Assessment 1 – Compare Pentesting Methodologies
EPT232 Ethical Hacking and Penetration Testing

Prepared by:
Smriti Parajuli (Student ID: MDS3000025)

Submitted to:
Sarada Hettiarachchi
Bachelor of Software Engineering (AI)
Media Design School

Date:
31st March 2025

1. Introduction

Penetration testing, also known as ethical hacking, is a structured approach to evaluating system security through controlled cyberattack simulations (Scarfone & Mell, 2008). This proactive practice enables organizations to identify and remediate vulnerabilities before they can be exploited. Given the legal, technical, and ethical complexities involved, standardized methodologies are essential. They provide a comprehensive framework for planning, execution, and reporting, while ensuring consistency, transparency, and alignment with security objectives (Scarfone & Mell, 2008). With the growing diversity of technologies and threats in modern enterprises, selecting the most appropriate methodology is critical. This report examines four widely adopted penetration testing methodologies—OSSTMM, PTES, OWASP WSTG, and MITRE ATT&CK—analyzing their scope, strengths, and limitations. It concludes with a recommendation for the most suitable approach to web application testing.

2. Comparison of Pentesting Methodologies

2.1. OSSTMM (Open-Source Security Testing Methodology Manual)

The Open Source Security Testing Methodology Manual (OSSTMM), developed by ISECOM, presents a scientific and metrics-driven approach to assessing operational security across digital, physical, and human vectors. It introduces measurable frameworks like the Risk Assessment Value (RAV) to ensure repeatability and objectivity in testing outcomes (Herzog, 2015).

A core strength of OSSTMM is its focus on data-driven evaluation, making it highly suitable for organizations that require evidence-based security analysis. Its scope enables holistic evaluation of complex environments, including network and physical access. However, OSSTMM can be challenging for newcomers, as it lacks detailed tooling guidance and step-by-step execution instructions. This complexity may hinder adoption by smaller teams or testers with limited experience. Overall, OSSTMM suits large enterprises needing layered security, including physical and human elements.

2.2. PTES (Penetration Testing Execution Standard)

The Penetration Testing Execution Standard (PTES) offers a structured, lifecycle-based framework comprising seven key phases: pre-engagement, intelligence gathering, threat

modeling, vulnerability analysis, exploitation, post-exploitation, and reporting (PTES, n.d.). This end-to-end approach ensures methodical consistency across different testing engagements.

PTES stands out for its focus on collaborative planning and communication, aligning testing efforts with organizational goals and security expectations. Its flexible structure enables testers to adapt the scope and depth of assessments based on business needs, risk tolerance, or compliance standards. However, PTES does not include tool-specific guidance or detailed technical test cases, making it less effective for specialized testing—particularly web applications, where more granular frameworks like OWASP WSTG are better suited. PTES is best for infrastructure and internal system assessments.

2.3. OWASP WSTG (Web Security Testing Guide)

The OWASP Web Security Testing Guide (WSTG) is a targeted methodology designed specifically for assessing the security of web applications through structured, repeatable, and comprehensive test cases. It aligns closely with the OWASP Top Ten, addressing critical web vulnerabilities such as SQL injection, cross-site scripting (XSS), broken authentication, and insecure deserialization (OWASP Foundation, 2023). WSTG organizes its testing into key categories—including input validation, authentication, session management, and error handling—allowing testers to perform systematic, full-stack assessments. Its strength lies in technical depth, ideal for detecting web vulnerabilities.

Although WSTG is limited to web-based systems and can be resource-intensive for large-scale applications, its rigor, industry relevance, and widespread adoption make it the most effective framework for organizations focused on web application security, regulatory compliance, and secure development practices.

2.4. MITRE ATT&CK Framework

The MITRE ATT&CK Framework is a globally recognized and continuously updated knowledge base that documents adversary tactics, techniques, and procedures (TTPs) derived from real-world threat intelligence (MITRE, 2022). Unlike conventional penetration testing methodologies, ATT&CK does not guide a full testing life cycle. Instead, it specializes in adversary emulation, making it particularly valuable for red teaming, threat hunting, and post-exploitation scenarios where understanding APT behavior is essential (Albahar, Alansari, & Jurcut, 2022). A key strength of the framework lies in its ability to simulate realistic attack

scenarios across various platforms (e.g., Windows, Linux, macOS, and cloud environments). This allows organizations to assess defenses and validate incident response (Albahar et al.2022). However, ATT&CK lacks coverage for early-stage testing activities such as reconnaissance, vulnerability scanning, and initial exploitation, making it unsuitable as a standalone penetration testing methodology (MITRE, 2022).

