CLASS 3

吴瑞欣-E41614059

Task1：查看这段代码的执行结果，解释%.20d 和%hn 的含义。

```
main(){
 int num=0x41414141;
 printf("Before: num = %#x \n", num);
 printf("%.20d%hn\n", num, &num);
 printf("After: num = %#x \n", num);
}
```

代码原样运行后报错：

```
[09/24/2018 05:57] seed@ubuntu:~/Desktop/lab2$ gcc pre1.c -o pre1
pre1.c: In function ‘main’:
pre1.c:3:2: warning: incompatible implicit declaration of built-in function ‘
ntf’ [enabled by default]
pre1.c:4:2: warning: format ‘%hn’ expects argument of type ‘short int *’, but
gument 3 has type ‘int *’ [-Wformat]
[09/24/2018 05:57] seed@ubuntu:~/Desktop/lab2$
```

添加头文件等信息后运行结果为：

```
[09/24/2018 06:00] seed@ubuntu:~/Desktop/lab2$ pre1
Before: num = 0x41414141
00000000001094795585
After: num = 0x41410014
```

%.20d：%m.n 格式中 m 为输出宽度，n 为精度控制。d 表示以十进制形式输出带符号整数，所以解释是为输出精度为 20 的整形量。

%hn: h 表示按短整型量输出，%n 并不告诉 printf（）显示什么内容，而是将已输出的字符个数放入到变元指向的变量中。在 printf（）调用返回后，这个变量将包含一个遇到%n 是字符输出的数目。

2. 解释 linux 用 root 执行下面这条命令 sysctl -w kernel.randomize_va_space=0 的含义和用途。

sysctl 是一个允许您改变正在运行中的 Linux 系统的接口. 它包含一些 TCP/IP 堆栈和虚拟内存系统的高级选项, 这可以让有经验的管理员提高引人注目的系统性能. 用 sysctl 可以读取设置超过五百个系统变量. 基于这点, sysctl 提供两个功能:读取和修改系统设置.

-w 临时改变某个指定参数的值

sysctl -w kernel.randomize_va_space=0 表示关掉 aslr 功能，ASLR（Address space layout randomization）是一种针对缓冲区溢出的安全保护技术，通过对栈、共享库映射等线性区布局的随机化，防止攻击者定位攻击代码位置，达到阻止溢出攻击的目的。

3、描述 fprintf、printf、sprintf、snprintf、vprintf 这几个函数的功能和差异。

fprintf：写入指定的流

printf：写入标准输出

sprintf:存入指定的数组 buf 内,会自动在结尾追加 null 字节。此外，因为 sprintf 可能会溢出，所以调用者要确保 buf 的尺寸

snprintf：相对于 sprintf 明确指定了尺寸，防止溢出问题

vprintf 标准库函数 vprintf 函数与 printf 函数类似,所不同的是，它用一个参数取代了变长参数表，且此参数通过调用 va_start 宏进行初始化。