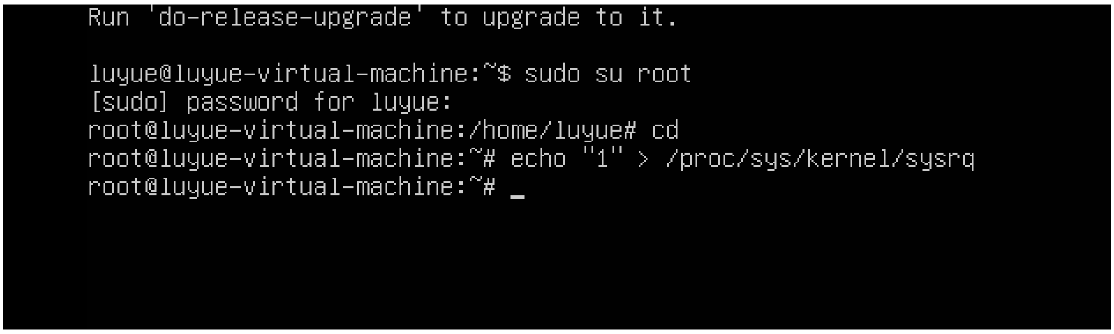
实验一:

SAK 组合键的使用

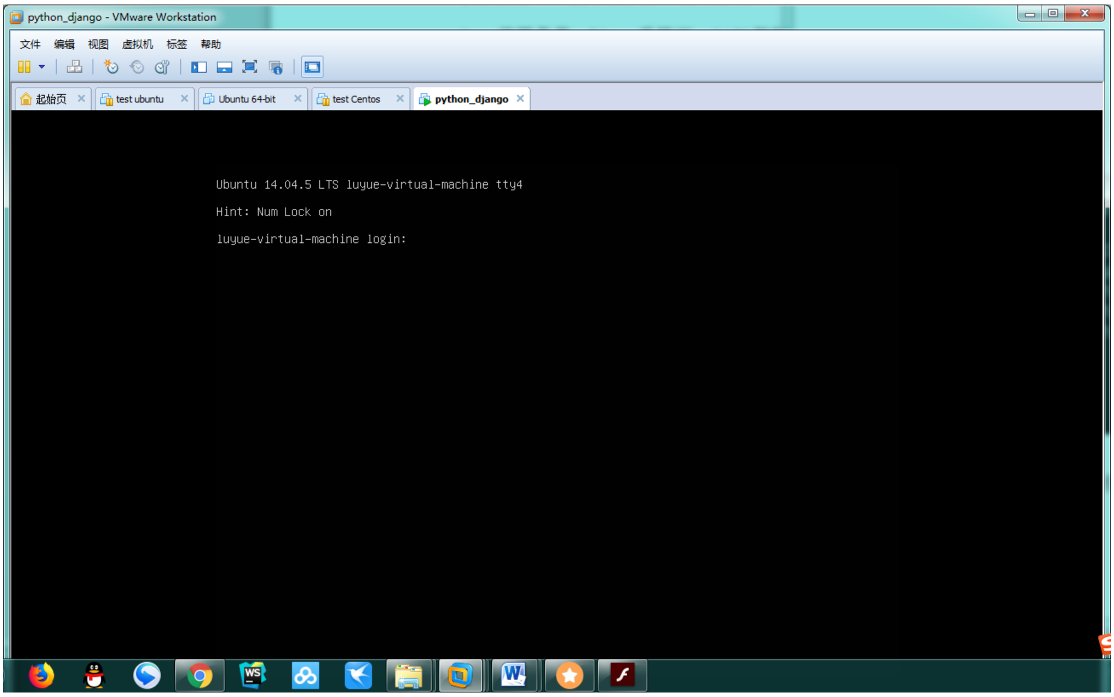
注意点:要先切换成 root 用户,其次要激活 SAK 组合键：echo “1” > /proc/sys/kernel/sysrq



```
Run 'do-release-upgrade' to upgrade to it.

luyue@luyue-virtual-machine:~$ sudo su root
[sudo] password for luyue:
root@luyue-virtual-machine:/home/luyue# cd
root@luyue-virtual-machine:~# echo "1" > /proc/sys/kernel/sysrq
root@luyue-virtual-machine:~# _
```

子任务一：使用组合键 K 登录系统

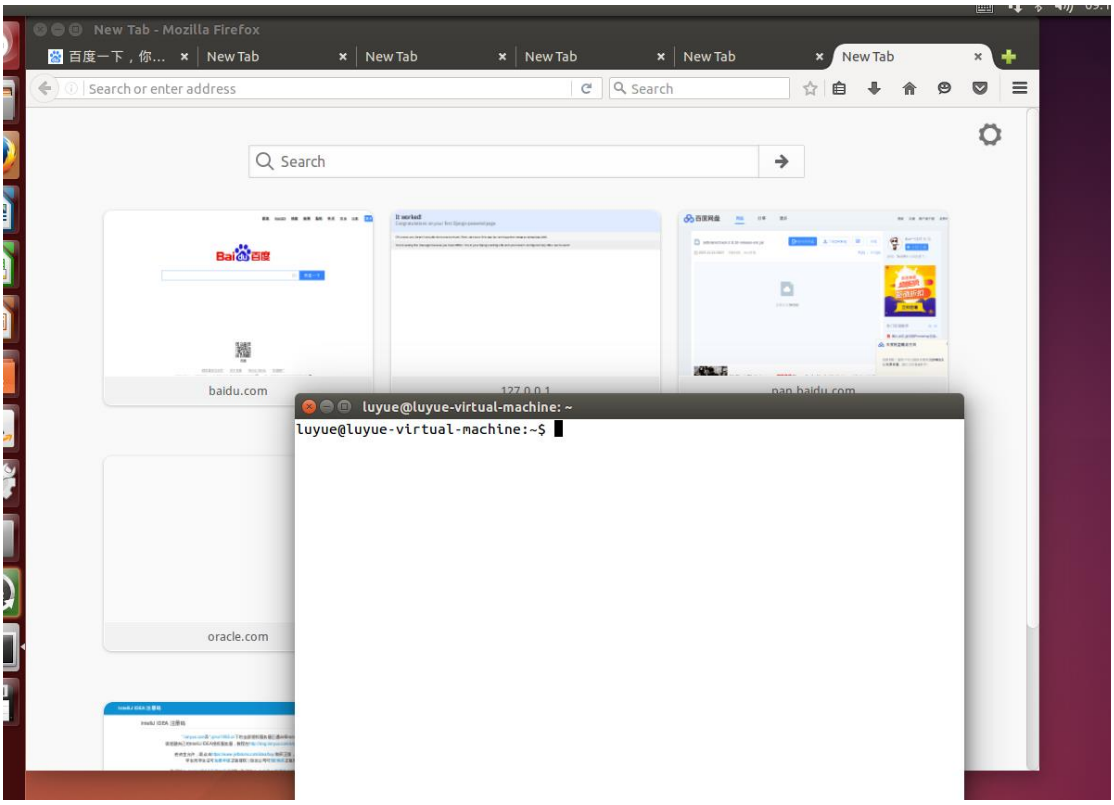
终止在当前虚拟终端上运行的所有进程


python_django - VMware Workstation
文件 编辑 视图 虚拟机 标签 帮助
起始页
test ubuntu
Ubuntu 64-bit
test Centos
python_django

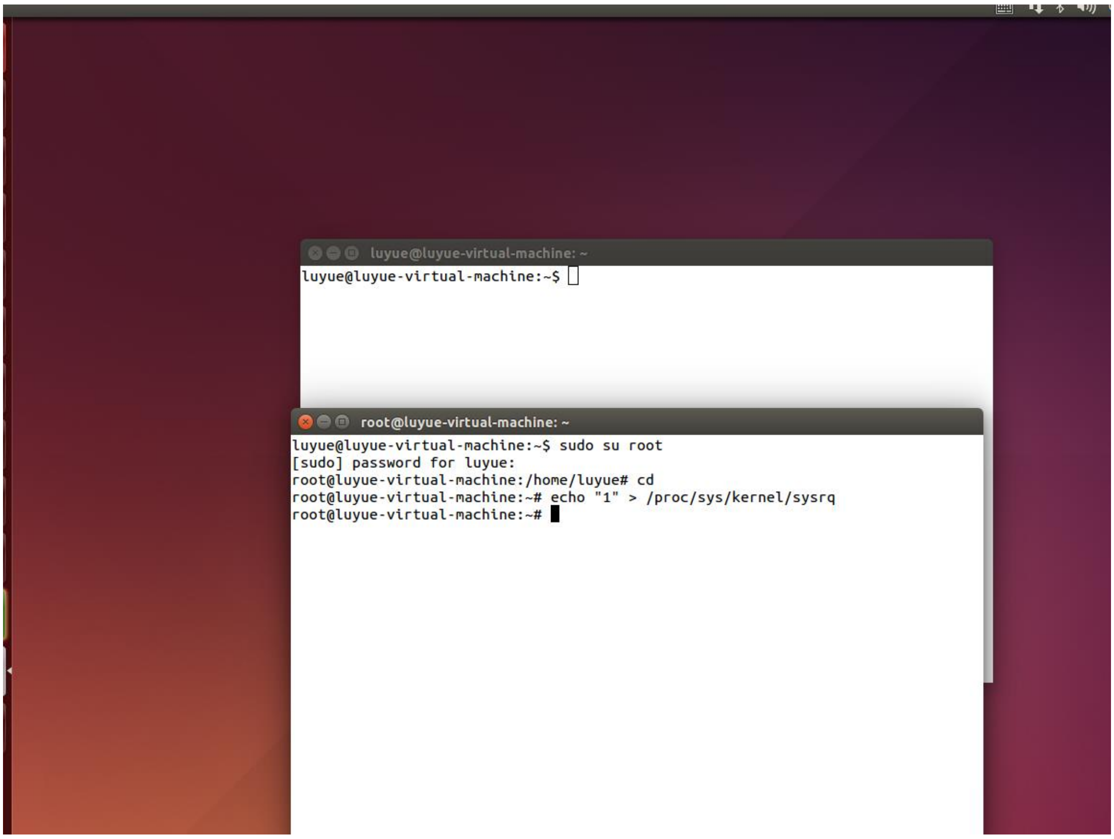
```
Ubuntu 14.04.5 LTS luyue-virtual-machine tty4

Hint: Num Lock on

luyue-virtual-machine login:
```

