一、给出完成下列各项功能所需要命令。陈述利用了该命令的哪个功能或选项。  
1.如何得知命令netstat众多选项中哪个选项可以打印出IP路由表？  
答：使用 man netstat命令查看netstat命令使用手册

2.删除文件名为-f的文件。

rm -- -f

3.在你完成上机作业过程中，使用什么命令将源程序文件mylist.c编译、链接生成可执行文件？可执行文件是什么名字？如何运行？

使用gcc mylist.c –o mylist命令编译、链接生成可执行文件，

可执行文件的名字是mylist，

使用命令./mylist运行。

4.去掉文件list.txt中的所有空行(所谓空行指：行内不含有任何除空格之外的字符)，存为新文件list-new.txt。

使用grep –v ’^ \*$’ list.txt > list-new.txt命令，

grep命令可以用正则表达式对文本文件过滤，-v选项用于筛选掉能匹配指定正则表达式的行，描述一个空行的正则表达式为^ \*$，即：从行首开始(^)，有零个到多个空格( \*)，然后是行尾($)

5.检索目录src以及其子孙目录中的所有文件名后缀为.c和.h文件，查找哪些文件中含有字符串TPDU，并列出在这文件中的行号。

使用find命令和grep命令。find命令可以在指定的目录树

中查找满足某个条件的文件或目录，并对查找到的满足条件的对象执行一个动作。指定查找条件为“文件名后缀为.c和.h”，动作为“查找哪些文件中含有字符串TPDU，并列出在这文件中的行号”，分别是find的-name和-exec选项。完整的命令为：

find src –name ”\*.[ch]” –exec grep –n TPDU {} /dev/null \;

这个命令的意思是在 src 目录下查找所有扩展名为 .c 或 .h 的文件，然后在这些文件中查找包含字符串 TPDU 的行，并输出这些行及其行号。其中，-name 参数用于指定要查找的文件名模式，-exec 参数用于在查找到的每个文件上执行一个命令。在这个命令中，{} 表示查找到的文件名，/dev/null 用于避免 grep 命令在只有一个文件名时输出文件名。如果您想要了解更多关于 find 和 grep 命令的信息。

6.文本文件fexc.c有几千行，保留了备份fexc0.c后另个程序员在fexc.c中作了多处修改，如何找出他在原先程序的基础上作了哪些修改？  
diff命令可以对文本文件进行比较，找出两个文件的差别。由于C语言源程序文件为文本文件，可以用diff完成上述功能。完整的命令为：diff fexc0.c fexc.c

7.用户使用低速网络从另台Linux中下载了一个2.2GB数据文件，他怀疑下载完该文件后远端文件又做了更新。如何用简便的方法验证本地和远端的两个文件的内容是否完全相同？

答：使用md5sum命令或sha1sum，分别利用本地和远端文件的16字节“消息摘要”，通过比较“消息摘要”来判断两文件内容是否完全相同。

8.目录work.d上周的备份目录为work.bak，仅有一小部分文件作了修改，如何仅仅将被修改过的文件和新创建的文件拷贝到备份目录？

答：cp命令实现了增量拷贝的功能，增量拷贝的基本功能就是检查源目录下的文件和目的目录下的同名文件的最后一次修改时间，当源文件的最后一次修改时间晚于目的文件的最后一次修改时间，或者同名的目的文件不存在时，才执行复制操作。完整的命令为：

cp –ur work.d work.bak

9.程序xftpd正在运行，随时间的变化，系统的内存资源越来越紧张。如何判断该程序在运行过程中是否存在内存泄漏？

答：ps命令的-l选项，可以打印出进程当前的SZ属性，即：进程的虚拟内存空间大小。当进程在运行过程中存在内存泄漏时，进程的虚拟内存空间大小会逐渐随时间增大。使用ps –l | grep xftpd可以看出进程xftpd属性。

这个命令的意思是列出所有进程的详细信息，并使用管道将输出传递给 grep 命令，以便在输出中搜索包含字符串 xftpd 的行。其中，-l 参数用于显示进程的详细信息，| 符号用于将 ps 命令的输出传递给 grep 命令

