Lab - 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.

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?

Answer Area
<!----><!---->

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?

Answer Area
<!----><!---->

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

Answer Area

<!----><!---->

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

Answer Area

<!----><!---->

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

Answer Area

<!----><!---->

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 Area

<!----><!---->

What are the seven main sections of the PTES?

Answer Area

<!----><!---->

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

Answer Area

<!----><!---->

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

Answer Area

<!----><!---->

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 Area

<!----><!---->

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

Answer Area

<!----><!---->

What is the stated purpose of the OWASP WSTG?

Answer Area

<!----><!---->

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

Answer Area
<!----><!---->

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?

Answer Area
<!----><!---->

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

Answer Area
<!----><!---->

b. In the page menu click **Resources** > **General Information** > **ATT&CK Design and Philosophy**.
c. Open and review the ATT&CK Design and Philosophy pdf.
What six common use cases for ATT&CK are described?

Answer Area
<!----><!---->

What are the three ATT&CK Technology Domains?

Answer Area
<!----><!---->

d. Go to the MITRE ATT&CK Enterprise matrix by opening the **Matrices** menu and choosing **Enterprise**.
e. 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** entry.

Review the information there.

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

Answer Area
<!----><!---->

f. 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 Area
<!----><!---->

Reflection Questions

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

Answer Area

<!----><!---->

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

Answer Area

<!----><!---->