📘 Glosario: Documentación de Resultados en Pentesting

---

1. Informe de Pruebas de Penetración

Documento técnico-estratégico que contiene los hallazgos, análisis de impacto y recomendaciones obtenidas durante una auditoría de seguridad o pentest.

---

2. Resumen Ejecutivo

Sección del informe orientada a tomadores de decisiones no técnicos. Resume las vulnerabilidades más críticas, su impacto y acciones prioritarias de mitigación.

---

3. Alcance de la Prueba

Delimitación acordada entre el equipo de seguridad y el cliente, que define qué sistemas serán evaluados, bajo qué condiciones y con qué limitaciones.

---

4. Metodología

Conjunto de estándares y procedimientos aplicados durante la prueba de seguridad. Ejemplos comunes: **OWASP Testing Guide**, **PTES**, **NIST SP 800-115**.

---

5. Hallazgo

Resultado individual de la evaluación que evidencia una debilidad o vulnerabilidad detectada en los sistemas o aplicaciones analizadas.

---

6. Evidencia Técnica

Prueba visual o textual que respalda un hallazgo, como capturas de pantalla, salidas de comandos, logs del sistema o trazas de red.

7. Impacto

Consecuencia potencial de la explotación de una vulnerabilidad, que puede afectar la confidencialidad, integridad o disponibilidad de la información.

---

8. Riesgo

Medida de la probabilidad de que una vulnerabilidad sea explotada y del daño que pueda causar. Se evalúa combinando severidad e impacto.

---

9. CVSS (Common Vulnerability Scoring System)

Sistema estándar para medir y clasificar la severidad de vulnerabilidades, en una escala de 0 a 10. Ayuda a priorizar la remediación.

---

10. Mitigación

Acciones técnicas o administrativas que reducen el riesgo asociado a una vulnerabilidad detectada.

---

11. Recomendación

Propuesta técnica redactada para resolver o disminuir el impacto de un hallazgo. Debe ser clara, específica y aplicable en el entorno evaluado.

---

12. Plantilla de Informe

Estructura estandarizada utilizada para documentar de forma coherente y profesional los resultados de una prueba de seguridad.

---

13. Audiencia Técnica

Conjunto de lectores del informe con conocimientos técnicos (como administradores, ingenieros o analistas de seguridad) que requieren detalles específicos del hallazgo.

---

14. Audiencia No Técnica

Grupo de interés compuesto por gerentes, directores o stakeholders que necesitan comprender el impacto sin entrar en detalles técnicos.

---

15. Herramientas de Reporte

Plataformas o aplicaciones utilizadas para generar informes estructurados de pentesting. Ejemplos: **Dradis**, **DefectDojo**, **Faraday**, **Pentest-Tools Reporting**.

---

16. Post-Mitigación

Revisión o validación realizada después de que se aplica una corrección, para asegurar que la vulnerabilidad ha sido eliminada o contenida.

---

17. Clasificación de Severidad

Proceso de asignar un nivel (bajo, medio, alto, crítico) a una vulnerabilidad, según su impacto potencial y facilidad de explotación.

---

18. Confidencialidad del Informe

Principio ético que establece que el contenido del informe de pruebas debe mantenerse reservado y solo debe ser compartido con personas autorizadas.

---

19. Accionabilidad

Cualidad de una recomendación que la hace fácil de aplicar y de implementar por los equipos técnicos del cliente o la organización evaluada.

---

20. Comunicación de Resultados

Proceso de entrega y explicación del informe técnico al cliente. Puede incluir una presentación ejecutiva, reunión de cierre o revisión conjunta de hallazgos.