In practice, ATT&CK is best used as a complementary tool alongside structured frameworks like PTES or OSSTMM. Its focus on adversarial realism makes it ideal for enhancing threat modeling and strengthening post-exploitation analysis within comprehensive security assessments.

2.5. Comparative Summary Table

The table below presents a consolidated comparison of the four penetration testing methodologies analyzed in this report.

Methodology	**Scope**	**Strengths**	**Limitations**	**Best Use Case**
OSSTMM	Physical, human, digital ops	Measurable, scientific, repeatable	Complex, lacks tool guidance	Enterprise operational environments
PTES	Full penetration lifecycle	Structured, end-to-end, broad coverage	Less focus on web, no tool suggestions	Network and infrastructure testing
OWASP WSTG	Web applications only	Detailed, OWASP-aligned, widely used	Time-consuming, web-only	Web app security assessments
MITRE ATT&CK	Threat simulation	Real-world threat mapping, up-to-date	No scanning/exploit steps, not standalone	Red teaming, post-exploitation analysis

Table 1. Comparative summary of penetration testing methodologies.Compiled by the author; informed by *(Herzog 2015); (PTES 2020); (OWASP 2023); (MITRE 2022)*.

2.6. Methodology Selection and Justification

Based on the comparative analysis, the OWASP Web Security Testing Guide (WSTG) is the most suitable framework for conducting penetration tests on web applications. Unlike broader methodologies such as PTES or OSSTMM, WSTG is purpose-built to address vulnerabilities specific to web environments—such as SQL injection, cross-site scripting (XSS), broken authentication, and insecure deserialization—which are consistently featured in the OWASP Top Ten (OWASP, 2023).

WSTG offers a test-case-driven structure with over a hundred detailed procedures organized across key areas including input validation, session management, and error handling. This structured, repeatable format ensures thorough assessments, particularly in regulated sectors like finance, healthcare, and e-commerce, where compliance and auditability are essential.

Further reinforcing its relevance, a recent empirical study by (Albahar, Alansari, and Jurcut 2022) found that even advanced penetration testing tools often deliver inconsistent results. This highlights the need for standardized, methodology-guided testing like OWASP WSTG to achieve consistent, high-quality vulnerability detection.

While PTES and OSSTMM remain strong choices for network and operational testing, they lack the technical granularity needed for application-layer assessments. Similarly, the MITRE ATT&CK framework excels in post-exploitation and threat emulation, but it does not support early testing stages such as scanning or exploitation.

In summary, OWASP WSTG's clear focus, in-depth structure, empirical support, and wide industry adoption make it the most effective and reliable choice for web application penetration testing.

3. Discussion & Analysis

3.1 Benefits and Challenges of Using Multiple Methodologies

Utilizing multiple penetration testing methodologies within a single engagement can significantly enhance the depth, accuracy, and overall coverage of a security assessment. For example, combining OSSTMM's metric-based evaluation, PTES's structured life cycle, and MITRE ATT&CK's threat emulation allows for a multi-dimensional approach that addresses operational, procedural, and adversarial aspects (Scarfone & Mell, 2008). This hybrid model

increases the likelihood of detecting complex vulnerabilities and strengthens validation by cross-verifying findings from multiple perspectives.

However, this approach also introduces challenges. Overlapping scopes, redundant efforts, and inconsistent terminology across frameworks can cause inefficiencies, extend testing timelines, and result in confusion during reporting. Varying outcomes may also complicate stakeholder interpretation and delay remediation efforts.

To address these issues, organizations should:

- Clearly define the testing scope and objectives beforehand.
- Align each methodology to relevant testing phases (e.g., PTES for engagement structure, MITRE for post-exploitation, OSSTMM for operational analysis).
- Establish communication protocols and assign clear responsibilities to ensure coordination among testing teams.

With proper management, this approach enhances visibility, threat coverage, and stakeholder confidence.

3.2 Penetration Testing Techniques: Black Box, White Box, and Grey Box

Penetration testing techniques are typically grouped into three main types—black box, white box, and grey box—each representing different levels of system knowledge and threat simulation (Ehmer & Khan, 2012).

1. **Black Box Testing:**
   Simulates an external attacker with no prior system knowledge. It targets publicly accessible assets like websites or login portals and is effective for assessing perimeter security. However, it may miss internal logic flaws due to limited visibility.

2. **White Box Testing**:
   Provides full access to the system's source code, architecture, and configurations. It enables deep analysis of code-level vulnerabilities and is ideal for secure development and compliance checks, though it lacks real-world attacker realism..

