

Cartografiando el pentesting: análisis comparativo de metodologías de seguridad informática

ACTIVIDAD 5

Francisco Javier Cruz Juarez - 177622

Maestro: Servando Lopez Contreras

Seguridad Informatica

ACTIVIDAD 05 - Cartografiando el pentesting

INDICE

1. Introducción	2
2. Tabla Comparativa de Metodologías	2
4. Bibliografías	3

ACTIVIDAD 05 - Cartografiando el pentesting

1. Introducción

El presente documento realiza un análisis comparativo de las principales metodologías y marcos de referencia utilizados en la industria de la ciberseguridad. El objetivo es identificar las características, fases y objetivos de cada estándar para determinar su aplicabilidad según distintos escenarios de evaluación técnica y cumplimiento normativo.

2. Tabla Comparativa de Metodologías

Metodología	A. Descripción	B. Fases de Implementación	C. Objetivo Principal	D. Escenarios de Uso	E. Orientación	F. Autor / Organismo	G. URL Oficial	H. Certificaciones	I. Versión
MITRE ATT&CK	Base de conocimientos de Tácticas y Técnicas basadas en ataques reales.	Tácticas, Técnicas y Procedimientos (TTPs).	Clasificar comportamientos de adversarios.	SOC, Threat Hunting y emulación de ataques.	Ataque / Defensa	MITRE Corporation	attack.mitre.org	CDE	v14
OWASP WSTG	Marco integral para pruebas de seguridad en aplicaciones web.	1. Recolección de información, 2. Configuración., 3. Identidad, 4. Autenticación, 5. Autorización, etc.	Evaluación técnica de controles en software web.	Auditorías web, móviles y de APIs.	Evaluación Técnica	OWASP Foundation	owasp.org	GWAPT, OSWE	v4.2
NIST SP 800-115	Guía técnica federal para realizar pruebas y exámenes de seguridad.	1. Planificación, 2. Descubrimiento, 3. Ejecución, 4. Post-ejecución.	Estandarizar pruebas técnicas y reportes.	Entornos gubernamentales y regulados.	Auditoría	NIST (EE.UU.)	csrc.nist.gov	Security+, CISSP	Final
OSSTMM	Estándar científico para la verificación de seguridad operacional.	1. Inducción, 2. Interacción, 3. Interrogación, 4. Evaluación.	Medición métrica de la seguridad (RAVs).	Redes, Wireless, Física e Ingeniería Social.	Evaluación Operativa	ISECOM	isecom.org	OPST, OPSA	3.0

ACTIVIDAD 05 - Cartografiando el pentesting

PTES	Estándar que define las etapas mínimas de un pentest de calidad.	1. Pre-engagement, 2. Intel, 3. Modelado, 4. Análisis, 5. Explotación, 6. Post-Exp, 7. Reporte.	Estandarizar el proceso comercial y técnico del pentest.	Auditorías profundas de infraestructura.	Ataque (Pentest)	Comunidad de Expertos	pentest-standard.org	OSCP, CPTS	1.1
ISSAF	Marco detallado que vincula la técnica con la gestión y auditoría.	1. Planificación, 2. Evaluación, 3. Informes, 4. Limpieza, 5. Destrucción.	Guía técnica paso a paso para auditorías completas.	Auditorías integrales de sistemas complejos.	Auditoría	OISSG	oissg.org	CISA (Base)	v0.2.1

4. Bibliografías

1. **Harper, A., et al. (2022).** *Gray Hat Hacking: The Ethical Hacker's Handbook* (6th ed.). McGraw-Hill Education.
2. **National Institute of Standards and Technology. (2008).** *Technical Guide to Information Security Testing and Assessment (SP 800-115)*. U.S. Department of Commerce.
3. **MITRE Corporation. (2023).** *ATT&CK Design and Philosophy*. Recuperado de <https://attack.mitre.org>
4. **OWASP Foundation. (2023).** *Web Security Testing Guide (WSTG)*. Recuperado de <https://owasp.org>