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.

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

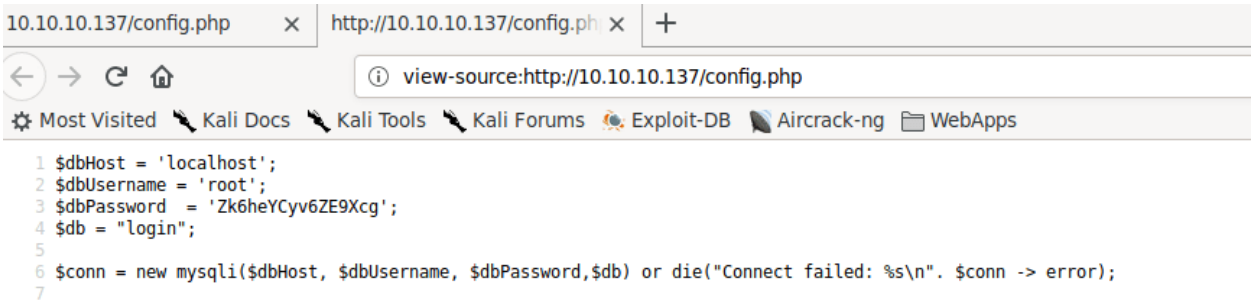
Running this, we see 5 open ports – 21, 22, 80, 3000, 8000. Next we enumerate these ports using **Nmap**:

```
nmap -A -p21,22,80,3000,8000 --min-rate 4000 -oA scans/nmap-tcpAll

# Nmap 7.70 scan initiated Fri Jun 14 20:11:08 2019 as: nmap -A -p21,22,80,3000,8000
Nmap scan report for 10.10.10.137
Host is up (0.068s 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 10.10.14.10
|      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
Warning: OSScan results may be unreliable because we could not find at least 1 open
Aggressive OS guesses: FreeBSD 11.0-RELEASE (91%), FreeBSD 11.0-RELEASE - 12.0-CURRE
No exact OS matches for host (test conditions non-ideal).
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



No Comments

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 port 8000 root

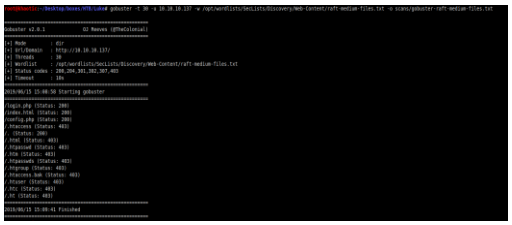
Enumeration

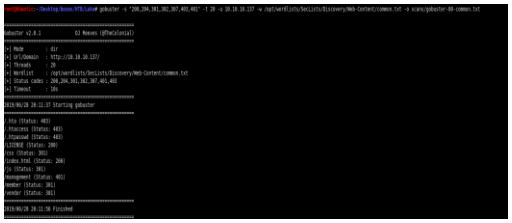
```
nmap -p- --min-rate 5000 10.10.10.137
```

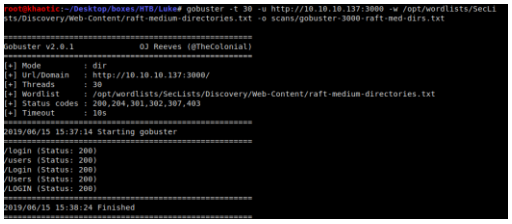
```
nmap -A -p21,22,80,3000,8000 --min-rate 4000 -oA scans/nmap-tcpAll

