第一套

第一题

参考答案：

【问题 1】

（1）机密性　（2）完整性　（3）可用性

【问题 2】

（a）信息体系结构　（b）业务体系结构

（c）解决方案和应用程序体系结构　（d）解决方案和应用程序体系结构

【问题 3】

（1）信息系统安全技术体系　（2）安全管理体系

（3）安全标准体系　（4）安全法律法规

【问题 4】

（1）物理安全　（2）网络安全　（3）主机安全

（4）数据安全　（5）独立评估　（6）安全应急机制

注：意思接近答对 4 点即可。

第二题

参考答案：

【问题 1】

（1）D　（2）C　（3）A

（4）G　（5）B　（6）C

【问题 2】

（7）192.168.20.1　（8）80　（9）192.168.20.2

（10）255.255.255.0　（11）192.168.20.1

【问题 3】

代理设置：打开浏览器，找到“Internet 选项”单击“Internet 选项”，弹出对话框，找到“连接”标签，单击“局域网设置 (L)” ，弹出代理设置对话框。

默认网关设置：打开“本地连接状态”对话框“属性 (P)”按钮，单击“本地连接属性”对话框“属性(R)”按钮，弹出默认网关设置对话框。

【问题 4】

无论是普通访问还是透明访问，在 IE 浏览器地址栏中输入：http：//192.168.10.2 回车后，如果访问成功，即可出现正确访问页面。

第三题

参考答案：

【问题 1】

（1）透明性（或隐蔽性）　　（2）鲁棒性　　（3）安全性

【问题 2】

（1）水印　　（2）编码器（或嵌入算法）

（3）解码器和比较器（或验证算法、提取算法、检测算法）

【问题 3】

（a）编码过程　　（b）解码过程　　（c）水印验证过程

【问题 4】

（1）版权保护　　（2）加指纹　　（3）标题与注释

（4）篡改提示　　（5）使用控制

注：意思接近答对 3 点即可。

第四题

参考答案：

【问题 1】

（1）远程镜像技术　　（2）快照技术　　（3）基于 IP 的 SAN 互连技术

【问题 2】

网络容灾备份系统从其对系统的保护程度来分，可以将容灾系统分为:数据容灾和应用容灾。

数据容灾：是指建立一个异地的数据系统，该系统是本地关键应用数据的一个可用复制。在本地数据及整个应用系统出现灾难时，系统至少在异地保存有一份可用的关键业务的数据，采用的主要技术是数据备份和数据复制技术。

应用容灾：是在数据容灾的基础上，在异地建立一套完整的与本地生产系统相当的备份应用系统(可以是互为备份)，在灾难情况下，远程系统迅速接管业务运行。数据容灾是抗御灾难的保障，雨应用容灾则是容灾系统建设的目标。主要的技术包括负载均衡、集群技术。

【问题 3】

局域网内部署的三台备用服务器，分别是 HIS、PACS 以及其他业务系统的容灾服务器。

为实现数据实时复制和操作系统、文件的定时备份，在 HIS 和 PACS 数据库服务器部署镜像软件，在 RIS、LIS、C1S 、EMR 等 4 台数据库服务器上分别部署连续数据保护 CDP 软件。

