2024-2025 学年度第 一 学期
《软件安全》期末考试试卷 A 卷(开 卷)

专业：_____ **学号：**_____ **姓名：**_____

说明：答案请全部写在答题纸上，写在试卷上无效。

未经主考教师同意，考试试卷、答题纸、草稿纸均不得带离考场，否则视为违规。

题号	一	二	三	四			总分
分值	30	32	24	14			100

一. 计算与分析题（共 3 小题，每小题 10 分，共 30 分）

1.下图为 Windows 下某 32 位 PE 文件的 16 进制数据截图。请分析并回答以下问题：

(1) 程序的基址（ImageBase）是多少？(2 分)

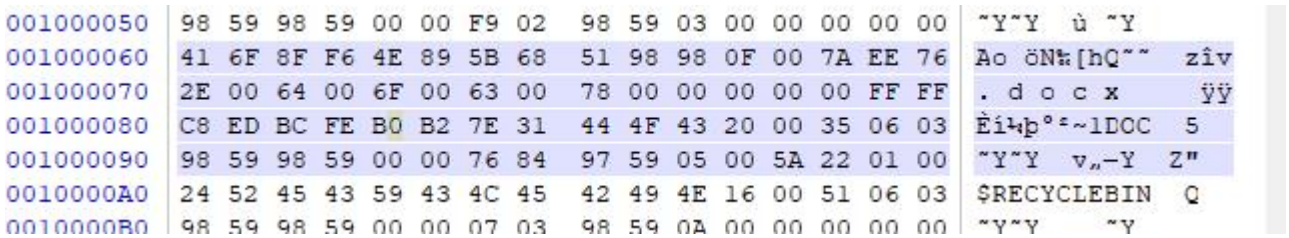
(2) 分别写出程序的入口点 VA 地址(Entrypoint)，IDT(Import Directory Table)及其对应的 IAT(Import Address Table)在运行时的 VA 地址？(共 4 分，入口点 2 分，其他各 1 分)

(3) 该程序的功能实际是执行 MessageBoxA 函数，请给出弹出对话框中两个字符串（标题字符串以及弹框文本字符串）的 VA 地址（共 4 分，各 2 分）。

```
          00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  已解码的文本
00000000  4D 5A 00 00 50 45 00 00 4C 01 01 00 68 40 10 00  MZ..PE..L...h@..
00000010  00 68 C1 00 40 00 EB 18 70 00 03 01 0B 01 00 00  .h..@...p.......
00000020  4D 65 73 73 61 67 65 42 6F 78 41 00 A8 00 00 00  MessageBoxA.....
00000030  68 D5 00 40 00 EB 0D 00 00 00 40 00 04 00 00 00  h..@......@.....
00000040  04 00 00 00 6A 00 FF 15 8C 00 40 00 05 00 00 00  ....j.....@.....
00000050  00 EB 09 00 0C 01 00 00 A8 00 00 00 89 C1 CD 29  .............)
00000060  02 00 00 00 00 00 00 00 00 00 00 00 75 73 65 72  ............user
00000070  33 32 2E 64 6C 6C 00 00 02 00 00 00 00 00 00 00  32.dll..........
00000080  00 00 00 00 AD 00 00 00 28 00 00 00 1E 00 00 00  ........(.......
00000090  00 00 00 00 00 01 00 00 A8 00 00 00 00 01 00 00  ................
000000A0  A8 00 00 00 00 00 00 00 E9 5F FF FF FF 00 00 00  .........._.....
000000B0  00 00 00 00 00 00 00 00 00 6C 00 00 00 8C 00 00  .........l......
000000C0  00 57 48 55 43 53 45 20 54 69 6E 79 20 50 45 3A  .WHUCSE Tiny PE:
000000D0  32 36 38 42 00 54 68 69 73 20 69 73 20 74 68 65  268B.This is the
000000E0  20 74 69 6E 69 65 73 74 20 50 45 20 66 69 6C 65   tiniest PE file
000000F0  20 61 66 74 65 72 20 56 69 73 74 61 20 74 68 65   after Vista the
00000100  6F 72 65 74 69 63 61 6C 6C 79 2E 00 +           oretically..+
```

