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 。

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 、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 、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. 以下哪些内容是安全日志要记录的内容（ABCD）

A. 各种类型的登录；

B. 对象的访问；

C. 进程追踪；

D. 特权使用；

E. we 年的修改。

4．入侵检测的主动响应行为包括（ ABC）

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带

来的影响。

优点：

提高信息安全体系中其他部分的完整性；

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：

无法弥补差的认证机制；

不能弥补网络协议的弱点；

不能弥补系统服务质量或完整性的缺陷；

如果没有人的干预，不能管理攻击调查；

不能指导安全策略的内容；

不能分析一个堵塞的网络。

给信息系统安全设计带来的影响是：其他安全技术，如：防火墙、身份认证、访问控制、安全审计等互补，但无法弥补这些系统本身的缺陷；可以为其他安全习题的完善提供有针对性的意见。

1. 分析包捕获机制的作用和局限性。
2. 包捕获为数据包捕获软件的设计提供了工作机制，作为sniffer、winpcao,wireshark,tcpdump等工具的底层原理提出。（2）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。

1. 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 IDS（入侵检测系统）是一个强大的网络入侵检测系统。它具有实时数据流量分析和记录IP网络数据包的能力，能够进行协议分析，对网络数据包内容进行搜索/匹配。它能够检测各种不同的攻击方式，对攻击进行实时报警。

Snort的结构由4大软件模块组成，它们分别是：

　　　（1）数据包嗅探模块——负责监听网络数据包，对网络进行分；

　　　（2）预处理模块——该模块用相应的插件来检查原始数据包，从中发现原始数据的“行为”，如端口扫描，IP碎片等，数据包经过预处理后才传到检测引擎；

　　　（3）检测模块——该模块是Snort的核心模块。当数据包从预处理器送过来后，检测引擎依据预先设置的规则检查数据包，一旦发现数据包中的内容和某条规则相匹配，就通知报警模块；

　　　（4）报警/日志模块——经检测引擎检查后的Snort数据需要以某种方式输出。如果检测引擎中的某条规则被匹配，则会触发一条报警，这条报警信息会通过网络、UNIXsocket、WindowsPopup(SMB)、SNMP协议的trap命令传送给日志文件，甚至可以将报警传送给第三方插件（如 SnortSam），另外报警信息也可以记入SQL数据库。

1. 在入侵检测系统中，如何获取直接监测数据？举例说明

为了监测主机CPU的负荷，可以直接从主机相应内核中获得数据。要监测inetd进程提供的网络服务，可以直接从inetd进程获取相关网络访问的数据。