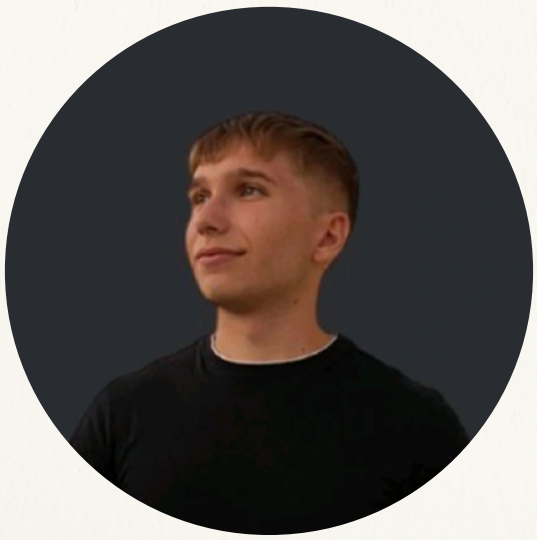
CAJAS

Negras Grises Negras en PENTESTING





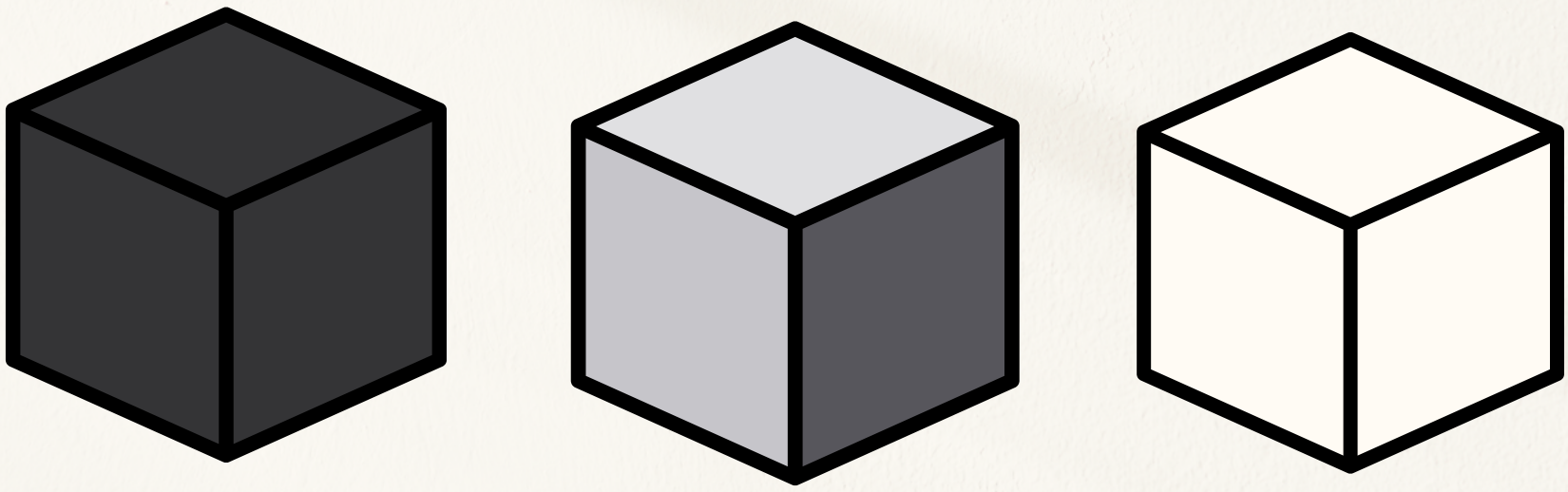
01 INTRODUCCIÓN AL PENTESTING

El pentesting es una prueba de ciberseguridad en la que se simulan ataques para **identificar vulnerabilidades** en sistemas, redes o aplicaciones. Ayuda a prevenir ataques reales al anticiparse a las amenazas. Es como probar todas las entradas de una casa para asegurarte de que están seguras.



02 LAS TRES CAJAS

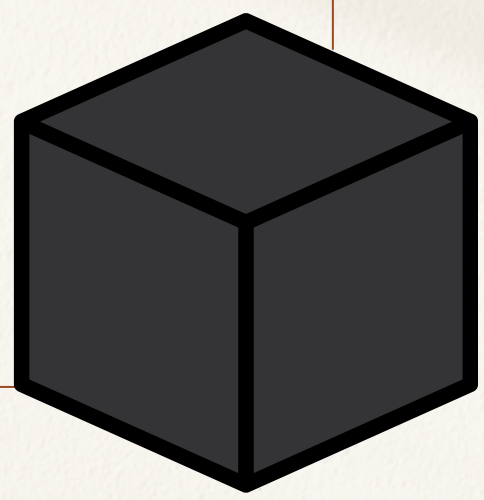
Las cajas negra, gris y blanca representan **niveles de acceso del pentester al sistema.** La caja negra simula un atacante externo sin información previa, la gris un atacante con acceso parcial, y la blanca un análisis interno con acceso total.



03 CAJA NEGRA

En la caja negra, el pentester **no tiene información previa del sistema**. Actúa como un atacante externo probando la seguridad perimetral, como contraseñas o configuraciones públicas. Es realista, pero no evalúa aspectos internos.

