



# Pentester Mentor Junior

Conviértete en un **Hacker Ético Profesional**  
en sólo **2 meses.**

Aprenderás mediante el **Gaming** y **desde Cero**.



+180mil

Alumnos participantes  
de Cursos Gratuitos



+25 Países

Con Alumnos de  
Hacker Mentor

**KIO.**

Un sistema Red Hat con Vulnerabilidades.

**ETERNAL.**

La vulnerabilidad más peligrosa de Windows.

**MONKEY.**

Un portal de Alumnos con muchos fallos.

**NAVIBOLT.**

Dos retos en uno, explotando vulnerabilidades en Linux.

**STEEL MOUNTAIN.**

Servicios web desactualizados y más vulnerabilidades de Windows.

**GAME ZONE.**

Inyección SQL para tomar control de la base de datos.

**ALFRED.**

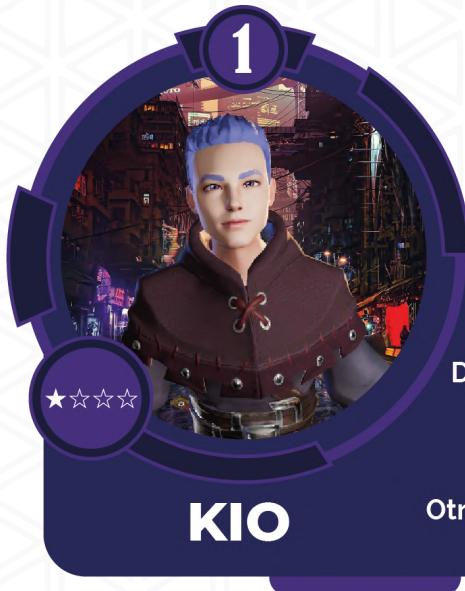
Un proyecto de software libre muy inseguro.

**ROBOT.**

Ataque a Wordpress.

**1 2 3 4 5 6 7 8**





**O.S.:** Linux  
**Dificultad:** Fácil ★  
**Puntos:** 100  
**Fases:** Enumeración - Escaneo  
**Otras Fases:** Reconocimiento - Explotación



## Caso

**Kio** ha detectado una intrusión en sus sistemas. Los administradores de seguridad de la organización no han podido encontrar el agujero de seguridad, pero creen que toda la intrusión pudo ocurrir desde un equipo Red Hat con algunos servicios desactualizados. Por esta razón te han contratado para que hagas un análisis y explotación de vulnerabilidades en sus sistemas para que puedan corregir los fallos. Es posible que exista más de una manera de explotación. **¿Estás listo?**



## ¿Qué vamos a hacer?

- Escaneo de hosts con netdiscover, arp-scan y nmap
- Escaneo de puertos abiertos, versiones de servicios y posibles vulnerabilidades con nmap
- Enumeración de servicios web con curl y posibles vulnerabilidades web con nikto
- Enumeración de tecnologías web con wappalyzer, whatweb y burpsuite
- Fuzzing de directorios con dirb, dirbuster, ffuf
- Enumeración de Samba con smbclient, smbmap y enum4linux
- Escaneo de vulnerabilidades con Nessus Essentials

- Distinción entre Reverse Shell vs Bind shell
- Diferenciación entre payloads por etapas y sin etapas
- Explotación manual y explotación automatizada con Metasploit
- Ataques de fuerza bruta a servicios activos con hydra y medusa
- Cracking de contraseñas con john the ripper
- Documentación de hallazgos con Cherry y Greenshot

