Ataques Comunes

Con ejercicios prácticos, vea cómo ocurren los ataques comunes y mejore su higiene cibernética para mantenerse más seguro en línea.

Tarea 1: Introducción.

En esta sala se analizarán algunas de las técnicas más comunes utilizadas por los atacantes para atacar a personas en línea. También enseñará algunas de las mejores formas de prevenir el éxito de cada técnica.

- **No answer needed**

Tarea 2: Ingeniería Social (Ataque Común).

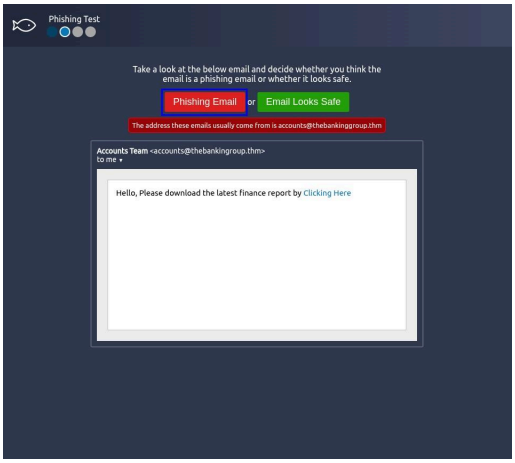
¿Qué es la Ingeniería Social?
La ingeniería social es un tipo de ciberataque que apunta a las personas para obtener información, a menudo llamada “People Hacking”. Consiste en manipular a la víctima para obtener datos, escalando poco a poco hasta acceder a información valiosa como cuentas bancarias.

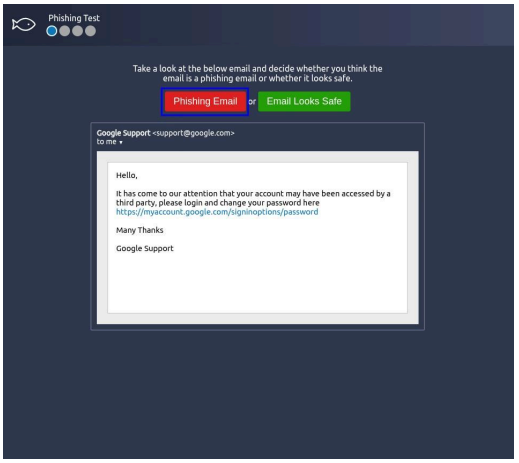
- Read the task information and watch the attached videos
  - **No answer needed**
- **Pregunta:** ¿Cuál era el objetivo original de Stuxnet?
  - **Respuesta: The Iran Nuclear Programme**

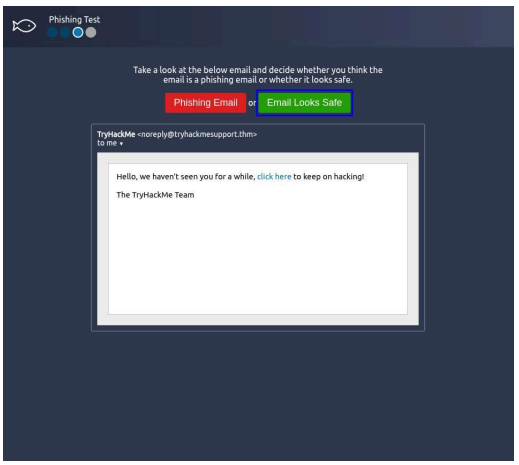
Tarea 3: Ingeniería Social: Phishing.

