2020 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/

信管网微信公众号

信管网客服微信号

试题一(共 14 分)

阅读下列说明，回答问题 1 至问题 6，将解答填入答题纸的对应栏内。

【说明】

Linux 系统通常将用户名相关信息存放在/etc/passwd 文件中，假如有/etc/passwd 文件的部分内容如下，请回答相关问题。

```
security@ubuntu：~$ cat/etc/passwd
user1：x：0：0：user：/home/user1：/bin/bash
user2：x：1000：1000：ubuntu64：/home/user2：/bin/bash
daemon：x：1：1：daemon：/usr/sbin：/usr/sbin/nologin
bin：x：2：2：bin：/bin：/usr/sbin/nologin
sys：x：3：3：sys：/dev：/usr/sbin/nologin
sync：x：4：65534：sync：/bin：/bin/sync
```

【问题 1】(2 分)

口令字文件/etc/passwd 是否允许任何用户访问?

【问题 2】(2 分)

根据上述/etc/passwd 显示的内容，给出系统权限最低的用户名字。

【问题 3】(2 分)

在 Linux 中，/etc/passwd 文件中每一行代表一个用户，每行记录又用冒号(：)分隔为 7 个字段，请问 Linux 操作系统是根据哪个字段来判断用户的?

【问题 4】(3 分)

根据上述/etc/passwd 显示的内容，请指出该系统中允许远程登录的用户名。

【问题 5】(2 分)

Linux 系统把用户密码保存在影子文件中，请给出影子文件的完整路径及其名字。

【问题 6】(3 分)

如果使用 Is-al 命令查看影子文件的详细信息，请给出数字形式表示的影子文件访问权限。

信管网参考答案：

【问题 1】

允许

【问题 2】

user 2

【问题 3】

第三个字段或者 UID 字段

【问题 4】

user 1, user 2,sync

【问题 5】

/etc/shadow

【问题 6】

640 或者 600 或者 400 或者 000

查看解析：www.cnitpm.com/st/5024219851.html

试题二(共 20 分)

阅读下列说明，回答问题 1 至问题 8，将解答填入答题纸的对应栏内。

【说明】

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。密码学中，根据加密和解密过程所采用密钥的特点可以将密码算法分为两类：对称密码算法和非对称密码算法。此外，密码技术还用于信息鉴别、数据完整性检验、数字签名等。

【问题 1】(3 分)

信息安全的基本目标包括：真实性、保密性、完整性、不可否认性、可控性、可用性、可审查性等。密码学的三大安全目标 C.I.A 分别表示什么?

【问题 2】(3 分)

RSA 公钥密码是一种基于大整数因子分解难题的公开密钥密码。对于 RSA 密码的参数：p.q，n，(n)，e，d，哪些参数是可以公开的?

【问题 3】(2 分)

如有 RSA 密码算法的公钥为(55，3)，请给出对小王的年龄 18 进行加密的密文结果。

【问题 4】(2 分)

对于 RSA 密码算法的公钥(55，3)，请给出对应私钥。

【问题 5】(2 分)

在 RSA 公钥算法中，公钥和私钥的关系是什么?

【问题 6】(2 分)

在 RSA 密码中，消息 m 的取值有什么限制?

【问题 7】(3 分)

是否可以直接使用 RSA 密码进行数字签名?如果可以，请给出消息 m 的数字签名计算公式。如果不可以，请给出原因。

【问题 8】(3 分)

上述 RSA 签名体制可以实现问题 1 所述的哪三个安全基本目标?

信管网参考答案：

【问题 1】

保密性、完整性、可用性。

【问题 2】

n，e

【问题 3】

2

【问题 4】

(55，27)

【问题 5】

e×d=1modp (n)；一个加密另一个可以解开；从一个密钥无法推导出另一个。【问题 6】

消息 m 的十进制表示值小于 n 的值。【问题 7】

可以。

签名：用私钥加密；验证：用公钥解密。签

名=memodn

【问题 8】

真实性、保密性、完整性

查看解析：www.cnitpm.com/st/5024315145.html

试题三、

【说明】防火墙作为网络安全防护的第一道屏障，通常用一系列的规则来实现网络攻击数据包的过滤。

【问题 1】(3 分)

