武汉大学国家网络安全学院
2019-2020 学年度第二学期
《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	总分
分值				

一. 计算题（共 3 小题，每小题 7 分，共 21 分）

1. 以下是某硬盘的分区表信息，计算各分区的大小。（最终结果的单位取 G，小数点后取 1 位，四舍五入，给出计算过程）

```
00000001B0  00 00 00 00 00 00 00 00  E0 A2 4A 62 00 00 80 01
00000001C0  01 00 0C EF FF FF 3F 00  00 00 31 3A 80 02 00 00
00000001D0  C1 FF 0F EF FF FF 70 3A  80 02 60 07 9C 1A 00 00
00000001E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000001F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 55 AA
```

2. 下图为某 PE 程序的引入节（.rdata 节）在内存中的存储布局，其开始位置的 RVA 为 2000H。试分析 MessageBox 函数和 wsprintfA 函数的真实地址。

地址	HEX 数据																ASCII
00402000	E2	BB	F8	76	00	00	00	00	11	EA	89	76	47	3F	85	76	乞 鴿 ....■陟vG?鄂
00402010	00	00	00	00	50	20	00	00	00	00	00	00	00	00	00	00	....P ----------
00402020	72	20	00	00	00	20	00	00	58	20	00	00	00	00	00	00	r ... ...X ------
00402030	00	00	00	00	9A	20	00	00	08	20	00	00	00	00	00	00	....?..■ ------
00402040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	----------------
00402050	64	20	00	00	00	00	00	00	8C	20	00	00	80	20	00	00	d ......?..■ --
00402060	00	00	00	00	80	00	45	78	69	74	50	72	6F	63	65	73	....■.ExitProces
00402070	73	00	6B	65	72	6E	65	6C	33	32	2E	64	6C	6C	00	00	s.kernel32.dll..
00402080	62	02	77	73	70	72	69	6E	74	66	41	00	9D	01	4D	65	b wsprintfA.?Me
00402090	73	73	61	67	65	42	6F	78	41	00	75	73	65	72	33	32	ssageBoxA.user32
004020A0	2E	64	6C	6C	00	00	00	00	00	00	00	00	00	00	00	00	.dll............
004020B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	----------------
004020C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	----------------
004020D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	----------------
004020E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	----------------
004020F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	----------------

3. 试画出以下函数调用 printf 函数时的栈帧结构，并给出该函数运行结果。（注：编译配置为 x86 平台，并关闭所有安全和优化选项）

```
int main(void)
{
    int i=1, j=2;
    char buf[]="1234";
    printf("%s %d %d %d\n", buf, i);
    return 0;
}
```

二、 **简答题**（共 6 小题，每小题 8 分，共 48 分）

1. 试阐述 NTFS 和 FAT32 的异同.
2. 木马的文件管理与资源管理器的文件管理有什么异同?
3. 计算机病毒的感染与黑客攻击的 Shellcode 注入有什么异同?
4. PE 结构中重定位节的结构，以及重定位的作用。
5. Fuzzing 对哪些缺陷挖掘有效？该挖掘方法存在哪些局限性？
6. 请描述 Windows 下的软件行为拦截方法和实现层次，请对各类软件行为拦截技术进行具体描述，并分析其优缺点。软件行为拦截在安全领域有哪些具体的应用？

三、 **缺陷分析题**（共 2 小题，第 1 小题 16 分，第 2 小题 15 分，共 31 分）

分析以下两个代码片断中存在的安全问题，说明其可能带来的安全风险，并尝试进行修补。

1. C 语言代码片断分析 **(16 分)**

行号	代码
	void handleConnection (int socket) {
1.	char user[100] ; char pass[200] ; char buff[400] ;
2.	int c = 0 ;
3.	strncpy (buff , "USER: " , 100) ;
4.	send (socket , buf f , 7 , 0) ;
5.	recv (socket , buf f , 400 , 0) ;
6.	strncpy (user , buff , 100) ;
7.	snprintf (buff , 400 , " Hello %s \ nPASS : " ,user) ;
8.	c = strlen (buff) + 1 ;
9.	send (socket , buff , c , 0) ;
10.	recv (socket , buff , 400 , 0) ;
11.	strcpy (pass , buff) ;
12.	strncpy (buff , "Logged in " , 100) ;
13.	send (socket , buff , 23 , 0) ;
	}

2. Python 代码片断分析 **(15 分)**

行号	代码
1.	def storePassword(username, password):
2.	hasher = hashlib.new(“md5”)
3.	hasher.update(password)
4.	hashedPassword = hasher.digest()
5.	return updateUserLogin(username, hashedPassword)