IGNITE COHORT 2 - Cybersecurity
Group 2

Assignment 2

Part 3:

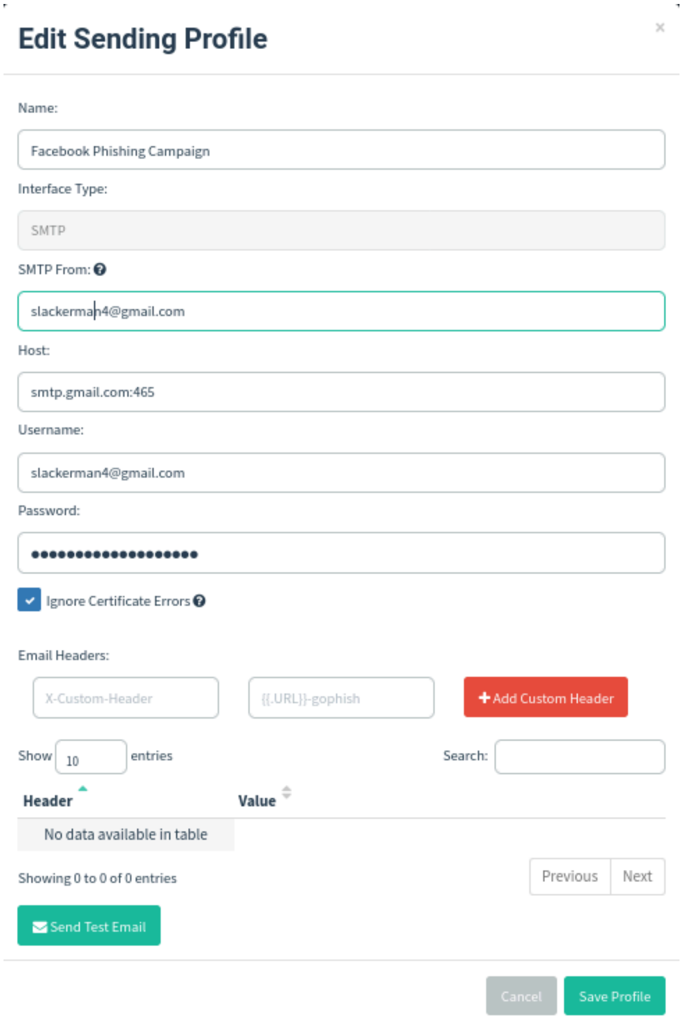
Gophish Phishing Campaign

Introduction

This report outlines the steps we took to launch a phishing campaign using the open-source framework Gophish. The objective of this phishing campaign is to simulate a phishing attempt aimed at collecting the emails and passwords of some users of the website “facebook.com,” and will serve as a good learning experience for us concerning the Social Engineering aspect of cybersecurity.

1. Sending Profile

The first step of the campaign was to configure the Sending Profile.
We closely followed the instructions provided to us by Mr. Victor Waliaula, but rather than writing the SMTP From in the format “First Last<email address>,” we omitted the First and Last portions as they caused an error when trying to send a test email.



Edit Sending Profile

Name: Facebook Phishing Campaign

Interface Type: SMTP

SMTP From: slackerman4@gmail.com

Host: smtp.gmail.com:465

Username: slackerman4@gmail.com

Password: ●●●●●●●●●●●●●●●●●●●

☑ Ignore Certificate Errors

Email Headers:

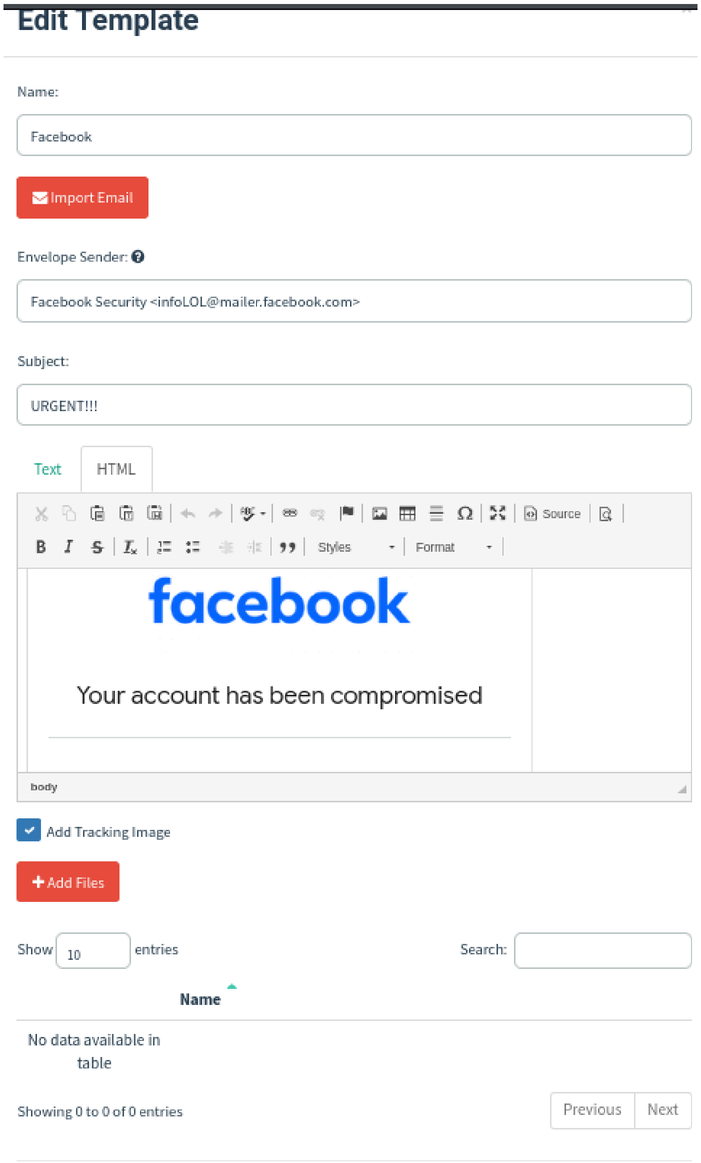
Show 10 entries

Header	Value
No data available in table	

Showing 0 to 0 of 0 entries

2. Email Template

When designing the email template, we repurposed a simple Gmail authentication email to link the potential victim to the Facebook login page. The hyperlink will redirect to the landing page.
For whatever reason, the Facebook logo does not appear in the final email, unfortunately.



Edit Template

Name: Facebook

Envelope Sender: Facebook Security <infoLOL@mailer.facebook.com>

Subject: URGENT!!!

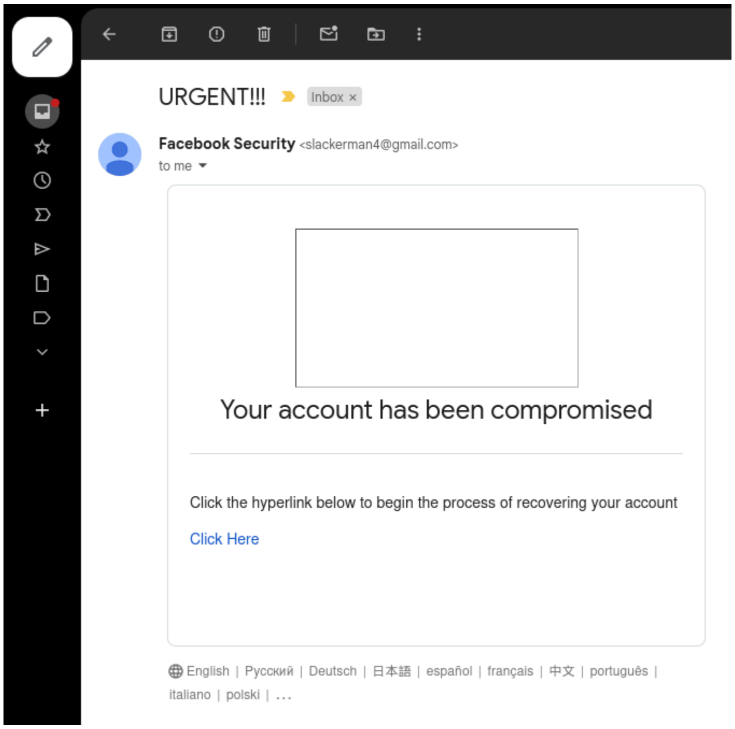
Your account has been compromised

☑ Add Tracking Image

Show 10 entries Search:

