Lab - Compare Pentesting Methodologies

Answers in red

Objectives

In this lab, you will complete the following objectives:

- Compare Various Pentesting Methodologies
- Conduct Research of Popular Pentesting Methodologies

Background / Scenario

You are conducting a penetration test for a customer. To show that your planned methods are valid, you will use well-known and accepted pentesting methodologies. Because there is more than one methodology to choose from, you decide to research and compare four of the most widely used methodologies to be familiar with the strengths of each.

Required Resources

- PC or mobile device with internet access

Instructions

Part 1: Conduct Research Popular Pentesting Methodologies

Using your favorite search engine, conduct research on four of the most popular pentesting methodologies:

- OSSTMM
- PTES
- OWASP WSTG
- MITRE ATT&CK

Step 1: Gather information about OSSTMM.

In this step, you will learn about the Open Source Security Testing Methodology Manual (OSSTMM), which includes a complete methodology for security assessment.

a. Navigate to https://www.isecom.org, click **RESEARCH** > **OSSTMM**.
b. On the OSSTMM main page, view the OSSTMM document.

What is the latest version of the manual and its copyright date?

The latest version is OSSTMM 3.02, published on December 14, 2010.

Although OSSTMM is old, it is still a good starting off point for planning and conducting

security tests and audits. It is important however to use it in combination with more up-to-date standards and methodologies.
What organization develops the OSSTMM? What do they do?

The Institute for Security and Open Methodologies (ISECOM) develops the OSSTMM. ISECOM is a non-profit organization focused on creating open research and methodologies for security testing. They maintain projects, certifications, and training related to operational security.

What are the stated primary and secondary purposes of the OSSTMM as stated in the OSSTMM publication?

- Primary Purpose: To provide a scientific methodology for accurate characterization of operational security (OpSec) through examination and correlation of test results in a consistent and reliable way.

- Secondary Purpose: To provide guidelines that, when followed correctly, allow an analyst to perform a certified OSSTMM audit**.** These include ensuring thorough testing, lawful compliance, quantifiable results, and consistency and repeatability

What six outcomes are assured then the OSSTM guidelines are correctly followed?

1. The test was conducted thoroughly.
2. The test included all necessary channels.
3. The posture for the test complied with the law.
4. The results are measurable in a quantifiable way.
5. The results are consistent and repeatable.
6. The results contain only facts derived from the tests themselves

What are the ten steps of applying the OSSTM when the 4 Point Process and Trifecta are combined?

1. Passively collect data of normal operations to comprehend the target.
2. Actively test operations by agitating operations beyond the normal baseline.
3. Analyze data received directly from the operations tested.
4. Analyze indirect data from resources and operators (i.e. workers, programs).
5. Correlate and reconcile intelligence from direct (step 3) and indirect (step 4) data test results to determine operational security processes.
6. Determine and reconcile errors.
7. Derive metrics from both normal and agitated operations.
8. Correlate and reconcile intelligence between normal and agitated (steps 1 and 2) operations to

determine the optimal level of protection and control which would best be implemented.
9. Map the optimal state of operations (step 8) to processes (step 5).
10. Create a gap analysis to determine what enhancements are needed for processes governing necessary protection and controls (step 5) to achieve the optimal operational state (step 8) from the current one.

Step 2: Gather Information About PTES.

The Penetration Testing Execution Standard is a comprehensive guide to the process of conducting penetration tests.

Navigate to www.pentest-standard.org.

What is the latest version of the standard?

The latest version of the standard is version 1

What are the seven main sections of the PTES?

1. Pre-engagement Interactions
2. Intelligence Gathering
3. Threat Modeling
4. Vulnerability Analysis
5. Exploitation
6. Post Exploitation
7. Reporting

What is the stated purpose of the PTES? (**Hint**: Look in the FAQs)

The purpose of the PTES is to provide businesses and security professionals with a common language and scope for performing penetration testing and security evaluations.

What document specifies tools and techniques to be used in the seven sections of the test?

The PTES Technical Guidlines

Step 3: Gather information about the OWASP WSTG.

The OWASP WSTG is a guide for testing the security of web applications and web services. It is not a general guide to penetration testing. Instead, it focuses on developing, deploying, and maintaining secure web applications.

