Principle of Pre-Engagement Activities

Perp: Khalid Ebn Elwleed Mohamed Ahmed

October 2025

Contents

Introduction

The engagement phase, often referred to as the **pre-engagement phase**, is one of the most critical stages in a penetration testing process. It establishes the foundation for the entire assessment by defining the **scope, objectives, and rules of engagement**. During this phase, both the client and the testing team align their expectations, clarify legal and contractual obligations, and determine success criteria.

Pre-Engagement Activities

When we talk about **Pre-Engagement activities** is a basic task that sets the stage for a successful penetration test. Help you break down the complexities of preparing for a penetration test. The importance of pre-engagement lies in:

- Ensuring Alignment.
- Legality.
- Success of penetration testing.

Regulations, Standards and Stakeholders

During the penetration testing process regulations and standards guide you to safeguarding the sensitive data and systems.

Operating within legal frameworks ensures **ethical and legal compliance**.

Regulations

Legally binding mandates demand adherence to data protection rules and it's different between countries. The common regulations such as:

1. ***General Data Protection Regulation (GDPR)***

   Linked within the **EU and for businesses dealing with EU citizen's data**. Impose strict rules on data processing and movement. Core element of GDPR:

   - Explicit permission for data processing.
   - Performing data processing impact assessments.

2. ***Gramm-leach-Bliley Act (GLBA)***

   It's known as the Financial Services Modernization Act of 1999. Used to protect the privacy of individual's financial information that is held by financial institutions.

Mandates security and confidentiality of financial information. Compliance involves:

- Conducting security measures like **encryption** and **access control.**
- Make security assessments to prevent data breaches.

3. ***Health Insurance Portability and Accountability Act (HIPAA)***

Regulates confidentiality and security of **health information in the U.S**. Provides **physical**, **administrative**, and **technical safeguards** for patient's data.

Specific requirements:

- Encrypting patient data is transmitted across open networks.
- Implementing secure access control.
- Conducting regular audits.

Standards

Standard is **not legal requirements** but essential for cybersecurity best practice. That's mean **Established by industry players.**

Common Standards that relate to cybersecurity:

1. ***Payment Card Industry Data Security Standard (PCL DSS)***
   Basis for securing payment card data,

Specific requirements:

- Maintaining a secure network.
- Implementing strong access control measures.
- Regularly monitoring and testing networks.

2. ***ISO/IEC 27000 Series***

Provide specifications for implementing, maintaining, and improving information security management systems. Help manage security of assets like **financial information, intelligence property, employee details,** and **information entrusted by third parties.**

Builds customer trust by demonstrating compliance with internationally recognized benchmarks.

Stakeholder

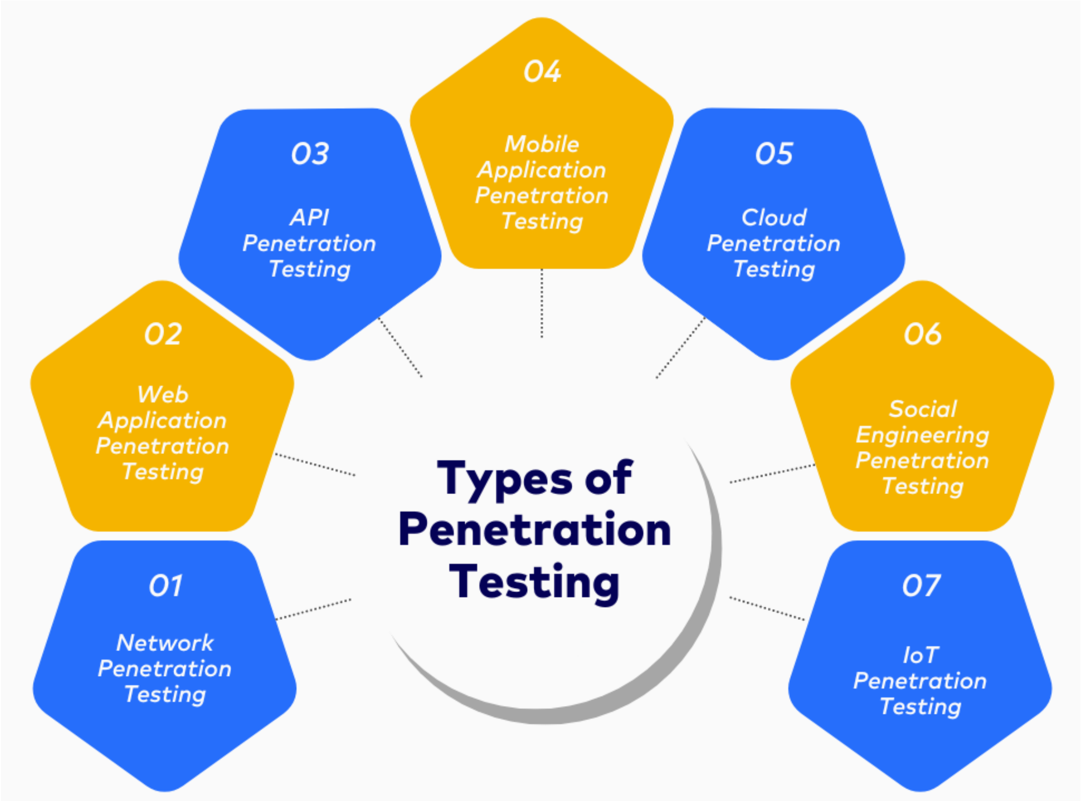
The alignment ensures that all parties **understand penetration testing objectives** and **outcomes.**

- **Aligns goals, budget, and timelines from technical teams** to executive leadership.
- Importance of ongoing training, reviewing and regular audits.

