Pentesting: ¿cómo y por qué?

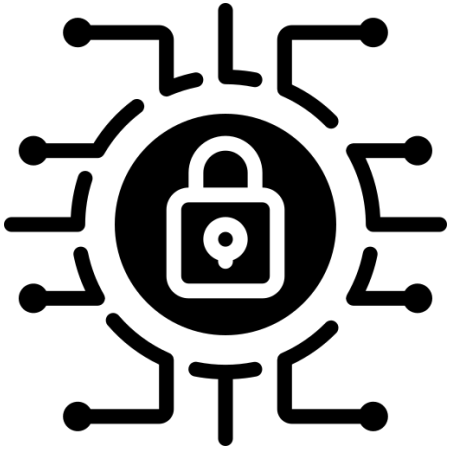
Cristina Mariscal

#Devday4w

¿Que es Pentest?

“Es un tipo de método de pruebas de seguridad para determinar si las vulnerabilidades dentro o entre componentes del sistema evaluado pueden explotarse para comprometer la aplicación, sus datos o los recursos de su entorno.” (NIST SP 800-95).

¿Para qué ejecutar Pentest?

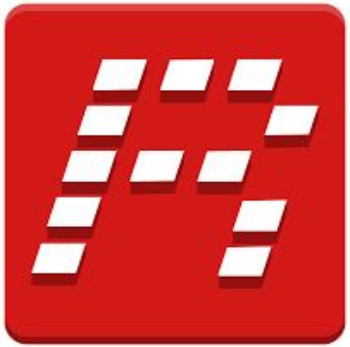


- Gestión de riesgos
- Respuesta ante incidentes
- Mejora continua y aseguramiento
- Auditorías, certificaciones y cumplimiento

¿Por qué es importante?

- Seguridad como parte de estrategia de negocio
- Sistema de gestión de la seguridad informática (ISMS)

Reconocimiento



Escaneo de vulnerabilidades

OpenVAS

Open Vulnerability Assessment Scanner

OWASP

Zed Attack Proxy

NMAP

OpenSCAP

WIRESHARK

Explotación

Metasploit

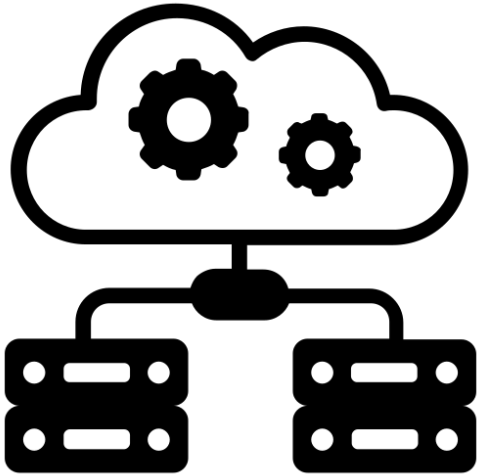
HOIC
High Orbit Ion Cannon

LOIC
Low Orbit Ion Cannon

sqlmap®

Armitage

Post-explotación



- Escalada de privilegios
- Escalar a otros sistemas
- Identificación del alcance
- Obtener información
- Persistencia: evaluar sistemas de control.

Informe

- Definición del alcance
- Detalles sobre la ejecución
- Documentación de hallazgos y vulnerabilidades
- Definición del impacto
- Evaluación de riesgos
- Proveer recomendaciones

¡Gracias!