全国计算机技术与软件专业技术资格（水平）考试

2017 年上半年 信息安全工程师 下午试卷 I

（考试时间 14:00～16:30 共 150 分钟）

请按下述要求正确填写答题纸

1. 本试卷共五道题，全部为必答题，每题 25 分，满分 75 分。
2. 在答题纸的指定位置填写你所在的省、自治区、直辖市、计划单列市的名称。
3. 在答题纸的指定位置填写准考证号、出生年月日和姓名。
4. 答题纸上除填写上述内容外只能写解答。
5. 解答时字迹务必清楚，字迹不清时，将不评分。

2017 年上半年信息安全工程师下午案例分析试题一真题与答案(共 11 分)

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?

试题一信管网参考答案：

【问题 1】

（1）机密性：维护对信息访问和公开经授权的限制，包括保护个人隐私和私有的信息。

（2）完整性：防止信息不适当的修改和毁坏，包括保证信息的不可抵赖性和真实性。

（3）可用性：保证信息及时且可靠的访问和使用。

【问题 2】

“不适用”通常针对机密性。

【问题 3】：

{（机密性，NA），（完整性，M），（可用性，M）}

最终答案以信管网题库答案为准：http://www.cnitpm.com

2017 年上半年信息安全工程师下午案例分析试题二真题与答案（共 6 分）

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。

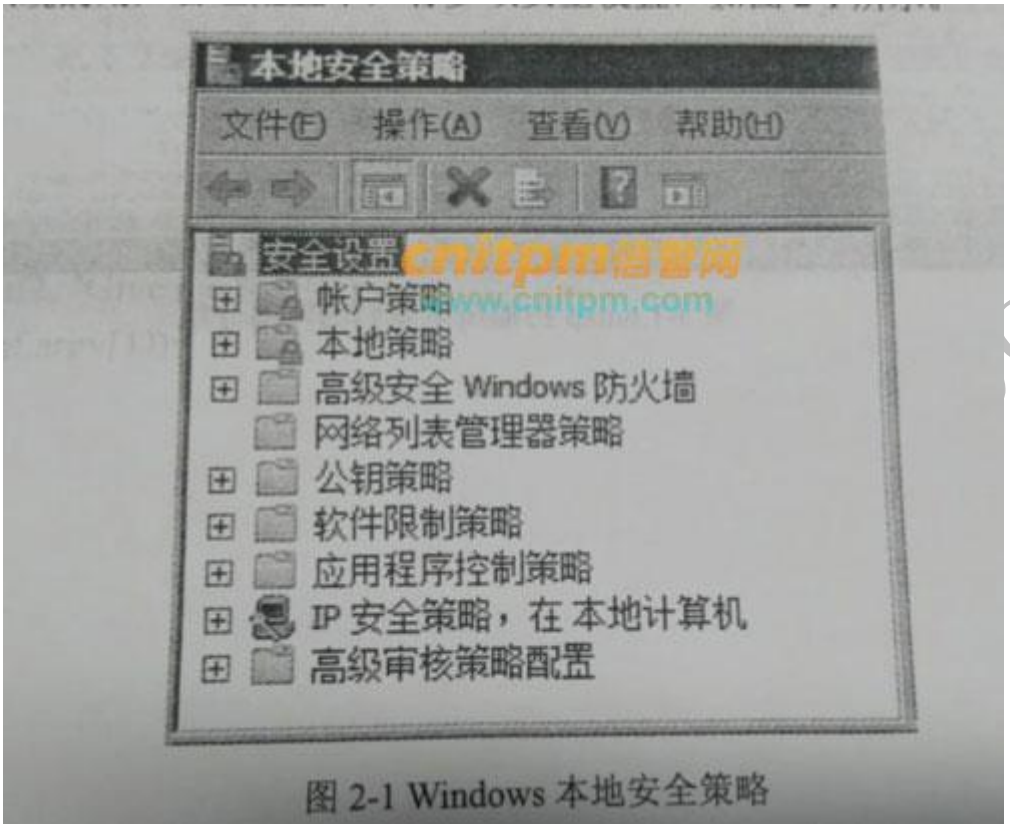

图 2-1 Windows 本地安全策略

【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

试题二信管网参考答案：

【问题 1】

帐号策略

【问题 2】

Abcd321 test123! 123@host

最终答案以信管网题库答案为准：http://www.cnitpm.com

2017 年上半年信息安全工程师下午案例分析试题三与答案(共 20 分)

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。

图 3-1 是在执行命令 nmap -sS *.*.*.*时所捕获到的网络分组。

97	192.168.220.129	192.168.220.1	64442→143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
100	192.168.220.1	192.168.220.129	143→64442 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
101	192.168.220.129	192.168.220.1	64442→135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
102	192.168.220.1	192.168.220.129	135→64442 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
103	192.168.220.129	192.168.220.1	64442→135 [RST] Seq=1 Win=0 Len=0
104	192.168.220.129	192.168.220.1	64442→139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
105	192.168.220.1	192.168.220.129	139→64442 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
106	192.168.220.129	192.168.220.1	64442→139 [RST] Seq=1 Win=0 Len=0
107	192.168.220.129	192.168.220.1	64442→443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
108	192.168.220.1	192.168.220.129	443→64442 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
109	192.168.220.129	192.168.220.1	64442→140 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
110	192.168.220.1	192.168.220.129	140→64442 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
111	192.168.220.129	192.168.220.1	64442→150 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
112	192.168.220.1	192.168.220.129	150→64442 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
113	192.168.220.129	192.168.220.1	64442→130 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
114	192.168.220.1	192.168.220.129	130→64442 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
115	192.168.220.129	192.168.220.1	64442→138 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
116	192.168.220.1	192.168.220.129	138→64442 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
117	192.168.220.129	192.168.220.1	64442→141 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
118	192.168.220.1	192.168.220.129	141→64442 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
119	192.168.220.129	192.168.220.1	64442→140 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
120	192.168.220.1	192.168.220.129	140→64442 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

