计算机科学与技术学院 2019-2020 学年第 2 学期　考试试卷

计算机系统基础（开卷 模拟考试）

2020.6.28

☐ **考试纪律：　独立完成，如发现抄袭或作弊，将按纪处理！**

☐ **诚信承诺：　自觉遵守考试纪律，独立完成考试**

不代考，不询问和抄袭他人答案。

☐ **答题要求：　用 A4 白色打印纸作答**

一、（5 分，每小题 5 分）简单题

（1）简述“存储程序”工作方式的基本思想。

二、（8 分）以下是两段 C 语言代码，函数 arith( )是直接用 C 语言写的，而 optarith( )是对 arith()函数以某个确定的 M 和 N 编译生成的机器代码反编译生成的。

```
#define M
#define N
int arith (int x, int y)
{
    int result = 0 ;
    result = x*M + y/N;
    return result;
}
int optarith ( int x, int y)
{
    int t = x;
    x << = m;
    x + = t;
    if ( y < 0 ) y+=a;
    y>>n;
    return x+y;
}
```

回答以下问题：

（1）设 **A** 是你学号的最后一位，按下列方式计算程序中 **m** 和 **n** 的值（十进制）。

m = 1+**A**%7 = _____

n = 1+**A**%5 = _____

（2）根据上面计算出来的 **m**、**n** 的值和函数 arith()，推断 optarith()函数中 **a** 的值是多少？

（3）根据 **m**、**n** 的值和函数 optarith()，推断函数 arith()中 M 和 N 的值各是多少？要求：写出必要的分析过程。

三、（18 分）已知以下关于 Lab3 Bang 阶段的信息，请完成填空。

```
08048e6d <test>:
 8048e6d:   55                      push   %ebp
 8048e6e:   89 e5                   mov    %esp,%ebp
 8048e70:   53                      push   %ebx
 8048e71:   83 ec 24                sub    $0x24,%esp
 8048e74:   e8 6e ff ff ff          call   8048de7 <uniqueval>
 8048e79:   89 45 f4                mov    %eax,-0xc(%ebp)
 8048e7c:   e8 6b 03 00 00          call   80491ec <getbuf>
 8048e81:   89 c3                   mov    %eax,%ebx
 8048e83:   e8 5f ff ff ff          call   8048de7 <uniqueval>
......
```

```
080491ec <getbuf>:
 80491ec:   55                      push   %ebp
 80491ed:   89 e5                   mov    %esp,%ebp
 80491ef:   83 ec 38                sub    $0x38,%esp
 80491f2:   8d 45 d8                lea    -0x28(%ebp),%eax
 80491f5:   89 04 24                mov    %eax,(%esp)
 80491f8:   e8 55 fb ff ff          call   8048d52 <Gets>
 80491fd:   b8 01 00 00 00          mov    $0x1,%eax
 8049202:   c9                      leave
 8049203:   c3                      ret
```

```
08048d05 <bang>:
 8048d05:   55                      push   %ebp
 8048d06:   89 e5                   mov    %esp,%ebp
 8048d08:   83 ec 18                sub    $0x18,%esp
 8048d0b:   a1 18 c2 04 08          mov    0x804c218,%eax
 8048d10:   3b 05 20 c2 04 08       cmp    0x804c220,%eax
 8048d16:   75 1e                   jne    8048d36 <bang+0x31>
 8048d18:   89 44 24 04             mov    %eax,0x4(%esp)
 8048d1c:   c7 04 24 e4 a2 04 08    movl   $0x804a2e4,(%esp)
 8048d23:   e8 a8 fb ff ff          call   80488d0 <printf@plt>
……
```

```
Breakpoint 2, 0x080491f2 in getbuf ()
(gdb) info r
eax            0x6f50c1c5   1867563461
ecx            0xf7fbd068   -134492056
edx            0xf7fbd3cc   -134491188
ebx            0x0  0
esp            0x55683458   0x55683458 <_reserved+1037400>
ebp            0x55683490   0x55683490 <_reserved+1037456>
esi            0x55686018   1432903704
edi            0x1  1
eip            0x80491f2    0x80491f2 <getbuf+6>
……
```

```
(gdb) x 0x804c218
0x804c218 <global_value>:   0x00000000
```

```
int global_value = 0;

void bang(int val)
{
    if (global_value == cookie) {
        printf("Aha Bang!: You set global_value to 0x%x.\n", global_value);
        validate(2);
    } else
        printf("Oh Misfire: global_value = 0x%x\n", global_value);
    exit(0);
}
```

回答以下问题（使用十六进制，第 1）小题每题 4 分，其余填空每空 1 分）：

1） 简述实现 bang 攻击的思路。

2） getbuf 函数中调用 Gets 函数后的返回地址是: (1)_____

3） getbuf 函数中申请的 40 字节缓冲区首地址为：(2)_____

4） 调用 getbuf 后，存放 getbuf 返回值的寄存器单元是: (3)_____

5） 调用 getbuf 时，getbuf 的栈帧底地址是：(4)_____

6） 攻击字符串的长度为: (5)_____字节

7） 全局变量 global_value 存储的地址是：(6)_____

8） 设 makecookie 采用了一个新的算法：**以你的学号首字母（U 或 I）后面的 8 个数字组成一个十六进制数，当作 cookie 使用**。

如 makecookie U201856789

0x20185678

你的 cookie 是：_____

以下是所设计的一个带有注释的攻击字符串文件的内容，请根据上面生成的新 cookie 填空：

c3 c3 c3 c3

b8 (7)_____ 25 /* mov (8)_____,%eax */

a3 18 c2 04 08 /* mov %eax, (9)_____*/

68 05 8d 04 08 /*push(10)_____*/

c3 /* ret */

90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90

（11）_____ （12）_____ （13）_____ （14）_____