

Esercizio obbligatorio

Edit Group

Name:

test phishing

+ Bulk Import Users

Download CSV Template

First Name

Last Name

Email

Position

+ Add

Show 10 entries

Search:

First Name	Last Name	Email	Position
Maria	Bianchi	zanchettamary...	

Showing 1 to 1 of 1 entries

Previous

1

Next

Close

Save changes

Text HTML

✂️ 📄 📧 📧 📧 | ⬅️ ➡️ | ABC ✓ | 🔗 🔗 | 🚩 | 🖼️ 📊 📊 | Ω | 🔗 🔗 | 📄 Source | 🔍

B *I* S | I_x | 1= =: | ⌵ ⌵ | ” | Styles | Normal

amazon.it

Ciao,

Abbiamo pensato che potesse interessarti sapere che abbiamo spedito il tuo ordine.

Il tuo ordine è andato a buon fine e non può più essere modificato. Se hai

body p

✓ Add Tracking Image

+ Add Files

Ho poi preparato il profilo per l'invio della mail di phishing.

✕

Edit Sending Profile

Name:

Amministrazione

Interface Type:

SMTP

SMTP From: ?

noreplyamazon@gmail.com

Host:

smtp.gmail.com

Username:

maria.zanchetta98@gmail.com

Password:

.....

☒ Ignore Certificate Errors ?

Email Headers:

X-Custom-Header

{{.URL}}-gophish

+ Add Custom Header

Per raccogliere i dati dell'utente, ho realizzato una landing page con il sito di DHL, proprio perché nella mail si chiede all'utente di autenticarsi su Amazon e di tracciare l'ordine appena spedito.

Tracciamento

Import Site

HTML

X Copy Paste Undo Redo ABC Font Color Background Color Link Unlink Flag Image Table List Omega Refresh Source Preview

B I S T_x Bullets Numbered List Indent Outdent Quote Styles Format

DHL

Traccia la tua spedizione

☒ Capture Submitted Data ?

☐ Capture Passwords

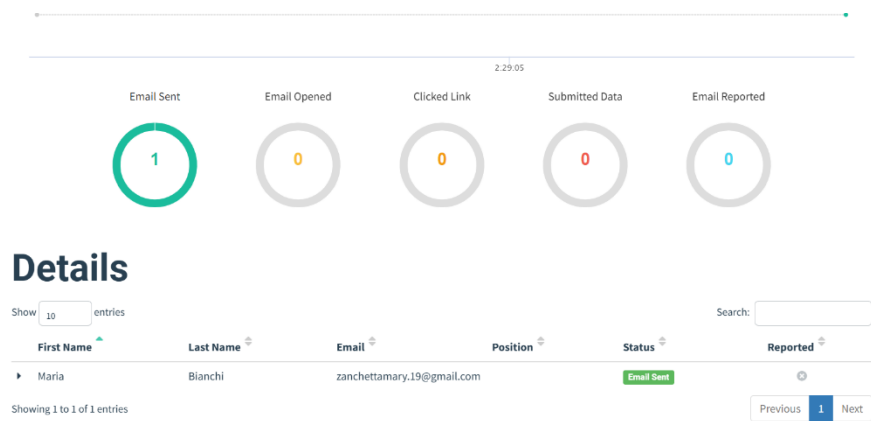
Warning:

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.dhl.com/it-it/home.html

Alla fine ho lanciato la campagna di phishing con quanto preparato in precedenza: l'invio della mail è andato a buon fine.



Ecco la mail di phishing inviata alla vittima.

