UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

ACTIVIDAD 05:

CARTOGRAFIANDO EL PENTESTING

Institución: Universidad Politécnica de San Luis Potosí

Materia:

CNO V – Seguridad Informática

Estudiante:

López Castro Diego – 182032

Profesor:

Mtro. Servando López Contreras

Fecha de entrega:

13 – Febrero – 2026

	Descripción breve de la metodología	Fases de implementación	Objetivo principal	Escenarios en los que se utiliza	Orientación	Autores u organismos responsables	URL del material oficial	Certificaciones asociadas	Versiones o actualizaciones vigentes
MTRE ATT&CK	Si bien no es precisamente una metodología, es un marco de referencia en donde se documentan tácticas y técnicas usadas por adversarios reales	**1.** Preparación **2.** Mapeo de técnicas **3.** Simulación **4.** Evaluación de la detección **5.** Respuesta	Identificar, clasificar y simular técnicas de ataques reales para poder evaluar las capacidades defensivas.	Para escenarios Red, Blue y PurpleTeam	Ataque y defensa	MITRE Corporation (The MITRE Corporation)	https://attack.mitre.org	MITRE ATT&CK DEFENDER™ (MAD)	La versión ATT&CK v18 (v18.0 y v18.1) fue la última actualización. Lanzada en octubre de 2025
OWASP WSTG	Guia detallada enfocada en la metodología para pruebas de seguridad de aplicaciones web	**1.** Recopilación de información **2.** Pruebas de gestión de configuración e implementación **3.** Pruebas de gestión de identidad **4.** Pruebas de autenticación **5.** Pruebas de autorización **6.** Pruebas de gestión de sesiones **7.** Pruebas de validación de entrada	Probar la seguridad de aplicaciones y servicios web	Auditorías para aplicaciones DevSecOps Evaluaciones de seguridad web	Evaluación de tipo ofensiva (Pruebas de penetración)	Open Worldwide Application Security Project (OWASP): - Rick Mitchell - Elie Saad - Rejah Rehim - Victoria Drake	https://owasp.org/www-project-web-security-testing-guide/	OWASP Web Security Testing Guide Training Course Certification	Versión 4.2. Actualización lanzada el 3 de diciembre de 2020

		8. Pruebas de manejo de errores **9.** Pruebas de criptografía débil **10.** Pruebas de lógica empresarial **11.** Pruebas del lado del cliente **12.** Pruebas API							
NIST SP 800-115	Guía metodológica que proporciona pruebas y evaluaciones de seguridad en sistemas de información, enfocada en pruebas técnicas	**1.** Planeación **2.** Descubrimiento **3.** Ataque **4.** Reporte	Dar una serie de lineamientos de forma estructurada para poder realizar pruebas técnicas de seguridad	Auditorías formales Entorno del gobierno Cumplimiento de las normas	Evaluación de control y evaluación técnica	National Institute of Standarts and Technology (NIST)	https://csrc.nist.gov/pubs/sp/800/115/final	NIST Cybersecurity Professional® NCSP® 800-115 Awareness Certificate	La actualización más reciente fue lanzada el 30 de septiembre de 2008
OSSTMM	Metodología científica, puesto que se basa en medidas cuantitativas, centrada en pruebas de seguridad de tipo operativa	**1.** Preparación previa al compromiso **2.** Recopilación de inteligencia **3.** Modelado de amenazas **4.** Análisis de vulnerabilidades **5.** Explotación **6.** Reporte **7.** Optimización	Medir de forma objetiva la seguridad usando las métricas cuantiativas	Evaluaciones sistemáticas y preventivas (auditorías integrales)	Evaluación de tipo ofensiva y para la validación	Institute for Security and Open Methodologies (ISECOM): • Pete Herzog • Marta Barceló • Bob Monroe • Kim Truett • Jaume Abella	https://www.isecom.org	- OSSTMM Professional Security Analyst - OSSTMM Professional Security Tester - OSSTMM Professional Security Expert - OSSTMM Wireless Security Expert - OSSTMM Certified Trust Analyst	La versión o actualización vigente fue la OSSTM 3, lanzada el 14 de diciembre de 2010

