上章回顾

- sed的工作流程是什么?
- sed中常见的选项有哪些?
- sed中常用的命令参数有哪些?

上章回顾

- sed的工作流程是什么?
- sed中常见的选项有哪些?
- sed中常用的命令参数有哪些?

一、账号安全控制

1、系统账户清理

- 将不必须登录系统账户的shell改为/sbin/nologin环境
- 锁定长期不登录系统的用户
- 删除无用的账号
- 锁定/etc/passwd和/etc/shadow文件

2、查看nologin用户

```
[root@localhost ~] cat /etc/passwd | grep /sbin/nologin
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
chrony:x:998:996::/var/lib/chrony:/sbin/nologin
```

1）查看可以登录到系统的用户

```
[root@localhost ~] cat /etc/passwd | grep -v /sbin/nologin
root:x:0:0:root:/root:/bin/bash
```

```
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
```

2）使用usermod、passwd命令管理用户

```
[root@localhost ~] cat /etc/passwd | grep zhangsan
zhangsan:x:1000:1000::/home/zhangsan:/bin/bash
[root@localhost ~] usermod -s /sbin/nologin zhangsan
[root@localhost ~] cat /etc/passwd | grep zhangsan
zhangsan:x:1000:1000::/home/zhangsan:/sbin/nologin
[root@localhost ~] su zhangsan
This account is currently not available.
[root@localhost ~] passwd -l lisi
锁定用户 lisi 的密码 。
passwd: 操作成功
[root@localhost ~] passwd  -S lisi
lisi LK 2024-01-10 0 99999 7 -1 (密码已被锁定。)
[root@localhost ~] passwd  -u lisi
解锁用户 lisi 的密码。
passwd: 操作成功
```

3、特殊的权限：s权限、t权限、r权限

1）suid（set user ID）

- **是一种特殊权限，仅设置在可执行文件中，而且仅在执行过程中有效；**
- **让普通用户在执行一些特定的二进制程序时，可以临时具有该文件的属主权限；**
- **suid权限可以使用数字表示，4表示添加；**

```
[lisi@localhost root]$ ifconfig ens33:1 192.168.1.10
SIOCSIFADDR: 不允许的操作
SIOCSIFFLAGS: 不允许的操作
[lisi@localhost root]$ su root
密码:
[root@localhost ~] chmod 4755 /sbin/ifconfig
[root@localhost ~] ll /sbin/ifconfig
-rwsr-xr-x. 1 root root 81976 8月   9 2019 /sbin/ifconfig
[root@localhost ~] su lisi
[lisi@localhost root]$ ifconfig ens33:1 192.168.1.10
```

```
[lisi@localhost root]$ ifconfig ens33:1
ens33:1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.10  netmask 255.255.255.0  broadcast 192.168.1.255
        ether 00:0c:29:f6:d0:6c  txqueuelen 1000  (Ethernet)
```

2）sgid（set group ID）

- 当给文件设置GUID位时，意味着执行文件的任何用户都将拥有与文件组所有者相同的权限
- 当GUID权限应用于目录时，在此目录中创建的所有子目录和文件将获得与主目录相同的组所有权（而不是创建文件和目录的用户的组所有权）。
- 当使用samba、ftp等文件服务器时，保证了不管任何人上传的目录或者文件属主和属组都是上层目录
- 可以使用chmod g+s 或者 chmod 2xxx 授权

```
[root@localhost ~] ll -d /data
drwxr-xr-x.   2 root root    6 1月  10 20:24 data
[root@localhost ~] chmod g+s /data/
[root@localhost ~] ll -d /date
drwxr-sr-x.   2 root root    6 1月  10 20:24 data
*-------------------------------------------------------*
[lisi@localhost data]$ ll
总用量 0
-rw-rw-r--. 1 lisi root 0 1月  10 20:25 a
drwxrwsr-x. 2 lisi root 6 1月  10 20:25 b
[lisi@localhost data]$
```

