武汉大学计算机学院

2016—2017 学年第 二 学期

《 软件安全 》 考试试卷（A 卷，开卷）

一、 计算题（4 小题，每小题 5 分，共 20 分）

1. 以下是某硬盘分区表信息，请计算出该磁盘第一个主分区及扩展分区的开始扇区位置（给出 16 进制）、扇区数（给出 16 进制），以及整个硬盘的大小（以 G 为单位，按 1K=1000 计算，小数点后取 1 位，四舍五入，给出计算过程）。

```
00000000432 00 00 00 00 00 00 00 00  24 3F C3 8C 00 00 80 01
00000000448 01 00 07 FE FF FF 3F 00  00 00 41 39 40 06 00 FE
00000000464 FF FF 0F FE FF FF 80 39  40 06 C1 12 F8 33 00 00
00000000480 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000000496 00 00 00 00 00 00 00 00  00 00 00 00 00 00 55 AA
```

2. 下图是某 U 盘［为 FAT32 文件系统］中某个文件的目录项，由引导扇区参数可知该分区每个簇包含 32 个扇区［512 字节 / 扇区］，请计算该文件的大小、首簇簇号及其所占用的簇数。［请填写十进制数字］

```
00C30C140  49 52 49 53 45 44 49 54  44 4C 4C 20 00 91 D0 5C  IRISEDITDLL .悌\
00C30C150  98 3F A7 4A 00 00 D0 5C  98 3F FB 2F 00 30 03 00  ?  ..攀??.0..
```

3. 下图为某 PE 程序的部分 16 进制数据截图，请分析该文件 data 节的具体信息（在文件及内存中的开始位置及大小），并计算内存中 RVA 地址 0000B341H 在该 PE 文件中的文件偏移地址。［给出 16 进制数据］

```
00000140h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000150h: 00 00 00 00 00 00 00 00 63 6F 64 65 00 00 00 00 ; ........code....
00000160h: 60 77 00 00 00 10 00 00 00 78 00 00 00 04 00 00 ; `w.......x......
00000170h: 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 ; ............ ..`
00000180h: 64 61 74 61 00 00 00 00 94 12 00 00 00 90 00 00 ; data....?...?.
00000190h: 00 06 00 00 00 7C 00 00 00 00 00 00 00 00 00 00 ; .....|..........
000001a0h: 00 00 00 00 40 00 00 C0 63 6F 6E 73 74 00 00 00 ; ....@..繲onst...
000001b0h: 60 2C 00 00 00 B0 00 00 00 2E 00 00 00 82 00 00 ; `,...?.....?..
000001c0h: 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 ; ............@..@
000001d0h: 2E 72 73 72 63 00 00 00 D0 35 00 00 00 E0 00 00 ; .rsrc...?...?..
000001e0h: 00 36 00 00 00 B0 00 00 00 00 00 00 00 00 00 00 ; .6...?.........
000001f0h: 00 00 00 00 40 00 00 40 2E 69 64 61 74 61 00 00 ; ....@..@.idata..
```

4. 下图为某程序的.rdata 节（开始位置 RVA：2000，文件偏移量：600H）在内存中的主要数据。请计算或分析：该程序引入目录表开始地址的 RVA，引入的三个函数的名称及真实地址，以及在 PE 文件中 608H-60BH 偏移处的值。

```
004020000 FA CA 81 7C 00 00 00 00 AD A8 D1 77 EA 07 D5 77 | ....  祺?鐣
004020010 00 00 00 00 50 20 00 00 00 00 00 00 00 00 00 00 ....P ..........
004020020 72 20 00 00 00 00 20 00 00 58 20 00 00 00 00 00 00 r ... ..X ......
004020030 00 00 00 00 9A 20 00 00 08 20 00 00 00 00 00 00 ....?..  ......
004020040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
004020050 64 20 00 00 00 00 00 00 00 20 00 00 8C 20 00 00 00 d ......  ..?..
004020060 00 00 00 00 00 00 45 78 69 74 50 72 6F 63 65 73 ......ExitProces
004020070 73 00 6B 65 72 6E 65 6C 33 32 2E 64 6C 6C 00 00 s.kernel32.dll..
004020080 62 02 77 73 70 72 69 6E 74 66 41 00 90 01 4D 65 b wsprintfA.?Me
004020090 73 73 61 67 65 42 6F 78 41 00 75 73 65 72 33 32 ssageBoxA.user32
0040200A0 2E 64 6C 6C 00 00 00 00 00 00 00 00 00 00 00 00 .dll............
0040200B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
```