Example:

Bank of Khartoum - Ensures compliance with the **Payment Card Industry Data Security Standard (PCI DSS)** to protect customer cardholder data and maintain secure payment operations.

Type of Assessment in Penetration Test


Types of Penetration Testing
01
Network Penetration Testing
02
Web Application Penetration Testing
03
API Penetration Testing
04
Mobile Application Penetration Testing
05
Cloud Penetration Testing
06
Social Engineering Penetration Testing
07
IoT Penetration Testing

Type of Agreements

- ### *Non-Disclosure Agreements (NDAs)*

It's **legally binding contract** that establishes a confidential relationship; The main purpose is

Purpose: Ensure that any information discovered during a penetration test remains confidential.

- ### *Master Service Agreements (MSAs)*

Foundational terms of the business relationship between a **service provider and the client,**

Includes:

i. Project Scope.
ii. Payment details.
iii. Confidentiality Clauses.
iv. Liability Issues.

Purpose: Clarifies how engagements are conducted, handles recurring costs, and addresses any additional charges.

- ### *Terms of Service (ToS)*

It's agreement that governs **the use of the service provided by the Penetration Test firm.**

Includes:

i. Rules and guidelines for using the penetration test services.
ii. User rights.
iii. Service limitations.
iv. Client's obligations.

Purpose: Verified clients understand their role in safeguarding test data, agree not to disclose or misuse sensitive security information.

- ### *Statements of Work (SoWs)*

Known as document that details the specifics of the **project or service provided.**

Includes:

i. Objectives and Deliverables.
ii. Scope of work.
iii. Timelines.
iv. Payment schedules.
v. Responsibilities of each party

Purpose: Ensures mutual understanding of project details, helps manage expectations, guides project execution.

Rule of Engagement

There are different rules of engagement you should be aware of before you are conducting a Penetration Test. Such as:

1. ***Exclusions***
   Areas or elements within the scope of the penetration test that are off limit, Some reasons of exclusions such as: (**Importance and confidential nature of the data, Potential for business disruption.**

2. ***Test Case***
   Predefined scenarios are developed to systematically **evaluate the security of the system.** Based on:
   - **Known vulnerabilities.**
   - **Potential threat vectors.**
   - **Specific concerns expressed by the client.**

3. ***Testing Window***
   Time frame agreed upon for Pen Test activities, The purpose of the testing window is to **minimize disruption to business operations** and **ensure testing reflects normal operational conditions.**

4. ***Goal Reprioritization***
   Depending on the **test's priorities and allowing to change** it as new information as discovered. Concentrate resources on the **most critical vulnerabilities.**

5. ***Post-Activity Business Impact Analysis***
   Assessing the potential consequences for the **client if identified vulnerabilities are exploited.** Aimed to clarify the link between **findings** and their impact on their impact on the business.

Shared Responsibility Model

- ***Hosting Providers***

  Aimed to secure the infrastructure, running all services offered to customers had some responsibility, such as:

  - Physical security of data centers.
  - Network hardware.
  - Server hardware.
  - Storage.
  - Virtualization layers.

- ***Customers***

  Manage the **security of software** and **systems on the hosting provider's infrastructure.** Responsibility such as:

  - Operating system patches and updates.
  - Application security.
  - Data protection through encryption and access controls.
  - Configure security settings and manage network traffic controls.

- ***Pen Testers***

  External auditors within the Shared Responsibility Model had different **responsibilities such as**:

  - Find vulnerabilities that threat actors could exploit.
  - Test the effectiveness of security controls.
  - Simulate attacks on both the hosting provider's infrastructure and customer's applications.
  - Provide detailed reports on vulnerabilities and suggest security enhancements.

Cloud Providers' Specialized Services

This model help customers understand and secure their specific cloud environments. Such as **(AWS, Microsoft Azure, Google Cloud). Tools such as:**

- Rusted Advisor, AWS Inspector.
- Security Center, Azure Advisor.
- Security Command Center, Google Cloud Armor.

Third-Party Service Providers

This role ensures that **products or services integrated** into the customer's environment **do not introduce new vulnerabilities** and maintain the overall security posture. **Responsibilities such as:**

- Secure and regularly update their software.
- Follow strict security protocols when accessing customer systems.

Example Scenario

Context

- Healthcare Management System hosted on AWS

Hosting Provider (AWS)

- Ensures physical security of data centers and availability of infrastructure.
- Manages the underlying hardware, storage, and networking components.

Customer (Healthcare Organization)

- Responsible for securing patient data, virtual servers, and health records databases.
- Implements access controls and ensures compliance with HIPAA regulations.

Penetration Tester

- Conducts regular security assessments on web portals, APIs, and cloud configurations.
- Identifies misconfigurations, vulnerabilities, and data exposure risks.

Third-Party Provider (Medical Imaging Service)

- Manages imaging data storage and transmission (e.g., X-rays, MRIs).
- Ensuring data is encrypted, and communication channels meet compliance standards.