HW5

- 作业
  1. IDS有哪些主要功能?
  2. 简述误用检测和异常检测。
  3. 简述snort的5个组成部分及其作用。
  4. 简述网络安全态势感知系统。

T1

- 网络流量的跟踪与分析功能：跟踪用户进出网络的所有活动，实时检测并分析用户在系统中的活动状态；实时统计网络流量，检测拒绝服务攻击等异常行为
- 已知攻击特征的识别功能：识别特定类型的攻击，并向控制台报警，为网络防护提供依据；根据定制的条件过滤重复告警事件，减轻传输与响应的压力
- 异常行为的分析、统计与响应功能：分析系统的异常行为模式，统计异常行为，并对异常行为做出响应
- 特征库的在线和离线升级功能：提供入侵检测规则的在线和离线升级，实时更新入侵特征库，不断提高 IDS 的入侵检测能力
- 数据文件的完整性检查功能：检查关键数据文件的完整性，识别并报告数据文件的改动情况
- 自定义的响应功能：定制实时响应策略；根据用户定义，经过系统过滤，对告警事件及时响应
- 系统漏洞的预报警功能：对新发现或新公布的系统漏洞特征进行预报警

- IDS 探测器集中管理功能：通过控制台收集探测器的状态和告警信息，控制各个探测器的行为

T2

- 误用检测：又称基于知识或特征的检测技术。工作原理是假定所有入侵行为和手段（及其变种）都能够表达为模式或特征（签名），对已知的入侵行为和手段进行分析，提取入侵特征，构建攻击模式或攻击签名，通过系统当前状态与攻击模式或攻击签名的匹配判断入侵行为。它是最成熟、应用最广泛的技术，优点是可以准确地检测已知的入侵行为，缺点是不能检测未知的入侵行为，关键在于如何表达入侵行为，即构建攻击模型以区分真正的入侵与正常行为
- 异常检测：又称基于行为的入侵检测技术，用于检测系统（主机或网络）中的异常行为。基本设想是入侵行为与正常的（合法的）活动有明显差异。工作原理为首先收集一段时间系统活动的历史数据，建立代表主机、用户或网络连接的正常行为描述，然后收集事件数据并使用不同方法判断所检测到的事件活动是否偏离正常行为模式，进而判断是否发生入侵

T3

1. 解码器：通过 libpcap 获得网络数据包后，数据会经过一系列解码器。首先填写链路级协议的包结构，然后解码为后续处理所需的信息，并将获取的信息送往预处理器，同时支持多种类型的网络接口
2. 预处理器：数据包会依次发送到注册过的一组预处理器，每个预处理器会检查数据包并决定是否查看。Snort 包含多种预处理器，分别实现不同功能，用户也可设计自定义预处理器以扩展入侵检测功能
3. 检测引擎：是 Snort 工作在入侵检测模式下的核心部分，采用基于规则匹配（误用检测）的方式检测每个数据包，一旦发现数据包特征符合某个规则定义，就会触发相应的处理操作

4. 输出插件：用于格式化警报信息，方便管理员根据公司环境配置易于理解、使用和查看的报警和日志方法，支持多种格式，能以更灵活的格式和表现形式向管理员呈现报警及日志信息
5. 日志 / 警报子系统：规则中定义了数据包的处理方式，其中 alter 和 log 操作由该子系统完成。日志子系统将解码得到的信息以 ASCII 码格式、tcpdump 等格式记录下来；警报子系统将报警信息发送到 syslog、socket 或数据库中

T4

网络安全态势感知系统:

可以看成是基于分布式入侵检测系统的综合安全监控系统，具有入侵检测、安全状态可视化展示、安全状态理解及趋势分析预测，以及网络监视和网络控制等功能，能更全面地掌握网络安全状况，为网络安全防护提供更有力的支持