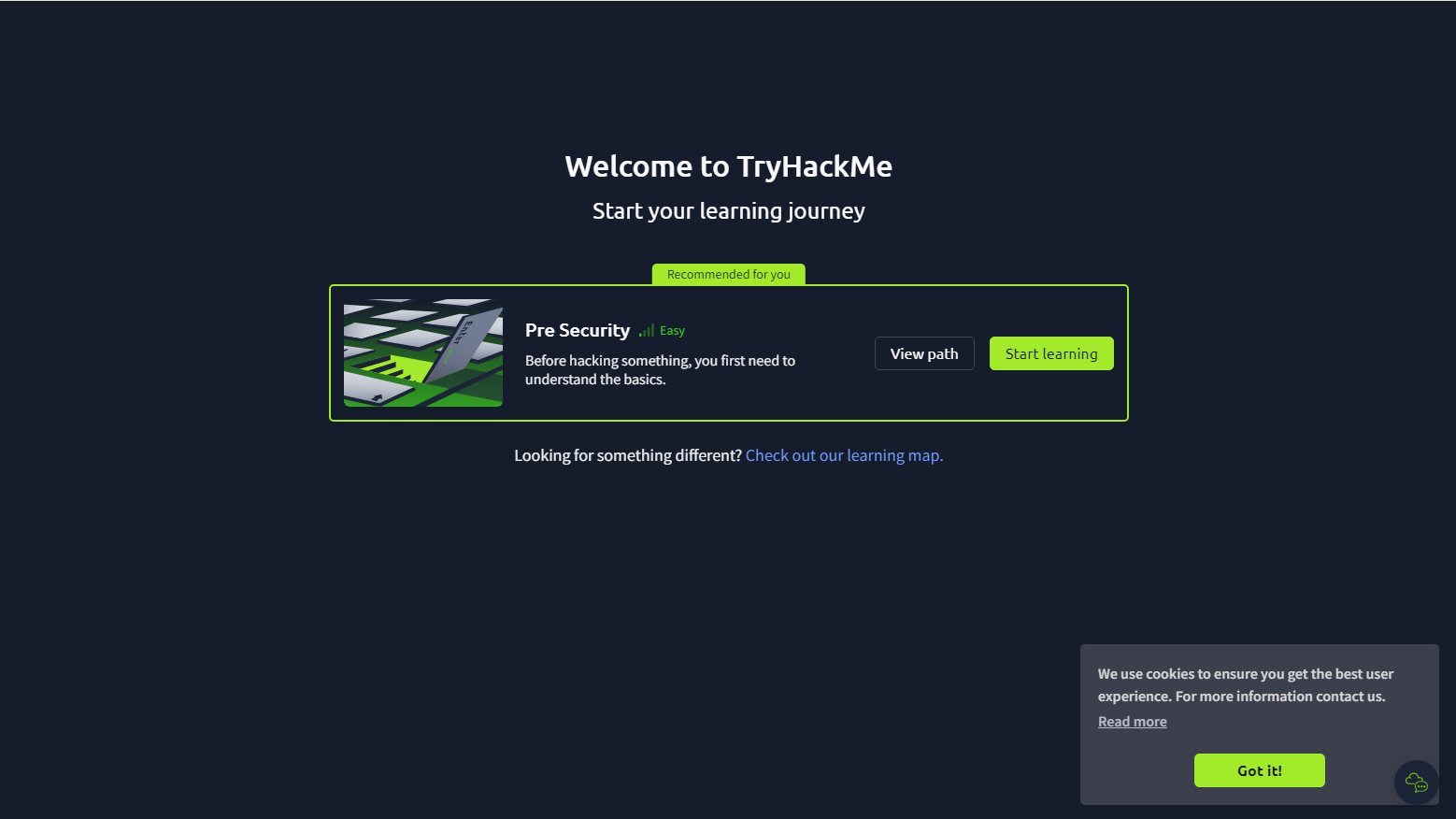
**Práctica de Hacking Ético**

Actividades

**1. Registro en Plataformas**

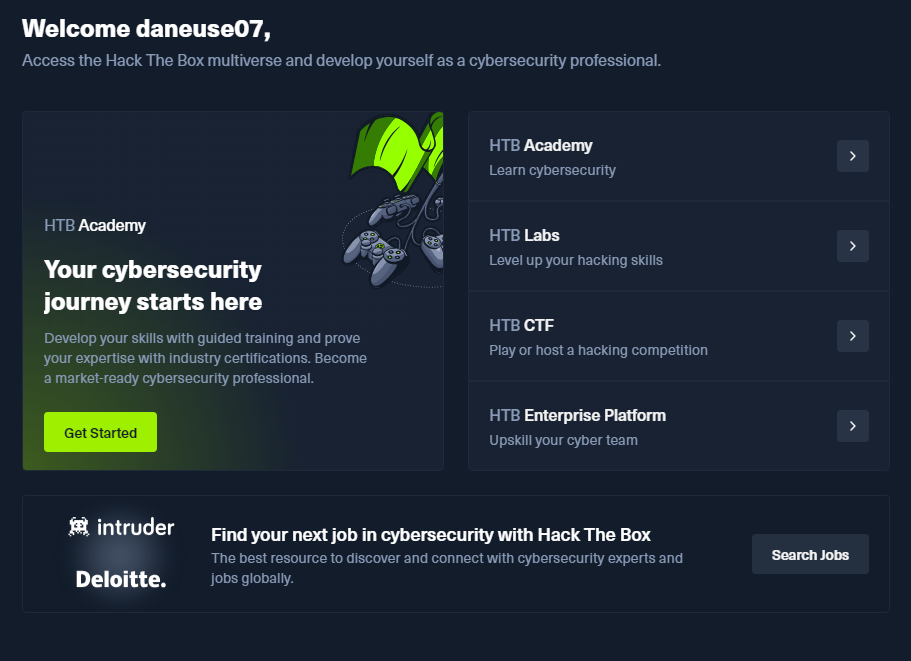
1. Crear una cuenta en TryHackMe: Visita