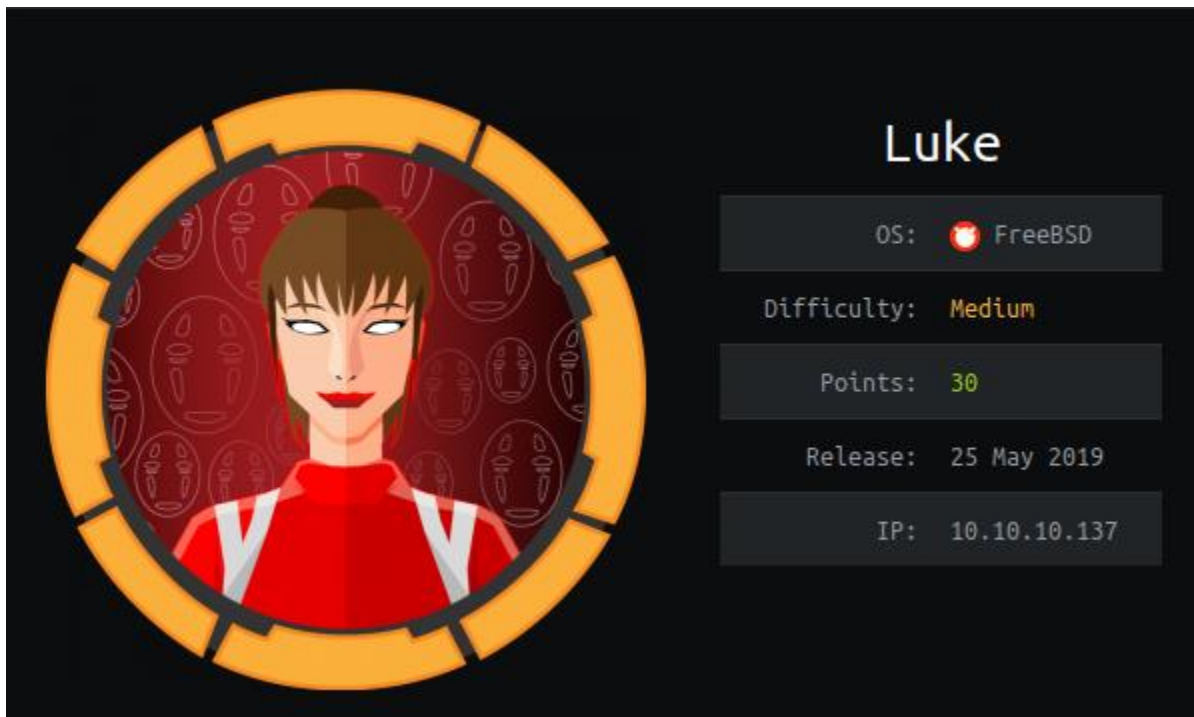


# Luke

## Hack the Box Write up



D.N.S Shihara

IT18209976

To solve this machine, we begin by enumerating all open ports. We see there is FTP, SSH, and 3 web servers running. After enumerating **port 80**, we find **config.php** and **/management**. **config.php** contains what appears to be database credentials, and **/management** is an HTTP Authentication protected directory. Enumerating the web server hosted at **port 3000**, we find 2 restful-style directories – **/users** and **/login**. We supply credentials the **/login** api to get the auth token. Using the auth token, we are able to view users, as well as gather their credentials. Using a pair of the credentials, we are able to gain access to the **/management** directory on **port 80**. Looking at **config.json**, we get another password. Using this password, and the user **root**, we are able to log into Ajenti on **port 8000**. From this web application, we are able to launch a virtual terminal as the **root** user, and read **user.txt** and **root.txt**

## Enumeration

Like all machines, we begin by enumerating all running services.

```
1 nmap -p- --min-rate 5000 10.10.10.137
```

