Obsession

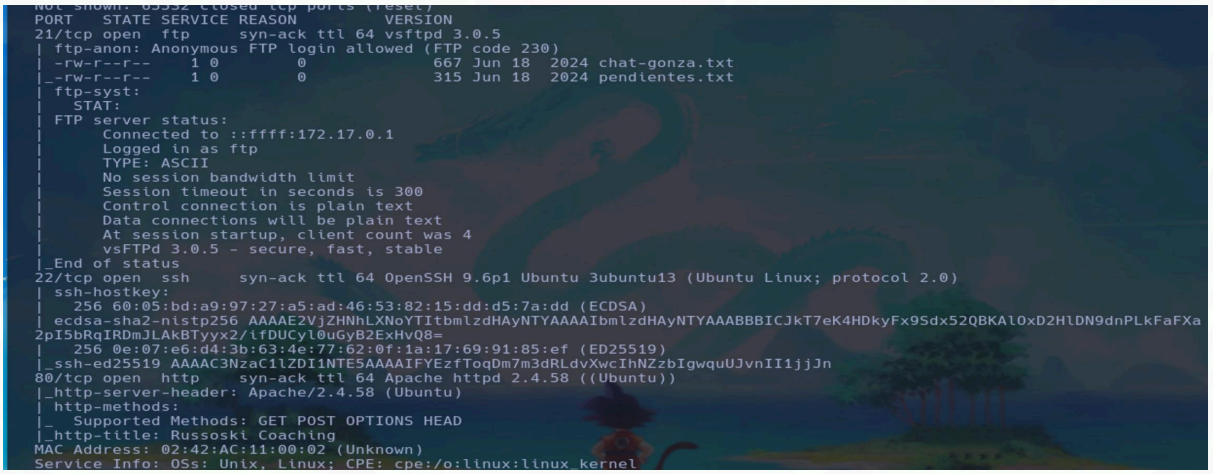
Una vez desplegada la máquina haremos un escaneo de puertos abiertos con nmap.

En mi casa utilizo el siguiente comando:

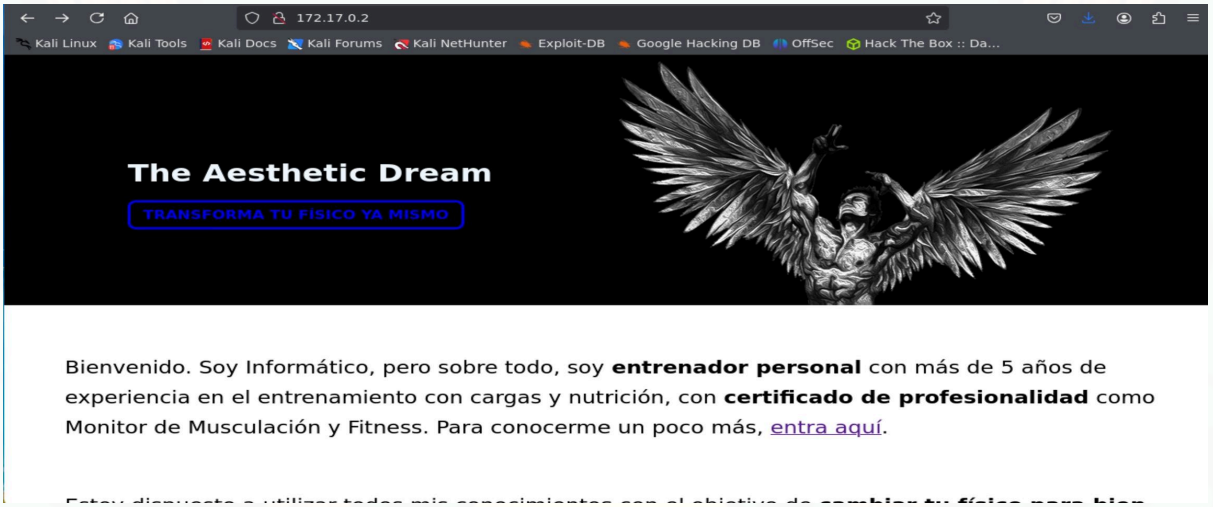
nmap -p- -sS -sC -sV --min-rate 5000 -n -vvv -Pn (ip objetivo)

- **-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.