图 3-1 给出了某用户 Widows 系统下的防火墙操作界面， 请写出 Windows 下打开以下界面的操作步骤。

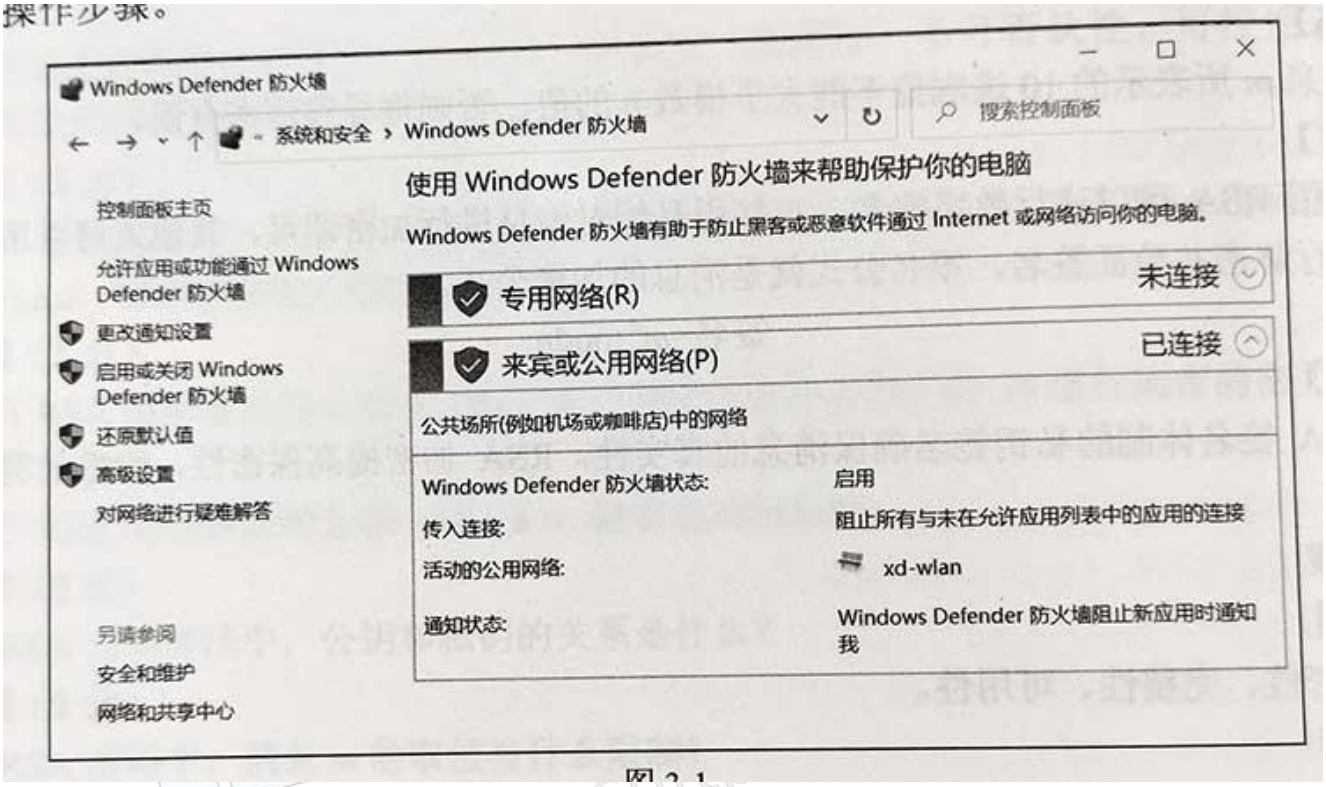


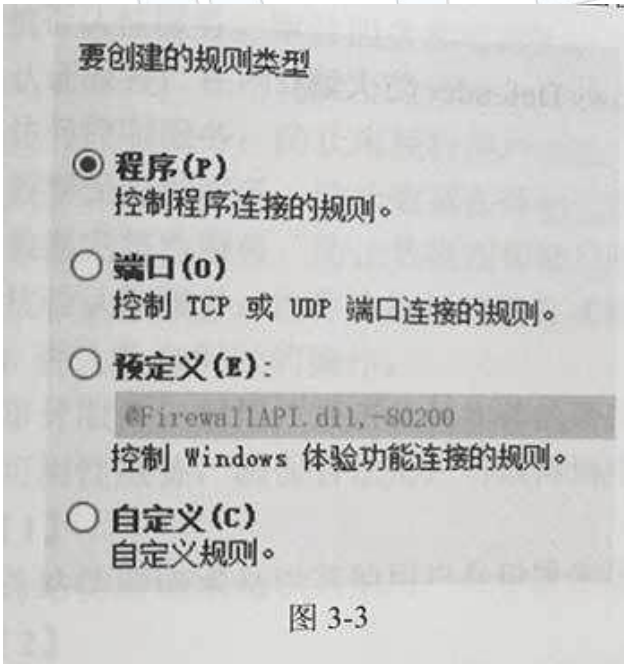
图 3-1

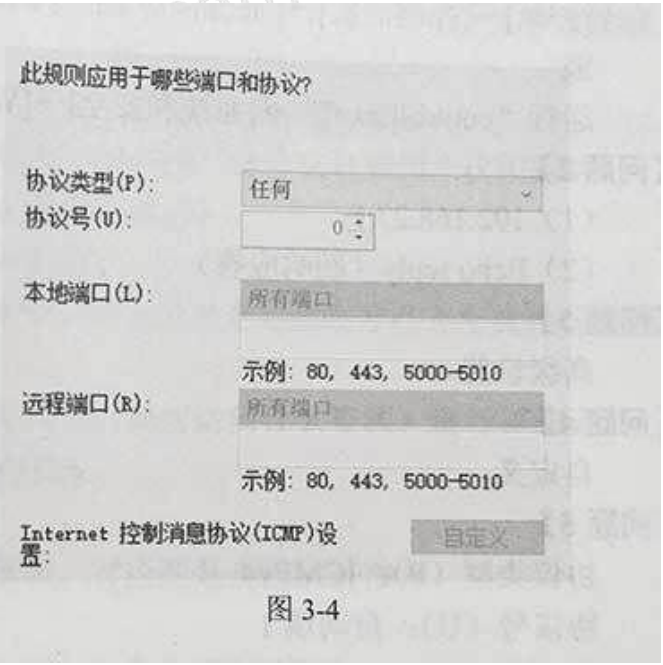
【问题 2】(4 分)

Smurf 拒绝服务攻击结合 IP 欺骗和 ICMP 回复方法使大量网络数据包充斥目标系统， 引起目标系统拒绝为正常请求提供服务。请根据图 3-2 回答下列问题。

(1)上述攻击针对的目标 IP 地址是多少?

(2) 在上述攻击中， 受害者将会收到 ICMP 协议的哪一种数据包?





```
Source          Destination      Protocol  Length  Info
192.168.27.1    192.168.27.255   ICMP          60  Echo (ping) request  id=0x0000, seq=0/0, ttl=64
192.168.27.1    192.168.27.255   ICMP          60  Echo (ping) request  id=0x0000, seq=0/0, ttl=64
192.168.27.1    192.168.27.255   ICMP          60  Echo (ping) request  id=0x0000, seq=0/0, ttl=64
192.168.27.1    192.168.27.255   ICMP          60  Echo (ping) request  id=0x0000, seq=0/0, ttl=64
192.168.27.1    192.168.27.255   ICMP          60  Echo (ping) request  id=0x0000, seq=0/0, ttl=64
