Username: Palm Beach State College IP Holder **Book:** Kali Linux – Assuring Security by Penetration Testing. No part of any chapter or book may be reproduced or transmitted in any form by any means without the prior written permission for reprints and excerpts from the publisher of the book or chapter. Redistribution or other use that violates the fair use privilege under U.S. copyright laws (see 17 USC107) or that otherwise violates these Terms of Service is strictly prohibited. Violators will be prosecuted to the full extent of U.S. Federal and Massachusetts laws.

Preparing the test plan

As the requirements have been gathered and verified by a client, it is time to draw a formal test plan that should reflect all of these requirements, in addition to other necessary information on the legal and commercial grounds of the testing process. The key variables involved in preparing a test plan are structured testing process, resource allocation, cost analysis, non-disclosure agreement, penetration testing contract, and rules of engagement. Each of these areas is addressed with their short descriptions as follows:

- **Structured testing process**: After analyzing the details provided by your customer, it may be important to restructure your testing methodology. For instance, if the social engineering service is about to be excluded, you would have to remove it from the formal testing process. Sometimes, this practice is known as **test process validation** . It is a repetitive task that has to be revisited whenever there is a change in client requirements. If there are any unnecessary steps involved during the test execution, it may result in a violation of the organization's policies and incur serious penalties. Additionally, based on the test type, there would be a number of changes to the test process. As an example, white box testing may not require the information gathering and target discovery phases, because the tester is already aware of the internal infrastructure.

  > **Tip**
  >
  > The validation of the network and environment data may be useful regardless of the test type. After all, the client may not know what their network really looks like!

- **Resource allocation**: Determining the expertise knowledge required to achieve the completeness of a test is one of the substantial areas. Thus, assigning an appropriately skilled penetration tester to a certain task may result in better security assessment. For instance, an application penetration testing requires a knowledgeable application security tester. This activity plays a significant role in the success of the penetration testing assignment.
- **Cost analysis**: The cost for penetration testing depends on several factors. This may involve the number of days allocated to fulfill the scope of a project, additional service requirements such as social engineering and physical security assessment, and the expertise knowledge required to assess the specific technology. From an industry viewpoint, this should combine a qualitative and quantitative value.
- **Non-disclosure Agreement (NDA)**: Before starting the test process, it is necessary to sign an NDA agreement that will reflect the interests of both parties: the client and penetration tester. Using such a mutual non-disclosure agreement should clear the terms and conditions under which the test should be aligned. The penetration tester should comply with these terms throughout the test process. Violating any single term of agreement can result in serious penalties or permanent exemption from the job.
- **Penetration testing contract**: There is always the need for a legal contract that will address the technical and business matters between the client and penetration tester. This is where the penetration testing contract comes in. The basic information in such contracts focuses on what testing services are being offered, their main objectives, how they will be conducted, payment declaration, and maintaining the confidentiality of the whole project. It is highly recommended that you have this document created by an attorney or legal counsel, as it will be used for most of your penetration testing activities.
- **Rules of engagement** (**ROE**): The process of penetration testing can be invasive and requires a clear understanding of the assessment's demands, support provided by the client, and type of potential impact or effect each assessment technique may have. Moreover, the tools used in the penetration testing processes should clearly state their purpose so that the tester can use them accordingly. The rules of engagement define all of these statements in a more detailed fashion to address the necessity of the technical criteria that should be followed during the test execution. You should never cross the boundaries set within the pre-agreed upon ROE.

By preparing each of these subparts of the test plan, you can ensure that you have a consistent view of the penetration testing process. This will provide a penetration tester with more specific assessment details that have been processed from the client requirements. It is always recommended that you prepare a test plan checklist, which can be used to verify the assessment criteria and its underlying terms with the contracting party. One of such exemplary types of checklist is discussed in the following section.

The test plan checklist

The following is an example of a set of questions that should be answered correctly before taking any further steps in the scope process:

- Are all the requirements promised during the RFP being met?
- Is the test scope defined clearly?
- Have all the testing entities been identified?
- Have all the non-testing entities been separately listed?
- Is there any specific testing process that will be followed?
- Is the testing process documented correctly?
- Will the deliverables be produced upon the completion of a test process?
- Has the entire target environment been researched and documented before?
- Have all the roles and responsibilities been assigned for the testing activities?

- Is there any third-party contractor to accomplish technology-specific assessment?
- Have any steps been taken to bring the project to a graceful closure?
- Has the disaster recovery plan been identified?
- Has the cost of the test project been finalized?
- Have the people who will approve the test plan been identified?
- Have the people who will accept the test results been identified?