3）sticky（粘着位）

- Sticky Bit 通常用于共享目录，如 /tmp 目录。在这类目录中，多个用户可能都有写权限，设置 Sticky Bit 可以确保每个用户只能删除或修改自己创建的文件，而不能随意删除或修改其他用户的文件，从而保证了文件的安全性和独立性。
- 可以使用 chmod 命令来设置 Sticky Bwit。用数字表示时，Sticky Bit 对应数字 1，例如 chmod 1777 可以将目录设置为具有 Sticky Bit 权限且其他权限为 rwxrwxrwx。用符号表示时，可以使用 chmod o+t 来添加 Sticky Bit 权限，chmod o-t 来去除 Sticky Bit 权限。
- Sticky Bit 主要应用于目录，但在某些特殊情况下，也可以对文件设置 Sticky Bit，不过这种情况比较少见，且不同的系统对此的支持和行为可能有所不同。

```
[root@localhost ~] chmod +t /data/
[root@localhost data] ll -d /data/
drwxrwsrwt. 3 root root 24 1月  10 21:02 /data/
[lisi@localhost data]$ ll
总用量 0
```

```
-rwxrwxrwx. 1 root root 0 1月  10 21:02 a
drwxrwsrwx. 2 root root 6 1月  10 20:25 b
[lisi@localhost data]$ rm -rf a
rm: 无法删除"a": 不允许的操作
```

4、使用getfacl、setfacl设置权限

1）getfacl：用于获取文件或目录的访问控制列表（ACL）。

- **-R：作用是递归地显示指定目录及其子目录下所有文件和目录的 ACL 规则。不过它并不会显示父目录的 ACL 规则。**

```
[root@localhost ~] getfacl /data/
getfacl: Removing leading '/' from absolute path names
# file: data/
# owner: root
# group: root
# flags: -st
user::rwx
group::rwx
other::rwx
```

- # file: data/：显示目标文件或目录的名称。
- # owner: root：显示文件或目录的所有者是 root 用户。
- # group: root：显示文件或目录所属的组是 root 组。
- # flags: -st：显示文件或目录的特殊权限标志，这里 -st 表示设置了 Sticky Bit 权限。
- user::rwx：表示文件所有者具有读（r）、写（w）和执行（x）权限。
- group::rwx：表示文件所属组的用户具有读（r）、写（w）和执行（x）权限。
- other::rwx：表示其他用户具有读（r）、写（w）和执行（x）权限。

2）setfacl：用于设置文件或目录的访问控制列表（ACL），ACL 可以让你对文件或目录的访问权限进行更细致的控制，除了传统的所有者、所属组和其他用户的权限之外，还能为特定用户或组设置权限。

- **-m：用于修改或添加 ACL 规则。可以针对特定的用户（u:）、组（g:）等设置权限。**
  - **setfacl -m u:lisi:rw /data/ 这条命令为用户 lisi 赋予了对 /data 目录的读（r）和写（w）权限。执行该命令后，使用 getfacl /data/ 查看 ACL 信息，会看到类似 user:lisi:rw- 的输出。**
- **-x：用于删除指定的 ACL 条目。**
  - **setfacl -x u:lisi /data/ 会删除用户 lisi 针对 /data 目录的 ACL 规则。再次使用 getfacl /data/ 查看时，user:lisi:rw- 条目将不再出现。**
- **-d：用于设置默认 ACL。当在一个目录上设置了默认 ACL 后，该目录下新创建的文件和子目录会继承这个默认 ACL，但不会对已存在的文件和子目录的 ACL 进行修改。**
  - **setfacl -d -m u:lisi:r /data/ 会为 /data 目录设置默认 ACL，之后在 /data 目录下新创建的文件和子目录，用户 lisi 都会有读权限。**