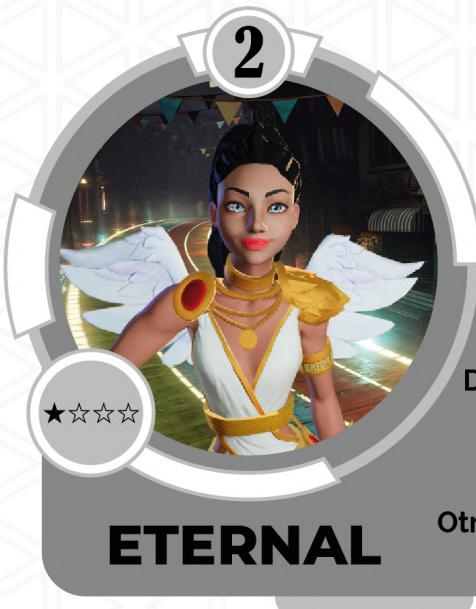


## Retos

Encontrar 3 banderas ocultas en diferentes ubicaciones del sistema.

- bandera1.txt – 33 puntos
- bandera2.txt – 33 puntos
- bandera3.txt – 34 puntos

Las banderas están en una función hash MD5, no es necesario descifrar el hash.



**ETERNAL**

O.S.: Windows

Dificultad: Fácil ★

Puntos: 100

Fases: Enumeración - Borrado de rastros

Otras Fases: Enumeración - Reconocimiento  
Persistencia



## Caso

**Eternal** es una consultora de seguridad que trabaja para empresas públicas y privadas alrededor del mundo. Recientemente en una de sus evaluaciones de seguridad a una organización detectó que existían varios equipos Windows 7 conectados a la red. Así que decidió explotar una de las vulnerabilidades más críticas y conocidas en la última década. **¿Te atreverías a investigar qué sucedió?**



## ¿Qué vamos a hacer?

- Escaneo de puertos abiertos, versiones de servicios y posibles vulnerabilidades en Samba
- Enumeración de información con rpcclient y enum4linux
- Conexión a recursos compartidos de manera anónima
- Preparación de shellcodes para equipos Windows de 32 y 64 bits
- Ejecución de exploits con metasploit y métodos manuales
- Denegación de servicio en equipos Windows
- Migración de procesos y ejecución de keylogger
- Dumpeo de credenciales y suplantación de tokens con kiwi e incognito



- Creación de usuarios administradores locales para persistencia
- Protocolos de Escritorio remoto y modificación de puertos abiertos
- Cracking de contraseñas NTLM
- Borrado de rastros



## Retos

Encontrar 2 banderas ocultas en diferentes ubicaciones del sistema.

- bandera1.txt – 50 puntos
- bandera2.txt – 50 puntos

Las banderas están en una función hash MD5, no es necesario descifrar el hash.



## Caso

**Monkey** es un programador de aplicaciones web y se le ha solicitado que desarrolle un portal de alumnos. Sin embargo, antes de que la aplicación web salga a producción se detectaron algunas fallas de seguridad que podrían ser críticas. **¿Podrías detectarlas?**



## ¿Qué vamos a hacer?

- Escaneo de puertos abiertos, versiones de servicios y posibles vulnerabilidades en ftp y http
- Enumeración de servicios ftp, ssh y http
- Fuzzing de directorios y archivos
- Credential Stuffing y password spraying
- Crackeo de hashes
- Subida de archivos al servidor web
- Shell reversas en lenguaje php
- Determinación de métodos de escalada de privilegios con linpeas y linuxprivchecker
- Cronjobs

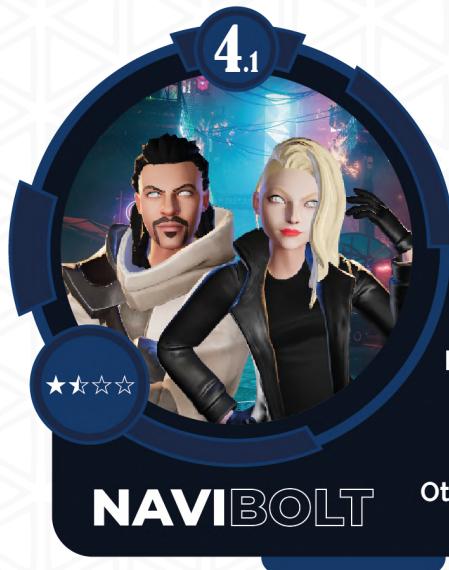


## Retos

Encontrar 2 banderas ocultas en diferentes ubicaciones del sistema.

