

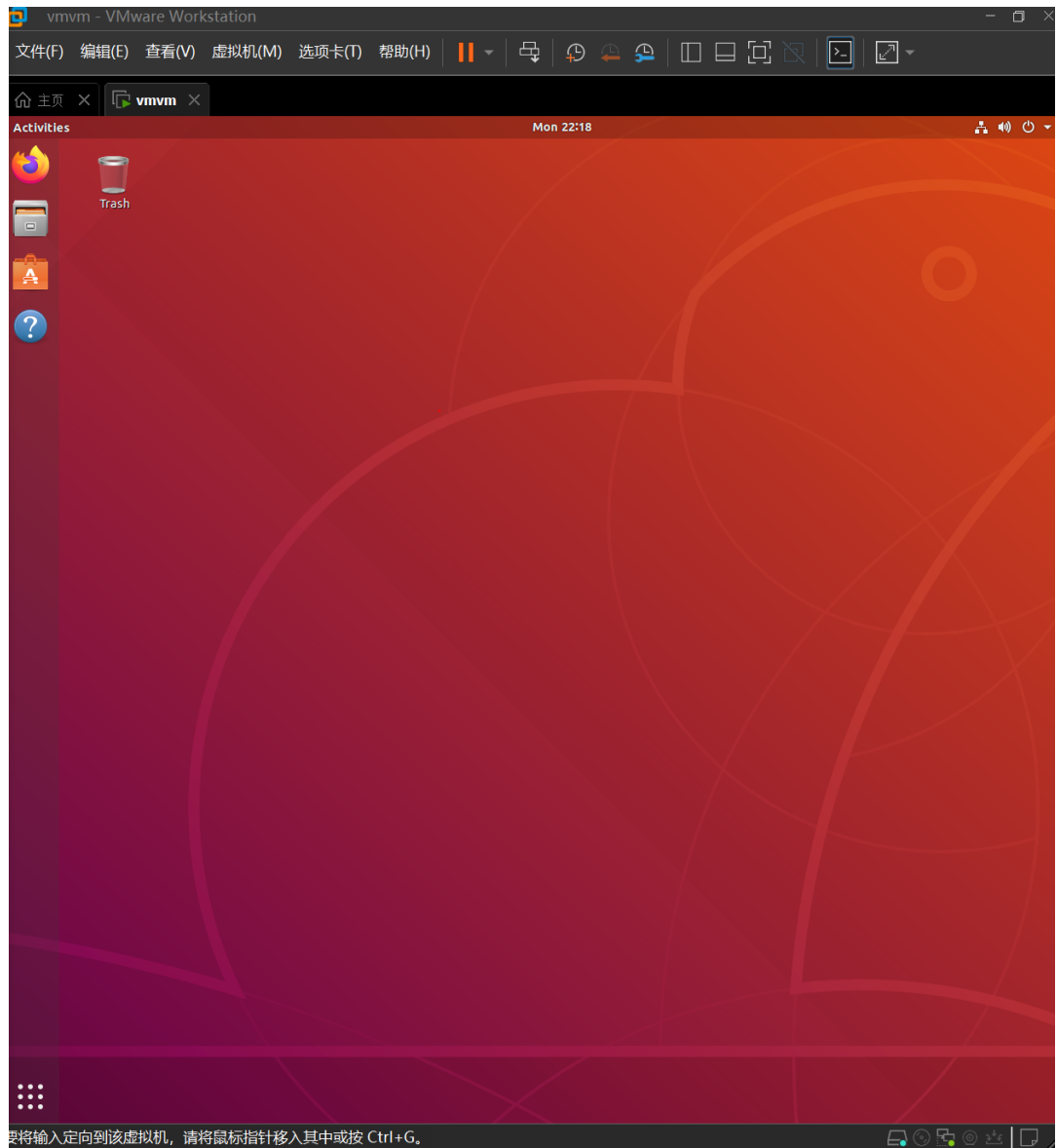
系统安全实验

521030910087 吴舒文

分析与思考

1. Linux实验

1. 打开Ubuntu虚拟机并登录



2. 打开Terminal，写出完成下列功能的Linux命令

1. 完整切换到root用户

```
root@ubuntu: /home/test
File Edit View Search Terminal Help
test@ubuntu:~$ sudo passwd root
[sudo] password for test:
Sorry, try again.
[sudo] password for test:
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
test@ubuntu:~$ su
Password:
root@ubuntu:/home/test#
```

