Walkthrough Tryhackme Free Roadmap

Common Attacks

Presentado por:
Ian E. Acosta Sian
Pentester Jr.

14 de Abril de 2025

Indice

1. Introducción

En esta sala se tratan las técnicas mas comunes que se utilizan para atacar a las personas online como ingenieria social, phishing, malware y ransomware, contraseñas y autenticación, MFA y administradores de contraseñas, seguridad en redes públicas, backups y actualizaciones y parches.
En este documento solo tratare aquellos desafíos que no requieran leer el contenido y contestar las preguntas en base al material proporcionado. ¡Vamos a ello!

2. What is Social Engineering?

Respuesta 1: No answer needed
Respuesta 2: **The Iran Nuclear Programme**

3. Social Engineering: Phishing

Respuesta 1: No answer needed

En este desafío se vera si luego de leer todo el material teórico pueden identificar mails de phishing. En el primer test se presenta un mail proveniente de **Google Support** con dirección **support@google.com**.

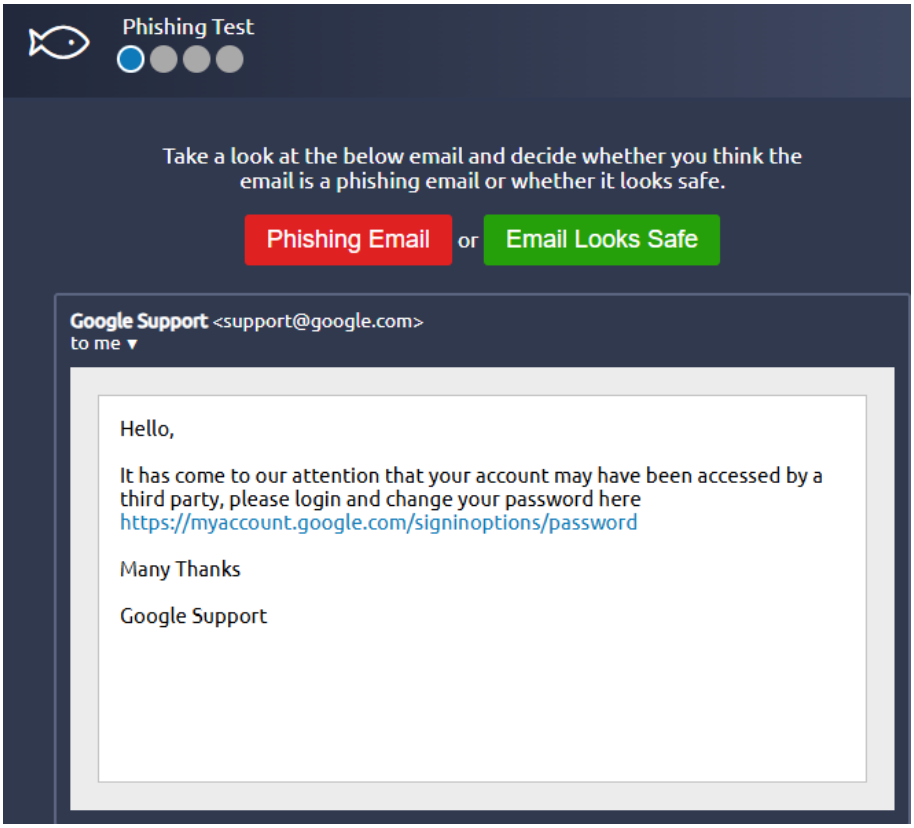

Figura 1: Mail enviado por Google Support

Al analizar el mail se puede ver que el link que proporciona redirecciona a una pagina web diferente a la que pertenecería la dirección.