- **-R：用于递归操作，可以结合不同参数实现递归添加、修改或删除 ACL 等操作。**
  - **递归添加权限：setfacl -R -m u:lisi:r /data/ 会递归地为 /data 目录及其子目录下的所有文件和目录，为用户 lisi 添加读权限。**
  - **递归删除所有 ACL 条目：setfacl -b -R /data/ 会递归地删除 /data 目录及其子目录下所有文件和目录的 ACL 规则。**

```
[root@localhost ~] setfacl -m u:lisi:rw /data/
[root@localhost ~] ll -d /data/
drwxrwsrwt+ 3 root root 24 1月  10 21:02 /data/
[root@localhost ~] getfacl /data/
getfacl: Removing leading '/' from absolute path names
# file: data/
# owner: root
# group: root
# flags: -st
user::rwx
user:lisi:rw-
group::rwx
mask::rwx
other::rwx

[root@localhost ~] setfacl -x u:lisi /data/
[root@localhost ~] getfacl /data/
getfacl: Removing leading '/' from absolute path names
# file: data/
# owner: root
# group: root
# flags: -st
user::rwx
group::rwx
mask::rwx
other::rwx
```

5、修改文件属性

1）root 用户的默认 umask 通常是 022，对于目录，权限是 777 - 022 = 755；对于文件，权限是 666 - 022 = 644。

2）普通用户的 umask 为 002，所以普通用户默认创建文件权限是 666 - 002 = 664，创建目录权限是 777 - 002 = 775。

3）可以通过/etc/bashrc /etc/profile文件设置umask，可以通过umask命令查看默认的权限

4）使用chattr、lsattr修改文件属性

- chattr：修改文件属性
  - i：添加 i 选项表示不能对文件做任何的修改、删除等操作，仅有root可以取消锁定
  - 一般用于锁定重要文件，如：passwd、shadow
- lsattr：查看文件属性

```
[root@localhost ~] chattr +i /data/a
[root@localhost ~] lsattr /data/a
----i----------- /data/a
[root@localhost ~] echo "111" > /data/a
-bash: /data/a: 权限不够
[root@localhost ~] chattr -i /data/a
[root@localhost ~] echo "111" > /data/a
[root@localhost ~] chattr +i /etc/passwd
[root@localhost ~] useradd test
useradd：无法打开 /etc/passwd
```

二、密码安全控制

1、设置密码有效期

1）仅针对新创建的用户有效

2）针对已有用户使用chage 命令设置

- chage -M 天数 用户：修改最长有效期
  - chage -M 30 zhangsan
- chage -d 0：表示下次登录时必须修改密码
  - change -d 0

3）文件中其他配置项

- PASS_MAX_DAYS 20 #密码最长使用期限
- PASS_MIN_DAYS 0 #密码最短使用期限
- PASS_MIN_LEN 5 #密码最小字符
- PASS_WARN_AGE 7 #密码临近多久到期时发出警告

```
[root@localhost ~] vim /etc/login.defs
PASS_MAX_DAYS 30

[root@localhost ~] useradd stub
[root@localhost ~] tail -1 /etc/shadow
stub:!!:19732:0:99999:7:::
```

```
[root@localhost ~] chage -M 10 stub
[root@localhost ~] tail -1 /etc/shadow
stub:!!:19732:0:10:7:::
```

> PASS_MAX_DAYS 20 #密码最长使用期限
> PASS_MIN_DAYS 0 #密码最短使用期限
> PASS_MIN_LEN 5 #密码最小字符
> PASS_WARN_AGE 7 #密码临近多久到期时发出警告

三、历史命令和自动注销

1、历史命令

1）减少记录的命令条数，减轻服务器运行压力

- /etc/profile：针对系统所有用户
- ~/.bash_profile：针对某个用户

```
[root@localhost ~] vim /etc/profile
HISTSIZE=100
```

2）注销用户后自动清空历史命令

- 在.bashrc文件中将HISTSIZE值改为0
- 在.bash_logout文件中添加 history -c，清空历史条目

```
[root@localhost ~] vim ~/.bashrc
export HISTSIZE=0
[root@localhost ~] vim ~/.bash_logout
# ~/.bash_logout
history -c

```

2、自动注销

1）当空闲时间超出时间后自动退出（单位是秒）

- 统一管理 vim /etc/profile
- 单独定制 vim ~/.bash_profile

```
[root@localhost ~] vim /etc/profile
export TMOUT=200
```

