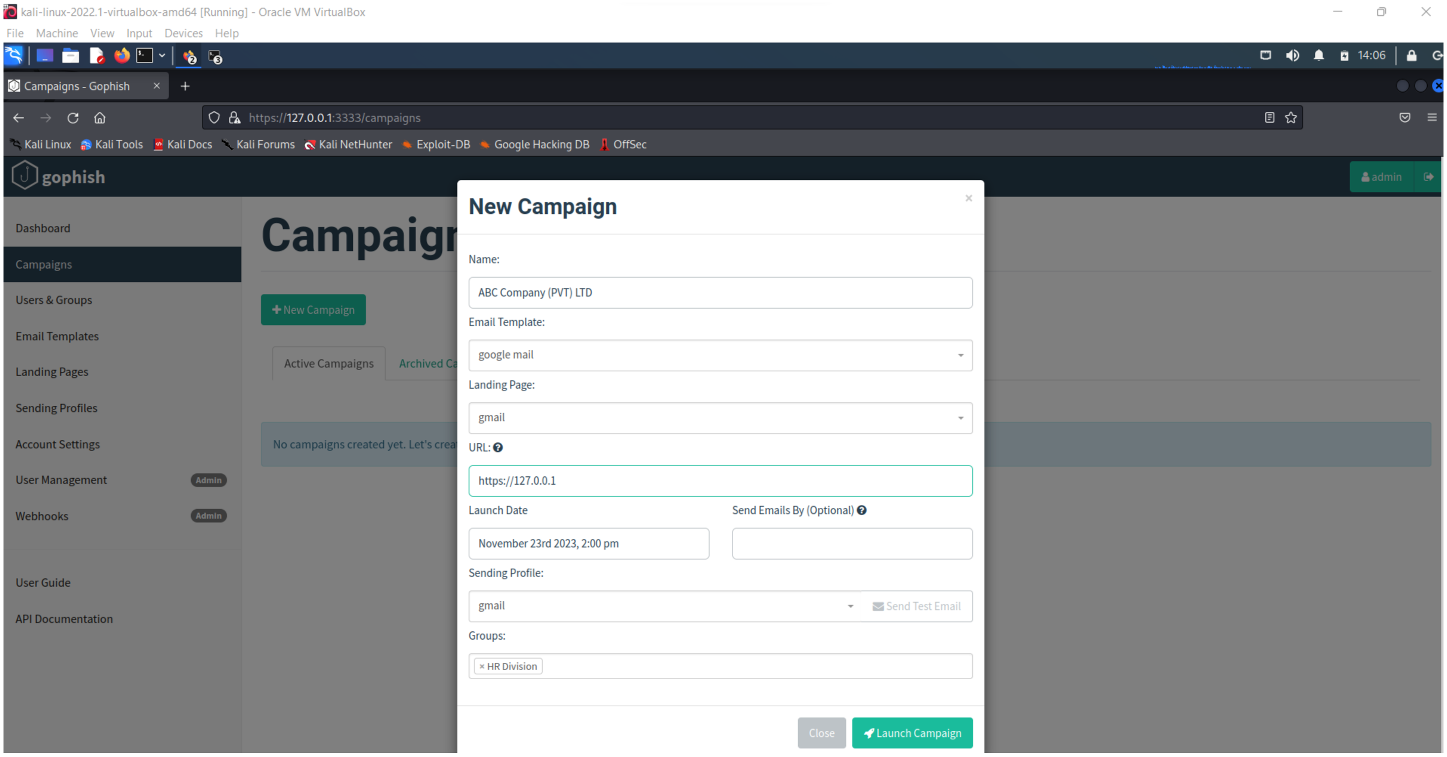
Showing 1 to 1 of 1 entries

Name	
HR Division	8:15 pm

Showing 1 to 1 of 1 entries

- In here we have to add user groups and groups. In here I just only added to HR person for group.

