BreakMySSH

Intrusión

Lo primero que haremos será comprobar si tenemos conectividad haciendo un ping. Como tenemos conectividad enumeraremos puertos con el comando `nmap -p- -sS -sC -sV --min-rate 5000 -n -vvv -Pn 172.17.0.2 -oN fastScan`.

Como podemos ver solo está abierto el puerto **22** así que probaremos a hacer fuerza bruta al usuario root con el comando `hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2`.

Como vemos encuentra la contraseña así que entramos por ssh.

Como hemos entrado directamente como root no tendremos que escalar privilegios.