一、填空题

1. 入侵是指任何试图破坏或危及信息系统资源的**完整性、机密性和可用性**的行为。

2. 入侵检测系统能够检测的入侵行为包括：**试图闯入、成功闯入、冒充其他用户、违反安全策略、合法用户的泄露和独占以及恶意使用资源**。

3. 审计数据的预处理方法包括：**数据融合、数据简化、数据集成、数据清理和数据变换**。

4. 入侵信号的主要分析方法：**模式匹配、统计分析、完整性分析**。

二、选择题

1. 基于网络的入侵检测系统，需要把网卡设置成（**D**）

A. 单播模式；B. 广播模式；C. 多播模式；D.混杂模式

2. 基于主机的入侵检测系统，需要收集以下哪些信息（**ACDE**）

A. 系统日志；B. 网络日志；C.目录和文件中的异常改变；D.程序中的异常行为；E. 物理形式的入侵信息

3. 下列关于包捕获机制的说法，正确的是：(**ABCD**)

A. 包捕获机制是依赖于操作系统

B. 包捕获机制是在数据链路层增加一个旁路处理器

C. 包捕获机制不影响网络协议栈对数据包的处理

D. 包过滤操作可以在用户空间或内核空间执行

4．入侵检测的主动响应行为包括（**ABC**）**ABCD**

A. 断开网络连接；B.杀死可疑程序；C.对攻击系统实施反击；D.增加审计日志；E.向管理员报警

5. 实现交换网络的数据捕获的方法包括：(**ABCD**)

A. 将数据包捕获程序安装在网络或代理服务器上。

B. 对交换机实行端口映射，将所有端口的数据包全部映射到监控端口上。

C. 在交换机和路由器之间连接一个Hub，将数据以广播的方式发送。

D. 采用ARP 欺骗，在负责数据包捕获的设备上实现整个网络的数据包转发。

三、简答题

1. 入侵检测系统的优、缺点是什么？分析这些优、缺点给信息系统安全设计所带来的影响。

**优点：**

1. **提高信息安全体系中其他部分的完整性；**
2. **提高系统的监控能力。能够从入口点到出口点跟踪用户的活动；能够识别和汇报文件的变化；能够侦测系统配置错误并纠正；能够识别特殊攻击类型并向系统安全管理员汇报，进行自动防御。**

**缺点：**

1. **无法弥补差的认证机制；**
2. **不能弥补网络协议的弱点；**
3. **不能弥补系统服务质量或完整性的缺陷；**
4. **如果没有人的干预，不能管理攻击调查；**
5. **不能指导安全策略的内容；**
6. **不能分析一个堵塞的网络；**
7. **不能处理有关pack-level攻击。**

**以上这些优缺点对信息系统安全设计的影响：**

**能够增强信息系统的完整性、监控能力，从而提高对入侵、攻击的抵御能力；但入侵检测系统更多是对原有协议、服务中存在的安全上的不足互补，而不是从根本上处理存在的弱点、缺陷，在进行设计时必须要考虑系统本身特点，做相应的调整。**

2. 分析包捕获机制的作用和局限性。

**包捕获为数据包捕获软件的设计提供了工作机制，作为sniffer, winpcap, wireshark, tcpdump等工具的底层原理提出；建立在目标系统上，帮助实现网络数据包实时获取、管理和控制。**

**BFT数据包捕获机制的局限性：虽然过滤一部分数据包在一定的程度上降低了系统的开销，提高了效率。但它的捕获和过滤都是在linux内核中完成。这样一来主要linux内核一更新，它也需要更新，降低了它的可移植性和通用性。**

**Libpcap数据包捕获机制的局限性：数据包经过了linux的内核网络协议栈，从网卡到用户空间的传递过程，存在多次的拷贝和中断响应，消耗大量的cpu时间片，降低系统整个体的数据分析能力。**

3. 安全日志和审计数据的区别？

**系统安全日志就是每次开关机、运行程序、系统报错时，这些信息都会被记录下来，保存在日志文件中。**

**审计数据可以直接监测获取，即从数据的产生或从属的对象直接获得数据，也可以间接监测获取，即从反映被监测对象行为的某个源获取数据。**

四、问答题

1、举例说明基于协议分析的入侵检测系统。

**Snort是一个通过实时抓取网络流量进行分析的入侵检测系统。Snort能够进行协议分析，并使用规则引擎来对网络数据包进行匹配、分析，用户可以自行定义规则来匹配相应的数据包，执行用户所设定的操作。**

**Zeek（之前名字是Bro）是另一个基于协议分析的入侵检测系统工具，使用脚本语言检测、分析网络数据包，并提供了广泛的协议支持。与Snort类似，Zeek也允许用户编写自定义脚本和规则来检测特定类型的安全事件。**

2、在入侵检测系统中，如何获取直接监测数据？举例说明

**1. 使用系统调用来监控：使用操作系统提供的接口记录操作系统和用户之间的交互。系统调用能够提供详细的日志信息，但同时需要处理的数据量也增大；**

**2. 使用内核模块：可以通过自行编写内核模块并加载到操作系统中，实现自由度更高的自定义操作，内核模块可以直接在内核空间运行，因此不易被攻击者发现和绕过，还可以更好地协调、控制主机资源；**

**3. 代理：安装一个代理程序在主机上，在主机和监视器之间中继数据。代理可以从操作系统接口中读取数据，然后发送到远程监视器，或者本地存储数据以供后期分析。**