2023-2024 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
							100

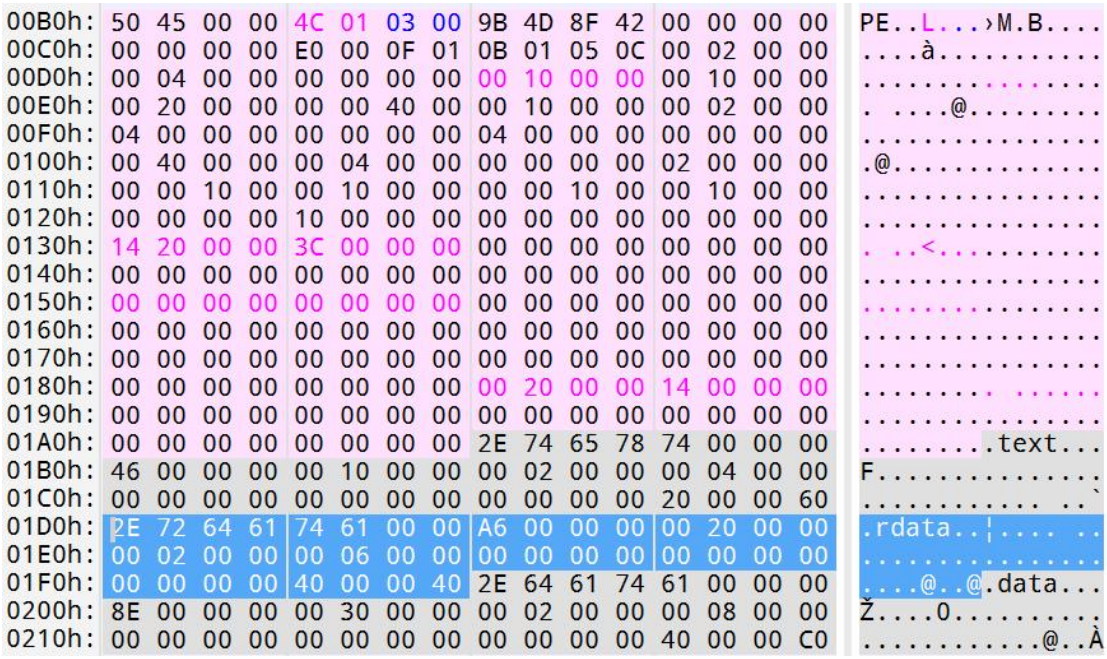
一. 计算与分析题（共 3 小题，共 30 分）

1. 下图为 Windows 下某 PE 文件（32 位）的片段截图，请问：

（1） 该程序从多少个 dll 中引入了 API 函数？（3 分）

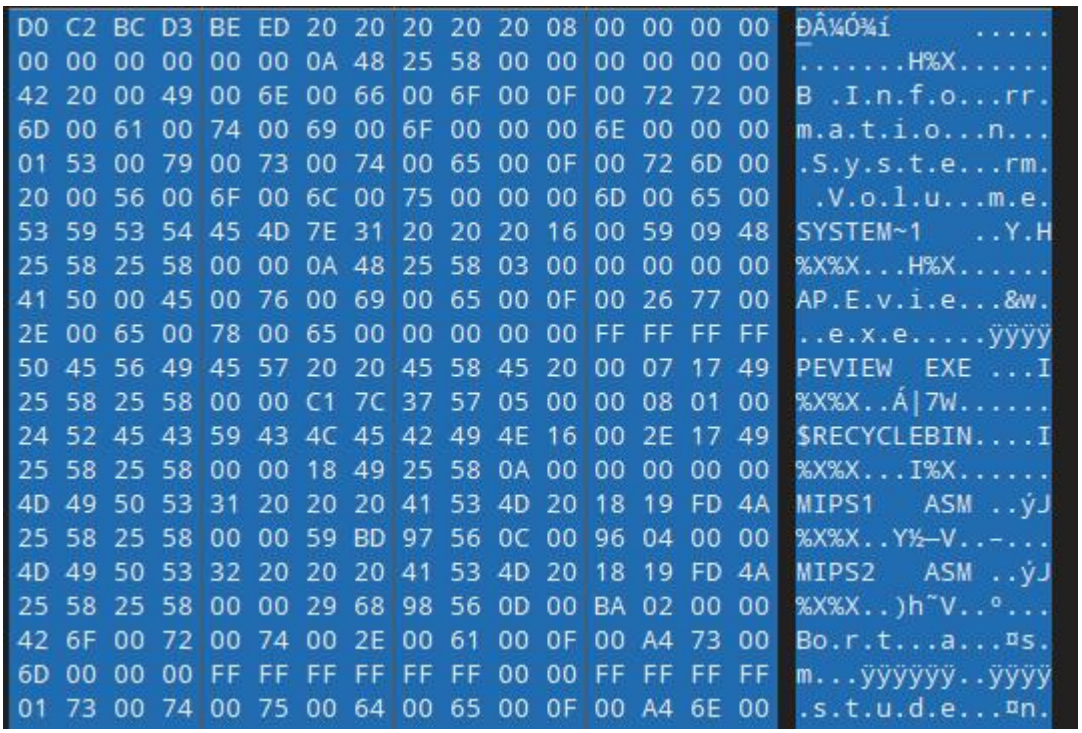
（2） 该程序从所有 dll 引入的总 API 函数个数为多少？（3 分）

（3） 该程序的 IDT 在文件中的起始地址是多少？（4 分）



Windows 下某 PE 文件的片段截图

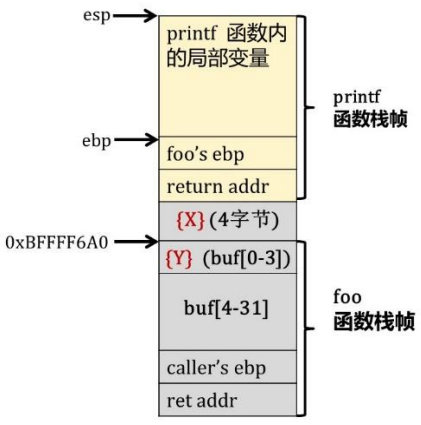
2. 以下是 010editor 中对某计算机 E 盘分区根的磁盘浏览情况，两个图分别表示目录项和 FAT 表项目，请根据图片所示，分析文件 PEview.exe 的文件大小（3 分）和簇链(簇编号从 0 开始，簇链形式如 1->2->3) （4 分），在已知一个簇大小为 0x4000h 的情况下，给出文件实际占用的空间（3 分）



3. 下图（a）为某程序的代码片段，其中 fmt 指向由用户输入的字符串，图（b）为该程序代码片段中**printf 函数被调用执行时**的内存堆栈结构和布局，其中 0xBFFFF6A0 为内存地址，此刻 fmt 指向的字符串为“\x00\xA1\xFF\xBF%s\n”。请根据内存布局，计算图（b）中的 X 值是多少（3 分），图（b）中的 Y 值是多少（3 分），并描述 printf 函数执行完成后的结果是什么（4 分）。

```
int foo (char *fmt) {
        char buf[32];
        strcpy(buf, fmt);
        printf(buf);
}
```

