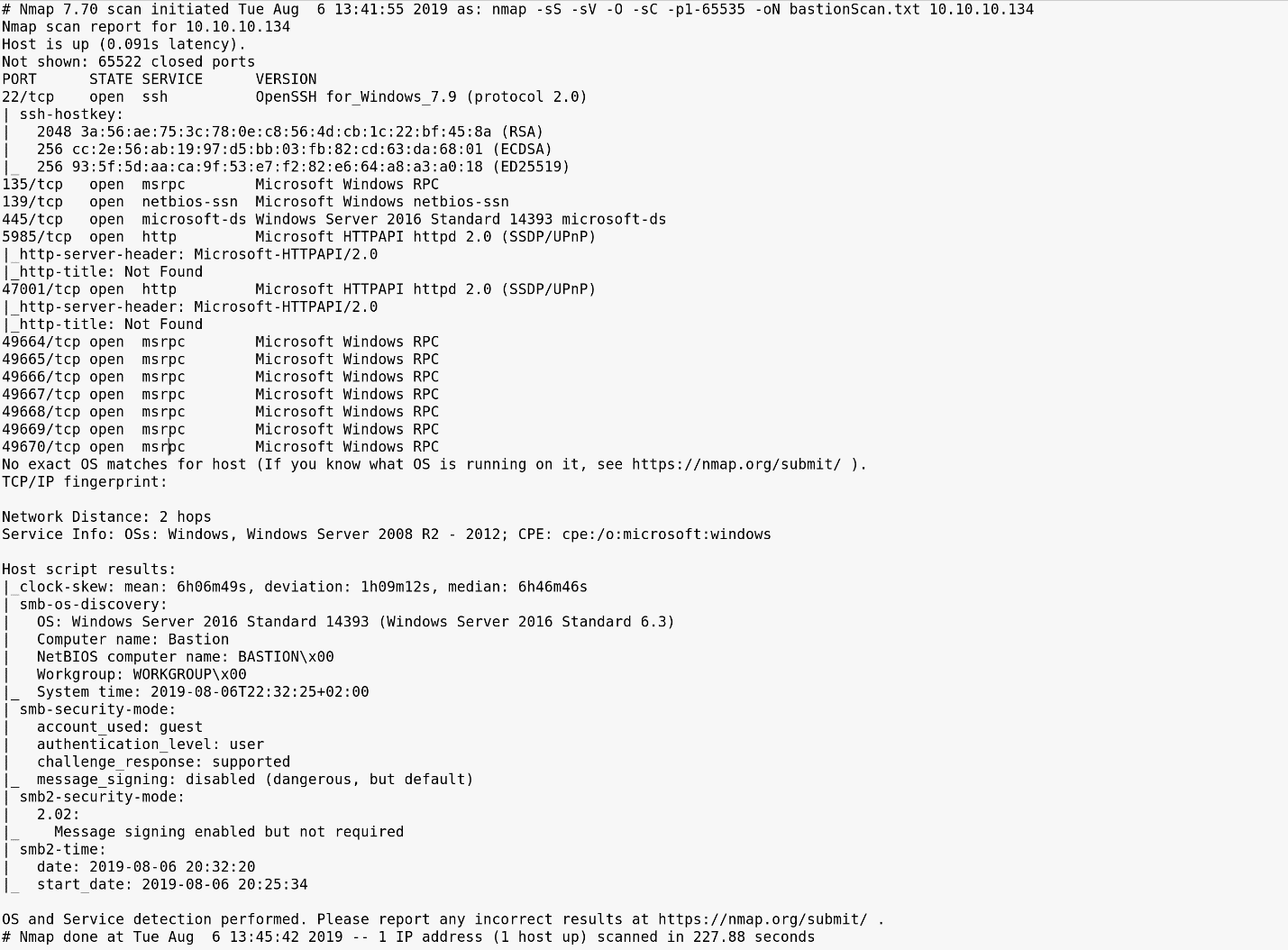
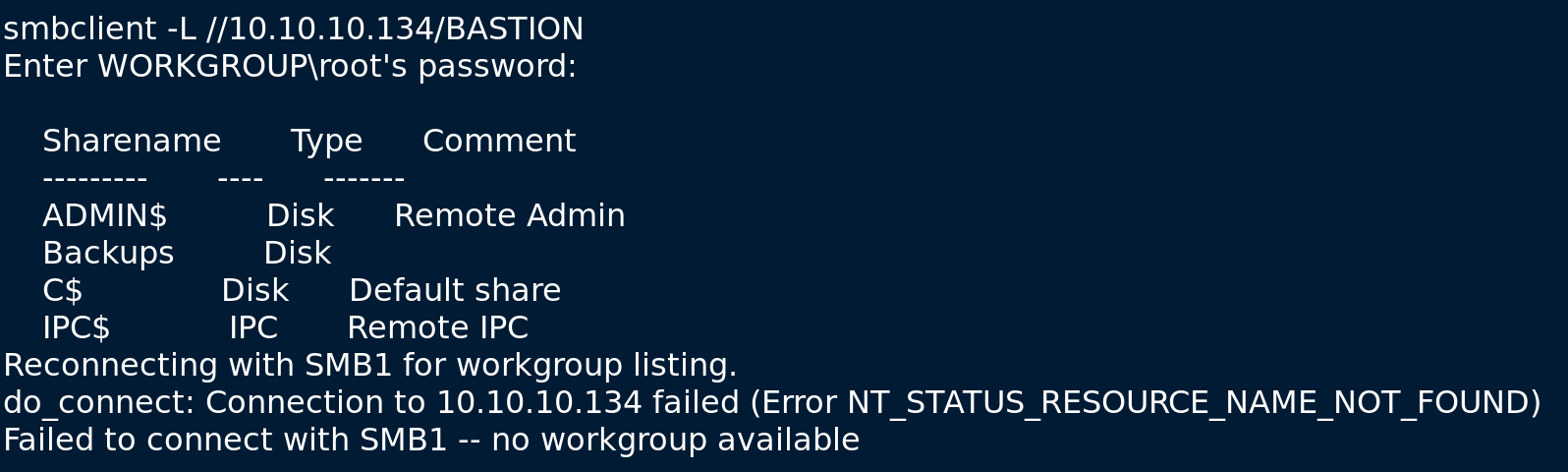
Bastion Writeup