2. 新建名为student的新账户

```
root@ubuntu: /home/test
File Edit View Search Terminal Help
test@ubuntu:~$ sudo passwd root
[sudo] password for test:
Sorry, try again.
[sudo] password for test:
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
test@ubuntu:~$ su
Password:
root@ubuntu:/home/test# useradd -m wsw
root@ubuntu:/home/test# useradd -m student
root@ubuntu:/home/test# passwd student
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@ubuntu:/home/test#
```

3. 查看账户列表，确认有student

```

root@ubuntu:/home/test# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mail List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106:./home/syslog:/usr/sbin/nologin
messagebus:x:103:107:./nonexistent:/usr/sbin/nologin
_apt:x:104:65534:./nonexistent:/usr/sbin/nologin
uidd:x:105:111:./run/uidd:/usr/sbin/nologin
avahi-autoipd:x:106:112:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:107:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:108:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
rtkit:x:109:114:RealtimeKit,,,:/proc:/usr/sbin/nologin
cups-pk-helper:x:110:116:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
speech-dispatcher:x:111:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
whoopsie:x:112:117:./nonexistent:/bin/false
kernoops:x:113:65534:Kernel Oops Tracking Daemon,,,:/usr/sbin/nologin
saned:x:114:119:./var/lib/saned:/usr/sbin/nologin
avahi:x:115:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
colord:x:116:121:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
hplip:x:117:7:HPLIP system user,,,:/var/run/hplip:/bin/false
geoclue:x:118:122:./var/lib/geoclue:/usr/sbin/nologin
pulse:x:119:123:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
gnome-initial-setup:x:120:65534:./run/gnome-initial-setup:/bin/false
gdm:x:121:125:Gnome Display Manager:/var/lib/gdm:/bin/false
test:x:1000:1000:Ubuntu1804,,,:/home/test:/bin/bash
student:x:1002:1002:./home/student:/bin/sh

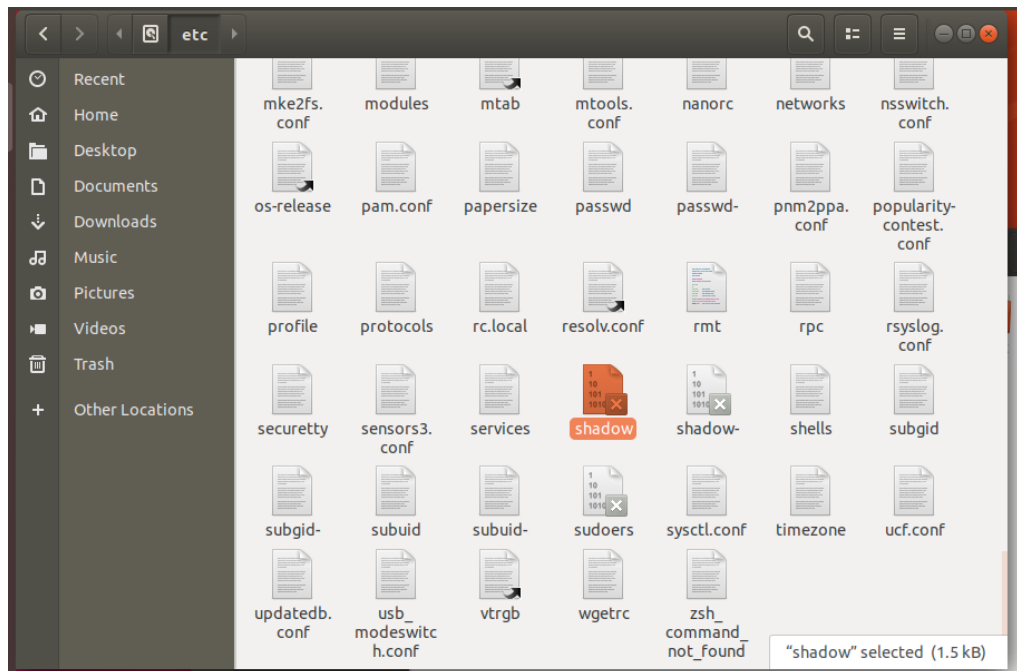
```

