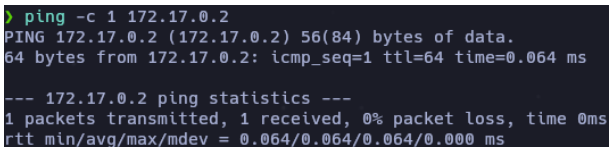
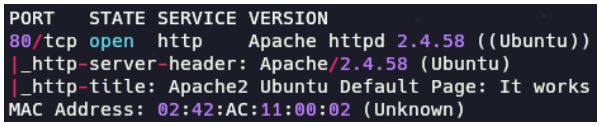
Desplegamos la máquina.

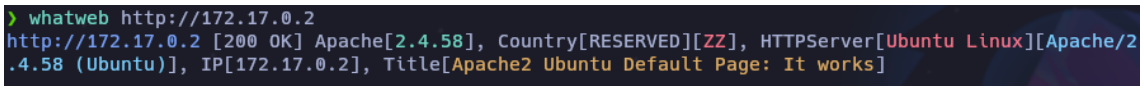
Le hacemos un ping para comprobar la conectividad y además con el ttl de 64 sabemos que estamos ante una máquina Linux.



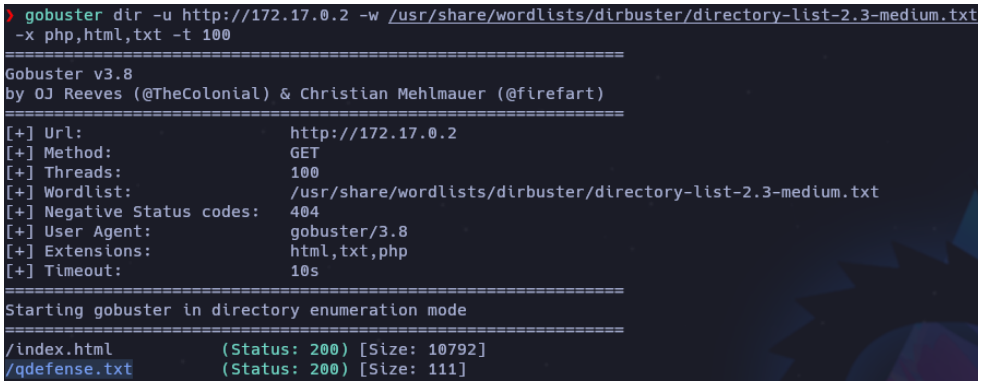
Con nmap vemos los puertos que están abiertos y sus servicios.



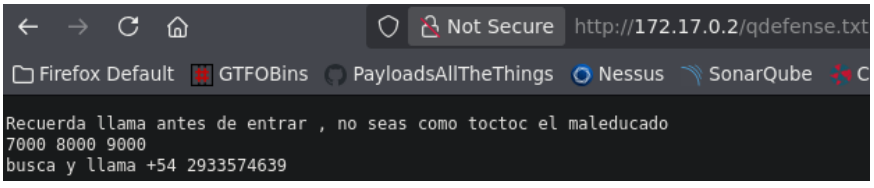
Con whatweb vemos las tecnologías que tiene la página web.



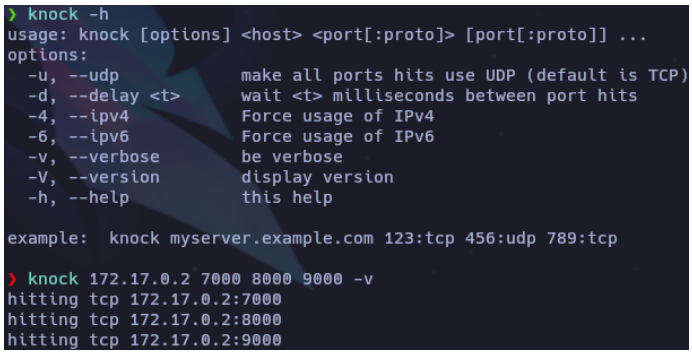
Con gobuster encontramos un archivo que estaba oculto en formato txt.