TryHackMe y regístrate para obtener una cuenta

gratuita.



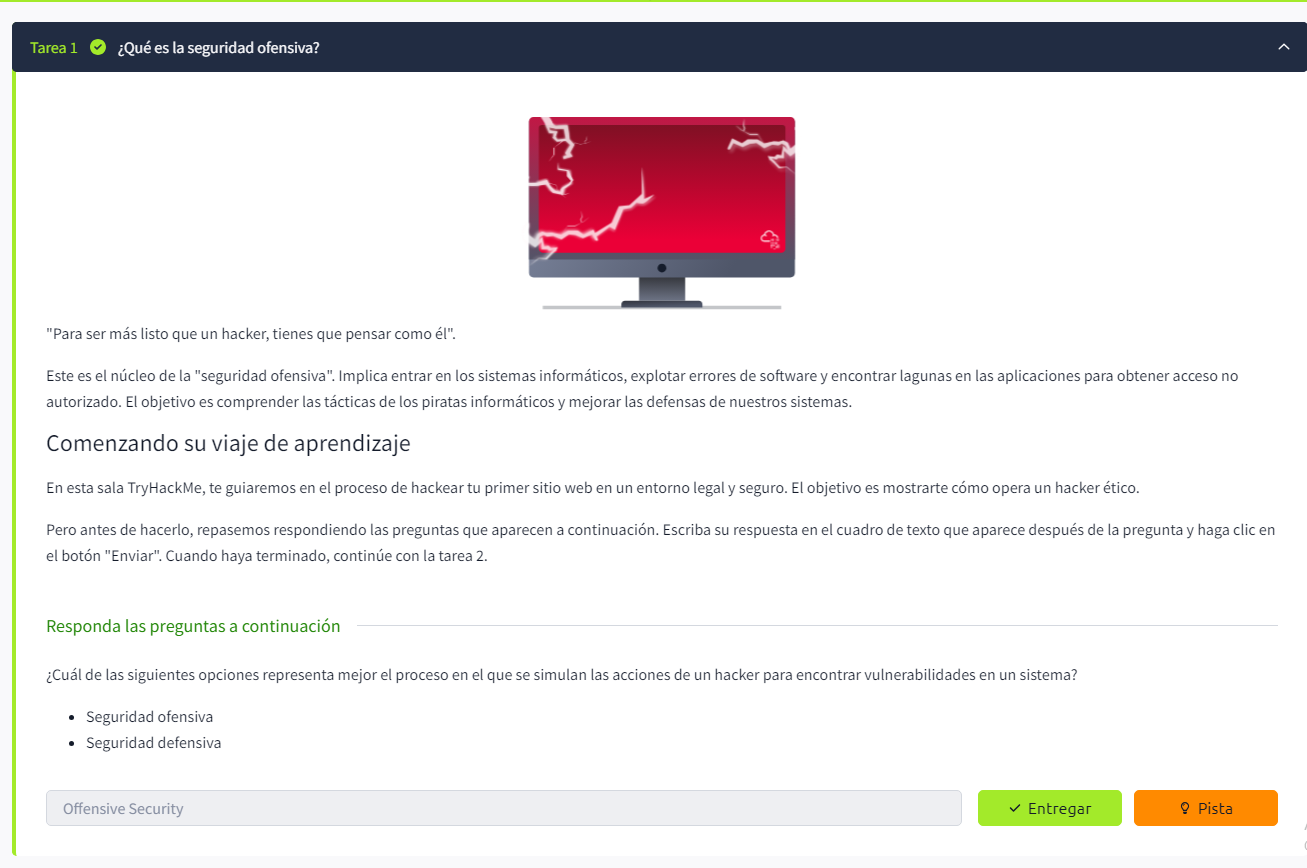
2. Crear una cuenta en Hack The Box: Visita Hack The Box y regístrate para obtener una cuenta

