# 2.5.6 Engagement Contract Facts

Before a penetration test can begin, there are a few key documents that must be completed and agreed on. These documents are designed to protect both the organization and the penetration tester.

Even though much of this information could be put into a single document, it makes things much clearer when all the details are separated out into the documents described in this table.

| Document | Description |
|---|---|
| Scope of Work | The Scope of Work is one of the more detailed documents for a project. This document spells out in detail the who, what, when, where, and why of the penetration test. Explicitly stated in the Scope of Work are details of all system aspects that can be tested, such as IP ranges, servers, and applications.<br><br>Anything not listed is off-limits to the ethical hacker. Off-limit features should also be explicitly stated in the Scope of Work document to avoid any confusion. This document will also define the test's time frame, purpose, and any special considerations. |
| Rules of Engagement | The Rules of Engagement document defines how the penetration test will be carried out. This document defines whether the test will be a white box, gray box, or black box test. Other details, such as how to handle sensitive data and who to notify in case something goes wrong, will be listed in the document. |
| Master Service Agreement | It is very common for companies to do business with each other multiple times. In these situations, a Master Service Agreement is useful. This document spells out many of the terms that are commonly used between the two companies, such as payment. This makes future contracts much easier to complete, as most details are already spelled out. |
| Non-Disclosure Agreement | This is a common legal contract outlining confidential material or information that will be shared during the assessment and the restrictions placed on it. This contract basically states that anything the tester finds cannot be shared, with the exception of those people stated in the document. |
| Permission to Test | This document is often referred to as the get-out-of-jail-free card. Since most people in the client's organization will not know about the penetration test occurring, this document is used if the penetration tester gets caught. This document is used only as a last resort, but explains what the penetration tester is doing and that the work is fully authorized. |