🏴‍☠️ Write-Up: Máquina "Pntopntobarra"

📌 **Plataforma: DockerLabs**
📌 **Dificultad: Fácil**
📌 **Autor: Joaquín Picazo**

🔎 Metodología de Pentesting

El proceso se realizó siguiendo la siguiente metodología:

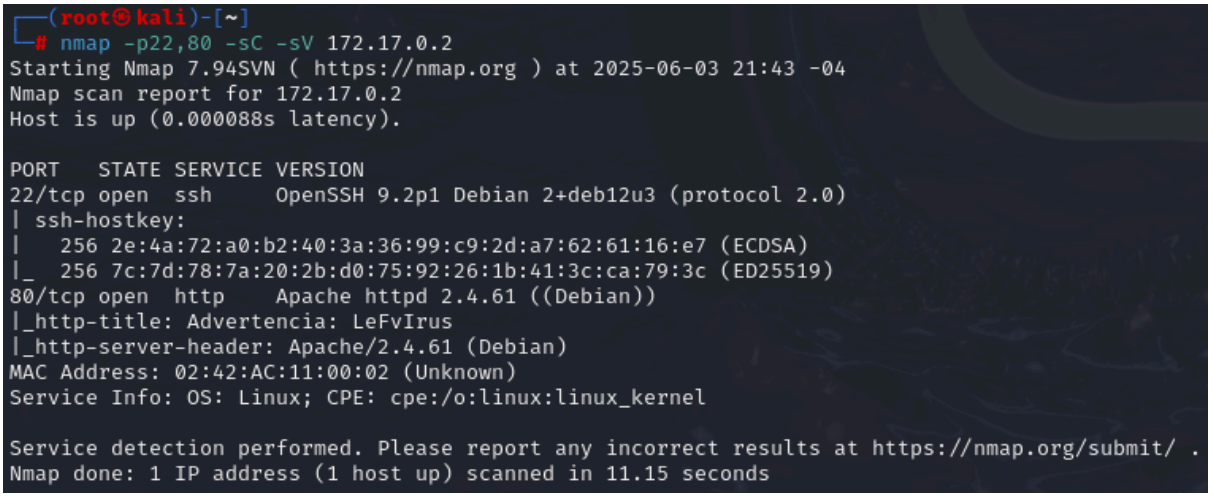
1️⃣ **Reconocimiento** – Recolección de información general sobre la máquina objetivo.
2️⃣ **Escaneo y Enumeración** – Identificación de servicios, tecnologías y versiones en uso.
3️⃣ **Explotación** – Uso de vulnerabilidades encontradas para obtener acceso al sistema.
4️⃣ **Escalada de Privilegios y Post-Explotación** – Obtención de permisos elevados hasta lograr acceso total para realizar una extracción de información.

📡 1. Reconocimiento y Recolección de Información

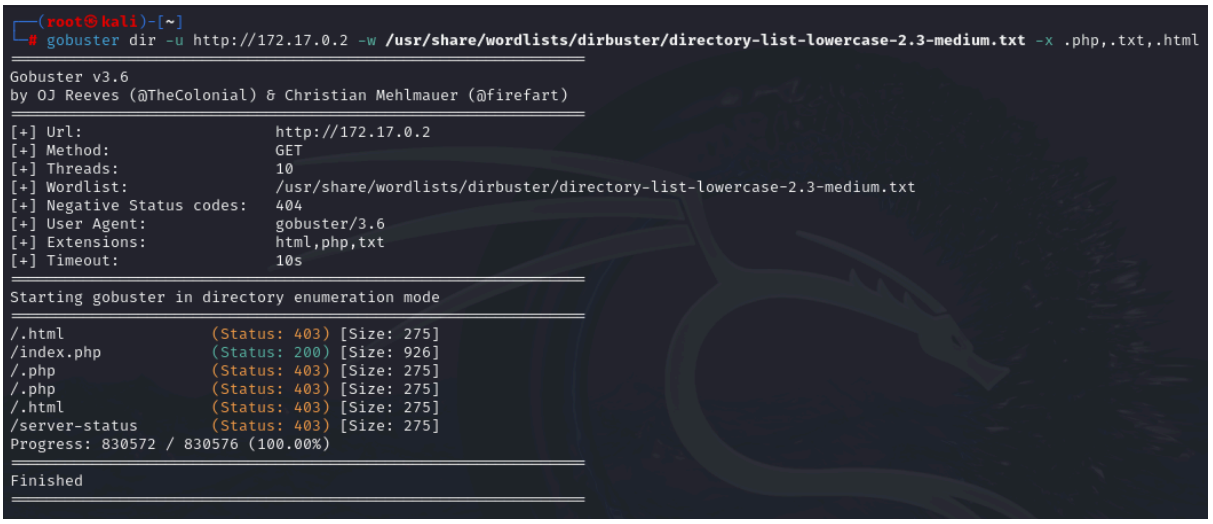
Realizo un escaneo simple para encontrar los puertos abiertos. Con **-Ss** hago un escaneo sigiloso de puertos TCP y **-Pn** porque ya se que el host está activo.