3. **Grey Box Testing:**
   Offers partial system knowledge—such as credentials or API documentation—emulating insider threats or semi-privileged users. It balances depth and realism, making it suitable for risk-based assessments, though its effectiveness varies with access level.

In conclusion, black box testing suits external threat simulation, white box excels in detailed audits, and grey box offers a practical middle ground. Choosing the right approach—or combining them—should align with organizational goals, risk tolerance, and compliance needs.

4. Ethical and Professional Considerations

Ethical hacking must be carried out with informed client consent, full transparency, and strict adherence to legal and professional standards. Penetration testers often gain access to highly sensitive data such as personally identifiable information (PII), financial records, and internal configurations, necessitating compliance with data protection laws like the GDPR and New Zealand's Privacy Act 2020 (Scarfone & Mell, 2008). A clearly defined scope of engagement—outlining permitted systems, techniques, and timelines—is essential to prevent unauthorized access and ensure legal boundaries are respected.

A real-world example from 2022 involved a security firm conducting a test on a New Zealand government department that unintentionally accessed live citizen data due to vague scope definitions. The incident, which prompted intervention by the Office of the Privacy Commissioner, highlights the importance of clear testing parameters and robust safeguards.

Testers must disclose vulnerabilities promptly and allow time for remediation. To minimize operational risks, they should use non-destructive tools, avoid denial-of-service (DoS) testing unless explicitly permitted, conduct tests in controlled environments, and monitor systems closely for unintended impact. Comprehensive documentation throughout the process supports accountability and facilitates post-engagement reviews.

In New Zealand, many organizations mandate NDAs and encourage adherence to ethical frameworks such as the OWASP Code of Ethics. Ultimately, ethical and legal lapses can result in reputational harm, regulatory penalties, and client distrust. Therefore, testers must uphold confidentiality, integrity, and lawful conduct, ensuring assessments strengthen, not jeopardize, trust.

5. Conclusion

This report examined four leading penetration testing methodologies—OSSTMM, PTES, OWASP WSTG, and MITRE ATT&CK—each offering distinct strengths across different phases of the testing lifecycle. OWASP WSTG stood out as the most suitable for web application testing due to its technical depth, structured test cases, and strong alignment with real-world threats. The analysis also emphasized the benefits of combining methodologies for broader coverage, though this requires careful planning to avoid redundancy. Ethical and legal responsibilities—such as client consent, confidentiality, and compliance with GDPR and the New Zealand Privacy Act 2020—were highlighted as essential to responsible testing.

In conclusion, methodology selection must balance technical needs and ethics to ensure effective testing

6. References:

1. Albahar, M., Alansari, D., & Jurcut, A. (2022). An empirical comparison of pen-testing tools for detecting web app vulnerabilities. *Electronics, 11*(19), 2991. https://doi.org/10.3390/electronics11192991

2. ENISA. (2022). *Guidelines for penetration testing*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/guidelines-for-penetration-testing

3. Ehmer, M., & Khan, F. (2012). Comparative study of white box, black box and grey box testing techniques. *International Journal of Advanced Computer Science and Applications, 3*(6), 12–18. https://doi.org/10.14569/IJACSA.2012.030603

4. Herzog, P. (2015). *OSSTMM: Open source security testing methodology manual* (3rd ed.). Institute for Security and Open Methodologies (ISECOM). https://www.isecom.org/OSSTMM.3.pdf

5. MITRE. (2022). *MITRE ATT&CK® framework*. https://attack.mitre.org/

6. National Institute of Standards and Technology. (2020). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

7. OWASP Foundation. (2023). *Web security testing guide (WSTG) v4.2*. https://owasp.org/www-project-web-security-testing-guide/

8. Penetration Testing Execution Standard. (n.d.). *PTES technical guidelines*. https://www.pentest-standard.org/index.php/Main_Page

9. Penetration Testing Execution Standard. (n.d.). *The penetration testing execution standard*. Retrieved March 28, 2025, from https://pentest-standard.readthedocs.io

10. Scarfone, K., & Mell, P. (2008). *Guide to information security testing and assessment* (NIST SP 800-115). National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/sp/800-115/final

11. Mohurle, S., & Patil, M. (2017). A brief study of WannaCry threat: Ransomware attack 2017.1938–1940.https://sbgsmedia.in/2018/05/10/2261f190e292ad93d6887198d7050dec.pdf

12. Alkhurayyif, Y., & Almarshdy, Y. S. (2024). Adopting automated penetration testing tools: A cost-effective approach to enhancing cybersecurity in small organizations. *Journal of Information Security and Cyber Crimes Research, 7*(1), 51–66. https://doi.org/10.26735/RJJT2453