gratuita.



**2. Introducción a TryHackMe**

1. Completar la sala “Introduction to Cyber Security”: En TryHackMe, busca y completa la sala “Introduction to Cyber Security” para familiarizarte con los conceptos básicos.



Tarea 1: Aprendí sobre la seguridad ofensiva, que implica simular las acciones de un hacker para encontrar vulnerabilidades en un sistema. Esto permite comprender las tácticas de los atacantes y fortalecer las defensas.



Tarea 2: Realicé un ejercicio práctico de hacking ético en un entorno simulado utilizando herramientas como Gobuster para encontrar directorios ocultos y acceder a ellos.

Abrí la máquina virtual y la terminal dentro de TryHackMe.

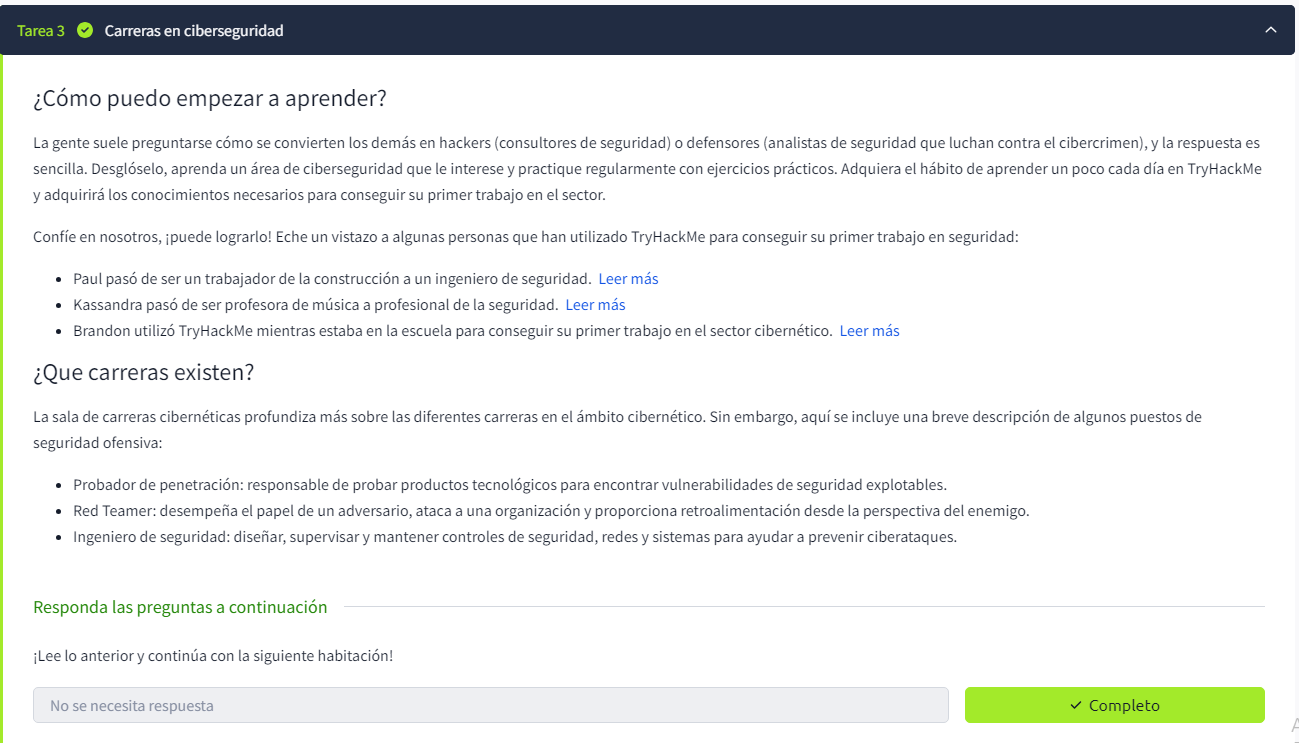
Ejecuté el comando:

gobuster -u http://fakebank.thm -w wordlist.txt dir

Esto reveló directorios ocultos, incluido /bank-transfer.

Accedí al directorio desde el navegador y transferí $2000 desde la cuenta 2276 a mi cuenta 8881.

Confirmé la transferencia verificando el nuevo saldo y el mensaje BANK-HACKED.

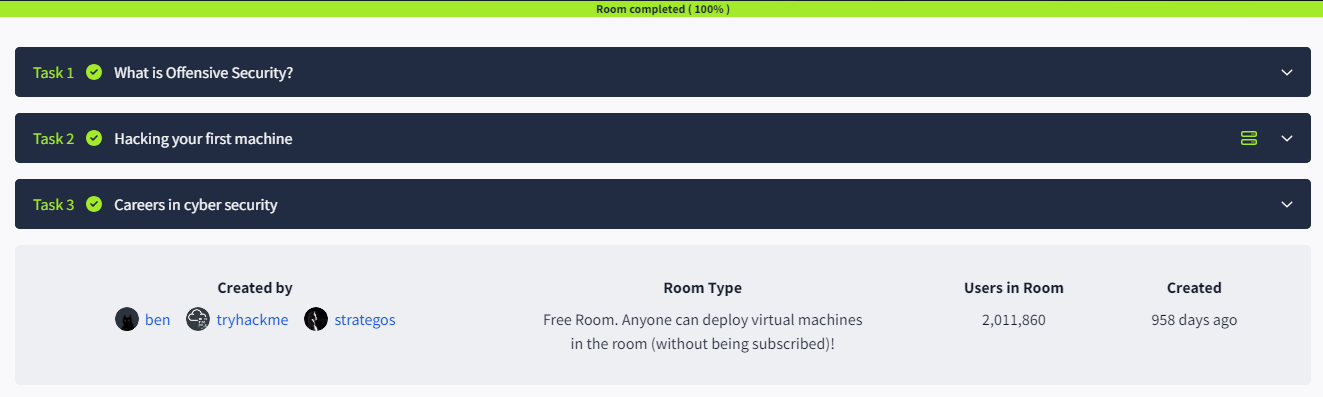


Tarea 3: Revisé información sobre las diferentes áreas en las que se puede trabajar en ciberseguridad. Me familiaricé con roles como:

Probador de penetración: Encuentra vulnerabilidades en productos tecnológicos.

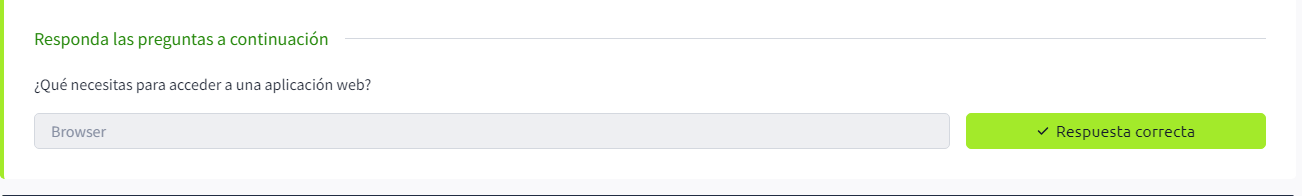
Red Teamer: Simula ataques para identificar fallos desde la perspectiva de un adversario.

Ingeniero de seguridad: Diseña y mantiene controles de seguridad para prevenir ciberataques.



