🏴‍☠️ Write-Up: Máquina "Consolelog"

📌 **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.

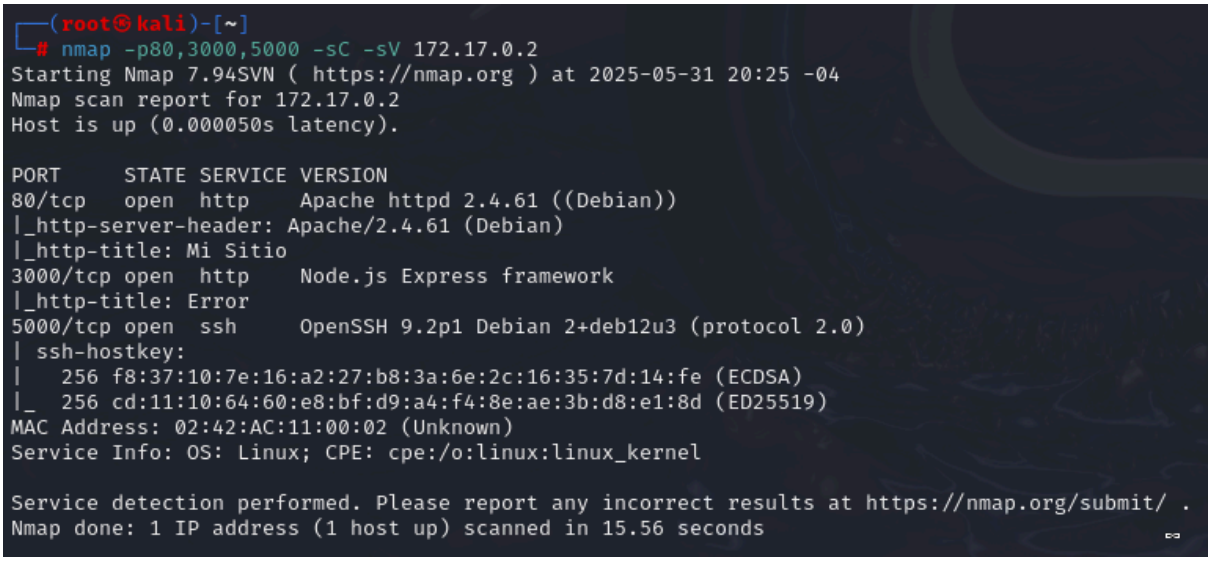
📡 1. Reconocimiento y Recolección de Información

Hago un escaneo muy simple para encontrar puertos abiertos en la máquina objetivo, dando como resultado que el puerto 80, 3000 y 5000 están abiertos.

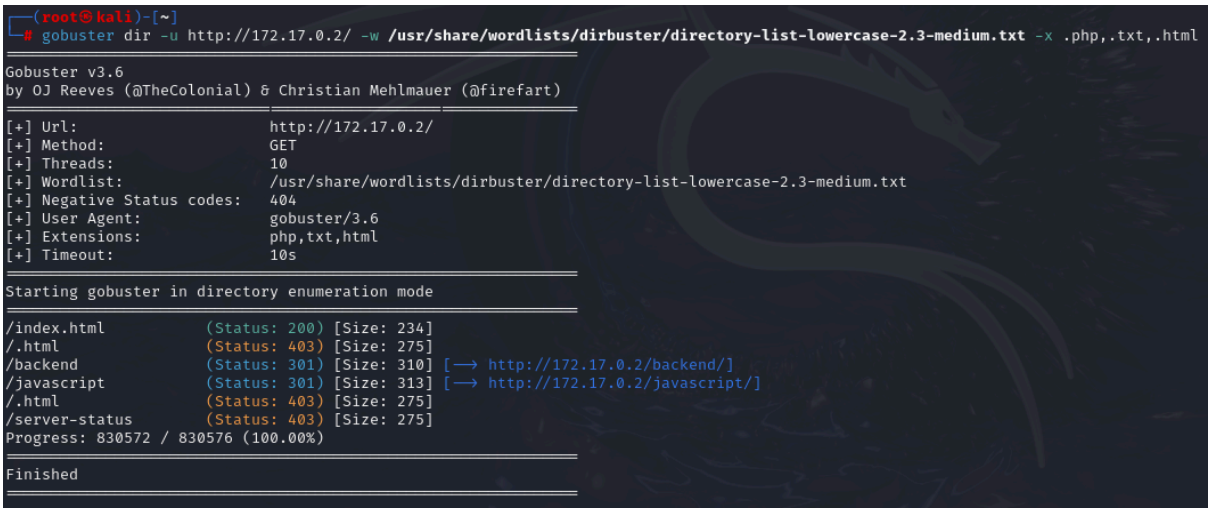
```
┌──(root㉿kali)-[~]
└─# nmap -p- --open -vvv 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-31 20:24 -04
Initiating ARP Ping Scan at 20:24
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 20:24, 0.18s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:24
Completed Parallel DNS resolution of 1 host. at 20:24, 0.02s elapsed
DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 20:24
Scanning 172.17.0.2 [65535 ports]
Discovered open port 80/tcp on 172.17.0.2
Discovered open port 5000/tcp on 172.17.0.2
Discovered open port 3000/tcp on 172.17.0.2
Completed SYN Stealth Scan at 20:25, 3.72s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.000028s latency).
Scanned at 2025-05-31 20:24:57 -04 for 4s
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE REASON
80/tcp   open  http    syn-ack ttl 64
3000/tcp open  ppp     syn-ack ttl 64
5000/tcp open  upnp    syn-ack ttl 64
MAC Address: 02:42:AC:11:00:02 (Unknown)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.31 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65537 (2.621MB)
```