2.以下是 Winhex 中对某计算机 E 盘分区引导扇区和某文件目录项情况，已知该文件名为《软件安全题目.docx》，请分析该文件数据存放的具体首簇位置（使用 10 进制）(3 分)，文件大小（16 进制）(3 分)，以及实际磁盘占用大小(不需要考虑目录项大小)(4 分)（提示：首簇号的高位在 1000094H）。

```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
000000000  EB 58 90 4D 53 44 4F 53  35 2E 30 00 02 20 0E 03  ëX MSDOS5.0
000000010  02 00 00 00 00 F8 00 00  3F 00 FF 00 00 08 00 00      ø  ? ÿ
000000020  00 00 E8 03 79 3E 00 00  00 00 00 00 02 00 00 00    è y>
```



```
001000050 98 59 98 59 00 00 F9 02  98 59 03 00 00 00 00 00 ˜Y˜Y  ù ˜Y
001000060 41 6F 8F F6 4E 89 5B 68  51 98 98 0F 00 7A EE 76 Ao öN‰[hQ˜˜  zîv
001000070 2E 00 64 00 6F 00 63 00  78 00 00 00 00 00 FF FF . d o c x     ÿÿ
001000080 C8 ED BC FE B0 B2 7E 31  44 4F 43 20 00 35 06 03 Èí¼þ°²~1DOC  5
001000090 98 59 98 59 00 00 76 84  97 59 05 00 5A 22 01 00 ˜Y˜Y  v„—Y  Z"
0010000A0 24 52 45 43 59 43 4C 45  42 49 4E 16 00 51 06 03 $RECYCLEBIN  Q
0010000B0 98 59 98 59 00 00 07 03  98 59 0A 00 00 00 00 00 ˜Y˜Y     ˜Y
```

3. 以下是某路由器固件的部分功能代码

```
#define MAX_BUFFER 128
#define CONFIG_FILE "/etc/router/config.conf"
void set_wifi_ssid(const char *ssid) {
    char command[MAX_BUFFER];
    snprintf(command, sizeof(command), "iwconfig wlan0 essid %s", ssid);
    system(command);
}

void configure_router_ip(const char *ip_address) {
    char buffer[BUFFER_SIZE];
    printf("Configuring router IP...\n");
    strcpy(buffer, ip_address);
    printf("Router IP set to: %s\n", buffer);
}
```

请分析并回答以下问题：

1） 指出上述两个函数可能包含的安全漏洞（指出一个即可），并分析原因及危害。（6 分）

2） 针对上述分析的对应漏洞请给出防御方法及代码或伪代码。（4 分）

提示：

*snprintf()，函数原型为 int snprintf(char *str, size_t size, const char *format, ...)。该函数将可变参数 “…” 按照 format 的格式格式化为字符串，然后再将其拷贝至 str 中。*

二. 简答题（共 4 小题，每小题 8 分，共 32 分）

1. 作为安全研究人员，当我们要通过网络平台、媒体、会议、竞赛等方式向社会发布网络产品安全漏洞信息时，应遵守哪些规定？

2. 简述恶意软件隐匿技术中的代码混淆原理，并给出检测思路。

3. 简述漏洞防护机制 DEP 和 ASLR 的原理及作用。

4. 什么是威胁情报？威胁情报对于未知恶意代码检测能够带来哪些促进？

三． 代码分析题（共 2 小题，每小题 12 分，共 24 分）

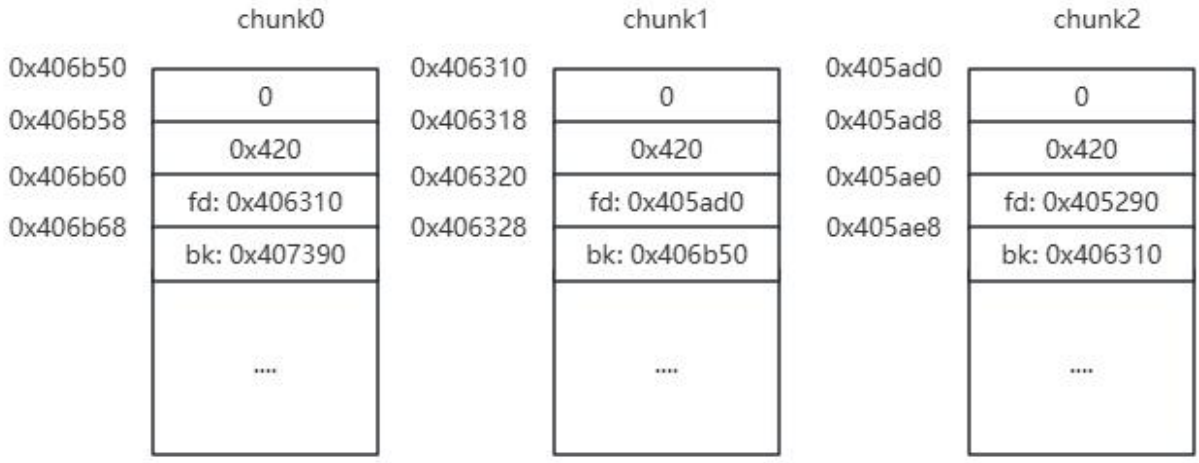
1. C 语言官方库 GNU libc 采用堆块（chunk）来管理堆结构， chunk 结构如下图所示：

```
struct malloc_chunk {
   INTERNAL_SIZE_T     prev_size;   /* 若前一个物理相邻的堆块占用，则该字段值为 0 */
   INTERNAL_SIZE_T     size;        /* 当前 chunk 的 size */
   /*以下空间为可供用户使用的 data 部分，malloc 调用返回后的指针指向该 data 段*/
   struct malloc_chunk* fd;         /* 双链表的前向指针*/
   struct malloc_chunk* bk;         /* 双链表的后向指针*/
   /*其它 data 部分，略*/
};
```

