



Ciberseguridad

Pentest y sus etapas



Concientización





Ciberseguridad



¿Qué es?

Un **Pentest** (Prueba de Penetración) es una simulación controlada de un ataque cibernético diseñada para identificar y corregir vulnerabilidades en sistemas, aplicaciones o redes. En otras palabras, es como un "*hackeo ético*" donde expertos en seguridad intentan encontrar puntos débiles antes de que lo hagan los atacantes reales.

Es como probar las cerraduras de una casa para asegurarte de que un ladrón no pueda entrar.

Concientización





Ciberseguridad



Consta de 5 etapas



Concientización





Ciberseguridad



1. Reconocimiento

El objetivo es recopilar toda la información posible sobre el sistema objetivo, sin interactuar directamente con él (reconocimiento pasivo) o interactuando directamente (reconocimiento activo).

- Buscar información pública: nombres de dominio, direcciones IP, servidores web, correos electrónicos.
- Examinar redes sociales y foros para encontrar datos sensibles
- Escanear redes para identificar dispositivos conectados.



Concientización





Ciberseguridad



2. Escaneo

En esta etapa, el pentester interactúa más con el sistema objetivo para identificar posibles puntos débiles. Se buscan servicios, puertos abiertos y versiones de software.

- Escanear puertos para identificar servicios expuestos (HTTP, SSH, etc.).
- Detectar versiones de software para buscar vulnerabilidades conocidas.
- Mapear la estructura de red de la organización.



Concientización





Ciberseguridad



3. Explotación

Aquí el pentester intenta explotar las vulnerabilidades encontradas en las etapas anteriores para acceder al sistema.

- Realizar ataques de fuerza bruta para descifrar contraseñas débiles.
- Usar exploits conocidos para aprovechar errores en el software.
- Subir shells maliciosas para obtener acceso remoto.



Concientización





Ciberseguridad



4. Post-Explotación

Si se logró acceder al sistema, esta etapa se enfoca en analizar cómo los atacantes podrían mantenerse dentro sin ser detectados y hasta dónde pueden llegar con ese acceso.

- Escalar privilegios para obtener acceso como administrador.
- Configurar puertas traseras para reingresar al sistema en el futuro. (*persistencia*)
- Exfiltrar datos sensibles sin alertar al sistema de seguridad.



Concientización





Ciberseguridad



5. Reporte

En esta etapa, se documentan todos los hallazgos, explicando las vulnerabilidades identificadas, su impacto y recomendaciones para solucionarlas.

- Crear una lista priorizada de vulnerabilidades con su nivel de criticidad.
- Proponer soluciones técnicas como actualizaciones, cambios de configuración o monitoreo adicional.
- Presentar un resumen ejecutivo para que los responsables de decisiones no técnicos entiendan los riesgos.



Concientización





Ciberseguridad

Seguininos y
unite al
discord para
seguir
aprendiendo

 Guardar

 Compartir

 Seguir

Concientización

