
Summary

In this chapter, we have explored some basic steps necessary to create a penetration testing report and discussed the core aspects of doing a presentation in front of the client. At first, we fully explained the methods of documenting your results from individual tools and suggested not to rely on single tools for your final results. As such, your experience and knowledge counts in verifying the test results before being documented. Make sure to keep your skills updated and sufficient to manually verify the findings when needed. Afterwards, we shed light on creating different types of reports with their documentation structures. These reports mainly focus on executive, managerial, and technical aspects of a security audit we carried out for our client. Additionally, we also provided a sample table of contents for a network-based penetration testing report to give you a basic idea for writing your own report. Thereafter, we discussed the value of live presentation and simulations to prove your findings, and how you should understand and convince your audiences from different backgrounds.

Finally, we have provided a generic list of the post testing procedures that can be a part of your remediation measures or recommendations to your client. This section provides a clear view of how you assist the target organization in the remediation process, being an advisor to their technical team or remediate yourself.