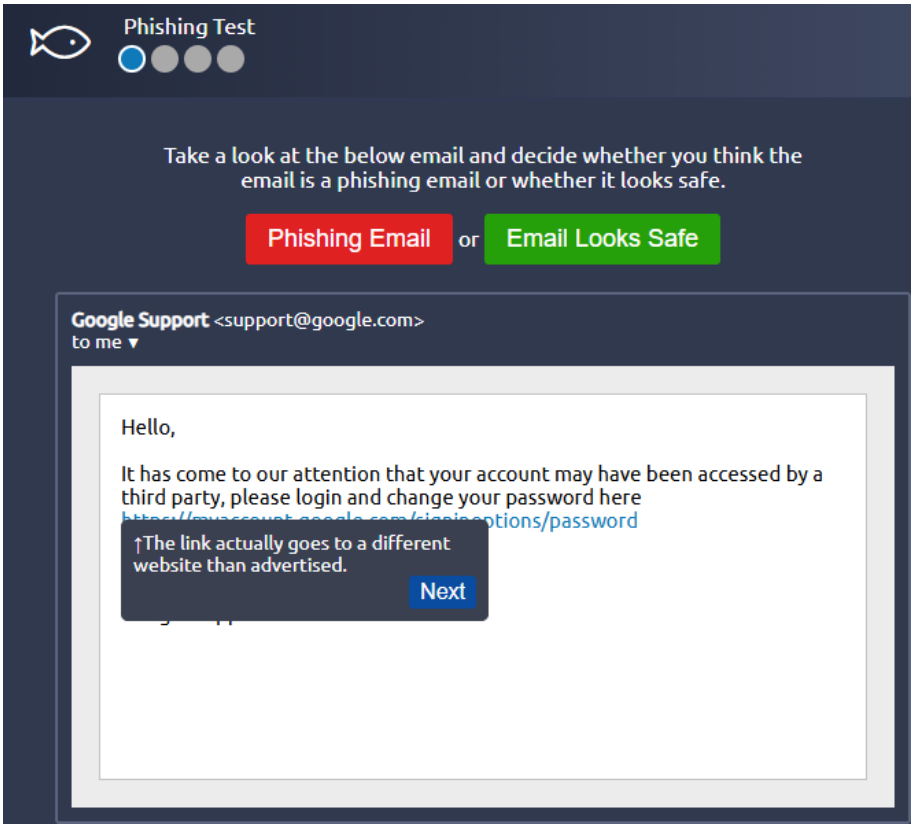

Figura 2: Elemento que hace que se un phishing

Por lo que la respuesta a este test seria que es un mail de phishing. Para el segundo test podemos determinar que es un mail de phishing ya que hay diferencia entre la dirección **accounts@thebankingroup.thm** y el link que redirecciona a **http://bankinggroup.sharedhosting/downloads/finance.xlsx**, la diferencia estaría en que hay una **g** de mas en el link.

