Homework4

吴承泽 SA23011083

Chapter6

1、IDS有哪些主要功能?

1. **信息收集**：IDS所收集的信息包括用户(合法用户和非法用户)在网络、系统、数据库及应用程序活动的状态和行为。
2. **信息分析**：对收集到的网络、系统、数据及用户活动的状态和行为信息等进行模式匹配、统计分析和完整性分析，得到实时检测所必需的信息。
3. **安全响应**：IDS在发现入侵行为后必然及时做出响应，包括终止网络服务、记录事件日志、报警和阻断等。

2、简述误用检测和异常检测。

误用检测：

误用检测技术又称基于知识或特征的检测技术。它假定所有入侵行为和手段(及其变种)都能够表达为一种模式或特征，并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。误用检测是最成熟、应用最广泛的技术。误用检测技术的优点在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。误用检测的关键在于如何表达入侵行为，即攻击模型的构建，把真正的入侵与正常行为区分开来。

异常检测：

异常检测技术又称为基于行为的入侵检测技术，用来检测系统（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)活动有明显的差异，即正常行为与异常行为有明显的差异。异常检测的工作原理是：首先收集一段时间系统活动的历史数据，再建立代表主机、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一些不同的方法来决定所检测到的事件活动是否偏离了正常行为模式，从而判断是否发生了入侵。

3、总结NIDS的脆弱性。

1. **检测的工作量很大**：NIDS需要高效的检测方法和大量的系统资源，NIDS的检测是资源密集型的，这在某种程度上使NIDS更加容易遭受DoS攻击。
2. **检测方法的局限性**：复杂的、智能化方法的作用十分有限，而AD方法(异常检测方法)受限于某些资源的请求使用在数据传输过程中的模糊性与隐含性，也难以在NIDS中发挥另人满意的功效。因此，特征匹配(MD，误用检测方法)成为NIDS分析引擎的一个不可或缺的功能模块。特征匹配作为一种轻量级的检测方法有其固有的缺陷，缺乏弹性（尤其是字符串匹配），如何完备定义匹配特征（也即匹配特征库的完备性）是决定检测性能的一个关键问题。特征匹配是脆弱的，这种脆弱性是固有的、可以在某个时间降低却不可以根除。事实上，目前很多Anti-NIDS技术都是针对特征匹配脆弱性的。
3. **网络协议的多样性与复杂性**：TCP/IP协议族本身十分庞杂，各种协议不下几十种，呈现横向跨越和纵向深入的两维分布。为了适应网络检测的需要，NIDS须对其中的大部分协议进行模拟分析检测工作，这会使得分析引擎变得臃肿而效率低下。更为重要的是部分协议（如IP协议、TCP协议等）非常复杂，使精确地模拟分析十分困难，其难度随着协议层次的上升而增加。到了应用层，这种模拟分析工作几乎无法继续。由于缺少主机信息，NIDS将难于理解应用层的意图，更无法模拟或理解某些应用提供的功能(如bash提供的tab键命令补齐功能、用箭头获得上一次输入的命令)作用于具体环境下所产生的效果。

4. **系统实现的差异：**具体实现时，各种系统不完全按RFC实现，对那些建议值和可选功能，会有自己的偏好。NIDS为了逼近各种系统的实现就必须尽可能多地了解每一种系统对这些不一致情况的处理方式，然后根据实际应用中检测保护的对象再决定分析动作。但这种想法在实际中并不完全可行，有些问题不仅仅是系统的实现问题，还包含了用户的配置选择（比如是否计算UDP数据报的校验和），因此很难做到与目标系统的一致性处理。另外，某些系统（如Unix）出于操作的自由性和应用的方便性，允许用户对网络底层进行直接操作，致使入侵者几乎可以随心所欲地构造各种奇特的数据包。

4、简述网络安全态势感知系统。

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。

Chapter7

1、简述TCSEC(受信计算机系统评测标准)标准的C2安全级4项关键功能。

1. 安全登录机制
2. 自主访问控制机制
3. 安全审计机制
4. 对象重用保护机制

2、在哪些情况下可能会发生输入验证攻击。

1. 程序无法辨认语法上不正确的输入。
2. 模块接受了无关的输入。
3. 模块没有能够处理遗漏的输入域。
4. 发生了域值相关性错误。

3、为什么root对其可执行文件设置用户ID许可会带来严重的安全隐患?

当设置了SUID时，进程的euid为该可执行文件的所有者(属主)的 uid，而不是执行该程序的用户的uid，因此，由该程序创建的进 程都有与该程序所有者相同的存取许可。这样，程序的所有者将 可通过程序的控制，在有限的范围内向用户发布不允许被公众访 问的信息。当某可执行文件是root创建的，如果设置了SUID，而该可执行文 件又被赋予了其他普通用户的可执行权限，则该程序被任何用户 运行时，对应的进程的euid是root，该进程可以访问任何文件。