Penetration Testing

tutorialspoint

SIMPLY EASY LEARNING

www.tutorialspoint.com

https://www.facebook.com/tutorialspointindia

https://twitter.com/tutorialspoint

About the Tutorial

Penetration Testing is used to find flaws in the system in order to take appropriate security measures to protect the data and maintain functionality. This tutorial provides a quick glimpse of the core concepts of Penetration Testing.

Audience

This tutorial has been prepared for beginners to help them understand the basics of Penetration Testing and how to use it in practice.

Prerequisites

Before proceeding with this tutorial, you should have a basic understanding of software testing and its related concepts.

Copyright & Disclaimer

We strive to update the contents of our website and tutorials as timely and as precisely as possible, however, the contents may contain inaccuracies or errors. Tutorials Point (I) Pvt. Ltd. provides no guarantee regarding the accuracy, timeliness or completeness of our website or its contents including this tutorial. If you discover any errors on our website or in this tutorial, please notify us at contact@tutorialspoint.com

Table of Contents

1. Penetration Testing — Introduction

What is Penetration Testing?

Penetration testing is a type of security testing that is used to test the insecurity of an application. It is conducted to find the security risk which might be present in the system.

If a system is not secured, then any attacker can disrupt or take authorized access to that system. Security risk is normally an accidental error that occurs while developing and implementing the software. For example, configuration errors, design errors, and software bugs, etc.

Why is Penetration Testing Required?

Penetration testing normally evaluates a system's ability to protect its networks, applications, endpoints and users from external or internal threats. It also attempts to protect the security controls and ensures only authorized access.

Penetration testing is essential because:

- It identifies a simulation environment i.e., how an intruder may attack the system through **white hat attack**.
- It helps to find weak areas where an intruder can attack to gain access to the computer's features and data.
- It supports to avoid **black hat attack** and protects the original data.
- It estimates the magnitude of the attack on potential business.
- It provides evidence to suggest, why it is important to increase investments in security aspect of technology.

When to Perform Penetration Testing?

Penetration testing is an essential feature that needs to be performed regularly for securing the functioning of a system. In addition to this, it should be performed whenever:

- Security system discovers new threats by attackers.
- You add a new network infrastructure.
- You update your system or install new software.
- You relocate your office.
- You set up a new end-user program/policy.

How is Penetration Testing Beneficial?

Penetration testing offers the following benefits::

- **Enhancement of the Management System**: It provides detailed information about the security threats. In addition to this, it also categorizes the degree of vulnerabilities and suggests you, which one is more vulnerable and which one is less. So, you can easily and accurately manage your security system by allocating the security resources accordingly.

- **Avoid Fines**: Penetration testing keeps your organization's major activities updated and complies with the auditing system. So, penetration testing protects you from giving fines.

- **Protection from Financial Damage**: A simple breach of security system may cause millions of dollars of damage. Penetration testing can protect your organization from such damages.

- **Customer Protection**: Breach of even a single customer's data may cause big financial damage as well as reputation damage. It protects the organizations who deal with the customers and keep their data intact.

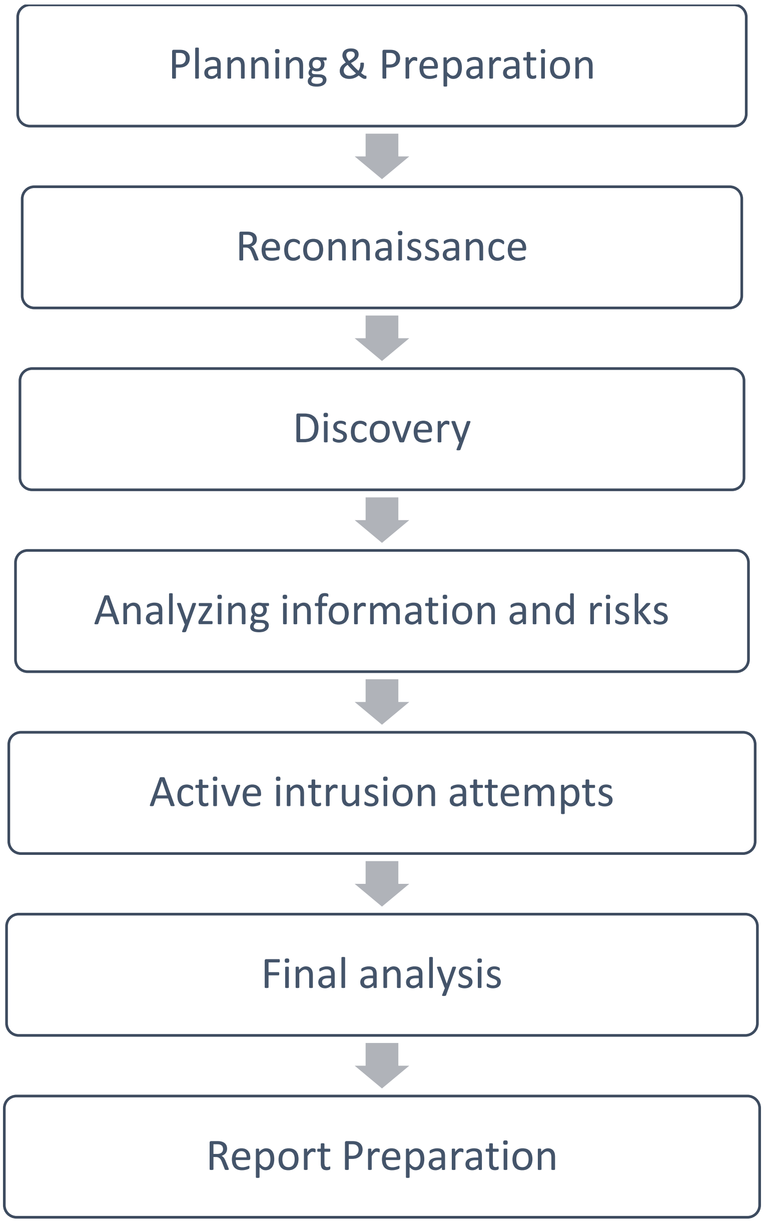
2. Penetration Testing — Penetration Testing Method

Penetration testing is a combination of techniques that considers various issues of the systems and tests, analyzes, and gives solutions. It is based on a structured procedure that performs penetration testing step-by-step.

This chapter describes various steps or phases of penetration testing method.

Steps of Penetration Testing Method

The following are the seven steps of penetration testing:


Planning & Preparation
Reconnaissance
Discovery
Analyzing information and risks
Active intrusion attempts
Final analysis
Report Preparation