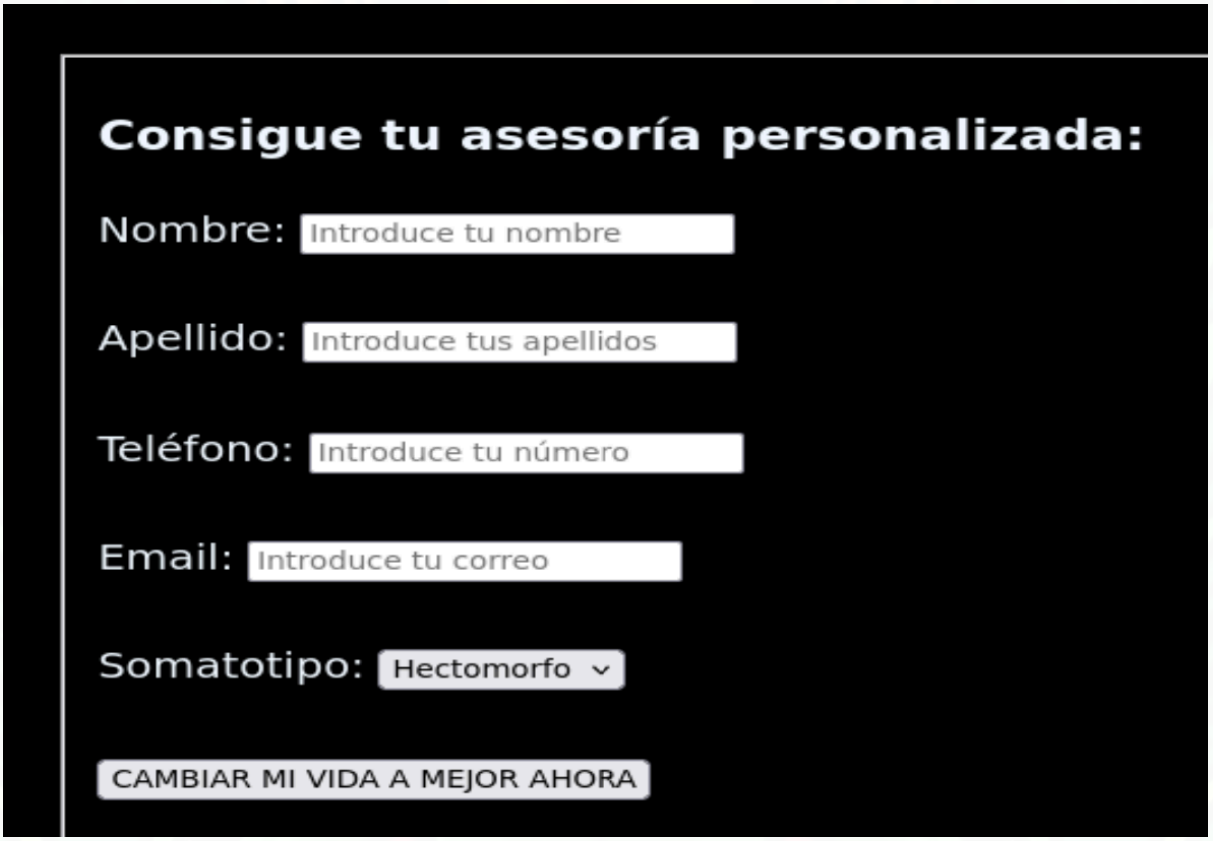
una vez realizado el escaneo vemos que tenemos tres puertos abiertos