4. 把student的密码设置为“student”，截图展示student密码存储位置。

```

root@ubuntu:/home/test# cat /etc/shadow
root:$6$BwZM0Lh$G5B7GLPr0yGXTUoBqXUTKZv4LgU0SVX339I3mCKQ0HvJ4UuoItp.Gi/t.wfG1txFY1mNUUH9ZFxfj/.NdMa0:19619:0:99999:7:::
daemon:*:18885:0:99999:7:::
bin:*:18885:0:99999:7:::
sys:*:18885:0:99999:7:::
sync:*:18885:0:99999:7:::
games:*:18885:0:99999:7:::
man:*:18885:0:99999:7:::
lp:*:18885:0:99999:7:::
mail:*:18885:0:99999:7:::
news:*:18885:0:99999:7:::
uucp:*:18885:0:99999:7:::
proxy:*:18885:0:99999:7:::
www-data:*:18885:0:99999:7:::
backup:*:18885:0:99999:7:::
list:*:18885:0:99999:7:::
irc:*:18885:0:99999:7:::
gnats:*:18885:0:99999:7:::
nobody:*:18885:0:99999:7:::
systemd-network:*:18885:0:99999:7:::
systemd-resolve:*:18885:0:99999:7:::
syslog:*:18885:0:99999:7:::
messagebus:*:18885:0:99999:7:::
_apt:*:18885:0:99999:7:::
uidd:*:18885:0:99999:7:::
avahi-autoipd:*:18885:0:99999:7:::
usbmux:*:18885:0:99999:7:::
dnsmasq:*:18885:0:99999:7:::
rtkit:*:18885:0:99999:7:::
cups-pk-helper:*:18885:0:99999:7:::
speech-dispatcher:*:18885:0:99999:7:::
whoopsie:*:18885:0:99999:7:::
kernoops:*:18885:0:99999:7:::
saned:*:18885:0:99999:7:::
avahi:*:18885:0:99999:7:::
colord:*:18885:0:99999:7:::
hplip:*:18885:0:99999:7:::
geoclue:*:18885:0:99999:7:::
pulse:*:18885:0:99999:7:::
gnome-initial-setup:*:18885:0:99999:7:::
gdm:*:18885:0:99999:7:::
test:$5$1w06lWl6kgd0hgZSKa2UCB/5j6655yVs1bzx0r.RpYVgoeUEw.aBHvWLT9C:19500:0:99999:7:::
student:$6$yojuc7YG60xzjHk003sQl/82Q1k9iThz9w.BsBkzq14kutgEYf5vP3SUHVdIfXlJa6wFqje26tKw5zKc13fAdpj07aG9v80:19619:0:99999:7:::

```



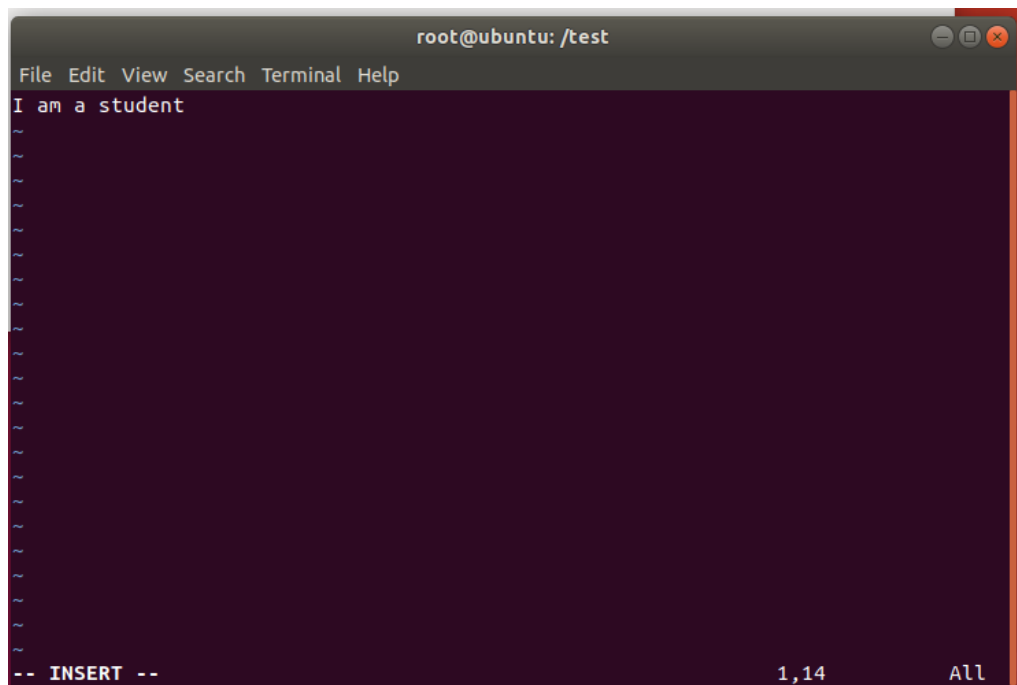
5. 在根目录下建立名为test的文件夹在根目录下建立名为test的文件夹

```
root@ubuntu:/home/test# cd /
root@ubuntu:/# mkdir test
root@ubuntu:/# cd test
root@ubuntu:/test#
```