🎯 2. Escaneo y Enumeración

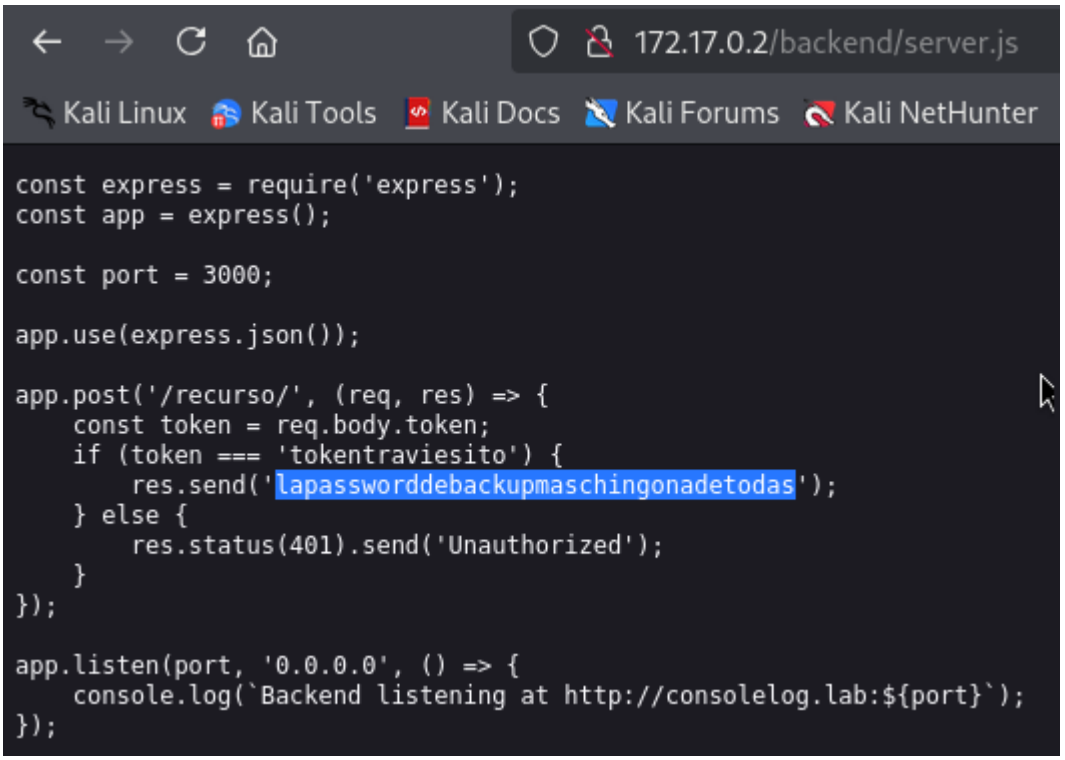
Hago un escaneo específicamente en los puertos encontrados anteriormente con la intención de encontrar versiones y más información de sus servicios.



