**说明**：本套面试笔试题为软谋教育多年的教学和学生就业指导过程中积累下来的宝贵资料，大部分来自于学员从面试现场带回来的真实笔试面试题，涵盖了主流的.NET笔试面试题，是您找工作的必胜法宝。

如果有技术问题无法理解或者新的建议，可以联系微信



信息安全工程师考试真题

一、单项选择

1、以下有关信息安全管理员职责的叙述，不正确的是（）

A、信息安全管理员应该对网络的总体安全布局进行规划

B、信息安全管理员应该对信息系统安全事件进行处理

C、信息安全管理员应该负责为用户编写安全应用程序

D、信息安全管理员应该对安全设备进行优化配置

**参考答案：C**

2、国家密码管理局于2006年发布了“无线局域网产品须使用的系列密码算法”，其中规定密钥协商算法应使用的是（）

A、DH

B、ECDSA

C、ECDH

D、CPK

**参考答案：C**

3、以下网络攻击中，（）属于被动攻击

A、拒绝服务攻击

B、重放

C、假冒

D、流量分析

**参考答案：D**

4、（）不属于对称加密算法

A、IDEA

B、DES

C、RCS

D、RSA

**参考答案：D**

5、面向身份信息的认证应用中，最常用的认证方法是（）

A、基于数据库的认证

B、基于摘要算法认证

C、基于PKI认证

D、基于账户名/口令认证

**参考答案：D**

6、如果发送方使用的加密密钥和接收方使用的解密密钥不相同，从其中一个密钥难以推出另一个密钥，这样的系统称为（）

A、公钥加密系统

B、单密钥加密系统

C、对称加密系统

D、常规加密系统

**参考答案：A**

7、S/Key口令是一种一次性口令生产方案，它可以对抗（）

A、恶意代码木马攻击

B、拒绝服务攻击

C、协议分析攻击

D、重放攻击

**参考答案：D**

8、防火墙作为一种被广泛使用的网络安全防御技术，其自身有一些限制，它不能阻止（）

A、内部威胁和病毒威胁

B、外部攻击

C、外部攻击、外部威胁和病毒威胁

D、外部攻击和外部威胁

**参考答案：A**

9、以下行为中，不属于威胁计算机网络安全的因素是（）

A、操作员安全配置不当而造成的安全漏洞

B、在不影响网络正常工作的情况下，进行截获、窃取、破译以获得重要机密信息

C、安装非正版软件

D、安装蜜罐系统

**参考答案：D**

10、电子商务系统除了面临一般的信息系统所涉及的安全威胁之外，更容易成为黑客分子的攻击目标，其安全性需求普遍高于一般的信息系统，电子商务系统中的信息安全需求不包括（）