子任务二：**使用 f 组合键杀死一个占用内存最多的进程**

首先打开几个网页



```
luyue@luyue-virtual-machine:~$ 
```

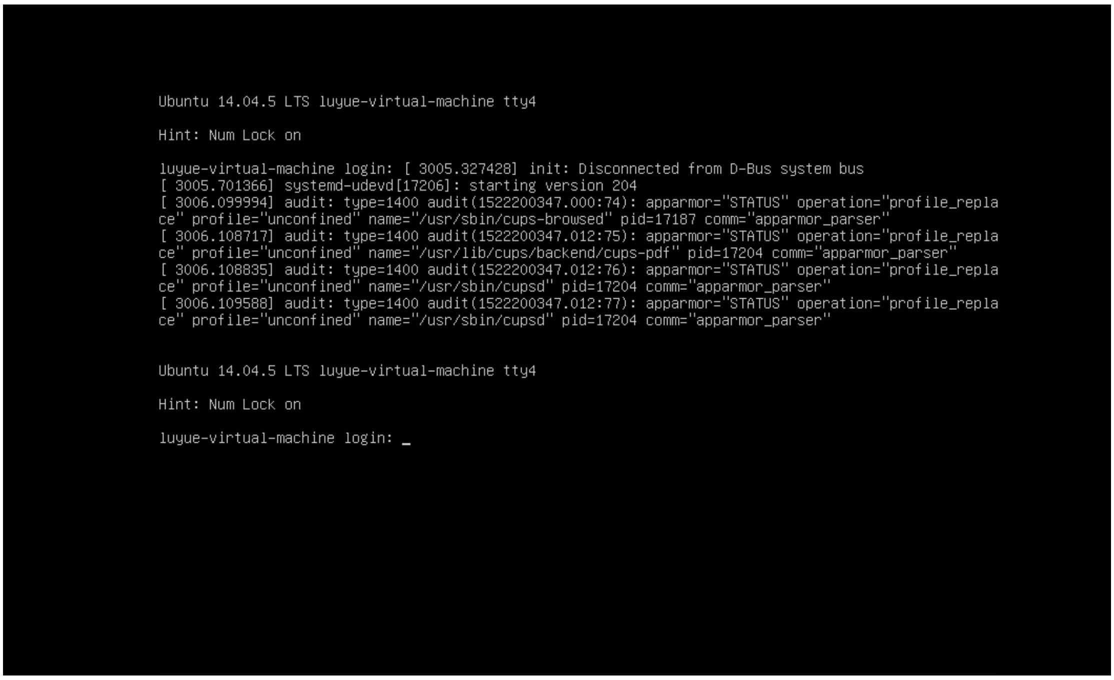


```
luyue@luyue-virtual-machine:~$ 
```

```
luyue@luyue-virtual-machine:~$ sudo su root
[sudo] password for luyue:
root@luyue-virtual-machine:/home/luyue# cd
root@luyue-virtual-machine:~# echo "1" > /proc/sys/kernel/sysrq
root@luyue-virtual-machine:~# 
```

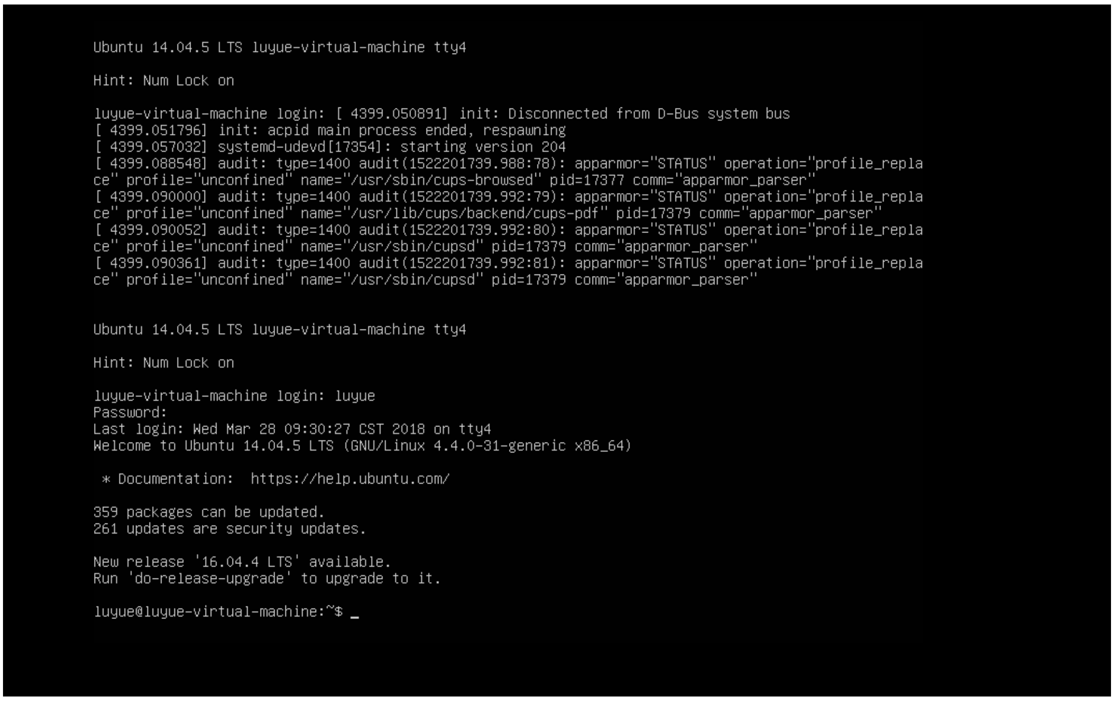
子任务三：杀死所有进程

i 组合键



```
Ubuntu 14.04.5 LTS luyue-virtual-machine tty4

Hint: Num Lock on

luyue-virtual-machine login: [ 3005.327428] init: Disconnected from D-Bus system bus
[ 3005.701366] systemd-udevd[17206]: starting version 204
[ 3006.099994] audit: type=1400 audit(1522200347.000:74): apparmor="STATUS" operation="profile_repla
ce" profile="unconfined" name="/usr/sbin/cups-browsed" pid=17187 comm="apparmor_parser"
[ 3006.108717] audit: type=1400 audit(1522200347.012:75): apparmor="STATUS" operation="profile_repla
ce" profile="unconfined" name="/usr/lib/cups/backend/cups-pdf" pid=17204 comm="apparmor_parser"
[ 3006.108835] audit: type=1400 audit(1522200347.012:76): apparmor="STATUS" operation="profile_repla
ce" profile="unconfined" name="/usr/sbin/cupsd" pid=17204 comm="apparmor_parser"
[ 3006.109588] audit: type=1400 audit(1522200347.012:77): apparmor="STATUS" operation="profile_repla
ce" profile="unconfined" name="/usr/sbin/cupsd" pid=17204 comm="apparmor_parser"


Ubuntu 14.04.5 LTS luyue-virtual-machine tty4

Hint: Num Lock on

luyue-virtual-machine login: _
```