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

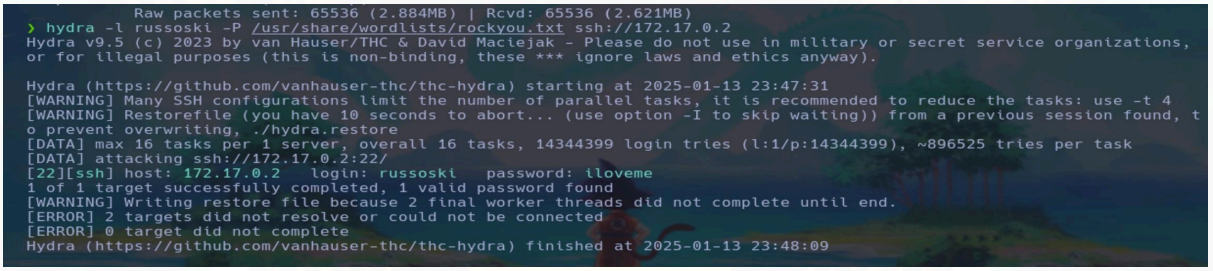


Curioseando un poco vemos como al enviar un formulario nos aparece un nombre

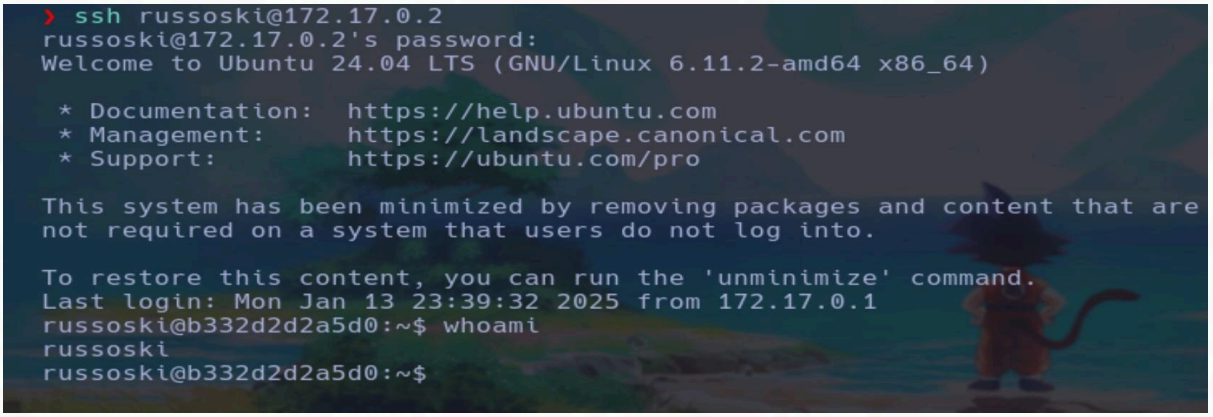


> **Has Tomado Una Gran Decisión**
>
> ---
>
> Gracias por enviar tu solicitud! Nos pondremos en contacto contigo pronto para informarte de precios y programas de entrenamiento y nutrición.
> Atentamente: el equipo de Russoski Coaching.
>
> ---