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.



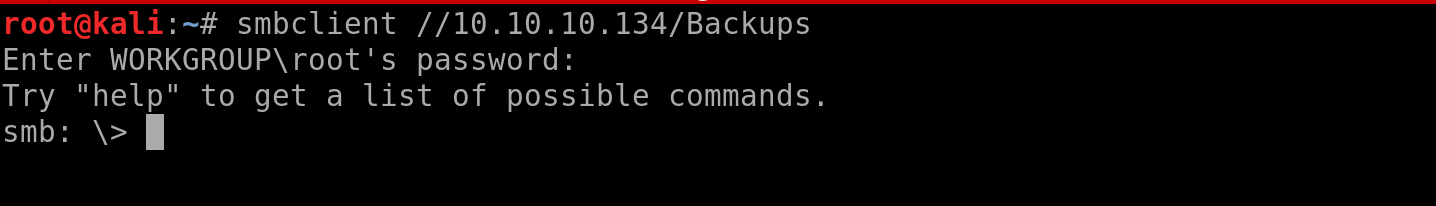
There are several open ports on this machine. Let’s attempt to connect to each port and see if any interesting information can be gleaned. Port 22 contains the standard SSH login and the version of SSH being used is not vulnerable to any RCE (Remote Code Execution) vulnerabilities. The next three ports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