192.168.27.1    192.168.27.255   ICMP          60  Echo (ping) request  id=0x0000, seq=0/0, ttl=64
192.168.27.1    192.168.27.255   ICMP          60  Echo (ping) request  id=0x0000, seq=0/0, ttl=64
192.168.27.1    192.168.27.255   ICMP          60  Echo (ping) request  id=0x0000, seq=0/0, ttl=64
192.168.27.1    192.168.27.255   ICMP          60  Echo (ping) request  id=0x0000, seq=0/0, ttl=64
192.168.27.1    192.168.27.255   ICMP          60  Echo (ping) request  id=0x0000, seq=0/0, ttl=64
192.168.27.1    192.168.27.255   ICMP          60  Echo (ping) request  id=0x0000, seq=0/0, ttl=64
192.168.27.1    192.168.27.255   ICMP          60  Echo (ping) request  id=0x0000, seq=0/0, ttl=64
192.168.27.1    192.168.27.255   ICMP          60  Echo (ping) request  id=0x0000, seq=0/0, ttl=64
```

图 3-2

【问题 3】(2 分)

如果要在 Windows 系统中对上述 Smurf 攻击进行过滤设置， 应该在图 3-1 中“允许应用或功能通过 Windows Defender 防火墙”下面的选项中选择哪一项?