【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 外部罔页 务器的目的。

表 3-1 防火墙过滤器规则表

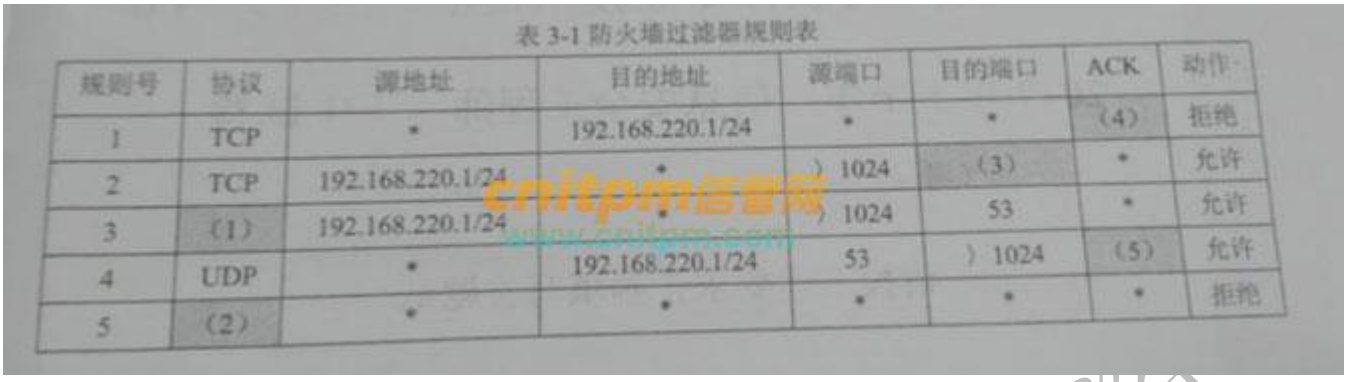

表 3-1 防火墙过滤器规则表

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。

试题三信管网参考答案：

【问题 1】

192.168.220.1

【问题 2】

TCP 协议

【问题 3】

同步信号，是 TCP/IP 建立连接时使用的握手信号。

【问题 4】

目标主机开放的端口为：135、139

判断依据：如果端口开放，目标主机会响应扫描主机的 SYN/ACK 连接请求；如果端口关闭，则目标主机回向扫描主机发送 RST 的响应。

【问题 5】

没有完成，这样做即使日志中对扫描有所记录，但是尝试进行连接的记录也要比全扫描少得多

【问题 6】

(1) UDP (2) * (3) 80 (4) 0 (5) 1

【问题 7】

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为攻击的源头或者跳板

2017 年上半年信息安全工程师下午案例分析试题四与答案（共 16 分）

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，表示输入的铭文的第 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？

试题四信管网参考答案：

【问题 1】

（1）10　（2）6　（3）1　（4）11

【问题 2】

0100

【问题 3】

M = (0123456789ABCDEF)16 = (00000001 00100011 01000101 01100111 10001001 10101011 11001101 11101111)2

经过 IP 置换，结果为：

M’ =（11001100 00000000 11001100 11111111 11110000 10101010 11110000 10101010）2

=（CC00CCFF0AAF0AA）16

【问题 4】

4 1 3 5 7 2 8 6

【问题 5】

弱密钥不受任何循环移位的影响，并且只能得到相同的子密钥，由全 0 或全 1 组成的密钥显然是弱密钥，子密钥生成过程中被分割的两部分分别为全 0 或全 1 时也是弱密钥。

2017 年上半年信息安全工程师下午案例分析试题五与答案（共 10 分）

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。

试题五信管网参考答案：

【问题 1】

攻击用户 C 可以通过以下手段获取报文 m：

1.用户 C 截获消息：（EPKB（m），A）

2.用户 C 篡改消息：（EPKB（m），C）

3.用户 B 返回消息：（EPKC（m），B）

4.用户 C 成功解密，最后得到明文 m。

【问题 2】

安全性提高了，能实现加密和认证的双重任务。

第一步，A 发给 B 消息是 A 首先用自己的秘密钥 SKA 对消息 m 加密，用于提供数字签名，再用接收方的公开钥 PKB 第 2 次加密，密文中包括明文的信息和 A 的身份信息。

第二步，接收方 B 收到密文，用自己的私钥先解密，再用对方的公钥验证发送方的身份是 A，实现了 B 对 A 的认证，并获取了明文。

第三步，B 发给 A 消息是 B 首先用自己的私钥 SKB 对消息 m 加密并签名，再用 A 的公开钥 PKA 第 2 次加密，密文中包括明文的信息和 A 的身份信息，还有 B 对接收的 m 的签名密文。

第四步，只有 A 才能用自己的私钥打开 B 送过来的密文，并且验证是 B 的签名，实现了 A 对 B 的认证，当 A 看见原样返回的 m，就知道 B 收到了 A 发送的明文 m 了。

2017 年上半年信息安全工程师下午案例分析试题六与答案（共 12 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】

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。

试题六信管网参考答案：

【问题 1】

1、堆栈。2、PUSH 和 POP。

【问题 2】

【问题 3】

用户输入 9 个字符的字符串，使其满足条件：前 8 个字符为任意字符和第 9 个字符为大写字母 A；

【问题 4】

缓冲区溢出。使用安全函数 strncpy（）来代替 strcpy（）函数。

最终答案以信管网题库答案为准：http://www.cnitpm.com