---

# Summary

This chapter introduced you to the amazing world of Kali Linux, which is a Live DVD Linux distribution that has been specially developed to help you in the penetration testing process. Kali is the successor of BackTrack, a famous Linux distribution focused on the purpose of penetration testing.

The chapter started with a brief description of Kali Linux's history. Next, it moved on to see what functionalities Kali Linux has to offer. The latest version of Kali Linux has many tools to help in penetration testing. Additionally, it also has tools for digital forensics, wireless, reverse engineering, and hardware hacking tasks.

The discussion continues on how to get Kali Linux and the several ways to install it. Kali Linux can be used as a Live DVD without installing it to the hard disk. It can be installed to the hard disk and can also be used as a portable distribution by installing it to a USB flash disk.

Before Kali Linux can be used properly in penetration testing, it needs to be configured for the network connection, using either a wired or wireless connection. We also discussed how to use several features in the VirtualBox machine to make it easier to work with the virtual machine; for example, installing additional tools, configuring shared folders, exporting the virtual machine for a backup purpose or to share it with other people, and taking a snapshot to back up the virtual machine temporarily.

As with any other software, Kali Linux also needs to be updated, whether we only update the software applications or the Linux kernel included in the distribution.

You may need to test your penetration testing skills; unfortunately, you don't have permission to do this to other servers as it is considered illegal in several countries. To help you with this, there are several intentionally vulnerable systems that can be installed and used on your own machine. In this chapter, we looked into Metasploitable 2 from Rapid7.

We also discussed several network services included with the latest Kali Linux, such as HTTP, MySQL, and SSH. We started by giving you a brief introduction to each service and then we continue with how to manage the service; for example, how to start or stop the service.

At the end of the chapter, we looked at installing additional information security tools that are not included in the latest Kali Linux version by default, such as the Nessus network scanner and Cisco password cracker.

In the next chapter, we will introduce you to several penetration testing methodologies.