# Nmap 7.70 scan initiated Fri Jun 14 20:11:08 2019 as: nmap -A -p21,22,80,3000,8000 --min-rate 4000 -oA scans/nmap-tcpAll 10.10.10.137
Nmap scan report for 10.10.10.137
Host is up (0.068s 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 10.10.14.10
|     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
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: FreeBSD 11.0-RELEASE (91%), FreeBSD 11.0-RELEASE - 12.0-CURRENT (90%), FreeBSD 11.0-CURRENT (89%), Android 4.0.1 - 4.0.4 (Linux 3.0) (89%), Linksys RV042 router (88%), D-Link DIR-300 WAP (88%), Motorola KreaTV (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%)
```

```
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 21/tcp)
HOP RTT      ADDRESS
1   66.57 ms 10.10.14.1
2   67.42 ms 10.10.10.137


OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Jun 14 20:14:01 2019 -- 1 IP address (1 host up) scanned in 174.04 seconds
```

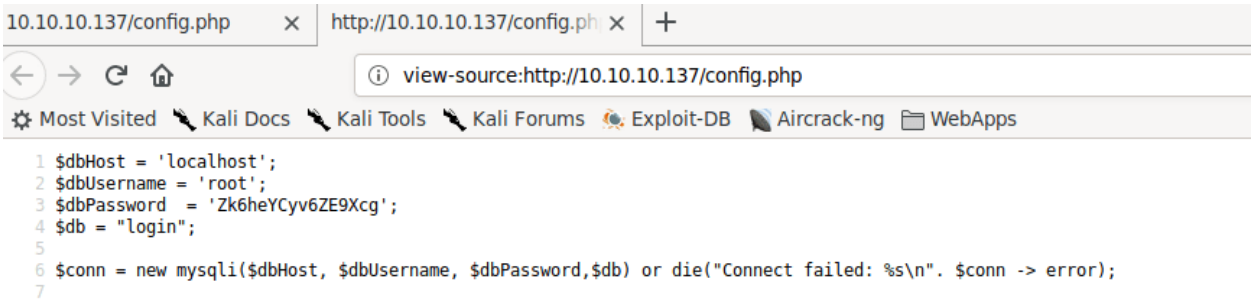




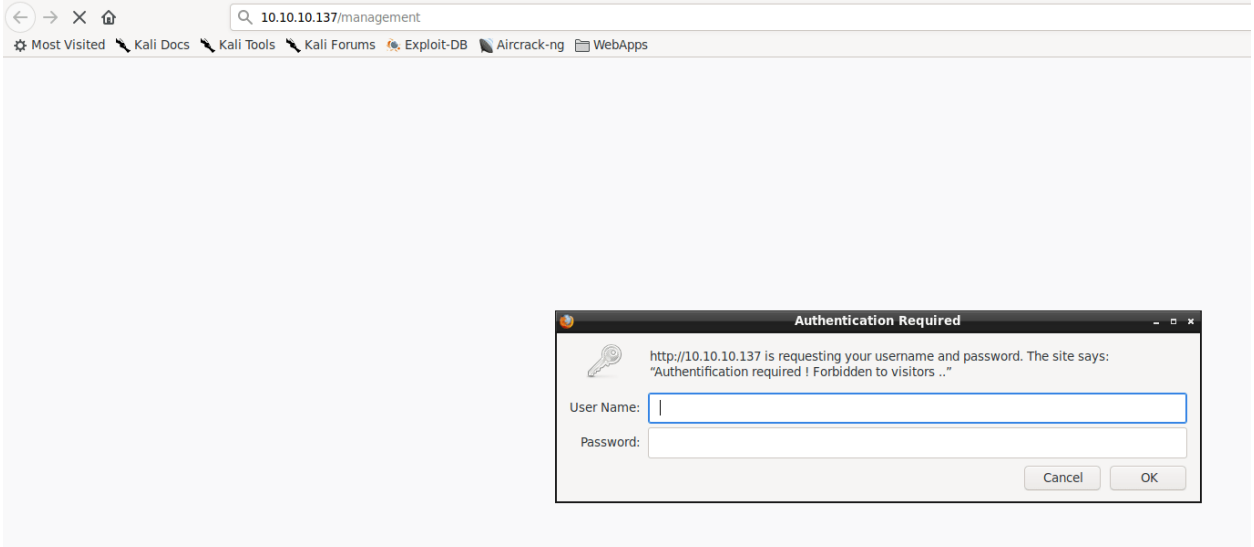


Getting an Auth Token

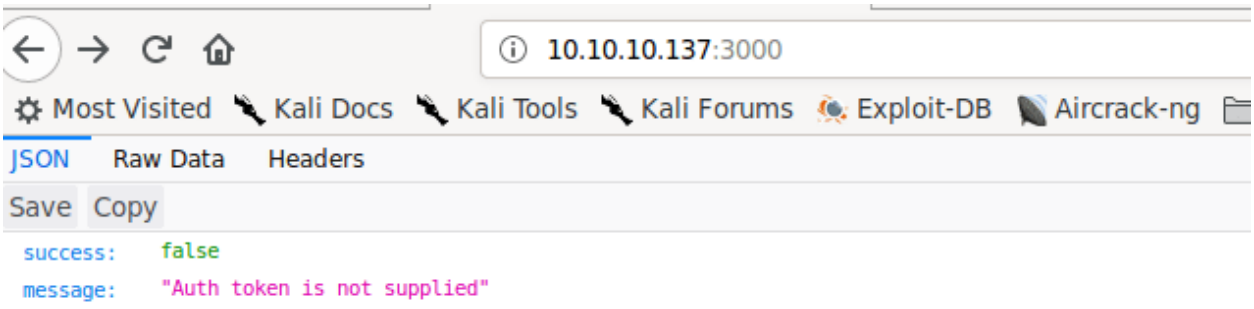
http://10.10.10.137/config.php



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.

