
Summary

In this chapter, we discussed the target discovery process. We started by discussing the purpose of target discovery: identifying the target machine and finding out the operating system used by the target machine. Then, we continued with the tools included with Kali Linux that can be used for identifying target machines.

We discussed the following tools: `ping`, `arping`, `fping`, `hping3`, `nping`, and `nbtscan`. We also discussed several tools specially developed to be used in an IPv6 environment, such as `alive6`, `detect-new-ip6`, and `passive_discovery6`.

At the end of this chapter, you learned about the tools that can be used to do OS fingerprinting: `p0f`, and briefly about the `nmap` capabilities for doing active operating system fingerprinting.

In the next chapter, we will talk about target enumeration and describe the tools included in Kali Linux that can be used for this purpose.