Summary

In this chapter, we discussed the operating system backdoors such as cymothoa, intersect, and metsvc, which can be used to maintain access on target machines.

Next, we discussed protocol tunneling tools that can wrap one network protocol to another. The goal of this protocol tunneling is to bypass any mechanism enacted by the target machine to limit our capability to connect to the outside world. The tools in this category are dns2tcp, iodine, ncat, proxychains, ptunnel, socat, sslh, and stunnel4.

At the end of this chapter, we briefly described the web backdoor tools. These tools can be used to generate a webshell backdoor on the target machine, and we can then connect to this backdoor.

In the next chapter, we will discuss documenting, reporting, and presenting the vulnerabilities found to the relevant parties.