HACKER MENTOR

Pentester Mentor Junior Certified

Conviértete en un **Hacker Ético** en solo 3 meses, aprenderás con nuestra **METODOLOGÍA GAMIFICADA** y **desde Cero.**

+180mil
Alumnos participantes de Cursos Gratuitos

+25 Países
Con Alumnos de Hacker Mentor

www.hacker-mentor.com

PMJ

1

NEBULA
Servidor Java antiguo expuesto con servicios desactualizados y múltiples vectores de intrusión.

2

BLUE
Equipo Windows 7 comprometido por una falla SMB con ejecución remota y propagación lateral.

3

UNIVERSITY
Servidor Linux con un formulario de subida nseguro y un binario }|SUID vulnerable.

4

DARK CORP
WordPress vulnerable y rutas mal configuradas que ocultan información sensible.

5

GAME ZONE
Sitio web de reseñas con inyecciones SQL ue permiten acceder a la base de datos.

6

STEEL MOUNTAIN
Servidor HTTP desactualizado con una vulnerabilidad crítica de ejecución remota.

7

PIVOT
Recurso de archivos compartidos accesible anónimamente que facilita movimiento lateral.

8

ALFRED
Proyecto de software libre comprometido: credenciales admin filtradas y suplantación.

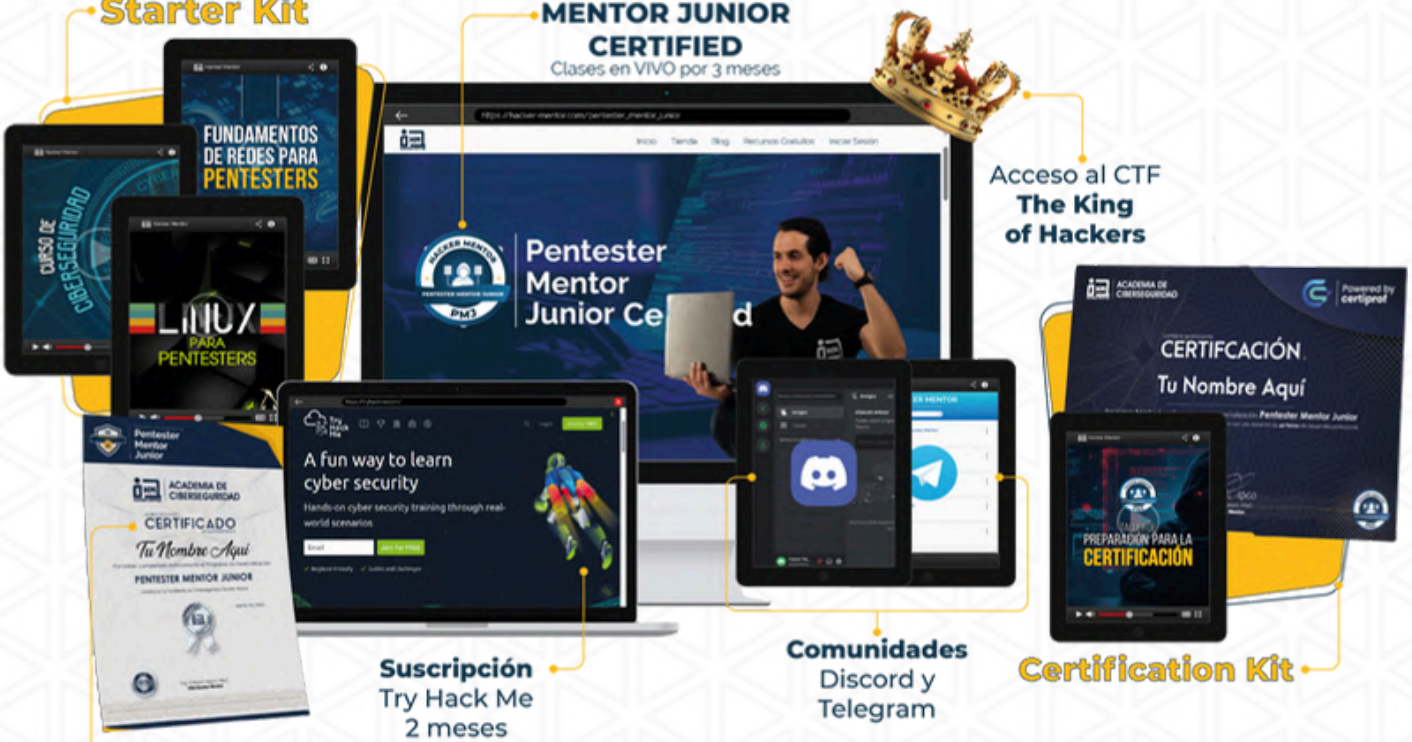
ACADEMIA DE CIBERSEGURIDAD

El Programa **se Compone de:**

Starter Kit

PENTESTER MENTOR JUNIOR CERTIFIED
Clases en VIVO por 3 meses

Acceso al CTF **The King of Hackers**



Suscripción
Try Hack Me
2 meses

Comunidades
Discord y
Telegram

Certification Kit

Certificación
Hacker Mentor PMJ

+4 BONOS

Curso Auditoría y Pentesting de Aplicaciones Móviles

Curso Hacking WiFi

