1. 入侵检测系统IDS—基本信息

\*入侵检测的基本概念：是对入侵行为的发觉，是指通过对计算机网络或计算机系统中的若干关键点收集信息并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。

\*基本功能：引入入侵检测系统（IDS），IDS可以获取流经内部网络中和非军事区中的关键链路的信息，能够对这些信息进行检测，发现包含在这些信息中与实施上述攻击过程有关的有害信息，并予以反制。

\*系统的组成：进行入侵检测的软件与硬件的组合便是入侵检测系统。

\*引入原因：

（1）入侵很容易

（2）防火墙不能保证绝对的安全

\*两种应用方式：

（1）在线方式

（2）杂凑方式



\*评价指标：（1）正确性（2）全面性（3）性能

\*分类：

1. 按照数据来源分：

A.基于主机的入侵检测（HIDS）—检测进入主机的信息流。

B.基于网络的入侵检测(NIDS）—检测流经关键网段的信息流。

C.混合型IDS—同时使用基于主机的IDS和基于网络的IDS。（优势互补）

（2）按照分析方法分:

A.误用(Misuse)入侵检测—首先总结正常操作应该具有的特征，当用户活动与正常行为有重大偏离时即被认为是入侵。

B.异常(Anomaly)入侵检测—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。

1. 入侵检测系统IDS—工作原理（流程）

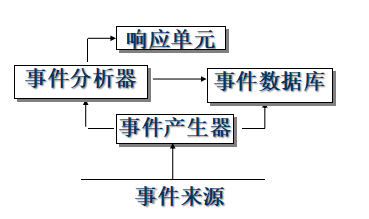
\*概念：

（1）事件产生器

（2）事件分析器

（3）相应单元

（4）事件数据库



\*具体过程：

（1）捕获信息

（2）检测异常信息

（3）反制异常信息

（4）报警

（5）登记与分析

3.入侵检测系统IDS—分类

\*按照数据来源分：

（1）基于主机的入侵检测（HIDS）—检测进入主机的信息流。

（2）基于网络的入侵检测(NIDS）—检测流经关键网段的信息流。

（3）混合型IDS—同时使用基于主机的IDS和基于网络的IDS。（优势互补）

\*按照分析方法分:

（1）误用(Misuse)入侵检测—首先总结正常操作应该具有的特征，当用户活动与正常行为有重大偏离时即被认为是入侵。

（2）异常(Anomaly)入侵检测—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。