Blandskron

# Análisis Ético de “La prueba sorpresa”

**Caso práctico**

Un pentester junior descubre, a través de una API interna mal configurada, un archivo `usuarios.db` accesible sin autenticación. Sin documentar ni notificar previamente, descarga la base de datos y ejecuta un script Python que imprime en consola todos los registros de usuarios. Más tarde, utiliza estos datos sin anonimizar en su portafolio personal como “prueba de habilidad” .

**Principios éticos vulnerados**

El primero es el **consentimiento informado**: antes de realizar cualquier acción invasiva —descarga de datos o ejecución de scripts contra sistemas sensibles— el pentester debe contar con autorización explícita que defina alcance y límites. Al omitir este acuerdo, actuó fuera del marco legal y contractual que protege tanto al profesional como a la empresa. El segundo es la **confidencialidad**: la obligación de proteger la información obtenida durante las pruebas impide divulgarla o exponerla en entornos públicos o personales. Al mostrar datos reales en su portafolio, violó la privacidad de los usuarios y puso en riesgo la reputación de la organización.

**Validez de la justificación “demostrar mis habilidades”**

No cabe. El hacking ético persigue mejorar la seguridad de la organización contratante, no el beneficio personal del pentester. Divulgar datos confidenciales, incluso sin revelar nombres de empresa, demuestra falta de juicio profesional y debilita la confianza que toda relación de auditoría debe basarse en la integridad y el respeto a la información. La motivación de aprendizaje o exhibición de pericia jamás justifica saltarse los acuerdos de confidencialidad ni exponer datos sensibles.

**Análisis técnico del script presentado**

El código abre directamente `usuarios.db` y ejecuta `SELECT * FROM usuarios`, extrayendo todas las columnas sin filtro ni paginación. Imprime dichos registros íntegros (`print(usuario)`), lo que expone contraseñas, correos u otros datos sensibles en texto claro. Además carece de control de errores y no registra ninguna metadata (horarios, IP de acceso), impidiendo el trazado de la acción. Esta práctica compromete la integridad y la confidencialidad de la base de datos.

**Medidas éticas y profesionales adecuadas**

Al identificar el acceso no autorizado a la base de datos, el pentester debió:

- Detener cualquier descarga o consulta masiva de datos.
- Documentar la vulnerabilidad en un informe interno y notificar de inmediato al responsable de seguridad.
- Solicitar la ampliación de alcance si era necesario extraer datos para pruebas controladas.

- Acordar un procedimiento seguro para la transferencia de datos (canales cifrados, entorno aislado).

- Anonimizar o mascarar datos personales antes de cualquier demostración o análisis externo.

**Implicancias legales**

La exposición de datos personales sin consentimiento puede infringir normas de protección de datos como el **GDPR** en Europa o leyes locales de privacidad. El pentester podría enfrentarse a responsabilidad penal o civil por acceso y divulgación indebida, mientras que la empresa corre riesgo de sanciones regulatorias, multas por brechas de seguridad y reclamaciones de afectados por violación de confidencialidad.

**Recomendaciones éticas generales para pentesters junior**

Adherirse siempre a un **Statement of Work** claro, firmado antes de iniciar pruebas; emplear **NDA** para proteger la información; usar entornos de prueba aislados y canales cifrados para el manejo de datos; y respetar siempre los principios de consentimiento, confidencialidad, transparencia y profesionalidad.