PROYECTO DE APLICACIÓN

1.Definiciones

1.1. Pruebas orientadas a un objetivo

Son pruebas diseñadas específicamente para evaluar sistemas o componentes críticos, en función de un propósito definido, como identificar vulnerabilidades específicas, evaluar el impacto de un ataque o determinar el tiempo de respuesta ante incidentes.

1.2. Comprobación externa

Consiste en evaluar la seguridad desde una perspectiva externa, simulando ataques realizados por actores no autorizados que intentan acceder a los sistemas o aplicaciones desde fuera de la organización.

1.3. Pruebas internas

Son evaluaciones realizadas desde dentro de la red de la organización, simulando un escenario en el que un atacante tiene acceso interno, ya sea por haber comprometido una cuenta o por estar físicamente presente en las instalaciones.

1.4. Pruebas a ciegas

En este enfoque, los evaluadores tienen información limitada o nula sobre el sistema o red objetivo antes de la prueba. Esto simula un escenario en el que un atacante externo tiene poca información inicial sobre el objetivo.

1.5. Pruebas de doble ciego

En este tipo de pruebas, tanto los evaluadores como el personal de seguridad de la organización desconocen los detalles del ejercicio, simulando un ataque sorpresa para evaluar la capacidad de detección y respuesta de la organización.

2.Metodologías y guías para pruebas de penetración en Infraestructuras Críticas (IC)

2.1. ISSAF (Information Systems Security Assessment Framework)

Un marco estructurado que detalla cada paso del proceso de evaluación de seguridad, desde la planificación hasta la ejecución y el informe. ISSAF se centra en análisis técnico y operativo para identificar vulnerabilidades y evaluar controles en sistemas complejos.

- **Ventajas:** Enfoque exhaustivo y técnico, adecuado para infraestructuras críticas con múltiples componentes.
- **Utilidad en IC:** Permite evaluar cada capa de seguridad en sistemas críticos como SCADA o sistemas industriales.

2.2. NIST SP 800-115 (Technical Guide to Information Security Testing and Assessment)
Proporciona una guía detallada para realizar pruebas de seguridad en sistemas de información. Su enfoque incluye reconocimiento, descubrimiento de vulnerabilidades, explotación y elaboración de informes.

- **Ventajas:** Basada en estándares gubernamentales de EE.UU., es ampliamente adoptada.
- **Utilidad en IC:** Ayuda a cumplir con normativas y estándares regulatorios, esenciales para infraestructuras críticas.

2.3. OSSTMM (Open Source Security Testing Methodology Manual)
Una metodología abierta y estandarizada para pruebas de seguridad. Cubre diferentes áreas, como redes, aplicaciones, sistemas humanos y procesos organizacionales.

- **Ventajas:** Metodología completa que aborda aspectos técnicos y no técnicos.
- **Utilidad en IC:** Proporciona un enfoque equilibrado para proteger tanto los sistemas tecnológicos como los procesos humanos asociados.

2.4. PTES (Penetration Testing Execution Standard)
Un estándar diseñado para estructurar las pruebas de penetración de manera clara y repetible. Incluye fases como reconocimiento, modelado de amenazas, explotación, post-explotación y análisis de riesgos.

- **Ventajas:** Proceso bien definido que incluye gestión de riesgos.
- **Utilidad en IC:** Su enfoque en riesgos permite priorizar la protección de los sistemas más críticos.

2.5. OWASP (Open Web Application Security Project)
Una guía centrada en pruebas de aplicaciones web, con enfoque en la identificación y explotación de vulnerabilidades comunes como inyección SQL, XSS y controles de acceso.

- **Ventajas:** Orientada a la seguridad de aplicaciones web.

- **Utilidad en IC:** Relevante para proteger interfaces web de sistemas críticos y prevenir ataques dirigidos.

3.Uso de metodologías y pruebas en la protección de Infraestructuras Críticas

En una organización encargada de la gestión de infraestructuras críticas, las metodologías y pruebas de penetración desempeñan un papel fundamental para garantizar su seguridad. El proceso comienza con una evaluación de riesgos inicial mediante el uso de PTES, que permite identificar y priorizar las áreas más críticas dentro de la infraestructura. A continuación, se realizan pruebas externas utilizando ISSAF y NIST SP 800-115, las cuales simulan ataques desde fuera de la red con el objetivo de evaluar la exposición pública de los sistemas.

Paralelamente, se llevan a cabo pruebas internas basadas en OSSTMM, con las que se analiza el comportamiento del sistema frente a amenazas internas, como accesos no autorizados por parte de empleados. También se implementa OWASP para realizar pruebas específicas en aplicaciones web asociadas a sistemas críticos, permitiendo identificar vulnerabilidades particulares en este tipo de entornos.

Como parte de una estrategia de seguridad continua, se planifican ejercicios de doble ciego que combinan múltiples metodologías con el propósito de evaluar la capacidad de respuesta y los procesos de detección de la organización ante ataques no anunciados. Finalmente, los hallazgos obtenidos durante las pruebas se documentan de manera detallada, y se aplican parches y medidas correctivas basadas en las recomendaciones proporcionadas por cada metodología.

Este enfoque integral permite identificar, evaluar y mitigar los riesgos de seguridad, garantizando así la continuidad operativa de las infraestructuras críticas frente a las amenazas emergentes.

- ## Bibliografía

Alumnos, A. (s/f). *Infraestructuras críticas: definición, planes, riesgos, amenazas y legislación*. LISA Institute. Recuperado el 22 de enero de 2025, de

https://www.lisainstitute.com/blogs/blog/infraestructuras-criticas?srsltid=AfmBOopQ1fcBUnz7R-Xw6fNTAEd-kfkrbj85a26BfoLeAggMRIwL-NPI

Canorea, E. (2024, marzo 14). *Proteger las infraestructuras críticas de los ciberataques*. Plain Concepts. https://www.plainconcepts.com/es/proteger-infraestructuras-criticas-ciberataques/

Finn, T. (2024, septiembre 30). Top metodologías de pruebas de penetración. *Ibm.com*. https://www.ibm.com/es-es/think/insights/pen-testing-methodology