Name
No data available in table

Showing 0 to 0 of 0 entries



URGENT!!! Inbox ×

Facebook Security <slackerman4@gmail.com>
to me

Your account has been compromised

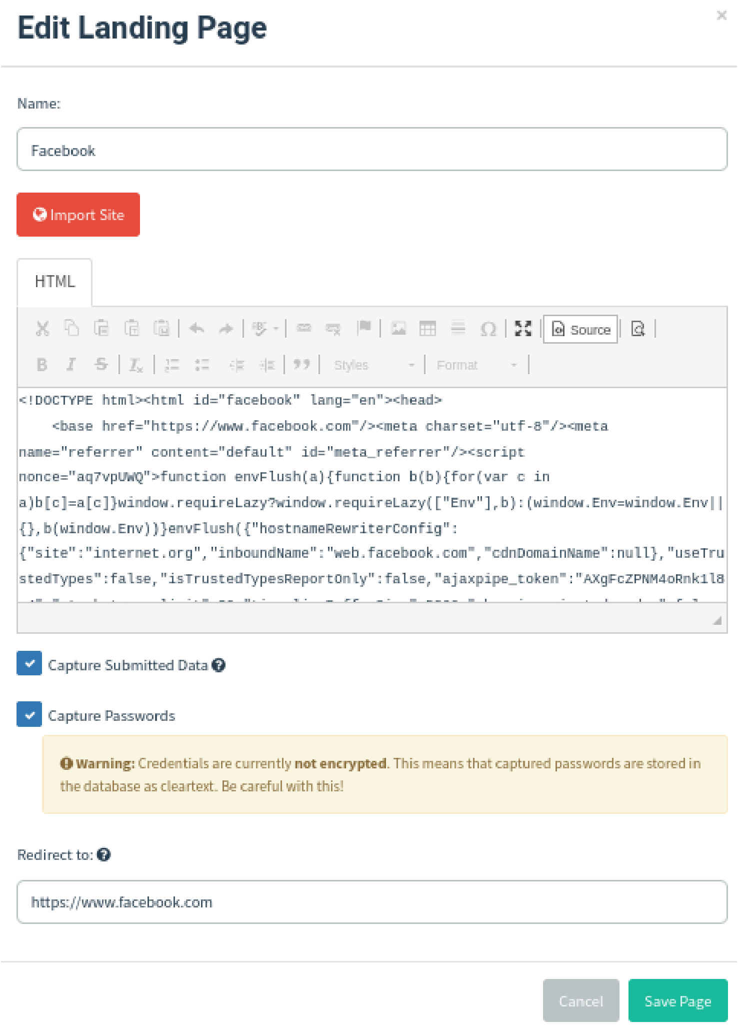
Click the hyperlink below to begin the process of recovering your account

Click Here

English | Русский | Deutsch | 日本語 | español | français | 中文 | português | italiano | polski | …

3. Landing Page

The landing page was simple to implement as we merely imported the Facebook homepage. Upon submission of the victim's data, they will be redirected to the normal Facebook website. This may alert them of the illegitimacy of the email, but we reckon they may simply try to login again under the belief that their earlier attempt was interrupted somehow.



Edit Landing Page

Name:

Facebook

```
<!DOCTYPE html><html id="facebook" lang="en"><head>
    <base href="https://www.facebook.com"/><meta charset="utf-8"/><meta
name="referrer" content="default" id="meta_referrer"/><script
nonce="aq7vpUWQ">function envFlush(a){function b(b){for(var c in
a)b[c]=a[c]}window.requireLazy?window.requireLazy(["Env"],b):(window.Env=window.Env||
{},b(window.Env))}envFlush({"hostnameRewriterConfig":
{"site":"internet.org","inboundName":"web.facebook.com","cdnDomainName":null},"useTru
stedTypes":false,"isTrustedTypesReportOnly":false,"ajaxpipe_token":"AXgFcZPNM4oRnk1l8
```