第五题

参考答案

【问题 1】

（1）对称加密算法：DES 算法、AES 算法、SM4 算法等

（2）非对称加密算法：RSA 算法、ElGamal 算法、椭圆曲线密码等

【问题 2】

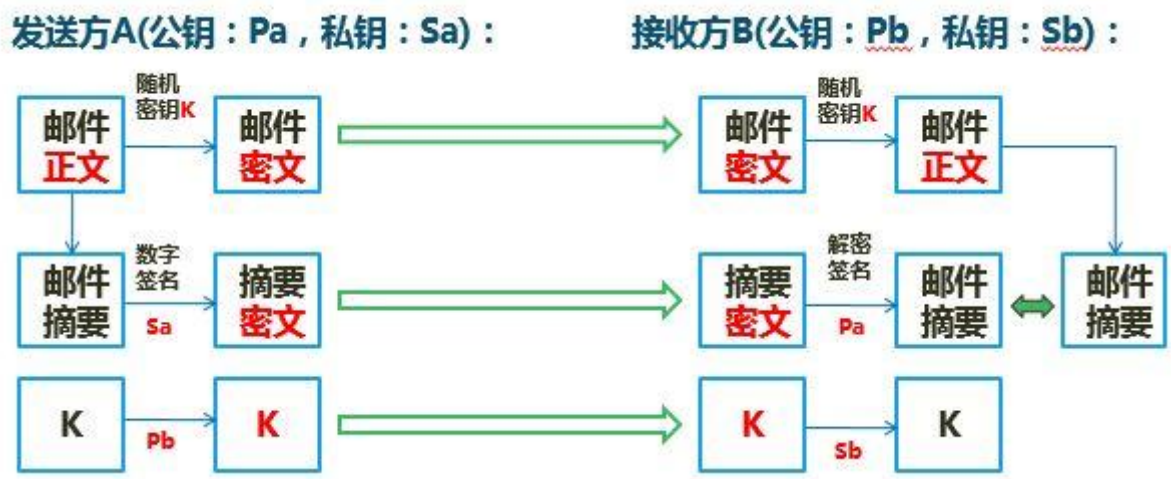
加解密时，发送方用对方的公钥加密，接收方用自己的私钥进行解密。

签名时，发送方用自己的私钥签名，接收方用对方的公钥验证其签名。

公钥是公开的，也就是说发送方和接收方的公钥是相互之间都知道的，包括其他的第三方也可以知道，而私钥是私有的，也就是说每个人的私钥只有自己知道，在加密时，发送方用对方的公钥加密，相应对方就只能用自己的私钥解密，这就保证了只有相应的接收方才能正确解密该信息；在签名时，发送方用自己的私钥进行签名，而私钥是每个人所独有的，任何人都不能伪造，相应的接收方在用发送方公钥进行验证时就能保证发送方的身份的合法性。

【问题 3】

具体设计如下：



第二套

第一题

参考答案：

【问题 1】

（1）安全法律法规与政策　（2）安全管理体系

（3）安全技术体系　（4）安全标准体系

【问题 2】

（5）安全依据　（6）初始阶段　（7）设计阶段

（8）实施阶段　（9）运维阶段　（10）最终处理阶段

【问题 3】

将信息系统分成两部分：在不可控的开放环境下运作的部分（开放式系统部分）；在可控的封闭环境下运作的部分（封部式系统部分）。

封闭式系统安全实现途径的特征主要有两点：一是由多个防火墙的组合来创建一个封闭的系统；二是使用入侵检测系统对封闭系统进行实时的威胁监视。

开放式系统的安全设计：利用两层以上的防火墙把信息系统网络分成多个子网，网络显示多层结构。两层防火墙将信息系统网络分成 Internet 、外网、内网 3 层结构，分别形成了用户端、 Web 服务器和应用服务器 3 个系统部分的运行环境。外网里放置的是一些提供公开服务的不敏感的服务器，如邮件服务器、网页服务器；内网中放置应用服务器，更里面一层的网络放置的是信息系统核心服务器，称为主机，一般使用专用编码、专用网络协议，核心数据资料都存放在这里。

【问题 4】

需要从 3 个方面进行综合考虑：风险分析、安全策略、安全架构。

第二题

参考答案：

【问题 1】

1、G　2、I　3、H　4、J　5、F　6、B　7、E　8、D　9、A　10、C

【问题 2】

A 是错误的，应该是广泛性。

【问题 3】

避免 SQL 注入的方法：

1、常使用自带的安全的 API ，完全避免使用解释器或提供参数化界面的 API 。

2、如果没法使用一个参数化的 API ，那么就使用解释器具体的 escape 语法来避免特

殊字符。比如，分号分隔符。

3、加强对用户输入的验证。使用正面的或"自名单"中的具有恰当的规范化的输入验证方法会有助于防止注入攻击。

【问题 4】

防止 XSS 需要将不可信数据与动态的浏览器内容区分开。

1、根据数据将要置于的 HTML 上下文（包括主体、属性、 JavaScript CSS URL)对所有的不可信数据进行恰当的转义 （escape) ，或者是去掉。没有 html 标签，页面就是安全的。