6. 进入test文件夹，建立名为student.txt的空文件

```
root@ubuntu:/test# touch student.txt
root@ubuntu:/test#
```

7. 用vim编辑student.txt，输入“I am a student”保存退出




```
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\test>cd /d D:\PwDump
系统找不到指定的路径。

C:\Documents and Settings\test>D:

D:\>cd PwDump

D:\PwDump>PwDump.exe
PwDump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

Administrator:500:78C7649CD439B9F9AAD3B435B51404EE:75D276BB172E352BE17A99641864C5BE:::
Guest:501:NO PASSWORD*****:NO PASSWORD*****:::
HelpAssistant:1000:A31E3992865C3A0CCFA8CC5ADCD9B696:FD026B5C854CB8861E741B531669A5BB:::
SUPPORT_388945a0:1002:NO PASSWORD*****:CED3AD45055295F3B57725BE1AB2AB04:::
test:1003:01FC5A6BE7BC6929AAD3B435B51404EE:0CB6948805F797BF2A82807973B89537:::

D:\PwDump>
```

```
C:\Documents and Settings\test>D:

D:\>cd PwDump

D:\PwDump>PwDump.exe > sam1.txt
PwDump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

D:\PwDump>net user 1 1 /add
命令成功完成。

D:\PwDump>net user 2 2 /add
命令成功完成。

D:\PwDump>PwDump.exe > sam2.txt
PwDump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es
```

sam1

```
sam1 - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

Administrator:500:78C7649CD439B9F9AAD3B435B51404EE:75D276BB172E352BE17A99641864C5BE:::
Guest:501:NO PASSWORD*****:NO PASSWORD*****:::
HelpAssistant:1000:A31E3992865C3A0CCFA8CC5ADCD9B696:FD026B5C854CB8861E741B531669A5BB:::
SUPPORT_388945a0:1002:NO PASSWORD*****:CED3AD45055295F3B57725BE1AB2AB04:::
test:1003:01FC5A6BE7BC6929AAD3B435B51404EE:0CB6948805F797BF2A82807973B89537:::
```

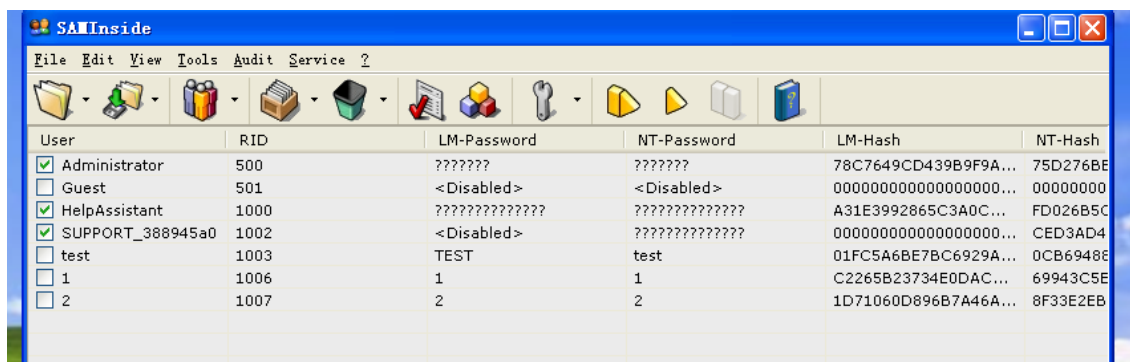
sam2

```
sam2 - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

Administrator:500:78C7649CD439B9F9AAD3B435B51404EE:75D276BB172E352BE17A99641864C5BE:::
Guest:501:NO PASSWORD*****:NO PASSWORD*****:::
HelpAssistant:1000:A31E3992865C3A0CCFA8CC5ADCD9B696:FD026B5C854CB8861E741B531669A5BB:::
SUPPORT_388945a0:1002:NO PASSWORD*****:CED3AD45055295F3B57725BE1AB2AB04:::
test:1003:01FC5A6BE7BC6929AAD3B435B51404EE:0CB6948805F797BF2A82807973B89537:::
1:1006:C2265B23734E0DACAAD3B435B51404EE:69943C5E63B4D2C1040BBCC15138B72B:::
2:1007:1D71060D896B7A46AAD3B435B51404EE:8F33E2EBE5960B8738D98A80363786B0:::
```

