2017 年上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/

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，回答问题 1 至问题 3，将解答写在答题纸的对 应栏内。

【说明】

安全目标的关键是实现安全的三大要素:机密性、完整性和可用性。对于一般性的信 息类型的安全分类有以下表达形式:

{（机密性，影响等级），（完整性，影响等级），（可用性，影 响等级）}

在上述表达式中，"影响等级"的值可以取为低 (L)、中(M)、高(H) 三级以及不适用 (NA)。

【问题 1】。 (6 分)

请简要说明机密性、完整性和可用性的含义。

【问题 2】(2 分)

对于影响等级"不适用"通常只针对哪个安全要素?

【问题 3 】(3 分)

如果一个普通人在它的个人 Web 服务器上管理其公开信息。请 问这种公开信息的安全分类是什么?

信管网参考答案:

【问题 1)】

机密性是确保信息仅被合法用户访问,而不被泄露给非授权用户、实体或过程,或供其利用的特性。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。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。

【问题 2】

机密性

【问题 3】

(机密性,NA),(完整性,M),(可用性,M)

查看解析：www.cnitpm.com/st/327583719.html

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，回答问题 1 和问题 2，将解答写在答题纸的对 应栏内。

【说明】

Windows 系统的用户管理配置中，有多项安全设置，如图 2-1 所示。

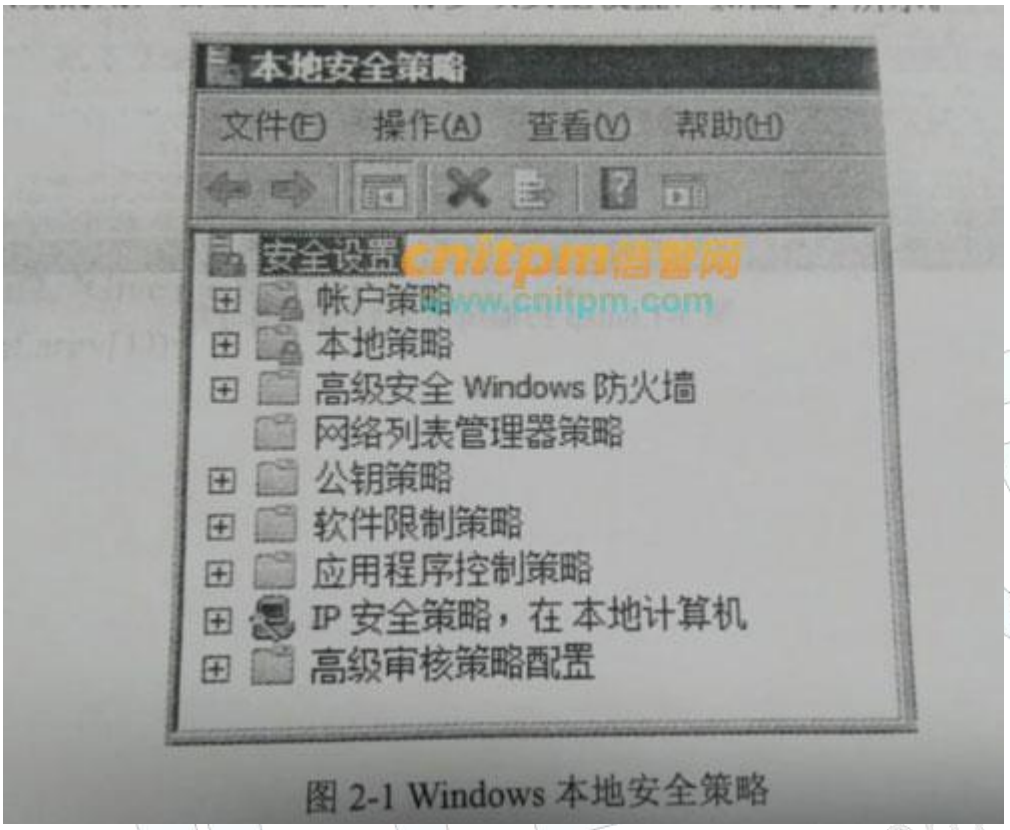


图 2-1 Windows 本地安全策略

【问题 1】(3 分)

请问密码和帐户锁定安全选项设置属于图中安全设置的哪一项?

【问题 2】(3 分)

Windows 的密码策略有一项安全策略就是要求密码必须符合复杂 性要求，如果启用此策略， 那么请问:用户 Administrator 拟选取的以下六个密码中的哪 些符合此策略?

123456 Admin123 Abcd321 Admin@ test123! 123@host

信管网参考答案:

【问题 1】

账户策略。

【问题 2】

Abcd321

test123!