Running this, we see 5 open ports – 21, 22, 80, 3000, 8000. Next we enumerate these ports using **Nmap**:

```
01 nmap -A -p21,22,80,3000,8000 --min-rate 4000 -oA scans/nmap-tcpAll
02
03 # Nmap 7.70 scan initiated Fri Jun 14 20:11:08 2019 as: nmap -A -p21,22,80,3000,8000
04 Nmap scan report for 10.10.10.137
05 Host is up (0.068s latency).
06
07 PORT      STATE SERVICE VERSION
08 21/tcp    open  ftp      vsftpd 3.0.3+ (ext.1)
09 | ftp-anon: Anonymous FTP login allowed (FTP code 230)
10 |_drwxr-xr-x  2 0          0          512 Apr 14 12:35 webapp
11 |_ftp-syst:
12 |_STAT:
13 |_FTP server status:
14 |_   Connected to 10.10.14.10
15 |_   Logged in as ftp
16 |_   TYPE: ASCII
17 |_   No session upload bandwidth limit
18 |_   No session download bandwidth limit
19 |_   Session timeout in seconds is 300
20 |_   Control connection is plain text
21 |_   Data connections will be plain text
22 |_   At session startup, client count was 3
23 |_   vsFTPD 3.0.3+ (ext.1) - secure, fast, stable
24 |_End of status
25 22/tcp    open  ssh?
26 80/tcp    open  http     Apache httpd 2.4.38 ((FreeBSD) PHP/7.3.3)
27 |_http-methods:
28 |_   Potentially risky methods: TRACE
29 |_http-server-header: Apache/2.4.38 (FreeBSD) PHP/7.3.3
30 |_http-title: Luke
31 3000/tcp  open  http     Node.js Express framework
32 |_http-title: Site doesn't have a title (application/json; charset=utf-8).
33 8000/tcp  open  http     Ajenti http control panel
34 |_http-title: Ajenti
35 Warning: OSScan results may be unreliable because we could not find at least 1 open
36 Aggressive OS guesses: FreeBSD 11.0-RELEASE (91%), FreeBSD 11.0-RELEASE - 12.0-CURRE
37 No exact OS matches for host (test conditions non-ideal).
38 Network Distance: 2 hops
```


## Getting an Auth Token

## Getting an Auth Token

Going to <http://10.10.10.137/config.php>, we get credentials for what appears to be a database

```
10.10.10.137/config.php x http://10.10.10.137/config.ph x +
view-source:http://10.10.10.137/config.php
Most Visited Kali Docs Kali Tools Kali Forums Exploit-DB Aircrack-ng WebApps
1 $dbHost = 'localhost';
2 $dbUsername = 'root';
3 $dbPassword = 'Zk6heYCyv6ZE9Xcg';
4 $db = "login";
5
6 $conn = new mysqli($dbHost, $dbUsername, $dbPassword,$db) or die("Connect failed: %s\n". $conn -> error);
7
```

[No Comments](#)



## Luke

OS:  FreeBSD

Difficulty: **Medium**

Points: **30**

Release: 25 May 2019

IP: 10.10.10.137

Jump Ahead: [Enum](#) - [Getting an auth token](#) - [Root](#) - [Resources](#)

## TL;DR;

```
port 80 config.php
/management config.php
/management
port 3000 /users /login
/login
/management
port 80 config.json
root
8000 port
root
```

