
Summary

In this chapter, we discussed how to escalate our privilege using a local privilege escalation exploit, doing password attacks, and how to do network sniffing and spoofing. The purpose of the tools mentioned in this chapter is to get elevated privileges. Sniffing and spoofing can also be used to leverage access into a broader area or to gain access into another machine within the network or outside the network, which probably contains more valuable information.

We started with a local privilege escalation exploit. After exploiting a service on the target machine, we found that we only have a low-level privilege and the next step to be taken is to escalate our privilege to a `root` privilege. One of the techniques that can be used is by exploiting a local vulnerability such as kernel vulnerability.

In the next section, we discussed how to attack passwords. There are two methods that can be used: offline attack and online attack. Most of the tools in an offline attack utilize rainbow tables to speed up the attack process, but it needs large hard disk space. An offline attack has advantage that it can be done at your own pace without triggering the account lockout. In an online attack, you need to be careful about the account being locked out.

We then discussed several tools that can be used to spoof the network traffic. In the last part of this chapter, we looked at several tools that can be used to sniff the network traffic. If you don't use encryption, all of your network data can be seen by these tools. While the sniffer is a passive tool, spoofer is an active tool because it sends something to your network.

In the next chapter, we will discuss how to maintain the access we have attained.