123(@host

查看解析：www.cnitpm.com/st/327598118.html

试题三、

阅读下列说明，回答问题 1 至问题 7，将解答写在答题纸的对应栏内。

【说明】

扫描技术是网络攻防的一种重要手段，在攻和防当中都有其重要意义。nmap 是一个 开放源码的网络扫描工具，可以查看网络系统 中有哪些主机在运行以及哪些服务是开放的。 namp 工具的命令选 项: sS 用于实现 SYN 扫描，该扫描类型是通过观察开放端口和关闭 端口对探测分组的响应来实现端口扫描的。请根据图 3-1 回答下列 问题。

【问题 1】 (2 分)

此次扫描的目标主机的 IP 地址是多少?

【问题 2】(2 分)

SYN 扫描采用的传输层协议名字是什么?

【问题 3】 (2 分)SYN 的含义是什么?

【问题 4】 (4 分)

目标主机开放了哪几个端口?简要说明判断依据。

【问题 5】(3 分)

每次扫描有没有完成完整的三次握手?这样做的目的是什么?

【问题 6】(5 分)

补全表 3-1 所示的防火墙过滤器规则的空(1) - (5)，达到防火墙禁止此类扫描流量进入和处出

网络 ，同时又能允许网内用户访问 外部网页服务器的目的。

表 3-1 防火墙过滤器规则表

表 3-1 防火墙过滤器规则表

规则号	协议	源地址	目的地址	源端口	目的端口	ACK	动作
1	TCP	*	192.168.220.1/24	*	*	(4)	拒绝
2	TCP	192.168.220.1/24	*	> 1024	(3)	*	允许
3	(1)	192.168.220.1/24	*	> 1024	53	*	允许
4	UDP	*	192.168.220.1/24	53	> 1024	(5)	允许
5	(2)	*	*	*	*	*	拒绝

【问题 7】 (2 分)

简要说明为什么防火墙需要在进出两个方向上对据数据包进行过滤。

信管网参考答案：

【问题 1】(2 分)

192.168.220.1

【问题 2】(2 分)

TCP 或者传输控制协议

【问题 3】(2 分)

TCP 协议的控制比特,表示请求同目标主机建立连接。

【问题 4】(4 分)

135 和 139。这两个端口对 SYN 请求包返回的是 SYN 和 ACK 肯定应答分组,表示端口是开放的。

【问题 5】(3 分)

没有。第三个握手包没有发送,不完成整个握手过程,是避免扫描行为被目标主机记录在案,逃避检测,实现隐蔽扫描。

【问题 6】(5 分,每空 1 分)

(1)UDP

(2)*

(3)80

(4)0

(5)1

【问题 7】(2 分)

在进入方向过滤是为了防止被人攻击，而在出口方向过滤则是为了防止自己成击的源头或者跳板。

查看解析：www.cnitpm.com/st/327608324.html

试题四、

阅读下列说明，回答问题 1 至问题 5，将解答写在答题纸的对 应栏内。

【说明】

DES 是一种分组密码，已知 DES 加密算法的某个 S 盒如表 4-1 所示。

表 4-1 S 盒

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	7	13	14	3	0	6	9	(1)	1	2	8	5	11	12	4	15
1	13	8	11	5	(2)	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	(3)	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	(4)	12	7	2	14

【问题 1】 (4 分)

请补全该 S 盒，填补其中的空(1) - (4)，将解答写在答题纸的对应栏内。

【问题 2】 (2 分)

如果该 S 盒的输入为 110011，请计算其二进制输出。

【问题 3】(6 分)

DES 加密的初始置换表如下：

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

置换时，从左上角的第一个元素开始，表示输入的明文的第 58 位置换成输出的第 1 位，输入明文的第 50 位置换成输出的第 2 位，从左至右，从上往下，依次类推。

DES 加密时，对输入的 64 位明文首先进行初始置换操作。

若置换输入的明文 M=0123456789ABCDEF(16 进制)，请计算其输出(16 进制表示)。

【问题 4】(2 分)

如果有简化的 DES 版本，其明文输入为 8 比特，初始置换表 IP 如下：

IP：2 6 3 1 4 8 5 7

请给出其逆初始置换表。

【问题 5】(2 分)

DES 加密算法存在一些弱点和不足，主要有密钥太短和存在弱密钥。请问，弱密钥的定义是什么？

信管网参考答案：

【问题 1】

(1)10

(2)6

(3)1

(4)11

【问题 2】

0100

【问题 3】

M=0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1011 1100 1101 1110

IP=1100 1100 0000 0000 1100 1100 1111 1111 1111 0000 10101010 1111 0000 1010 1010

P= CcoOCCFF FOAAFOAA(十六进制)

