

[Año]

CARTOGRAFEANDO EL PENTESTING

SEGURIDAD INFORMATICA ACTIVIDAD 5

LUIS EDUARDO AZNAR CUEVAS 179880

Introducción

Los marcos MTRE ATT&CK, OWASP WSTG, NIST SP 800-115, OSSTMM, PTES, ISSAF proporcionan guías estructuradas para comprender tácticas de ataque, realizar pruebas de penetración y evaluar la seguridad de sistemas de información.

MITRE Corporation desarrolló MITRE ATT&CK, un marco de conocimiento que clasifica tácticas y técnicas utilizadas por adversarios reales, permitiendo analizar comportamientos de ataque y fortalecer estrategias de defensa.

Por su parte, OWASP publica la OWASP Web Security Testing Guide, una guía especializada en pruebas de seguridad para aplicaciones web, enfocada en la identificación de vulnerabilidades comunes.

El National Institute of Standards and Technology desarrolló la NIST SP 800-115, que proporciona lineamientos técnicos para la planificación y ejecución de pruebas de seguridad y evaluaciones técnicas.

Asimismo, el OSSTMM ofrece una metodología integral para pruebas de seguridad basadas en métricas verificables, mientras que el PTES establece un estándar estructurado para la ejecución de pruebas de penetración, desde la fase de pre-engagement hasta el reporte final.

Finalmente, el ISSAF integra prácticas técnicas y procedimientos detallados para la evaluación de la seguridad en sistemas de información.

En conjunto, estos marcos y estándares permiten estructurar procesos de análisis de amenazas, evaluación de vulnerabilidades y pruebas de penetración, contribuyendo a fortalecer la postura de seguridad de las organizaciones frente a un entorno de amenazas cada vez más complejo.

| Metodología | Descripción breve | Fases de implementación | Objetivo principal | Escenarios de uso | Orient. | Org. | URL | Certific. | Vigencia |
|-----------------|--|--|--|--|----------------------|--|---|--|------------------------------|
| MITRE ATT&CK | Base de conocimiento que clasifica tácticas y técnicas usadas por atacantes reales. No es guía de pentesting paso a paso, sino marco de referencia de comportamiento adversario. | 1. Reconocimiento de amenazas 2. Mapeo de técnicas 3. Simulación/red teaming 4. Evaluación de cobertura defensiva | Identificar, modelar y detectar técnicas de ataque reales. | SOC, Blue Team, Red Team, Threat Hunting, análisis post-incidente. | Evaluación y defensa | MITRE Corporation | https://attack.mitre.org | ATT&CK Fundamentals, Threat Intelligence, Detection Engineering y Purple Teaming | 2025, actualización continua |
| OWASP WSTG | Guía de pruebas de seguridad para aplicaciones web basada en riesgos. Estándar práctico para pentesting web. | 1. Antes de que comience el desarrollo 2. Durante la definición y el diseño 3. Durante el desarrollo 4. Durante la implementación/despliegue 5. Durante el mantenimiento y las operaciones | Detectar vulnerabilidades en aplicaciones web. | Web apps, APIs, comercio electrónico, fintech. | Ataque, evaluación | OWASP Foundation | OWASP Web Security Testing Guide | No posee una certificación directa | Versión 4.2 |
| NIST SP 800-115 | Guía técnica del gobierno de EE.UU. para pruebas de seguridad y evaluación de controles. | Despliegue – Mantenimiento y Operaciones | Evaluación de controles de seguridad organizacionales. | Entornos gubernamentales, corporativos, auditorías | Evaluación y ataque | NIST (National Institute of Standards) | https://csrc.nist.gov/publications/detail/sp/800-115/final | CISSP, CISA (alineadas a NIST) | Publicado 2008 |

| | | | | | | | | | |
|---------|---|--|---|--|-----------------------|--|--|--|----------------------------|
| | | | | formale s. | | and Tec hnology) | | | |
| OSSTM M | Metodología científica para medir seguridad operativa. Se enfoca en métricas y objetividad. | 1. Preparación 2. Recolección de información 3. Análisis de superficie de ataque 4. Métricas y reporte | Medir seguridad de forma cuantificable. | Infraestructura, redes, telecomunicaciones, físico. | Evaluaci ón | ISE CO M | https://www.i secom.org/O SSTMM.3.p df | OPSA (OSSTM M Professional Security Analyst) y OPST (OSSTM M Professional Security Tester) | Versión 3.0.2 |
| PTES | Marco práctico para estructurar pruebas de penetración de inicio a fin. | 1.Pre-engagement 2. Inteligencia 3. Modelado de amenazas 4. Análisis de vulnerabilida des5. Explotación 6Post-exploitación 7. Reporte | Estandarizar el proceso completo de pentesting. | Empresas privadas, consultoría, auditorías externas. | Ataque y evaluaci ón. | PTE S Technical Guidelines | http://www.p entest-standard.org | No tiene certificación directa | 2014 |
| ISSAF | Marco detallado de pruebas técnicas estructuradas por dominio de seguridad. | Definición y Diseño – Despliegue – Mantenimiento y Operaciones | Evaluareguridad en múltiples capas. | Redes corporativas, servidores, infraestructura TI. | Ataque y evaluaci ón. | OIS SG (Open Information Systems Security Group) | http://www.ois sg.org/issaf | No cuenta con certificación directa | Última publicación en 2006 |

Conclusión

Los estándares de prevención de ataques no solo facilitan la identificación de vulnerabilidades y la simulación controlada de ataques, sino que también promueven buenas prácticas, documentación formal y procesos repetibles que elevan la madurez de la seguridad organizacional. Su aplicación integrada permite pasar de un enfoque reactivo a uno proactivo, fortaleciendo la capacidad de detección, respuesta y mitigación ante amenazas reales.