New Campaign Creation



New Campaign

Name: ABC Company (PVT) LTD

Email Template: google mail

Landing Page: gmail

URL: https://127.0.0.1

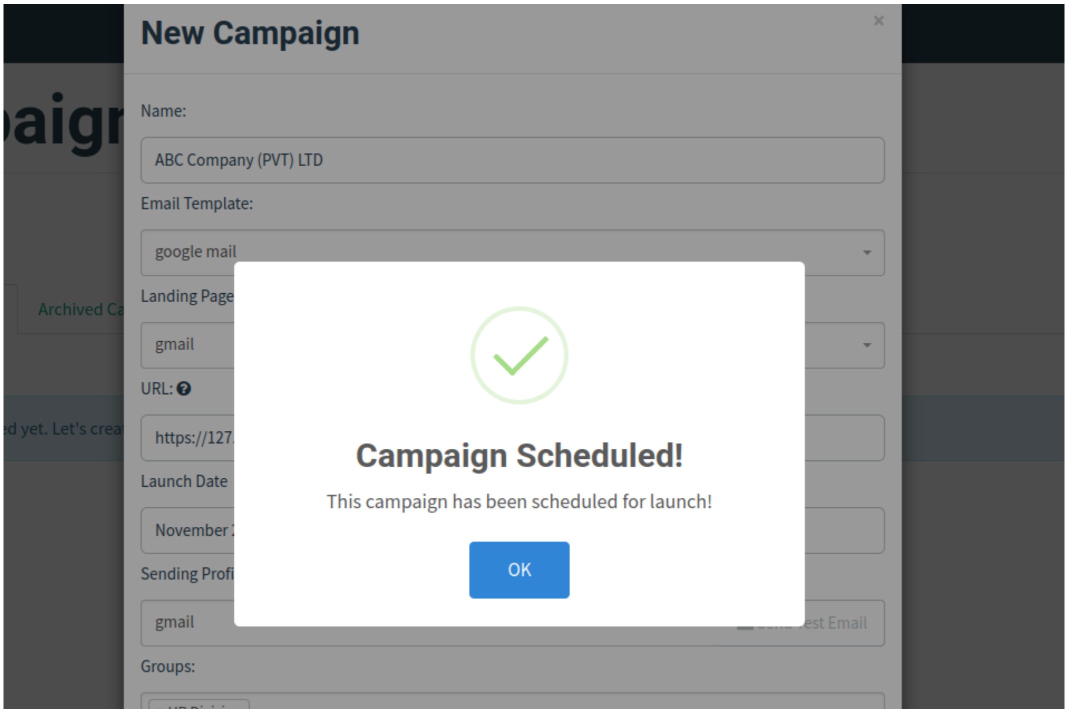
Launch Date: November 23rd 2023, 2:00 pm

Send Emails By (Optional):

Sending Profile: gmail

Groups: × HR Division

- We have to use a purchased similar domain for real world applicati



New Campaign

Name: ABC Company (PVT) LTD

Email Template: google mail

Landing Page: gmail

URL: https://127.