Taller Principales Certificaciones de Hacking Ético

Taller Cómo Conseguir Trabajo en Ciberseguridad

En CUALQUIER parte del MUNDO,
en CUALQUIER DISPOSITIVO

Metodología Gamificada

Nuestra metodología te permite competir por un lugar en el Ranking Final de nuestro programa y ganar premios por parte de nuestra Academia

RANKING FINAL

DEL PROGRAMA

Pentester Mentor Junior

FINAL | GRUPO X

1		EDUARDO R.	929,5
2		ERIK R.	923
3		JAVIER V.	879
4		WILLY C.	857,5
5		ABDUL A.	796

Reto 01 - Nebula

Caso

La empresa Nebula Labs detectó actividad anómala en uno de sus servidores de desarrollo expuesto a Internet. El equipo cree que el incidente provino de una aplicación Java antigua desplegada junto a servicios auxiliares desactualizados. Se te contrata para replicar la intrusión en laboratorio, enumerar los vectores y proponer mitigaciones. Se sospecha que existen múltiples caminos para obtener acceso y escalar privilegios. ¿Listo?

Plan de acción

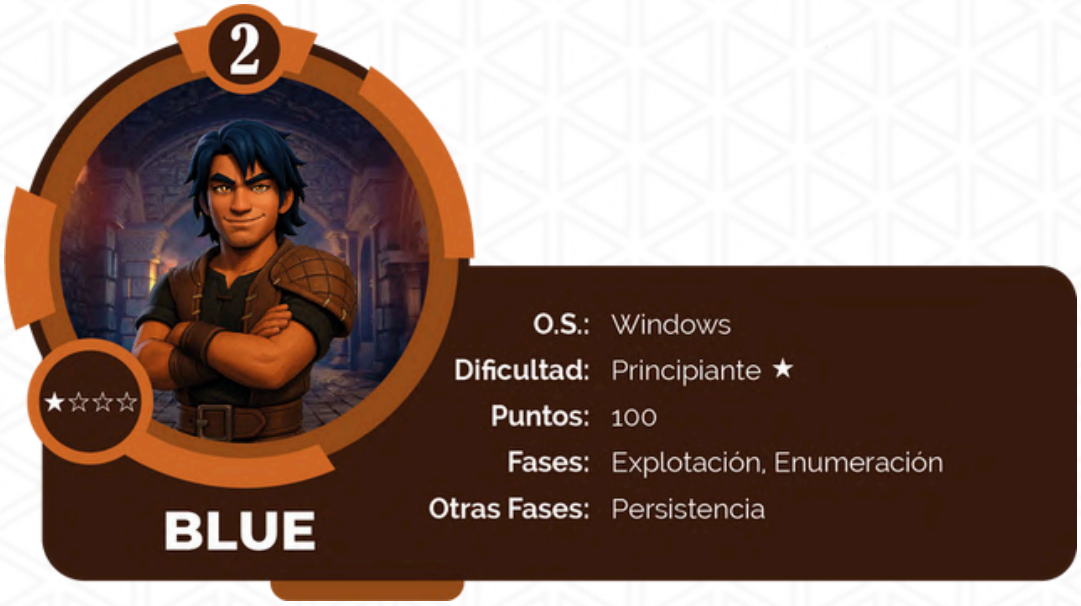
- Descubrimiento de host netdiscover / arp-scan / nmap
- Escaneo de puertos/servicios nmap (-sC -sV -p-)
- Enumeración web curl / whatweb / nikto / burpsuite
- Fuzzing dirb / ffuf → /development/
- Enumeración Samba smbclient / smbmap / enum4linux
- Escaneo de vulnerabilidades
- Nessus Essentials → CVEs en Struts/Tomcat + config insegura Samba.
- Escalada de privilegios - binarios SUID , claves SSH expuestas
- Ataques de fuerza bruta a servicios activos con hydra y medusa
- Documentación de hallazgos con Cherry y Greenshot

