# ¿Caja negra o caja blanca? Descubre qué es un test de intrusión o Hacking Ético

Un pentest (“Penetration Test”), o prueba/test de penetración/intrusión, es un método para evaluar los sistemas de información y la red de una organización simulando un ataque para encontrar vulnerabilidades que permitirían a potenciales atacantes robar información o afectar los activos de la misma (malware, ataques DoS, etc.). Las medidas y controles de seguridad son analizados para encontrar debilidades, fallos técnicos y vulnerabilidades.

Estas pruebas se realizan utilizando técnicas y herramientas similares y en muchos casos las mismas que utilizan los atacantes, pero sin perjudicar a la organización ni realizar actividades ilícitas. Los tests de intrusión realizados para otras partes (por ejemplo, los clientes) deben ir precedidas de un acuerdo firmado donde se defina el alcance del mismo, así como las restricciones y/o limitaciones de las pruebas.

## ¿Cómo se realiza una prueba de intrusión?

Se establecen distintas fases para la realización de estas pruebas:

Fase I: Obtener información del objetivo.

Fase II: Escaneo pre-ataque. Identificación de puertos de entrada, estructura, equipos accesibles. Obtención de detalles de sistemas operativos y estructuras de red. Batería de test de vulnerabilidades.

Fase III: Explotación manual de vulnerabilidades detectadas. Análisis de vulnerabilidades. Pruebas de obtención de acceso, passwords, toma de control. Pruebas de borrado de huellas.

Fase IV: Informe. Resumen ejecutivo. Pruebas realizadas. Vulnerabilidades detectadas. Recomendaciones para su solución.

## Tipos de pentesting

Caja negra (“Black Box”): se basan en que los pentesters no disponen de conocimiento previo acerca de la infraestructura que va a ser probada. Es el tipo de test de intrusión más parecido a un ataque real. Suele ser realizado por personal especializado externo a las organizaciones.

Caja blanca (“White Box”): se trata del test más completo ya que se parte de un conocimiento completo previo de la infraestructura a ser probada. Normalmente lo realiza personal interno de las organizaciones o se contrata a alguien externo si la empresa no dispone de trabajadores especializados.

Caja gris (“Grey Box”): se parte de un conocimiento parcial previo de la infraestructura objetivo del test. Suele ser el tipo de pentest recomendado cuando se contrata a empresas especializadas.

## Beneficios de los pentests

Ayudan a las organizaciones a probar sus capacidades de ciberseguridad.

Descubrir las debilidades en la seguridad de las TIC de la organización antes que los atacantes.

Definir planes de acción correctivos y preventivos de ciberseguridad y justificar a la alta dirección las inversiones requeridas.

Contribuir a la continuidad de negocio de las empresas.

Los pentests son básicos para la seguridad de empresas y organizaciones, prevenir ataques virtuales y saber responder en caso de incidentes.