Launch Date: November

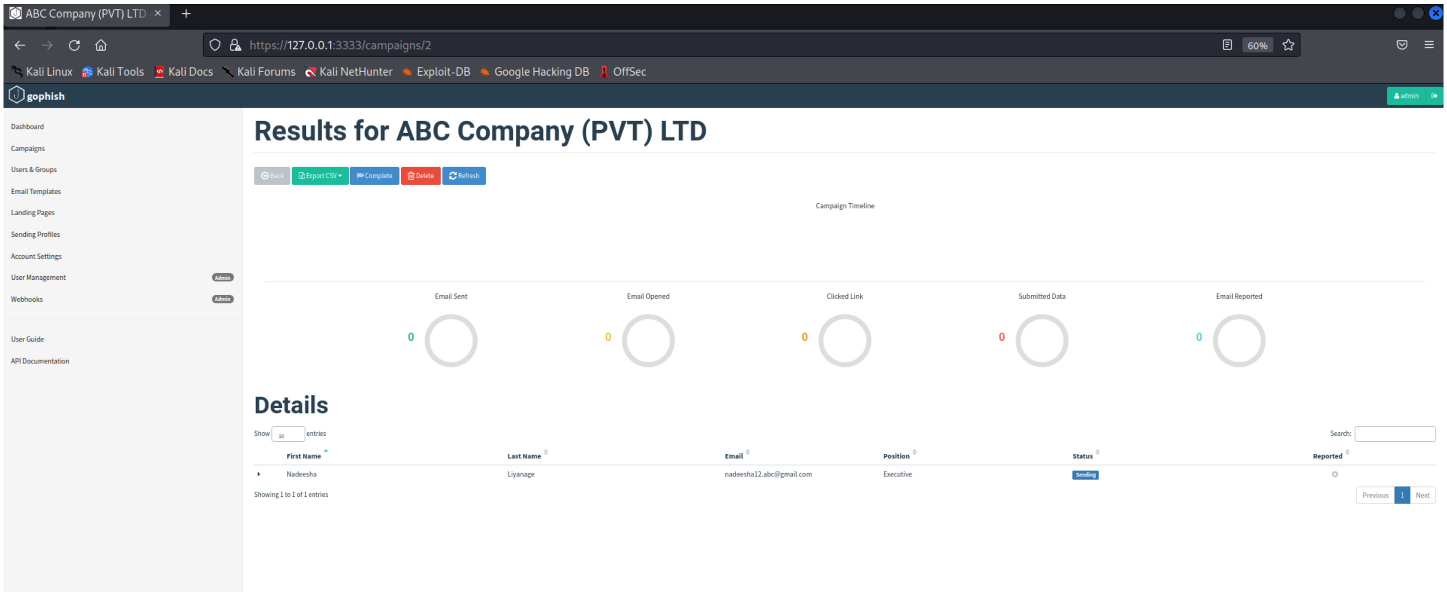
Sending Profile: gmail

Groups:

Campaign Scheduled!

This campaign has been scheduled for launch!

- After the campaign scheduled, if some employee will trap into the mail open , clicked , enter credentials oe reported we can see here. And also we can create datafiles also.



https://127.0.0.1:3333/campaigns/2

Results for ABC Company (PVT) LTD

Campaign Timeline

Email Sent	Email Opened	Clicked Link	Submitted Data	Email Reported
0	0	0	0	0

Details

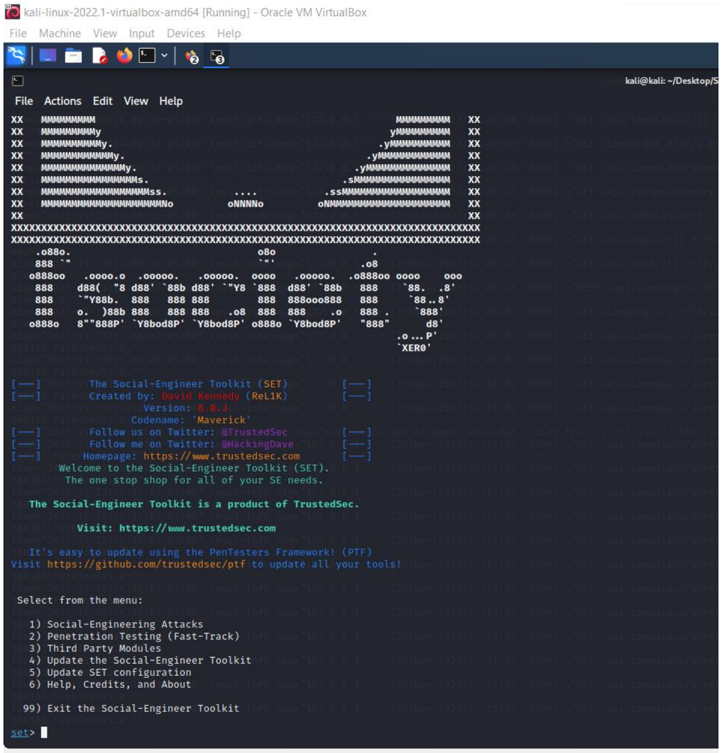
Show 10 entries

First Name	Last Name	Email	Position	Status	Reported
Nadeesha	Liyanage	nadeesha12.abc@gmail.com	Executive	Sending	⊗