🎯 2. Escaneo y Enumeración

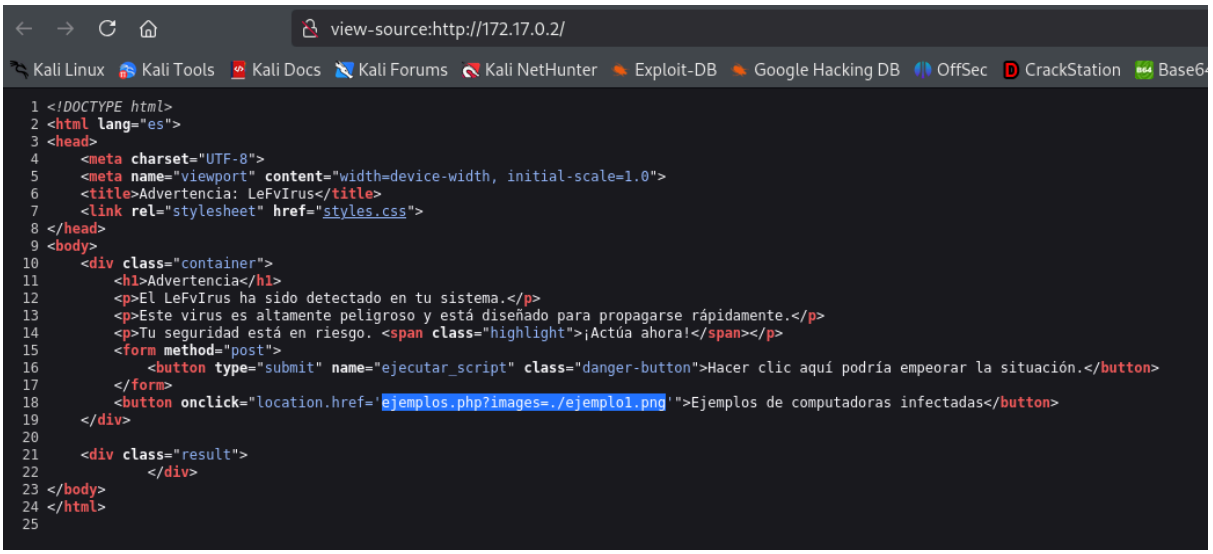
Escaneo de forma más profunda los puertos encontrados anteriormente para ver sus servicios y versiones a mayor detalle.



Con Gobuster busco directorios en la web, sin embargo, no encuentra nada interesante.