A、交易的真实性

B、交易的保密性和完整性

C、交易的可撤销性

D、交易的不可抵赖性

**参考答案：C**

11、以下关于认证技术的叙述中，错误的是（）

A、指纹识别技术的利用可以分为验证和识别

B、数字签名是十六进制的字符串

C、身份认证是用来对信息系统中实体的合法性进行验证的方法

D、消息认证能够确定接收方收到的消息是否被篡改过

**参考答案：B**

12、有一种原则是对信息进行均衡、全面的防护，提高整个系统的安全性能，该原则称为（）

A、动态化原则

B、木桶原则

C、等级性原则

D、整体原则

**参考答案：D**

13、在以下网络威胁中，（）不属于信息泄露

A、数据窃听

B、流量分析

C、偷窃用户账户

D、暴力破解

**参考答案：D**

14、未授权的实体得到了数据的访问权，这属于对安全的（）

A、机密性

B、完整性

C、合法性

D、可用性

**参考答案：A**

15、按照密码系统对明文的处理方法，密码系统可以分为（）

A、置换密码系统和易位密码

B、密码学系统和密码分析学系统

C、对称密码系统和非对称密码系统

D、分级密码系统和序列密码系统

**参考答案：A**

16、数字签名最常见的实现方法是建立在（）的组合基础之上

A、公钥密码体制和对称密码体制

B、对称密码体制和MD5摘要算法

C、公钥密码体制和单向安全散列函数算法

D、公证系统和MD4摘要算法

**参考答案：C**

17、以下选项中，不属于生物识别方法的是（）

A、指纹识别

B、声音识别

C、虹膜识别

D、个人标记号识别

**参考答案：D**

18、计算机取证是将计算机调查和分析技术应用于对潜在的、有法律效应的确定和提取。以下关于计算机取证的描述中，错误的是（）

A、计算机取证包括对以磁介质编码信息方式存储的计算机证据的提取和归档

B、计算机取证围绕电子证据进行，电子证据具有高科技性等特点

C、计算机取证包括保护目标计算机系统，确定收集和保存电子证据，必须在开计算机的状态下进行

D、计算机取证是一门在犯罪进行过程中或之后手机证据

**参考答案：C**

19、注入语句：http：//xxx.xxx.xxx/abc.asp?p=YYanduser>0不仅可以判断服务器的后台数据库是否为SQL-SERVER，还可以得到（）

A、当前连接数据库的用户数据

B、当前连接数据库的用户名

C、当前连接数据库的用户口令

D、当前连接的数据库名

**参考答案：B**

20、数字水印技术通过在数字化的多媒体数据中嵌入隐蔽的水印标记，可以有效地对数字多媒体数据的版权保护等功能。以下各项工，不属于数字水印在数字版权保护必须满足的基本应用需求的是（）

