13-2-2026

CNO V: Seguridad Informática

Hernández Fernández Diego Osvaldo – 182217

Mtro. Servando López Contreras

ACTIVIDAD 05

Análisis comparativo de metodologías de seguridad informática

Metodología	Descripción Breve	Fases de Implementación	Objetivo Principal	Escenarios de Uso	Orientación	Autores / Organismo	URL Oficial	Certificaciones Asociadas	Versiones Vigentes
MITRE ATT&CK	Fuente de información global sobre el modus operandi de los ciberdelincuentes, construida exclusivamente con datos del mundo real.	1. Preparación. 2. Mapeo. 3. Análisis de Brechas. 4. Maduración. 5. Validación.	Comprender e identificar el modus operandi y las metodologías de ataque (TTP).	Threat Hunting, Red Teaming, Respuesta a Incidentes, Emulación de Adversarios, Análisis de Brechas (Gap Analysis).	Ofensiva y Defensiva.	MITRE Corporation	https://attack.mitre.org	Certificación Oficial: MITRE ATT&CK Defender (MAD) por MITRE Engenuity. Certificaciones que lo integran: SANS GCTI, CompTIA CySA+, y Microsoft SC-200	La versión vigente de MITRE ATT&CK es la v18.1.
OWASP WSTG	Es el marco de trabajo más completo y detallado para realizar pruebas de penetración y auditorías de seguridad en aplicaciones y servicios web.	1. Recopilación de información 2. Pruebas de configuración y despliegue 3. Gestión de identidad 4. Autenticación 5. Autorización 6. Gestión de sesiones 7. Validación de entradas 8. Manejo de errores 9. Criptografía débil 10. Lógica de negocio 11. Pruebas en el lado del cliente 12. Pruebas de API	Identificación y contención de amenazas en entornos web.	Auditoría de aplicaciones web, desarrollo seguro (SDLC), pruebas de penetración, Bug Bounty web**.**	Evaluación / Defensiva.	OWASP (Open Worldwide Application Security Project)	https://owasp.org/www-project-web-security-testing-guide/	El marco de OWASP WSTG no posee una certificación propia emitida por la fundación, sin embargo cuenta con acreditaciones de hacking web entre las más destacadas se encuentra la eWPT y su versión avanzada eWPTX	La versión vigente oficial de la OWASP WSTG es la v4.2
NIST SP 800-115	Guía Técnica para Pruebas y Evaluaciones de Seguridad de la Información	1. Planificación 2. Descubrimiento 3. Ataque/Ejecución 4. Reporte	Establece los lineamientos y procedimientos para realizar pruebas de seguridad.	Ejecución de pruebas de penetración y análisis de vulnerabilidades, Auditorías de cumplimiento regulatorio (FISMA/HIPAA), Validación de controles de seguridad.	Evaluación / Cumplimiento.	**NIST** (Instituto Nacional de Estándares y Tecnología, EE.UU.)	https://csrc.nist.gov	Al ser un estándar del gobierno de EE. UU., NIST no emite certificaciones propias, sin embargo, CISA, CISSP, CEH, CompTIA PenTest+ y CySA+, utilizan las fases de evaluación del NIST como referencia para sus exámenes teóricos	La versión vigente oficial es la Revision 1

OSSTMM	Es un marco de trabajo científico creado por ISECOM para evaluaciones de seguridad, fundamentado en la recolección de hechos comprobables y datos cuantificables.	1. Seguridad Humana 2. Física 3. Inalámbrica 4. Telecomunicaciones 5. Redes de Datos	Proporciona una metodología científica y medible para evaluar la seguridad operativa de una organización	Auditorías de seguridad operativa integral (física, humana y lógica), Pruebas de ingeniería social y Verificación de confianza en controles de seguridad.	Evaluación / Medición científica.	**ISECOM** (Pete Herzog)	https://www.isecom.org	OPST (OSSTMM Professional Security Tester), OPSA (OSSTMM Professional Security Analyst), OPSE (OSSTMM Professional Security Expert) y OWSE (OSSTMM Wireless Security Expert).	La versión vigente oficial es la OSSTMM 3.0
PTES	Es un estándar desarrollado por la comunidad de profesionales de seguridad para definir un marco de ejecución común en las pruebas de penetración.	1. Pre-compromiso 2. Inteligencia 3. Modelado e amenazas 4. Análisis de vuln. 5. Explotación 6. Post-explotación 7. Informes.	Estandariza la calidad del pentesting para alinear expectativas y diferenciar claramente un análisis profesional profundo de un simple escaneo automatizado.	Estandarización de servicios de pentesting para el área comercial, Definición de Reglas de Compromiso (RoE), Ejecución de pruebas avanzadas.	Ofensiva.	Fue desarrollado por un comité de profesionales en seguridad ofensiva	http://www.pentest-standard.org/index.php/Main_Page	El PTES no tiene una certificación propia emitida por su comité. Sin embargo, las certificaciones como OSCP, OSWE, CPENT , GPEN y LPT. Estas certificaciones validan las habilidades técnicas que el PTES describe	La versión vigente oficial es la versión 1.1
ISSAF	Es un marco de evaluación de seguridad integral y extremadamente detallado que organiza las pruebas en pasos técnicos específicos.	1. Recopilación 2. Mapeo 3. Identificación Vuln. 4. Penetración 5. Acceso/Escalado 6. Enumeración 7. Compromiso remoto 8. Mantener acceso 9. Borrado de huellas.	Proporciona un marco técnico exhaustivo que relacione cada fase de una evaluación de seguridad con herramientas y metodologías específicas.	Auditorías técnicas exhaustivas de redes, sistemas operativos y bases de datos,	Ofensiva / Evaluación.	**OISSG** (Open Information Systems Security Group)	No se encontró link	No tiene una certificación única con su nombre, pero es el estándar que fundamenta las certificaciones de auditoría técnica más pesadas como CISA, CISSP, CEH, CPENT.	La versión más completa de este marco es la ISSAF Draft 0.2.1.

Referencias.

MITRE Corporation. (2025). MITRE ATT&CK® v14: Design and Philosophy. https://attack.mitre.org/

Cybersecurity & Infrastructure Security Agency (CISA). (2023). Best Practices for MITRE ATT&CK® Mapping. U.S. Department of Homeland Security. https://www.cisa.gov/news-events/news/best-practices-mitre-attckr-mapping

OWASP Foundation. (2024). Web Security Testing Guide (WSTG) v4.2. https://owasp.org/www-project-web-security-testing-guide/

Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). Technical Guide to Information Security Testing and Assessment (NIST Special Publication 800-115). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-115

National Institute of Standards and Technology. (2024). NIST Cybersecurity Framework (CSF) 2.0. U.S. Department of Commerce. https://www.nist.gov/cyberframework

Herzog, P. (2010). OSSTMM 3: The Open Source Security Testing Methodology Manual. Institute for Security and Open Methodologies (ISECOM). https://www.isecom.org/OSSTMM.3.pdf

ISECOM. (2021). Security Metrics and Operational Security Analysis. Institute for Security and Open Methodologies. https://www.isecom.org/research.html

PTES Team. (2014). The Penetration Testing Execution Standard. http://www.pentest-standard.org/index.php/Main_Page

SANS Institute. (2023). A Guide to the Penetration Testing Execution Standard (PTES). SANS Reading Room. https://www.sans.org/white-papers/

Cisco Networking Academy. (2024). Seguridad Informática - Hacker Ético [Módulos de curso]. Cisco Systems, Inc. https://www.netacad.com/es/courses/ethical-hacker?courseLang=es-XL