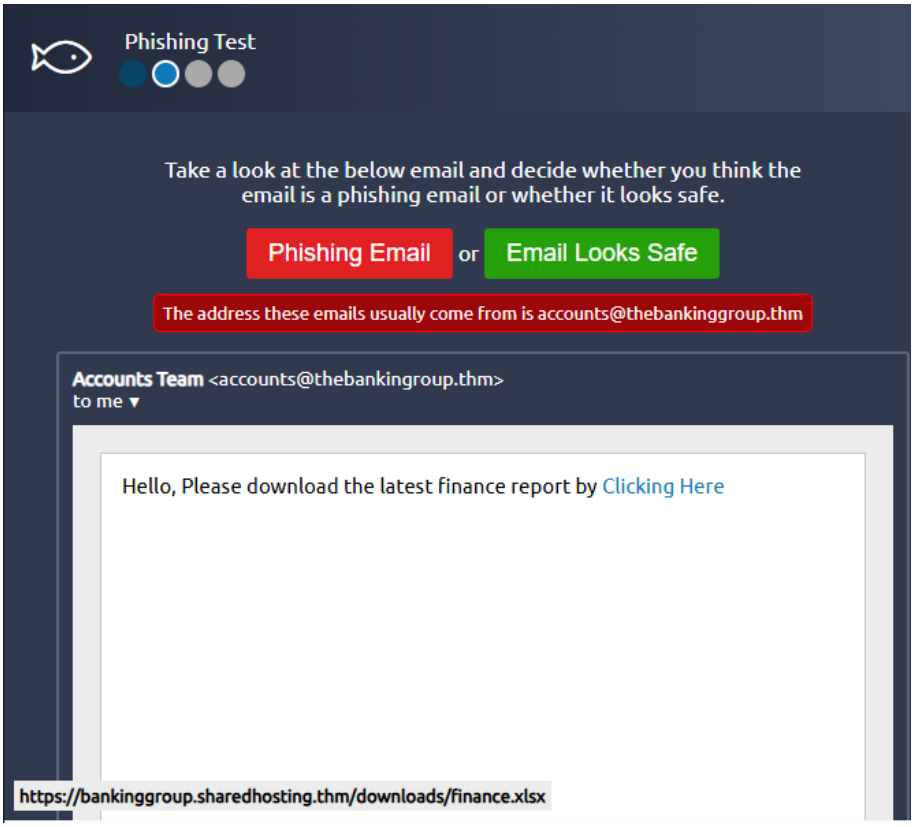

Figura 3: mail de accounts@thebankingroup.thm

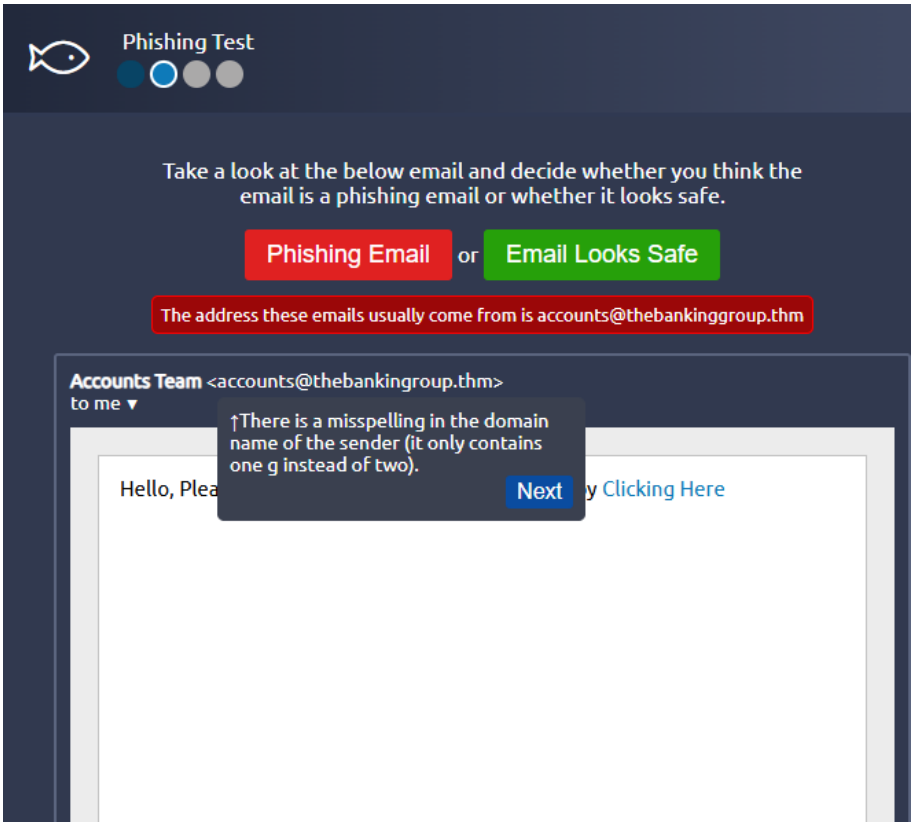

Figura 4: Respuesta del test

En el siguiente test se presenta un mail de **TryHackMe** con dirección **noreplay@tryhackmesupport.thm** y un link adjunto que redirecciona a **https://tryhackme.com**.

