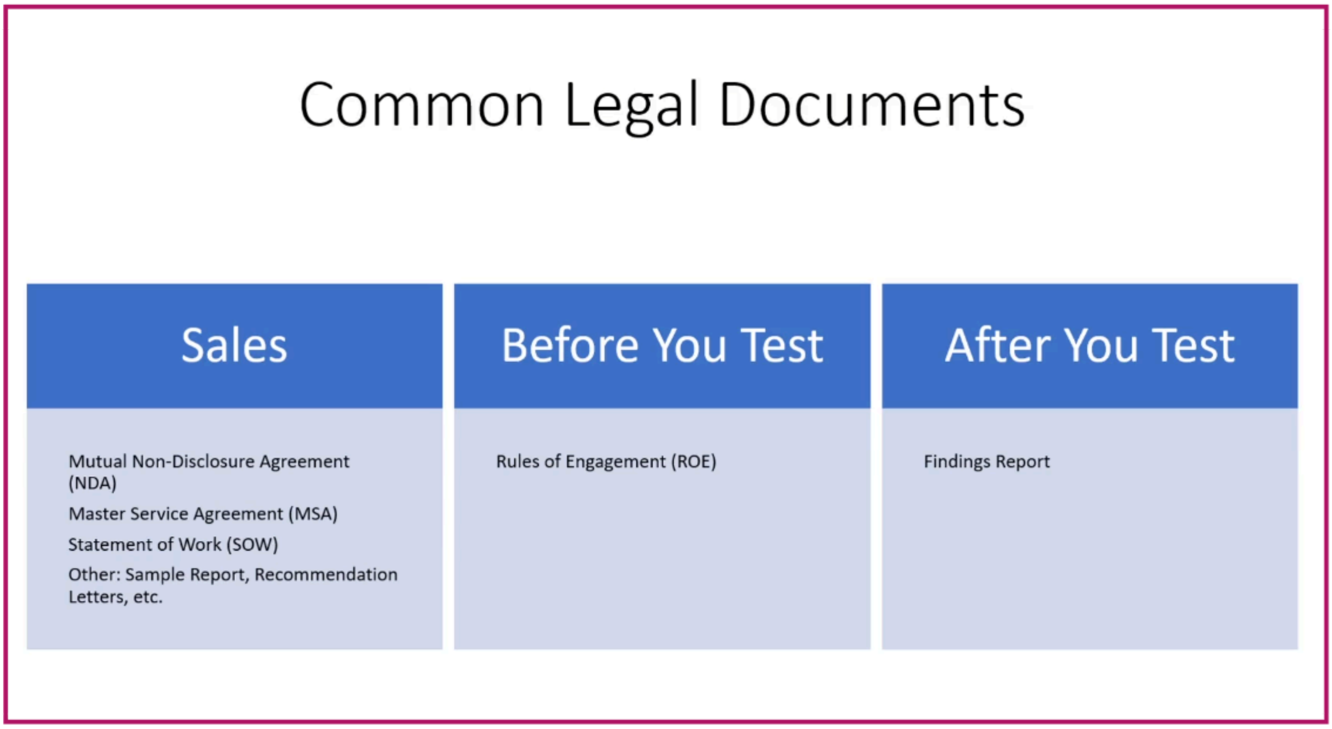
01 - Common Legal Documents



Common Legal Documents

Sales	Before You Test	After You Test
Mutual Non-Disclosure Agreement (NDA) Master Service Agreement (MSA) Statement of Work (SOW) Other: Sample Report, Recommendation Letters, etc.	Rules of Engagement (ROE)	Findings Report

These represents the documents in each phase of the process beginning from the sales of the assessment to after testing.

Mutual Non-Disclosure Agreement (NDA). Pretty obvious. This is a document saying we are prohibited to disclose any information regarding this company to competitors, or any other company that are not them.

When we talk about the scope of the assessment during the sales meeting with the client, we are going to put together 2 items: The Master Service Agreement (MSA), and the Statement of Work (SOW).

Master Service Agreement (MSA) : Contractual Document. This will "specify your performance objectives and kind of outline the responsibilities of both the parties." It is a blank agreement that covers multiple contracts, meaning we could be using the same for many contracts.

Statement of Work (SOW) : This is specific to a contract itself, a single contract. In here, we are going to talk about activities, deliverables, timelines, how much it is going to pay.

During the sales process, it is a good idea to have a sample report, and if we have recommendation letters take them as well.

Rules of Engagement (ROE) : This will cover specifics of our testing. Ex: we have 100 IP Addresses to test. In the ROE, we are going to have the exact IP Addresses we are to test, the actions we can perform, the domains we can attack. Usually, DOS is out of scope because if it is in a live environment (if what we are testing is in production), this would be bad for the business, and social engineering would not be done in an engagement with the Penetration Testing. It would be an assessment on its own assessment. **WE CANNOT START OUR PENETRATION TESTING BEFORE THIS DOCUMENT IS SIGNED**. (CYA - Cover Your Ass) (This is what you told me to test, here is what I am testing, and here is what I am allowed(or not allowed) to do).

Finally, the most important document as a Penetration Tester is going to be : The Findings Report.

Findings Report: This is going to detail what we found from a high level and a technical level.

We can find example of these on Google (Rapid7 has examples).