Con gobuster busco directorios en la web que corre en el puerto 80. Solo podrían ser interesantes **/index.html**, **/backend** y **/javascript**.

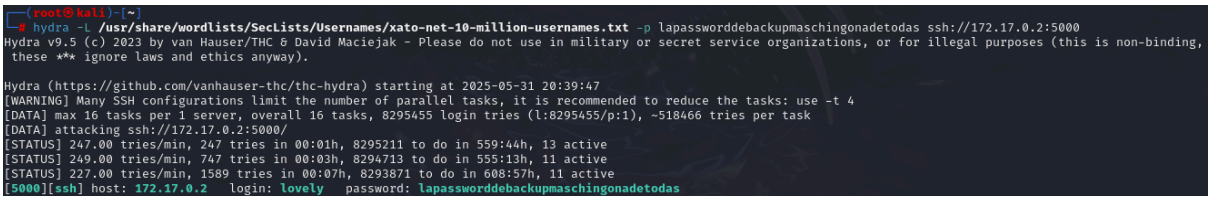


Al ingresar a /backend encuentro varios archivos, uno de esos es server.js. Al ingresar, veo que prácticamente si el token enviado es tokentraviesito, responde con la contraseña “lapassworddebackupmaschingonadetodas”.

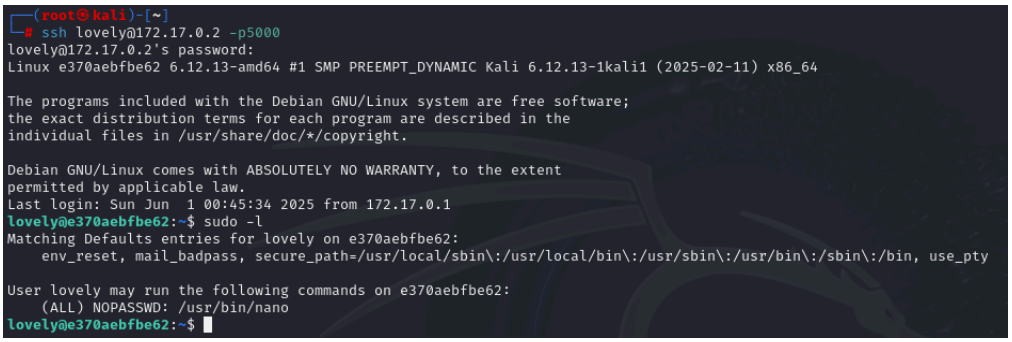


💥 3. Explotación de Vulnerabilidades

Como solo tengo la contraseña pero no un usuario. Utilizo fuerza bruta con Hydra al servicio SSH usando un diccionario de usernames para intentar encontrar credenciales válidas. Finalmente, encuentro un usuario que coincide con la contraseña encontrada.

