# ACTIVIDAD 05

## CARTOGRAFIANDO EL PENTESTING: ANÁLISIS COMPARATIVO DE METODOLOGÍAS DE SEGURIDAD INFORMÁTICA

**Alonso Castillo Omar Karim 179033**

CNO V – Ciberseguridad

Mtro. Servando López Contreras

Alonso Castillo Omar Karim

Universidad Politécnica de San Luis Potosí

| Metodología | Descripción | Fases de Implementación | Objetivo Principal | Escenarios de Uso | Orientación | Autor u Organismo | Certificaciones | Vigencia o Versión | URL Oficial |
|---|---|---|---|---|---|---|---|---|---|
| **MITRE ATT&CK** | Base de conocimiento de tácticas y técnicas adversarias basadas en observaciones del mundo real. | 1. Reconnaissance<br><br>2. Resource Development<br><br>3. Initial Access<br><br>4. Execution<br><br>5. Persistence<br><br>6. Privilege Escalation<br><br>7. Defense Evasion<br><br>8. Credential Access<br><br>9. Discovery<br><br>10. Lateral Movement<br><br>11. Collection<br><br>12. Command and Control<br><br>13. Exfiltration<br><br>14. Impact | Clasificación y entendimiento del comportamiento del adversario. | Threat Intelligence, Detección de intrusos, Emulación de adversarios. | Ofensiva (Adversary Simulation) / Defensiva | MITRE Corporation | MITRE ATT&CK Defender (MAD) | v18 (Oct 2025) | attack.mitre.org |
| **OWASP WSTG** | Guía principal para pruebas | 1. Information Gathering | Evaluación técnica de | Auditoría de aplicaciones | Evaluación / Testing | OWASP Foundation | N/A (Estándar abierto) | v4.2 (Stable) / v5 (Dev) | owasp.org/wstg |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | de seguridad en aplicaciones web y servicios web. | 2. Config. & Deployment Management Testing<br><br>3. Identity Management Testing<br><br>4. Authentication Testing<br><br>5. Authorization Testing<br><br>6. Session Management Testing<br><br>7. Input Validation Testing<br><br>8. Error Handling<br><br>9. Cryptography<br><br>10. Business Logic Testing<br><br>11. Client-side Testing<br><br>12. API Testing | seguridad en aplicaciones web. | Web, Desarrollo Seguro (SDLC). | | | | | |
| **NIST SP 800-115** | Guía técnica para realizar evaluaciones de seguridad de la | 1. Planning<br><br>2. Discovery<br><br>3. Attack | Estandarización de evaluaciones técnicas para gestión de riesgos. | Gobierno federal (EE.UU.), Cumplimiento | Evaluación / Auditoría | NIST (National Institute of Standards and Technology) | N/A (Referencia para otras certs) | Rev 1 (2008) - Vigente | csrc.nist.gov |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | información y pentesting. | 4. Reporting | | normativo, Empresas. | | | | | |
| **OSSTMM** | Manual de metodología científica para pruebas de seguridad operativa y métricas. | 1. Induction Phase<br><br>2. Interaction Phase<br><br>3. Investigation Phase<br><br>4. Intervention Phase | Medición científica de la seguridad operativa (métricas). | Auditoría de seguridad operativa, Medición de confianza. | Evaluación / Auditoría | ISECOM | OPST, OPSA, OPSE | v3.0 (Oficial) / v4 (Draft) | isecom.org |
| **PTES** | Estándar ejecutiva para realizar pruebas de penetración completas y estructuradas. | 1. Pre-engagement Interactions<br><br>2. Intelligence Gathering<br><br>3. Threat Modeling<br><br>4. Vulnerability Analysis<br><br>5. Exploitation<br><br>6. Post Exploitation<br><br>7. Reporting | Estandarizar la ejecución y reporte de pentesting profesional. | Consultoría de Pentesting, Pruebas de penetración comerciales. | Ataque (Simulación) | PTES Team (Comunidad) | N/A | V1.0 (Estándar continuo) | pentest-standard.org |
| **ISSAF** | Framework estructurado (antiguo) que vincula fases de pentesting con herramientas específicas. | 1. Planning and Preparation<br><br>2. Assessment (Steps: Info Gathering, Network Mapping, Vuln ID, Penetration, Gaining Access, Priv Esc, | Guía detallada paso a paso vinculada a herramientas. | Formación académica, Referencia histórica de pentesting. | Evaluación / Ataque | OISSG (Open Information Systems Security Group) | N/A (Descontinuada) | Legacy / Descontinuado | N/A (Sitio inactivo) |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Maintaining Access, Covering Tracks)<br><br>3. Reporting, Cleanup & Destroy Artifacts | | | | | | | |

---

**Bibliografía / Referencias**


- **MITRE Corporation.** (2025). *MITRE ATT&CK®: Design and Philosophy*. Recuperado de https://attack.mitre.org
- **OWASP Foundation.** (2020). *Web Security Testing Guide (WSTG) v4.2*. Recuperado de https://owasp.org/www-project-web-security-testing-guide/
- **NIST.** (2008). *Technical Guide to Information Security Testing and Assessment (SP 800-115)*. National Institute of Standards and Technology. Recuperado de https://csrc.nist.gov/publications/detail/sp/800-115/final
- **ISECOM.** (2010). *The Open Source Security Testing Methodology Manual (OSSTMM) 3.0*. Recuperado de https://www.isecom.org/
- **The PTES Team.** (2014). *The Penetration Testing Execution Standard*. Recuperado de http://www.pentest-standard.org/
- **OISSG.** (Legacy). *Information Systems Security Assessment Framework (ISSAF)*. (Nota: El proyecto oficial se encuentra descontinuado y su sitio web inactivo, se conserva como referencia académica).