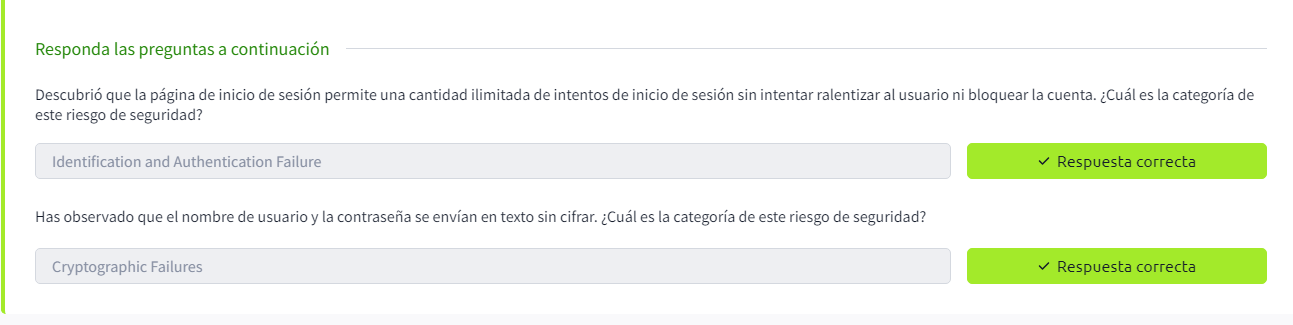
2. Explorar la sala “Web Application Security”: Completa los desafíos de la sala “Web Application

Security” para aprender sobre vulnerabilidades comunes en aplicaciones web.



Tarea 1: En esta tarea aprendí sobre las aplicaciones web, que son programas que se ejecutan en un servidor remoto y se acceden a través de un navegador web estándar como Chrome, Firefox o Safari. Estas aplicaciones no requieren instalación en el equipo del usuario, lo que las hace más accesibles y versátiles. Se presentaron ejemplos de aplicaciones web como correo electrónico, paquetes de oficina en línea y tiendas en línea.

Además, entendí cómo funcionan las bases de datos en las aplicaciones web y cómo se conectan con servidores para manejar información como productos, clientes y ventas. También se explicó la importancia de los programas de recompensas por errores, que incentivan a los expertos en seguridad a identificar vulnerabilidades en los sistemas de una empresa.



Tarea 2: Estudié los riesgos principales:

Identification and Authentication Failure: Contraseñas débiles o intentos ilimitados de inicio de sesión.

Broken Access Control: Acceso no autorizado a datos de otros usuarios.

Inyección: Inserción de código malicioso por falta de validación.

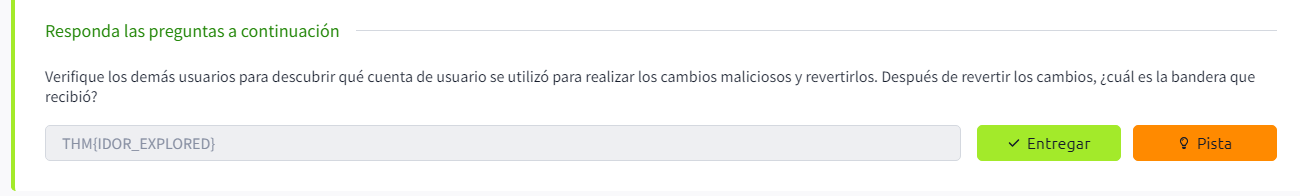
Cryptographic Failures: Envío de datos sin cifrar o uso de algoritmos débiles.

Respondí las preguntas:

Intentos ilimitados de inicio de sesión: Identification and Authentication Failure.

Datos enviados sin cifrar: Cryptographic Failures.

La actividad me permitió comprender cómo proteger aplicaciones web frente a ataques comunes.



Exploré la vulnerabilidad IDOR: Identifiqué cómo un atacante podría acceder o manipular datos restringidos al probar IDs secuenciales en URLs.