A、安全性

B、隐蔽性

C、鲁棒性

D、可见性

**参考答案：D**

21、有一种攻击是不断对网络服务系统进行干扰，改变其正常的作业流程，执行无关程序使系统响应减慢甚至瘫痪。这种攻击叫做（）

A、重放攻击

B、拒绝服务攻击

C、反射攻击

D、服务攻击

**参考答案：B**

22、在访问因特网时，为了防止Web页面中恶意代码对自己计算机的损害，可以采取的防范措施是（）

A、将要访问的Web站点按其可信度分配到浏览器的不同安全区域

B、在浏览器中安装数字证书

C、利用IP安全协议访问Web站点

D、利用SSL访问Web站点

**参考答案：A**

23、下列说法中，错误的是（）

A、服务攻击是针对某种特定攻击的网络应用的攻击

B、主要的渗入威胁有特洛伊木马和陷阱

C、非服务攻击是针对网络层协议而进行的

D、对于在线业务系统的安全风险评估，应采用最小影响原则

**参考答案：B**

24、依据国家信息安全等级保护相关标准，军用不对外公开的信息系统至少应该属于（）

A、二级及二级以上

B、三级及三级以上

C、四级及四级以上

D、无极

**参考答案：B**

25、电子邮件是传播恶意代码的重要途径，为了防止电子邮件中的恶意代码的攻击，用（）方式阅读电子邮件

A、网页

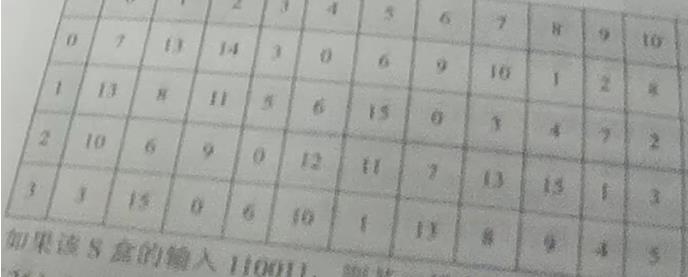
B、纯文本

C、程序

D、会话

**参考答案：B**

26、已知DES算法的S盒如下：



如果该S盒的输入110011，则其二进制输出为（）

A、0110

B、1001

C、0100

D、0101

**参考答案：C**

27、在IPv4的数据报格式中，字段（）最适合于携带隐藏信息

A、生存时间

B、源IP地址

C、版本

D、标识

**参考答案：D**

28、Kerberos是一种常用的身份认证协议，它采用的加密算法是（）

A、Elgamal

B、DES

C、MD5

D、RSA

**参考答案：B**

29、以下关于加密技术的叙述中，错误的是（）

A、对称密码体制的加密密钥和解密密钥是相同的

B、密码分析的目的就是千方百计地寻找密钥或明文

C、对称密码体制中加密算法和解密算法是保密的

D、所有的密钥都有生存周期

**参考答案：C**

30、移动用户有些属性信息需要受到保护，这些信息一旦泄露，会对公众用户的生命财产安全构成威胁。以下各项中，不需要被保护的属性是（）

A、用户身份（ID）

B、用户位置信息

C、终端设备信息

D、公众运营商信息

**参考答案：D**

31、以下关于数字证书的叙述中，错误的是（）

A、证书通常有CA安全认证中心发放

B、证书携带持有者的公开密钥

C、证书的有效性可以通过验证持有者的签名

D、证书通常携带CA的公开密钥

**参考答案：D**

32、密码分析学是研究密码破译的科学，在密码分析过程中，破译密文的关键是（）

A、截获密文

B、截获密文并获得密钥

C、截获密文，了解加密算法和解密算法

D、截获密文，获得密钥并了解解密算法

**参考答案：D**

33、利用公开密钥算法进行数据加密时，采用的方法是（）

A、发送方用公开密钥加密，接收方用公开密钥解密

B、发送方用私有密钥加密，接收方用私有密钥解密

C、发送方用公开密钥加密，接收方用私有密钥解密

D、发送方用私有密钥加密，接收方用公开密钥解密

**参考答案：C**

34、数字信封技术能够（）

A、对发送者和接收者的身份进行认证

B、保证数据在传输过程中的安全性

C、防止交易中的抵赖发送

D、隐藏发送者的身份

**参考答案：B**

35、在DES加密算法中，密钥长度和被加密的分组长度分别是（）

A、56位和64位

B、56位和56位

C、64位和64位

D、64位和56位

**参考答案：A**

36、甲不但怀疑乙发给他的被造人篡改，而且怀疑乙的公钥也是被人冒充的，为了消除甲的疑虑，甲和乙决定找一个双方都信任的第三方来签发数字证书，这个第三方为（）

A、国际电信联盟电信标准分部（ITU-T）

B、国家安全局（NSA）

C、认证中心（CA）

D、国家标准化组织（ISO）

**参考答案：C**

37、WI-FI网络安全接入是一种保护无线网络安全的系统，WPA加密模式不包括（）

A、WPA和WPA2

B、WPA-PSK

C、WEP

D、WPA2-PSK

**参考答案：C**

38、特洛伊木马攻击的威胁类型属于（）

A、授权侵犯威胁

B、渗入威胁

C、植入威胁

D、旁路控制威胁

**参考答案：C**

39、信息通过网络进行传输的过程中，存在着被篡改的风险，为了解决这一安全问题，通常采用的安全防护技术是（）

A、加密技术

B、匿名技术

C、消息认证技术

D、数据备份技术

**参考答案：C**

40、甲收到一份来自乙的电子订单后，将订单中的货物送达到乙时，乙否认自己曾经发送过这份订单，为了解除这种纷争，采用的安全技术是（）

A、数字签名技术

B、数字证书

C、消息认证码

D、身份认证技术

**参考答案：A**

41、目前使用的防杀病毒软件的作用是（）

A、检查计算机是否感染病毒，清除已感染的任何病毒

B、杜绝病毒对计算机的侵害

C、查出已感染的任何病毒，清除部分已感染病毒

D、检查计算机是否感染病毒，清除部分已感染病毒