☑ Capture Submitted Data

☑ Capture Passwords

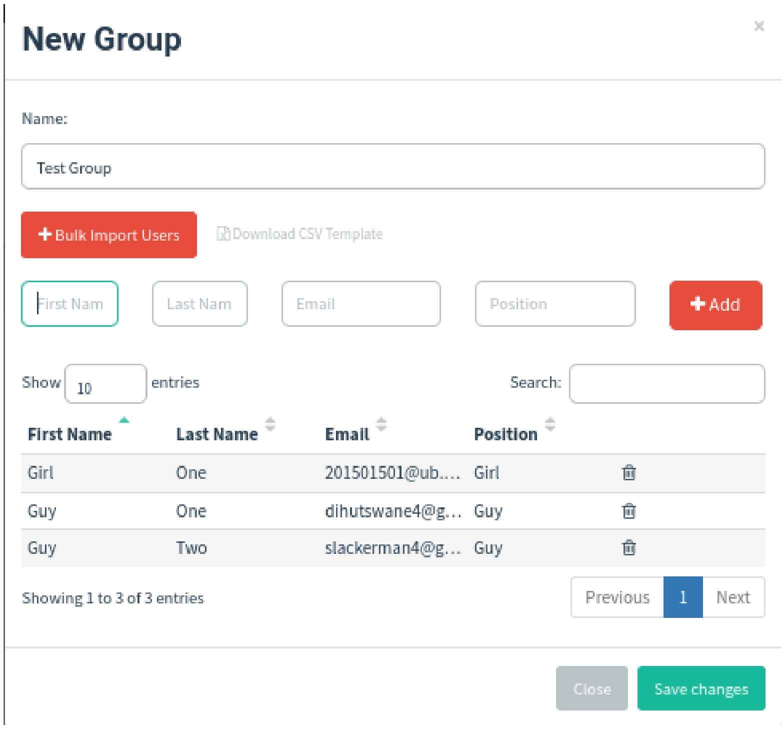
Warning: Credentials are currently **not encrypted**. This means that captured passwords are stored in the database as cleartext. Be careful with this!

Redirect to:

https://www.facebook.com

4. Users and Groups

Three emails were used in the campaign; all owned by Dihutswane Mosienyane.



New Group

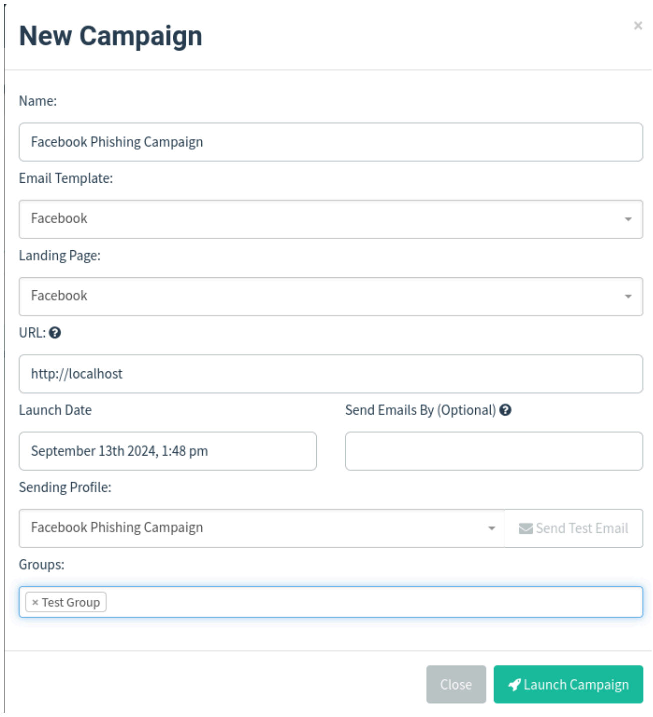
Name: Test Group

Show 10 entries

First Name	Last Name	Email	Position	
Girl	One	201501501@ub.…	Girl	🗑
Guy	One	dihutswane4@g…	Guy	🗑
Guy	Two	slackerman4@g…	Guy	🗑

