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.

Summary

This chapter explains the target scoping aspect of penetration testing. If you are planning on performing professional penetration testing, this step should be high on your list of priorities. The main objective of this chapter is to provide a necessary guideline on formalizing the test requirements. For this purpose, a scope process has been introduced to highlight and describe each factor that builds a practical roadmap towards the test execution. The scope process comprises five independent elements, which are gathering client requirements, preparing test plan, profiling test boundaries, defining business objectives, and project management and scheduling. The aim of a scope process is to acquire and manage as much information as possible about the target environment, which can be useful throughout the penetration testing process. As discussed in the chapter, we have summarized each part of the scope processes in the following manner:

- Gathering client requirements provides a practical guideline on what information should be gathered from a client or customer in order to conduct the penetration testing successfully. Covering the data on the types of penetration testing, infrastructure information, organization profile, budget outlook, time allocation, and type of deliverables are some of the most important areas that should be cleared at this stage.
- Preparing a test plan combines structured testing process, resource allocation, cost analysis, non-disclosure agreement, penetration testing contract, and rules of engagement. All these branches constitute a step-by-step process to prepare a formal test plan that should reflect the actual client requirements, legal and commercial prospects, resource and cost data, and the rules of engagement. Additionally, we have also provided an exemplary type of checklist that can be used to ensure the integrity of a test plan.
- Profiling test boundaries provides a guideline on what type of limitations and restrictions may occur while justifying the client requirements. These can be in the form of technology limitations, knowledge limitations, or other infrastructure restrictions posed by the client to control the process of penetration testing. These test boundaries can be clearly identified from the client requirements. There are certain procedures that can be followed to overcome these limitations.
- Defining business objectives focuses on key benefits that a client may get from the penetration testing service. This section provides a set of general objectives structured according to the assessment criteria and the industry achievement.
- Project management and scheduling is a vital part of a scope process. Once all the requirements have been gathered and aligned according to the test plan, it's time to allocate proper resources and timescale for each identified task. By using some advanced project management tools, one can easily keep a track of all these tasks assigned to specific resources under the defined timeline. This can help increase the test productivity and efficiency.

In the next chapter, we will illustrate the practical reconnaissance process that contributes a key role in penetration testing. This includes probing the public resources, DNS servers, search engines, and other logical information on target infrastructure.