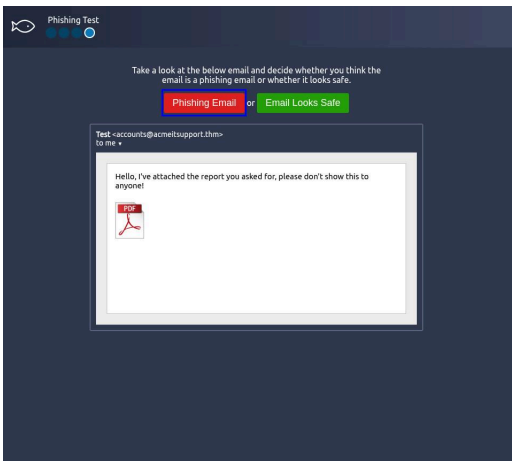
El phishing es un ciberataque común para engañar a individuos y empresas, como primer paso para infiltrarse en redes corporativas. Aunque hay herramientas para combatirlo, sigue siendo muy efectivo.

- **No answer needed**
- **Pregunta:** What is the flag?









➢ **Respuesta: THM{I_CAUGHT_ALL_THE_PHISH}**

Tarea 4: Malware y Ransomware

El malware es un software malicioso usado para robar datos, dañar sistemas o ejecutar comandos remotos (C2). Incluye tipos como ransomware y permite controlar equipos infectados.

- **Pregunta:** What currency did the Wannacry attackers request payment in?
  - ➢ **Respuesta: Bitcoin**

Tarea 5: Contraseña y autenticación.

Las contraseñas son clave en la autenticación, pero su mala gestión (como reutilizarlas o exponerlas) las vuelve vulnerables, incluso si son fuertes.

- **Put yourself in the shoes of a malicious hacker. You have managed to dump the password database for an online service, but you still have to crack those hashes!**
  Click the green button at the start of the task to deploy the interactive hash brute-forcer!
  - ➢ **No answer needed**
- **Based on the content of the website, you have generated a list of likely passwords, which is as follows:**

  TryH@ckMe
  TryHackMe123
  THM123456
  qwertyuiop123
  TryHackMe2021
  TryHackMe123!
  TryHackMe345
  TryHackM3!

  Copy the list of passwords into the "Password List" field of the hash cracker, then click "Go"!
  - ➢ **No answer needed**
- **Look at the "Current Word / Hash" section of the hash cracker.**
  Notice that for each word in the list you entered, the cracker is creating an MD5 hash of the word then comparing it to the Target Hash. If the two hashes match then the password has been found!
  The hash cracker should find the password that matches the target hash very quickly.
- **Pregunta:** What is the password?