Showing 1 to 1 of 1 entries

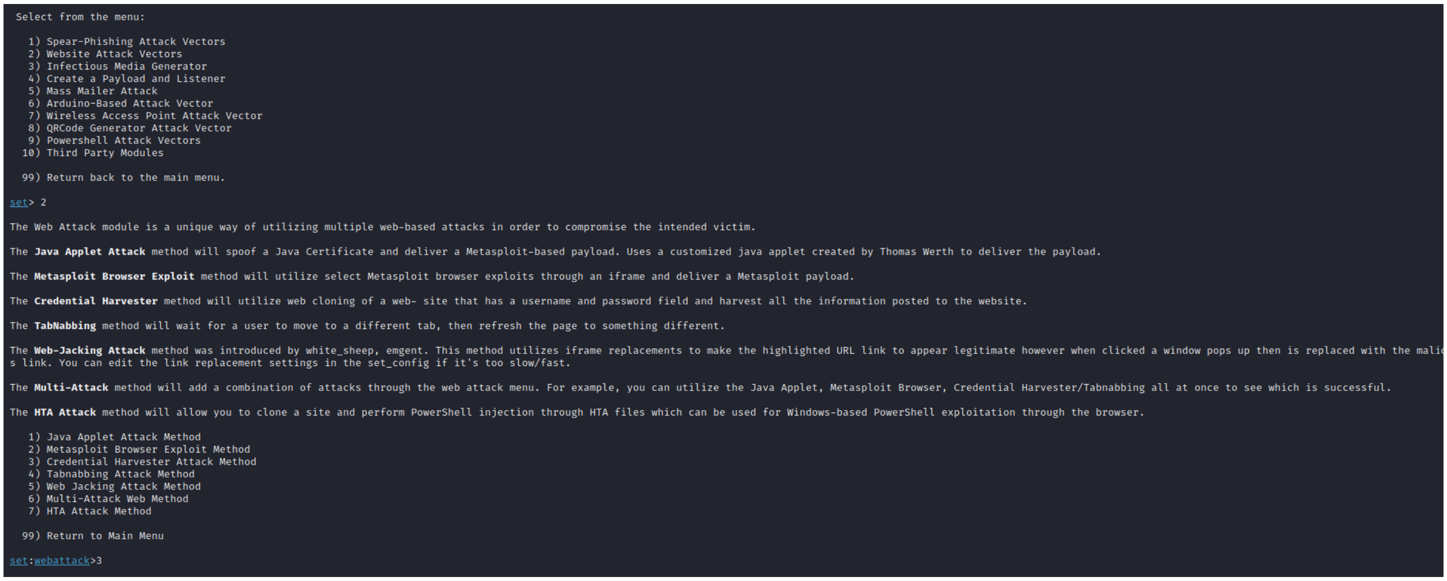
Credential Harvesting with SET – Social Engineering Toolkit

- This method can create phishing templates and can perform spear phishing attacks and also various attacks.


kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~/Desktop/S
File Actions Edit View Help

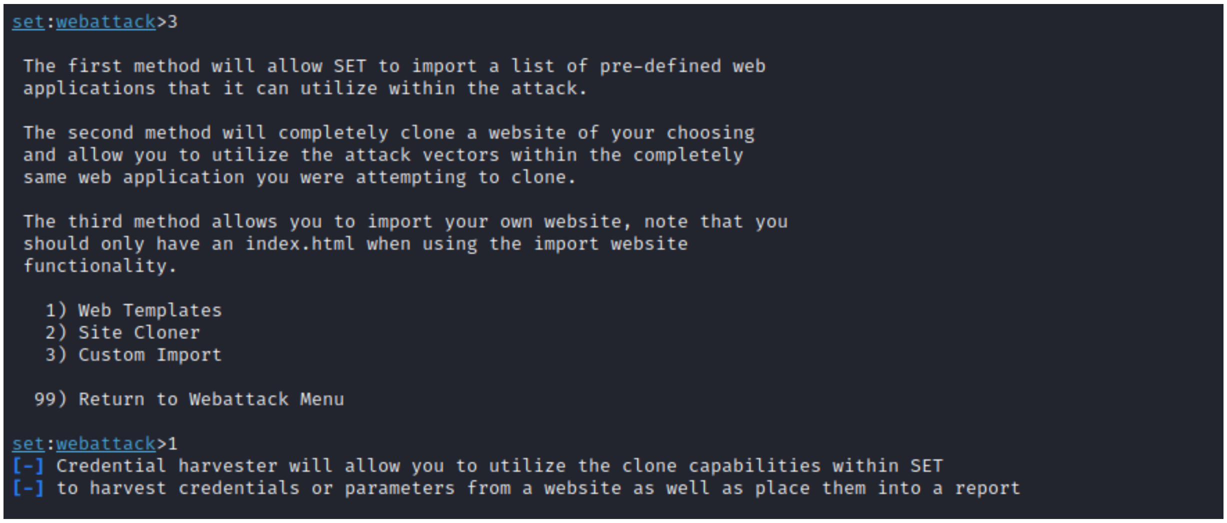
```
XX   MMMMMMMMM                                             MMMMMMMMM   XX
XX   MMMMMMMMMy                                           yMMMMMMMMM   XX
XX   MMMMMMMMMMy.                                       .yMMMMMMMMMM   XX
XX   MMMMMMMMMMMMy.                                   .yMMMMMMMMMMMM   XX
XX   MMMMMMMMMMMMMMy.                               .yMMMMMMMMMMMMMM   XX
XX   MMMMMMMMMMMMMMMMs.                           .sMMMMMMMMMMMMMMMM   XX
XX   MMMMMMMMMMMMMMMMMMss.          ....        .ssMMMMMMMMMMMMMMMMMM   XX
XX   MMMMMMMMMMMMMMMMMMMMNo         oNNNNo       oNMMMMMMMMMMMMMMMMMMMM   XX
XX                                                                     XX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
    .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> 
```