10.如何让系统每10秒一次周期性地列出正在下载的文件a.dat的大小？

答：自动地重复执行一个命令，利用shell的循环机制。让shell睡眠10秒钟的命令

为sleep 10。整个命令为：

while true; do ls –l a.dat; sleep 10;done

二．(共20分，每小题2分)下列说法是否正确，简要阐述理由。

1.Linux中普通用户忘记登录口令，可以通过超级用户root查出当前口令，然后重新登录。

答：错误。root也不能查出用户的登录口令，但是可以重设登录口令，让用户使用新口令登录。可以更改不能查看口令

2.Linux中命令ls -l与命令ls -l \*的执行结果相同，都是列出当前目录下的所有文件。

答：错误。ls -l列出当前目录下的所有文件和目录。\*代表当下目录下的所有目录及文件，ls –l \*列出当前目录下的所有文件（不包括目录）以及当前目录下所有目录中的内容。

一个列出当前目录下的所有文件和目录，另一个先列出当前目录下的所有文件，之后会接着列出所有子目录下的内容。

3.命令ln仅允许对普通文件实现硬连接，对目录不许硬连接操作。所以，所有目录的link数总为1。

答：错误。尽管命令ln仅允许对普通文件实现硬连接，对目录不许硬连接操作，但是，目录的硬连接由系统自动实现，当前目录下的.文件和子目录中的..文件，均是指向当前目录的硬连接，在创建新目录时系统自动实现。所以，目录的link数会大于1，一般情况下目录的link数=直属子目录数+2。

4.Linux文件权限设计为简单的三级控制，用户liu对用户sun的文件data.txt要么具有全部的读权限，要么不可以读。因此，没有办法限制liu只对文件的指定部分读。

答：错误。可以利用SUID权限，用户sun将文件data.txt的读写权限设置为rw-------，由文件所有者sun自己编写程序以实现对文件的访问，程序中的访问当然可以限制只对文件的指定部分读，但是该程序文件的属性应当为rws--x--x，用户liu只有执行这个可程序程序文件才能实现对文件data.txt的访问。

5.Linux的进程调度程序能保证大部分进程处于运行状态，只有少数进程处于阻塞状态，否则，系统的性能将大大下降。

答：错误。事实上，恰恰相反，大部分进程处于“阻塞”状态，只有所等待的条件满足后才能转换为“运行状态”。进程调度程序仅调度那些运行状态的进程。将进程的状态从“阻塞”转换为“运行”不是调度程序的任务，仅取决于外部条件的变化。

6.程序从启动运行到运行结束总共持续了t秒，占用用户时间为t1秒，系统时间为t2秒，所以有t=t1+t2成立。

答：错误。除了t1,t2，还有进程阻塞的时间。一般来说，会有t>t1+t2.

7.fork后得到两个几乎完全相同的进程，但是对内存的占用不会成倍增加。

答：正确。fork后，从逻辑上可以得到两个几乎完全相同的进程，父子进程有独立的数据段、堆栈段和指令段，但是，操作系统可以通过使用copy-on-write技术等方式，使得父子进程共享同一段物理内存，除了代码段可以共享之外，也可以共享数据段和堆栈段。

操作系统可以通过一些技术使父子进程共享同一段物理内存。

8.在bash中，圆括号和花括号都可以括起一组命令，两者没什么区别。

答：错误。首先，语法不同：（）是元字符，而｛｝不是，语法分别是（list）和{ list;}。其次,语义不同：（）执行需要重启一个子shell进程，在子进程中执行圆括号内的各个命令，而｛｝在当前shell进程中执行。

两者语法语义(用法)不同。

9.使用socket利用TCP协议编写通信程序，bind调用只应该在服务端使用，客户端使用这一调用没有意义。

答：错误。bind调用的目的是指定一个网络连接的本地端点名。客户端程序一般不使用bind调用，操作系统自动为socket分配本地IP地址和本地TCP端口号。如果本计算机有多个IP地址，客户要求必须使用其中的某个地址，或者，客户需要指定本地端口号，那么就需要用bind调用，然后再执行connect调用。

根据用户需要可以使用bind调用来指定地址或本地端口号。

10.程序用socket机制通过系统调用ret=send(sock,buf,1024,0)向远端TCP主机发送1024字节数据，系统调用执行成功的标志是返回一个非负数的整数值，ret的返回值为1024，由于TCP提供了可靠的传输层服务，所以可以断定这1024字节数据已经成功地传输到了接收端进程。

答：错误。send成功返回只能说明1024字节的数据已经拷贝到发送缓冲区中，但不能确定已经成功地传输到了接收端进程。

三．简答题

1.在字符终端上执行cat /usr/bin/\*之后屏幕开始显示乱码，按下Ctrl-C中止后，无论从键盘输入什么内容，屏幕回显的内容都是各种线条等制表符号。解释产生这一现象的原因。