四、用户切换和提权

1、su命令切换用户

1）su - 用户：切换用户，“-”表示连同shell环境一起切换

> su 命令：这种方式属于非登录式切换，不会执行目标用户的登录脚本（如 .bash_profile 或 .profile）。这意味着一些在登录时需要初始化的环境设置不会被加载。
>
> su - 命令：属于登录式切换，会执行目标用户的登录脚本，从而加载目标用户完整的登录环境，确保所有必要的环境变量和设置都被正确初始化。

2）可以通过文件限制用户是否可以使用 su 命令

- **wheel组**
  - **是一个特殊的系统用户组，组中用户拥有部分root的功能和权限**
  - **主要用来归纳一些特殊的系统用户，用来对服务器进行一些日常管理以及高级操作**
- **/etc/pam.d/su文件：可插入式身份验证模块**
  - **auth required pamwheel.so useuid：允许wheel组中的用户登录。**

```
[root@localhost ~] gpasswd -a zhangsan wheel
正在将用户“zhangsan”加入到“wheel”组中
[root@localhost ~] cat /etc/group | grep wheel
wheel:x:10:zhangsan
[root@localhost ~] vim /etc/pam.d/su
.....
auth required pam_wheel.so use_uid

[root@localhost ~] su - zhangsan
[zhangsan@localhost root]$ su - lisi
密码：
上一次登录：三 1月 10 20:05:06 CST 2024pts/0 上
[lisi@localhost ~]$ su - zhangsan
密码：
su：拒绝权限
```

2、sudo用户提权

1）用户提权命令，服务器中一般都在使用普通用户完成着日常管理，那么无法避免需要完成一些高级操作，当普通用户没有执行权限时，必须使用sudo命令来利用root的身份完成操作

2）使用visudo命令或者 vim /etc/sudoers 进入文件中为普通用户、组授权

```
[aaa@localhost ~]$ passwd zhangsan
passwd：只有根用户才能指定用户名。
[aaa@localhost ~]$ sudo passwd zhangsan
```

```
我们信任您已经从系统管理员那里了解了日常注意事项。
总结起来无外乎这三点：

    #1) 尊重别人的隐私。
    #2) 输入前要先考虑(后果和风险)。
    #3) 权力越大，责任越大。

[sudo] aaa 的密码：
aaa 不在 sudoers 文件中。此事将被报告。

[root@localhost ~] vim /etc/sudoers
#对用户授权sudo
root    ALL=(ALL) ALL
aaa     ALL=/usr/bin/passwd,/usr/sbin/usermod
bbb     ALL=NOPASSWD: /usr/sbin/fdisk
ccc     ALL=/sbin/*,!/sbin/ifconfig
## 对组授权sudo ,其中wheel组内的所有成员可以运行所有的命令,建议注释此行，存在安全隐患
#%wheel ALL=(ALL) ALL
%admin  ALL=NOPASSWD: /usr/sbin/fdisk

[aaa@localhost ~]$ sudo passwd zhangsan
更改用户 zhangsan 的密码 。
新的 密码：
无效的密码： 密码少于 8 个字符