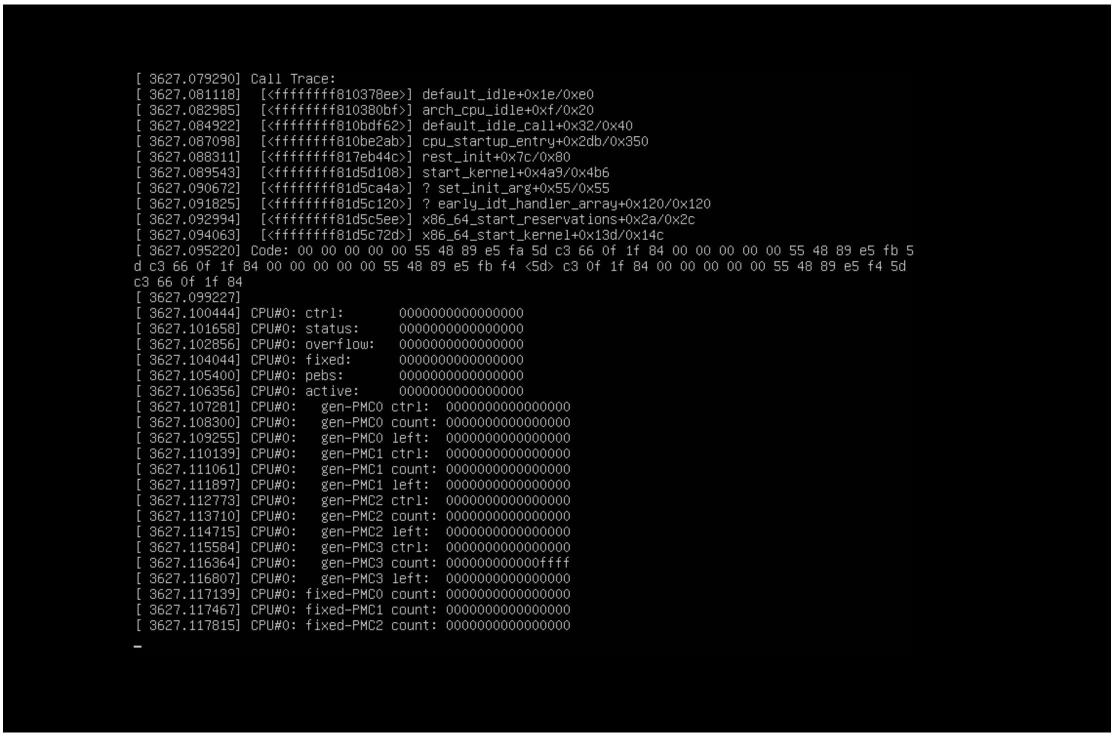
e 组合键：



```
Ubuntu 14.04.5 LTS luyue-virtual-machine tty4

Hint: Num Lock on

luyue-virtual-machine login: [ 4399.050891] init: Disconnected from D-Bus system bus
[ 4399.051796] init: acpid main process ended, respawning
[ 4399.057032] systemd-udevd[17354]: starting version 204
[ 4399.088548] audit: type=1400 audit(1522201739.988:78): apparmor="STATUS" operation="profile_repla
ce" profile="unconfined" name="/usr/sbin/cups-browsed" pid=17377 comm="apparmor_parser"
[ 4399.090000] audit: type=1400 audit(1522201739.992:79): apparmor="STATUS" operation="profile_repla
ce" profile="unconfined" name="/usr/lib/cups/backend/cups-pdf" pid=17379 comm="apparmor_parser"
[ 4399.090052] audit: type=1400 audit(1522201739.992:80): apparmor="STATUS" operation="profile_repla
ce" profile="unconfined" name="/usr/sbin/cupsd" pid=17379 comm="apparmor_parser"
[ 4399.090361] audit: type=1400 audit(1522201739.992:81): apparmor="STATUS" operation="profile_repla
ce" profile="unconfined" name="/usr/sbin/cupsd" pid=17379 comm="apparmor_parser"


Ubuntu 14.04.5 LTS luyue-virtual-machine tty4

Hint: Num Lock on

luyue-virtual-machine login: luyue
Password:
Last login: Wed Mar 28 09:30:27 CST 2018 on tty4
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

359 packages can be updated.
261 updates are security updates.

New release '16.04.4 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

luyue@luyue-virtual-machine:~$ _
```

所有进程被杀死

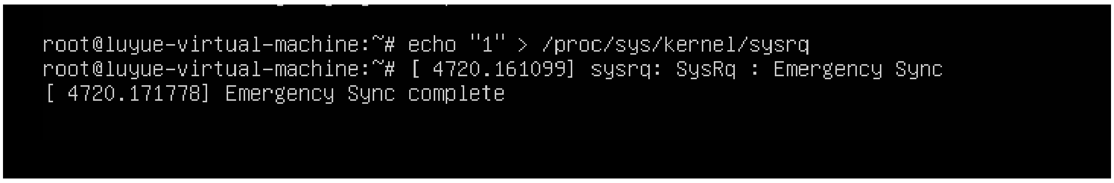
子任务三：p 组合键：**查看当前寄存器信息**



```
[ 3627.079290] Call Trace:
[ 3627.081118]  [<ffffffff810378ee>] default_idle+0x1e/0xe0
[ 3627.082985]  [<ffffffff810380bf>] arch_cpu_idle+0xf/0x20
[ 3627.084922]  [<ffffffff810bdf62>] default_idle_call+0x32/0x40
[ 3627.087098]  [<ffffffff810be2ab>] cpu_startup_entry+0x2db/0x350
[ 3627.088311]  [<ffffffff817eb44c>] rest_init+0x7c/0x80
[ 3627.089543]  [<ffffffff81d5d108>] start_kernel+0x4a9/0x4b6
[ 3627.090672]  [<ffffffff81d5ca4a>] ? set_init_arg+0x55/0x55
[ 3627.091825]  [<ffffffff81d5c120>] ? early_idt_handler_array+0x120/0x120
[ 3627.092994]  [<ffffffff81d5c5ee>] x86_64_start_reservations+0x2a/0x2c
[ 3627.094063]  [<ffffffff81d5c72d>] x86_64_start_kernel+0x13d/0x14c
[ 3627.095220] Code: 00 00 00 00 00 55 48 89 e5 fa 5d c3 66 0f 1f 84 00 00 00 00 00 55 48 89 e5 fb 5
d c3 66 0f 1f 84 00 00 00 00 00 55 48 89 e5 fb f4 <5d> c3 0f 1f 84 00 00 00 00 00 55 48 89 e5 f4 5d
c3 66 0f 1f 84
[ 3627.099227]
[ 3627.100444] CPU#0: ctrl:       0000000000000000
[ 3627.101658] CPU#0: status:     0000000000000000
[ 3627.102856] CPU#0: overflow:   0000000000000000
[ 3627.104044] CPU#0: fixed:      0000000000000000
[ 3627.105400] CPU#0: pebs:       0000000000000000
[ 3627.106356] CPU#0: active:     0000000000000000
[ 3627.107281] CPU#0:   gen-PMC0 ctrl:  0000000000000000
[ 3627.108300] CPU#0:   gen-PMC0 count: 0000000000000000
[ 3627.109255] CPU#0:   gen-PMC0 left:  0000000000000000
[ 3627.110139] CPU#0:   gen-PMC1 ctrl:  0000000000000000
[ 3627.111061] CPU#0:   gen-PMC1 count: 0000000000000000
[ 3627.111897] CPU#0:   gen-PMC1 left:  0000000000000000
[ 3627.112773] CPU#0:   gen-PMC2 ctrl:  0000000000000000
[ 3627.113710] CPU#0:   gen-PMC2 count: 0000000000000000
[ 3627.114715] CPU#0:   gen-PMC2 left:  0000000000000000
[ 3627.115584] CPU#0:   gen-PMC3 ctrl:  0000000000000000
[ 3627.116364] CPU#0:   gen-PMC3 count: 000000000000ffff
[ 3627.116807] CPU#0:   gen-PMC3 left:  0000000000000000
[ 3627.117139] CPU#0: fixed-PMC0 count: 0000000000000000
[ 3627.117467] CPU#0: fixed-PMC1 count: 0000000000000000
[ 3627.117815] CPU#0: fixed-PMC2 count: 0000000000000000
_
```