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**

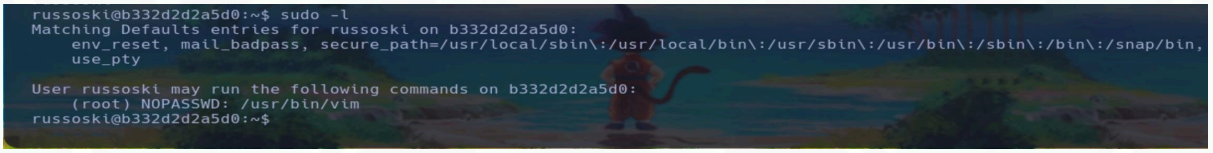


Entramos por el puerto ssh con: **ssh russoski@172.17.0.2**



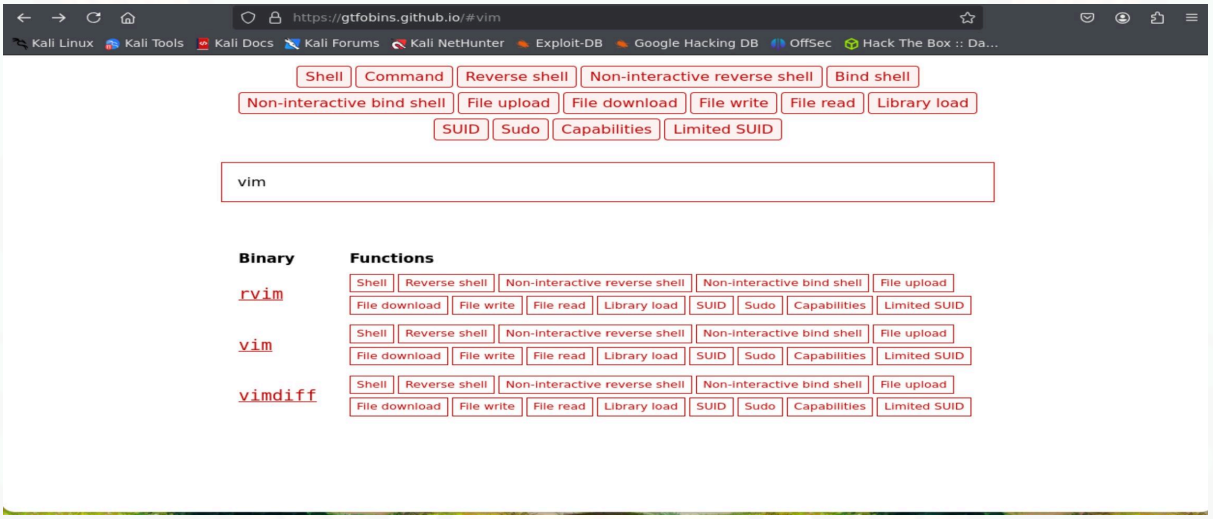
Una vez dentro con el comando whoami aparece que usuario somos por lo que vemos que no somos root , habrá que escalar privilegios.

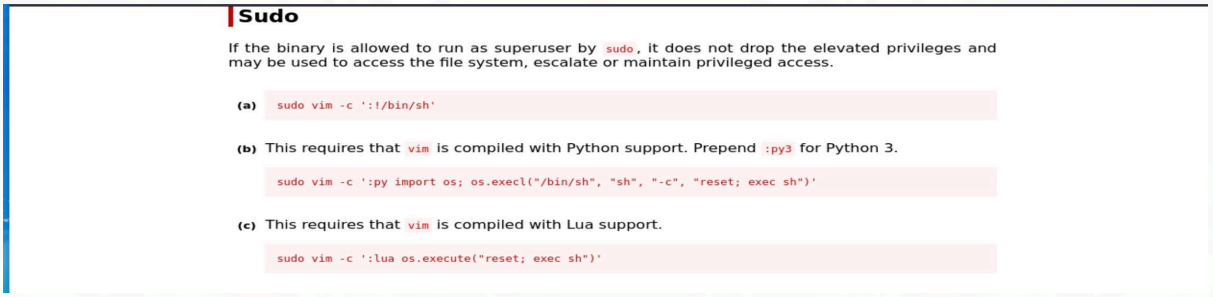
Una forma sencilla es buscar binarios Sudo que podamos aprovechar para escalar privilegios con el comando : **sudo -l**



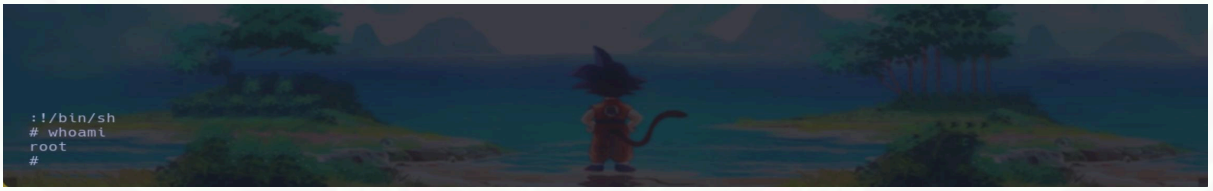
Para encontrar las vulnerabilidades recomiendo esta pagina: https://gtfobins.github.io/

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.