
Types of reports

After gathering every single piece of your verified test results, they must be combined into a systematic and structured report before submitting to the target stakeholder. There are three different types of reports; each has its own schema and layout relevant to the interests of a business entity involved in the penetration testing project. The types of reports are as follows:

- Executive report
- Management report
- Technical report

These reports are prepared according to the level of understanding and ability to grasp the information conveyed by the penetration tester. We have detailed each report type and its reporting structure with basic elements that may be necessary to accomplish your goal. It is important to note that all of these reports should abide by non-disclosure policy, legal notice, and penetration testing agreement before being handed to the stakeholders.

The executive report

The executive report, a type of assessment report, is shorter and more concise to point the high-level view of the penetration testing output from a business strategy perspective. The report is prepared for C level executives within a target organization (CEO, CTO, CIO, and so on). It must be populated with some basic elements as follows:

- **Project objective**: This section defines the mutually agreed criteria for the penetration testing project between you and your client.
- **Vulnerability risk classification**: This section explains the risk levels (critical, high, medium, low, and informational) used in the report. These levels should clearly differentiate and highlight the technical security exposure in terms of severity.
- **Executive summary**: This section briefly describes the purpose and goal of the penetration testing assignment under the defined methodology. It also highlights the number of vulnerabilities discovered and exploited successfully.
- **Statistics**: This section details the vulnerabilities discovered in the target network infrastructure. These can also be drawn in the form of a pie chart or in any other intuitive format.
- **Risk matrix**: This section quantifies and categorizes all the discovered vulnerabilities, identifies the resources potentially affected, and lists the discoveries, references, and recommendations in a shorthand format.

It is always an idealistic approach to be creative and expressive while preparing an executive report and to keep in mind that you are not required to reflect upon the technical grounds of your assessment results, but rather give factual information processed from those results. The overall size of the report should be two to four pages.

The management report

The management report is generally designed to cover the issues including regulatory and compliance measurement in terms of target security posture. Practically, it should extend the executive report with a number of sections that may interest the **Human Resource** (**HR**) and other management people, and assist in their legal proceedings. Following are the key parts that may provide you with valuable grounds for the creation of such a report:

- **Compliance achievement**: This initiates a list of known standards and maps each of its sections or subsections with the current security disposition. It should highlight any regulatory violations that occurred, which might inadvertently expose the target infrastructure and pose serious threats.
- **Testing methodology**: This should be described briefly and should contain enough details that may help the management people to understand the penetration testing lifecycle.
- **Assumptions and limitations**: This highlights the known factors that may have prevented the penetration tester from reaching a particular objective.
- **Change management**: This is sometimes considered a part of the remediation process; however, it is mainly targeted towards the strategic methods and procedures that handle all the changes in a controlled IT environment. The suggestions and recommendations that evolve from security assessment should remain consistent with a change in the procedures, in order to minimize the impact of an unexpected event upon the service.
- **Configuration management**: This focuses on the consistency of the functional operation and performance of a system. In the context of system security, it follows any change that may have been introduced to the target environment (hardware, software, physical attributes, and others). These configuration changes should be monitored and controlled to maintain the system configuration state.

As a responsible and knowledgeable penetration tester, it is your duty to clarify any management terms before you proceed with the penetration testing lifecycle. This exercise definitely involves one-to-one conversations and agreements on target-specific assessment criteria, such as what kind of compliance or standard frameworks have to be evaluated, are there any restrictions while following a particular test path, will the changes suggested be sustainable in a target environment, or will the current system state be affected if any configuration changes are introduced. These factors all jointly establish a management view of the current security state in a target environment, and provide suggestions and recommendations following the technical security assessment.

The technical report

The technical assessment report plays a very important role in addressing the security issues raised during the penetration testing engagement. This type of report is generally developed for techies who want to understand the core security features handled by the target system. The report will detail the vulnerabilities, how they can be exploited, what business impact they could bring, and how resistant solutions can be developed to thwart any known threats. It has to communicate with all-in-one secure guidelines for protecting the network infrastructure. So far, we have already discussed the basic elements of the executive and management reports. In the technical report, we extend these elements and include some special themes that may draw substantial interests for the technical team at the target organization. Sometimes, sections such as project objectives, vulnerability risk classification, risk matrix, statistics, testing methodology, and assumptions and limitations are also a part of the technical report. The technical report consists of the following sections:

- **Security issues**: The security issues raised during the penetration testing process should be clearly cited in detail, such that for each applied attack method, you must mention the list of affected resources, its implications, original request and response data, simulated attack request and response data, provide reference to external sources for the remediation team, and give professional recommendations to fix the discovered vulnerabilities in the target IT environment.
- **Vulnerabilities map**: This provides a list of discovered vulnerabilities found in the target infrastructure, each of which should be easily matched to the resource identifier (for example, the IP address and target name).
- **Exploits map**: This provides a list of the successfully checked and verified exploits that worked against the target. It is also crucial to mention whether the exploit was private or public. It may be beneficial to detail the source of the exploit code and for how long it has been available.
- **Best practices**: This emphasizes the better design, implementation, and operational security procedures the target may lack. For instance, in a large enterprise environment, deploying an edge-level security could be advantageous to reduce the number of threats before they make their way into a corporate network. Such solutions are very handy and do not require technical engagement with production systems or legacy code.

Generally speaking, the technical report brings forward the ground realities to the associative members of the organization concerned. This report plays a significant role in the risk management process and will likely be used to create actionable remediation tasks.