重新输入新的 密码：
passwd：所有的身份验证令牌已经成功更新。

[aaa@localhost ~]$ su - bbb
密码：
[bbb@localhost ~]$ fdisk -l
fdisk: 打不开 /dev/sda: 权限不够
fdisk: 打不开 /dev/sr0: 权限不够
fdisk: 打不开 /dev/mapper/centos-root: 权限不够
fdisk: 打不开 /dev/mapper/centos-swap: 权限不够

[bbb@localhost ~]$ sudo fdisk -l /dev/sda
磁盘 /dev/sda：21.5 GB, 21474836480 字节，41943040 个扇区
Units = 扇区 of 1 * 512 = 512 bytes
扇区大小(逻辑/物理)：512 字节 / 512 字节
I/O 大小(最小/最佳)：512 字节 / 512 字节
磁盘标签类型：dos
```

```
磁盘标识符：0x000be28e

   设备 Boot      Start         End      Blocks   Id  System
/dev/sda1   *        2048     2099199     1048576   83  Linux
/dev/sda2         2099200    41943039    19921920   8e  Linux LVM

[bbb@localhost ~]$ sudo passwd aaa

我们信任您已经从系统管理员那里了解了日常注意事项。
总结起来无外乎这三点：

    #1) 尊重别人的隐私。
    #2) 输入前要先考虑(后果和风险)。
    #3) 权力越大，责任越大。

[sudo] bbb 的密码：
对不起，用户 bbb 无权以 root 的身份在 localhost 上执行 /bin/passwd aaa。
[bbb@localhost ~]$
[ccc@localhost ~]$ sudo ifconfig ens33:1 192.168.1.1

我们信任您已经从系统管理员那里了解了日常注意事项。
总结起来无外乎这三点：

    #1) 尊重别人的隐私。
    #2) 输入前要先考虑(后果和风险)。
    #3) 权力越大，责任越大。

[sudo] ccc 的密码：
对不起，用户 ccc 无权以 root 的身份在 localhost 上执行 /sbin/ifconfig ens33:1 192.168.1.1。
[ccc@localhost ~]$ fdisk -l /dev/sda
fdisk: 打不开 /dev/sda: 权限不够
[ccc@localhost ~]$ sudo fdisk -l /dev/sda
[sudo] ccc 的密码：

磁盘 /dev/sda：21.5 GB, 21474836480 字节，41943040 个扇区
Units = 扇区 of 1 * 512 = 512 bytes
扇区大小(逻辑/物理)：512 字节 / 512 字节
I/O 大小(最小/最佳)：512 字节 / 512 字节
磁盘标签类型：dos
磁盘标识符：0x000be28e

   设备 Boot      Start         End      Blocks   Id  System
```

```
/dev/sda1   *        2048     2099199     1048576   83  Linux
/dev/sda2         2099200    41943039    19921920   8e  Linux LVM
```