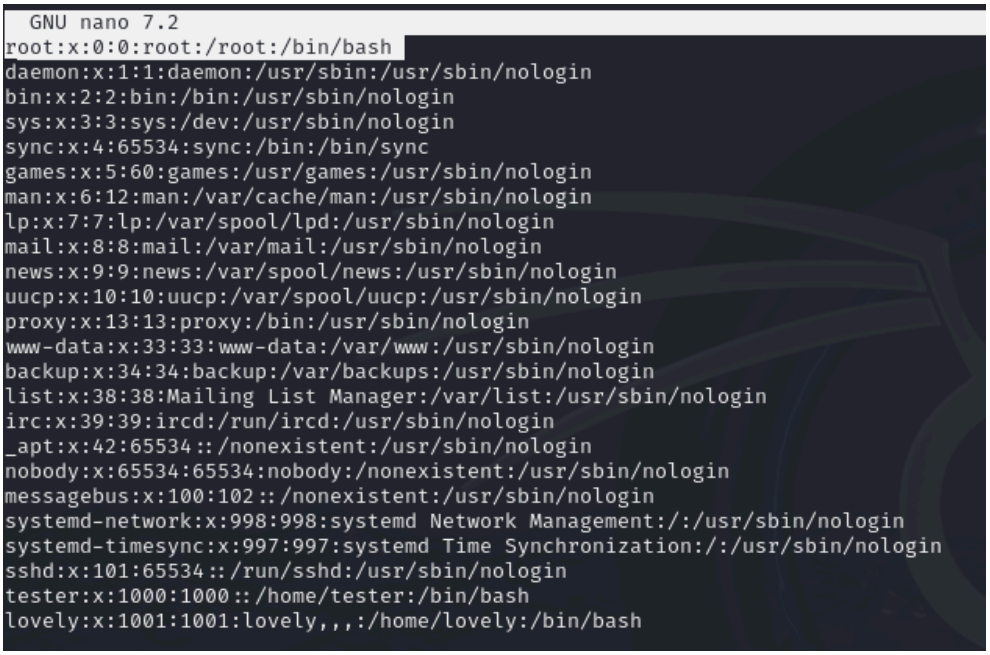


Ingreso por el puerto 5000 del servicio SSH. Con “sudo -l” obtengo que el usuario puede usar nano como sudo. Por ende, pensándolo bien y explorando los directorios decido usar nano para modificar /etc/passwd