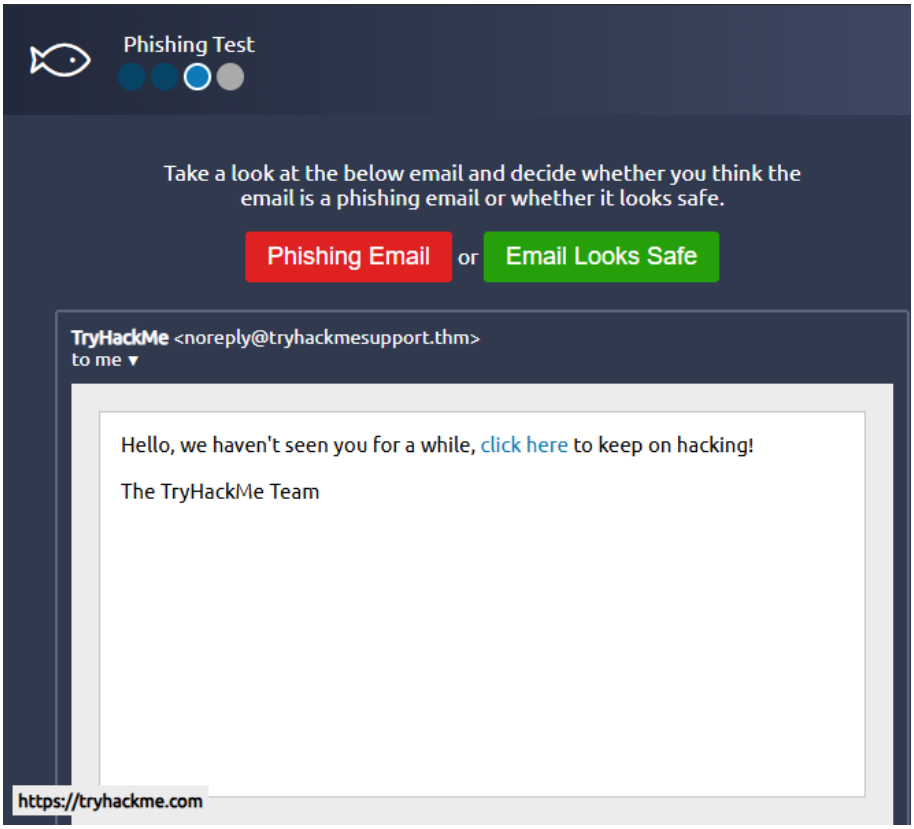

Figura 5: Mail de TryHackMe

Este mail es totalmente legitimo ya que todo esta correcto, tanto al mail como el sitio al que redirecciona concuerda con el mail, validando la identidad de entidad que dice ser.
Para el ultimo test se presenta un mail de **accounts@acmeitsupport.thm** con un archivo PDF adjunto. Acá será un mail de phishing por la razón que nunca hay que confiar en archivos adjuntos de fuentes que no conozcas o inesperadas, ya que puede tratarse de un malware.