子任务4：磁盘同步

S 组合键：

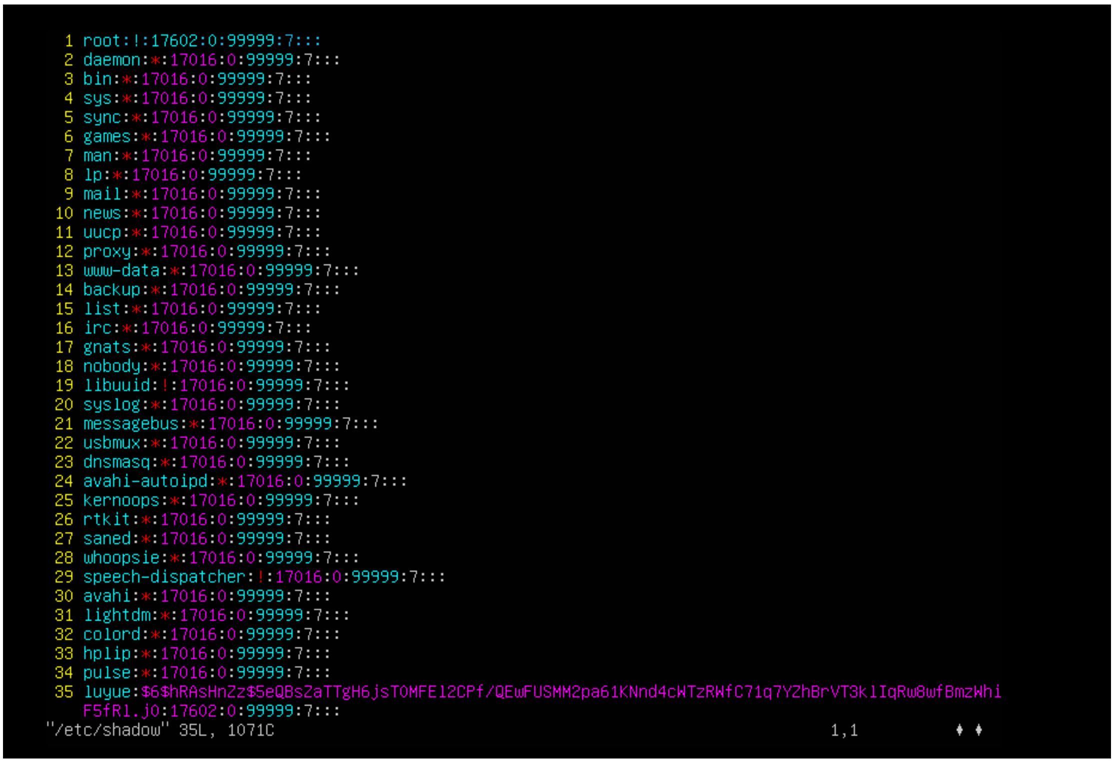


```
root@luyue-virtual-machine:~# echo "1" > /proc/sys/kernel/sysrq
root@luyue-virtual-machine:~# [ 4720.161099] sysrq: SysRq : Emergency Sync
[ 4720.171778] Emergency Sync complete
```

实验二：

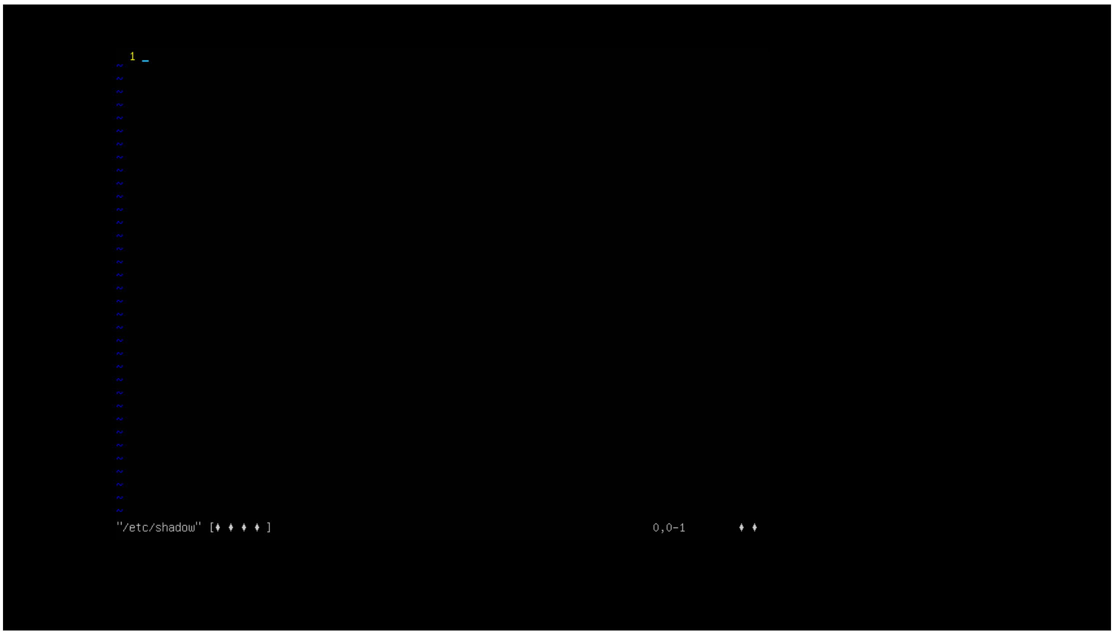
子任务一：

root 用户登录



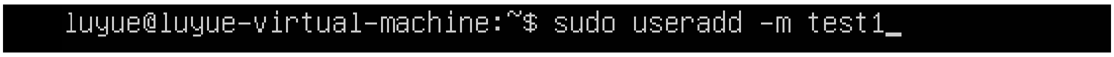
```
root:!:17602:0:99999:7:::
daemon:*:17016:0:99999:7:::
bin:*:17016:0:99999:7:::
sys:*:17016:0:99999:7:::
sync:*:17016:0:99999:7:::
games:*:17016:0:99999:7:::
man:*:17016:0:99999:7:::
lp:*:17016:0:99999:7:::
mail:*:17016:0:99999:7:::
news:*:17016:0:99999:7:::
uucp:*:17016:0:99999:7:::
proxy:*:17016:0:99999:7:::
www-data:*:17016:0:99999:7:::
backup:*:17016:0:99999:7:::
list:*:17016:0:99999:7:::
irc:*:17016:0:99999:7:::
gnats:*:17016:0:99999:7:::
nobody:*:17016:0:99999:7:::
libuuid:!:17016:0:99999:7:::
syslog:*:17016:0:99999:7:::
messagebus:*:17016:0:99999:7:::
usbmux:*:17016:0:99999:7:::
dnsmasq:*:17016:0:99999:7:::
avahi-autoipd:*:17016:0:99999:7:::
kernoops:*:17016:0:99999:7:::
rtkit:*:17016:0:99999:7:::
saned:*:17016:0:99999:7:::
whoopsie:*:17016:0:99999:7:::
speech-dispatcher:!:17016:0:99999:7:::
avahi:*:17016:0:99999:7:::
lightdm:*:17016:0:99999:7:::
colord:*:17016:0:99999:7:::
hplip:*:17016:0:99999:7:::
pulse:*:17016:0:99999:7:::
luyue:$6$hRAsHnZz$5eQBsZaTTgH6jsTOMFEl2CPf/QEwFUSMM2pa61KNnd4cWTzRWfC71q7YZhBrVT3klIqRw8wfBmzWhi
F5fRl.j0:17602:0:99999:7:::
"/etc/shadow" 35L, 1071C                                              1,1           ♦ ♦
```

普通用户登录：

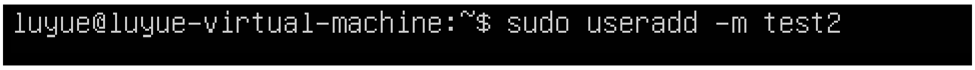


```
  1 _
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"/etc/shadow" [♦ ♦ ♦ ♦ ]                                        0,0-1        ♦ ♦
```

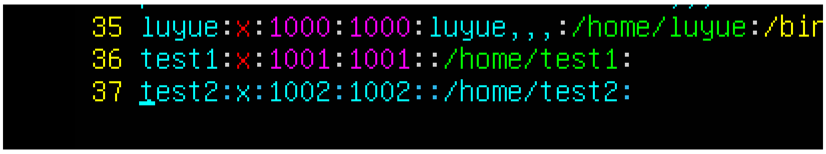
子任务二：UID 唯一性



```
luyue@luyue-virtual-machine:~$ sudo useradd -m test1_
```



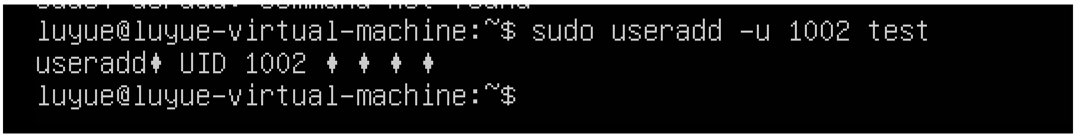
```
luyue@luyue-virtual-machine:~$ sudo useradd -m test2
```



```
luyue:x:1000:1000:luyue,,,:/home/luyue:/bir
test1:x:1001:1001::/home/test1:
test2:x:1002:1002::/home/test2:
```