Messaggio originale

ID messaggio	<1730035743922846600.15536.7294810494069564856@LAPTOP-8DODVQPI>
Creato alle:	27 ottobre 2024 alle ore 14:29 (consegnato dopo 3 secondi)
Da:	maria.zanchetta98@gmail.com Tramite gophish
A:	Maria Bianchi <zanchettamary.19@gmail.com>
Oggetto:	Verifica dell'account per la spedizione
SPF:	PASS con l'IP 209.85.220.41 Ulteriori informazioni
DKIM:	'PASS' con il dominio gmail.com Ulteriori informazioni
DMARC:	'PASS' Ulteriori informazioni

[Scarica messaggio originale](#)

[Copia negli appunti](#)

Ho poi fatto pratica con SET, Social Engineering Toolkit, per clonare il sito suggerito dall'esercizio, ossia <http://testphp.vulnweb.com/login.php>. La clonazione del sito ha avuto successo.

```
Shell No. 1
File Actions Edit View Help
1) Web Templates
2) Site Cloner
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 * — login information below.

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:

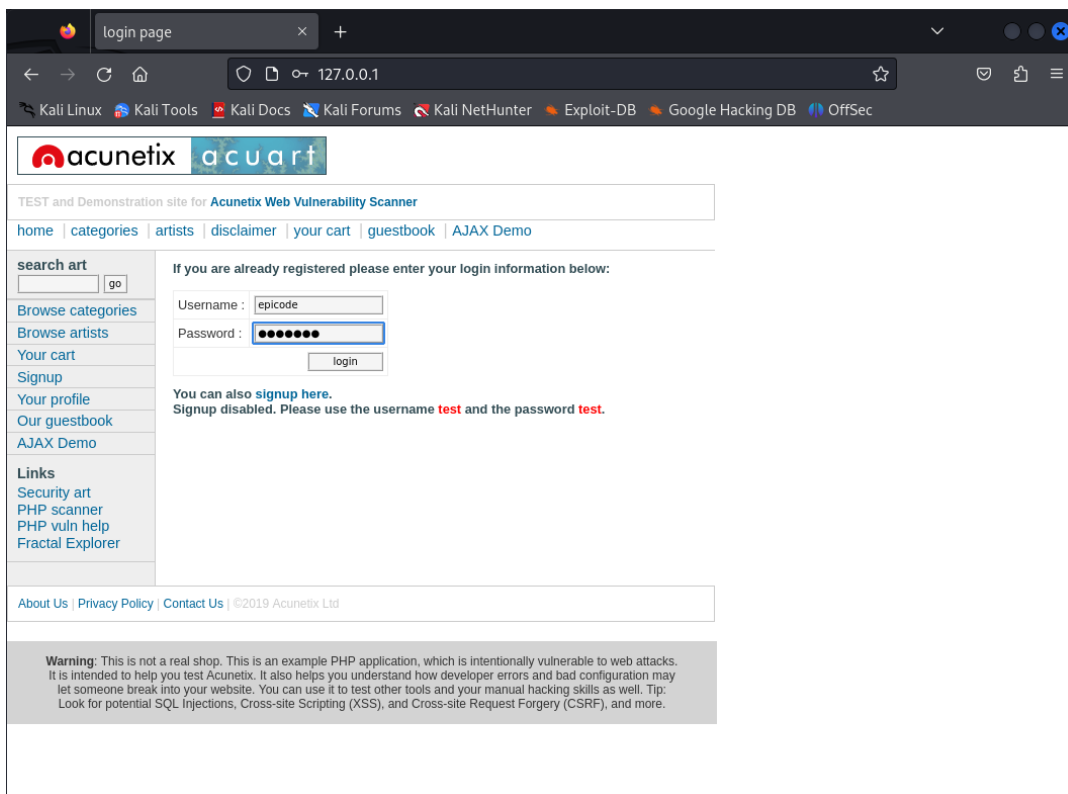
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser 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 [10.0.2.15]: 127.0.0.1
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: http://testphp.vulnweb.com/login.php

[*] Cloning the website: http://testphp.vulnweb.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, 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:
```

Ho poi provato ad inserire delle credenziali nel sito clonato, raggiungendolo con l'IP della mia Kali.



SET ha registrato lo username e la password della vittima, quindi il sito clonato funziona correttamente e raccoglie le informazioni della vittima.