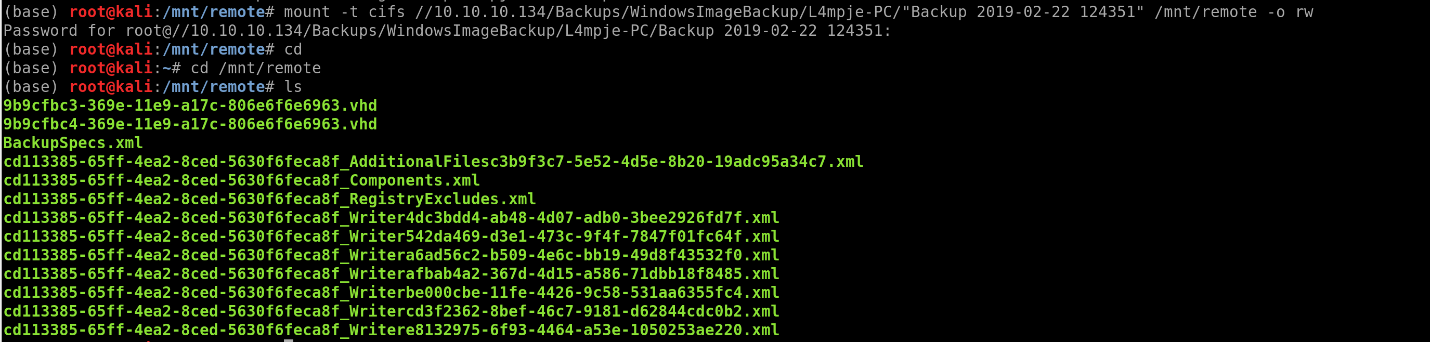


The screenshot, shown above, reveals that the target allows smb null sessions (no password is required to view shares). In addition, the Backups share does not appear to be protected. Checking the rest of the ports does not uncover any other useful information.

**Exploring Backups**

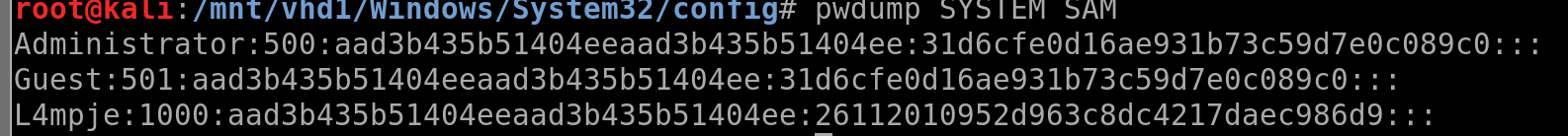
The tool smbclient can be used to connect to a share by dropping the -L flag.



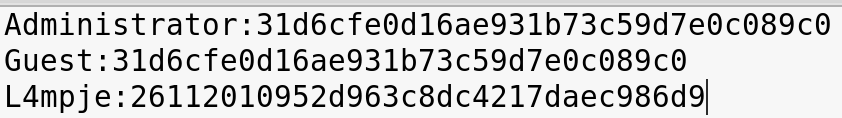
Exploring the Backups share reveals two VHD (virtual hard drive files). We can use the mount and guestmount utilities to explore the two VHD files. Open a new terminal window and navigate to /mnt directory. Next create two directories, in this writeup the directories remote and vhd1 were created. Finally 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.

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. 

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.



