武汉大学国家网络安全学院
2022-2023 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 20 分）

1. 以下是某硬盘的分区表信息，该硬盘只有一个分区，请给出该分区起始和结束扇区位置，以及分区的大小（**给出计算过程即可**）（5 分）

```
0000001B0  00 00 00 00 00 2C 44 63  D1 A5 D1 A5 00 00 80 01
0000001C0  01 00 07 FE FF FF 3F 00  00 00 25 97 FF 04 00 00
0000001D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000001E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000001F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 55 AA
```

2. 已知文件对齐量与内存对齐量都是 0x1000。下面是 PE 文件导入表相关结构和数据在 010Editor 编辑器和 OD 内存中的截图片段，试分析：（1）USER32 模块对应的 IDT 项的开始 RVA 地址。（2）USER32.dll 模块中 GetDlgItem 函数的 VA 地址？（10 分）

（1）010Editor 中的两段数据（IDT 表及 INT（Import Name Table，指向 DLL 和 API 名字的字符串）表部分数据）：

IDT：

```
4430h  00 00 00 00 54 45 00 00 00 40 00 00 00 45 00 00  ....TE...@...E..
4440h  00 00 00 00 00 00 00 00 E4 45 00 00 9C 40 00 00  ........äE..œ@..
4450h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
4460h  00 00 00 00 D4 46 00 00 38 45 00 00 46 45 00 00  ....ÔF..8E..FE..
```

INT：

```
45E0h  65 6D 00 00 55 53 45 52 33 32 2E 64 6C 6C 00 00  em..USER32.dll..
45F0h  66 01 47 65 74 53 74 61 72 74 75 70 49 6E 66 6F  f.GetStartupInfo
```

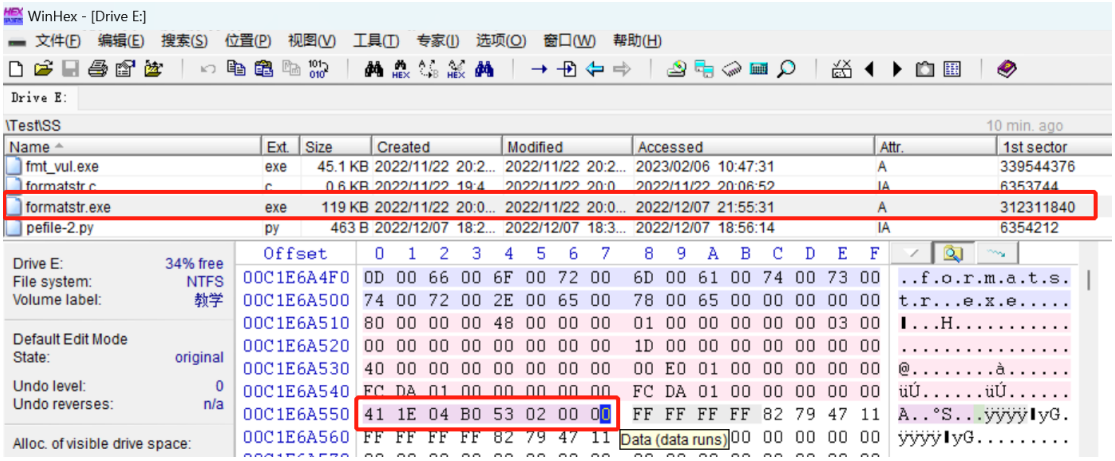
（2）OD 下的内存数据（INT 表字段的对应字符串区域、INT 表、IAT 表的部分数据）：

```
004045B0  74 44 6C 67 49 74 65 6D 54 65 78 74 41 00 63 01  tDlgItemTextA.c.
004045C0  47 65 74 57 69 6E 64 6F 77 54 65 78 74 4C 65 6E  GetWindowTextLen
004045D0  67 74 68 41 00 00 05 01 47 65 74 44 6C 67 49 74  gthA....GetDlgIt
004045E0  65 6D 00 00 55 53 45 52 33 32 2E 64 6C 6C 00 00  em..USER32.dll..
004045F0  66 01 47 65 74 53 74 61 72 74 75 70 49 6E 66 6F  f.GetStartupInfo
00404600  41 00 DA 00 47 65 74 43 6F 6D 6D 61 6E 64 4C 69  A.Ú.GetCommandLi
00404610  6E 65 41 00 8E 01 47 65 74 56 65 72 73 69 6F 6E  neA...GetVersion
```

```
00404500  BE 45 00 00 D6 45 00 00 8C 45 00 00 AC 45 00 00  ¾E..ÖE...E..¬E..
00404510  9E 45 00 00 62 45 00 00 7A 45 00 00 6E 45 00 00  .E..bE..zE..nE..
00404520  00 00 00 00 3A 01 47 65 74 4D 6F 64 75 6C 65 48  ....:.GetModuleH
00404530  61 6E 64 6C 65 41 00 00 A3 01 47 6C 6F 62 61 6C  andleA..£.Global
```

```
0040409C 30 33 A6 75 90 27 A6 75 80 4A A6 75 B0 27 A6 75 03¦u.'¦u.J¦u°'¦u
004040AC 90 3D A6 75 E0 3A A6 75 C0 1C A6 75 90 21 A6 75 .=¦uà:¦uÀ.¦u.!¦u
004040BC 00 00 00 00 FF FF FF FF 5A 13 40 00 6E 13 40 00 ....ÿÿÿÿZ.@.n.@.
004040CC 72 75 6E 74 69 6D 65 20 65 72 72 6F 72 20 00 00 runtime error ..
004040DC 0D 0A 00 00 54 4C 4F 53 53 20 65 72 72 6F 72 0D ....TLOSS error.
004040EC 0A 00 00 00 53 49 4E 47 20 65 72 72 6F 72 0D 0A ....SING error..
004040FC 00 00 00 00 44 4F 4D 41 49 4E 20 65 72 72 6F 72 ....DOMAIN error
0040410C 0D 0A 00 00 52 36 30 32 38 0D 0A 2D 20 75 6E 61 ....R6028..- una
0040411C 62 6C 65 20 74 6F 20 69 6E 69 74 69 61 6C 69 7A ble to initializ
0040412C 65 20 68 65 61 70 0D 0A 00 00 00 00 52 36 30 32 e heap......R602
```