Showing 1 to 3 of 3 entries

5.Launching The Campaign



New Campaign

Name: Facebook Phishing Campaign

Email Template: Facebook

Landing Page: Facebook

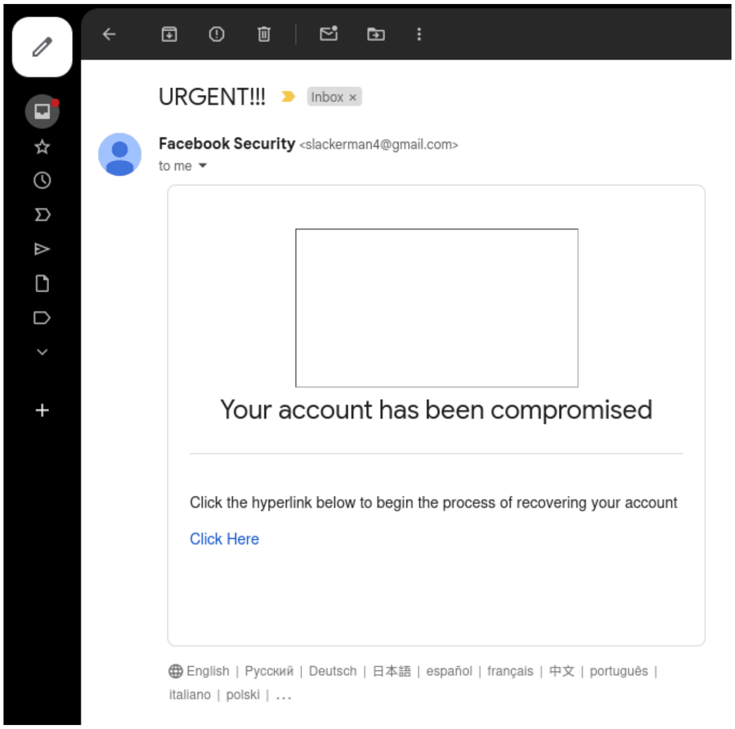
URL: http://localhost

Launch Date: September 13th 2024, 1:48 pm

Send Emails By (Optional):

Sending Profile: Facebook Phishing Campaign

Groups: × Test Group



URGENT!!! Inbox ×

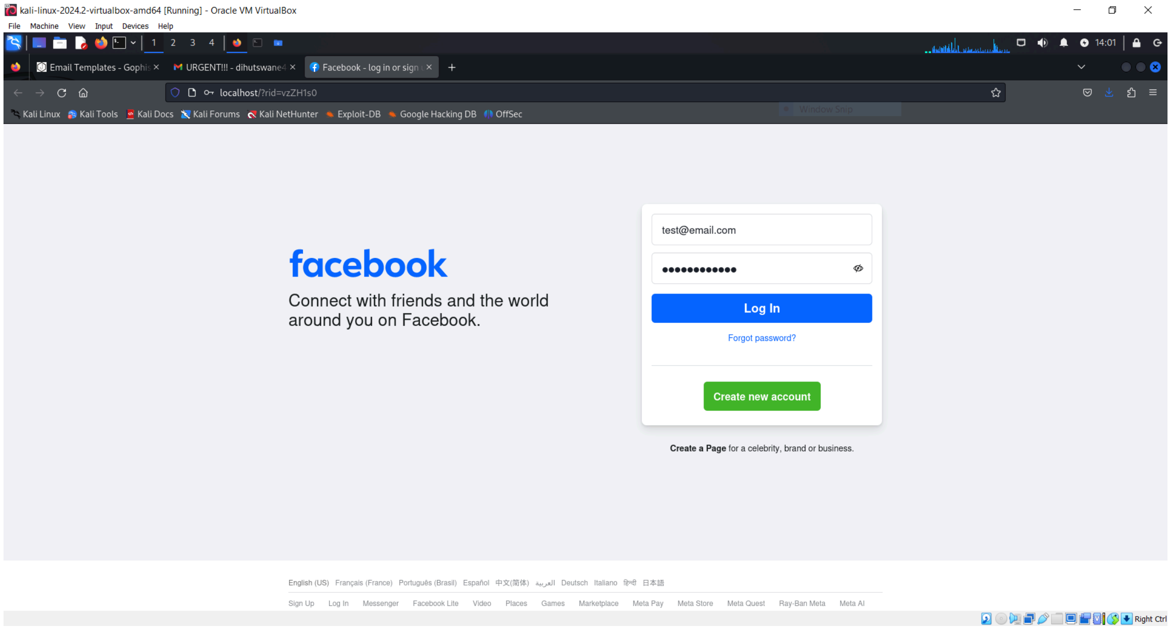
Facebook Security <slackerman4@gmail.com>
to me