多了新用户1和2的信息，各行以冒号分割；各字段以三个连续冒号分割。结构可以表示成：
username:RID:LM-Hash:NT-Hash；第一个字段代表用户名；第二个字段是RID；第三个字段是经过LM加密算法生成的hash值；第四个字段是NTLM加密算法生成的hash值。

3. 根据口令破解的情况，给出安全性较高的用户口令的建议



User	RID	LM-Password	NT-Password	LM-Hash	NT-Hash
<input checked="" type="checkbox"/> Administrator	500	???????	???????	78C7649CD439B9F9A...	75D276BE
<input type="checkbox"/> Guest	501	<Disabled>	<Disabled>	0000000000000000...	00000000
<input checked="" type="checkbox"/> HelpAssistant	1000	???????????????	???????????????	A31E3992865C3A0C...	FD026B5C
<input checked="" type="checkbox"/> SUPPORT_388945a0	1002	<Disabled>	???????????????	0000000000000000...	CED3AD4
<input type="checkbox"/> test	1003	TEST	test	01FC5A6BE7BC6929A...	0CB6948E
<input type="checkbox"/> 1	1006	1	1	C2265B23734E0DAC...	69943C5E
<input type="checkbox"/> 2	1007	2	2	1D71060D896B7A46A...	8F33E2EB

不同用户应当采用不同的口令，避免使用相同的口令，防止不同用户被同时破解；口令与用户名之间应当没有语义或者逻辑上的联系；口令长度应当足够长，并且包含但不限于数字、字母、符号，同时避免字母或者数字是连续的，或者字母在键盘上连续等，防止枚举攻击；口令应当不涉及使用者的身份信息，比如生日以及身份证号等。可以生成强口令妥善保管。

4. 在Linux系统中bash文件的权限为“-rwxr-xr-x”，其含义是什么？用数字表示该文件的权限应为多少？

文件所有者可读可写可执行，文件所属用户组可读不可写可执行，其他人可读不可写可执行。对应755

5. 对于一个普通文本文件和一个机密文本文件，为保证实用性与安全性，分别设置怎样的权限较为合理，为什么？

普通文件可以设为754，-rwxr-xr---，因为保证实用性需要打开所有者的全部权限，给同组用户打开可读和可执行，同时最好防止别人恶意修改、执行，因此关闭其他人写权限和执行权限，另外因为不涉密所以可以打开可读；机密文件可以设为700，-rwx-----，为保证实用性打开所有者的全部权限，为保证机密安全性关闭其他人所有权限。

实验总结

通过这次实验我对linux和windows的命令行使用更熟练了，对操作系统的访问控制的理解更加深入，对Windows和Linux所采用的访问控制策略以及协议有了更加深入的理解；又了解了一种Linux系统的常见报错，学会了其处理方法。

总结一下SAM文件的特性：在系统运行期间，SAM文件被system账号锁定，即使是administrator账号也无法对其进行删除或拷贝等操作，需要特殊工具通过特殊方式才可以获取。SAM文件中的密码信息并非是使用明文形式保存，而是保存着两种不同加密算法得到的hash值。内存中可能会出现以明文形式存储的密码，易导致密码泄露；同时可以从repair目录攫取备份的SAM。

另了解了windows实验中出现的NTLM加密：NTLM可以在非Active Directory域成员或者Windows 2000以下版本的Windows计算机上使用；NTLM协议的配置和管理比较简单，适用于小型和中型组织；NTLM协议不仅仅适用于Windows操作系统，还适用于其他操作系统和应用程序。但是NTLM使用的哈希算法已被证实安全性较差，易被破解；NTLM协议不支持跨域认证，这意味着在多域环境下，用户需要为每个域分别进行认证。NTLM可能受到以下攻击：针对NTLM v1 hash的枚举攻击；针对Net-NTLM的重放攻击；中间人攻击。

实验中遇到的问题或建议

实验中运行apt install vim遇到Could not get lock /var/lib/dpkg/lock-frontent - open 报错，无法安装vim，使用lsof /var/lib/dpkg/lock-frontent命令找到对应进程后杀掉

```
Output information may be incomplete.
COMMAND    PID USER   FD   TYPE DEVICE SIZE/OFF  NODE NAME
unattended 2954 root    5uW  REG   8,1      0 943591 /var/lib/dpkg/lock-frontent
root@ubuntu:/home/test# kill 2954
```

之后成功安装vim

