

Penetration Testing Process:

Link to challenge: <https://academy.hackthebox.com/module/90>

(log in required)

Class: Tier I | Fundamental | General

## Penetration Testing Phases - Assessment Specific Stages

**Pre-Engagement:**

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

**Answer:** 7

**Method:**

This stage also requires the preparation of several documents before a penetration test can be conducted that must be signed by our client and us so that the declaration of consent can also be presented in written form if required. Otherwise the penetration test could breach the [Computer Misuse Act](#). These documents include, but are not limited to:

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:

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

**Answer:** Predictive

**Method:**

### 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.

## Post-Exploitation:

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

**Answer:** 3

**Method:**

Evasive testing is divided into three different categories:

**Evasive**

**Hybrid Evasive**

**Non-Evasive**

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

**Answer:** PCI-DSS

**Method:**

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

# Penetration Testing Phases - Assessment Specific Stages

## Post-Engagement:

**Question:** 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

## Method:

### Deliverable Acceptance

The Scope of Work should clearly define the acceptance of any project deliverables. In penetration test assessments, generally, we deliver a report marked **DRAFT** and give the client a chance to review and comment. Once the client has submitted feedback (i.e., management responses, requests for clarification/changes, additional evidence, etc.) either by email or (ideally) during a report review meeting, we can issue them a new version of the report marked **FINAL**. Some audit firms that clients may be beholden to will not accept a penetration test report with a **DRAFT** designation. Other companies will not care, but keeping a uniform approach across all customers is best.