
Summary

In this chapter, we discussed the process of identifying and analyzing the critical security vulnerabilities based on the selection of tools from Kali Linux. We also mentioned three main classes of vulnerabilities—design, implementation, and operational—and discussed how they could fall into two generic types of vulnerabilities: local and remote. Afterwards, we discussed several vulnerability taxonomies that could be followed by the security auditor to categorize the security flaws according to their unifying commonality pattern. In order to carry out a vulnerability assessment, we have presented you with a number of tools that combine the automated and manual inspection techniques. These tools are divided according to their specialized technology audit category, such as OpenVAS (an all-in-one assessment tool), Cisco, Fuzzy testing, SMB, SNMP, and web application security assessment tools.

In the next chapter, we will discuss the art of deception and explain various ways to exploit human vulnerabilities in order to acquire the target. Although this process is sometimes optional, it is considered vital when there is a lack of information to exploit the target infrastructure.