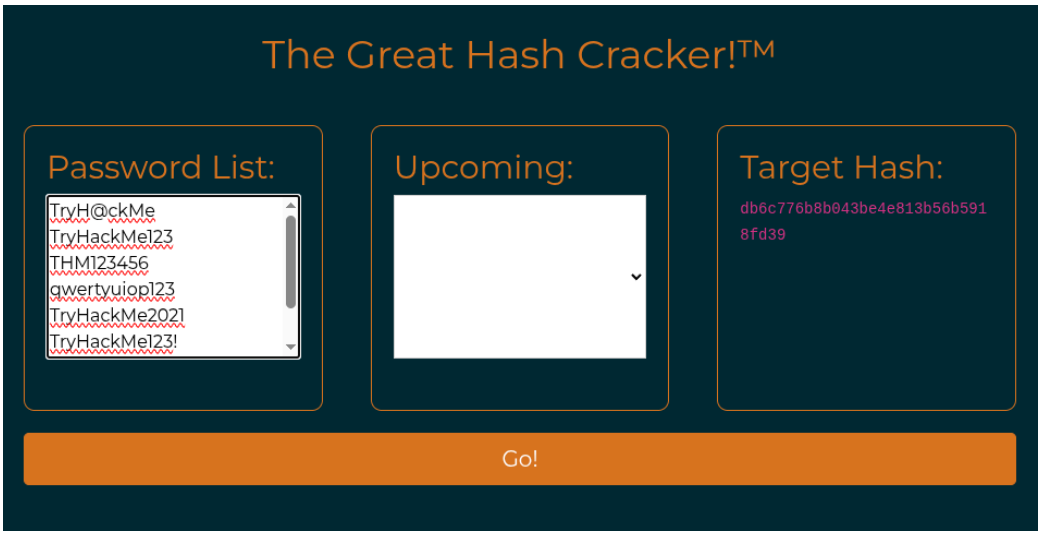


Figura 1

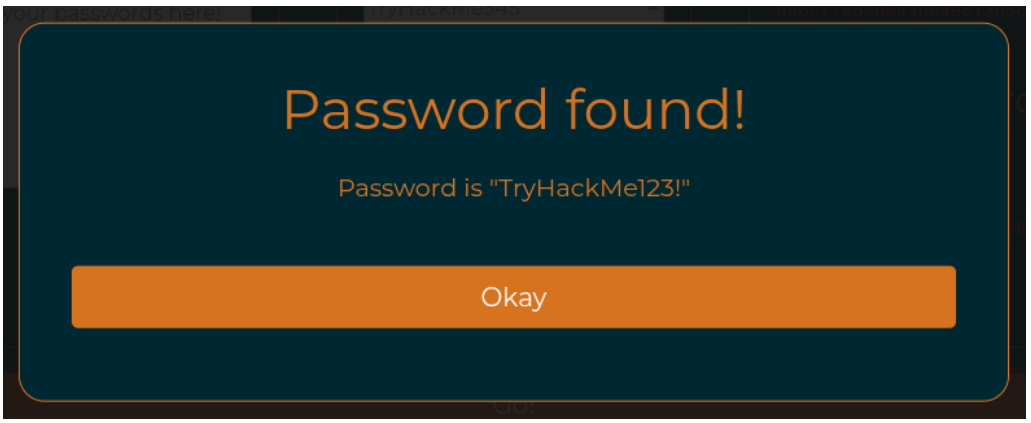


Figura 2 (Resultado)

- ➢ **Respuesta: TryHackMe123!**

- ❖ **This is a very simple, browser-based example; however, in reality local hash cracking with a wordlist isn't any more complex from a high-level perspective — it's the same technique, but with a lot more potential passwords!**
  Hopefully this example illustrates why it is so important to choose a strong password — even if the passwords are hashed appropriately.
  In the next task we will look at some of the common account protection measures, as well as how to generate secure passwords.
  - ➢ **No answer needed**