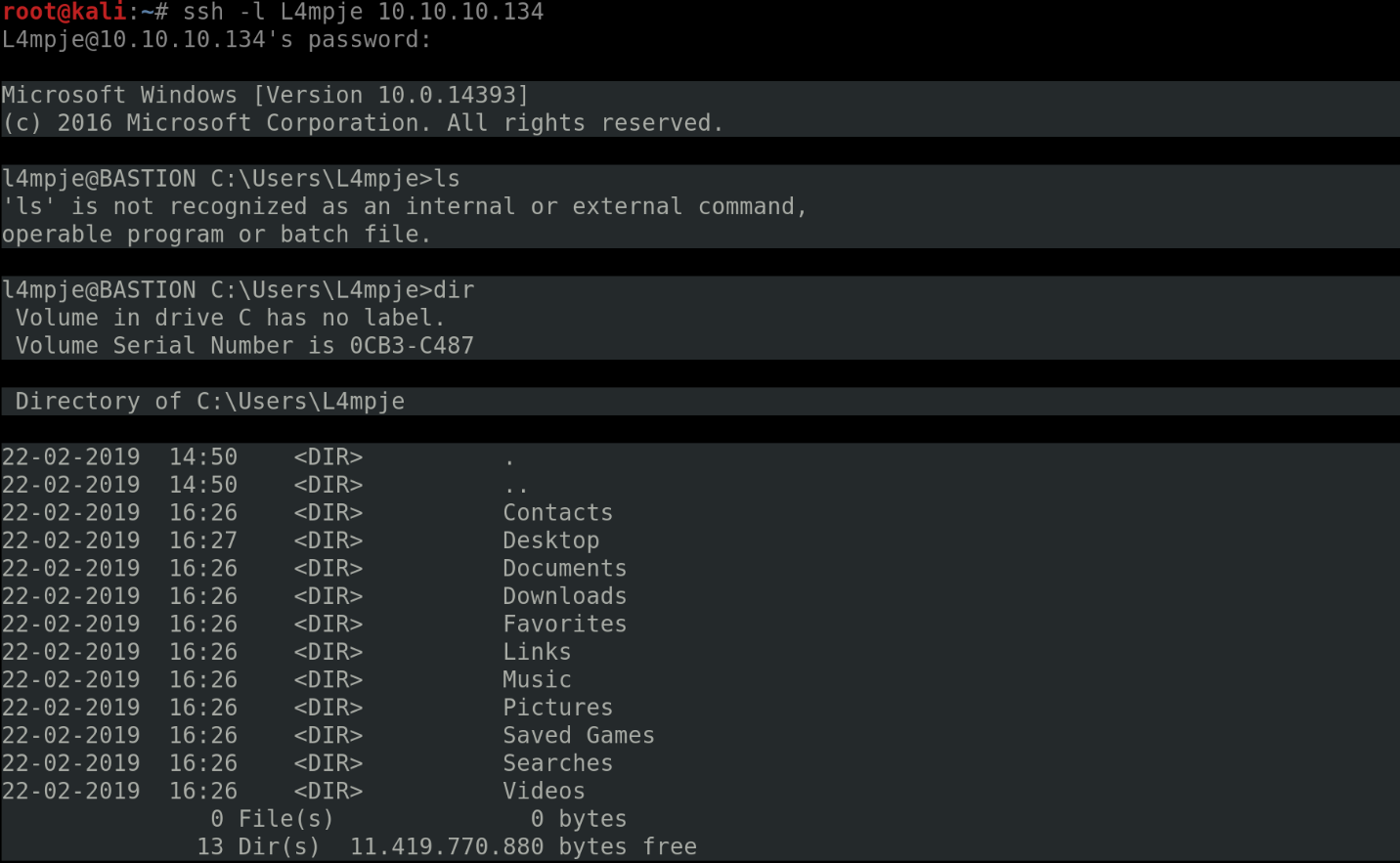
Now that we have the password hashes we can attempt to crack them. Windows uses NTLM hashing. The lm portion of the hash occurs first followed by a : and the NT version of the hash. Notice that the lm hashes that we obtained were all the same. The LM portion of the hash is the same for each because it 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:



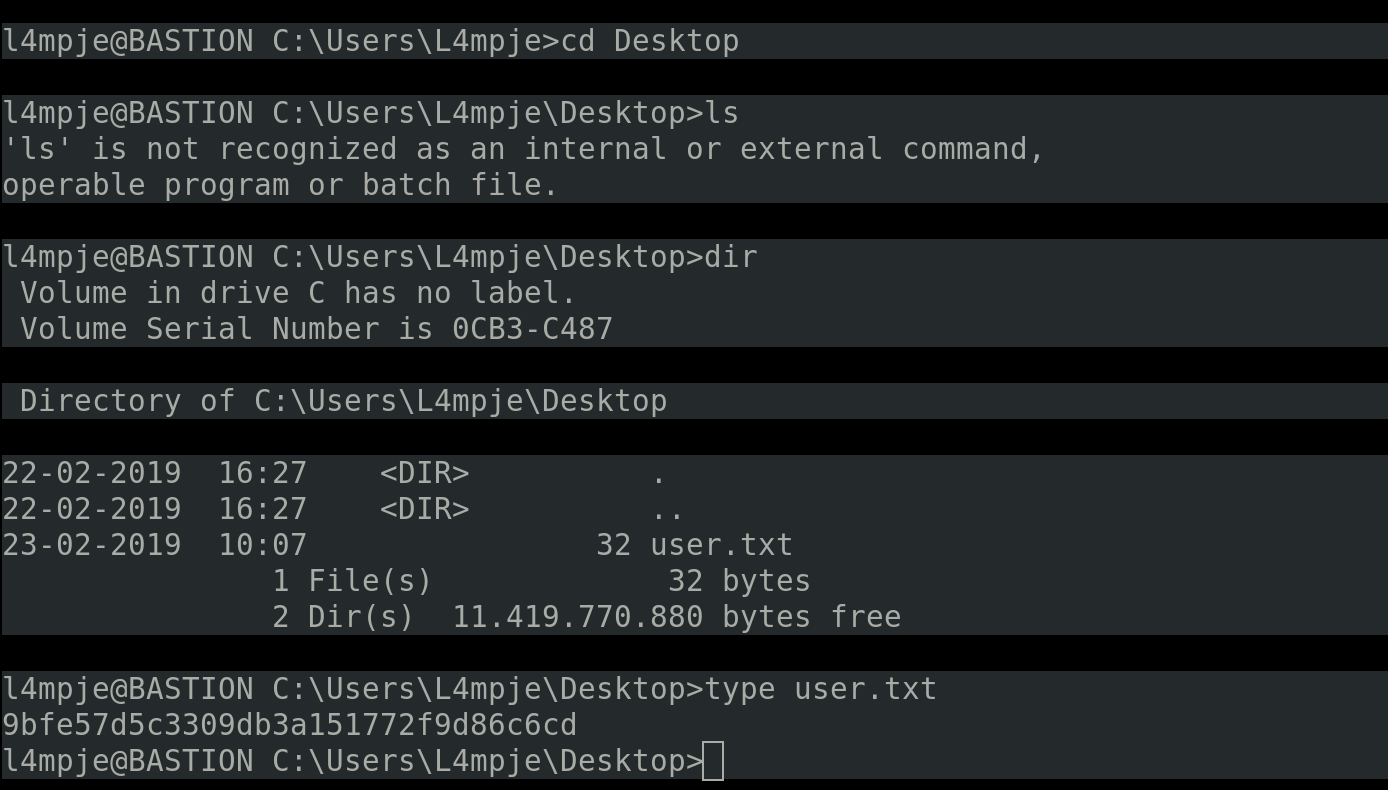
To run hashcat on this file issue the command: hashcat -a0 -m1000 --username hashCat.txt /usr/share/wordlists/rockyou.txt --force. Once the session completes issue the command hashcat -a0 -m1000 --username --show hashCat.txt /usr/share/wordlists/rockyou.txt. **PLACE SSH password here**.

Accessing the System

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



Navigate to the Desktop to find the user flag.