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]: 127.0.0.1
[~] SET supports both HTTP and HTTPS
[~] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: http://testphp.vulnweb.com/login.php

[*] Cloning the website: http://testphp.vulnweb.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, 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 - - [24/Oct/2024 17:02:44] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [24/Oct/2024 17:02:45] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE PASSWORD FIELD FOUND: uname=epicode
POSSIBLE PASSWORD FIELD FOUND: pass=epicode
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Esercizio facoltativo

A questo punto, ho fatto analizzare a ChatGPT la mail di phishing creata con Gophish, chiedendo di verificare dallo screenshot se si tratta di una possibile e-mail malevola e di spiegare gli elementi e gli indicatori che fanno pensare ad una e-mail sospetta. ChatGPT ha riconosciuto con successo che si tratta di una e-mail di phishing malevola, dimostrandosi effettivamente più efficace nel riconoscere la mail malevola, che invece non era stata fermata da sistemi di difesa tradizionali come SPF, DKIM e DMARC. L'uso di un indirizzo privato e non aziendale, la nomina di Gophish e l'oggetto generico della mail hanno fatto sospettare a ChatGPT che si tratti di una mail fraudolenta e non autentica, anche se ha superato i controlli di SPF, DKIM e DMARC. Questo dimostra l'utilità di ricorrere all'intelligenza artificiale per individuare una mail di phishing in caso di sospetti. Questa è la risposta data da ChatGPT.

Esamina questa e-mail, se può essere malevola o sospetta. Se è sospetta, spiega nel dettaglio gli elementi e gli indicatori che fanno pensare ad un'e-mail sospetta.



L'email mostrata potrebbe essere sospetta per alcuni motivi, principalmente legati all'uso di **Gophish** e al contenuto generico dell'oggetto. Ecco un'analisi più dettagliata:

1. Uso di Gophish

- **Gophish** è una piattaforma utilizzata per creare campagne di phishing simulate, generalmente per addestramento alla sicurezza aziendale. Tuttavia, se questa email non fa parte di un esercizio di phishing autorizzato, potrebbe essere un tentativo malevolo.
- Il fatto che sia stata inviata tramite Gophish dovrebbe destare sospetti, soprattutto se l'azienda o il destinatario non è a conoscenza di un test di phishing in corso.

2. Indirizzo Mittente e Destinatario

- Mittente: maria.zanchetta98@gmail.com
- Destinatario: Maria Bianchi <zanchettamaria19@gmail.com>
- L'uso di indirizzi Gmail gratuiti per richieste come "Verifica dell'account per la spedizione" è

- L'uso di indirizzi Gmail gratuiti per richieste come "Verifica dell'account per la spedizione" è sospetto, poiché le email di verifica dell'account di solito provengono da domini aziendali legittimi e non da indirizzi personali o generici.

3. Oggetto Generico

- L'oggetto, "Verifica dell'account per la spedizione", è vago e generico. I messaggi di verifica dell'account normalmente contengono dettagli più specifici per assicurare l'utente sull'autenticità del mittente.

4. Autenticazione (SPF, DKIM, DMARC)

- SPF, DKIM e DMARC risultano tutti con esito **PASS**, il che indica che l'email è tecnicamente autentica e che proviene da un server autorizzato a inviare email per il dominio gmail.com. Tuttavia, questo non elimina la possibilità che si tratti di un'email fraudolenta: il phishing può avvenire anche attraverso account di posta elettronica compromessi o falsi.

5. Possibile Tecnica di Phishing

- La combinazione di un mittente generico, l'oggetto vago e l'uso di Gophish suggerisce che questa email potrebbe essere un tentativo di phishing. Potrebbe mirare a indurre il destinatario a cliccare su un link o a fornire informazioni riservate sotto la copertura di una "verifica dell'account".



Consigli di Mitigazione

- **Non cliccare su link** o scaricare allegati presenti in questo messaggio, se ce ne sono.
- **Contattare il mittente** (se si conosce) tramite un altro canale per verificare la legittimità della richiesta.
- **Segnalare l'email** come phishing o sospetta, specialmente se si tratta di un account aziendale.
- Verificare con il reparto IT o sicurezza aziendale se sono in corso campagne di phishing simulate tramite Gophish.

Conclusione

Data la presenza di Gophish, è probabile che l'email faccia parte di un esercizio di simulazione di phishing. Tuttavia, senza conferme, va trattata con sospetto e considerata potenzialmente malevola.