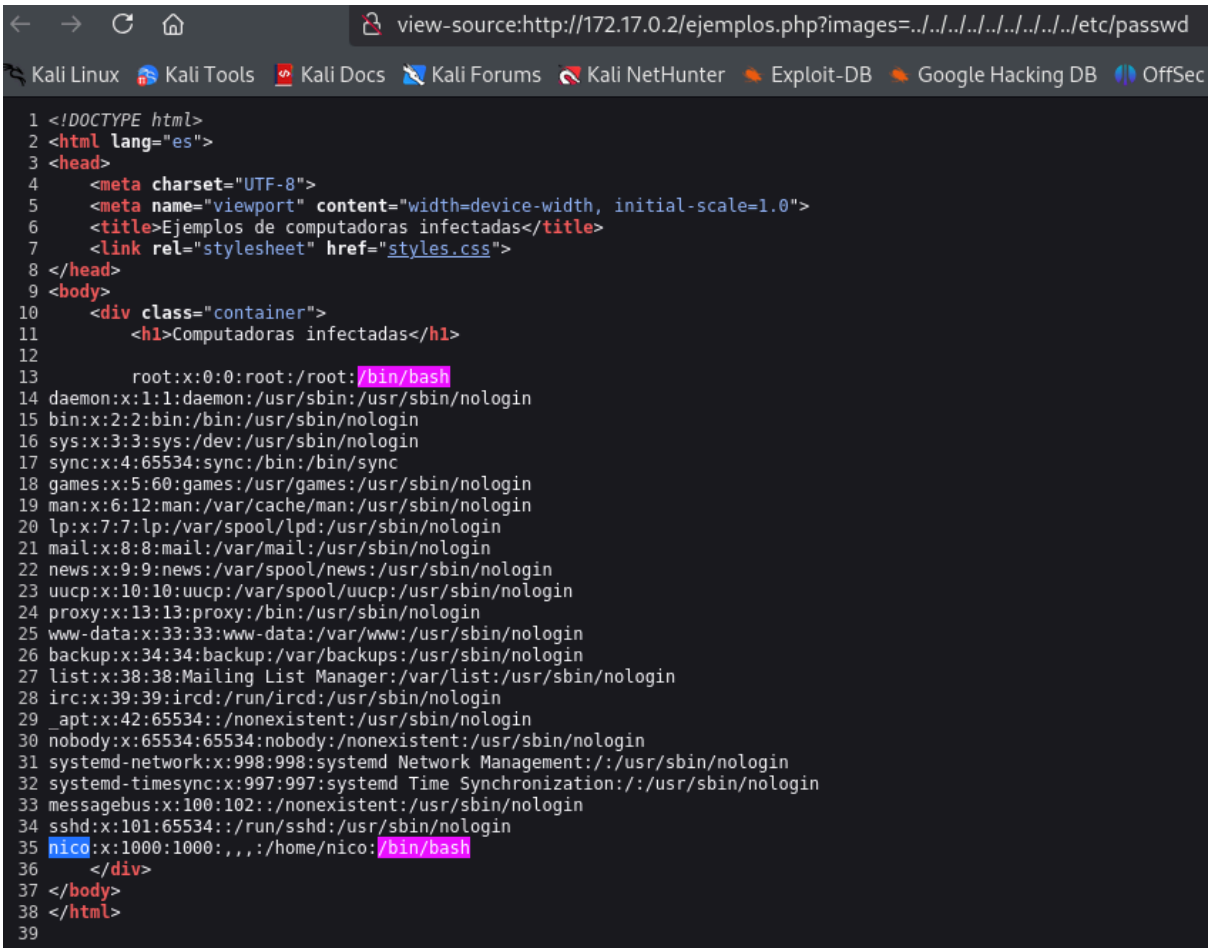


Reviso directamente el código fuente de la principal interfaz de la web y encuentro que para acceder a una imagen usa una petición en la url usando la variable “**images**”. Puedo intentar acceder a otros archivos si es que no está configurado correctamente.