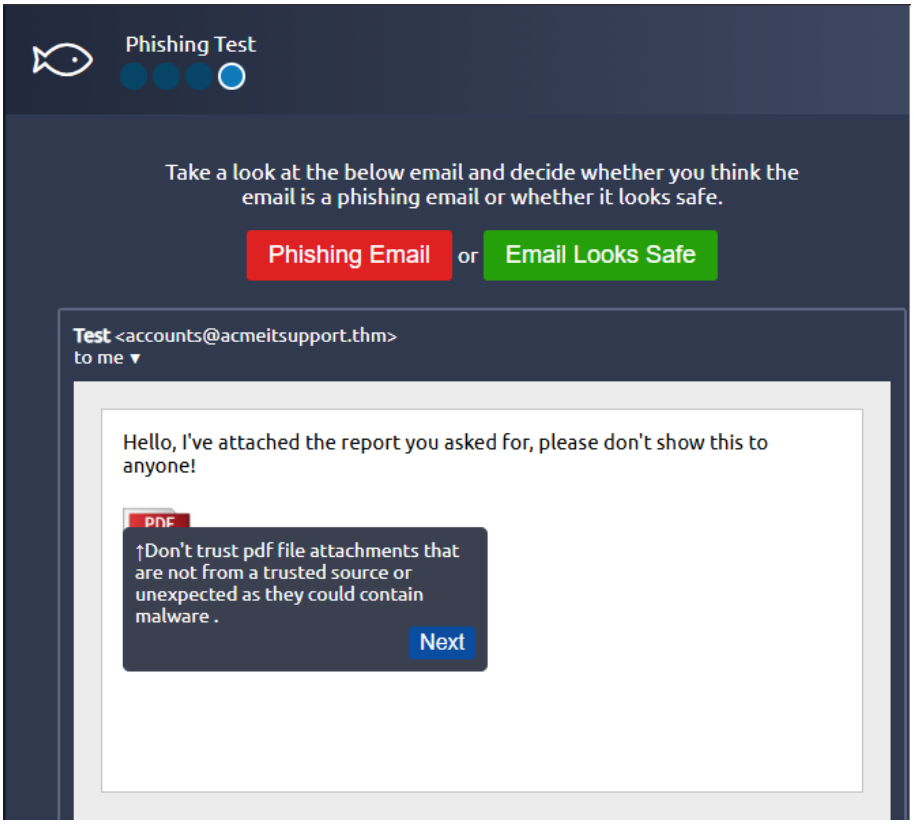

Figura 6: Mail con archivo adjunto

Terminando cada uno de las pruebas se muestra el flag **THM{I_CAUGHT_ALL_THE_PHISH}** para poder responder a la respuesta 2 del desafío.

4. Malware and Ransomware

Respuesta: **Bitcoin**

5. Passwords and Authentication

Respuesta 1: No answer needed
Respuesta 2: No answer needed
Respuesta 4: No answer needed

Para resolver esta tarea debemos abrir el sitio web que nos brinda la sala **The Great Hash Cracker!**, copiamos y pegamos la lista de posibles contraseñas y la pegamos en la pagina, damos en **Go!** para que se comprube el **Hash**.