2、"白名单"的，具有恰当的规范化和解码功能的输入验证方法同样会有助于防止跨站脚本。

3、用内容安全策略 （CSP) 来抵御整个网站的跨站脚本攻击。

4、用户学会控制自己的好奇心，尽量不去单击页面中不安全的链接。

防止跨站请求伪造，通常需要在每个 HTTP 请求中添加一个不可预测的令牌。这种令牌至少应该对每一个用户会话来说是唯一的。

1、将独有的令牌包含在一个隐藏字段中。这将使得该令牌通过 Http 请求体发送，避免其包含在 URL 中从而被暴露出来。

2、该独有令牌同样可以包含在 URL 中或作为一个 URL 参数。

3、要求用户重新认证或者判明他们是一个真实的用户也可以前护 CSRF 攻击。

第三题

参考答案：

【问题 1】

（1）untrust （2）1.1.1.1/24 （3）1.1.1.254 （4）1.2.2.2

（5）trust （6）10.3.0.1/24

【问题 2】

配置内网接口 GE1/0/2 的 DHCP 服务。

【问题 3】

（7）10.3.0.2 （8）10.3.0.254 （9）255.255.255.0 （10）10.3.0.1

（11）1.2.2.2 （12）trust （13）untrust （14）10.3.0.0/24

（15）trust

【问题 4】。

有 3 种检验方式。

方法一：查看接口 GE 1/ 0/1 的公网地址配置是否正确，物理状态和 IPv4 状态是否为 Up。

方法二：在内部网络中的 PC 上通过 ipconfig/all 命令检查网卡是否正确分配到私网地址和 DNS 地址。

方法三：检查内部网络中的 PC 是否能通过域名访问 Internet，若能访问，则表示配置成功。

第四题

参考答案：

【问题 1】

ABC

【问题 2】

1、C　　2、B　　3、A

【问题 3】

关联规则挖掘问题可以划分成两个子问题：

（1）发现频繁项目集　　（2）生成关联规则

【问题 4】

（1）表示用户 A 经常执行 vi 命令，执行命令时所使用的参数通常是.c 为后缀名的文件，该模式的置信度为 45%，支持度为 5%。

（2）表示用户经常执行的命令序列是：首先用 vi 编辑 c 程序，然后用 gcc 编译再使用 gdb 进行程序的调试，该模式的支持度为 40%。

（3）经过分析可以判断出用户 A 应该是一个 C 程序员，其工作时间是每天的上午，并且通常从 IP 为 192.168.1.201 的客户机登录到 IP 为 192.168.1.119 的主机上进行编程操作。如果在实际的检测过程中，发现某一天该用户突然在晚间登录，或者从一个陌生的 IP 地址登录到系统主机，或者在登录过程中执行了大量与编程无关的操作，访问主机的敏感口录和文件，则可以推断出该用户出现了某种异常。