（a）代码片段



(b) 调用 printf 时的内存布局

二． 简答题（共 5 小题，每小题 6 分，共 30 分）

1. 重定位是 PE 文件的一种常用机制，那哪些类型的数据需要进行重定位，为什么？

2. 随着恶意软件检测手段的不断丰富，恶意软件检测逃避技术也在不断升级。请简要描述至少三种不同的检测逃避手段。

3. 请简单描述 UAF（Use After Free）漏洞的形成原因与危害。

4. 请结合栈溢出漏洞利用过程，描述 GS 和 DEP 阻止漏洞利用的时间点和作用机制。

5. 什么是" 非法获取计算机信息系统数据、非法控制计算机信息系统罪"，其 "情节严重"情形具体包括哪些？

三. 分析题（共 2 小题，共 30 分）

1. 以下代码片段节选自某 x86 架构的恶意软件样本，该样本通过运行时动态解密真正函数的方法来躲避查杀。提示：

1） fcmovu 为 FPU（浮点处理单元）指令。fnstenv byte ptr [esp-0Ch]会将最后执行的一条 FPU 指令相关的协处理器的信息按结构保存在指定的内存中，其中偏移 12 字节处就是最后执行的 FPU 指令的运行时地址。在下面这段代码中，这两条指令运行完成后栈顶保存的就是 fcmovu 的运行时地址，即 0x0040758B。

2） 此类恶意样本均使用了“一条 FPU 指令+fnstenv byte ptr [esp-0Ch]”的组合来获取程序的 eip 地址。请分析以下代码片段，并回答以下 2 个问题。

1） 详细介绍这段解密函数的实现逻辑，并给出待解密部分的起始地址，待解密部分的长度。（10 分）

2） 归纳总结从此类恶意样本中提取待解密部分并进行解密的思路。（5 分）

```
loc_407586:
   00407586 BA 15 E9 DC A4     mov     edx, 0A4DCE915h
   0040758B DA D9              fcmovu  st, st(1)
   0040758D D9 74 24 F4        fnstenv byte ptr [esp-0Ch]
   00407591 5E                 pop     esi
   00407592 29 C9              sub     ecx, ecx
   00407594 B1 74              mov     cl, 74h
loc_407596:
   00407596 31 56 14           xor     [esi+16h], edx
   00407599 83 C6 04           add     esi, 4
   0040759C 03 56 10           add     edx, [esi+12h]
   0040759F E2 F5              loop    loc_407596
```

2. 说明，以下代码为同学们使用 C 语言编写的图书管理系统，主要采用双向链表的数据结构来实现对图书书目的管理，每条书目表示为双向链表中的一个节点。功能方面，用户根据不同的选项，实现图书的添加（代码略）、编辑（Edit_Item 函数）和删除（Delete_Item 函数）等，试分析以下代码片段，指出代码中存在的安全问题（4 分）、触发条件并简要分析利用过程（8 分）以及可能的漏洞利用危害（3 分）。

```
1.  struct one_book {
2.      char name[255];
3.      int id;
```

```
    int size = 255;
    struct one_book * prev = NULL;
    struct one_book * next = NULL;
};

void Delete_Item (struct one_book *pb) {
    if (pb && pb->next && pb->prev) {
        pb->next->prev = pb-> prev;
        pb->prev->next = pb-> next;
        free(pb);
        pb = NULL;
    }
}

void Edit_Item (struct one_book * pb, char * received)  {
    if (pb) {
        strcpy( pb->name, received );
        pb->size = strlen(received);
    }
}
```

四. 综合题（共 1 题，每题 10 分，共 10 分）

2022 年 6 月，西北工业大学发布《公开声明》称，该校遭受境外网络攻击。中国国家计算机病毒应急处理中心和 360 公司全程参与了此案的技术分析工作，全面还原了相关攻击事件的总体概貌、技术特征、攻击武器、攻击路径和攻击源头，主要特征表现在 1）战术针对性强，采取半自动化攻击流程，单点突破、逐步渗透、长期窃密，目标包括内部主机、服务器、运维网、办公网的核心设备及终端、网络节点设备等，2）搜集的敏感数据包括业务管理的账号口令、操作记录以及系统日志、网络边界设备账号口令、业务设备访问权限、路由器等设备配置信息、FTP 服务器文档资料信息。3）渗透路径复杂，先后使用了 54 台跳板机和代理服务器，主要分布在日本、韩国、瑞典、波兰、乌克兰等 17 个国家，其中 70%位于中国周边国家，如日本和韩国。

请结合课程学习内容和上述案例，谈谈软件安全和网络攻防活动在发展趋势和演化规律等方面的认识（10 分）。