It is not necessary that an experienced penetration tester can write a good report, as writing report of penetration testing is an art that needs to be learnt separately.

What is Report Writing?

In penetration testing, report writing is a comprehensive task that includes methodology, procedures, proper explanation of report content and design, detailed example of testing report, and tester’s personal experience. Once the report is prepared, it is shared among the senior management staff and technical team of target organizations. If any such kind of need arises in future, this report is used as the reference.

Report Writing Stages

Due to the comprehensive writing work involved, penetration report writing is classified into the following stages −

* Report Planning
* Information Collection
* Writing the First Draft
* Review and Finalization



Report Planning

Report planning starts with the objectives, which help readers to understand the main points of the penetration testing. This part describes why the testing is conducted, what are the benefits of pen testing, etc. Secondly, report planning also includes the time taken for the testing.

Major elements of report writing are −

* **Objectives** − It describes the overall purpose and benefits of pen testing.
* **Time** − Inclusion of time is very important, as it gives the accurate status of the system. Suppose, if anything wrong happens later, this report will save the tester, as the report will illustrate the risks and vulnerabilities in the penetration testing scope during the specific period of time.
* **Target Audience** − Pen testing report also needs to include target audience, such as information security manager, information technology manager, chief information security officer, and technical team.
* **Report Classification** − Since, it is highly confidential which carry server IP addresses, application information, vulnerability, threats, it needs to be classified properly. However, this classification needs to be done on the basis of target organization which has an information classification policy.
* **Report Distribution** − Number of copies and report distribution should be mentioned in the scope of work. It also needs to mention that the hardcopies can be controlled by printing a limited number of copies attached with its number and the receiver’s name.

Information Collection

Because of the complicated and lengthy processes, pen tester is required to mention every step to make sure that he collected all the information in all the stages of testing. Along with the methods, he also needs to mention about the systems and tools, scanning results, vulnerability assessments, details of his findings, etc.

Writing the First Draft

Once, the tester is ready with all tools and information, now he needs to start the first draft. Primarily, he needs to write the first draft in the details – mentioning everything i.e. all activities, processes, and experiences.

Review and Finalization

Once the report is drafted, it has to be reviewed first by the drafter himself and then by his seniors or colleagues who may have assisted him. While reviewing, reviewer is expected to check every detail of the report and find any flaw that needs to be corrected.

Content of Penetration Testing Report

Following is the typical content of a penetration testing report −

|  |
| --- |
| Executive Summary   * Scope of work * Project objectives * Assumption * Timeline * Summary of findings * Summary of recommendation   Methodology |