- bandera1.txt – 50 puntos
- bandera2.txt – 50 puntos

Las banderas están en una función hash MD5, no es necesario descifrar el hash.



O.S.: Linux  
**Dificultad:** Fácil - Medio ★★  
**Puntos:** 100  
**Fases:** Explotación  
**Otras Fases:** Enumeración - Escaneo



## Caso

La empresa **Navigator** necesita de tu ayuda! Tienen montado un servidor web con múltiples dominios y determinaron que están siendo atacados. El código fuente a veces da más información de la que debería. ¿Estás listo?



## ¿Qué vamos a hacer?

- Escaneo de puertos abiertos, versiones de servicios y posibles vulnerabilidades en dns y http
- Agregar dominios en archivos de configuración
- Mala configuración en código fuente público
- Fuzzing de directorios y archivos
- Explotación de gestores de contenido
- Escalada de privilegios con ayuda de linpeas
- Escalada de privilegios con binarios SUID



## Retos

Encontrar 2 banderas ocultas en diferentes ubicaciones del sistema.

- bandera1.txt – 50 puntos
- bandera2.txt – 50 puntos

Las banderas están en una función hash MD5, no es necesario descifrar el hash.



**4.2**



★★★☆☆

**NAVI BOLT**

**O.S.:** Linux  
**Dificultad:** Fácil - Medio ★★  
**Puntos:** 100  
**Fases:** Enumeración - Persistencia  
**Otras Fases:** Escaneo - Explotación



## Caso

Un grupo ciberdelincuente denominado **Bolt** está atacando varios sistemas informáticos a nivel mundial. Se han encontrado con un gestor de contenido (CMS) con varias vulnerabilidades y que les permitió controlar algunos equipos y posteriormente tomar control de los servidores de la organización. **Detecta las vulnerabilidades y corrígelas rápidamente.**



## ¿Qué vamos a hacer?

- Escaneo de puertos abiertos, versiones de servicios y posibles vulnerabilidades en nfs y http
- Mala configuración de archivos visibles en servidor web
- Fuzzing de directorios y archivos
- Fuerza bruta a archivos comprimidos zip
- Conexiones remotas utilizando clave pública/privada
- Explotación de servicios web desactualizados
- Escalada de privilegios utilizando binarios obsoletos



## Retos

Encontrar 3 banderas ocultas en diferentes ubicaciones del sistema.

- bandera1.txt – 33 puntos
- bandera2.txt – 33 puntos
- bandera3.txt – 34 puntos

Las banderas están en una función hash MD5, no es necesario descifrar el hash.



A circular mission card featuring a female character with blonde hair and a black hoodie, standing on a rooftop overlooking a city skyline. The number '5' is at the top, and a five-star rating icon is at the bottom left. The card contains the following information:

**O.S.:** Windows  
**Dificultad:** Medio - Difícil ★★★  
**Puntos:** 100  
**Fases:** Explotación  
Escalación de privilegios  
**STEEL MOUNTAIN** **Otras Fases:** Enumeración - Escaneo



## Caso

**Steel Mountain**, una empresa de seguridad de datos, ha descubierto una vulnerabilidad crítica en uno de sus servidores de archivos HTTP que permite la ejecución de código remoto.

Tu misión es **identificar y corregir esta vulnerabilidad** lo antes posible.



## ¿Qué vamos a hacer?

- Escaneo de puertos abiertos, versiones de servicios y posibles vulnerabilidades en servicios http
- Fuzzing de directorios y archivos
- Explotación de un servidor de archivos HTTP
  - Mediante metasploit
  - Con método manual
- Crackeo de hash
- Enumeración de posibles métodos de escalación de privilegios
- Explotación de vulnerabilidad Unquoted Service Path



## Retos

Encontrar 2 banderas ocultas en diferentes ubicaciones del sistema.