二、 简答题（7 小题，每小题 6 分，共 42 分）

1. U 盘比较常见的文件系统格式是 FAT32，假设其中存储的一个 DOC 文件被无意删除，试给出手动恢复的原理和过程。

2. 请描述 PE 结构中重定位节的结构，以及重定位的作用。

3. “攻击者使用网络木马进行远程文件操作”与“用户自身使用资源管理器进行本地文件操作”存在多方面的差别，请给出可用于在用户计算机中检测区分这两类活动的技术特征。

4. 计算机病毒的文件感染与漏洞攻击的 Shellcode 注入有哪些异同？

5. 请描述 Windows 下至少 3 种不同的软件行为拦截方法和实现层次，并简要说明其优缺点。

6. 如何对一款远程控制型网络木马的控制者进行溯源追踪？

7. ASLR、DEP、GS、SafeSEH 是常见的四种漏洞利用阻止技术，分别用于干扰或阻止漏洞利用流程中的特定环节，如果按照其对应的特定环节在漏洞利用流程中发生作用的先后顺序来排列，其顺序应该是怎样的？并请说明理由。

三、 分析题（3 小题，每小题 6 份，共 18 分）

1. 某重要用户的计算机感染了某种恶意软件，安全人员对其 C 盘进行了格式化、重装，但重启之后发现该计算机再次了感染该病毒，请分析可能存在的原因。

2. 请分析以下代码存在的缺陷及危害，并请给出防护思路。

```
admin1=request("admin")
password1=request("password")
set rs=server.CreateObject("ADODB.RecordSet")
rs.open "select * from T_admin where admin='" & admin1 & "' and
password='"& password1 &"'",conn,1
if rs.eof and rs.bof then
 response.write"<SCRIPT language=JavaScript>alert('用户名或密码不正确！
 ');"
 response.write"javascript:history.go(-1)</SCRIPT>"
 response.end
else
 session("admin")=rs("admin")
 response.redirect "admin.asp"
end if
```

3. 下面代码中存在漏洞，请分析其漏洞类型、漏洞成因和利用方式

```
int main(int argc, char** argv)
{
  printf(argv[1]);
  return 0;
}
```

四、 综合设计题（2 小题，每小题 10 份，共 20 分）

1. 针对以下函数（目标系统及程序开启了 DEP），请通过 password 来设计一个 payload，该 payload 的 shellcode 触发后执行一个计算器程序。(使用示例：WinExec("calc.exe",SW_SHOW))

   a) 指出该函数存在的安全缺陷。(2 分)

   b) 通过控制 password 设计该 payload，并画出其栈中结构布局。(6 分)

   c) 给出该类型的 Shellcode 的检测思路。(2 分)

```
#define PASSWORD "1234567"
int verify_password (char *password)
{
   char buffer[8];
   int authenticated;
   authenticated=strcmp(password,PASSWORD);
   strcpy(buffer,password);
   return authenticated;
}
```

2. Windows 的堆管理有堆块的分配、释放和合并操作。试结合堆块分配，分析其堆溢出的机理和防御。

   a) 当堆块元数据没有保护时，请以“堆分配”为背景设计一个堆溢出的实例。(5 分)

   b) 给出该实例中往任意地址(如 0x77AABBCC)写任意数据(如 0x0C0C0C0C)的机理。(3 分)

   c) 给出该实例的防御方法。(2 分)

```
Remove (ListNode *node)
{node->blink->flink=node->flink;
      node->flink->blink=node->blink;}
```

堆分配的操作