
Summary

In this chapter, we pointed out several key areas necessary for the process of target exploitation. At the beginning, we provided an overview of vulnerability research that highlights the requirement for a penetration tester to hold necessary knowledge and skills, which in turn become effective for vulnerability assessment. Afterwards, we presented a list of online repositories from where you can reach a number of publicly disclosed vulnerabilities and exploit codes. In the final section, we demonstrated the practical use of an advanced exploitation toolkit named the Metasploit framework. The exercises provided are purely designed to explore and understand the target acquisition process through tactical exploitation methods. Additionally, we have also interpreted the insights of exploit development by analyzing each step of the sample exploit code from a framework to help you understand the basic skeleton and construction strategy.

In the next chapter, we will discuss the process of privilege escalation using various tools and techniques and how it is beneficial once the target is acquired.