

2016 年下半年信息安全工程师 《案例分析》真题答案及解析

本资料由信管网(www.cnitpm.com)整理发布，供信管网学员使用！

信管网是专业软考中高级与 PMP 考试培训服务网站。提供了考试资讯、考试报名、成绩查询、资料下载、在线答题、考试培训、项目管理人才交流、企业内训等服务。

信管网资料库提供了备考软考的精品学习资料；信管网案例分析频道和论文频道拥有丰富的案例范例和论文范例，信管网考试中心拥有软考中高级历年真题和超过 5000 多道试题免费在线测试；信管网每年指导考生超 100000+人。

信管网——专业、专注、专心，成就你的项目管理师梦想！

信管网：www.cnitpm.com

信管网考试中心：www.cnitpm.com/exam/

信管网培训中心：www.cnitpm.com/wx/

注：本资料由信管网整理后提供给学员使用，未经许可，严禁商业使用。

信管网微信公众号



信管网客服微信号



**试题一、**

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，为了保证密钥的安全，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， M_i , $i=1, 2, \dots, n$ 表示明文分组， C_i , $i=1, 2, \dots, n$ 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？

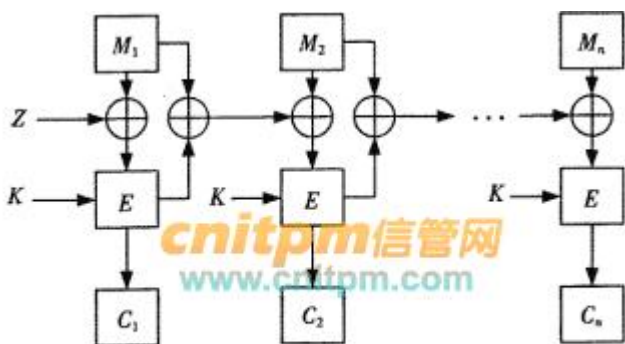


图1-1

信管网参考答案：

**【问题一】**

密码学的安全目标包括:保密性、完整性、可用性

(1)保密性:保密性是确保信息仅被合法用户访问,而不被暴露给非授权的用户、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。该加密过程属于 PCBC 模式。

PCBC 模式的缺点是:加密和解密错误传播无界: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,需要特殊处理。

缺点:当 M_i 或 C_i 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。

查看解析: www.cnitpm.com/st/2851526776.html



联系我们



往期真题下载 ↓ ↓



更多精品资料 ↓ ↓



在线考试题库 ↓ ↓



**试题二、**

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。



图 2-1

【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】

针对信息系统的访问控制包含主体、客体和授权访问三个要素。

【问题 2】



【问题 2】

能力表: 主体 Administrator: Traceroute.mpg: 读取, 运行。

访问控制列表: 客体 traceroute.mpg<administrator,rx>。

访问控制矩阵:

	Traceroute.mpg
Administrator	r, x

注:

能力表和访问控制列表也可采用链表形式表示, 具体如下:

能力表: Administrator



Traceroute.mpg: r, x

访问控制列表: Traceroute.mpg



Administrator: r, x

查看解析: www.cnitpm.com/st/2851629359.html

往期真题下载 ↓ ↓



更多精品资料 ↓ ↓



在线考试题库 ↓ ↓



**试题三、**

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 给出了一种防火墙的体系结构。

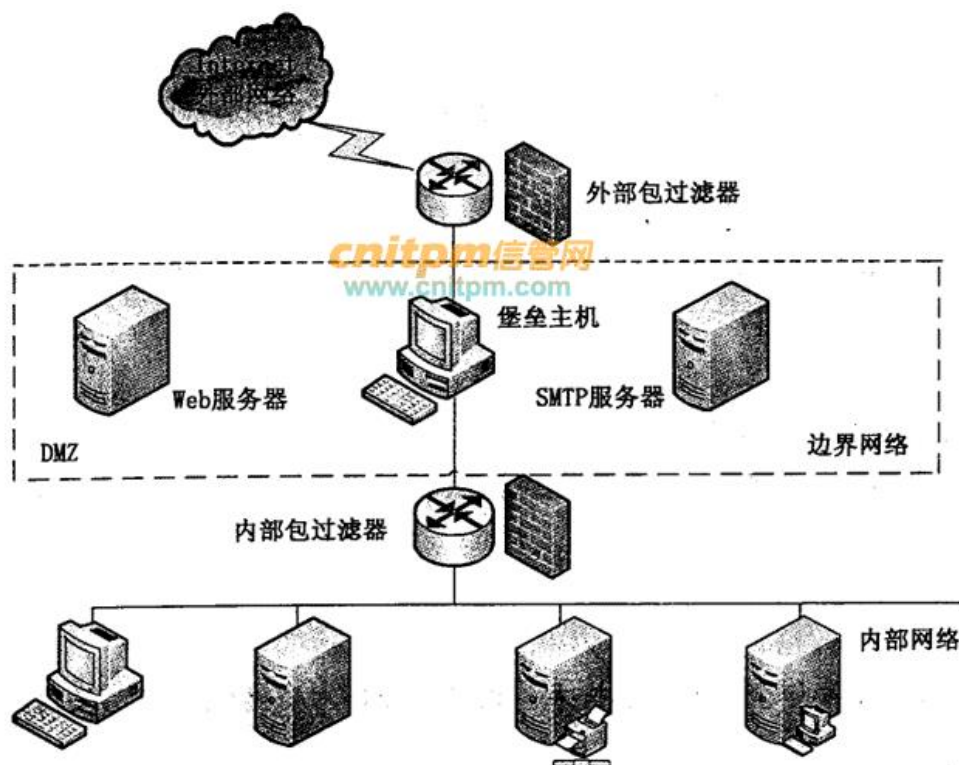


图 3-1

【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。

表3-1内部包过滤器规则表

规则号	协议	源地址	目的地址	源端口	目的端口	动作	方向
1	*	*	*	*	*	拒绝	*

表3-2外部包过滤器规则表

规则号	协议	源地址	目的地址	源端口	目的端口	动作	方向
1	TCP	*	10.20.100.6	> 1024	80	允许	入
2	TCP	10.20.100.6	*	80	> 1024	允许	出
3	TCP	(1)	(2)	> 1024	25	允许	入
4	TCP	(3)	(4)	25	> 1024	允许	出
5	(5)	(6)	*	> 1024	53	允许	入
6	(7)	*	(8)	53	> 1024	允许	出
7	*	*	*	*	*	拒绝	*

信管网参考答案：

【问题 1】

(1) 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。

(2) (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。

(3) (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。

【问题 2】

(1) 该图描述的是(被)屏蔽子网体系结构。



(2) 外部包过滤器主要用于保护周边网路和内部网络,是屏蔽子网体系结构的第一道屏障。内部包过滤器主要用于隔离周边网路和内部网络,是屏蔽子网体系结构的第二道屏障。

【问题 3】

- (1)*
- (2) 10.20.100.8
- (3) 10.20.100.8
- (4)*
- (5) UDP
- (6) 10.20.100.*
- (7) UDP
- (8) 10.20.100.*

查看解析: www.cnitpm.com/st/285173752.html

往期真题下载 ↓ ↓



更多精品资料 ↓ ↓



在线考试题库 ↓ ↓



**试题四、**

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 \rightarrow B: A

2. B \rightarrow A: $\{B, Nb\}_{pk(A)}$

3. A \rightarrow 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 1】

认证与加密的区别在于：加密用以确保数据的保密性，阻止对手的被动攻击；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。