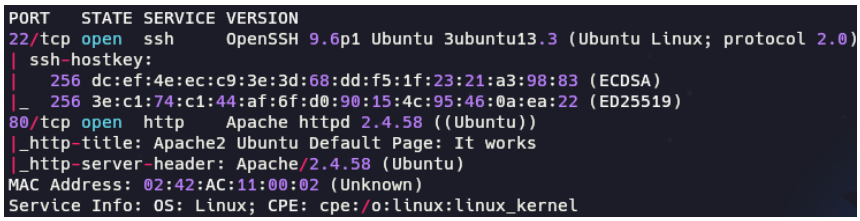
Y vemos que nos da como una especie de pista de posibles puertos que podríamos probar.



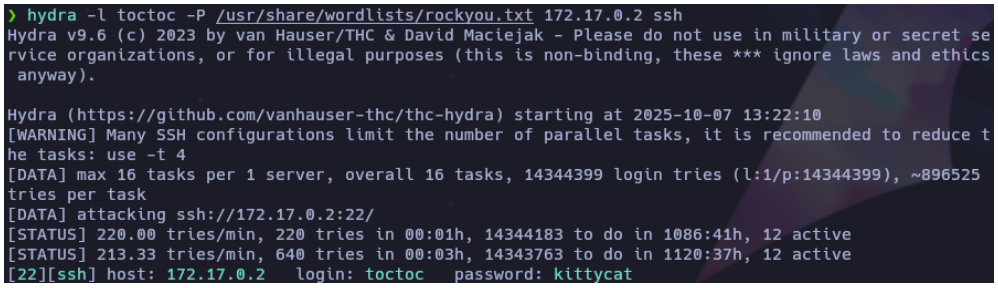
Realizamos port knocking con dichos puertos con la herramienta que nos trae Kali de base.



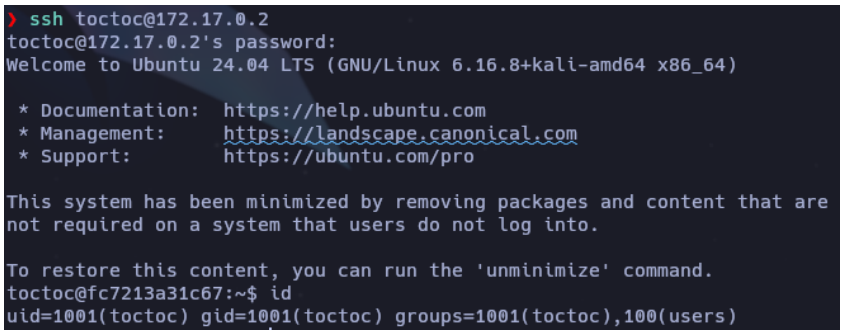
Tras realizar port knocking volvemos a comprobar los puertos con nmap para ver si se abre alguno más.



Ahora como sabemos que tenemos el puerto 22 con el servicio ssh abierto y en la pista anterior nos dio un nombre, vamos a aplicar fuerza bruta.

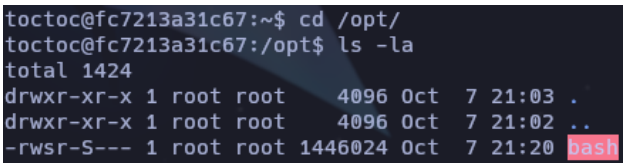


Una vez sabemos contraseña y usuario nos metemos mediante ssh y además comprobamos que no esté en ningún grupo especial.



Con sudo -l vemos que tenemos una posibilidad de escalar privilegios a root.

Nos metemos en la carpeta de opt y vemos que tenemos permisos SUID.



Ya que es root el propietario de esa bash lo único que tenemos que hacer es iniciarla con sudo y el parámetro -p para que mantenga dichos privilegios de root. Listo.