

《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	32	32	24	12			100

一. 计算与分析题（共 4 小题，每小题 8 分，共 32 分）

1. 以下是 Winhex 查看到的某 NTFS 分区下“组织.doc”文件的 FILERECORD，该文件 DataRun 开始位置为 0x18F16540，请分析（需要给出分析计算思路）：

(1) 该文件的具体存储位置（起始簇号及簇数, 以 16 进制表示）[4 分]

(2) 该分区的每簇大小[4 分]

Name	Ext.	Size	Created
..		4.1 KB	2021/06/30 09:46:13.9
.		4.1 KB	2021/06/30 09:45:11.6
演示视频		4.1 KB	2021/06/30 09:45:12.2
others		4.1 KB	2021/06/30 09:45:15.8
组织.doc	doc	25.5 KB	2021/06/30 09:45:12.1

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI	ASCII
0018F164A0	00	00	00	00	00	00	02	00	4E	00	00	00	18	00	01	00	N	
0018F164B0	6A	01	02	00	00	00	02	00	84	72	EB	90	51	6D	D7	01	j	„rë Qm×
0018F164C0	84	72	EB	90	51	6D	D7	01	84	72	EB	90	51	6D	D7	01	„rë Qm×	„rë Qm×
0018F164D0	84	72	EB	90	51	6D	D7	01	00	70	00	00	00	00	00	00	„rë Qm×	p
0018F164E0	00	00	00	00	00	00	00	00	20	00	00	00	00	00	00	00		
0018F164F0	06	03	C4	7E	C7	7E	2E	00	64	00	6F	00	63	00	00	00	Ä~Ç~. d o c	
0018F16500	80	00	00	00	48	00	00	00	01	00	00	00	00	00	01	00	€	H
0018F16510	00	00	00	00	00	00	00	00	06	00	00	00	00	00	00	00		
0018F16520	40	00	00	00	00	00	00	00	00	70	00	00	00	00	00	00	@	p
0018F16530	00	66	00	00	00	00	00	00	00	66	00	00	00	00	00	00	f	f
0018F16540	41	07	47	94	3A	01	00	00	FF	FF	FF	FF	82	79	47	11	A G”:	ÿÿÿÿ,yG
0018F16550	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
0018F16560	00	Data (data runs)	00	00	00	00	00	00	00	00	00	00	00	00	00	00		

2. 已知某可执行程序的引出目录表 RVA 为 0x00092C70，下图为该程序的区段信息，请计算引出目录表在文件中的偏移位置（需要给出计算过程）。[答案和计算过程各 4 分]

No	名称	虚拟大小	虚拟偏移	实际大小	实际偏移	特征码
01	.text	00063F72	00010000	00064000	00001000	60000020
02	.data	00029FB0	00080000	0002A000	00065000	40000040
03	.data	00000C78	000B0000	00001000	0008F000	C0000040
04	.didat	00000034	000C0000	00001000	00090000	C0000040
05	.rsrc	00000520	000D0000	00001000	00091000	40000040
06	.reloc	00004818	000E0000	00005000	00092000	42000040
*	验证 ...			000036E8	00097000	

3. 下图为 Windows 下某 PE 文件的片段截图，请问：

- (1) 程序的引入函数目录表（IDT）表的 RVA 是多少？（2 分）
- (2) 该程序从多少个 dll 中引入了 API 函数？（3 分）
- (3) 该程序从所有 dll 引入的总 API 函数个数为多少？（3 分）

0100h:	50 45 00 00 4C 01 05 00	57 0B E8 60 00 00 00 00	PE...L...W.e`....
0110h:	00 00 00 00 E0 00 02 01	0B 01 0E 10 00 14 00 00à.....
0120h:	00 A6 00 00 00 00 00 00	26 18 00 00 00 10 00 00	...!.....&....
0130h:	00 30 00 00 00 00 40 00	00 10 00 00 00 02 00 00	.0....@.....
0140h:	05 00 01 00 00 00 00 00	05 00 01 00 00 00 00 00
0150h:	00 00 01 00 00 04 00 00	81 D5 01 00 02 00 40 81õ....@.
0160h:	00 00 10 00 00 10 00 00	00 00 10 00 00 10 00 00
0170h:	00 00 00 00 10 00 00 00	00 00 00 00 00 00 00 00
0180h:	5C 39 00 00 DC 00 00 00	00 60 00 00 10 8D 00 00	\9..Û....`.....
0190h:	00 00 00 00 00 00 00 00	00 BE 00 00 C8 29 00 00¾..È)..
01A0h:	00 F0 00 00 64 02 00 00	40 33 00 00 70 00 00 00	.ð..d...@3..p...
01B0h:	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
01C0h:	00 00 00 00 00 00 00 00	B0 33 00 00 40 00 00 00°3..@...
01D0h:	00 00 00 00 00 00 00 00	00 30 00 00 14 01 00 000.....
01E0h:	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
01F0h:	00 00 00 00 00 00 00 00	2E 74 65 78 74 00 00 00text...
0200h:	75 13 00 00 00 10 00 00	14 00 00 00 04 00 00 00	u.....
0210h:	00 00 00 00 00 00 00 00	00 00 00 00 20 00 00 60`
0220h:	2E 72 64 61 74 61 00 00	90 10 00 00 00 30 00 00	.rdata[.....0..
0230h:	00 13 00 00 00 10 00 00	00 00 00 00 00 00 00 00	