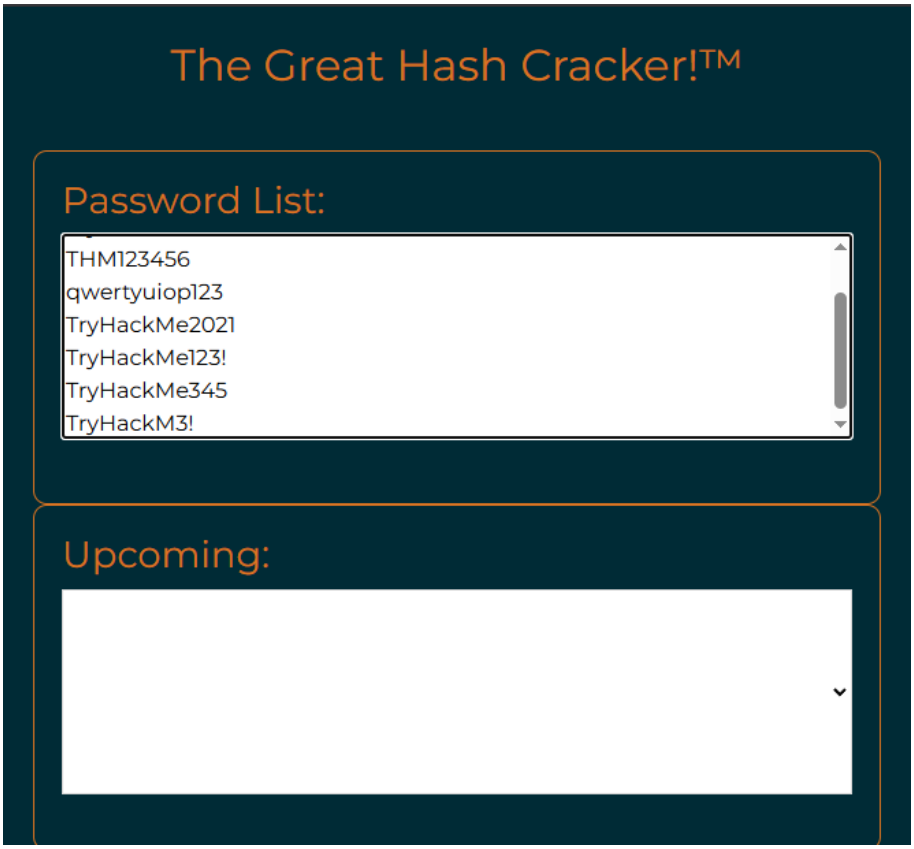

Figura 7: The Great Hash Cracker! con lista de contraseñas

Así al finalizar podemos dar con la contraseña **TryHackMe123!** que es la respuesta 3 para responder a este desafío.

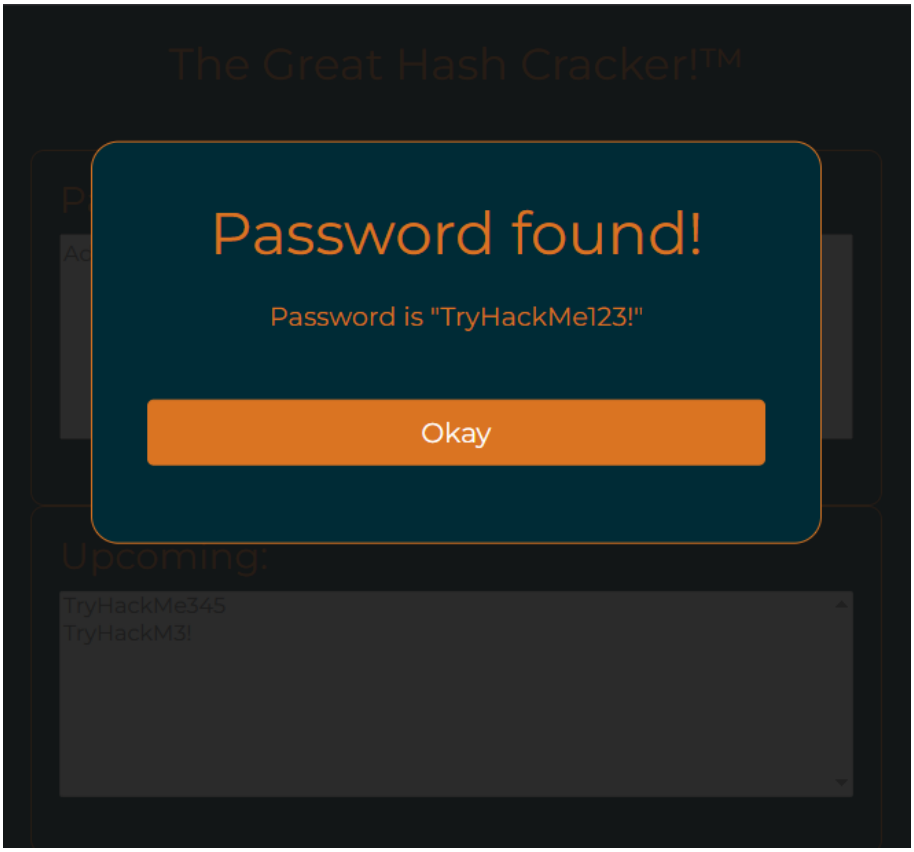

Figura 8: Contraseña encontrada

6. Multi-Factor Authentication and Password Managers

Respuesta: **App**

7. Public Network Safety

Respuesta 1: No answer needed
Respuesta 2: No answer needed

8. Backups

Respuesta 1: **3**
Respuesta 2: **1**

9. Updates and Patches

Respuesta 1: No answer needed