Luke

Luke was a simple box with no privilege escalation, there was alot of enumeration, so lets get started.

Nmap

nmap -sC -sV -oA nmap/luke 10.10.10.137

```
# Nmap 7.70 scan initiated Mon May 27 05:07:59 2019 as: nmap -sC -sV -oA Luke 10.10.10.137
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-27 15:57 IST
Nmap scan report for luke.io (10.10.10.137)
Host is up (0.16s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE    VERSION
21/tcp   open  ftp        vsftpd 3.0.3+ (ext.1)
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 0        0             512 Apr 14 12:35 webapp
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.15.153
|      Logged in as ftp
|      TYPE: ASCII
|      No session upload bandwidth limit
|      No session download bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 6
|      vsFTPd 3.0.3+ (ext.1) - secure, fast, stable
|_End of status
22/tcp   open  SSH-2.0-OpenSSH_7.8 FreeBSD-20180909
80/tcp   open  http       Apache httpd 2.4.38 ((FreeBSD) PHP/7.3.3)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.38 (FreeBSD) PHP/7.3.3
|_http-title: Luke
3000/tcp open  http       Node.js Express framework
|_http-title: Site doesn't have a title (application/json; charset=utf-8).
8000/tcp open  http       Ajenti http control panel
|_http-title: Ajenti

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 97.18 seconds
```

FTP

The FTP had anonymous login allowed, so logging in with credentials,

```
Username: anonymous
Password:
```

we find a file for_Chihiro.txt inside webapp, which had the following contents:

```
Dear Chihiro !!

As you told me that you wanted to learn Web Development and Frontend, I can give you a little push by showing the sources of
the actual website I've created .
Normally you should know where to look but hurry up because I will delete them soon because of our security policies !

Derry
```

Nothing usefull here.

Web

run gobuster on all the ports (i.e 80,3000,8000),

```
gobuster -e -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.10.137/users -f -x php -s 200,204,301,302,307,403,401,500
```

we find the following files.

```
3000=========================
http://10.10.10.137:3000/login/ (Status: 200)
http://10.10.10.137:3000/users/ (Status: 200)
http://10.10.10.137:3000/Login/ (Status: 200)
http://10.10.10.137:3000/Users/ (Status: 200)
80=========================
http://10.10.10.137/login.php (Status: 200)
http://10.10.10.137/member/ (Status: 200)
http://10.10.10.137/management/ (Status: 401)
http://10.10.10.137/css/ (Status: 200)
http://10.10.10.137/js/ (Status: 200)
http://10.10.10.137/vendor/ (Status: 200)
http://10.10.10.137/config.php (Status: 200)
8000=========================
```

Inside config.php on port 80, we creds

```
$dbHost = 'localhost'; $dbUsername = 'root'; $dbPassword = 'Zk6heYCyv6ZE9Xcg'; $db = "login"; $conn = new mysqli($dbHost, $dbUsername, $dbPassword,$db) or die("Connect failed: %s\n". $conn -> error
```

we dont know yet where these go, so continue the enumeration.

Port 3000

On port 3000, we found a json webapp, and it inside it a login (the webserver at 3000 is not case-sensitive thus Users and users or Login and login are same). Making a post request to http://10.10.10.137:3000/login with creds found. I used python for it. we get the auth token and then further exploring the users as authenticated we get a list of users.

```
[{"ID":"1","name":"Admin","Role":"Superuser"},{"ID":"2","name":"Derry","Role":"Web Admin"},{"ID":"3","name":"Yuri","Role":"Beta Tester"},{"ID":"4","name":"Dory","Role":"Supporter"}]
```

And if we explore http://10.10.10.137:3000/users/username we get their respective passwords (I used Burp-Intruder for this). We getting the following data in-total.

```
Admin:WX5b7)>/rp$U)FW
Derry:rZ86wwLvx7jUxtch
Yuri:bet@tester87
Dory:5y:!xa=ybfe)/QD
root:KpMasng6S5EtTy9Z
```

Port 80

After trying the password (i used hydra to try them all at login) at all logins found, we find that the http-auth at http://10.10.10.137/management/ has the creds

```
Derry:!xa=ybfe)/QD
```

Inside we are found the list of files, and inside config.json we find the creds to Ajenti Login at port 8000

```
root:KpMasng6S5EtTy9Z
```

Root Shell

Inside we get nice interface, we find terminal gui that has root privileges leading us to get root shell.