Práctica de hacking ético que no requiere la instalación de software en los equipos de los estudiantes.

Utilizaremos plataformas en línea que ofrecen entornos controlados para practicar habilidades de

hacking ético.

Práctica de Hacking Ético

Objetivo

El objetivo de esta práctica es que los estudiantes aprendan y apliquen técnicas de hacking ético

utilizando plataformas en línea, sin necesidad de instalar software adicional en sus computadoras.

Requisitos Previos

• Conocimientos básicos de redes y sistemas operativos.

• Familiaridad con conceptos de seguridad informática.

Herramientas Necesarias

• TryHackMe: Plataforma en línea para aprender y practicar hacking ético.

• Hack The Box: Plataforma en línea con desafíos de hacking ético.

• Google Chrome o Mozilla Firefox: Navegadores web para acceder a las plataformas.

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.

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

Security” para aprender sobre vulnerabilidades comunes en aplicaciones web.

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.

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.

5. Documentación

1. Informe de Resultados: Documenta todos los pasos realizados, las herramientas utilizadas, las

vulnerabilidades encontradas y las explotaciones realizadas. Incluye capturas de pantalla y

explicaciones detalladas.

Evaluación

La evaluación se basará en la precisión y claridad del informe de resultados, así como en la capacidad del

estudiante para identificar y explotar vulnerabilidades de manera ética y responsable.