答：由于这个目录下是一些可执行文件，不是文本文件。不可正常打印的字节序列顺序发往终端，当终端收到的字节序列中凑巧有正好是一个终端控制转义序列，这个转义序列导致终端字符集发生了改变。

由于该目录下是可执行文件，不是文本文件，故终端会显示为乱码。终止之后，还看到乱码是因为可能在刚才的传输中某些控制转义序列已经发了过来，并改变了终端字符集。

2.用户在字符终端上使用vi命令编辑文件，当按下Ctrl-S执行存盘(Save)操作后，终端就进入了冻结状态，随后从键盘输入了多个命令，终端显示不发生任何改变。解释产生这一现象的原因。

Ctrl-S并不执行存盘操作，因为Ctrl-S 是一个控制字符，用于暂停终端的输出。当按下 Ctrl-S 时，终端会进入冻结状态，不再显示新的输出。此时只有按下Ctrl-Q才能使冻结的终端恢复。所以，在按下Ctrl-Q之前，终端的输出会一直处于“冻结”状态。

3.写出能满足下列要求的正则表达式:

(1) 第一个字符必须是字母，其余字符必须是字母或数字或下划线。

(2) 匹配C语言算式a[i]\*b[j]，允许星号两侧有多余的空格。

写出vi中能实现下列替换要求的命令：

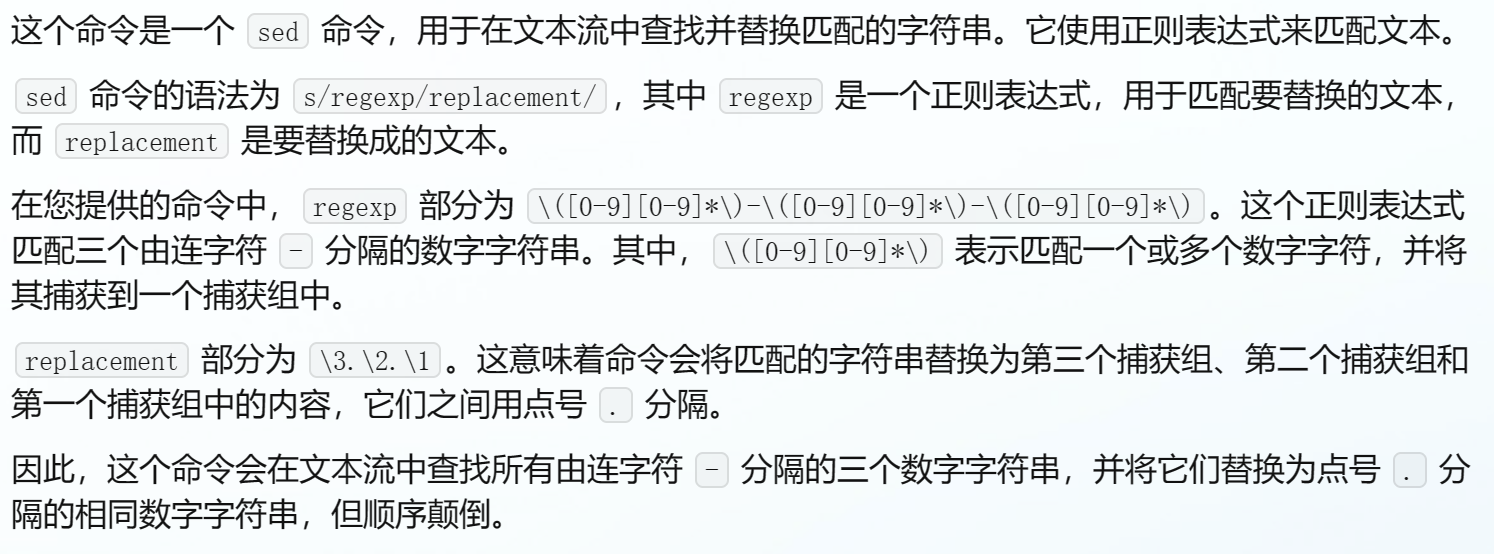
(3) 将格式为“日-月-年”的日期数据，如：27-06-2017，替换为“年.月.日”格式，如：2017.06.27。

(4) 将HTML文件中所有以尖括号括起来的标签部分替换为空格。

(1) [A-Za-z][a-zA-Z0-9\_]\*

(2) a\[i] \*\\* \*b\[j]

(3) s/\([0-9][0-9]\*\)-\([0-9][0-9]\*\)-\([0-9][0-9]\*\)/\3.\2.\1/



(4) s/<[^<>]\*>/ /



4.Linux中某个普通磁盘文件对所有用户赋予了读写权限，但删除该文件失败。导致可修改文件无法删除的原因是什么？

文件的删除权限取决于其所在目录的写入权限，而不是文件本身的权限。即使文件对所有用户都具有读写权限，但如果用户没有对该文件所在目录的写入权限，那么用户仍然无法删除该文件。

5.在当前目录/home/sun下执行chmod 000 . 命令后， 随后执行chmod 777 . 命令失败。为什么会失败？这样导致当前目录无法访问，如何解除这一困境？

执行 chmod 000 . 命令后，该目录的权限设置为 000，这意味着所有用户（包括目录所有者）都无法读取、写入或执行该目录。由于您无法访问该目录，因此随后执行的 chmod 777 . 命令会失败。

使用chmod 777 /home/sun可以解除这一困境。

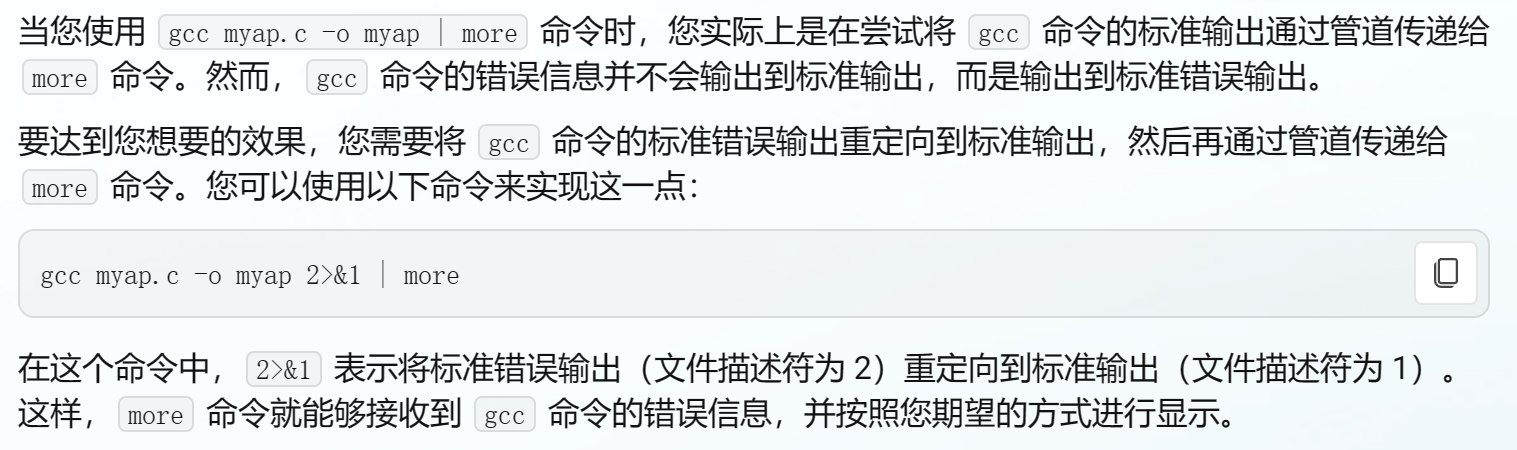
6.在Windows下输入命令名，系统首先检索当前目录下是否有这个可执行文件，检索不到，会逐个检查PATH环境变量列出的各目录。Linux不自动检索当前目录，而且环境变量PATH中一般不含当前目录./，为什么？

出于安全方面的考虑，假如用户a在/tmp目录下创建名为ls的恶意程序，并对所用用户赋予执行权限x。当用户b在/tmp目录下执行命令ls，由于PATH中含有./分量，将以用户b的身份执行/tmp/ls，因而造成安全问题。

7.当前目录下具有可执行属性的bash脚本文件a.sh，在bash提示符下执行命令./a.sh与. a.sh (将前个命令的斜线换成空格)，有什么区别？

./a.sh 将创建子进程，在子shell中执行当前目录下的a.sh脚本里的程序；. a.sh 将在当前的Shell中执行a.sh脚本。

8.命令gcc myap.c -o myap因源程序有大量问题，错误信息很多，为什么用gcc myap.c -o myap | more不能做到每显示一屏后暂停等待按下空格键再继续显示？要达到这个目的，应怎样使用这些命令？



9.在同一台Linux上的两个进程之间交换数据可以通过下列两种方式。一，使用TCP Socket完成；二，两进程共享内存，并使用信号量(semaphore)的P/V操作操作完成。两种方式各有那些利弊？

使用TCP socket对程序员来说操作简便，但是数据需要在内核与用户进程之间进行两次拷贝。共享内存对于程序员操作复杂，但是不需要拷贝数据，效率较高。

使用TCP socket对程序员来说操作简便，但数据传输速度慢。共享内存对于程序员操作复杂，但数据传送速度快。

10.在bash命令提示符下输入下列内容后按下回车，会导致Linux操作系统崩溃吗？如果系统不崩溃的话，会出现什么现象？为什么？

内容：a(){a; };a

//可能少了空格

这个命令首先定义了一个函数a，函数中的内容就是调用自己（递归）；其次，调用函数a。这种递归死循环不会导致系统崩溃，但是会导致当前的shell进程的堆栈段不停生长，当超过极限之后，当前shell进程崩溃。

四．程序分析题（共10分）

某Linux系统在TCP端口12345提供一种专用的文件传输服务。下面的服务器端程序采用“多进程并发”的方法同时为多个客户端服务。每到达一个TCP连接就创建一个子进程运行可执行文件**xftpd**负责与这个客户端之间的文件传输。源程序省略了相关头文件和异常情况处理。

|  |
| --- |
| **1 int main(void)**  **2 {**  **3 int admin\_sock, data\_sock;**  **4 char str[16];**  **5 static struct sockaddr\_in name;**  **6 admin\_sock = socket(AF\_INET, SOCK\_STREAM, 0);**  **7 name.sin\_family = AF\_INET;**  **8 name.sin\_addr.s\_addr = INADDR\_ANY;**  **9 name.sin\_port = htons(12345);**  **10 bind(admin\_sock, &name, sizeof(name));**  **11 listen(admin\_sock, 5);**  **12 signal(SIGCLD, SIG\_IGN);**  **13 for (;;) {**  **14 data\_sock = accept(admin\_sock, 0, 0);**  **15 if (fork() == 0) {**  **16 close(admin\_sock);**  **17 sprintf(fd\_str, "%d", data\_sock);**  **18 execlp("xftpd", "xftpd", str, 0);**  **19 printf("run xftpd\n");**  **20 exit(1);**  **21 }**  **22 close(data\_sock);**  **23 }**  **24 }** |

1. 上述源程序中，有哪些数据（包括变量和常量）被存放在数据段？有哪些数据被存放在堆栈段？
2. 上述服务器进程大部分时间处于阻塞状态，程序中的哪条语句导致进程进入阻塞状态？阻塞状态在什么时机被解除？
3. 如果删除上述程序中的第12行，会有什么问题？
4. 如果删除上述程序中的第22行，会有什么问题？
5. 客户完成文件传输操作后断开TCP连接，第19行的语句未执行打印动作，为什么？

**1. 第 17,18,19 行都有用引号包起来的字符串数据，这些常量数据放在数据段；第 5 行的变量 name 声明为 static，它也被安排在数据段。其他的三个变量 admin\_sock，data\_sock，str，都是在函数内部定义的 auto 型变量，在堆栈段分配存储空间。第 7,8，9 行，11 行等等的 int 型常数以及其他行常数0，存放在指令段，属于“立即寻址型”指令操作数。**

**2. 第 14 条语句的 accept 调用导致进程进入阻塞状态。当有新的 TCP 连接到来时，从阻塞状态中解除。**

**3. 第 12 行宣称忽略掉 SIGCLD 信号，当子进程中止时，将自动丢弃子进程的僵尸。如果缺少这条语句，那么子进程结束后将不会被自动回收，这将导致系统中出现大量僵尸进程。，会导致操作系统内核中的进程槽耗光，无法创建新进程。**

**4. 第 22 行的 close 有两个重要功能。第一，父进程将不再使用的文件描述符 close，否则，父进程打开的文件描述符越来越多，当超过了单进程的最大打开文件数之后，以后再来 TCP 连接就无法成功 accept。第二，只有父进程 close 之后并且子进程也 close 时，客户端才能得到 TCP 被关闭的信息，否则，即使子进程 xftpd 崩溃，客户端 TCP 也得不到连接断开的消息。**

**一，父进程无法关闭套接字，所以套接字会越来越多，当超过了单进程的最大打开数后，后面来的TCP连接就无法成功accept。二，父进程不close的话，客户端TCP不会得到连接断开的消息。**

**5. 只要第 18 行的 exec 调用执行成功，子进程全部代码段被毁掉，被替换成文件 xftpd 中的代码段，自然第 19 行的程序也被毁掉，所以，只要 第 18 行 exec 执行成功，第 19 行的 printf 就不会有机会执行。这个printf 有机会执行的前提条件是 exec 执行失败。**

五．编程题（共 10 分）

1. (4 分)编写一个完整的 C 语言程序，打印所有的命令行参数和选项。

int main(int argc, char \*\*argv)

{

int i;

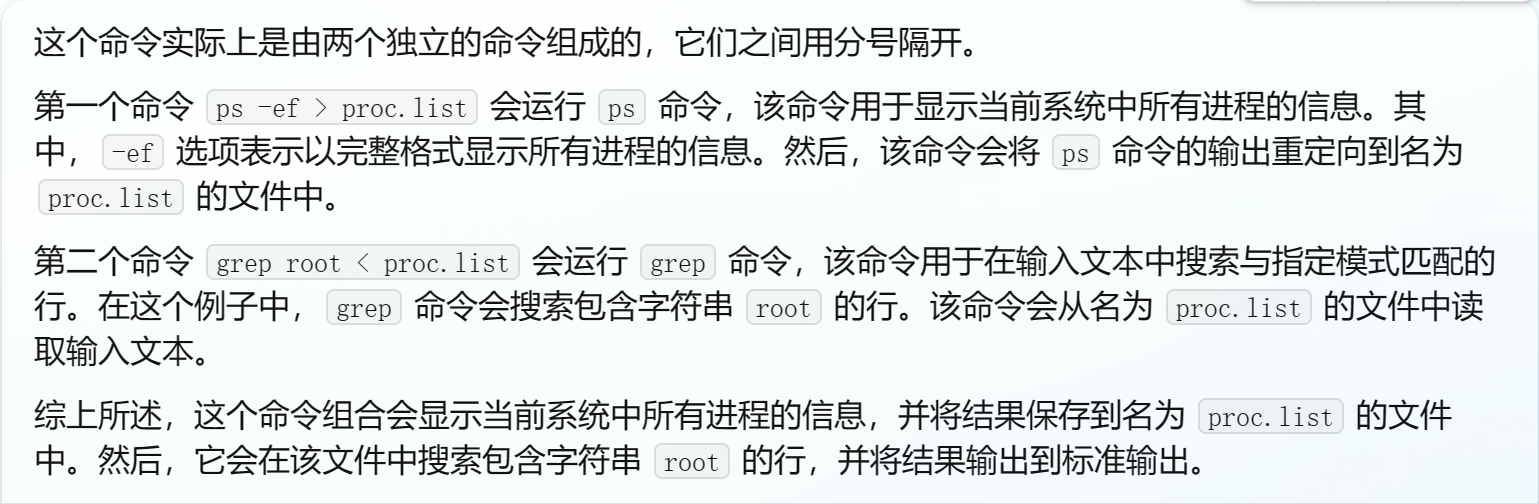
for (i = 0; i < argc; i++)

printf("%d: [%s]\n", i, argv[i]);

}

2. (6分)使用Linux与进程管理有关的系统调用，编写 C语言程序，使用与下列shell命令相同的机制完成同样的功能。

**ps -ef > proc.list; grep root < proc.list**



为简化编程，假设系统调用执行均能成功，不考虑失败的情况。

int main()

{

int fd, sv; // 定义文件描述符和状态变量

if (fork() == 0) { // 创建子进程

fd = open("proc.list", O\_CREAT | O\_WRONLY, 0666); // 打开或创建文件

dup2(fd, 1); // 将标准输出(数字1代表)重定向到文件(fd代表)

close(fd); // 关闭文件描述符

execlp("ps", "ps", "-ef", 0); // 运行 ps -ef 命令

} else { // 父进程

wait(&sv); // 等待子进程结束

fd = open("proc.list", O\_RDONLY); // 以只读方式打开文件

dup2(fd, 0); // 将标准输入(数字0代表)重定向到文件(fd代表)

close(fd); // 关闭文件描述符

execlp("grep", "grep", "root", 0); // 运行 grep root 命令

}

}

execlp函数解释：

execlp 函数用于在当前进程中执行一个新的程序。它接受可变数量的参数，第一个参数 file 指定要执行的程序的文件名。接下来的参数 argv0、argv1 等指定传递给新程序的命令行参数。最后一个参数必须是 0，表示参数列表的结束。