						• Robert R. Lee • Nicolas Mayencourt • Raoul Chiesa			
PTES	Guía de estándar abierto que desarrolla un proceso completo y técnico sobre pruebas de penetración	**1.** Interacciones previas al compromiso **2.** Recopilación de inteligencia **3.** Modelado de amenazas **4.** Análisis de vulnerabilidades **5.** Explotación **6.** Post-explotación **7.** Informes	Mostrar un estándar en el proceso técnico y en la organización de las pruebas de penetración	Pruebas de penetración a nivel corporativo, además de pruebas externas e internas	Ataque de tipo ofensivo de forma estructurada	Comunidad de PTES	http://www.pentest-standard.org/index.php/Main_Page	- EC-Certified Ethical Hacker (CEH) - C)PEH Certified Professional Ethical Hacker - Licensed Penetration Tester (LPT) - GIAC Penetration Tester (GPEN) - GIAC Web Application Penetration Test (GWAPT) - Certified Penetration Tester - Certified Expert Penetration Tester	La versión vigente es la versión 1.1 PTES technical guidelines
ISSAF	Metodología extensa y detallada para realizar pruebas de penetración y evaluaciones de seguridad	**1.** Recopilación de información **2.** Asignación de red **3.** Identificación de vulnerabilidades **4.** Penetración **5.** Obtener acceso y escalamiento de privilegios **6.** Más enumeración	Mostrar un marco detallado para realizar pruebas de penetración completas y todo lo necesario para hacerlo	Se puede usar en un escenario de auditorías técnicas, en donde se hagan pruebas internas de infraestructura	Evaluación en la parte ofensiva	Open Information Security Group (OISSG)	https://pymesec.org/issaf/	No se encuentran certificaciones asociadas, puesto que la comunidad original quedó descontinuada y no hay autoridad formal que emita la certificación	La versión vigente fue lanzada en 2004, como la versión 0.2.1

		7. Comprometer a usuarios / sitios remotos **8.** Mantener el acceso **9.** Cubriendo las pistas							

Referencias bibliográficas

Cisco Networking Academy. (2026). 1.2 Exploración de las metodologías de pruebas de penetración. Recuperado el 12 de febrero de 2026, de Cisco Networking Academy | Seguridad Informática-Hacker ético: https://www.netacad.com/launch?id=3b07bfc3-9b21-4dbd-909b-a235416df136&tab=curriculum&view=3d7507ef-98e1-51ac-b102-6bdb7618f7a4

Cybersecurity Education Guides. (2026). What Is The PTES (Penetration Testing Execution Standard)? Recuperado el 12 de febrero de 2026, de Cybersecurity Education Guides: https://www.cybersecurityeducationguides.org/what-is-the-ptes-penetration-testing-execution-standard/

Herzog, P. (2010). OSSTMM 3. Recuperado el 12 de febrero de 2026, de ISECOM: https://www.isecom.org/OSSTMM.3.pdf

ISECOM. (2026). Research. Recuperado el 12 de febrero de 2026, de ISECOM: https://www.isecom.org/research.html#content5-9d

MITRE Corporation. (2025). Get Started. Recuperado el 12 de febrero de 2026, de MITRE ATT&CK: https://attack.mitre.org/resources/

MITRE Corporation. (2026). ATT&CK. Recuperado el 12 de febrero de 2026, de MITRE ATT&CK: https://attack.mitre.org

MITRE Corporation. (2026). MITRE ATT&CK DEFENDER™ (MAD). Recuperado el 12 de febrero de 2026, de MAD20: https://mad20.com

National Institute of Standarts and Security (NIST). (septiembre de 2008). NIST SP 800-115 Technical Guide to Information Security Testing and Assessment. Recuperado el 12 de febrero de 2026, de CSRC NIST: https://csrc.nist.gov/pubs/sp/800/115/final

National Institute of Standarts and Security (NIST). (2026). NIST Cybersecurity Professional®. Recuperado el 12 de febrero de 2026, de NIST Cybersecurity Professional: https://www.nistcybersecurityprofessional.website/nist-800-115-awareness-certificate

OISSG. (30 de abril de 2006). Information Sistems Security Assessment Framework (ISSAF) Draft 0.2.1. Recuperado el 12 de febrero de 2026, de Untrusted Network: https://untrustednetwork.net/files/issaf0.2.1.pdf

Open Information Security Group (OISSG). (2024). ISSAF. Obtenido de PYMESEC: https://pymesec.org/issaf/

OWASP. (03 de diciembre de 2020). Release v4.2. Recuperado el 12 de febrero de 2026, de GitHub: https://github.com/OWASP/wstg/releases/tag/v4.2

OWASP. (2026). OWASP Web Security Testing Guide. Recuperado el 12 de febrero de 2026, de OWASP: https://owasp.org/www-project-web-security-testing-guide/

OWASP. (2026). OWASP Web Security Testing Guide. Recuperado el 12 de febrero de 2026, de GitHub: https://github.com/OWASP/wstg

OWASP. (2026). OWASP Web Security Testing Guide Training Course. Recuperado el 12 de febrero de 2026, de NobleProg: https://www.nobleprog.mx/en/cc/owaspwstg

OWASP. (2026). WSTG - Latest. Recuperado el 12 de febrero de 2026, de OWASP: https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/00-Introduction_and_Objectives/README

PTES. (16 de agosto de 2014). Main Page. Recuperado el 12 de febrero de 2026, de PentTest Standard: http://www.pentest-standard.org/index.php/Main_Page

Scarfone, K., Souppaya, M., Cody , A., & Orebaugh, A. (septiembre de 2008). Technical Guide to Information Security Testing and Assessment. Recuperado el 12 de febrero de 2026, de NIST: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf