信息安全作业 10

190110429-何为

1. 误用检测和异常检测有什么区别?

答:

（1） 概念:

误用检测是事先定义出已知的入侵行为的入侵特征，将实际环境中的数据与之匹配，根据匹配程度来判断是否发生了入侵攻击行为。

异常检测是根据使用者的行为或资源使用状况的程度与正常状态下的标准特征(活动轮廓）之间的偏差来判断是否遭到入侵。如果偏差高于阈值，则发生异常。

（2） 主要缺陷:

误用检测检测范围受已有知识的局限，无法检测未知的攻击类型；其次，将具体入侵手段抽象成知识具有一定困难，而且建立的入侵特征库需要不断更新维护。

对异常检测的 IDS 来说，得到正常行为或状态的标准特征以及确定阈值具有较大的难度。

（3） 特点:

基于误用检测的 IDS 检测准确率很高。

异常检测不依赖于某个具体行为是否出现，通用性较强。但基于异常检测的 IDS 往往漏报率低，但误报率高。

2. 什么是 CIDF 模型，包含哪些内容?

答:

CIDF 是一个入侵检测系统的通用模型。包括以下组件：事件产生器，用 E 盒表示；事件分析器，用 A 盒表示；响应单元，用 R 盒表示；事件数据库，用 D 盒表示。工作流程为 E 盒通过传感器收集事件数据，并将信息传送给 A 盒和 D 盒；A 盒检测误用模式；D 盒存储来自 A、E 盒的数据，并为额外的分析提供信息；R 盒从 A、E 盒中提取数据，D 盒启动适当的响应。

3. 有人说，“防火墙的包过滤技术发展到应用层，就可以取代入侵检测系统。”你认为正确与否，为什么?

答:

错误。

传统的防火墙主要是包过滤防火墙，实现的是网络层控制 ——截获网络中的数据包，根据协议进行解析，最后利用包头的关键字段和预设的过滤规则做对比，决定是否转发该数据包。随着应用层各种应用的丰富，越来越多的应用层协议出现，黑客可以直接在应用层发起攻击。防火墙的包过滤技术发展到应用层可以一定程度上发挥入侵检测系统的作用，但不能替代。

入侵检测系统是一种对网络传输进行即时监视，在发现可疑传输时发出警报或者采取主动反应措施的网络安全系统。一般认为，防火墙属于静态防范措施，而入侵检测系统为动态防范措施，是对防火墙的有效补充。在信息收集、信息分析、结果处理方面发挥了巨大的作用，是不能被其替代的。