

**长沙理工大学**

计算机与通信工程学院

课程第四次作业

**课程名称**： **网络设计与集成 \_\_\_\_**

**年级**： **大三 班级**： **网络2102班**

**学号**： **202108060918 姓名**： **王俊\_\_\_\_**

**完成日期**： **2024 年 6 月**  **3 日**

**授课老师： 刘青\_\_\_\_\_\_\_\_\_\_\_\_\_**

1. 试分析在网络设计中IDS可部署在哪些位置，各有什么作用？

在网络设计中，IDS可以部署在多个关键位置以监测和响应潜在的网络攻击。以下是IDS常见的部署位置及其作用：

**1. 防火墙之前**

**作用：**在防火墙之前部署IDS可以检测到试图穿越防火墙的攻击尝试，提供额外的一层安全监测。这样，IDS可以捕获那些可能被防火墙放行的数据包，并且在它们达到内部网络之前就进行识别和响应。

**示例：**Internet接入点，ISP边界，或任何外部网络接口。

**2. 防火墙之后**

**作用：**位于防火墙之后的IDS可以监测已经穿透防火墙的流量，以及内部网络中的横向移动（lateral movement）攻击，这些攻击可能是由已经成功突破外围防御的攻击者发起的。

**示例：**核心交换机，内部子网边界。

**3. 服务器区域**

**作用：**部署在服务器区域的IDS能够特别关注关键资产，如数据库服务器、应用服务器等，这些地方往往是攻击者的主要目标。

**示例：**数据中心入口处，特定的服务器集群。

**4. 重点保护网段**

**作用：**在财务部门、研发部门等敏感区域部署IDS，可以专注于监测这些网段的异常活动，因为这些地方往往存储有高价值的信息。

**示例：**财务子网，研发子网。

**5. 内部子网间**

**作用：**在内部不同子网之间部署IDS可以帮助监测子网间的异常通信，这有助于识别内部威胁或已经被感染的主机。

**示例：**两个不同业务部门之间的网络边界。

**6. 主机级别**

**作用：**基于主机的IDS（HIDS）直接在系统上运行，监测系统日志、文件访问和应用程序行为，可以检测到网络IDS可能无法发现的本地攻击或恶意软件。

**示例：**关键服务器，工作站。

**7. 分布式部署**

**作用：**在多个位置部署IDS传感器，形成一个分布式检测网络，可以提供更全面的网络覆盖，增强检测能力和响应速度。

**示例：**整个企业网络的多个关键点。

1. 简述安全威胁的表现形式有哪些？

安全威胁的表现形式包括:信息泄露、媒体废弃(如报废的硬盘)、人员不慎、非授权访问、旁路控制(如线路搭接)、假冒、窃听、电磁信号截获、完整性侵犯(如篡改 Email 内容)、数据截获与修改、物理侵入、重放(如后台屏幕录像或键盘扫描)、业务否认、业务拒绝、资源耗尽、业务欺骗、业务流分析、特洛伊木马程序等。

3.简述接入网的核心功能。

接入网的核心功能是其架构中的关键组成部分，主要负责处理和适配用户网络接口UNI与业务节点接口SNI之间的通信要求。核心功能的主要职责在于确保接入网能够正确地将用户的数据和服务请求传输至核心网，同时也能将核心网的服务反馈给用户。

具体而言，接入网的核心功能主要包括以下几点：

1. **适配与转换：**
   * 完成UNI和SNI承载通路的要求与公共传送承载通路之间的适配。
   * 可能涉及到协议转换、信号格式调整、速率匹配等，以确保数据能够在不同的接口标准下顺畅传输。
2. **交叉连接与复用**：
   * 提供数据的交叉连接，即数据可以在多个输入和输出之间灵活分配。
   * 实现数据的复用，即将低速数据流合并成高速数据流，以便更高效地利用带宽资源。
3. **承载通路管理**：
   * 管理和控制承载通路的建立、维护和释放，确保数据传输的可靠性和服务质量（QoS）。
4. **信号处理**：
   * 包括但不限于信令转换、A/D和D/A转换，确保数字信号与模拟信号之间的正确转换，以及信令信息的正确处理。
5. **资源管理**：
   * 对接入网内的资源进行管理和调度，保证资源的有效利用和分配。
6. **安全性与保护**：
   * 提供必要的安全机制，保护数据免受未授权访问和干扰，确保网络的稳定性和安全性。

接入网的核心功能是确保接入网作为一个透明的传输管道，能够高效、准确地将用户数据传递至核心网，并从核心网返回数据至用户端，同时提供必要的管理和保护措施。这一功能是接入网能够作为用户与核心网之间的桥梁的关键所在。