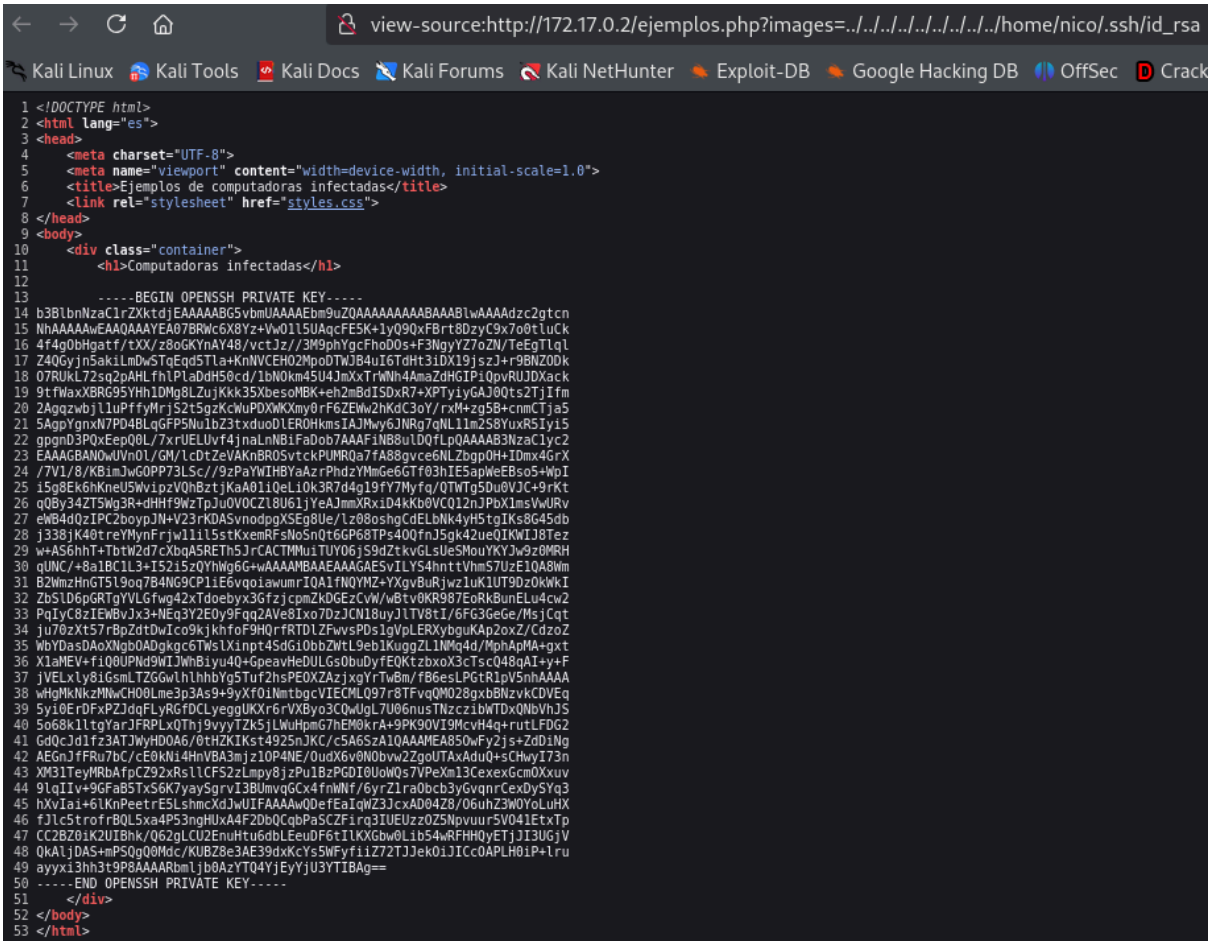


💥 3. Explotación de Vulnerabilidades

Usando la url con la variable, envío una petición para ir al directorio raíz para luego acceder al archivo **/etc/passwd** y leer su contenido. Se ve que el usuario root y **nico** tienen acceso a la terminal y uso de comandos bash.