## Enumeration

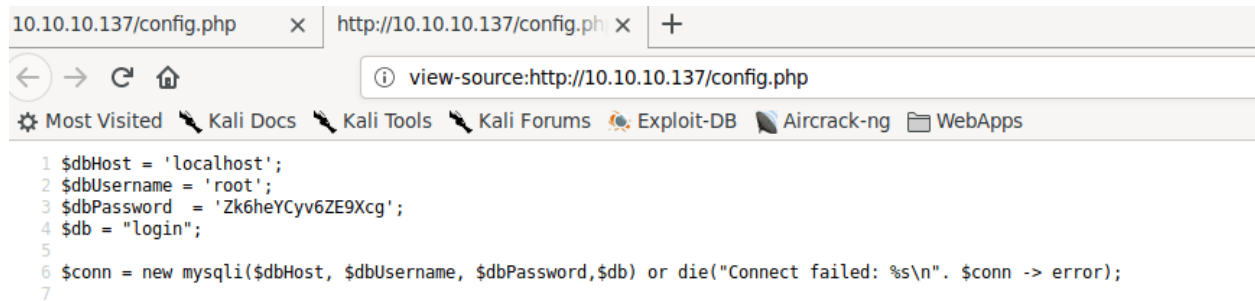
```
1 nmap -p- --min-rate 5000 10.10.10.137
```

```
01 nmap -A -p21,22,80,3000,8000 --min-rate 4000 -oA scans/nmap-tcpAll
02
03 # Nmap 7.70 scan initiated Fri Jun 14 20:11:08 2019 as: nmap -A -p21,22,80,3000,8000 -
04 -min-rate 4000 -oA scans/nmap-tcpAll 10.10.10.137
05 Nmap scan report for 10.10.10.137
06 Host is up (0.068s latency).
07
08 PORT      STATE SERVICE VERSION
09 21/tcp    open  ftp      vsftpd 3.0.3+ (ext.1)
10 | ftp-anon: Anonymous FTP login allowed (FTP code 230)
11 |_drwxr-xr-x  2 0      0          512 Apr 14 12:35 webapp
```

```
12| ftp-syst:
13|  STAT:
14|  FTP server status:
15|    Connected to 10.10.14.10
16|    Logged in as ftp
17|    TYPE: ASCII
18|    No session upload bandwidth limit
19|    No session download bandwidth limit
20|    Session timeout in seconds is 300
21|    Control connection is plain text
22|    Data connections will be plain text
23|    At session startup, client count was 3
24|    vsFTPD 3.0.3+ (ext.1) - secure, fast, stable
25|_End of status
26| 22/tcp  open  ssh?
27| 80/tcp  open  http  Apache httpd 2.4.38 ((FreeBSD) PHP/7.3.3)
28|_http-methods:
29|_ Potentially risky methods: TRACE
30|_http-server-header: Apache/2.4.38 (FreeBSD) PHP/7.3.3
31|_http-title: Luke
32|3000/tcp open  http  Node.js Express framework
33|_http-title: Site doesn't have a title (application/json; charset=utf-8).
34|8000/tcp open  http  Ajenti http control panel
35|_http-title: Ajenti
36|Warning: OSScan results may be unreliable because we could not find at least 1 open and
37|1 closed port
38|Aggressive OS guesses: FreeBSD 11.0-RELEASE (91%), FreeBSD 11.0-RELEASE - 12.0-
39|CURRENT (90%), FreeBSD 11.0-CURRENT (89%), Android 4.0.1 - 4.0.4 (Linux 3.0)
40|(89%), Linksys RV042 router (88%), D-Link DIR-300 WAP (88%), Motorola KreaTV
41|(Linux 2.6.32) (87%), FreeBSD 11.0-STABLE (87%), Android 6.0 - 7.1.2 (Linux 3.18 -
4.4.1) (87%), Android 7.1.2 (Linux 3.4) (87%)
```