空闲堆块的管理采用双向链表。现给定某进程的内存布局如下图所示，其中 chunk0、chunk1、chunk2 均为空闲堆块、并使用双链表连接在一起。注意：这 3 个堆块非物理相邻。

堆使用过程中的 malloc、free 等操作均可能对双向链表进行 unlink 操作，其示意代码如下：

```
FD = p->fd;
BK = p->bk;
FD->bk = BK;
BK->fd = FD;
```



请根据以上信息，回答以下问题：

(1). 若此时需要针对 chunk1 进行 unlink 操作，请简述 unlink 中涉及到的具体内存读写单元和值。（4 分）

(2). 请根据 unlink 操作的过程，分析可能存在的安全隐患，并给出一种具体的攻击场景（4 分）

(3). 给出至少一种防御 unlink 攻击的方法？(4)

2. 以下是互联网流行的某段长度为 61 字节的 Shellcode 的全部数据及对应的反汇编代码。

```
char shellcode[] =
"\x31\xC9"                          //xor ecx,ecx
"\x64\x8B\x71\x30"                  //mov esi,[fs:ecx+0x30]
"\x8B\x76\x0C"                      //mov esi,[esi+0xc]
"\x8B\x76\x1C"                      //mov esi,[esi+0x1c]
"\x8B\x36"                          //mov esi,[esi]
"\x8B\x06"                          //mov eax,[esi]
"\x8B\x68\x08"                      //mov ebp,[eax+0x8]
"\xEB\x20"                          //jmp short 0x35
"\x5B"                              //pop ebx
"\x53"                              //push ebx
"\x55"                              //push ebp
"\x5B"                              //pop ebx
"\x81\xEB\x11\x11\x11\x11"      //sub ebx,0x11111111
"\x81\xC3\xDA\x3F\x1A\x11"      //add ebx,0x111a3fda (for seven X86 add ebx,0x1119f7a6)
"\xFF\xD3"                          //call ebx
"\x81\xC3\x11\x11\x11\x11"      //add ebx,0x11111111
"\x81\xEB\x8C\xCC\x18\x11"      //sub ebx,0x1118cc8c (for seven X86 sub ebx,0x1114ccd7)
"\xFF\xD3"                          //call ebx
"\xE8\xDB\xFF\xFF\xFF"              //call dword 0x15
//db "cmd"
"\x63\x6d\x64";
```

请分析以上代码，并回答以下问题：

（1）该段代码中“"\x8B\x68\x08" ”这一行(第 7 行加粗行)指令执行之后，ebp 中存放的数据是什么含义？【提示：fs:[30]指向了 PEB（进程环境块）结构】（3 分）

（2）该段代码中“"\xEB\x20" ”指令（jmp+call）的作用是什么？（3 分）其下一行语句“\x5B”执行后，ebx 指向的数据是什么？（2 分）

（3）该段代码的总体功能是什么？(4 分)

四．综合题（共 1 小题，每小题 14 分，共 14 分）

2024 年 10 月，某大型企业的企业资源规划（ERP）系统遭遇了精心策划的恶意代码植入攻击。攻击者通过渗透进为 ERP 系统提供第三方插件（DLL）的供应商，在其更新的插件中植入了恶意代码。当该企业用户下载并安装这些被篡改的插件时，恶意代码（Malware）悄无声息地进入了 ERP 系统，实现了对系统的远程控制和数据窃取。攻击导致企业核心数据泄露，ERP 系统部分功能模块瘫痪，严重影响了企业的正常生产和运营管理，并带来了巨大的经济损失和法律与合规风险。

（1）针对该攻击场景给出防御思路和方法。（7 分）

（2）分析这些防御措施的合理性和局限性。（7 分）