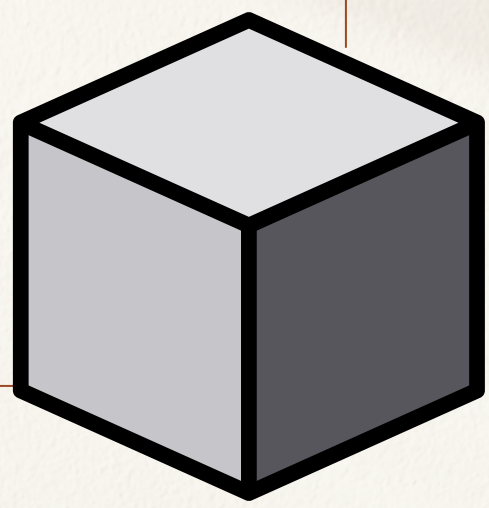
Es como intentar entrar a un edificio sin conocer el plano ni tener las llaves, buscando entradas visibles.



04 CAJA GRIS

En la caja gris, el pentester tiene **acceso limitado**, como credenciales o esquemas básicos. Evalúa tanto el exterior como partes internas, simulando un atacante con acceso parcial, como un empleado malintencionado.

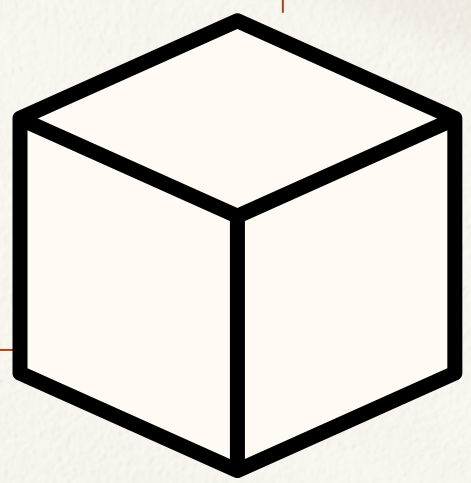
Es como entrar a un edificio con un plano incompleto y algo de información, pero sin acceso total.



05 CAJA BLANCA

La caja blanca permite un análisis completo con **acceso a toda la información interna**, como código y configuraciones. Es ideal para auditorías exhaustivas, aunque menos realista para ataques externos.

Es como tener todas las llaves, el plano y acceso al sistema de seguridad del edificio.



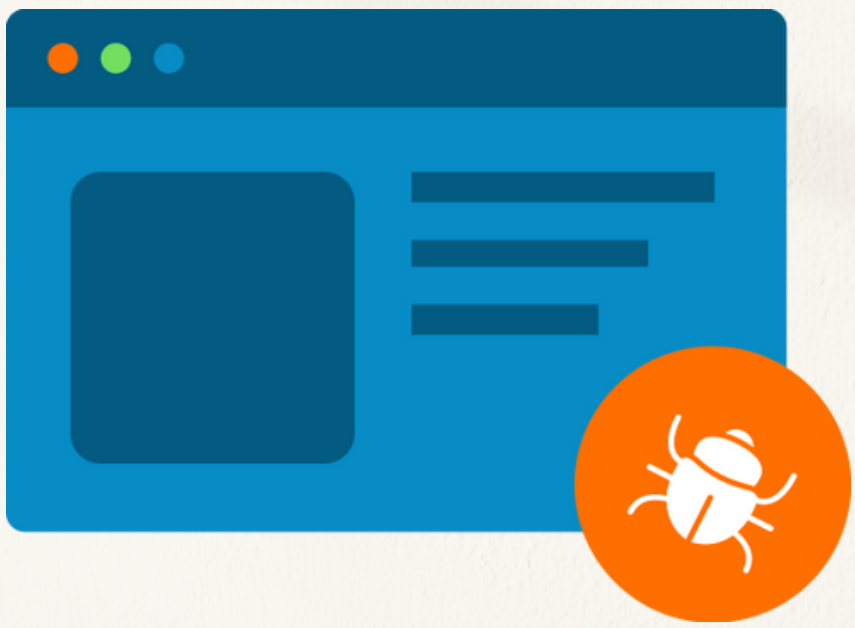
06 APLICACIONES

- **Caja Negra:** simula ataques reales.
- **Caja Gris:** combina análisis interno y externo.
- **Caja Blanca:** permite auditorías completas. Implementarlas asegura una cobertura integral contra ataques.



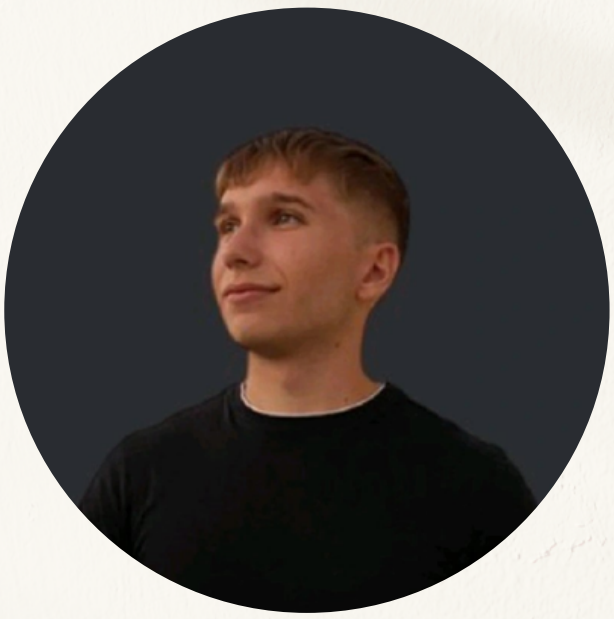
07 EJEMPLOS PRÁCTICOS

- **Caja Negra:** Escaneo con Nmap y ataque de fuerza bruta.
- **Caja Gris:** Uso de credenciales limitadas para explotar vulnerabilidades internas.
- **Caja Blanca:** Revisión de código y simulación de ataques internos.



¡GRACIAS!

CONECTEMOS Y APRENDAMOS JUNTOS



@SAULRUIZPLAZA