
Network penetration testing report (sample contents)

Just as there are different types of penetration testing, there are different types of report structures. We have presented a generic version of a network-based penetration testing report that can be extended to utilize almost any other type (for example, web application, firewall, wireless networks, and so on). In addition to the following table of contents, you would also want a cover page which states the testing company's name, type of report, scan date, author name, document revision number, and a short copyright and confidential statement.

The following would be the table of contents for a network-based penetration testing report:

- Legal notice
- Penetration testing agreement
- Introduction
- Project objective
- Assumptions and imitations
- Vulnerability risk scale
- Executive summary
- Risk matrix
- Testing methodology
- Security threats
- Recommendations
- Vulnerabilities map
- Exploits map
- Compliance assessment
- Change management
- Best practices
- Annexes

As you can see, we have combined all types of reports into one single complete report with a definitive structure. Each of these sections can have its own relevant subsections that can better categorize the test results in a greater detail. For instance, the annexes section can be used to list the technical details and analysis of a test process, logs of activities, raw data from various security tools, details of the research conducted, references to the Internet sources, and glossary. Depending on the type of report being requested by your client, it is solely your duty to understand the importance and value of your position before beginning a penetration test.