第五题

参考答案：

【问题 1】

认证和数字签名技术的区别。

（1）认证总是基于某种收发双方共享的保密数据来认证被鉴别对象的真实性，而数字签名中用于验证签名的数据是公开的。

（2）认证允许收发双方互相验证其真实性，不准许第三者验证，而数字签名允许收发双方和第三者都能验证。

（3）数字签名具有发送方不能抵赖、接收方不能伪造和具有在公证人前解决纠纷的能力，而认证则不一定具备。

【问题 2】

在上述口令验证机制中，会存在下列一些问题：

（1）攻击者可能从口令表中获取用户口令。因为用户的口令以明文形式存储在系统中，系统管理员可以获得所有口令，攻击者也可利用系统的漏洞来获得他人的口令。

（2）攻击者可能在传输线路上截获用户口令。因为用户的口令在用户终端到系统的线路上以明文形式传输，所以攻击者可在传输线路上截获用户口令。

（3）用户和系统的地位不平等。这里只有系统强制性地验证用户的身份，而用户无法验证系统的身份。

改进的口令验证机制有：（1）利用单向函数加密口令，（2）利用数字签名方法验证口令，（3）口令的双向验证，（4）一次性口令。

【问题 3】

消息认证码 MAC 是属于报文内容认证方法。

具体认证过程：假定通信双方共享秘密钥 K，若发送方 A 向接收方 B 发送报文 M，则 A 计算 MAC=C(M ， K) ，并将报文 MAC 发送给接收方：

A→ B: M‖MAC

接收方收到报文后用相同的秘密钥 K 进行相同的计算得出新的 MAC，并将其与接收到的 MAC 进行比较，若二者相等，则可以判定：

（1）接收方可以相信报文未被修改；（2）接收方可以相信报文来自意定的发送方。

第三套

第一题

参考答案：

【问题 1】

（1）安全服务　（2）协议层次　（3）系统单元

（4）认证　（5）访问控制　（6）数据保密　（7）可用性

【问题 2】

1、最小权限原则　　2、纵深防御原则

3、防御多样性原则　　4、防御整体性原则

【问题 3】

典型的校园网络结构应该包括三个层次：核心层、汇聚层、接入层。

接入层：主要功能是为最终用户提供网络接入。

汇聚层：是网络接入层和核心层之间的分界点。

核心层：核心层的主要目的是尽可能快地交接数据。主要是用来提供交换区块间的连接、提供到其他区块的访问。

【问题 4】

根据网络体系结构的设计思想和校园网络所遇到的网络安全成胁，校园网络需要组合必要的安全设备和安全服务来构建网络安全系统，提供路由安全、路由过滤、防火墙、 IDS、

VPN 、电子邮件安全、 Web 安全、身份认证、DDOS 防御、病毒防范和补丁服务及 WAF 等。

作为一个安全的电子邮件系统应该具备以下功能：系统本身具有较强的稳定性和可靠性；应具有与防病毒系统集成的病毒邮件查杀、处理能力；具有灵活的垃圾邮件防范机制；具有严格的发信认证机制和反邮件中继功能，从而避免本身成为垃圾邮件和病毒邮件的发送源。

第二题

参考答案：

【问题 1】

（1）untrust （2）1.1.1.2/29 （3）trust （4）10.1.1.1/24 （5）trust
（6）untrust （7）untrust （8）trust （9）untrust （10）local
（11）local （12）untrust
（13）1.1.1.2 （14）vpdnuser （15）Hello123 （16）Admin@123

【问题 2】

配置接口 GE0/0/1，地址池起始 IP：10.1.2.2 地址池结束 IP：10.1.2.100

【问题 3】

进入“控制面板→网络和共享中心”，右击 “VPN 连接”选择属性，打开“VPN 连接属性设置”对话框。

【问题 4】

连接 VPN，在防火墙上查看到 IPSec 隧道监控信息和 L2TP 通道监控信息。

第三题

参考答案：

【问题 1】

流量大小

【问题 2】

1、 基于实时抓包的流量监控技术 2、基于 SNMP/RMON 的流量监控技术
3、基于数据采集探针的流量监控技术 4、基于 NetFlow/sFlow 的流量监控技术