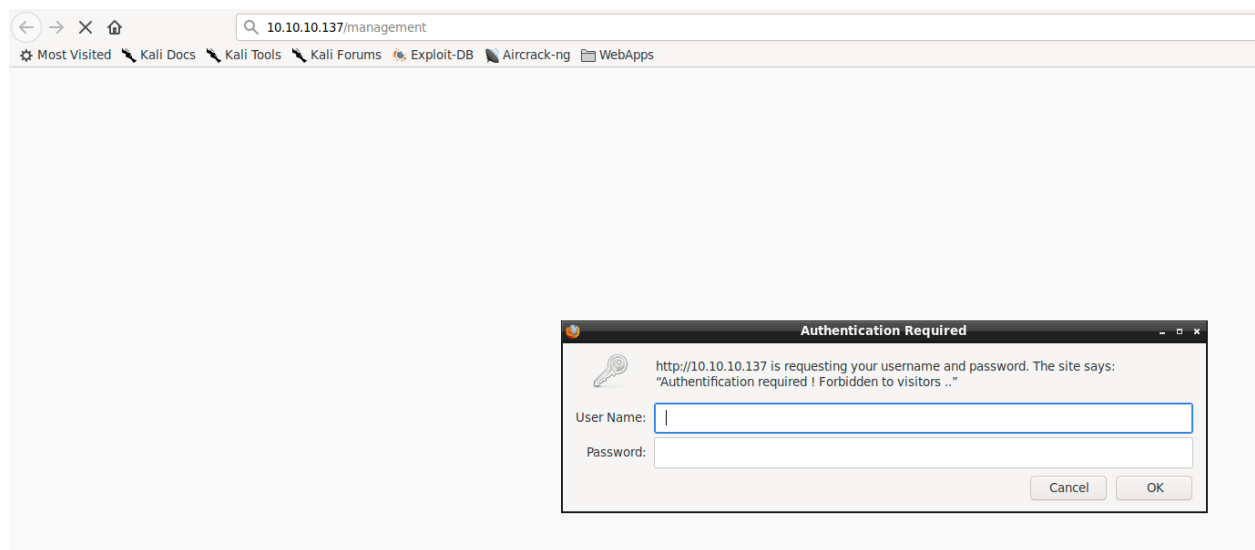


```
http://10.10.10.137/config.php
```

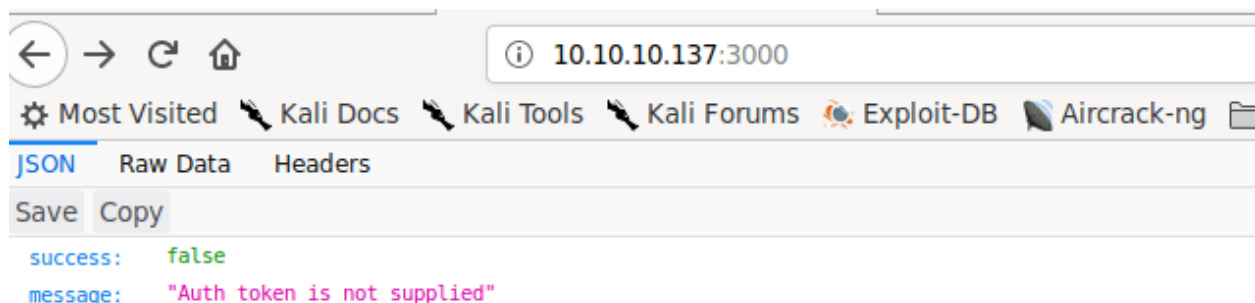


```
1 $dbHost = 'localhost';
2 $dbUsername = 'root';
3 $dbPassword = 'Zk6heYCyv6ZE9Xcg';
4 $db = "login";
5
6 $conn = new mysqli($dbHost, $dbUsername, $dbPassword,$db) or die("Connect failed: %s\n". $conn -> error);
7
```

Trying these credentials on `/login.php` doesn't give us any access, so we take a look at `/management`, but we also need to supply credentials to get in. Using the ones we have found so far does not provide us access. We will look for more credentials and try again later.



Going to `http://10.10.10.137:3000`, we are told we need to supply an auth token.



Doing some research on this error message, we should be able to get our auth token by submitting credential to the `/login` file which we found in our earlier enumeration. Using the password we found earlier, we are able to get our token, but we had to guess the username as `admin` like the article uses. Taking the token and submitting it to `http://10.10.10.137:3000/`, we are greeted as `admin`.