**参考答案：D**

42、IP地址分为全球地址和专用地址，以下属于专用地址的是（）

A、172.168.1.2

B、10.1.2.3

C、168.1.2.3

D、192.172.1.2

**参考答案：B**

43、下列报告中，不属于信息安全风险评估识别阶段的是（）

A、资产价值分析报告

B、风险评估报告

C、威胁分析报告

D、已有安全威胁分析报告

**参考答案：B**

44、计算机犯罪是指利用信息科学技术且以计算机跟踪对象的犯罪行为，与其他类型的犯罪相比，具有明显的特征，下列说法中错误的是（）

A、计算机犯罪具有隐蔽性

B、计算机犯罪具有高智能性，罪犯可能掌握一些其他高科技手段

C、计算机犯罪具有很强的破坏性

D、计算机犯罪没有犯罪现场

**参考答案：D**

45、以下对OSI（开放系统互联）参考模型中数据链路层的功能叙述中，描述最贴切是（）

A、保证数据正确的顺序、无差错和完整

B、控制报文通过网络的路由选择

C、提供用户与网络的接口

D、处理信号通过介质的传输

**参考答案：A**

46、深度流检测技术就是以流为基本研究对象，判断网络流是否异常的一种网络安全技术，其主要组成部分通常不包括（）

A、流特征选择

B、流特征提供

C、分类器

D、响应

**参考答案：D**

47、一个全局的安全框架必须包含的安全结构因素是（）

A、审计、完整性、保密性、可用性

B、审计、完整性、身份认证、保密性、可用性

C、审计、完整性、身份认证、可用性

D、审计、完整性、身份认证、保密性

**参考答案：B**

48、以下不属于网络安全控制技术的是（）

A、防火墙技术

B、访问控制

C、入侵检测技术

D、差错控制

**参考答案：D**

49、病毒的引导过程不包含（）

A、保证计算机或网络系统的原有功能

B、窃取系统部分内存

C、使自身有关代码取代或扩充原有系统功能

D、删除引导扇区

**参考答案：D**

50、网络系统中针对海量数据的加密，通常不采用（）

A、链路加密

B、会话加密

C、公钥加密

D、端对端加密

**参考答案：C**

51、安全备份的策略不包括（）

A、所有网络基础设施设备的配置和软件

B、所有提供网络服务的服务器配置

C、网络服务

D、定期验证备份文件的正确性和完整性

**参考答案：C**

52、以下关于安全套接层协议（SSL）的叙述中，错误的是（）

A、是一种应用层安全协议

B、为TCP/IP连接提供数据加密

C、为TCP/IP连接提供服务器认证

D、提供数据安全机制

**参考答案：A**

53、入侵检测系统放置在防火墙内部所带来的好处是（）

A、减少对防火墙的攻击

B、降低入侵检测

C、增加对低层次攻击的检测

D、增加检测能力和检测范围

**参考答案：B**

54、智能卡是指粘贴或嵌有集成电路芯片的一种便携式卡片塑胶，智能卡的片内操作系统（COS）是智能卡芯片内的一个监控软件，以下不属于COS组成部分的是（）

A、通讯管理模块

B、数据管理模块

C、安全管理模块

D、文件管理模块

**参考答案：B**

55、以下关于IPSec协议的叙述中，正确的是（）

A、IPSec协议是解决IP协议安全问题的一

B、IPSec协议不能提供完整性

C、IPSec协议不能提供机密性保护

D、IPSec协议不能提供认证功能

**参考答案：A**

56、不属于物理安全威胁的是（）

A、自然灾害

B、物理攻击

C、硬件故障

D、系统安全管理人员培训不够

**参考答案：D**

57、以下关于网络钓鱼的说法中，不正确的是（）

A、网络钓鱼融合了伪装、欺骗等多种攻击方式

B、网络钓鱼与Web服务没有关系

C、典型的网络钓鱼攻击都将被攻击者引诱到一个通过精心设计的钓鱼网站上

D、网络钓鱼是“社会工程攻击”是一种形式

**参考答案：B**

58、以下关于隧道技术说法不正确的是（）

A、隧道技术可以用来解决TCP/IP协议的某种安全威胁问题

B、隧道技术的本质是用一种协议来传输另外一种协议

C、IPSec协议中不会使用隧道技术

D、虚拟专用网中可以采用隧道技术

**参考答案：C**

59、安全电子交易协议SET是有VISA和MasterCard两大信用卡组织联合开发的电子商务安全协议。以下关于SET的叙述中，正确的是（）

A、SET是一种基于流密码的协议

B、SET不需要可信的第三方认证中心的参与

C、SET要实现的主要目标包括保障付款安全，确定应用的互通性和达到全球市场的可接受性

D、SET通过向电子商务各参与方发放验证码来确认各方的身份，保证网上支付的安全性

**参考答案：C**

60、在PKI中，不属于CA的任务是（）

A、证书的办法

B、证书的审改

C、证书的备份

D、证书的加密

**参考答案：D**

61、以下关于VPN的叙述中，正确的是（）

A、VPN指的是用户通过公用网络建立的临时的、安全的连接

B、VPN指的是用户自己租用线路，和公共网络物理上完全隔离的、安全的线路

C、VPN不能做到信息认证和身份认证

D、VPN只能提供身份认证，不能提供数据加密的功能

**参考答案：A**

62、扫描技术（）

A、只能作为攻击工具

B、只能作为防御工具

C、只能作为检查系统漏洞的工具

D、既可以作为工具，也可以作为防御工具