Navigate to https://owasp.org/www-project-web-security-testing-guide/.

What is the latest version of the WSTG standard?

The latest version of the WSTG standard is version 4.2

Access the current stable version of the WSTG. What are the five phases of the Web Security Testing Framework?

The five phases are as follows:
Phase 1 - Before development begins
Phase 2 - During definition and design
Phase 3 - During development
Phase 4 - During Deployment
Phase 5 - During Maintenance and Operations

What is the stated purpose of the OWASP WSTG?

The stated purpose of the OWASP WSTG is to provide a comprehensive guide for testing the security of web applications. It describes techniques, methods, tools and resources for testing the most common web application security issues.

What are the twelve categories of active tests defined in the OWASP Web Testing Framework?

The twelve categories of active tests defined in the OWASP Web Testing Framework are:
1. Information gathering
2. Configuration and deployment management testing
3. Identity management testing
4. Authentication testing
5. Authorization testing
6. Session management testing
7. Input validation testing
8. Error Handling
9. Cryptography
10. Business logic testing
11. Client-side testing
12. API testing

Step 4: Gather information about MITRE ATT&CK.

MITRE ATT&CK is a detailed knowledgebase of attacker tactics, techniques, and procedures (TTP) that have been gathered from real attacks. It is not a manual or standard regarding how to conduct penetration tests. However, penetration testers can use it for ideas and guidance about how to exploit vulnerabilities as part of a test.

a. Navigate to https://attack.mitre.org.

What is the latest version of the ATT&CK standard?

The latest version of the ATT&CK standard is version 13

Why did MITRE develop ATT&CK? (**Hint**: Look in the FAQs)

MITRE ATT&CK was developed as a way to document common tactics, techniques, and procedures (TTPs) that advanced persistent threats use against Windows enterprise networks.

What six common use cases for ATT&CK are described?

The six common use cases are:
1. Adversary Emulation
2. Red Teaming
3. Behavioral Analytics Development
4. Defensive Gap Assessment
5. SOC Maturity Assessment
6. Cyber Treat Intelligence Enrichment.

What are the three ATT&CK Technology Domains?

The three ATT&CK Technology Domains are:
1. Enterprise
2. Mobile
3. ICS

What are three sub-techniques that are provided for this technique?

The three sub-techniques that are provided for this technique are:
1. Techniques for gathering credentials
2. Email addresses
3. Employee names

Who is the Lazarus Group? They conducted a campaign to gather email addresses for later attacks. How did they gather and use email addresses?

The Lazarus Group is a state sponsored cyber threat group from North Korea.
They used fake phishing attacks and other attacks to gather email addresses that were used in phishing campaigns.

Reflection Questions

1. You researched four popular pentesting methodologies in this lab. Name at least two additional pentesting methodologies that are in common use.

Two additional pentesting methodologies include:

1. ISSAF which is developed by the Open Information Systems Security Group (OISSG), ISSAF is a comprehensive framework that outlines detailed procedures for conducting security assessments, focusing on policy compliance**,** technical controls**,** and risk mitigation across IT environments. It's highly technical and maps closely to real-world attacker behavior.

2. NIST SP 800-115 which is a U.S. government standard that provides a structured approach to planning, executing, and reporting on technical security tests like vulnerability scans, penetration tests, and security assessments. It emphasizes preparation, discovery, attack, and post-test activities**.**

2. Why is it important to follow a recognized pentesting methodology?

Following a recognized penetration testing methodology is important because it ensures the assessment is structured, consistent, and comprehensive. It helps testers systematically cover all relevant attack surfaces, such as networks, applications, physical infrastructure, and human factors. A formal methodology also provides documentation that makes the testing process and results defensible in case of audits, client disputes, or legal scrutiny. By aligning with industry standards like PTES, OSSTMM, or NIST 800-115, testers gain credibility and demonstrate professionalism. Moreover, using a methodology helps manage risks by preventing scope creep and ensuring that tests remain within legal and contractual boundaries. Ultimately, it improves the efficiency, effectiveness, and trustworthiness of the penetration testing process.