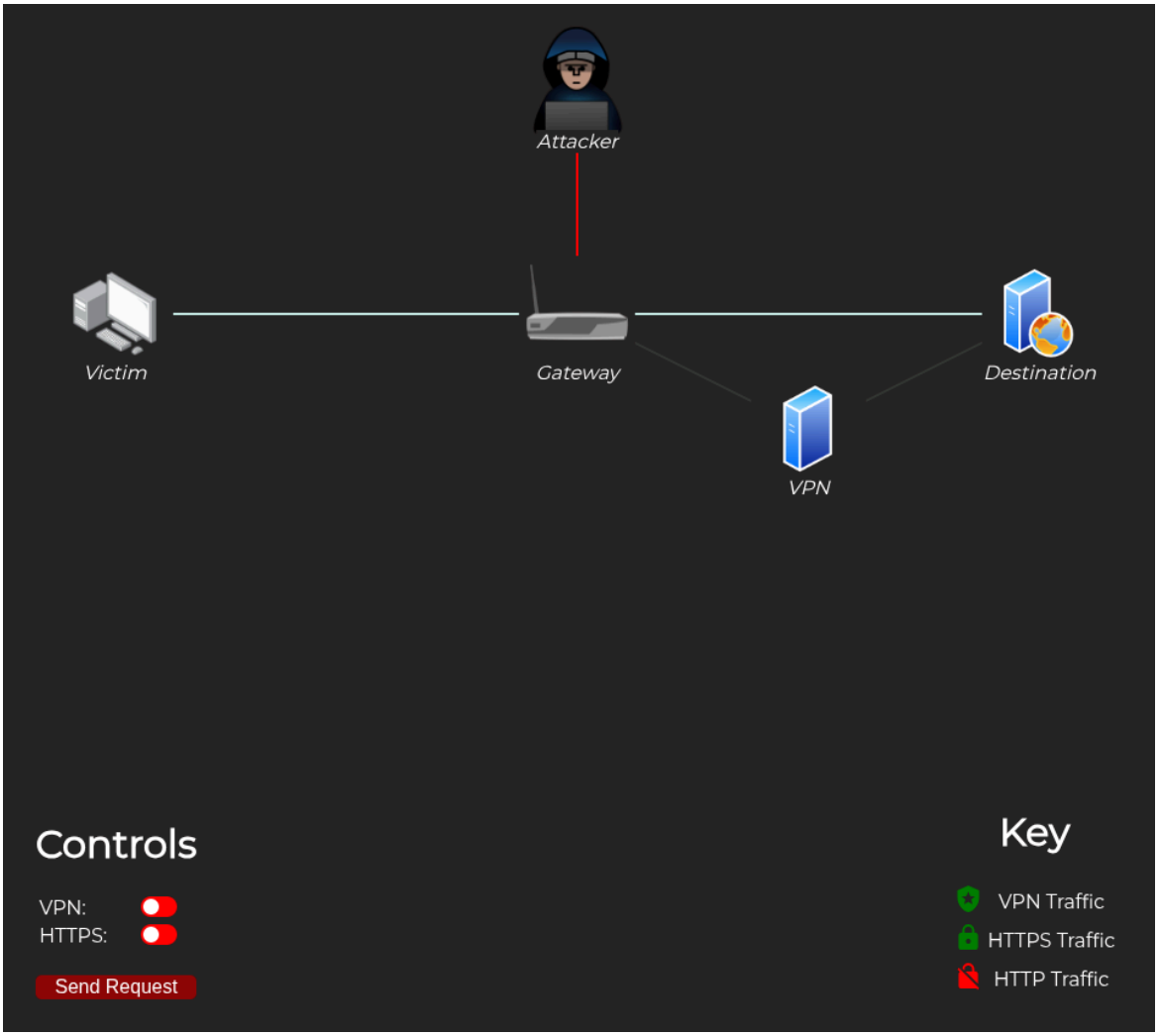
Tarea 6: Administradores de contraseña y autenticación multifactor.

Esta tarea explica cómo mejorar la seguridad de contraseñas usando gestores de contraseñas y autenticación multifactor (MFA).

- ❖ **Pregunta:** Where you have the option, which should you use as a second authentication factor between SMS based TOTPs or Authenticator App based TOTPs (SMS or App)?
  - ➢ **Respuesta: App**

Tarea 7: Seguridad de la Red Pública.

El WiFi público, aunque conveniente, representa un riesgo de seguridad importante que muchos usuarios subestiman.



- **Deploy the interactive content by clicking the green button at the top of the task.**
  - **No answer needed**
- **The interactive content for this task demonstrates what can happen if information is sent over a potentially unsafe network with various types of encryption (or lack thereof). There is no flag for this task, but you are encouraged to try each of the different scenarios, mixing and matching the options provided in the control box at the bottom right of the screen.**
  - **No answer needed**

Tarea 8: Copias de seguridad.

Las copias de seguridad son esenciales para proteger y recuperar datos críticos, ya sea con métodos simples (Google Drive) o soluciones automatizadas.

- **Pregunta:** What is the minimum number of up-to-date backups you should make?
  - **Respuesta: 3**
- **Pregunta:** Of these, how many (at minimum) should be stored in another location?
  - **Respuesta: 1**

Tarea 9: Actualización y parches.

Las actualizaciones de software corrigen errores, añaden funciones y parchean vulnerabilidades críticas para mantener la seguridad.

- **(Optional) Complete the Blue room on TryHackMe to see the brutal effects of the Eternal Blue exploit in action against an unpatched machine for yourself!**
  - **No answer needed**

Tarea 10: Conclusión.

Para concluir: Existen múltiples vectores de ataque cibernético, pero también defensas accesibles. Esta sala enseña medidas prácticas de seguridad para usuarios, sin requerir expertise técnico.

- **No answer needed**