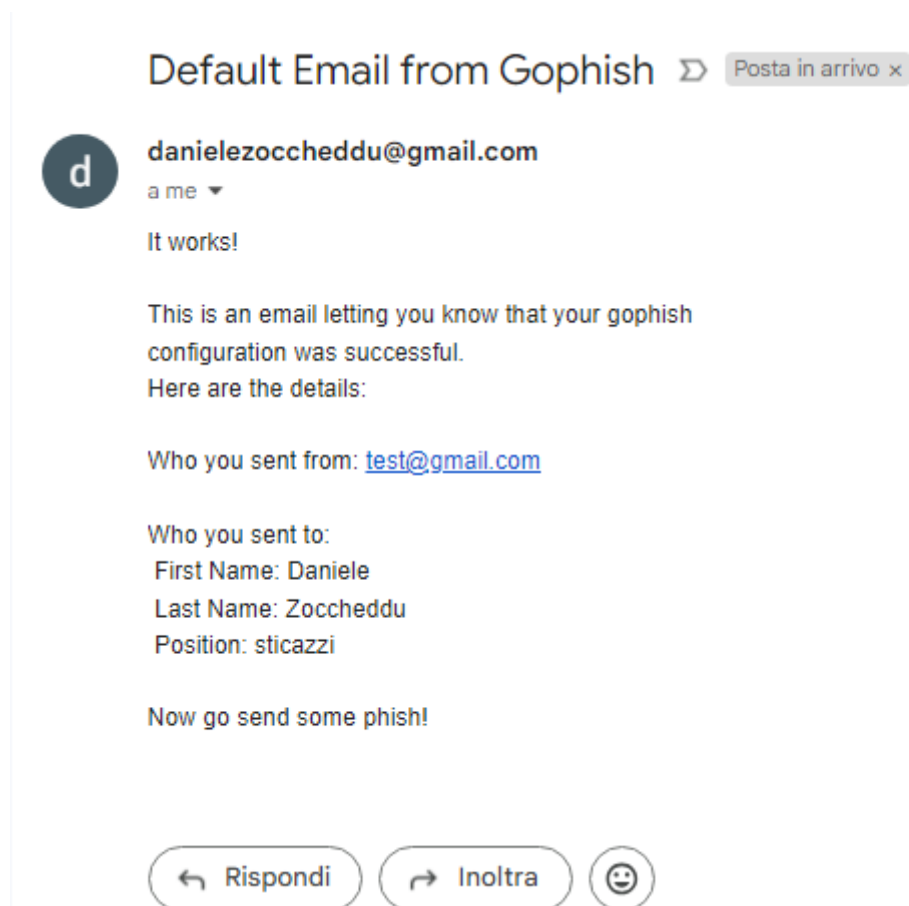


W23D4 - Pratica

Gophish

Ho cambiato utenza e password in admin admin1234!!!



```
[*] 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:
10.0.2.15 - - [25/Oct/2024 14:10:28] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: uname=username
POSSIBLE PASSWORD FIELD FOUND: uname=username
POSSIBLE PASSWORD FIELD FOUND: pass=password
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

ecco l'email che ha inviato (l'ho fatta copiando un mio reso di amazon)

Il tuo reso di Samsung Aspirapolvere Senza Fili... > Posta in arrivo x



danielezoccheddu@gmail.com

a prova ▼



Salve Daniele,

Abbiamo accettato la tua richiesta di reso. Dopo aver ricevuto l'articolo indicato sotto, emetteremo il rimborso.

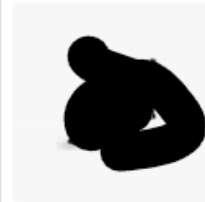
Riepilogo resi

Data del ritiro:

Entro 3 giorni lavorativi†

[Visualizza l'indirizzo di raccolta](#)

[Visualizza lo stato del reso e del rimborso](#)



Rimborso stimato:

Il rimborso verrà visualizzato sul tuo Credit Card in 5-7 giorni lavorativi dopo che avremo ricevuto l'articolo.

Esercizio facoltativo

Ho dato a chatgpt la mail e mi ha risposto così:

Questa email presenta alcuni segnali di possibile phishing, anche se a prima vista potrebbe sembrare un'email di conferma di reso da parte di Amazon. Analizziamo i dettagli critici:

Segnali sospetti

1. Return-Path e indirizzo di provenienza:

- L'email proviene da `<danielezoccheddu@gmail.com>`, un indirizzo generico, non da un dominio ufficiale di Amazon (es. `amazon.it` o `amazon.com`).
- Inoltre, nel campo `X-Google-Original-From` è presente un altro indirizzo, `<test@gmail.com>`, che non è associato ad Amazon.

2. Struttura dei link:

- I link contenuti nel messaggio puntano a `10.0.2.15`, un indirizzo IP privato e non valido per raggiungere Amazon, che utilizza domini sicuri e pubblici (`amazon.it` o `amazon.com`). Questo è un forte segnale di phishing, in cui si tenta di dirottare l'utente verso un sito locale o un server privato.
- Anche il dominio `amazon.it` nei link di esempio contiene codici di tracciamento falsi. Tuttavia, è tipico delle email di phishing inserire URL validi in modo che la mail sembri affidabile, pur indirizzando l'utente altrove quando si clicca sui link principali.

3. Intestazione e testo dell'email:

- Il messaggio contiene dettagli realistici (importo del rimborso, data di ritiro, etc.), ma il layout e la struttura sono più complessi e ingombranti rispetto a una classica email di conferma da Amazon. Il messaggio sembra replicare lo stile di Amazon, ma contiene errori di codifica (ad esempio `è` e `'`), che spesso si trovano in email contraffatte.
- La presenza di un'ampia porzione di codice HTML e CSS di scarsa qualità (ad esempio, con molte istruzioni inline e inutilmente ridondanti) è un altro segnale che si tratta di un'email generata per imitare Amazon.

4. X-Mailer: gophish:

- Il campo `X-Mailer` indica che la mail è stata creata con "gophish," uno strumento comune per simulazioni di phishing usato in contesti legittimi ma anche dai truffatori.

Conclusione

Questa email appare contraffatta. Se cliccato, il link presente potrebbe rimandare a un sito falso progettato per raccogliere dati personali o di pagamento. Raccomando di non cliccare su alcun link e di segnalare il messaggio come phishing.