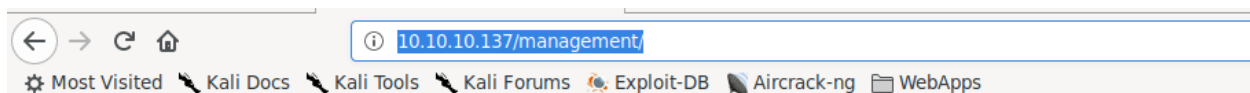


## Getting Root

Using the token to view the `/users` file, we are able to see all the users. Assuming this is a RESTful api, we attempt to look at each user's directory, where we are then given credentials for each user.



Taking the credentials we found from the RESTful api, we attempt to use them to access `http://10.10.10.137/management`, and are granted access as the `Derry` user. Looking at the `config.json` file, we see references to **port 8000**, and a password.

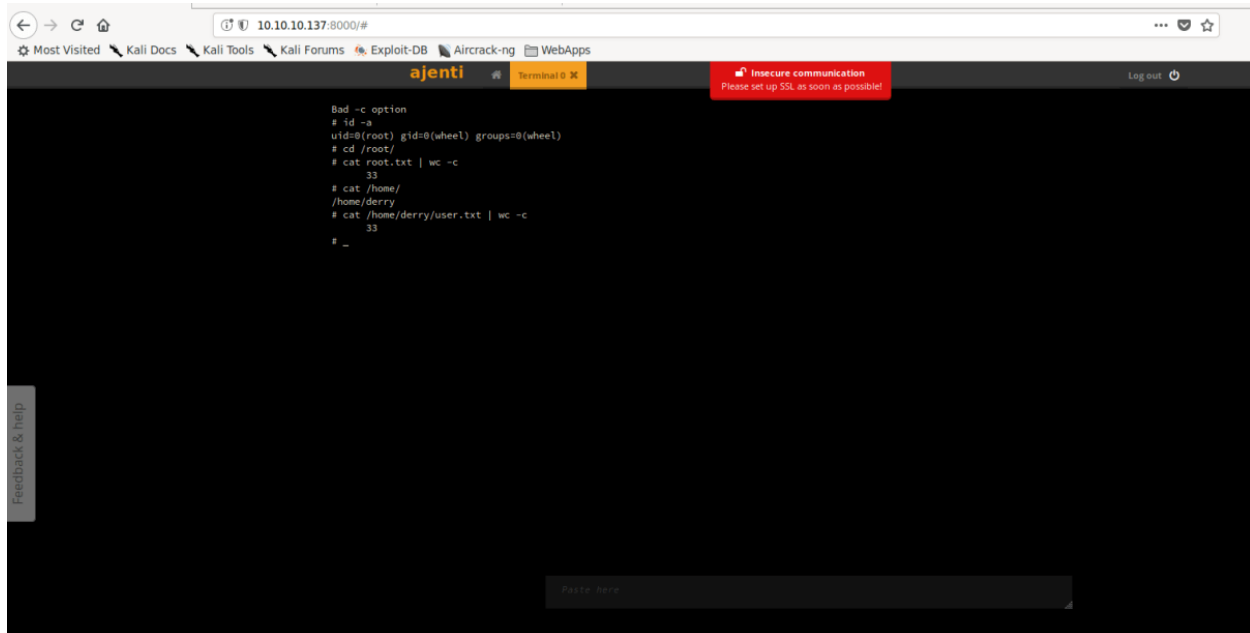


## Index of /management

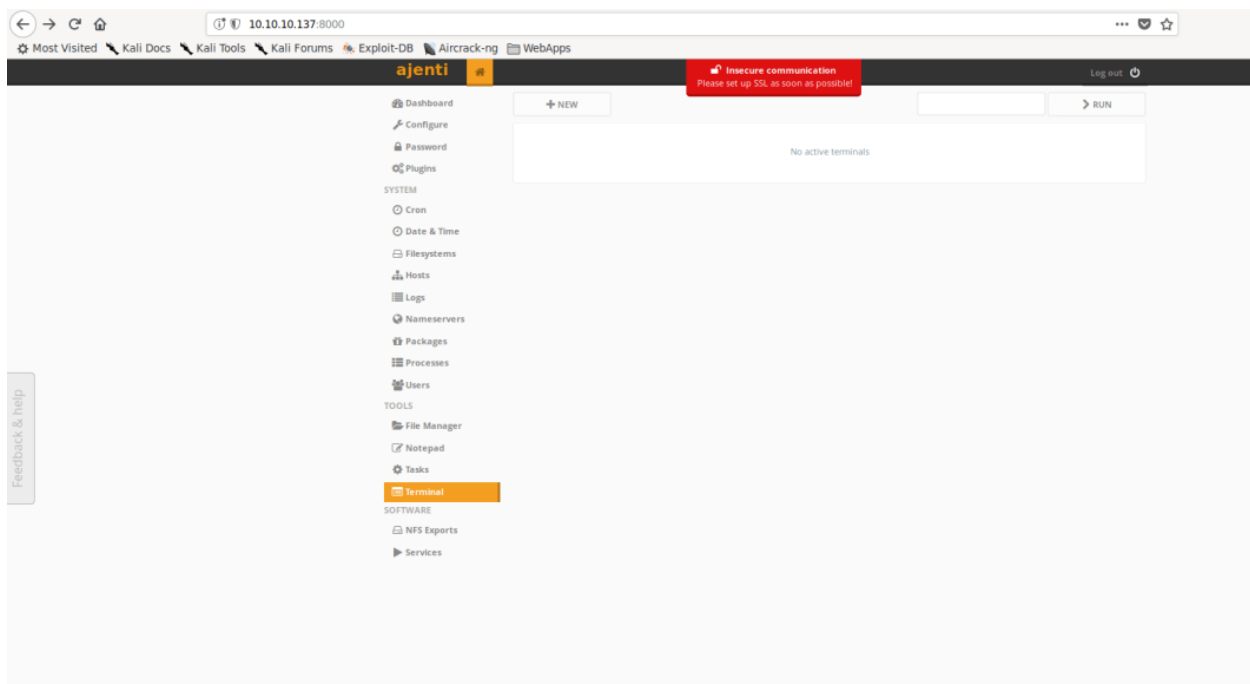
- [Parent Directory](#)
- [config.json](#)
- [config.php](#)
- [login.php](#)



Going to `http://10.10.10.137:8000`, we see **Ajenti** is hosted on this port. Doing some research into Ajenti, we learn it's a GUI for server management. Server management UIs typically use system accounts for authentication, so we attempt the use the user `root` and the password we just found. Doing so, we are granted access to the UI. On the main page, we click **Terminal->New**, to create a new terminal. Clicking the newly created virtual terminal grants us a shell as `root`. In the virtual terminal, we are able to locate and read `user.txt` and `root.txt`.



The screenshot shows a web browser window with the address bar at `10.10.10.137:8000/#`. The browser's bookmark bar includes links to 'Most Visited', 'Kali Docs', 'Kali Tools', 'Kali Forums', 'Exploit-DB', 'Aircrack-ng', and 'WebApps'. The page title is 'ajenti'. A red banner at the top right says 'Insecure communication Please set up SSL as soon as possible!'. A 'Log out' link is in the top right corner. The main content area is a terminal window with a black background and white text. The terminal output shows a shell prompt `#` followed by the command `id -a`, which returns `uid=0(root) gid=0(wheel) groups=0(wheel)`. The user then runs `cd /root/`, `cat root.txt | wc -c` (output: 33), `cat /home/`, `/home/derry`, `cat /home/derry/user.txt | wc -c` (output: 33), and finally `cat /home/derry/user.txt` (output: 33). A 'Feedback & help' button is on the left side of the terminal window.



Watch this on you tube <https://youtu.be/8E3qNmzSRaA>