【问题 4】

IP-1: 4 1 3 5 7 2 8 6

【问题 5】

若 k 为给定的密钥,如果由 k 所产生的子密钥都相同,则 k 称为弱密钥。

查看解析：www.cnitpm.com/st/3276125797.html

试题五、

阅读下列说明，回答问题 1 和问题 2，将解答写在答题纸的对应栏内。

【说明】

在公钥体制中，每一用户 U 都有自己的公开密钥 PKu 和私钥 SKu 。如果任意两个用户 A 和 B 按以下方式通信：

A 发给 B 消息 [EpKB (m)，A] 。

其中 Ek(m)代表用密钥 K 对消息 m 进行加密。

B 收到以后，自动向 A 返回消息【EPkA(m),B】，以使 A 知道 B 确实收到消息 m。

【问题 1】 (4 分)

用户 C 怎样通过攻击手段获取用户 A 发送给用户 B 的消息 m。

【问题 2】 (6 分)

若通信格式变为:

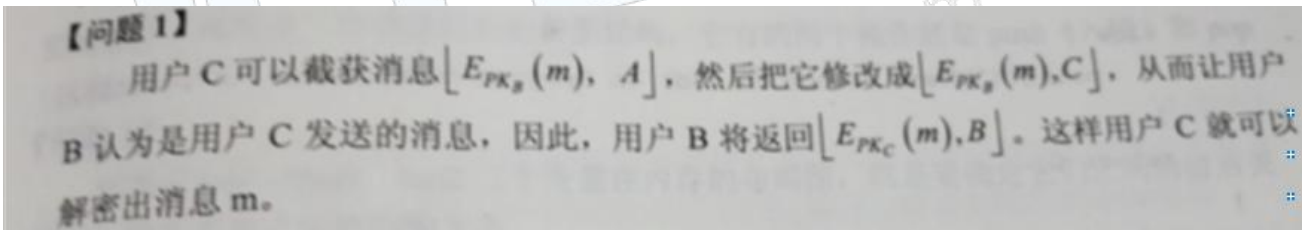
A 给 B 发消息:EPKB(ESKA(m)，m ，A)

B 给 A 发消息: EpKA(EsKN (m)，m，B)

这时的安全性如何?请分析 A，B 此时是如何相互认证并传递消息的。

信管网参考答案：

【问题 1】



【问题 2】

此时,由于消息是用用户 A 的私钥签名的,而且用户无法看到其中的任何内容,包括 m 和 A。因此用户 C 无法获得消息 m。存在重放攻击。

用户 B(只能是用户 B)可以通过用用户 A 的公钥来验证消息的来源和完整性,如果用 A 的公钥解密出来的消息 m 和用 B 的私钥解密出来的消息 m 相同,则可认为消息确实是 A 发送的。同样用户 A 也可以利用 $E_{PK_A}\left(E_{SK_B}(m), m, B\right)$ 来验证用户 B 的身份

查看解析：www.cnitpm.com/st/3276228341.html

试题六、

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】

基于 Windows32 位系统分析下列代码，回答相关问题 。

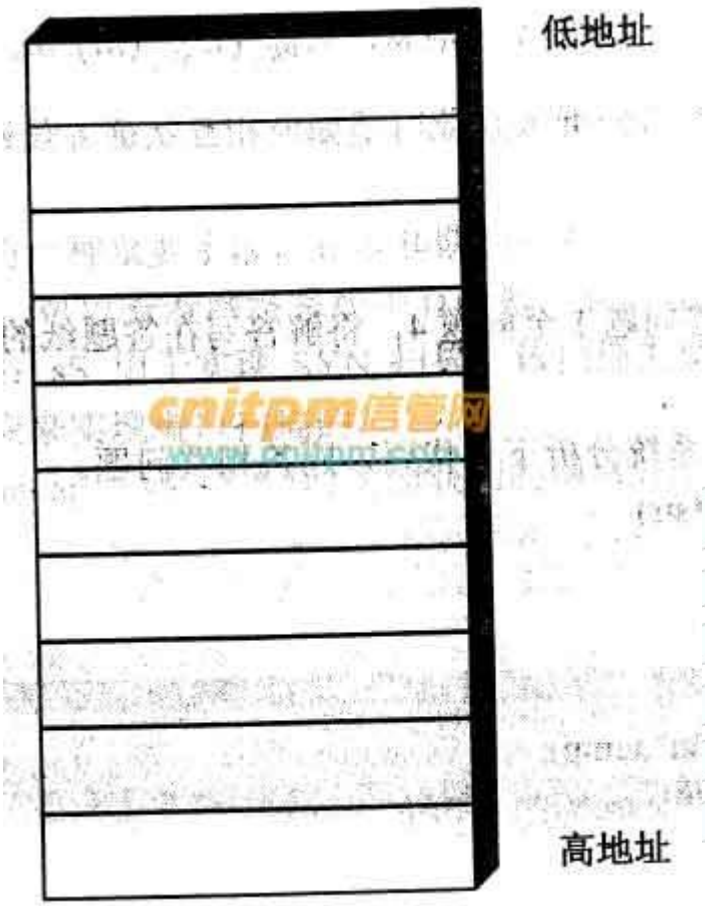
```
void Challenge(char *str)
{
char temp[9]={0};
strncpy(temp, str, 8);
printf("temp=%s\n", temp);
if(strcmp(temp"Please!@")==0){
printf("KEY: ****");
}
}
int main(int argc, char *argv[ ])
{
Char buf2[16]
Int check=1;
Char buf[8]
Strcpy (buf2, "give me key! !");
strcpy(buf, argv[1]);
if(check==65) {
Challenge(buf);
}
else {
printf("Check is not 65 (%d) \n Program terminated!!\n", check);
}
Return 0;
}
```