【问题 4】(2 分)

要对入站的 ICMP 协议数据包设置过滤规则， 应选择图 3-3 的哪个选项?

【问题 5】(4 分)

在图 3-4 的端口和协议设置界面中，请分别给出“协议类型(P)”“协议号(U)”“本地端口(L)”“远程端口(R)”的具体设置值。

要创建的规则类型

● 程序(P)
控制程序连接的规则。

○ 端口(O)
控制 TCP 或 UDP 端口连接的规则。

○ 预定义(E):
@FirewallAPI.dll,-80200
控制 Windows 体验功能连接的规则。

○ 自定义(C)
自定义规则。

图 3-3

此规则应用于哪些端口和协议?

协议类型(P): 任何
协议号(U): 0
本地端口(L): 所有端口
示例: 80, 443, 5000-5010
远程端口(R): 所有端口
示例: 80, 443, 5000-5010
Internet 控制消息协议(ICMP)设置:

图 3-4

信管网参考答案：

【问题 1】

[开始]一[控制面板]一[系统和安全]-[Windows Defender 防火墙]或运行“control[.exe]”一[系统和安全]一[Windows Defender 防火墙

【问题 2】

(1)192.168.27.1

(2) Echo reply(回响应答)

【问题 3】

高级设置。

【问题 4】

自定义。

【问题 5】

协议类型(P)： ICMPv4

协议号(U):自动填 1

本地端口(L):不用填或空白

远程端口(R):不用填或空白

查看解析：www.cnitpm.com/st/5024418443.html

试题四(共 12 分)

阅读下列说明，回答问题 1 至问题 6，将解答填入答题纸的对应栏内。

【说明】

ISO 安全体系结构包含的安全服务有七大类，即：①认证服务；②访问控制服务；③数据保密性服务；④数据完整性服务；⑤抗否认性服务；⑥审计服务；⑦可用性服务。

请问以下各种安全威胁或者安全攻击可以采用对应的哪些安全服务来解决或者缓解。请直接用上述编号①~⑦作答。

【问题 1】(2 分)

针对跨站伪造请求攻击可以采用哪些安全服务来解决或者缓解?

【问题 2】(2 分)

针对口令明文传输漏洞攻击可以采用哪些安全服务来解决或者缓解?

【问题 3】(2 分)

针对 Smurf 攻击可以采用哪些安全服务来解决或者缓解?

【问题 4】(2 分)

针对签名伪造攻击可以采用哪些安全服务来解决或者缓解?

【问题 5】(2 分)

针对攻击进行追踪溯源时，可以采用哪些安全服务?

【问题 6】(2 分)

如果下载的软件被植入木马，可以采用哪些安全服务来进行解决或者缓解?

信管网参考答案：

【问题 1】①

【问题 2】③

【问题 3】⑦

【问题 4】⑤

【问题 5】⑥

【问题 6】④

查看解析：www.cnitpm.com/st/502451754.html

试题五、

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】

代码安全漏洞往往是系统或者网络被攻破的头号杀手。在 C 语言程序开发中，由于 C 语言自身语法的一些特性，很容易出现各种安全漏洞。因此，应该在 C 程序开发中充分利用现有开发工具提供的各种安全编译选项，减少出现漏洞的可能性。

【问题 1】(4 分)

图 5-1 给出了一段有漏洞的 C 语言代码(注：行首数字是代码行号)，请问，上述代码存在哪种类型的安全漏洞?该漏洞和 C 语言数组的哪一个特性有关?

```
4  #include "stdafx.h"
5  #include <string.h>
6  #define PASSWORD "1234567"
7  int verify_password(char *password)
8  {
9      int authenticated = 128;
10     char buffer[8];
11     authenticated = strcmp(password, PASSWORD);
12     strcpy(buffer, password); //over flowed here!
13     return authenticated;
14 }
```

图 5-1

【问题 2】(4 分)

