

270 - SEGURIDAD

Practica hacking ético con retos CTF en tu laboratorio

Aprende cómo atacan los delincuentes para saber defenderte, usando máquinas vulnerables a propósito y sin salir de tu laboratorio.



NIVEL
Avanzado

TIEMPO
1 h

CATEGORÍA
Seguridad

WEB
soporteinformatico360.com

Los retos CTF son ejercicios legales en los que buscas una bandera oculta en un sistema preparado para ello. Es la mejor forma de aprender ciberseguridad sin poner en riesgo a nadie.

■ Qué necesitas

- ✓ Un PC con 16 GB de RAM o más
- ✓ Una máquina vulnerable a propósito
- ✓ VirtualBox o un programa similar
- ✓ Una cuenta gratuita en una plataforma de retos

■ Paso a paso

01

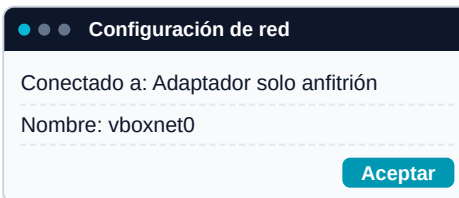
Empieza por retos en línea

Plataformas como picoCTF, TryHackMe o Hack The Box ofrecen retos guiados y legales. Empieza por los de nivel principiante.

02

Monta un laboratorio aislado

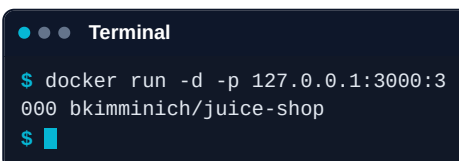
En VirtualBox crea una red Solo anfitrión y conecta ahí tus máquinas. Así no tocan tu red de casa ni Internet.



03

Añade una máquina de prácticas

Usa máquinas creadas para fallar, como Metasploitable 2 o OWASP Juice Shop. Juice Shop se arranca con Docker en tu equipo.



04

Haz una instantánea

Antes de empezar, guarda una instantánea de cada máquina virtual. Si algo se rompe, vuelves atrás en segundos.



05

Reconoce tu objetivo

Escanea solo la IP de tu máquina de laboratorio para ver sus servicios. Apunta versiones y puertos abiertos.

```
Terminal
$ nmap -sV 192.168.56.101
$
```

06

Piensa como defensor

Por cada fallo que encuentres, anota cómo se corregiría: actualizar, cerrar un puerto o cambiar una contraseña. Eso es lo que aplicarás en tus equipos.

■ Consejos

CONSEJO 1

Lleva un cuaderno con cada reto: qué probaste y qué aprendiste.

CONSEJO 2

Nunca conectes una máquina vulnerable a tu red real ni a Internet.

CONSEJO 3

Si quieres formar a tu equipo de empresa, un técnico puede montar el laboratorio.



Importante: Practica solo en tu laboratorio, en tus equipos o en plataformas que lo autorizan. Atacar sistemas ajenos sin permiso es delito, aunque sea por curiosidad. Las máquinas vulnerables a propósito deben estar siempre aisladas.

¿Prefieres que lo hagamos por ti?

Diagnóstico sin compromiso y presupuesto cerrado antes de empezar. soporte@soporteinformatico360.com
En taller, a domicilio en Madrid o por asistencia remota. soporteinformatico360.com

910 117 112