Your account has been compromised

Click the hyperlink below to begin the process of recovering your account

Click Here

English | Русский | Deutsch | 日本語 | español | français | 中文 | português | italiano | polski | …


kali-linux-2024.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Email Templates - Gophi
URGENT!!! - dihutswane4
Facebook - log in or sign
localhost/?rid=vzZH1s0
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
14:01

facebook

Connect with friends and the world around you on Facebook.

test@email.com

•••••••••••••

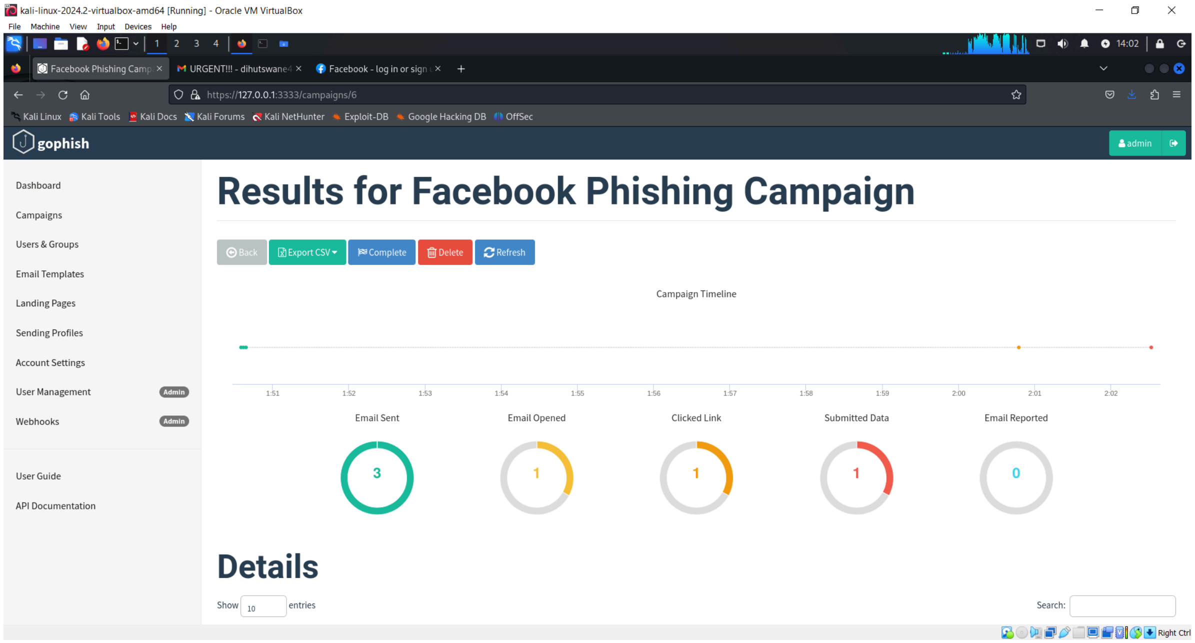
Log In

Forgot password?

Create new account

Create a Page for a celebrity, brand or business.

English (US) Français (France) Português (Brasil) Español 中文(简体) العربية Deutsch Italiano हिंदी 日本語
Sign Up Log In Messenger Facebook Lite Video Places Games Marketplace Meta Pay Meta Store Meta Quest Ray-Ban Meta Meta AI
Right Ctrl

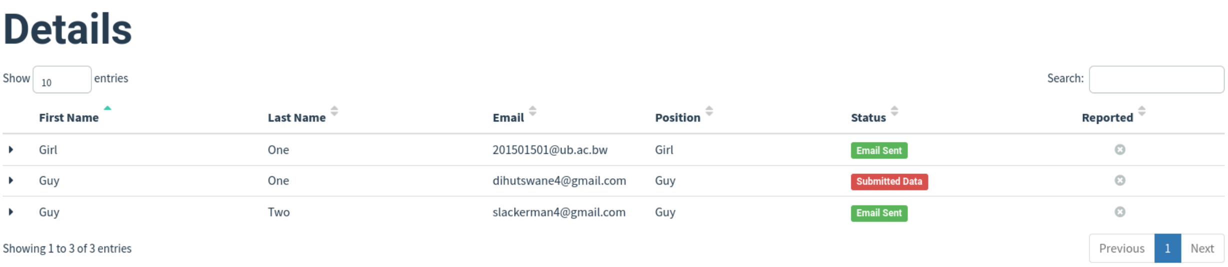

kali-linux-2024.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Facebook Phishing Camp
URGENT!!! - dihutswane4
Facebook - log in or sign
https://127.0.0.1:3333/campaigns/6
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
14:02
gophish
admin
Dashboard
Campaigns
Users & Groups
Email Templates
Landing Pages
Sending Profiles
Account Settings
User Management Admin
Webhooks Admin
User Guide
API Documentation