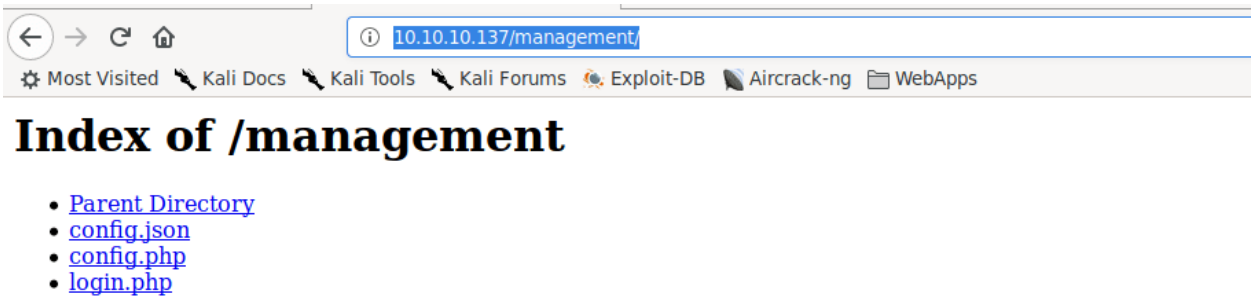


Doing some research on this error message, we should be able to get our auth token by submitting credential to the /login file which we found in our earlier enumeration. Using the password we found earlier, we are able to get our token, but we had to guess the username as admin like the article uses.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

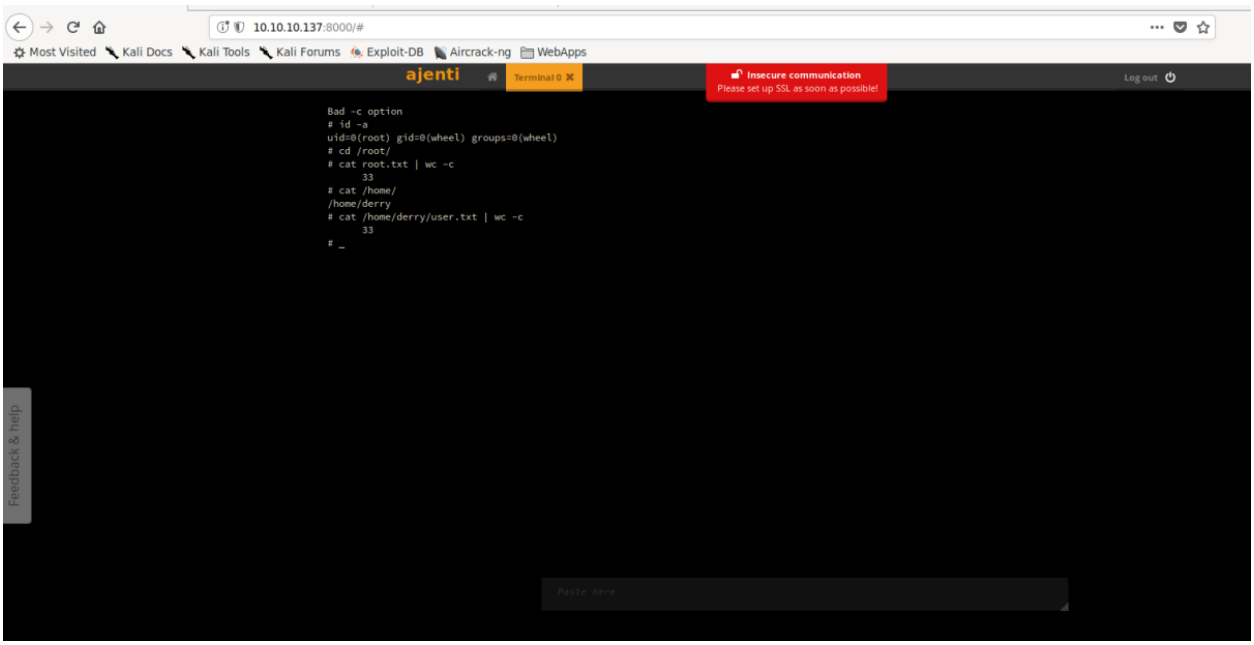