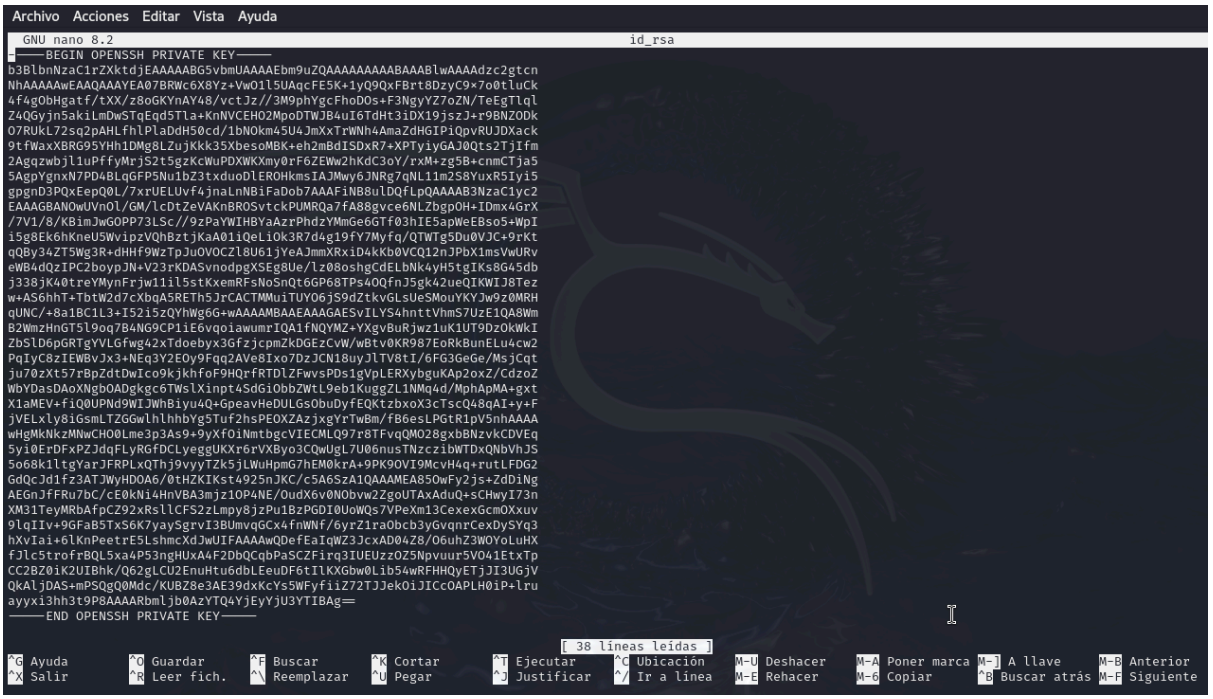


Como ahora ya sé que existe el usuario **nico**, intento acceder a su clave **RSA** para acceder por **SSH**.



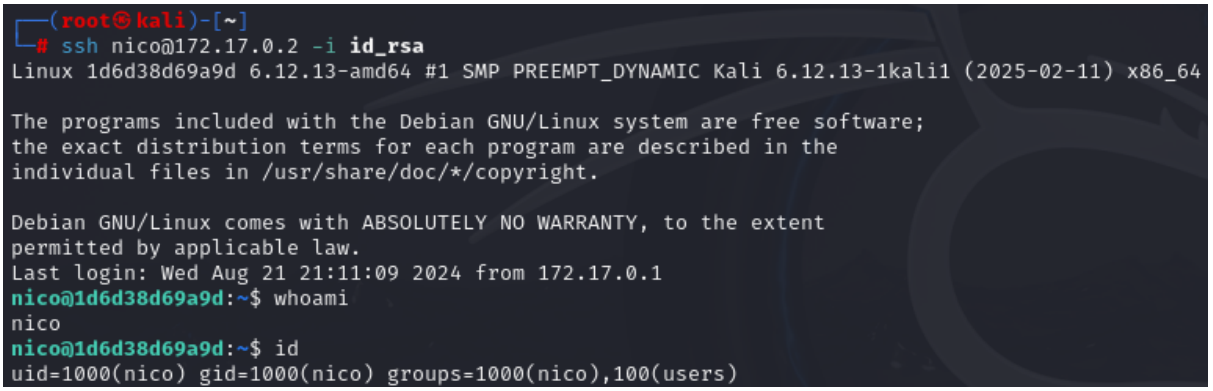
Creo un archivo con nano llamado id_rsa y pego todo el contenido de la clave **RSA** del usuario "**nico**".

Quedaría algo así:



Hago que solo yo como root en mi máquina tenga permisos por seguridad y no sea rechazado al usarlo en **SSH**.

Uso el la clave **RSA** guardada en id_rsa para acceder por **SSH** como usuario “**nico**”.



