HACKTHEBOX

Tier I Fundamental General

This module teaches the penetration testing process broken down into each stage and discussed in detail. We will cover many aspects of the role of a penetration tester during a penetration test, explained and illustrated with detailed examples. The module also covers pre-engagement steps like the criteria for establishing a contract with a client for a penetration testing engagement.

By: Saezel

Last Updated: 17 October 2024

Pre-Engagement

Pre-engagement is the stage of preparation for the actual penetration test. During this stage, many questions are asked, and some contractual agreements are made. The client informs us about what they want to be tested, and we explain in detail how to make the test as efficient as possible.

How many documents must be prepared in total for a penetration test?

Answer: 7

	Document	Timing for Creation
1	Non-Disclosure Agreement (NDA)	After Initial Contact
2	Scoping Questionnaire	Before the Pre-Engagement Meeting
3	Scoping Document	During the Pre-Engagement Meeting
4	Penetration Testing Proposal (Contract/Scope of Work (SoW))	During the Pre-engagement Meeting
5	Rules of Engagement (RoE)	Before the Kick-Off Meeting
6	Contractors Agreement (Physical Assessments)	Before the Kick-Off Meeting
7	Reports	During and after the conducted Penetration Test

Vulnerability Assessment

During the vulnerability assessment phase, we examine and analyze the information gathered during the information gathering phase. The vulnerability assessment phase is an analytical process based on the findings.

What type of analysis can be used to predict future probabilities?

Answer: Predictive

Analysis Type	Description
Descriptive	Descriptive analysis is essential in any data analysis. On the one hand, it describes a data set based on individual characteristics. It helps to detect possible errors in data collection or outliers in the data set.
Diagnostic	Diagnostic analysis clarifies conditions' causes, effects, and interactions. Doing so provides insights that are obtained through correlations and interpretation. We must take a backward-looking view, similar to descriptive analysis, with the subtle difference that we try to find reasons for events and developments.
Predictive	By evaluating historical and current data, predictive analysis creates a predictive model for future probabilities. Based on the results of descriptive and diagnostic analyses, this method of data analysis makes it possible to identify trends, detect deviations from expected values at an early stage, and predict future occurrences as accurately as possible.
Prescriptive	Prescriptive analytics aims to narrow down what actions to take to eliminate or prevent a future problem or trigger a specific activity or process.

Post-Exploitation

The Post-Exploitation stage aims to obtain sensitive and security-relevant information from a local perspective and business-relevant information that, in most cases, requires higher privileges than a standard user.

How many types of evasive testing are mentioned in this section?

Answer: 3

Evasive testing is divided into three different categories:

	Type of Testing	Description	Key Differences
1	Evasive	Focuses on avoiding detection while executing penetration tests. The aim is to identify blind spots in defenses.	Primarily seeks to remain undetected; if detected, it can still provide value by revealing gaps in monitoring processes.
2	Hybrid Evasive	Combines evasive techniques with specific testing goals. Targets defined components or security measures.	Allows for more controlled testing, focusing on certain departments or servers. Balances evasion with the need to assess particular defenses.
3	Non-Evasive	Conducted with full knowledge of security measures in place, often triggering defenses intentionally for assessment.	Aims to maximize information gathering without hiding; may trigger alerts but is useful for evaluating the effectiveness of security measures. Often used in tandem with evasive methods.

What is the name of the security standard for credit card payments that a company must adhere to? (Answer Format: acronym)

Answer: PCI-DSS

(PCI-DSS) - The Payment Card Industry Data Security Standard

Post-Engagement

The Post-engagement stage refers to the phase that occurs after a penetration testing engagement is completed, where the focus shifts to analyzing and documenting the findings. During this stage, the testing team compiles a comprehensive report detailing vulnerabilities discovered, the methodologies used, and recommendations for remediation.

What designation do we typically give a report when it is first delivered to a client for a chance to review and comment? (One word)

Answer: DRAFT

Stage	Description
Draft Report	Initial report containing findings, recommendations, and details tailored to the client's environment marked as DRAFT
Report Review Meeting	Discussion with the client to go through the draft, clarify findings, and address any questions or changes.
Deliverable Acceptance	Finalization of the report after client feedback; issues a new version marked as FINAL.
Post-Remediation Testing	Verification of remediated findings; issuance of a post-remediation report showing the state of the environment.
Close Out	Final report delivery, secure data handling, invoicing, and follow-up for client satisfaction.