3.以下是 Winhex 中对某计算机 E 盘分区某目录文件浏览情况，请分析该分区 formatstr.exe 文件数据存放的具体首簇位置（使用 16 机制），簇的数量（10 进制），以及该分区每个簇的大小（提示：DataRun 的位置在 00C1E6A550）。**（5 分）**



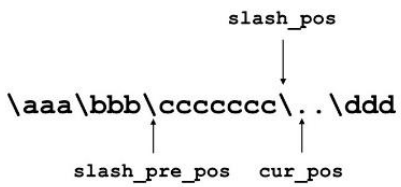
二． 简答题（共 5 小题，每小题 6 分，共 30 分）

1. 什么是缓冲区溢出？它的危害及防范措施有哪些？
2. PE 病毒的感染方式有哪些，他们各有哪些特色和局限性?
3. APT（Advanced Persistent Threat）恶意代码与普通恶意代码存在哪些差异?存在这些差异的本质原因是什么?
4. 按照木马客户端和服务器端在远程控制连接过程中的主动性和所扮演的角色，远程控制木马的连接方式有哪些?各有何优缺点?
5. 当前世界正面临百年未有之大变局，新一轮科技革命、产业变革正深入推进。请列举不少于三种的科技革命或产业革命，并阐述与软件安全的关联。

三. 分析题（共 2 小题，共 30 分）

1. （15 分）以下代码片段节选自某著名微软漏洞，该段代码的输入为表示路径的字符串，其主要功能检测路径中可能存在的相对路径（如‘.\’或‘..\’），转换为绝对路径。