- *First select 1.Social enjineering attacks*



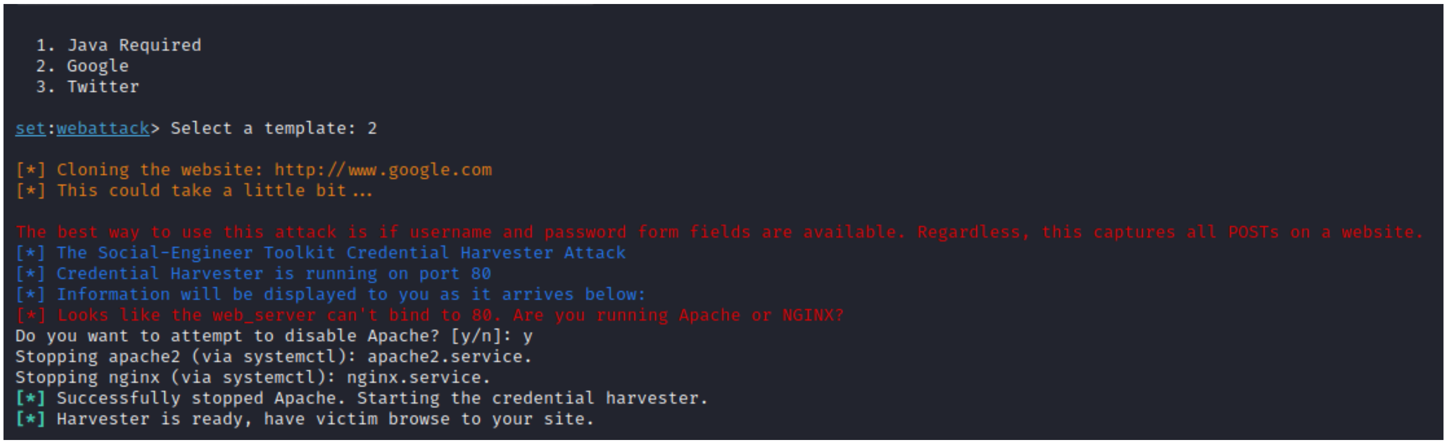
```
 Select from the menu:

   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

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 is replaced with the malic
s link. You can edit the link replacement settings in the set_config if it's 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
```

- Then press 2 for go inside to the web Attack vectors.

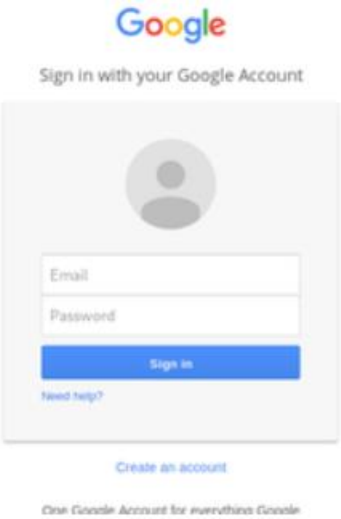


```
set:webattack>3

 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
[-] 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
```

- Then we can go either 1 or 2 . I go with one. Then we can go to our localhost and then we can find the phishing page



```
  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:
[*] Looks like the web_server can't bind to 80. Are you running Apache or NGINX?
Do you want to attempt to disable Apache? [y/n]: y
Stopping apache2 (via systemctl): apache2.service.
Stopping nginx (via systemctl): nginx.service.
[*] Successfully stopped Apache. Starting the credential harvester.
[*] Harvester is ready, have victim browse to your site.
```


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

- If someone enter their credential, we can find on /var/www/html file.