Getting Root

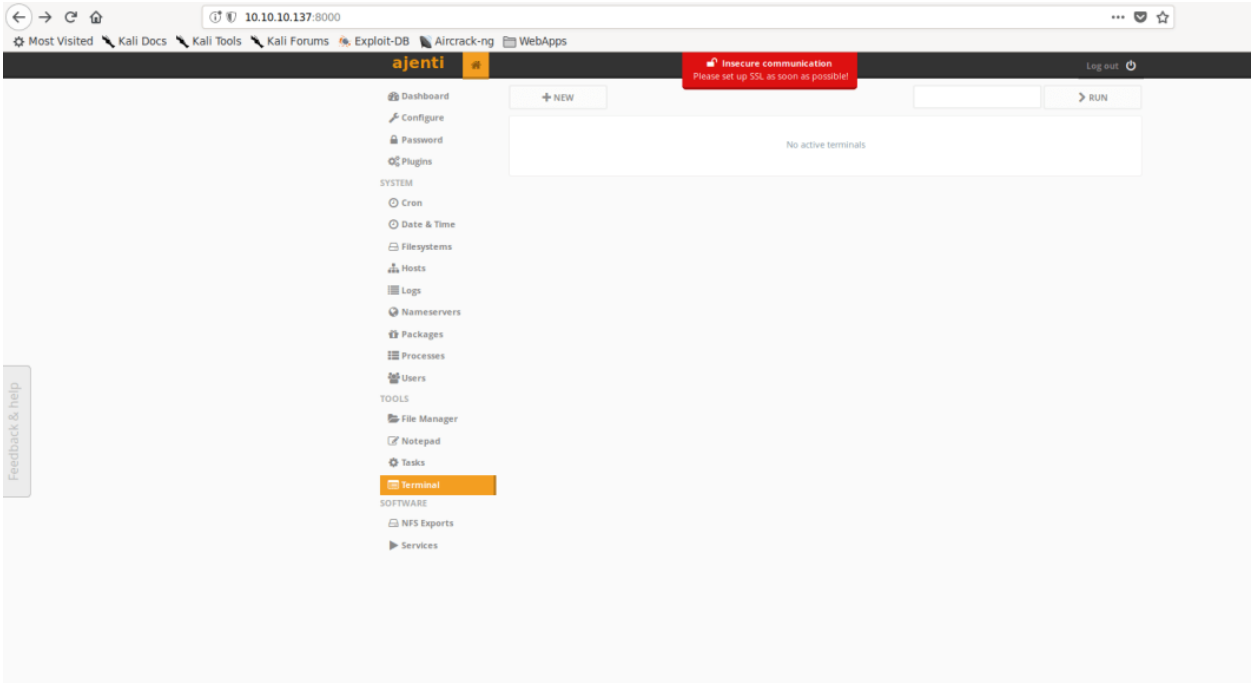
Using the token to view the /users file, we are able to see all the users. Assuming this is a RESTful api, we attempt to look at each user's directory, where we are then given credentials for each user.

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.



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.





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