Evaluación de Seguridad

Test de Penetración (Pentesting) — Metodología del servicio

¿Qué es un test de penetración?

Un test de penetración es una evaluación de seguridad en la que simulamos, de forma controlada y autorizada, las mismas técnicas que utilizaría un atacante real, con un objetivo opuesto: encontrar las debilidades antes que ellos y ayudarte a corregirlas. El proceso se realiza por etapas, de lo más general a lo más específico. A continuación explicamos qué se hace en cada una y por qué es importante para tu organización.

1 Alcance y autorización

Qué hacemos: Definimos junto a vos exactamente qué sistemas se van a evaluar (sitios web, dominios, servidores), en qué fechas y con qué límites, y se firma una autorización formal.

Por qué importa: Garantiza que todo el trabajo se realice de forma legal, ordenada y sin afectar la operación de tu negocio.

2 Reconocimiento (recopilación de información)

Qué hacemos: Reunimos toda la información pública disponible sobre tus sistemas: dominios y subdominios, registros técnicos, tecnologías utilizadas y datos que pudieran estar expuestos en internet sin que lo sepas.

Por qué importa: Un atacante real siempre empieza por aquí. Ver lo mismo que vería él nos permite anticiparnos a sus movimientos.

3 Mapeo de la superficie de ataque

Qué hacemos: Identificamos todos los posibles puntos de entrada: páginas, formularios, secciones de acceso, direcciones y archivos que estén accesibles públicamente.

Por qué importa: Cada punto de entrada es una puerta potencial. Mapearlas todas asegura que ninguna quede sin revisar.

4 Análisis de la aplicación web

Qué hacemos: Revisamos en detalle cómo está construido tu sitio: su configuración de seguridad, la protección de la conexión (certificados), el manejo de la información y si hay datos sensibles expuestos en el código.

Por qué importa: Muchos problemas no se ven a simple vista: están en cómo está configurado el sistema por dentro.

5 Detección de vulnerabilidades

Qué hacemos: Analizamos los sistemas contra una base de miles de fallas de seguridad conocidas, para detectar debilidades que podrían llegar a aprovecharse.

Por qué importa: Permite identificar riesgos concretos antes de que lo haga alguien con malas intenciones.

6 Pruebas de explotación controlada

Qué hacemos: Cuando detectamos una posible falla, la comprobamos de manera segura y controlada para confirmar si es real y qué alcance tendría. En ningún momento se dañan ni se alteran tus datos.

Por qué importa: Distingue un riesgo teórico de uno real y demostrable, respaldado con evidencia.

7 Verificación de hallazgos

Qué hacemos: Cada hallazgo se vuelve a comprobar para descartar falsas alarmas y medir su gravedad real dentro del contexto de tu negocio.

Por qué importa: Te entregamos únicamente información precisa y accionable, sin ruido ni exageraciones.

8 Informe y recomendaciones

Qué hacemos: Elaboramos un informe claro con cada hallazgo, su nivel de riesgo, el impacto para tu negocio y los pasos concretos para solucionarlo, incluyendo un resumen entendible sin conocimientos técnicos.

Por qué importa: Es la hoja de ruta para dejar tus sistemas más seguros de forma priorizada.

Qué recibís al finalizar

- Informe ejecutivo, con un resumen claro para la toma de decisiones.
- Informe técnico detallado de cada hallazgo, con su evidencia.
- Clasificación de cada riesgo por nivel de severidad.
- Recomendaciones de solución, priorizadas por importancia.
- Acompañamiento para resolver dudas sobre la remediación.

El objetivo final no es solo encontrar fallas, sino dejar tu plataforma medible y verificablemente más segura, protegiendo tu información y la de tus clientes.