参数 path 为即为由用户输入的、表示路径的字符串，在执行过程中，path 所指向的字符串保存在栈上。为便于理解，path 及代码中的各个变量作用如下示所示。



提示：
1）若 path 为“\aaa\bbb\cccccc\..\ddd”，则代码执行完成后将 path 转变为“\aaa\bbb\ddd”。
2）若 path 为“\aaa\..\..\..\ddd”，则代码执行可能会导致安全问题。
分析以下代码片段，
1） 说明该漏洞的类型及危害。（5 分）
2） 详细说明漏洞的触发机理。（10 分）

```
int FormatFolder(char * path)
{
    char * cur _pos = path;
    char * slash_pos = NULL,   slash_pre_pos = NULL;
    char v6, v7, v8;

    while ( *cur _pos ) {
        if ( *cur _pos == '\\' )  {      /*注释：'\\'为'\'的转义字符*/
            slash_pre_pos = slash_pos;
            slash_pos = cur_pos;
        } //end if
        else if ( *cur _pos == '.'  && cur_pos[1] == '.' ) {
            if ( cur_pos[2] == '\\'   || ! cur_pos[2] )    {
                if ( ! slash_pre_pos )
                    return 0;
                strcpy(slash_pre_pos, cur_pos + 2);    /*注释：用来消除'..\'，漏洞可疑点*/
                slash_pos = slash_pre_pos;
                cur_pos_ = slash_pre_pos;
                for ( j = slash_pre_pos - 1; *j != '\\' && j != path; --j ) ; /*注：漏洞可疑点*/
                slash_pre_pos = (*j == '\\' ?   j : 0);
            } //end if
        } //end else if
        cur_pos++;
    } //end while
    return 1;
}
```

4. 一个程序的核心功能部分的源代码如下图，已知某两次输入输出结果如右图所示，（1）若希望在输出时字符串 a 内容为“hello“，该如何构造输入（说明两次键盘输入的内容）？（2）该程序存在什么安全缺陷，如何利用？（15 分）

```
void func(int n, char* x)
{
        char tmp[100];
        printf("input tmp= ");
        scanf("%s", tmp);
        memcpy(x, tmp, n);
}

int main(void)
{
        int n;
        char a[6] = "01234";
        char b[6] = "56789";
        printf("input n= ");
        scanf("%d", &n);
        func(n,b);
        printf("a=%s\nb=%s\n", a, b);
        return 0;
}
```

```
┌──(root㉿kali)-[~/ruanjiananquan-chuti]
└─# ./test
input n= 6
input tmp= abcde
a=01234
b=abcde

┌──(root㉿kali)-[~/ruanjiananquan-chuti]
└─# ./test
input n= 20
input tmp= abcdefghijklmnopqrst
a=ghijklmnopqrst
b=abcdefghijklmnopqrst
```

四. 综合题（共 2 小题，每小题 10 分，共 20 分）

1. 陈同学是电脑游戏爱好者，为了不耽误学习，他在游戏 QQ 群里以非常低的价格购买一款挂机软件。为了检查安全性和效果，他用最新的杀毒软件对拟购买的挂机软件进行了安全性检测，并试用了一天，未发现问题。于是花钱购买了该软件的注册码。在向该软件提交注册码的瞬间，他注意到鼠标旁边出现了旋转不止的沙漏，过程持续了大概 10 秒。第二天重启电脑登录 QQ 后不久，QQ 被踢下线了，之后再也无法登录自己的 QQ。请分析：

（1）陈同学在执行了软件注册操作之后，他的电脑中可能发生了哪些事件？

（2）导致他 QQ 无法登录的可能原因和过程。

（3）请结合陈同学的教训，谈谈如何检测和预防自己遭受此类攻击。

2. 2017 年 4 月，黑客组织“影子经纪人”（Shadow Brokers）通过网络泄露了美国 NSA 大量漏洞利用工具。其中的“永恒之蓝”（ETERNALBLUE）”和“永恒浪漫”（ETERNALROMANCE）”，分别利用了微软文件共享协议 SMBv1 中的两个漏洞，以实现远程代码执行。很快，2017 年 5 月，基于“永恒之蓝”漏洞开发的勒索软件 WannaCry 在全球范围内爆发。紧接着，2017 年 6 月，另一个勒索病毒 Petya 肆虐全球，Petya 同时利用了“永恒之蓝”和“永恒浪漫”漏洞。这些恶意软件在全球范围内的扩散，给政府、企业和个人造成了巨大损失。请结合此案例，谈谈你对以下问题的看法：

（1）软件漏洞与恶意代码之间的关系。

（2）软件漏洞研究对于恶意代码防御的意义。

（3）网络安全从业人员遵守《网络产品安全漏洞管理规定》的必要性。