3）使用sudo -l查看当前用户拥有哪些root权限

```
[aaa@localhost ~]$ sudo -l
[sudo] aaa 的密码：
匹配 %2$s 上 %1$s 的默认条目：
    !visiblepw, always_set_home, match_group_by_gid, always_query_group_plugin, env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS", env_keep+="MAIL
    PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONETARY LC_NAME LC_NUMERIC
    LC_PAPER LC_TELEPHONE", env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY", secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

用户 aaa 可以在 localhost 上运行以下命令：
    (root) /usr/bin/passwd, /usr/sbin/usermod
```

4）设置sudo日志文件，查看sudo使用情况

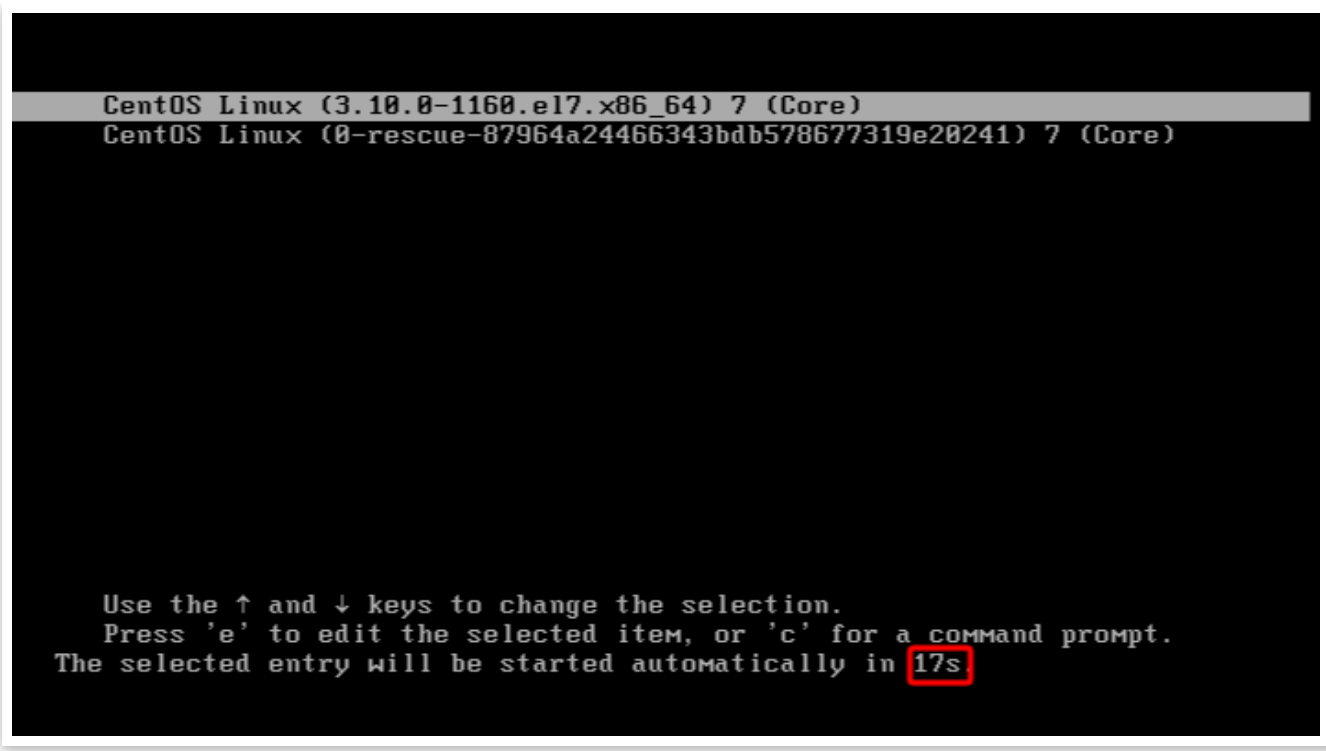
```
[root@localhost ~] vim /etc/sudoers
Defaults logfile="/var/log/sudo"
[root@localhost ~] tail -f /var/log/sudo
Jan 10 22:59:07 : bbb : user NOT in sudoers ; TTY=pts/1 ; PWD=/home/ccc ;
    USER=root ; COMMAND=/sbin/fdisk -l
```

五、系统引导与登录

1、开启安全控制

1）增加GRUB引导时间

```
[root@localhost ~] /boot/grub2/grub.cfg
set timeout=20
```



2）用于linux可以通过GRUB引导菜单中输入 e 进入编辑模式，修改系统参数，安全性较低，设置进入时需要输入账号密码，账号默认为root

- grub2-setpassword：设置密码
- user.cfg：存储密码的文件，自动创建，如果取消密码删除文件即可

```
[root@localhost ~] grub2-setpassword
Enter password:
Confirm password:
[root@localhost grub2] ls
device.map  fonts  grub.cfg  grubenv  i386-pc  locale  user.cfg
```

2、终端登录控制

1）禁止普通用户登录

- touch /etc/nologin：拒绝普通用户登录，想要恢复直接删除文件即可

六、弱口令检测与端口扫描

1、弱口令检测

1）使用john工具破解弱口令账号

- make：编译软件
- clean linux-x86-64：清除之前可能产生的可执行文件以及其他相关文件

```
[root@localhost ~] tar zxvf john-1.9.0.tar.gz -C /usr/src
[root@localhost ~] cd /usr/src/john-1.9.0
[root@localhost ~] cd src
```

```
[root@localhost ~] make clean linux-x86-64
#根据系统版本进行编译（不需要配置，要求安装gcc gcc-c++）
#在run目录下 就会生成john工具
```