图 5-2 给出了 C 程序的典型内存布局，请回答如下问题。

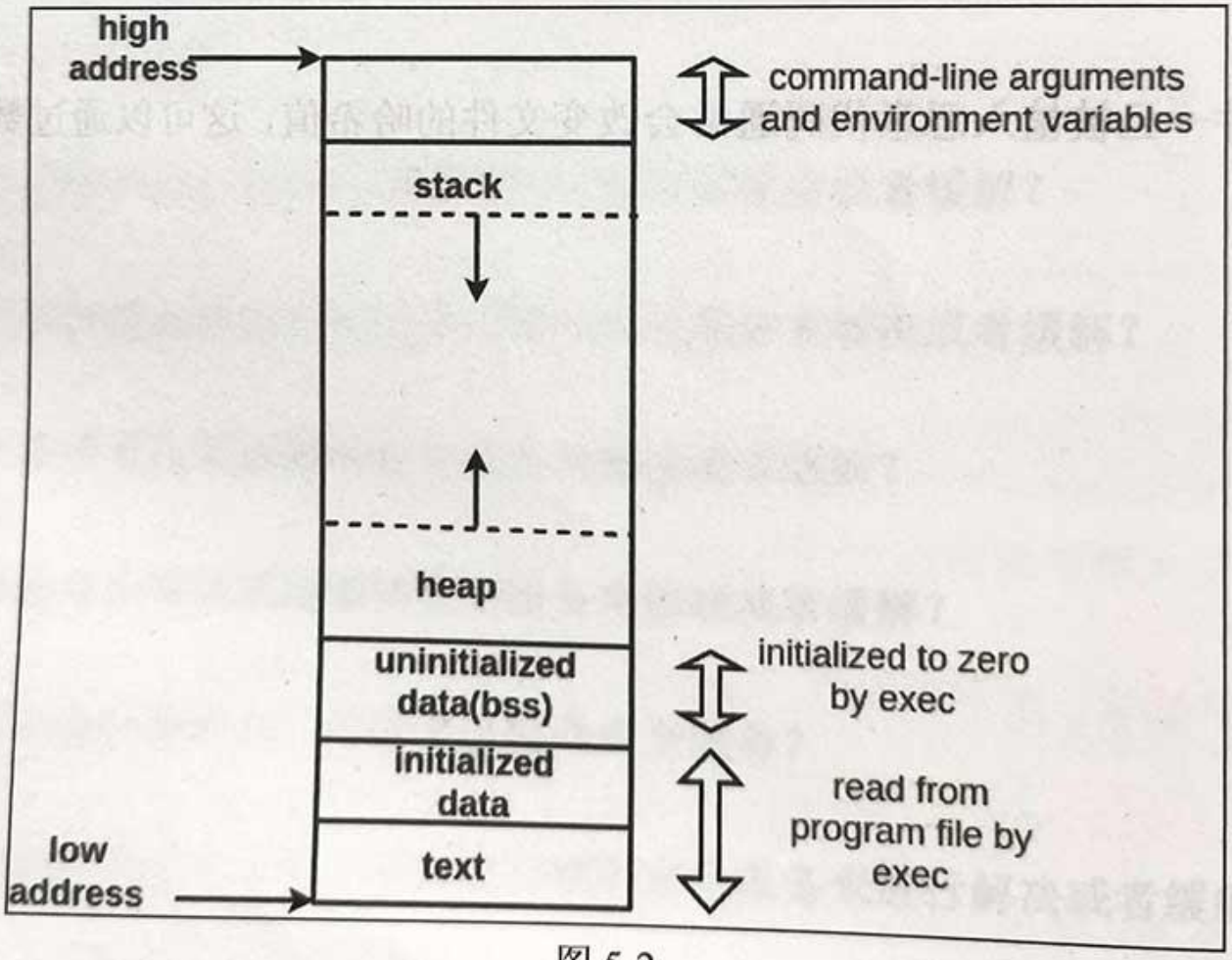


图 5-2

(1)请问图 5-1 的代码中第 9 行的变量 authenticated 保存在图 5-2 所示的哪个区域中？

(2)请问 stack 的两个典型操作是什么？

(3)在图 5-2 中的 stack 区域保存数撕时， 其地址增长方向是往高地址还是往低地址更高?