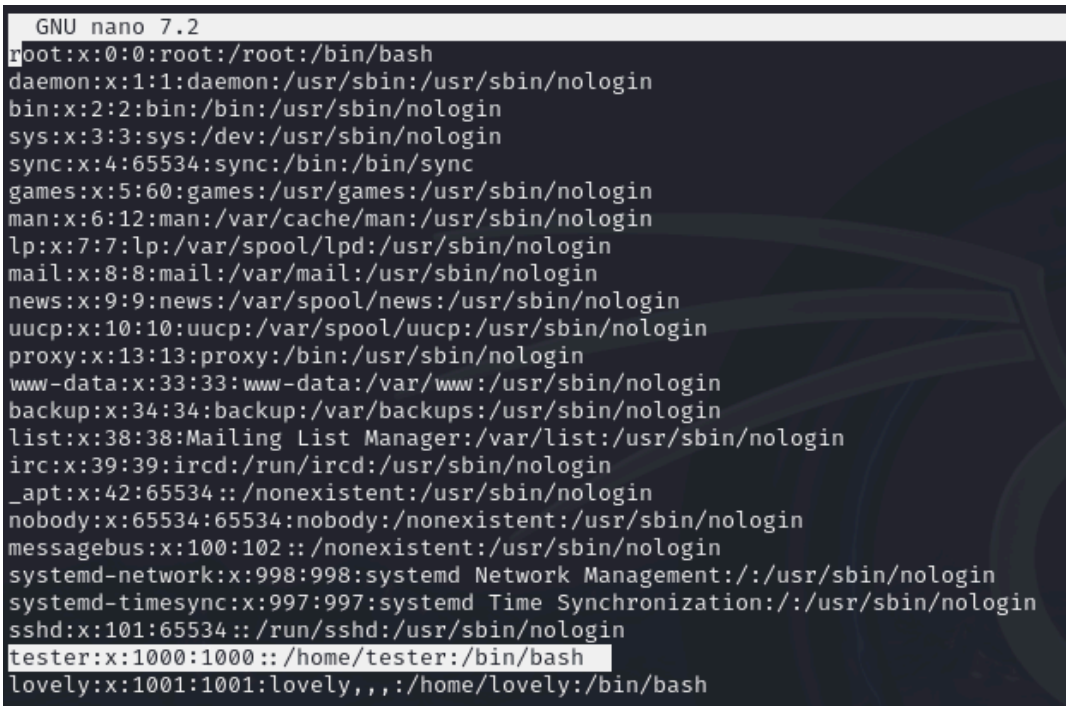


🔐 4. Escalada de Privilegios y Post-explotación

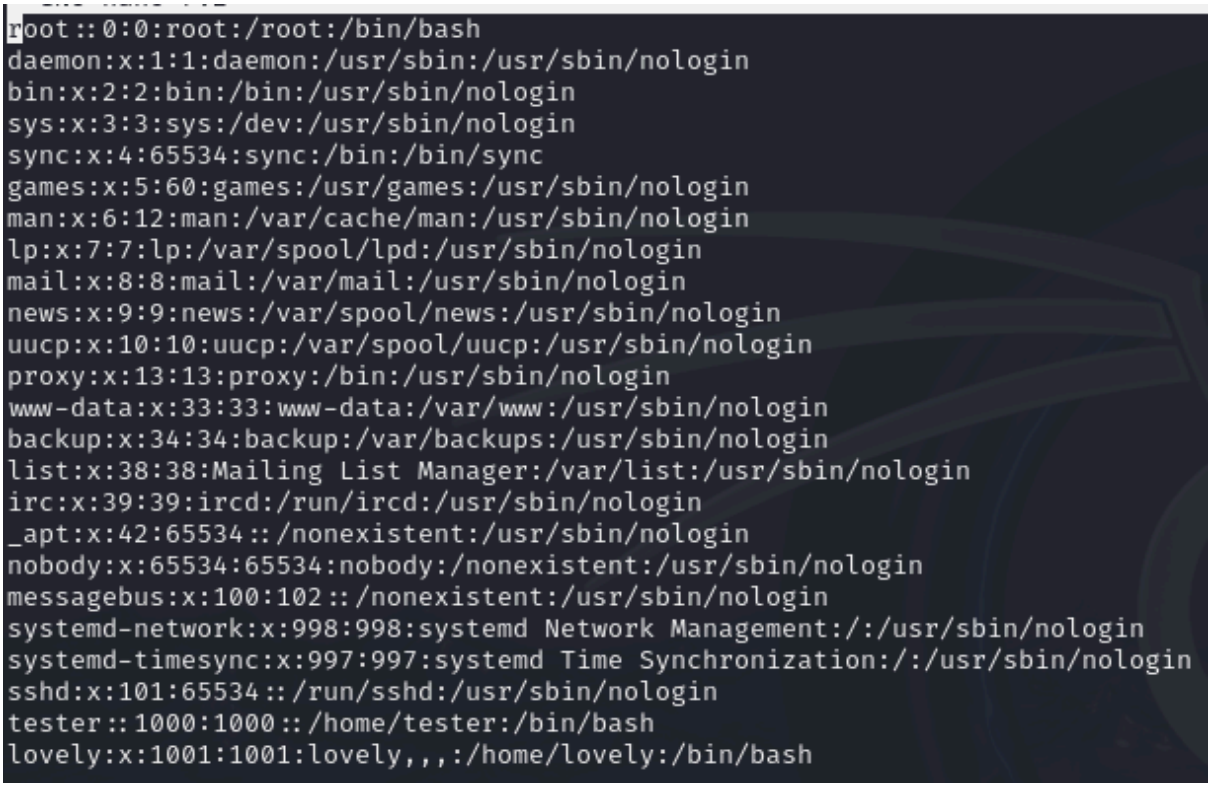
Identifico que existe el usuario root, pide contraseña para acceder al usuario y puede usar bash.



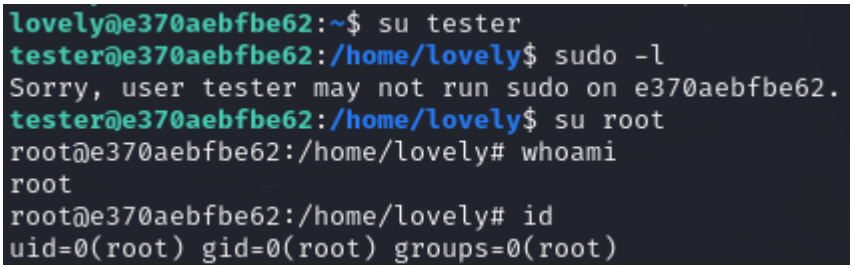
También, identifico que existe el usuario tester, pide contraseña para acceder al usuario y puede usar bash.



Con nano quito la “x” a root y tester para poder entrar a ese usuario sin tener que ingresar contraseña.



Finalmente, funcionó y puedo cambiar de usuario entre tester y root sin necesidad de colocar contraseña.



🏆 Banderas y Resultados

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