Summary

This chapter introduced you to the information gathering phase. It is usually the first phase that is done during the penetration testing process. In this phase, you collect as much information as you can about the target organization. By knowing the target organization, it will be easier when we want to attack the target. There is a Chinese proverb which says:

> *Know yourself, know your enemy, and you shall win a hundred battles without loss.*

This saying can't be more true than in penetration testing.

We described several tools included in Kali Linux that can be used for information gathering. We started by listing several public websites that can be used to gather information about the target organization. Next, we described how to use tools to collect domain registration information. Then, we described tools that can be used to get DNS information. Later on, we explored tools for collecting routing information. In the final part of the chapter, we described tools that utilize search engine capabilities.

In the next chapter, we will discuss how to discover a target.