【问题 2】

(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) Nb 的取值应当随机和不可预测

【问题 3】

计算哈希值是为了使中间人无法知道 Nb 的产生信息。

【问题 4】



联系我们



存在重放攻击和中间人攻击的安全缺陷。针对重放攻击的解决思路是加入时间戳、验证码等信息；针对中间人攻击的解决思路是加入针对身份的验证。

查看解析：www.cnitpm.com/st/2851829992.html

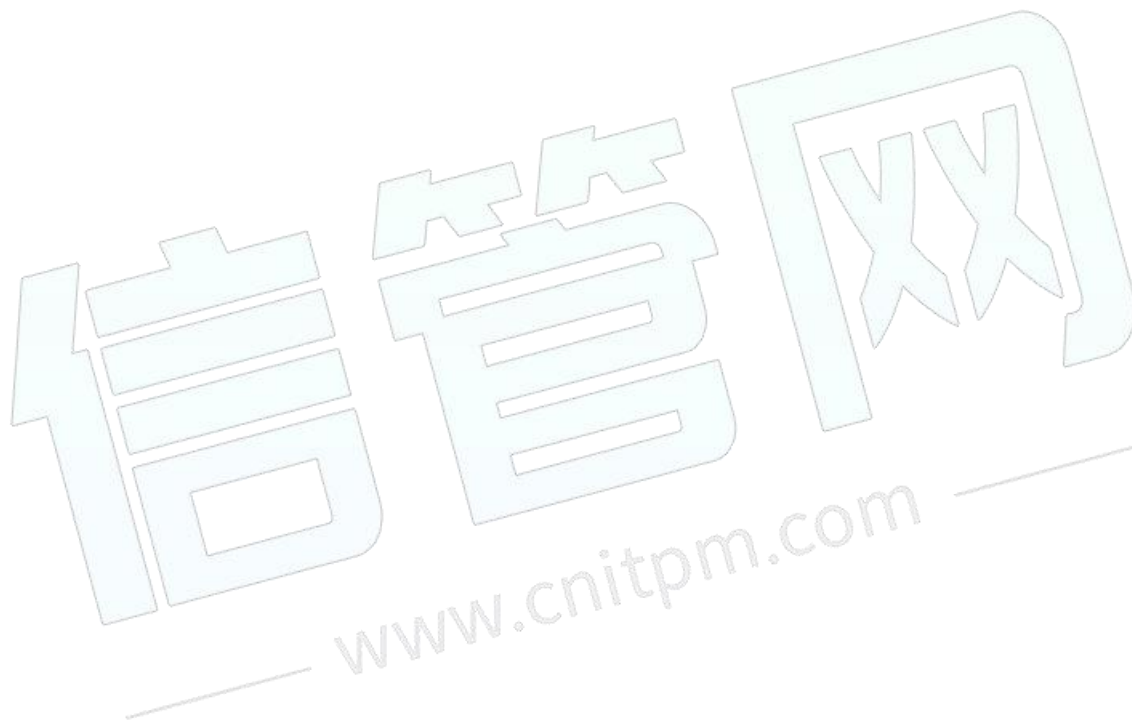
往期真题下载 ↓ ↓



更多精品资料 ↓ ↓



在线考试题库 ↓ ↓





试题五、

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。

```
[...]  
char origPassword[12] = "Secret";  
char userPassword[12];  
[...]  
gets(userPassword); /* 读取用户输入的口令*/  
[...]  
if(strncmp(origPassword, userPassword, 12) != 0)  
{  
    printf("Password doesn't match!\n");  
    exit(-1);  
}  
[...]  
/* 口令认证通过时允许用户访问*/  
[...]
```

【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 1】

输入字符串的样式只要满足: 前 12 个字符和后续的 12 个字符一样; 就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

即字符串形如:



str1	str2	str3
------	------	------

其中, str1 与 str3 前 12 个字符完全一致, str2 的长度刚好可以填充 userPassword 和 origPassword 之间堆栈缓冲区的位置, 且 str1str2str3 所形成的字符串不会引起代码运行崩溃。

【问题 2】

存在缓冲区溢出攻击的安全隐患。解决思路是检查用户输入的口令的长度信息。

查看解析: www.cnitpm.com/st/2851921939.html

往期真题下载 ↓ ↓



更多精品资料 ↓ ↓



在线考试题库 ↓ ↓