4. 请阅读以下程序，并：

- (1) 请画出该程序执行到 printf 函数内部第一条指令时的栈帧结构（4 分）
- (2) 指出该程序存在的漏洞（2 分）
- (3) 请对照自己画的栈帧结构，写出 printf 的输出结果。（2 分）

```
int main(void)
{
    int i=1;
    char buf[]="rjaql234";
    printf("%s %d %d %d\n", buf, i);
    return 0;
}
```

二. 简答题（共 4 小题，每小题 8 分，共 32 分）

- (1) 与普通恶意代码相比，勒索软件攻击有何突出特点（至少 3 项）？并描述对应特点背后的原因。
- (2) 在众多恶意软件检测方法中，哪些方法可以用于检测未知恶意代码（至少 4 种）？请简要描述其检测未知恶意代码的机制。
- (3) 漏洞的通用阻断技术包括 GS、DEP、ASLR、SafeSEH 等，请简要描述其阻断机理。
- (4) 什么是堆喷射？如何检测或阻止堆喷射（给出至少两种思路）？

三. 综合题（共 2 小题，每小题 12 分，共 24 分）

1. 下表列出了一个真实的 APT 恶意软件的功能片段，给出了部分反汇编代码以及对应的数据内容，试分析该功能片段：

- (1) 结合表中代码，推测 sub_4012B0 函数的作用，分析 byte_408040、byte_408060 数据内容分别表示什么内容；（4 分）
- (2) 结合表中代码，试描述该片段的执行流程和行为；（6 分）
- (3) 分析恶意代码作者以下列方式编写代码的原因。（2 分）

【提示：LoadLibraryA 函数原型是：HMODULE LoadLibraryA(LPCTSTR lpLibFileName)；

GetProcAddress 函数原型是：FARPROC GetProcAddress(HMODULE hModule, LPCSTR lpProcName)】

部分反汇编代码 & 对应的数据

sub_401300		.data:00408040 byte_408040
.text:00401300	push esi	db 36h, 0E4h, 77h, 63h, 78h, 0BFh, 3Ch,
.text:00401301	push 0Dh	0E2h, 49h, 86h, 85h, 93h, 5Bh, 3 dup(0)
.text:00401303	push offset byte_408040	;ascii: '6 鎗 cx',0BFh,3Ch,'鉦曉攀',0
.text:00401308	call sub_4012B0	
.text:0040130D	add esp, 8	
.text:00401310	push eax	.data:00408060 byte_408060
.text:00401311	call ds:LoadLibraryA	db 0EAh, 60h, 0EFh, 0F7h, 0ADh, 49h, 0B7h,
.text:00401317	mov esi, eax	78h, 86h, 38h, 5Bh, 0A6h, 64h, 0CDh, 0E4h, 0
.text:00401319	test esi, esi	;ascii: '闖秣璉穢',86h,38h,['弯',0
.text:0040131B	jz loc_4015AC	
.text:00401321	push 0Fh	
.text:00401323	push offset byte_408060	.data:00408070 byte_408070
.text:00401328	call sub_4012B0	db 31h, 0EEh, 64h, 69h, 51h, 0BAh, 6Dh,0A2h,
.text:0040132D	add esp, 8	6, 2 dup(90h), 0BEh, 5Bh, 3 dup(0)
.text:00401330	push eax	;ascii: '1 賴 iQ 簪',0A2h,6,'惇縵',0
.text:00401331	push esi	
.text:00401332	call ds:GetProcAddress	
.text:00401338	push 0Dh	.data:00408080 byte_408080
.text:0040133A	push offset byte_408070	db 7, 33h, 2 dup(24h), 0Dh, 28h, 23h, 33h,
.text:0040133F	mov dword_408F48, eax	20h, 33h, 38h, 41h
.text:00401344	call sub_4012B0	;ascii: 7,'3\$\$',0Dh,'(#3 38A'
.text:00401349	add esp, 8	
.text:0040134C	push eax	
.text:0040134D	push esi	
.text:0040134E	call dword_408F48	
.text:00401354	push 0Ch	
.text:00401356	push offset byte_408080	
.text:0040135B	mov dword_408F44, eax	
.text:00401360	call sub_4012B0	
.text:00401365	add esp, 8	
.text:00401368	push eax	
.text:00401369	push esi	
.text:0040136A	call dword_408F48	

2. 以下是一个 C 语言编写的代码片段，要求：

- (1) 简要介绍该函数的输入输出和主要功能？（4 分）
- (2) 使用该函数是否会带来安全风险？请简要分析。（4 分）
- (3) 给出你对该函数的修改意见，并写出修改后的函数代码。（4 分）

行号	代码
(1)	char *hello(char *dst, const char *src){
(2)	assert(NULL!=dst && NULL!=src);
(3)	char *p = dst;
(4)	while((*dst++ = *src++) != '\0');
(5)	return p;
(6)	}

四. 论述题【共 1 题，12 分】

2021 年 7 月，工业和信息化部、国家互联网信息办公室、公安部联合印发通知，公布《网络产品安全漏洞管理规定》（下称《规定》），自 2021 年 9 月 1 日起施行。《规定》明确提出，从事网络产品安全漏洞发现、收集的组织或者个人通过网络平台、媒体、会议、竞赛等方式向社会发布网络产品安全漏洞信息的，应当遵循必要、真实、客观以及有利于防范网络安全风险的原则，并不得刻意夸大网络产品安全漏洞的危害和风险，不得利用网络产品安全漏洞信息实施恶意炒作或者进行诈骗、敲诈勒索等违法犯罪活动；不得将未公开的网络产品安全漏洞信息向网络产品提供者之外的境外组织或者个人提供。

请结合课程学习内容，谈谈对该《规定》的认识，以及软件安全从业者合法使用技术的必要性。