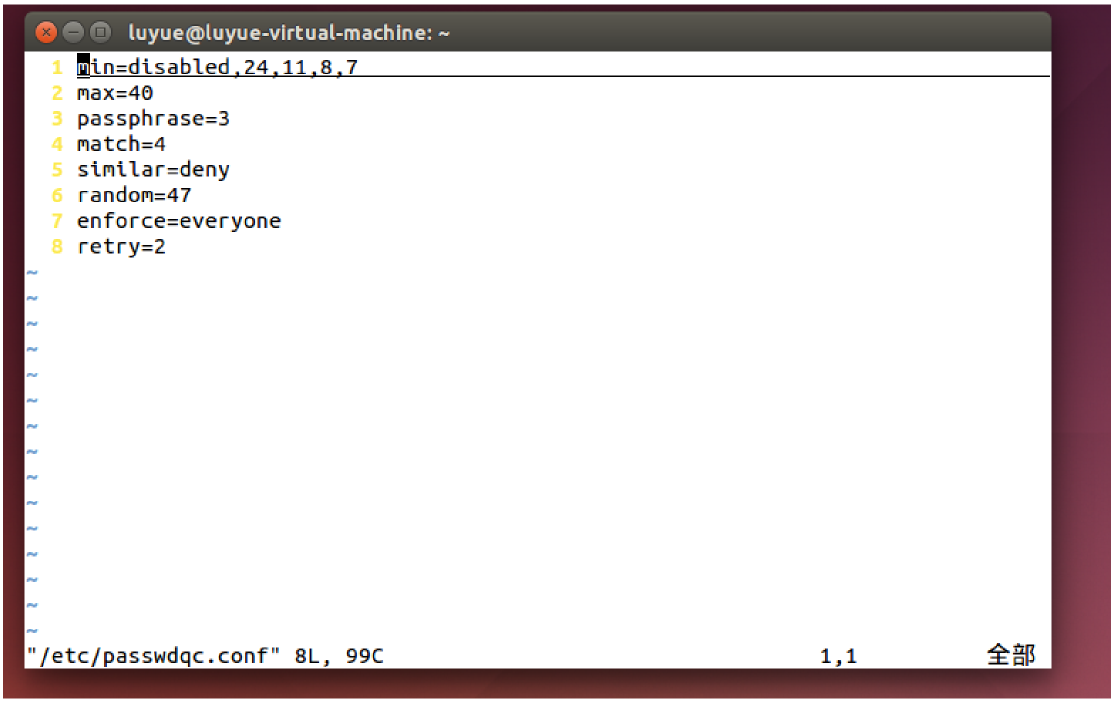
子任务三：

用户标识之验证新用户是否可以使用已存在 UID

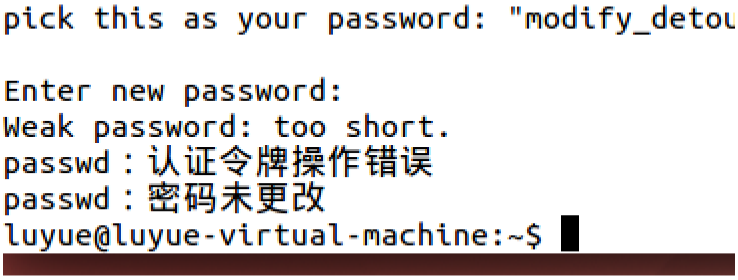


```
luyue@luyue-virtual-machine:~$ sudo useradd -u 1002 test
useradd� UID 1002 � � � �
luyue@luyue-virtual-machine:~$
```

子任务四：强口令配置，口令输入次数限定

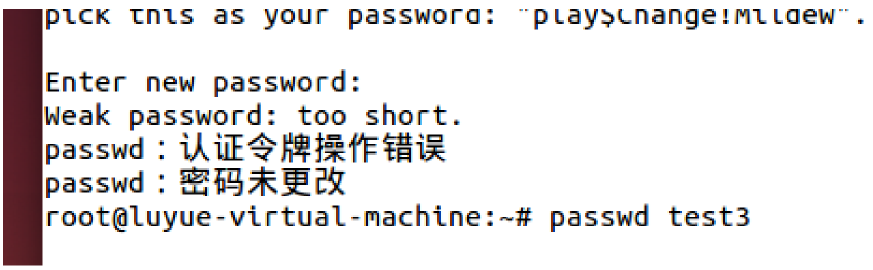


```
min=disabled,24,11,8,7
max=40
passphrase=3
match=4
similar=deny
random=47
enforce=everyone
retry=2
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"/etc/passwdqc.conf" 8L, 99C                    1,1         全部
```

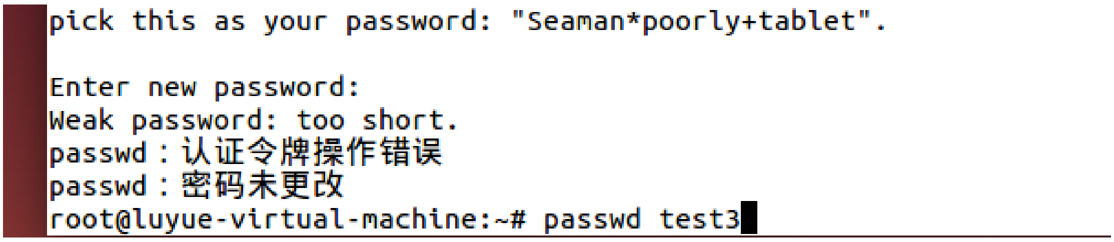


```
pick this as your password: "modify_detou

Enter new password:
Weak password: too short.
passwd：认证令牌操作错误
passwd：密码未更改
luyue@luyue-virtual-machine:~$
```

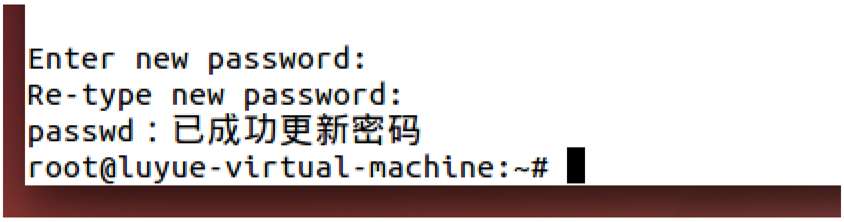
子任务五：强口令配置实践，对口令字符长度限定设置



```
pick this as your password: "play$change!Mildew".

Enter new password:
Weak password: too short.
passwd：认证令牌操作错误
passwd：密码未更改
root@luyue-virtual-machine:~# passwd test3
```



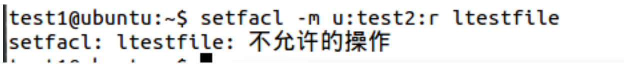
```
pick this as your password: "Seaman*poorly+tablet".

Enter new password:
Weak password: too short.
passwd：认证令牌操作错误
passwd：密码未更改
root@luyue-virtual-machine:~# passwd test3
```



```
Enter new password:
Re-type new password:
passwd：已成功更新密码
root@luyue-virtual-machine:~#
```

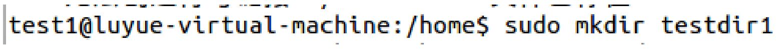
实验三：操作系统自主访问控制

子任务一：自主访问控制与磁盘文件

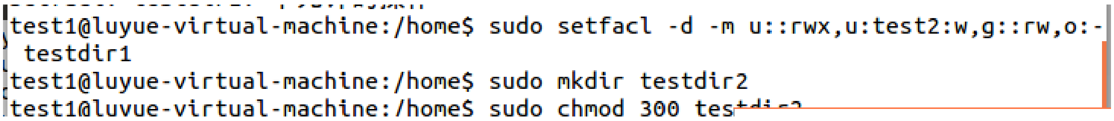


```
test1@ubuntu:~$ setfacl -m u:test2:r ltestfile
setfacl: ltestfile: 不允许的操作
```

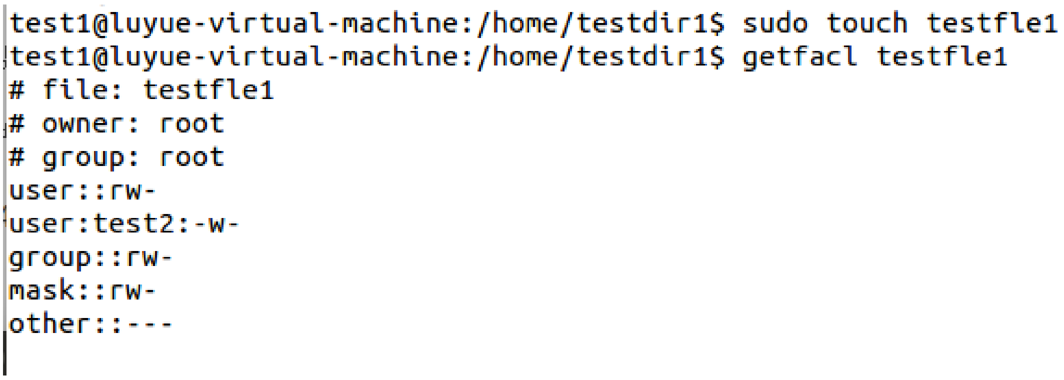
子任务二：文件权限继承



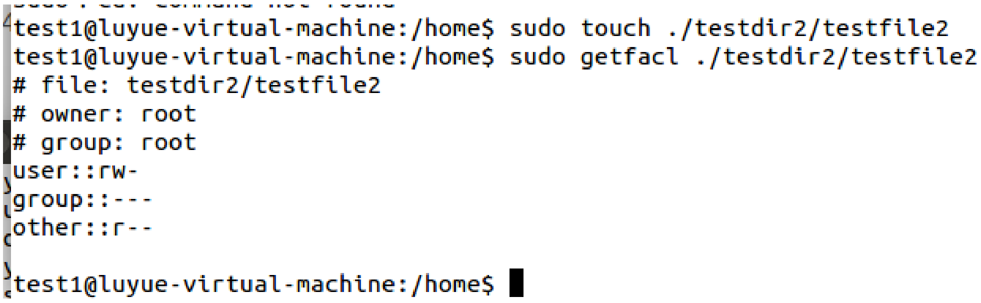
```
test1@luyue-virtual-machine:/home$ sudo mkdir testdir1
```



```
test1@luyue-virtual-machine:/home$ sudo setfacl -d -m u::rwx,u:test2:w,g::rw,o:-
 testdir1
test1@luyue-virtual-machine:/home$ sudo mkdir testdir2
test1@luyue-virtual-machine:/home$ sudo chmod 300 testdir2
```