Retos

Encontrar :

- 1 directorio oculto
- Usuario del sistema y su contraseña
- Bandera final de root

Reto 02 - Blue



Caso

En una evaluación de seguridad interna se detectó que varios equipos con Windows 7 seguían conectados a la red. Uno de esos equipos, llamado Blue, mostró comportamiento anómalo: tráfico SMB saliente hacia IPs internas y creación de procesos inusuales. La hipótesis inicial es que se aprovechó una vulnerabilidad crítica de SMB/Windows con capacidad de ejecución remota y propagación lateral. Se abre investigación para identificar vector inicial, alcance y remediaciones.

¿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.

- Hashes de Windows
- Bandera 1
- Bandera 2
- Bandera 3

ACADEMIA DE CIBERSEGURIDAD

Reto 03 - University

Caso

University ha dejado expuesto a internet un servidor Linux con varios servicios abiertos. Durante una auditoría interna, los analistas descubrieron un sitio web corriendo en un puerto no estándar que incluye una página de carga de archivos. Al parecer, este formulario está mal implementado y podría permitir la ejecución de código remoto. Además, en la máquina se detectó un binario SUID sospechoso que podría usarse para escalar privilegios.
Tu misión: enumerar, obtener acceso inicial y llegar a root documentando cada paso.

¿Qué vamos a hacer?

- Escaneo de puertos abiertos, versiones de servicios y posibles vulnerabilidades
- Enumeración de servicio http
- Fuzzing de directorios y archivos
- Subida de archivos al servidor web
- Burpsuite para fuzzing de extensiones
- Shell reversas en lenguaje php
- Determinación de métodos de escalada de privilegios con linpeas y linuxprivchecker
- Binarios SUID
- Mitagaciones

Retos

Bandera 1
Bandera 2

ACADEMIA DE CIBERSEGURIDAD

Reto 04 - DarkCorp

Caso

La empresa DarkCorp ha sufrido una intrusión sospechosa. Como pentester, tu misión es realizar un ataque controlado a uno de sus servidores expuestos para detectar fallos críticos. Se rumorea que usan un WordPress vulnerable y que ocultan información sensible en rutas mal configuradas. Tu objetivo será obtener acceso inicial, escalar privilegios y capturar tres banderas que simulan información confidencial de la compañía.

¿Qué vamos a hacer?

- Reconocimiento (Nmap + enumeración web).
- Fuzzing → WordPress login.
- Fuerza bruta con diccionario filtrado.
- Shell vía 404.php.
- Escalación con binario SUID (nmap).
- Persistencia con llaves id rsa

Retos

Bandera 1
Bandera 2
Bandera 3

ACADEMIA DE CIBERSEGURIDAD

Reto 05 - 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.

ACADEMIA DE CIBERSEGURIDAD

Reto 06 - Steel Mountain

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.

Reto 07 - Pivot

Caso

Eres el equipo rojo interno contratado por la organización “AceroNova” para auditar un servidor en el perímetro. Un inventario rápido muestra un recurso de archivos compartidos accesible anónimamente. La gerencia teme que la fuga de documentos y la configuración de red permitan a un atacante moverse lateralmente hacia sistemas internos críticos.

¿Qué vamos a hacer?

- Enumerar la máquina Pivot y confirmar acceso anónimo al share SMB.
- Localizar y extraer información sensible en el share que permita avanzar (credenciales, rutas, urls).
- Realizar un ataque de credenciales (laboratorio: diccionario) contra el objetivo indicado y recuperar un documento confidencial.
- Encontrar un sitio WordPress expuesto con un plugin vulnerable a LFI y explicar el riesgo.
- Recuperar una llave SSH desde el servidor web y usarla para autenticarse (laboratorio).
- Escalar privilegios en la máquina objetivo por cronjob o binario SUID.
- Detectar la segunda interfaz de red en Cobalt, pivotar (en lab aislado) y enumerar la red interna para encontrar otro equipo vulnerable.
- Documentar IOCs, detecciones y remediaciones.

Retos

Bandera 1
Bandera 2
Pivoting

Reto 08- Alfred

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: H4x0r"

¿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.