
Chapter 5. Target Discovery

In this chapter, we will describe the process of discovering machines on the target network using various tools available in Kali Linux. We will explain the following topics:

- A description of the target discovery process
- The method used to identify target machines using the tools in Kali Linux
- The steps required to find the operating systems of the target machines (operating system fingerprinting)

To help you understand these concepts easily, we will use a virtual network as the target network.

Starting off with target discovery

After we have gathered information about our target network from third-party sources, such as search engines, the next step would be to discover our target machines. The purpose of this process is as follows:

- To find out which machine in the target network is available. If the target machine is not available, we won't continue the penetration testing process on that machine and move to the next machine.
- To find the underlying operating system used by the target machine.

Collecting the previously mentioned information will help us during the vulnerabilities mapping process.

We can utilize the tools provided in Kali Linux for the target discovery process. Most of these tools are available in the **Information Gathering** menu, with the following submenus:

- **Identify Live Hosts**
- **OS Fingerprinting**

In this chapter, we will only describe a few important tools in each category. The tools are selected based on the functionality, popularity, and the tool development activity.