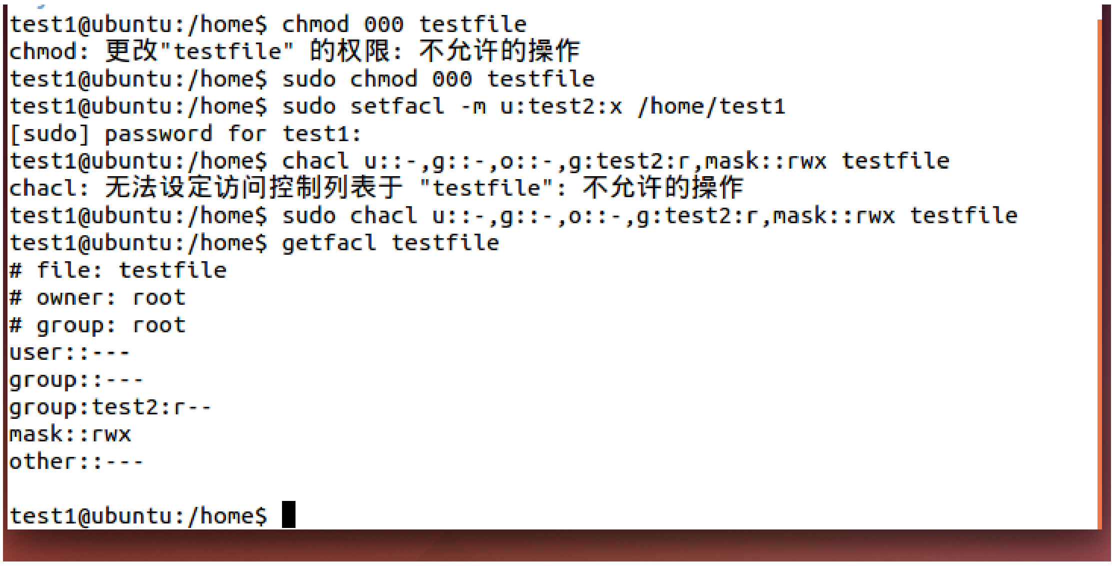


```
test1@luyue-virtual-machine:/home/testdir1$ sudo touch testfle1
test1@luyue-virtual-machine:/home/testdir1$ getfacl testfle1
# file: testfle1
# owner: root
# group: root
user::rw-
user:test2:-w-
group::rw-
mask::rw-
other::---
```

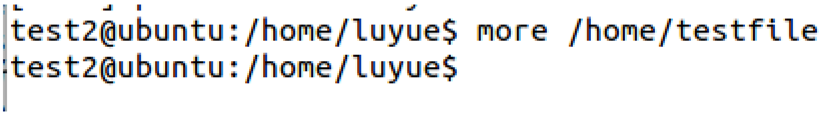


```
test1@luyue-virtual-machine:/home$ sudo touch ./testdir2/testfile2
test1@luyue-virtual-machine:/home$ sudo getfacl ./testdir2/testfile2
# file: testdir2/testfile2
# owner: root
# group: root
user::rw-
group::---
other::r--

test1@luyue-virtual-machine:/home$ █
```

子任务三：用户组权限

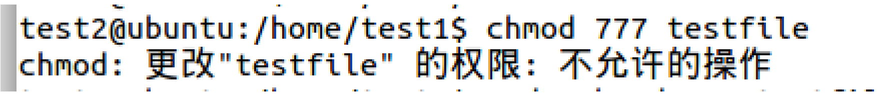


```
test1@ubuntu:/home$ chmod 000 testfile
chmod: 更改"testfile" 的权限: 不允许的操作
test1@ubuntu:/home$ sudo chmod 000 testfile
test1@ubuntu:/home$ sudo setfacl -m u:test2:x /home/test1
[sudo] password for test1:
test1@ubuntu:/home$ chacl u::-,g::-,o::-,g:test2:r,mask::rwx testfile
chacl: 无法设定访问控制列表于 "testfile": 不允许的操作
test1@ubuntu:/home$ sudo chacl u::-,g::-,o::-,g:test2:r,mask::rwx testfile
test1@ubuntu:/home$ getfacl testfile
# file: testfile
# owner: root
# group: root
user::---
group::---
group:test2:r--
mask::rwx
other::---

test1@ubuntu:/home$ █
```

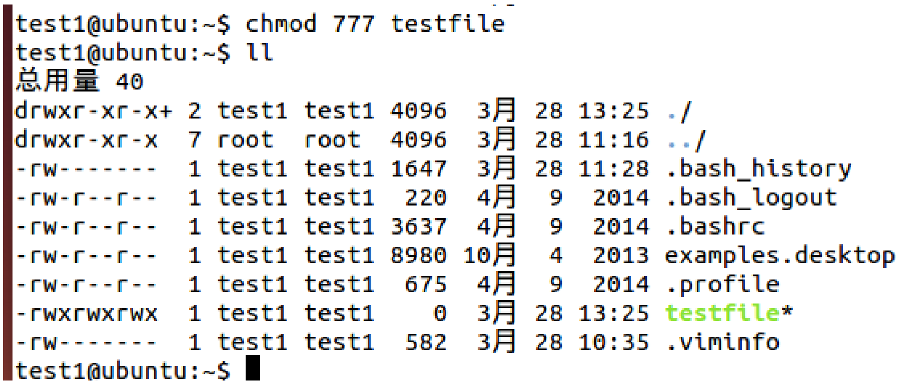


```
test2@ubuntu:/home/luyue$ more /home/testfile
test2@ubuntu:/home/luyue$
```

子任务四：自主访问控制与属主



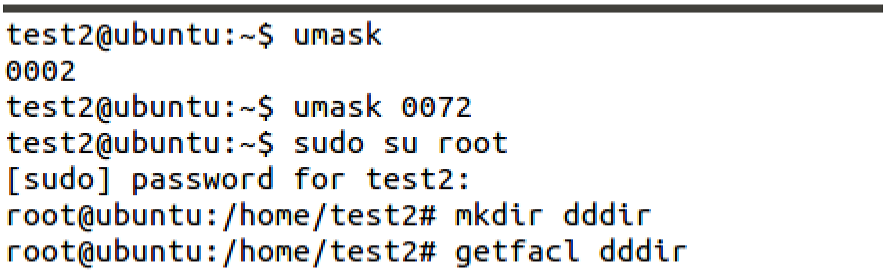
```
test2@ubuntu:/home/test1$ chmod 777 testfile
chmod: 更改"testfile" 的权限: 不允许的操作
```



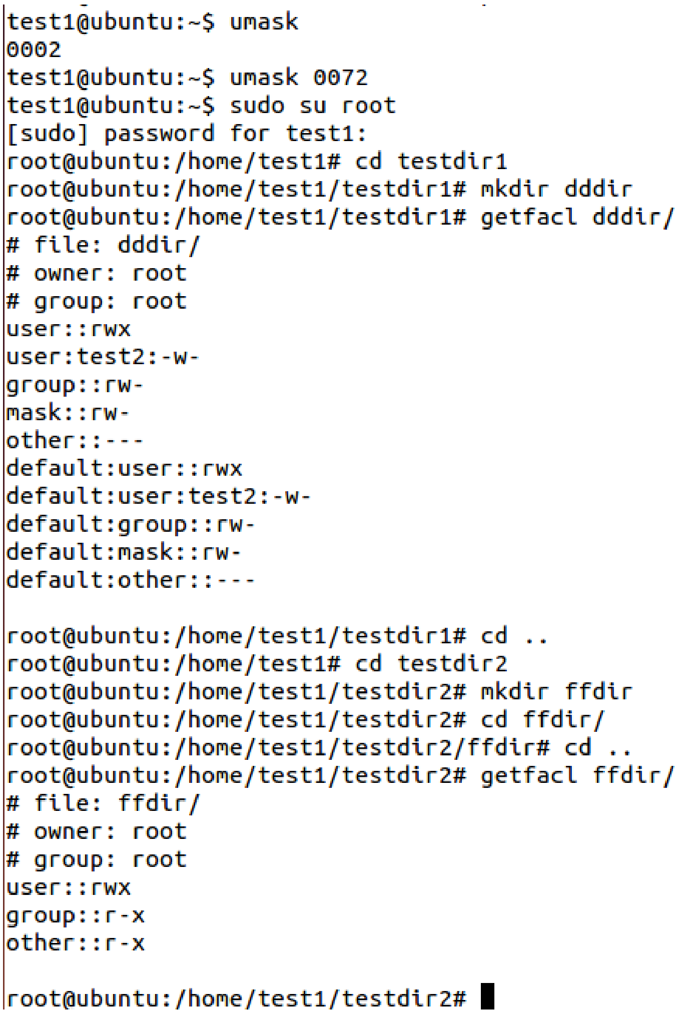
```
test1@ubuntu:~$ chmod 777 testfile
test1@ubuntu:~$ ll
总用量 40
drwxr-xr-x+ 2 test1 test1 4096  3月  28 13:25 ./
drwxr-xr-x  7 root  root  4096  3月  28 11:16 ../
-rw-------  1 test1 test1 1647  3月  28 11:28 .bash_history
-rw-r--r--  1 test1 test1  220  4月   9  2014 .bash_logout
-rw-r--r--  1 test1 test1 3637  4月   9  2014 .bashrc
-rw-r--r--  1 test1 test1 8980 10月   4  2013 examples.desktop
-rw-r--r--  1 test1 test1  675  4月   9  2014 .profile
-rwxrwxrwx  1 test1 test1    0  3月  28 13:25 testfile*
-rw-------  1 test1 test1  582  3月  28 10:35 .viminfo
test1@ubuntu:~$ █
```

