



# **Análisis de Seguridad y Pruebas de Penetración**

## Introducción

- La seguridad informática es un pilar esencial en la era digital.
- Se requieren enfoques proactivos:
  - ✓ Análisis de seguridad
  - ✓ Pruebas de penetración (Pentesting)
- Objetivo: detectar vulnerabilidades antes que los atacantes.



## ¿Qué es el Análisis de Seguridad?

 Evaluación sistemática de una infraestructura tecnológica

 Objetivos:

- Identificar vulnerabilidades
- Medir nivel actual de seguridad
- Cumplir normas como ISO/IEC 27001 y NIST
- Emitir recomendaciones técnicas



## ¿Qué son las Pruebas de Penetración?

 Simulación autorizada de ataques reales

 Objetivos:

- Detectar vulnerabilidades explotables
- Evaluar detección y respuesta organizacional
- Validar controles de seguridad existentes



## Fases del Pentesting (Modelo OWASP/PTES)

- 1. Reconocimiento (OSINT)
- 1. Escaneo (Scan activo)
- 1. Explotación (Ataques controlados)
- 1. Mantenimiento del acceso (Persistencia)
- 1. Informe y remediación





## Fase 1 – Reconocimiento

 **Recopilación pasiva de información pública**

 **Herramientas:**

- Google Hacking
- Shodan
- WHOIS
- LinkedIn

 **Objetivo:** descubrir vectores de ataque sin alertar al objetivo



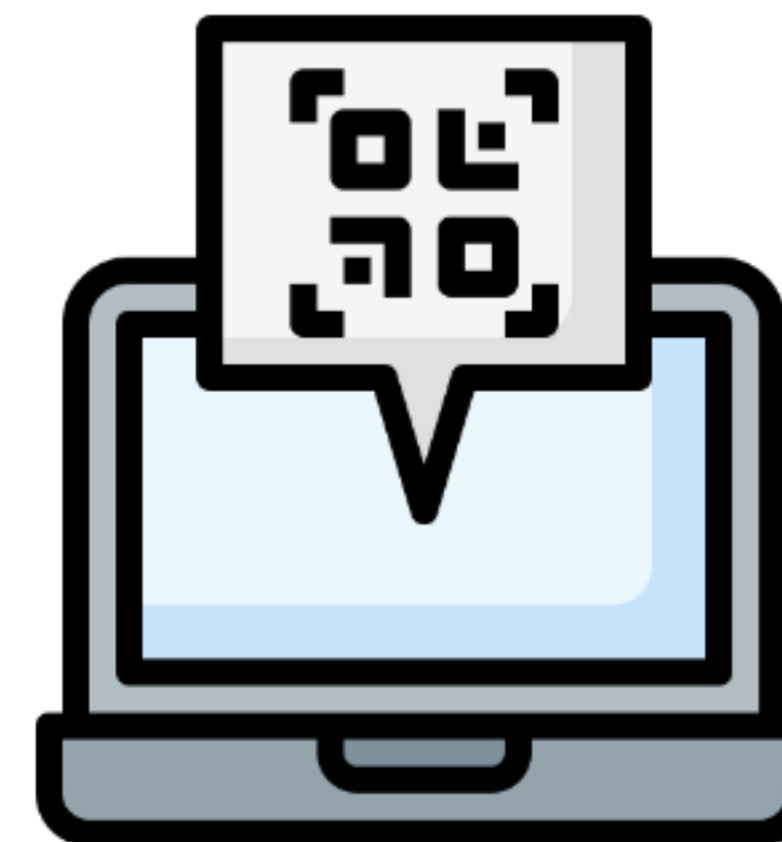
## Fase 2 – Escaneo

 Evaluación activa de puertos y servicios

 Herramientas:

- Nmap
- Nessus
- OpenVAS
- Burp Suite

 Resultado: mapa técnico de vulnerabilidades potenciales



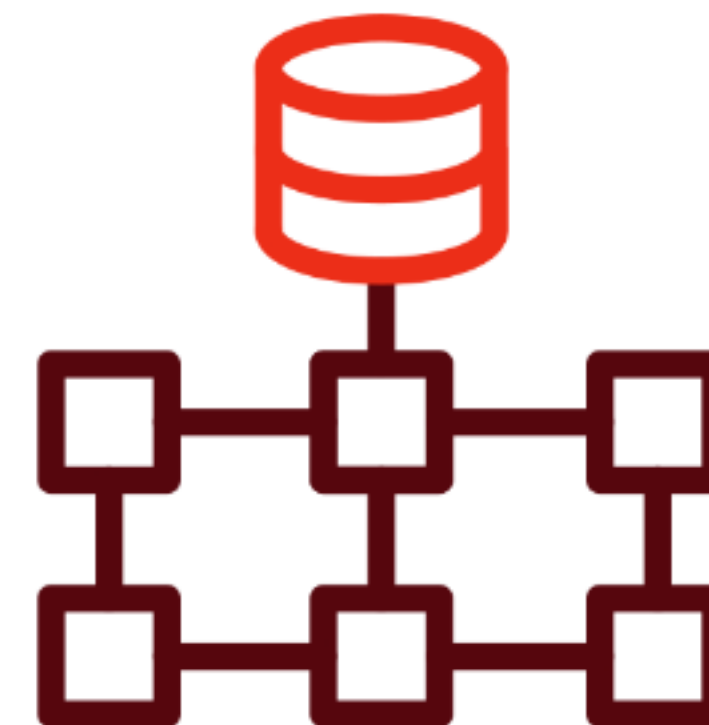
## Fase 3 – Explotación

💣 **Uso real de exploits para demostrar el impacto**

🧰 **Herramientas:**

- Metasploit
- Sqlmap
- Hydra

🚧 **Importancia: confirmar amenazas reales, no teóricas**





## Fase 4 – Mantenimiento del Acceso

 Simula cómo un atacante mantendría presencia

 Técnicas:

- Backdoors
- Shells persistentes
- Rootkits

 Objetivo: evaluar respuesta y monitoreo interno



## Fase 5 – Informe y Remediación

### Creación de un informe profesional

#### Debe incluir:

- Vulnerabilidades halladas
- Reproducción del ataque
- Severidad (CVSS)
- Recomendaciones técnicas



## Consideraciones Éticas y Legales

 **Requiere autorización escrita**  
 **Principios clave:**

- Confidencialidad
- Integridad de la información recolectada
- Cumplimiento normativo (GDPR, CFAA, etc.)



## Entornos Controlados


 Pruebas deben realizarse en laboratorios o entornos duplicados

 Beneficios:

- Evita afectación productiva
- Reproduce ataques sin riesgo real
- Mejora precisión en resultados



## Conclusión

-  **El análisis de seguridad y pentesting son claves para:**
- Fortalecer defensas
  - Prevenir incidentes
  - Cumplir normativas
  - Construir una postura de ciberseguridad sólida y sostenible