Actividad realizada:

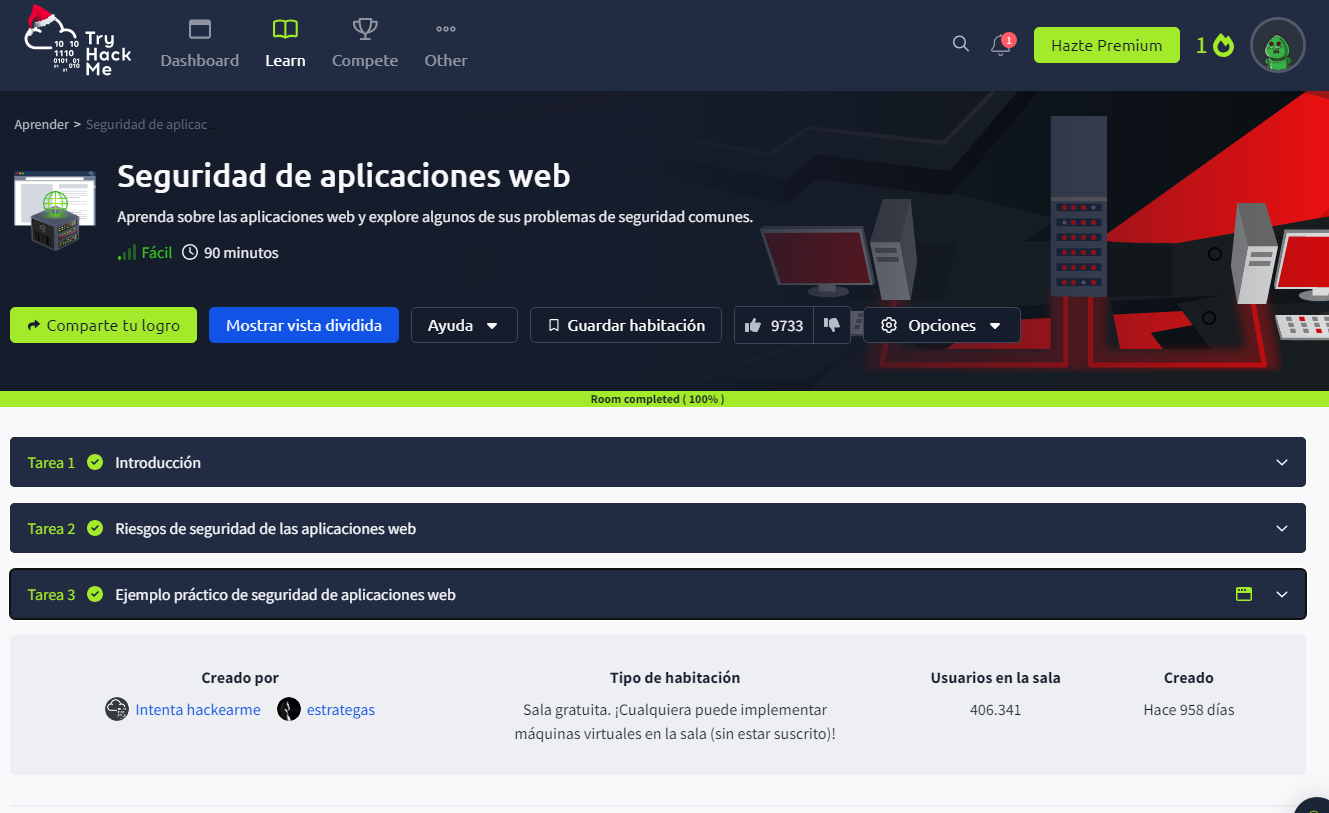
Analicé el sistema de inventario vulnerable.

Accedí a otras cuentas de usuario al modificar el parámetro id en la URL.

Identifiqué al usuario que realizó los cambios maliciosos y revertí sus acciones.

Resultado: Recuperé el funcionamiento correcto del inventario.