(4)对于图 5-1 代码中的第 9 行和第 10 行代码的两个变量，哪个变量对应的内存地

【问题 3】(6 分)

微软的 Visual Studio 提供了很多安全相关的编译选项， 图 5-3 给出了图 5-1 中代码相关的工程属性页而的截图。请回答以下问题。

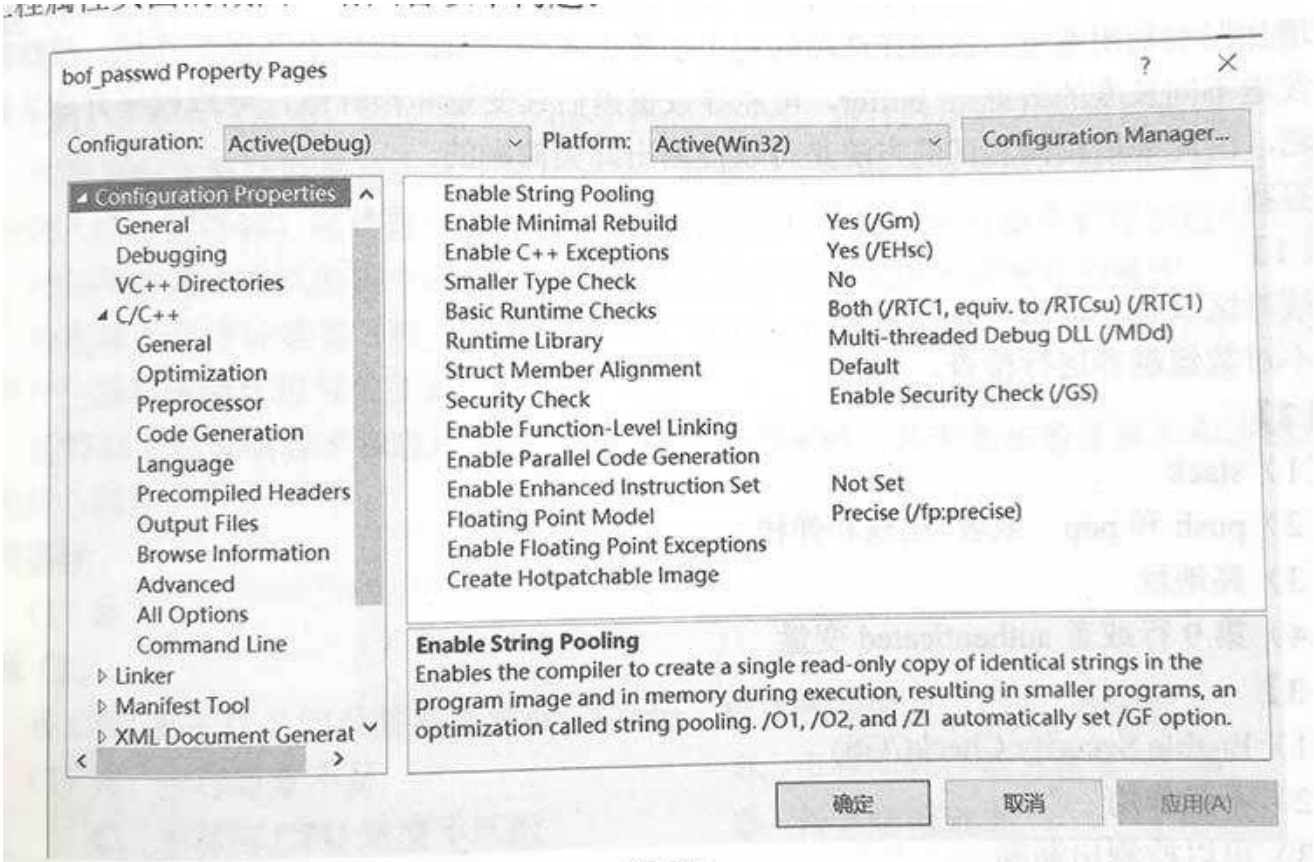


图 5-3

(1)请问图 5-3 中哪项配置可以有效缓解上述代码存在的安全漏洞?

(2)如果把图 5-1 中第 10 行代码改为 char buffer[4]; 图 5-3 的安全编译选项是否还起作用?

(3)模糊测试是否可以检测出上述代码的安全漏洞?

信管网参考答案:

【问题 1】

缓冲区(栈)溢出。

不对数组越界进行检查。

【问题 2】

(1)stack

(2)push 和 pop 或者压栈和弹栈

(3)高地址

(4)第 9 行或者 authenticated 变量

【问题 3】

(1) Enable Security Check(/GS)

(2)不起作用

(3)可以检测出漏洞

查看解析：www.cnitpm.com/st/502465698.html