2）使用john工具完成密码破解

- 首先将shadow文件复制出来，仅保留新创建的用户，建议新用户密码为纯数字等简单密码
- 密码复杂程度越高破解速度越慢，实验环境中基础密码即可
- --format=crypt选项表示直接将密文密码解析为明文
- --show：格式化显示出所有被破解的密码
- --wordlist：结合密码字典匹配

```
[root@localhost run] cp /etc/shadow ~/1.txt
[root@localhost run] cat ~/1.txt
aaa:$6$W4ShBSPX$Dlz9HZopCjC.6sgFG0.cuEJMqURyi1o31c8QD2X9TMlenju7PavMcS4Qw0w5l/58ykIBV3kqIgOqMd.2qGXCa0:19732:0:99999:7:::
bbb:$6$BzAH3urE$Ru7vRJ0VllL.FwabzJod1z8VH.15USxeCBA1vVZLqzMuJq4TgUGhEnLIIvr.HsBGjZejQ7IW3nMkOqNb1wyJk/:19732:0:99999:7:::
[root@localhost run] ./john --format=crypt ~/1.txt
Loaded 2 password hashes with 2 different salts (crypt, generic crypt(3) [?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
123              (bbb)
123              (aaa)
2g 0:00:00:18 100% 2/3 0.1078g/s 317.7p/s 323.7c/s 323.7C/s 123456..pepper
Use the "--show" option to display all of the cracked passwords reliably
Session completed

[root@localhost run] ./john --show ~/1.txt
aaa:123:19732:0:99999:7:::
bbb:123:19732:0:99999:7:::

2 password hashes cracked, 0 left

[root@localhost run] ./john --wordlist=./password.lst /root/shadow.txt
```

2、使用nmap进行端口扫描

1）全称叫做：网络映射器（Network Mapper），是一种网络连接端扫描软件

2）是网络管理员必备软件之一，可以评估网络安全，也可以被黑客用来检测开放的端口

3）直接yum 安装 nmap

- nmap 127.0.0.1 #查看当前主机的TCP所有开放端口
- nmap -sU 127.0.0.1 #查看当前主机的UDP所有开放端口

- nmap -p 22 192.168.37.0/24 #查看192.168.37.0网段所有主机22端口的开放情况,ssh
- nmap -n -sP 192.168.37.0/24 #检测192.168.37.0/24网段有哪些存活主机，-n 禁用反向解析

4）常用的扫描类型

- -sS，TCP SYN扫描（半开）
- -sT，TCP 连接扫描（全开）
- -sF，TCP FIN扫描
- -sU，UDP扫描
- -sP，ICMP扫描
- -P0，跳过ping检测

```
[root@localhost run] yum -y install nmap
```

作业：

机试

su 命令管理

1、创建两个用户，其中一个可以使用 su 命令切换，另一个拒绝

sudo 命令管理

1、两个用户

a 具有 ifconfig、fdisk命令

b 具有/usr/sbin/目录下的所有命令，除 shutdown、reboot

笔试

#检查账号情况

cat /etc/passwd | grep /sbin/nologin #禁止终端登录的账号

cat /etc/passwd | grep -v /sbin/nologin #重点关注没有禁止终端登录的账号

#禁止账号登录

usermod -s /sbin/nologin nologintest #禁止用户nologintest终端登录 -s shell 指定新的shell

#恢复账号登录

usermod -s /bin/bash nologintest #恢复用户nologintest终端登录

#锁定账号

passwd -l nologintest #-l lock 锁定账号

#查看锁定状态

passwd -S nologintest #-s status 查看账号锁定状态

cat /etc/shadow #用户名后面有两个!!号

#解锁账号

passwd -u nologintest #-u unlock 解锁账号

#给编辑grub引导参数加密码

grub2-setpassword

#这个过程创建了一个/boot/grub2/user.cfg配置文件，其中包含已经加密的密码。密码的用户是root。

#如果想要删除密码，直接删除/boot/grub2/user.cfg文件就可以。

#弱口令检测

cp /etc/shadow /software/aa.txt

cd run #进入到john工具所在的run目录内

./john /software/aa.txt

./john --show /software/aa.txt #查看已经检测出来的用户有哪些

#端口检测

nmap 127.0.0.1 #查看当前主机的TCP所有开放端口

nmap -sU 127.0.0.1 #查看当前主机的UDP所有开放端口

nmap -p 22 192.168.37.0/24 #查看192.168.37.0网段所有主机22端口的开放情况,ssh

nmap -n -sP 192.168.37.0/24 #检测192.168.37.0/24网段有哪些存活主机，-n 禁用反向解析