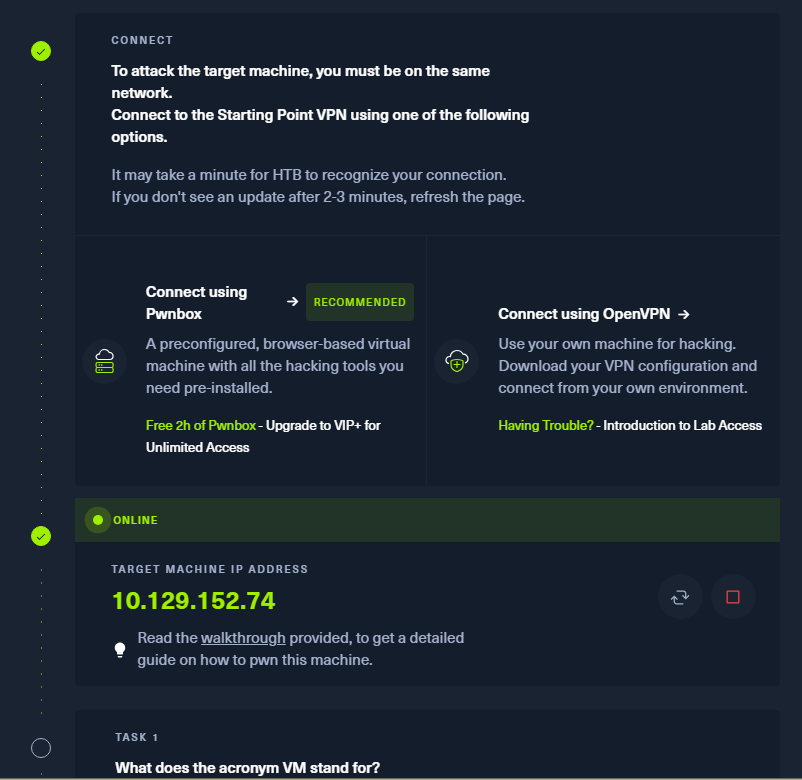
Obtuve la bandera: THM{IDOR\_EXPLORED}



**3. Desafíos en Hack The Box**

1. Resolver máquinas “Starting Point”: En Hack The Box, accede a la sección “Starting Point” y

resuelve las máquinas disponibles para principiantes.



Conexión a la VPN de HTB: Me conecté a la VPN de Hack The Box usando la opción de OpenVPN para acceder a la red de laboratorio de HTB.

Interacción con la máquina objetivo: Utilicé herramientas de línea de comandos y servicios de escaneo para identificar información relevante y acceder al sistema.

Pruebas de conectividad: Usé comandos como ping para verificar la conexión a la máquina objetivo.

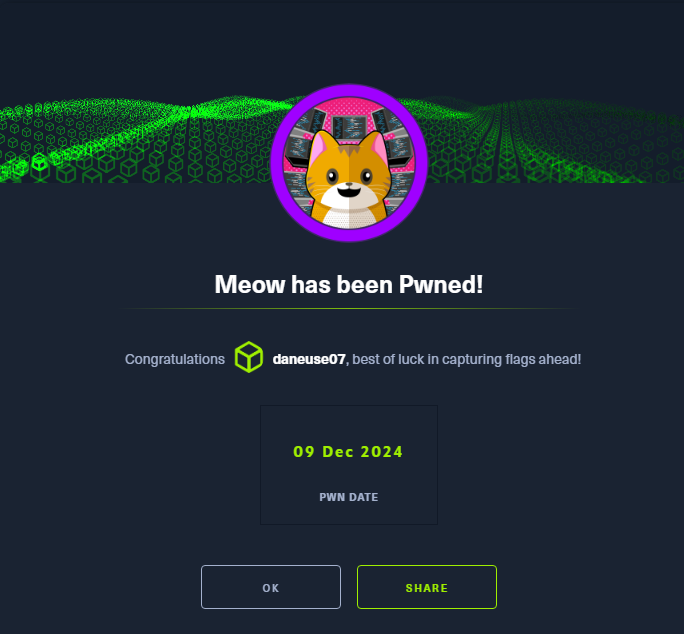
Escaneo de puertos: Empleé herramientas para encontrar puertos abiertos y los servicios que se ejecutan en ellos, como nmap.

Exploración de servicios: Identifiqué el servicio corriendo en el puerto 23/tcp (telnet) y confirmé la posibilidad de login.

Acceso a la máquina: Descubrí un usuario que podía iniciar sesión en la máquina a través de telnet con una contraseña en blanco.

Obtención de privilegios de root: Exploté las vulnerabilidades para ganar acceso de root y localicé la flag de root.

Entrega de la flag: Ingresé la bandera encontrada en la plataforma de HTB en la sección "Submit Flag" para completar el desafío.



2. Participar en un CTF (Capture The Flag): Participa en un desafío CTF en Hack The Box para poner

a prueba tus habilidades en un entorno competitivo.

**4. Análisis de Vulnerabilidades**

1. Utilizar herramientas en línea: Usa herramientas en línea como Pentest-Tools para realizar

análisis de vulnerabilidades en sitios web de prueba proporcionados por las plataformas.

