Assignment 2 - Compare Pentesting Methodologies

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.

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

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

Answer: The latest version of the OSSTMM is version 3.0, and its copyright date is 2010. Although OSSTMM is old, it is still a good starting off point for planning and conducting

Assignment 2 - Compare Pentesting Methodologies

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?

Answer: The OSSTMM was developed by the Institute for Security and Open Methodologies (ISECOM), a non-profit organization that provides research, certifications, and develop open-source security methodologies for security testing and analysis.

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

Answer: The primary purpose of the OSSTMM is to provide a structured methodology for testing and analyzing the operational security of any environment. And the second being is to provide a means of measurement that is both qualitative and quantitative, allowing for the accurate assessment of the security state.

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

Answer: Here are six outcomes are assured then the OSSTM guidelines are correctly following below:

i. Operational Security Efficiency
ii. Transparency
iii. Measurement Accuracy
iv. Security Assurance
v. Risk Reduction
vi. Compliance.

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

Answer: The Open Source Security Testing Methodology Manual (OSSTM) is a comprehensive framework used for security testing and assessment. When combining the 4 Point Process with the Trifecta, the methodology becomes a structured approach to ensure thorough security evaluation. Let's break down each step:

- **4 Point Process**
    i. Define the Scope
    ii. Assess the Target

Assignment 2 - Compare Pentesting Methodologies

iii. Test the Target
iv. Report Findings

- **Trifecta**

v. Security Posture Evaluation
vi. Operational Security Measurement
vii. Verification and Validation
viii. Threat and Vulnerability Analysis
ix. Impact Analysis
x. Recommendations for Improvement

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?
Answer: v1.0 although a v2.0 is in the works soon

What are the seven main sections of the PTES?
Answer: The seven main sections of the Penetration Testing Execution Standard (PTES) are:

i. Pre-engagement Interactions
ii. Intelligence Gathering
iii. Threat Modeling
iv. Vulnerability Analysis
v. Exploitation
vi. Post Exploitation
vii. Reporting

What is the stated purpose of the PTES? (Hint: Look in the FAQs)
Answer: The stated purpose of the PTES (Penetration Testing Execution Standard) is to provide both businesses and security service providers with a common language and scope for performing penetration testing (i.e. Security evaluations).

Assignment 2 - Compare Pentesting Methodologies

What document specifies tools and techniques to be used in the seven sections of the test?
Answer: The document that specifies tools and techniques to be used in the seven sections of the Penetration Testing Execution Standard (PTES) is the PTES **Technical Guidelines.**
This document provides detailed guidance on tools, techniques, and methodologies that should be applied during the different phases of a penetration test, which include pre-engagement interactions, intelligence gathering, threat modeling, vulnerability analysis, exploitation, post-exploitation, and reporting.

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?
Answer: The latest stable version of the OWASP Web Security Testing Guide (WSTG) is **version 4.2**, released on December 3, 2020. This version introduces new testing scenarios, updates existing chapters, and offers an improved writing style and chapter layout.

Access the current stable version of the WSTG. What are the five phases of the Web Security Testing Framework?
Answer: The Web Security Testing Framework (WSTF) is a structured approach to testing the security of web applications. It is designed to help security professionals systematically identify and address vulnerabilities. The five phases of the Web Security Testing Framework are:

i. Information Gathering
ii. Configuration and Deployment Management Testing
iii. Identity Management Testing
iv. Authentication Testing

Assignment 2 - Compare Pentesting Methodologies

v. Authorization Testing

What is the stated purpose of the OWASP WSTG?
Answer: The stated purpose of the OWASP Web Security Testing Guide (WSTG) is to provide a comprehensive framework for testing the security of web applications. The OWASP (Open Web Application Security Project) Web Security Testing Guide (WSTG) is a well-known resource in the field of web application security.

What are the twelve categories of active tests defined in the OWASP Web Testing Framework?
Answer: The OWASP Web Testing Framework is a comprehensive guide for testing the security of web applications. It includes various categories of tests to identify vulnerabilities and ensure the security of web applications. The twelve categories of active tests in the OWASP Web Testing Framework are:

i. Information Gathering
ii. Configuration and Deployment Management Testing
iii. Identity Management Testing
iv. Authentication Testing
v. Authorization Testing
vi. Session Management Testing
vii. Input Validation Testing
viii. Error Handling and Logging
ix. Data Protection Testing
x. Business Logic Testing
xi. Client-Side Testing
xii. 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

Assignment 2 - Compare Pentesting Methodologies

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.

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

What is the latest version of the ATT&CK standard?
Answer: As of October 31, 2024, the latest version of the MITRE ATT&CK framework is **version 16.1**.

Why did MITRE develop ATT&CK? (Hint: Look in the FAQs)
Answer: The MITRE ATT&CK framework was developed to advance the field of cybersecurity by providing actionable, real-world intelligence on attacker behavior and helping organizations to better protect themselves against sophisticated threats.

- In the page menu click **Resources** > **General Information** > **ATT&CK Design and Philosophy**.
- Open and review the ATT&CK Design and Philosophy pdf.

What six common use cases for ATT&CK are described?
Answer: The MITRE ATT&CK framework is a comprehensive matrix of tactics and techniques used by adversaries to achieve their objectives. It is widely used in cybersecurity for various purposes. Here are six common use cases for ATT&CK:

i. Threat Intelligence
ii. Detection and Monitoring
iii. Incident Response
iv. Red Teaming and Adversary Emulation
v. Security Engineering and Architecture
vi. Threat Hunting

What are the three ATT&CK Technology Domains?
Answer: The three ATT&CK Technology Domains are Enterprise, Cloud and Mobile.

- Go to the MITRE ATT&CK Enterprise matrix by opening the Matrices menu and choosing Enterprise.

Assignment 2 - Compare Pentesting Methodologies

- The matrix represents tactics as column headers with techniques arranged as entries in each column. For information on a given technique, click its entry. Additional information is shown on the information page. The information page can include sub-techniques, procedures, mitigations, detection methods, and references. Not all techniques include procedures.
- In the column for the Reconnaissance tactic, click the Gather Victim Identity Information Review the information there.

What are three sub-techniques that are provided for this technique?
Answer: The sub-techniques provided for a particular technique, it seems like the context is related to a framework or a set of techniques, possibly from a cybersecurity perspective, such as the MITRE ATT&CK framework.
The three sub-techniques are:

i. T1589.001: Search Open Websites/Domains
ii. T1589.002: Search Open Technical Databases
iii. T1589.003: Search Open Social Media

- Select the Email Addresses sub-technique. Review the information there.
- Look at the entries under Procedures.

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

Answer: The Lazarus Group is a North Korean state-sponsored hacking organization known for cyber espionage, financial theft, and disruptive attacks.
They gathered email addresses through spear phishing, data scraping from platforms like LinkedIn, third-party breaches, and malware-infected documents. Once collected, they used these emails for phishing attacks, credential theft, malware deployment, and supply chain attacks, often targeting financial institutions, cryptocurrency firms, and defense organizations.

Reflection Questions

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

Assignment 2 - Compare Pentesting Methodologies

Answer: Two least additional popular pretesting methodologies are:

i. **ISSAF (Information Systems Security Assessment Framework):** ISSAF provides a comprehensive framework for security assessments, including penetration testing.

ii. **CTF (Capture the Flag):** While not a formal methodology, Capture the Flag (CTF) exercises are a popular approach for testing and demonstrating penetration testing skills.

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

Answer: Following a recognized penetration testing methodology helps ensure thorough, effective, and reliable security assessments, leading to better protection against potential threats and vulnerabilities.