**参考答案：D**

63、包过滤技术防火墙在过滤数据包时，一般不关心（）

A、数据包的源地址

B、数据包的协议类型

C、数据包的目的地址

D、数据包的内容

**参考答案：D**

64、以下关于网络流量监控的叙述中，不正确的是（）

A、流量检测中所检测的流量通常采集自主机节点、服务器、路由器接口和路径等

B、数据采集探针是专门用于获取网络链路流量的硬件设备

C、流量监控能够有效实现对敏感数据的过滤

D、网络流量监控分析的基础是协议行为解析技术

**参考答案：C**

65、两个密钥三重DES加密：C=CK1[DK2[EK1[P]]],K1≠K2，其中有效的密钥为（）

A、56

B、128

C、168

D、112

**参考答案：D**

66、设在RSA的公钥密码体制中，公钥为（c，n）=（13,35），则私钥为（）

A、11

B、13

C、15

D、17

**参考答案：B**

67、杂凑函数SHAI的输入分组长度为（）比特

A、128

B、258

C、512

D、1024

**参考答案：C**

68、AES结构由以下4个不同的模块组成，其中（）是非线性模块

A、字节代换

B、行移位

C、列混淆

D、轮密钥加

**参考答案：A**

69、67mod119的逆元是（）

A、52

B、67

C、16

D、19

**参考答案：C**

70、在DES算法中，需要进行16轮加密，每一轮的子密钥长度为（）

A、16

B、32

C、48

D、64

**参考答案：C**

71-75（1）isthescienceofhidinginformation.Whereasthegoalofcryptographyistomakedataunreadablebyathirdparty.thegoalofsteganographyistohidethedatafromathirdparty.Inthisarticle,Iwilldiscusswhatsteganographyis,whatpurposesitserves,andwillprovideanexampleusingavailablesoftware.

Therearealargenumberofsteganographic（2）thatmostofusarefamiliarwith(especiallyifyouwatchalotofspymovies),rangingfrominvisibleinkandmicrodotstosecretingahiddenmessageinthesecondletterofeachwordofalargebodyoftextandspreadspectrumradiocommunication.Withcomputersandnetworks,therearemanyotherwaysofhidinginformations,suchas:

Covertchannels(c,g,Lokiandsomedistributeddenial-of-servicetoolsusetheInternetControl（3）Protocol,orICMP,asthecommunicationchannelbetweenthe“badguy”andacompromicyedsystem)

HiddentextwithinWebpages

Hidingfilesin“plainsight”(c,g.whatbetterplaceto“hide”afilethanwithanimportantsoundingnameinthec:\winntsystem32directory)

Nullciphers(c,g,usingthefirstletterofeachwordtoformahiddenmessageinanotherwiseinnocuoustext)

steganographytoday,however,issignificantlymore（4）thantheexampleaboutsuggest,allowingausertohidelargeamountsofinformationwithinimageandaudio.Theseformsofsteganographyoftenareusedinconjunctionwithcryptographysotheinformationisdoubleprotected;firstitisencryptedandthenhiddensothatanadvertisementfirst.findtheinformation(anoftendifficulttaskinandofitself)andthedecryptedit.

Thesimplestapproachtohidingdatawithinanimagefileiscalled（5）signatureinsertion.Inthismethod,wecantakethebinaryrepresentationofthehiddendataandthebitofeachbytewithinthecovertimage.Ifweareusing24-bitcolortheamountandwillbeminimumandindiscriminatetothehumaneye.