课后作业：

子任务一：目录权限继承

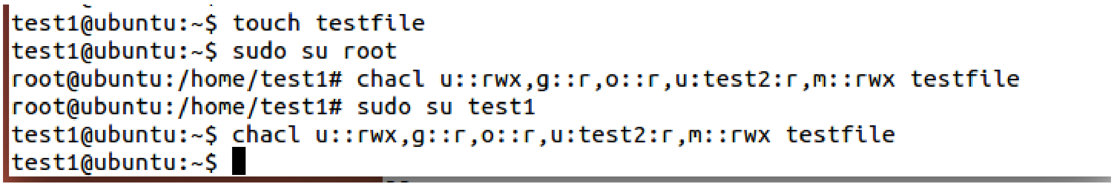


```
test2@ubuntu:~$ umask
0002
test2@ubuntu:~$ umask 0072
test2@ubuntu:~$ sudo su root
[sudo] password for test2:
root@ubuntu:/home/test2# mkdir dddir
root@ubuntu:/home/test2# getfacl dddir
```



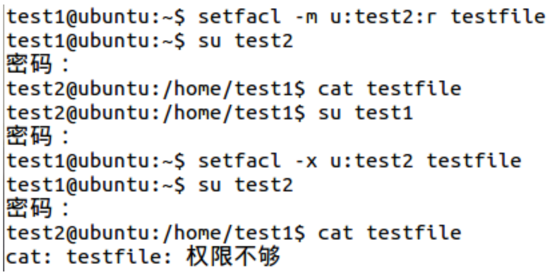
```
test1@ubuntu:~$ umask
0002
test1@ubuntu:~$ umask 0072
test1@ubuntu:~$ sudo su root
[sudo] password for test1:
root@ubuntu:/home/test1# cd testdir1
root@ubuntu:/home/test1/testdir1# mkdir dddir
root@ubuntu:/home/test1/testdir1# getfacl dddir/
# file: dddir/
# owner: root
# group: root
user::rwx
user:test2:-w-
group::rw-
mask::rw-
other::---
default:user::rwx
default:user:test2:-w-
default:group::rw-
default:mask::rw-
default:other::---

root@ubuntu:/home/test1/testdir1# cd ..
root@ubuntu:/home/test1# cd testdir2
root@ubuntu:/home/test1/testdir2# mkdir ffdir
root@ubuntu:/home/test1/testdir2# cd ffdir/
root@ubuntu:/home/test1/testdir2/ffdir# cd ..
root@ubuntu:/home/test1/testdir2# getfacl ffdir/
# file: ffdir/
# owner: root
# group: root
user::rwx
group::r-x
other::r-x

root@ubuntu:/home/test1/testdir2# 
```

子任务二：**访问控制规则可以被修改**



```
test1@ubuntu:~$ touch testfile
test1@ubuntu:~$ sudo su root
root@ubuntu:/home/test1# chacl u::rwx,g::r,o::r,u:test2:r,m::rwx testfile
root@ubuntu:/home/test1# sudo su test1
test1@ubuntu:~$ chacl u::rwx,g::r,o::r,u:test2:r,m::rwx testfile
test1@ubuntu:~$ 
```

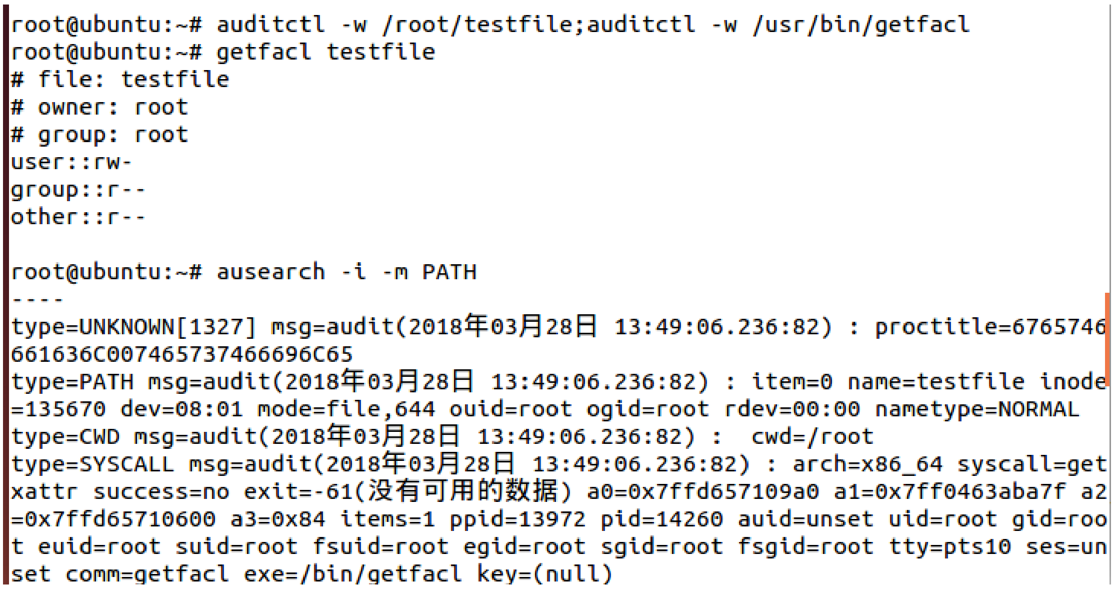
子任务三：**系统中提供了删除对客体访问控制权限的机制**



```
test1@ubuntu:~$ setfacl -m u:test2:r testfile
test1@ubuntu:~$ su test2
密码：
test2@ubuntu:/home/test1$ cat testfile
test2@ubuntu:/home/test1$ su test1
密码：
test1@ubuntu:~$ setfacl -x u:test2 testfile
test1@ubuntu:~$ su test2
密码：
test2@ubuntu:/home/test1$ cat testfile
cat: testfile: 权限不够
```

