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.

Chapter 3. Target Scoping

Target Scoping is defined as an empirical process to gather target assessment requirements and characterize each of its parameters in order to generate a test plan, its limitations, business objectives, and time schedule. This process plays an important role in defining clear objectives towards any kind of security assessment. By determining these key objectives, one can easily draw a practical road map of what will be tested, how it will be tested, what resources will be allocated, what limitations will be applied, what business objectives will be achieved, and how the test project will be planned and scheduled. Thus, we have combined all of these elements and presented them in a formalized **scope process** to achieve the required goal. The following are the key concepts that will be discussed in this chapter:

- **Gathering client requirements**: This deals with accumulating information about the target environment through verbal or written communication.
- **Preparing the test plan**: This depends on different sets of variables. These variables may include shaping the actual requirements into a structured testing process, legal agreements, cost analysis, and resource allocation.
- **Profiling test boundaries**: This determines the limitations associated with the penetration testing assignment. These can be a limitation of technology, knowledge, or a formal restriction on the client's IT environment.
- **Defining business objectives**: This is a process of aligning business views with the technical objectives of the penetration testing program.
- **Project management and scheduling**: This directs every other step of the penetration testing process with a proper timeline for test execution. This can be achieved using a number of advanced project management tools.

It is highly recommended that you follow the scope process in order to ensure test consistency and a greater probability of success. Additionally, this process can also be adjusted according to the given situation and test factors. Without any such process, there will be a greater chance of failure as the requirements gathered will have no proper definitions and procedures to follow. This can lead the entire penetration testing project into danger and may result in an unexpected business interruption. At this stage, paying special attention to the penetration testing process would make an excellent contribution towards the rest of the test phases and clear the perspectives of both technical and management areas. The key is to acquire as much information beforehand as possible from the client to formulate a strategic path that reflects the multiple aspects of penetration testing. These may include negotiable legal terms, contractual agreement, resource allocation, test limitations, core competencies, infrastructure information, timescales, and rules of engagement. As a part of best practices, the scope process addresses each of the attributes that are necessary to initiate our penetration testing project in a professional manner.

Each step constitutes unique information that is aligned in a logical order to pursue the test execution successfully. This also governs any legal matters to be resolved at an early stage. Hence, we will explain each of these steps in more detail in the following section. Keep in mind that it will be easier for both the client and penetration testing consultant to further understand the process of testing if all the information gathered is managed in an organized manner.

Gathering client requirements

This step provides a generic guideline that can be drawn in the form of a questionnaire to devise all the information about target infrastructure from a client. A client can be any subject who is legally and commercially bound to the target organization. Thus, for the success of the penetration testing project, it is critical to identify all internal and external stakeholders at an early stage of a project and analyze their levels of interest, expectations, importance, and influence. A strategy can then be developed to approach each stakeholder with their requirements and involvement in the penetration testing project in order to maximize positive influences and mitigate potential negative impacts.

> **Tip**
>
> It is solely the duty of the penetration tester to verify the identity of the contracting party before taking any further steps.

The basic purpose of gathering client requirements is to open a true and authentic channel by which the pentester can obtain any information that may be necessary for the testing process. Once the test requirements have been identified, the client should validate them in order to remove any misleading information. This will ensure that the developed test plan is consistent and complete.

Creating the customer requirements form

We have listed some of the commonly asked questions and considerations that may be used as a basis to create a conventional customer requirements form. It is important to note that this list can be extended or shortened according to the goal of a client.

- Collect basic information such as company name, address, website, contact person(s) details, e-mail address, and telephone number(s).
- Determine the key objectives behind the penetration testing project.
- Determine the penetration test type (with or without specific criteria):
  - Black box testing
  - White box testing
  - External testing
  - Internal testing

  - Social engineering included
  - Social engineering excluded
  - Investigate employee background information
  - Adopt employee's fake identity (legal council may be required)
  - Denial of service included
  - Denial of service excluded
  - Penetrate business partner systems

- How many servers, workstations, and network devices need to be tested?
- Which operating system technologies are supported by your infrastructure?
- Which network devices need to be tested? Firewalls, routers, switches, load balancers, IDS, IPS, or any other appliances?
- Are disaster recovery plans in place? If yes, whom should we contact?
- Are there any administrators currently managing your network?
- Is there any specific requirement to comply with industry standards? If yes, list them.
- Who will be the point of contact for this project?
- What is the timeline allocated for this project?
- What is your budget for this project?
- List any miscellaneous requirements, if necessary.

The deliverables assessment form

The following is an example of the type of items expected from a deliverables assessment form. This list is not holistic and items should be added or removed based on customer expectations and needs:

- What types of reports are expected?
  - Executive reports
  - Technical assessment reports
  - Developer reports
- In which format do you prefer the report to be delivered? PDF, HTML, or DOC.
- How should the report be submitted? Encrypted e-mail or printed?
- Who is responsible for receiving these reports?
  - Employee
  - Shareholder
  - Stakeholder

By using such a concise and comprehensive inquiry form, you can easily extract the customer requirements and fulfill the test plan accordingly.