第15章作业参考解答

1、有了防火墙，为什么还需要入侵检测？

答：

主要是因为网络防火墙技术有一些不足之处，包括：第一，入侵者可寻找防火墙背后可能敞开的后门；第二，不能阻止内部攻击；第三，通常不能提供实时的入侵检测能力；第四，不能主动跟踪入侵者；第五，不能对病毒进行有效防护。所以需要入侵检测系统作为防火墙的有效补充，共同构建网络安全保障体系，这种补充主要表现在以下几个方面：

1）入侵检测可以发现内部的攻击事件以及合法用户的越权访问行为，而位于网络边界的防火墙对于这些类型的攻击活动无能为力。

2）如果防火墙开放的网络服务存在安全漏洞，入侵检测系统可以在网络攻击发生时及时发现并进行告警。

3）在防火墙配置不完善的条件下，攻击者可能利用配置漏洞穿越防火墙，入侵检测系统能够发现此类攻击行为。

4）对于加密的网络通信，防火墙无法检测，但是监视主机活动的入侵检测系统能够发现入侵。

5）入侵检测系统能够有效发现入侵企图。如果防火墙允许外网访问某台主机，当攻击者利用扫描工具对主机实施扫描时，防火墙会直接放行，但是入侵检测系统能够识别此类网络异常并进行告警。

6）入侵检测系统可以提供丰富的审计信息，详细记录网络攻击过程，帮助管理员发现网络中的脆弱点。

2、与入侵检测相比，网络欺骗防御技术有什么优势？

答：与传统入侵检测相比，网络欺骗防御检测入侵的主动性更强，采用欺骗技术来迷惑、引诱攻击者进行攻击，同时对攻击者的行为进行严密的监视和控制，因而更能准确地检测一些未知攻击、高水平攻击，并了解攻击的细节，部分解决了传统入侵检测系统的误报和漏报问题，同时还具有防御攻击的能力。

3、比较分析特征检测与异常检测方法的优缺点。

答：特征检测方法的基本思路是事先提取出描述各类攻击活动的特征信息，利用攻击特征对指定的数据内容进行监视，一旦发现攻击特征在监视的数据中出现，即判定系统内发生了相应的攻击活动。

异常检测方法首先总结出正常活动的特征，建立相应的行为模式。在入侵检测的过程中，以正常的行为模式为基础进行判定，将当前活动与代表正常的行为模式进行比较，如果当前活动与正常行为模式匹配，则认为活动正常；而如果两者存在显著偏差，则判定出现了攻击。

特征检测方法只能检测已知攻击，误报率低，无法检测未知攻击，而异常检测方法可以检测未知攻击，但误报率高。