【问题 1】(3 分)

main 函数内的三个本地变量所在的内存区域称为什么?它的两个最基本操作是什么？

【问题 2】(3 分)

画出 buf，check，buf2 三个变量在内存的布局图。



【问题 3】(2 分)

应该给程序提供什么样的命令行参数值(通过 argv 变量传递)才能使程序执行流程进入判断语句 If(check=65)....然后调用 challenge( )函数。

【问题 4】(4 分)

上述代码所存在的漏洞名字是什么，针对本例代码，请简要说明如何修正上述代码以修补次漏洞。

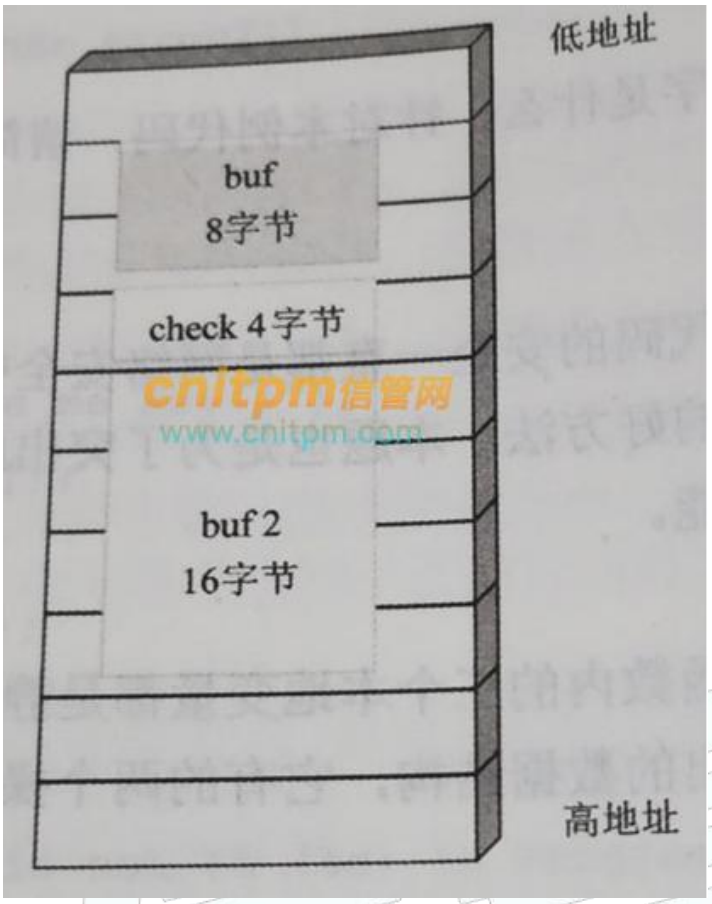
信管网参考答案：

【问题 1】

堆栈，push(压栈)和 pop(弹栈)操作

【问题 2】

变量的先后关系、每个变量所占空间、增长方向(数组)



【问题 3】

覆盖超过 buf 数组个字节，也就是输入参数形如:********A。注意大小端。

前面 8 个任意的非零字符都可以,后跟一个大写的 A 字符,因为 A 字符的 ASCI 码值等于 65。

【问题 4】

缓存溢出或者栈溢出。

对输入参数的长度进行检查。

查看解析：www.cnitpm.com/st/327636549.html