- user.txt – 50 puntos
- root.txt – 50 puntos

Las banderas están en una función hash MD5, no es necesario descifrar el hash.



O.S.: Linux  
**Dificultad:** Medio - Difícil ★★★  
**Puntos:** 100  
**Fases:** Explotación  
Escalación de privilegios  
**Otras Fases:** Enumeración - Escaneo

## GAME ZONE



## Caso

"Game Zone" es un sitio web de reseñas de videojuegos que presenta varias vulnerabilidades de inyección SQL (SQLi) . Tu misión es aprovechar esta vulnerabilidad para obtener acceso a la base de datos del sitio y extraer información confidencial



## ¿Qué vamos a hacer?

- Escaneo de puertos abiertos, versiones de servicios y posibles vulnerabilidades en servicios http y ssh
- Fuzzing de directorios y archivos
- Enumeración del sitio web
- Explotación de varias vulnerabilidades SQLi
  - Mediante sqlmap
  - Con método manual
- Crackeo de hashes (crackstation, john the ripper)
- Enumeración de posibles métodos de escalación de privilegios
  - Configuración de archivos (/var/www/html)
  - Puertos locales abiertos
  - SSH tunneling
- Explotación de vulnerabilidad crítica en Webmin



## Retos

Encontrar 2 banderas ocultas en diferentes ubicaciones del sistema.

- user.txt – 50 puntos
- root.txt – 50 puntos

Las banderas están en una función hash MD5, no es necesario descifrar el hash.



O.S.: Windows

Dificultad: Medio - Difícil ★★★

Puntos: 100

Fases: Explotación

Otras Fases: Enumeración - Reconocimiento



## Caso

Alfred está desarrollando un proyecto de software libre pero no se ha preocupado demasiado por la seguridad. Se han logrado infiltrar en sus sistemas para obtener y suplantar las credenciales del administrador. Le han dejado una nota:

**"Limpiamos, optimizamos y aceleramos tu PC – Att: H4xor"**



## ¿Qué vamos a hacer?

- Lo descubrirás en el camino

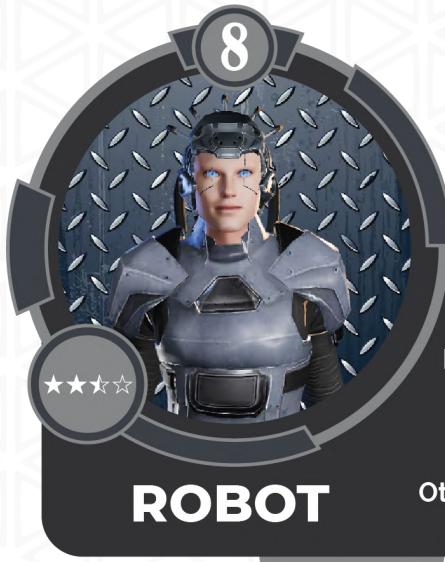


## Retos

Encontrar 2 banderas ocultas en diferentes ubicaciones del sistema.

- user.txt – 50 puntos
- root.txt – 50 puntos

Las banderas están en una función hash MD5, no es necesario descifrar el hash.



**ROBOT**

O.S.: Linux  
Dificultad: Medio - Difícil ★★★  
Puntos: 100  
Fases: Enumeración - Explotación  
Otras Fases: Escaneo



## Caso

¿Un gestor de contenidos Wordpress y uso de credenciales débiles? Una muy mala combinación.



## ¿Qué vamos a hacer?

- Lo descubrirás en el camino



## Retos

Encontrar 2 banderas ocultas en diferentes ubicaciones del sistema.

- bandera1.txt – 50 puntos
- bandera2.txt – 50 puntos

Las banderas están en una función hash MD5, no es necesario descifrar el hash.