（1）A、Cryptography

B、Geography

C、Stenography

D、Steganography

（2）A、methods

B、software

C、tools

D、services

（3）A、Member

B、Management

C、Message

D、Mail

（4）A、powerful

B、sophistication

C、advanced

D、easy

（5）A、least

B、most

C、much

D、less

**参考答案：A、A、C、B、A**

二、案例分析

**试题一（共20分）**

阅读下列说明和图，回答问题1至问题3，将解答填入答题纸的对应栏内。

【说明】

研究密码编码的科学称为密码编码学，研究密码破译的科学称为密码分析学，密码编码学和密码分析学共同组成密码学。密码学作为信息安全的关键技术，在信息安全领域有着广泛的应用。

【问题1】（9分）

密码学的安全目标至少包括哪三个方面？具体内涵是什么？

【问题2】（3分）

对下列违规安全事件，指出各个事件分别违反了安全目标中的哪些项？

（1）小明抄袭了小丽的家庭作业。

（2）小明私自修改了自己的成绩。

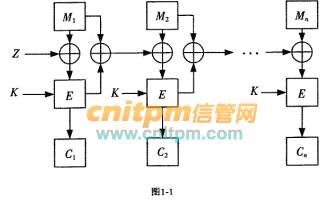
（3）小李窃取了小刘的学位证号码、登录口令信息、并通过学位信息系统更改了小刘的学位信息记录和登陆口令，将系统中小刘的学位信息用一份伪造的信息替代，造成小刘无法访问学位信息系统。

【问题3】（3分）

现代密码体制的安全性通常取决于密钥的安全，文了保证密钥的安全，密钥管理包括哪些技术问题？

【问题4】（5分）

在图1-1给出的加密过程中，Mi，i=1，2，…，n表示明文分组，Ci，i=1,2，…，n表示密文分组，Z表示初始序列，K表示密钥，E表示分组加密过程。该分组加密过程属于哪种工作模式？这种分组密码的工作模式有什么缺点？



**信管网参考答案：**

【问题一】

（1）保密性：保密性是确保信息仅被合法用户访问，而不被地露给非授权的用户、实体或过程，或供其利用的特性。即防止信息泄漏给非授权个人或实体，信息只为授权用户使用的特性。

（2）完整性：完整性是指所有资源只能由授权方或以授权的方式进行修改，即信息未经授权不能进行改变的特性。信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏和丢失的特性。

（3）可用性：可用性是指所有资源在适当的时候可以由授权方访问，即信息可被授权实体访问并按需求使用的特性。信息服务在需要时，允许授权用户或实体使用的特性，或者是网络部分受损或需要降级使用时，仍能为授权用户提供有效服务的特性。

【问题二】

（1）保密性

（2）完整性

（3）可用性

【问题三】

答：密钥管理包括密钥的产生、存储、分配、组织、使用、停用、更换、销毁等一系列技术问题。

【问题四】

明密文链接模式。

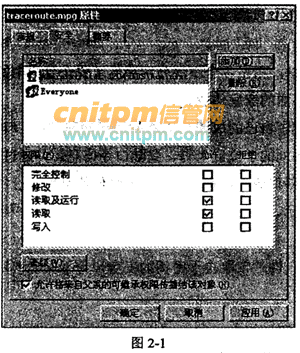
缺点：当Mi或Ci中发生一位错误时，自此以后的密文全都发生错误，即具有错误传播无界的特性，不利于磁盘文件加密。并且要求数据的长度是密码分组长度的整数倍，否则最后一个数据块将是短块，这时需要特殊处理。

**试题二（共10分）**

阅读下列说明和图，回答问题1至问题2，将解答填入答题纸的对应栏内。

【说明】

访问控制是对信息系统资源进行保护的重要措施，适当的访问控制能够阻止未经授权的用户有意或者无意地获取资源。访问控制一般是在操作系统的控制下，按照事先确定的规则决定是否允许用户对资源的访问。图2-1给出了某系统对客体traceroute.mpg实施的访问控制规则。



