第 12 章　安全领域的数据包分析

虽然本书主要集中于如何使用数据包分析技术解决网络故障，但在现实世界中，很多数据包分析工作都是为了解决安全问题。当入侵分析师检查来自可疑入侵者的网络流量，或取证人员调查恶意软件在主机上的感染程度时，就会用到数据包分析的方法。面向安全的数据包分析是一个很大的话题，都可以另写一本书了，本章只是带你尝尝鲜。

在本章，我们将扮演一位安全从业者，学习在网络层分析「肉鸡」[1]系统的各个方面。我们将涉及网络侦察、恶意的流量重定向，以及系统漏洞利用。接着，我们将扮演一位入侵分析师，剖析来自入侵检测系统的警报流量。即使你不是安全从业者，通过阅读本章，你也可以获得一些对网络安全的关键洞察。