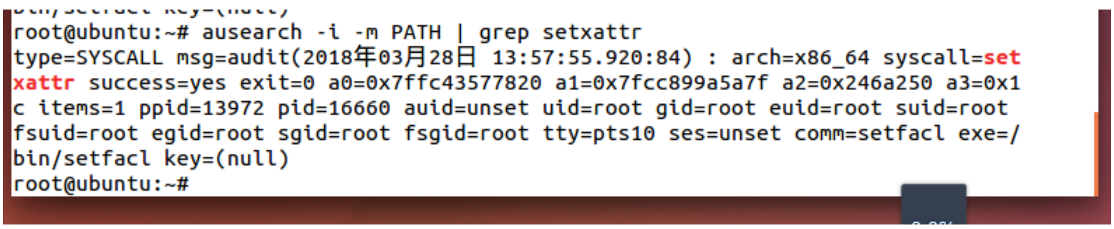
实验四：审计服务

子任务一：自主访问控制相关管理的审计之“查看文件权限”的审计



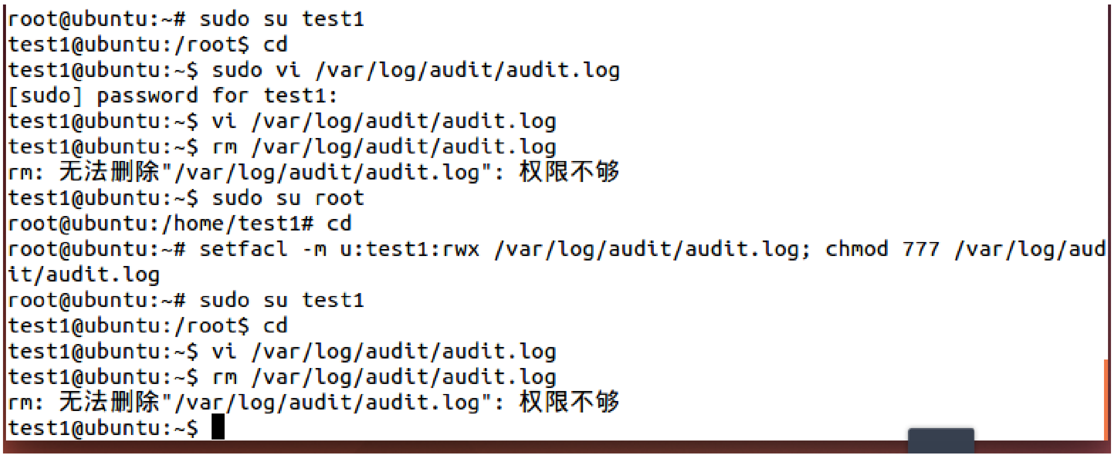
```
root@ubuntu:~# auditctl -w /root/testfile;auditctl -w /usr/bin/getfacl
root@ubuntu:~# getfacl testfile
# file: testfile
# owner: root
# group: root
user::rw-
group::r--
other::r--

root@ubuntu:~# ausearch -i -m PATH
----
type=UNKNOWN[1327] msg=audit(2018年03月28日 13:49:06.236:82) : proctitle=6765746
661636C007465737466696C65
type=PATH msg=audit(2018年03月28日 13:49:06.236:82) : item=0 name=testfile inode
=135670 dev=08:01 mode=file,644 ouid=root ogid=root rdev=00:00 nametype=NORMAL
type=CWD msg=audit(2018年03月28日 13:49:06.236:82) :  cwd=/root
type=SYSCALL msg=audit(2018年03月28日 13:49:06.236:82) : arch=x86_64 syscall=get
xattr success=no exit=-61(没有可用的数据) a0=0x7ffd657109a0 a1=0x7ff0463aba7f a2
=0x7ffd65710600 a3=0x84 items=1 ppid=13972 pid=14260 auid=unset uid=root gid=roo
t euid=root suid=root fsuid=root egid=root sgid=root fsgid=root tty=pts10 ses=un
set comm=getfacl exe=/bin/getfacl key=(null)
```

子任务二：



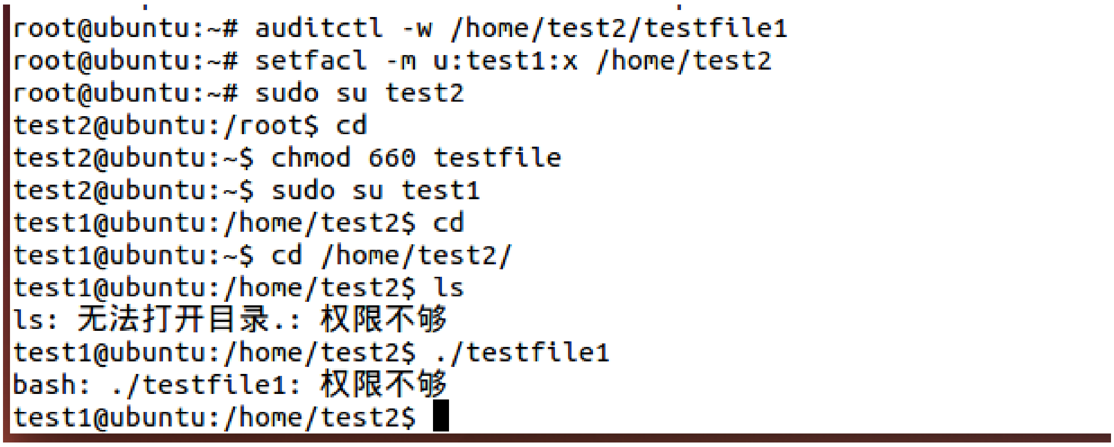
```
bin/setfacl key=(null)
root@ubuntu:~# ausearch -i -m PATH | grep setxattr
type=SYSCALL msg=audit(2018年03月28日 13:57:55.920:84) : arch=x86_64 syscall=set
xattr success=yes exit=0 a0=0x7ffc43577820 a1=0x7fcc899a5a7f a2=0x246a250 a3=0x1
c items=1 ppid=13972 pid=16660 auid=unset uid=root gid=root euid=root suid=root
fsuid=root egid=root sgid=root fsgid=root tty=pts10 ses=unset comm=setfacl exe=/
bin/setfacl key=(null)
root@ubuntu:~#
```

子任务三：

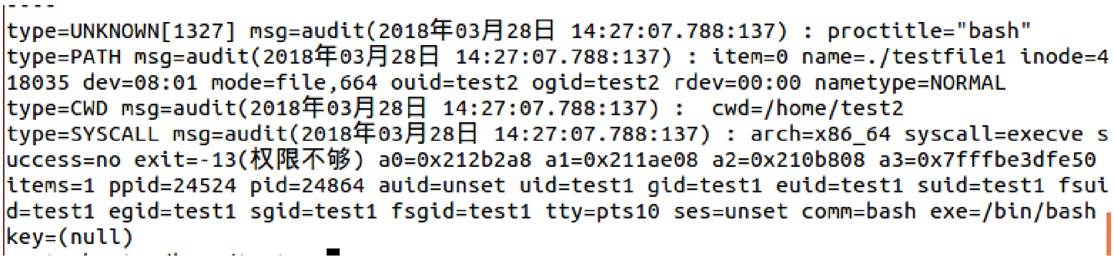


```
root@ubuntu:~# sudo su test1
test1@ubuntu:/root$ cd
test1@ubuntu:~$ sudo vi /var/log/audit/audit.log
[sudo] password for test1:
test1@ubuntu:~$ vi /var/log/audit/audit.log
test1@ubuntu:~$ rm /var/log/audit/audit.log
rm: 无法删除"/var/log/audit/audit.log": 权限不够
test1@ubuntu:~$ sudo su root
root@ubuntu:/home/test1# cd
root@ubuntu:~# setfacl -m u:test1:rwx /var/log/audit/audit.log; chmod 777 /var/log/aud
it/audit.log
root@ubuntu:~# sudo su test1
test1@ubuntu:/root$ cd
test1@ubuntu:~$ vi /var/log/audit/audit.log
test1@ubuntu:~$ rm /var/log/audit/audit.log
rm: 无法删除"/var/log/audit/audit.log": 权限不够
test1@ubuntu:~$ 
```

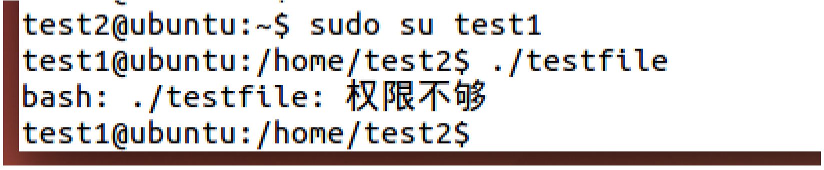
子任务四：



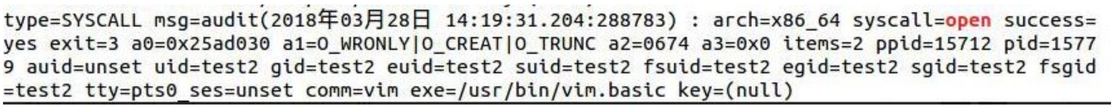
```
root@ubuntu:~# auditctl -w /home/test2/testfile1
root@ubuntu:~# setfacl -m u:test1:x /home/test2
root@ubuntu:~# sudo su test2
test2@ubuntu:/root$ cd
test2@ubuntu:~$ chmod 660 testfile
test2@ubuntu:~$ sudo su test1
test1@ubuntu:/home/test2$ cd
test1@ubuntu:~$ cd /home/test2/
test1@ubuntu:/home/test2$ ls
ls: 无法打开目录.: 权限不够
test1@ubuntu:/home/test2$ ./testfile1
bash: ./testfile1: 权限不够
test1@ubuntu:/home/test2$ 
```



```
----
type=UNKNOWN[1327] msg=audit(2018年03月28日 14:27:07.788:137) : proctitle="bash"
type=PATH msg=audit(2018年03月28日 14:27:07.788:137) : item=0 name=./testfile1 inode=4
18035 dev=08:01 mode=file,664 ouid=test2 ogid=test2 rdev=00:00 nametype=NORMAL
type=CWD msg=audit(2018年03月28日 14:27:07.788:137) :  cwd=/home/test2
type=SYSCALL msg=audit(2018年03月28日 14:27:07.788:137) : arch=x86_64 syscall=execve s
uccess=no exit=-13(权限不够) a0=0x212b2a8 a1=0x211ae08 a2=0x210b808 a3=0x7fffbe3dfe50
items=1 ppid=24524 pid=24864 auid=unset uid=test1 gid=test1 euid=test1 suid=test1 fsui
d=test1 egid=test1 sgid=test1 fsgid=test1 tty=pts10 ses=unset comm=bash exe=/bin/bash
key=(null)
```



```
test2@ubuntu:~$ sudo su test1
test1@ubuntu:/home/test2$ ./testfile
bash: ./testfile: 权限不够
test1@ubuntu:/home/test2$
```



```
type=SYSCALL msg=audit(2018年03月28日 14:19:31.204:288783) : arch=x86_64 syscall=open success=
yes exit=3 a0=0x25ad030 a1=O_WRONLY|O_CREAT|O_TRUNC a2=0674 a3=0x0 items=2 ppid=15712 pid=1577
9 auid=unset uid=test2 gid=test2 euid=test2 suid=test2 fsuid=test2 egid=test2 sgid=test2 fsgid
=test2 tty=pts0 ses=unset comm=vim exe=/usr/bin/vim.basic key=(null)
```