【问题1】（3分）

针对信息系统的访问控制包含哪些基本要素？

【问题2】（7分）

分别写出图2-1中用户Administrator对应三种访问控制实现方法，即能力表、访问控制表、访问控制矩阵下的访问控制规则。

**信管网参考答案：**

【问题1】

主体、客体、授权访问

【问题二】

能力表：

（主体）Administrator<（客体）traceroute.mpg：读取，运行>

访问控制表：

（客体）traceroute.mpg<（主体）Administrator：读取，运行>

访问控制矩阵：



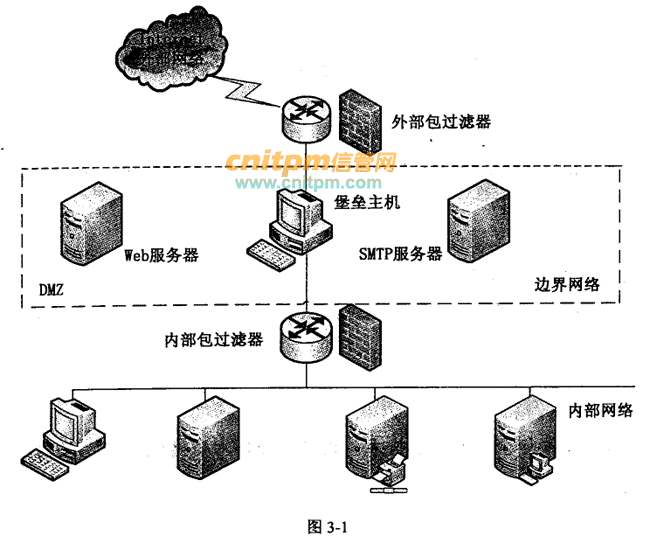
**试题三（共19分）**

阅读下列说明和图，回答问题1至问题3，将解答填入答题纸的对应栏内。

【说明】

防火墙是一种广泛应用的网络安全防御技术，它阻挡对网络的非法访问和不安全的数据传递，保护本地系统和网络免于受到安全威胁。

图3-1改出了一种防火墙的体系结构。



【问题1】（6分）

防火墙的体系结构主要有：

（1）双重宿主主机体系结构；

（2）（被）屏蔽主机体系结构；

（3）（被）屏蔽子网体系结构；

请简要说明这三种体系结构的特点。

【问题2】（5分）

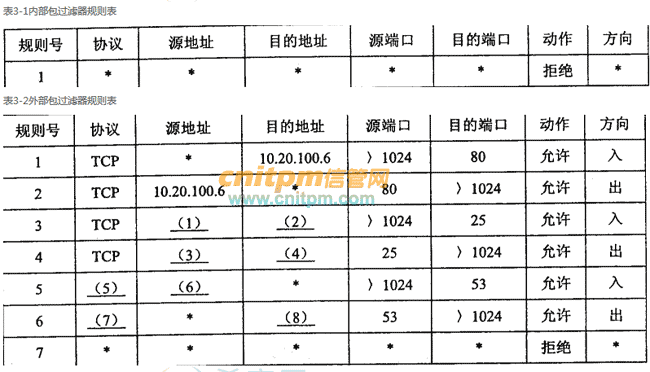
（1）图3-1描述的是哪一种防火墙的体系结构？

（2）其中内部包过滤器和外部包过滤器的作用分别是什么？

【问题3】（8分）

设图3-1中外部包过滤器的外部IP地址为10.20.100.1，内部IP地址为10.20.100.2，内部包过滤器的外部IP地址为10.20.100.3，内部IP地址为192.168.0.1，DMZ中Web服务器IP为10.20.100.6，SMTP服务器IP为10.20.100.8.

关于包过滤器，要求实现以下功能，不允许内部网络用户访问外网和DMZ，外部网络用户只允许访问DMZ中的Web服务器和SMTP服务器。内部包过滤器规则如表3-1所示。请完成外部包过滤器规则表3-2，将对应空缺表项的答案填入答题纸对应栏内。



**信管网参考答案：**

【问题一】

双重宿主主机体系结构：双重宿主主机体系结构是指以一台双重宿主主机作为防火墙系统的主体，执行分离外部网络与内部网络的任务。

被屏蔽主机体系结构：被屏蔽主机体系结构是指通过一个单独的路由器和内部网络上的堡垒主机共同构成防火墙，主要通过数据包过滤实现内外网络的隔离和对内网的保护。

被屏蔽子网体系结构：被屏蔽子网体系结构将防火墙的概念扩充至一个由两台路由器包围起来的周边网络，并且将容易受到攻击的堡垒主机都置于这个周边网络中。其主要由四个部件构成，分别为:周边网络、外部路由器、内部路由器以及堡垒主机。

【问题二】

（1）屏蔽子网体系结构。

（2）内部路由器：内部路由器用于隔离周边网络和内部网络，是屏蔽子网体系结构的第二道屏障。在其上设置了针对内部用户的访问过滤规划，对内部用户访问周边网络和外部网络进行限制。

