第七讲 入侵检测技术

测试点 7-1

1. 入侵检测如何分类？

① 按数据检测方法

异常检测模型（Anomaly Detection）：首先总结正常操作应该具有的特征（用户轮廓），当用户活动与正常行为有重大偏离时即被认为是入侵

误用检测模型（Misuse Detection)：收集非正常操作的行为特征，建立相关的特征库，当监测的用户或系统行为与库中的记录相匹配时，系统就认为这种行为是入侵

② 按系统结构

集中式：系统的各个模块包括数据的收集分析集中在一台主机上运行

分布式：系统的各个模块分布在不同的计算机和设备上

③ 按时效性

离线入侵检测系统（off-line IDS）：将一段时间内的数据存储起来，然后定时发给数据处理单元进行分析，如果在这段时间内有攻击发生就报警。

在线入侵检测系统（On-line IDS）：对采集到的状态数据进行实时分析和攻击预警，大多数 IDS 所采用的办法，由于计算机硬件速度的提高，使得对攻击的实时检测和响应成为可能。

④ 按数据来源

基于主机的入侵检测系统（HIDS）:运行于被检测的主机之上，通过查询、监听当前系统的各种资源的使用运行状态，发现系统资源被非法使用和修改的事件，进行上报和处理。

基于网络的入侵检测系统（NIDS）：通过在共享网段上对通信数据的侦听采集数据，分析可疑现象。这类系统不需要主机提供严格的审计，对主机资源消耗少，并可以提供对网络通用的保护而无需顾及异构主机的不同架构。

混合型入侵检测系统（Hybrid IDS）：

网络节点入侵检测系统（NNIDS）

文件完整性检测系统

2. 入侵检测系统的主要技术指标有哪些？

① 误报（率）：检测系统在检测时把系统的正常行为判为入侵行为的错误被称为误报。检测系统在检测过程中出现误报的概率称为系统的误报率。

② 漏报（率）：检测系统在检测时把某些入侵行为判为正常行为的错误现象称为漏报。检测系统在检测过程中出现漏警的概率称为系统的漏报率。

③ 其他的还包括处理性能、完备性、容错性、及时性及体系架构等参考指标。

3. 常用的未知攻击检测方法有哪些？

基于异常的检测：

① 统计分析：记录的具体操作包括：CPU 的使用，I/O 的使用，使用地点及时间，邮件使用，编辑器使用，编译器使用，所创建、删除、访问或改变的目录及文件，网络上活动等。

② 数据挖掘 :数据挖掘是指从大量实体数据抽象出模型的处理 ;目的是要从海量数据中提取对用户有用的数据；这些模型经常在数据中发现对其它检测方式不是很明显的异常。