Bitácora de Laboratorio - TryHackMe

# 1. Información general

Nombre del laboratorio: Offensive Security Intro

Plataforma: TryHackMe

Fecha de realización: 18/05/2025

Duración aproximada: 15 Mins.

# 2. Objetivos del laboratorio

- Comprender el rol de un hacker ético  
- Aprender a identificar vulnerabilidades comunes en sitios web  
- Realizar pruebas básicas de penetración en un entorno controlado  
- Familiarizarse con herramientas y técnicas de seguridad ofensiva

# 3. Actividades realizadas

En este laboratorio realice una simulación de un ataque a una web de “fakebank.thm” que tenía una vulnerabilidad en un directorio oculto.

Primero se realizó un escaneo a la Web con Gobuster, utilizando “gobuster dir -u http://fakebank.thm -w /usr/share/wordlists/dirb/common.txt” la wordlist fue entregada por el curso, se encontró una dirección oculta disponible /bank-transfer.

Luego se accedió a la dirección encontrada y se simulo una transferencia logrando la realización de forma exitosa.

Finalmente se verifico que la realización de la transferencia fuera exitosa volviendo a la pagina principal reflejando la transacción.

# 4. Capturas de pantalla (opcional)

Capturas de pantalla:

Texto

El contenido generado por IA puede ser incorrecto.

Interfaz de usuario gráfica, Texto, Aplicación

El contenido generado por IA puede ser incorrecto.

# 5. Reflexión técnica y aprendizajes

Esto me hizo reflexionar sobre la importancia de ocultar correctamente directorios administrativos o sensibles en plataformas institucionales y cómo las pruebas de caja negra pueden revelar errores básicos de configuración.

# 6. Palabras clave aprendidas

* Gobuster.
* Directorio oculto
* Escaneo web