外部路由器：外部路由器的主要作用在于保护周边网络和内部网络，是屏蔽子网体系结构的第一道屏障。在其上设置了对周边网络和内部网络进行访问的过滤规则，该规则主要针对外网用户。

【问题三】

（1）\*（2）10.20.100.8（3）10.20.100.8

（4）\*（5）UDP（6）10.20.100.3

（7）UDP（8）10.20.100.3

**试题四（共18分）**

阅读下列说明，回答问题1至问题4，将解答写在答题纸的对应栏内。

【说明】

用户的身份认证是许多应用系统的第一道防线、身份识别对确保系统和数据的安全保密及其重要，以下过程给出了实现用户B对用户A身份的认证过程。

1.B–>B：A

2.B–>A：{B，Nb}pk（A）

3.A–>B：b（Nb）

此处A和B是认证实体，Nb是一个随机值，pk（A）表示实体A的公钥、{B，Nb}pk（A）表示用A的公钥对消息BNb进行加密处理，b（Nb）表示用哈希算法h对Nb计算哈希值。

【问题1】（5分）

认证和加密有哪些区别？

【问题2】（6分）

（1）包含在消息2中的“Nb”起什么作用？

（2）“Nb”的选择应满足什么条件？

【问题3】（3分）

为什么消息3中的Nb要计算哈希值？

【问题4】（4分）

上述协议存在什么安全缺陷？请给出相应的解决思路。

**信管网参考答案：**

【问题一】

认证和加密的区别在于：加密用以确保数据的保密性，阻止对手的被动攻击，如截取，窃听等；而认证用以确保报文发送者和接收者的真实性以及报文的完整性，阻止对手的主动攻击，如冒充、篡改、重播等。

【问题二】

（1）Nb是一个随机值，只有发送方B和A知道，起到抗重放攻击作用。

（2）应具备随机性，不易被猜测。

【问题三】

哈希算法具有单向性，经过哈希值运算之后的随机数，即使被攻击者截获也无法对该随机数进行还原，获取该随机数Nb的产生信息。

【问题四】

攻击者可以通过截获h（Nb）冒充用户A的身份给用户B发送h（Nb）。

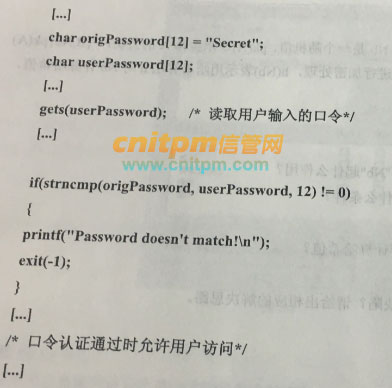
解决思路：用户A通过将A的标识和随机数Nb进行哈希运算，将其哈希值h（A，Nb）发送给用户B，用户B接收后，利用哈希函数对自己保存的用户标识A和随机数Nb进行加密，并与接收到的h（A，Nb）进行比较。若两者相等，则用户B确认用户A的身份是真实的，否则认为用户A的身份是不真实的。

**试题五（共8分）**

阅读下列说明和代码，回答问题1和问题2，将解答卸载答题纸的对应栏内。

【说明】

某一本地口令验证函数（C语言环境，X86\_32指令集）包含如下关键代码：某用户的口令保存在字符数组origPassword中，用户输入的口令保存在字符数组userPassword中，如果两个数组中的内容相同则允许进入系统。



【问题1】（4分）

用户在调用gets()函数时输入什么样式的字符串，可以在不知道原始口令“Secret”的情况下绕过该口令验证函数的限制？

【问题2】（4分）

上述代码存在什么类型的安全隐患？请给出消除该安全隐患的思路。

**信管网参考答案：**

【问题一】

只要输入长度为24的字符串，其前12个字符和后12个字符一样即可。

【问题二】

gets（）函数必须保证输入长度不会超过缓冲区，一旦输入大于12个字符的口令就会造成缓冲区溢出。

解决思路：使用安全函数来代替gets（）函数，或者对用户输入进行检查和校对，可通过if条件语句判断用户输入是否越界。