【问题 3】

（1） 有效性、可靠性、实时性
（2） A、深度流检测技术（DFI） B、深度包检测技术（DPI）

【问题 4】

（1）过滤设置模块 （2）监听捕获模块
（3）协议解析模块 （4）数据保存加载模块
（5）数据显示模块

第四题

参考答案：

【问题 1】

（1）标准性原则 （2）关键业务原则 （3）可控性原则 （4）最小影响原则

【问题 2】

（1）资产 （2）威胁 （3）脆弱性

【问题 3】

（1）威胁识别 （2）脆弱性识别

（3）资产识别 （4）风险值

A、定性计算方法 B、定量计算方法

【问题 4】

（1） 《风险评估方案》 （2） 《己有安全措施分析报告》

（2） 《风险评估报告》 （4） 《安全整改建议》

第五题

参考答案：

【问题 1】

1、单向性 2、抗弱碰撞性 3、抗强碰撞性

【问题 2】

填充 512 位。填充方法：是在报文后附加一个 1 和 511 个 0 。然后附上表示填充前报文长度的 64 位数据

【问题 3】

（1）160 位的缓冲区，由 5 个 32 位的寄存器（ABCDE）组成

（2）4 轮运算组成，每轮运算迭代 20 步，前 16 步迭代中压缩函数的输入是原报文分组的内容。

【问题 4】

Hash 算法的核心是压缩函数。

设计安全 Hash 函数时，重要的是要设计具有抗碰撞能力的压缩函数，并且该压缩函数的输入是定长的。

第四套

第一题

参考答案：

【问题 1】

（1）安全需求（2）评估实施（3）评估结果（4）等级认证

（5）安全环境（6）安全目标（7）安全需求 （8）评估规范

（9）策划与组织（10）开发与采购（11）实施与交付

（12）运行与维护 （13）更新与废弃

（14）识别目标（15）识别输入（16）生成模糊测试数据（17）执行模糊测试数据 （18）确定可利用性

【问题 2】

过程可控性

【问题 3】

信息系统安全测评方法主要有模糊测试和代码审计。

采用代码审计方法。

【问题 4】

首先应将信息系统试运行 6 个月。

第二题

参考答案：

【问题 1】

（1）1.1.1.1 （2）255.255.255.0 （3）untrust

（4）10.3.0.1 （5）255.255.255.0 （6）trust

【问题 2】

（7）trust （8）untrust （9）default （10）default

（11）trust （12）untrust （13）游戏、媒体共享 （14）禁止

（15）trust （16）untrust （17）any （18）允许

【问题 3】

（19）trust （20）untrust （21）禁止

【问题 4】

高层管理者安全策略验证：验证高层管理者是否能够不受限制的访问 Internet ，如果是则证明高层管理者的安全策略配置成功。

市场员工安全策略验证：验证市场员工的用户是否能够访问 Internet，而且访问 Internet 时不能使用 NGFW 定义的游戏和媒体共享应用。如果是则证明市场员工的安全策略配置成功。

研发员工安全策略验证：验证研发员工用户是否不能访 Internet。如果是则证明研发员工的安全策略配置成功。

或者选择“监控→日志→策略命中日志”分别查看高窟管理者、市场员工、研发员工是否命中正确的安全策略。

第三题

参考答案：

【问题 1】

1、交易的真实性　　2、交易的完整性

3、交易的保密性　　4、交易的不可抵赖性

【问题 2】

（1）交易安全　（2）行为安全　（3）数据安全　（4）服务安全

（5）网络安全　（6）物理安全

（7）安全治理　（8）安全运维　（9）安全评估　（10）应急管理

【问题 3】

（11）信息安全管理　（12）信息安全服务　（13）信息安全模块

（14）数据应用　（15）网络　（16）系统　（17）物理环境

【问题 4】

系统安全包括防病毒技术、主机安全加固、操作系统安全等技术。

第四题

参考答案：

【问题 1】

这四项技术分别是隧道技术、加解密技术、密钥管理技术、使用者与设备身份认证技术等。其中隧道技术是 VPN 的基本技术。

【问题 2】

1、基于 MPLS 的 VPN　　2、基于隧道协议的 VPN

3、基于虚拟电路的 VPN　4、应用层 VPN

【问题 3】

应用层 VPN 包括有 SOCKS 协议、SSL 安全套接字协议、安全 HTTP 协议、安全电子邮件协议等。

基于 IPSec 的 VPN 包括有两种应用模式：隧道模式和传输模式。

【问题 4】

应该采用基于 MPLS 的 VPN。MPLS VPN 安全性高，采用 MPLS 作为通道机制实现透明报文传输，MPLS 标签交换路径(LSP)具有与 FR 和 ATMVCC 相类似的安全性；另外，用户还可以

设置防火墙和采用数据加密的方法，进一步提高安全性。具有强大的扩展性。包括两点：网络中可以容纳的 VPN 数目很大；同一 VPN 用户很容易扩充。具有灵活的控制策略。可以制定特殊的控制策略，满足不同用户的特殊要求，实现增值服务。

第五题

参考答案：

【问题 1】

初级密钥：直接用于加解密数据（通信，文件）

二级密钥：用于保护初级密钥

主密钥：保护二级密钥和初级密钥

【问题 2】

（1）交易的真实性　　（2）交易的完整性

（3）交易的保密性　　（4）交易的不可抵赖性

【问题 3】

公钥证书能以明文的形式进行存储和分发。

使用公钥证书的主要好处有：1、用户只要获得其他用户的证书，就可以获得其他用户的公钥。2、用户只要获得 CA 的公钥，就可以安全地认证其他用户的公钥。因此公钥证书为公钥的分发奠定了基础，成为公钥密码在大型网络系统中应用的关键技术。

【问题 4】

1、证书申请　　2、RA 确认用户的合法性　　4、RA 提交用户申请信息到 CA

6、CA 将用户证书传给受理该用户的 RA

7、RA 将证书传给用户或者用户自己取回证书