Results for Facebook Phishing Campaign

Email Sent	Email Opened	Clicked Link	Submitted Data	Email Reported
3	1	1	1	0

Details

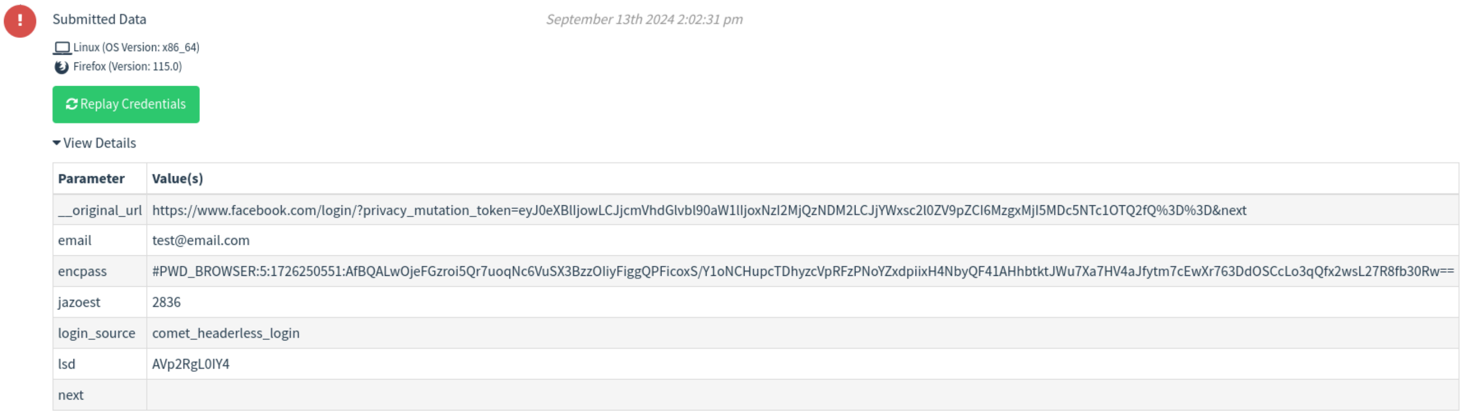
Show 10 entries Search:


Details

Show 10 entries Search:

	First Name	Last Name	Email	Position	Status	Reported
▸	Girl	One	201501501@ub.ac.bw	Girl	Email Sent	⊗
▸	Guy	One	dihutswane4@gmail.com	Guy	Submitted Data	⊗
▸	Guy	Two	slackerman4@gmail.com	Guy	Email Sent	⊗

Showing 1 to 3 of 3 entries



Submitted Data

September 13th 2024 2:02:31 pm

Linux (OS Version: x86_64)
Firefox (Version: 115.0)

Parameter	Value(s)
__original_url	https://www.facebook.com/login/?privacy_mutation_token=eyJ0eXBlIjowLCJjcmVhdGlvbl90aW1lIjoxNzI2MjQzNDM2LCJjYWxsc2l0ZV9pZCI6MzgxMjI5MDc5NTc1OTQ2fQ%3D%3D&next
email	test@email.com
encpass	#PWD_BROWSER:5:1726250551:AfBQALwOjeFGzroi5Qr7uoqNc6VuSX3BzzOliyFiggQPFicoxS/Y1oNCHupcTDhyzcVpRFzPNoYZxdpiixH4NbyQF41AHhbtktJWu7Xa7HV4aJfytm7cEwXr763DdOSCcLo3qQfx2wsL27R8fb30Rw==
jazoest	2836
login_source	comet_headerless_login
lsd	AVp2RgL0IY4
next	

Conclusion

The phishing campaign was somewhat successful in the end. We were able to capture one of the victim’s email addresses, but their password was in an encrypted format. We will continue to research on how to rectify this, but thanks to Mr. Victor Waliaula’s notes, we learned a great deal about phishing.