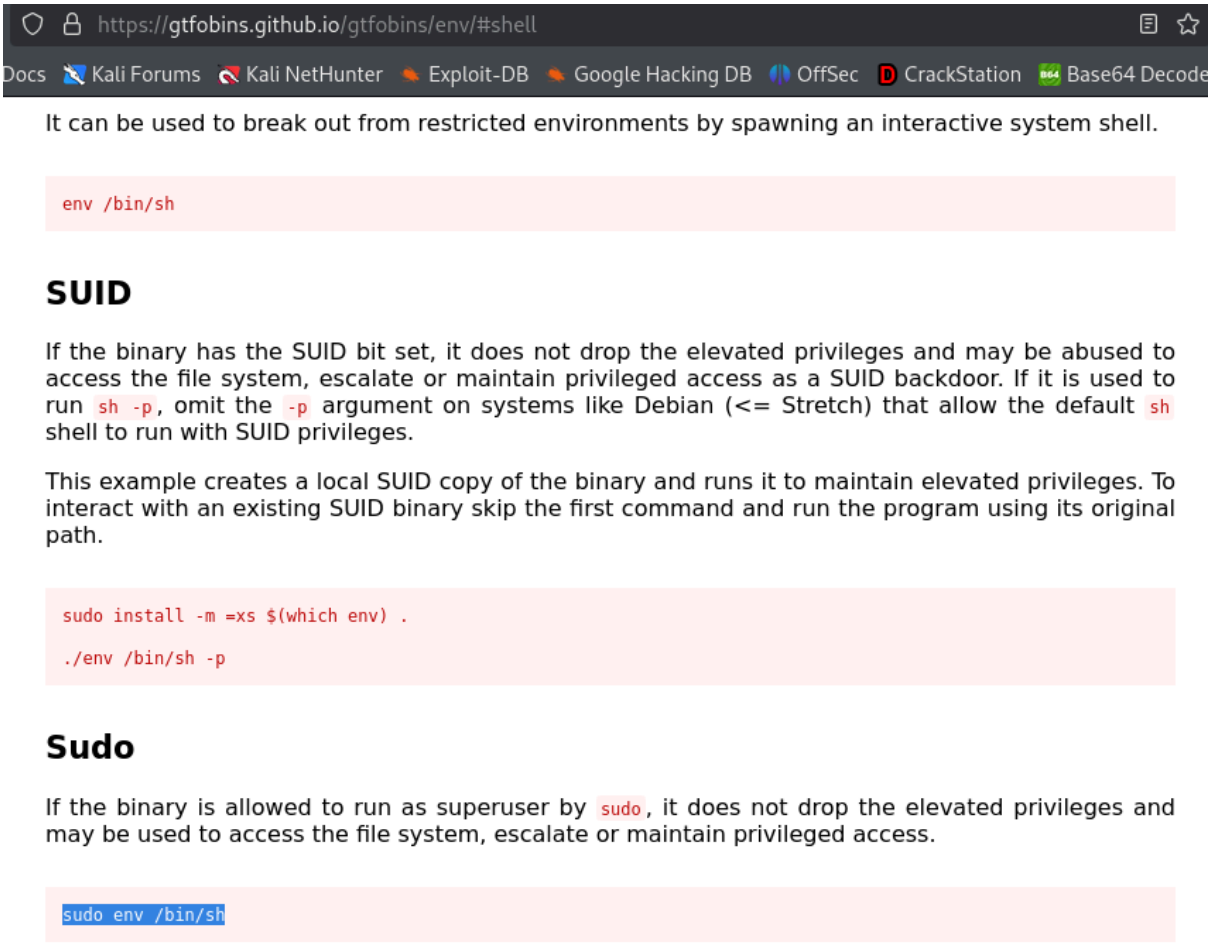
🔐 4. Escalada de Privilegios y Post-explotación

Ya ingresado, aplico un “**sudo -l**” para ver qué archivos pueden ejecutarse como sudo y encuentro un archivo llamado “**env**” que puede ser ejecutado por cualquier usuario pero como si fuera superusuario.

```
nico@1d6d38d69a9d:~$ sudo -l
Matching Defaults entries for nico on 1d6d38d69a9d:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User nico may run the following commands on 1d6d38d69a9d:
    (ALL) NOPASSWD: /bin/env
```

En GTFOBINS busco si existe un comando para escalar privilegios con “**env**” y efectivamente existe uno.



Ingreso el comando encontrado para escalar privilegios con “**env**” al poder usarse como sudo. Finalmente, soy root.

```
nico@1d6d38d69a9d:~$ sudo env /bin/sh
# whoami
root
# id
uid=0(root) gid=0(root) groups=0(root)
```

🏆 Banderas y Resultados

✔ **Usuario:** Se obtuvo acceso como usuario no privilegiado.
✔ **Root:** Se logró escalar privilegios hasta obtener control total del sistema.