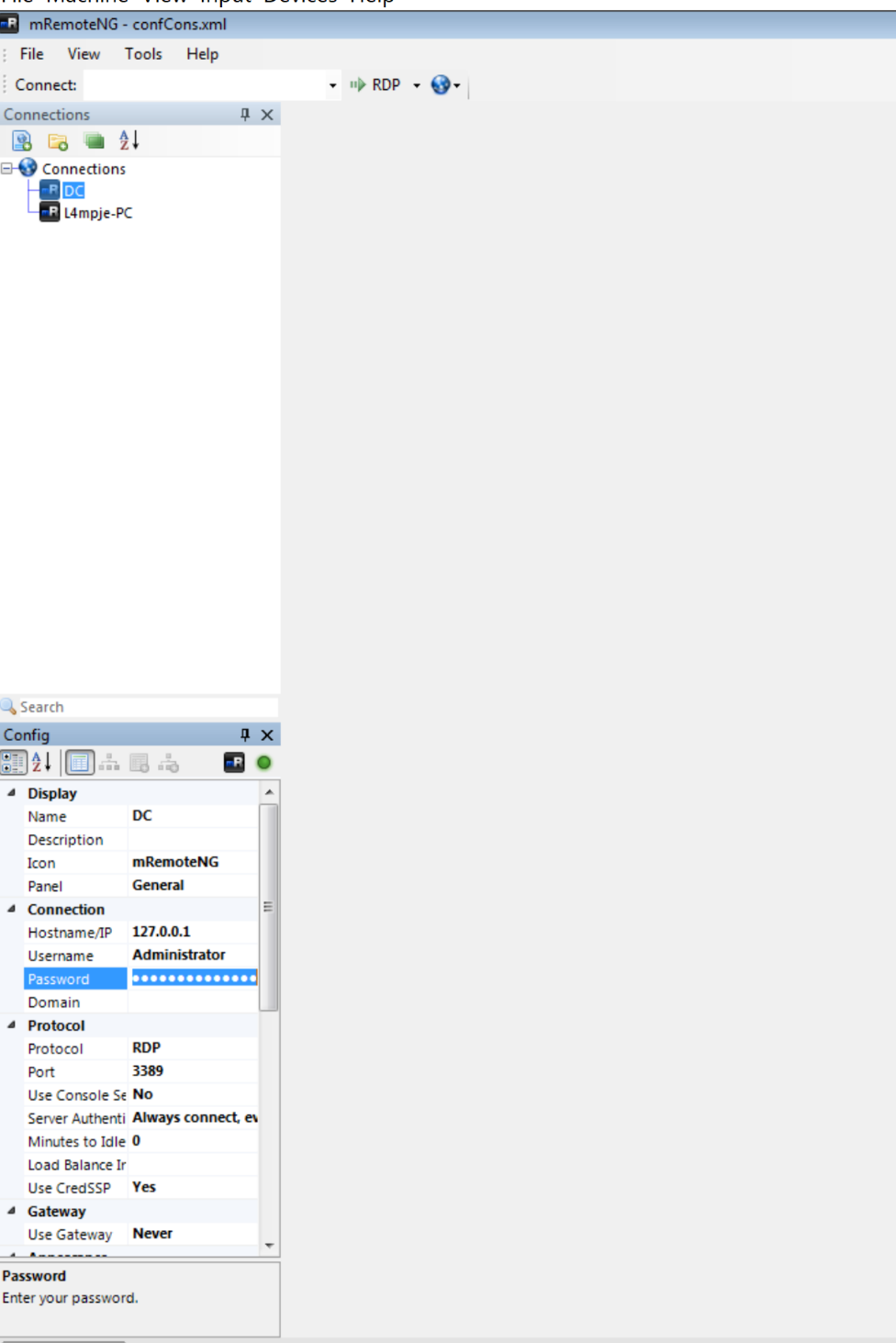
Getting System

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.

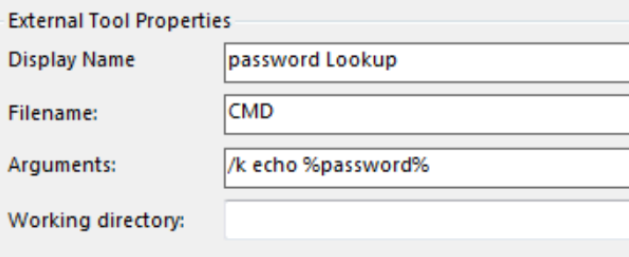


Unfortunately, the passwords are encrypted. Luckily, since this is a configuration file, we can decrypt the passwords by installing a local copy of mRemoteNG on a, windows seven virtual machine, and replacing the data between the mngr tags, on our copy of mRemoteNG, with the data from Bastion’s confCons.xml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

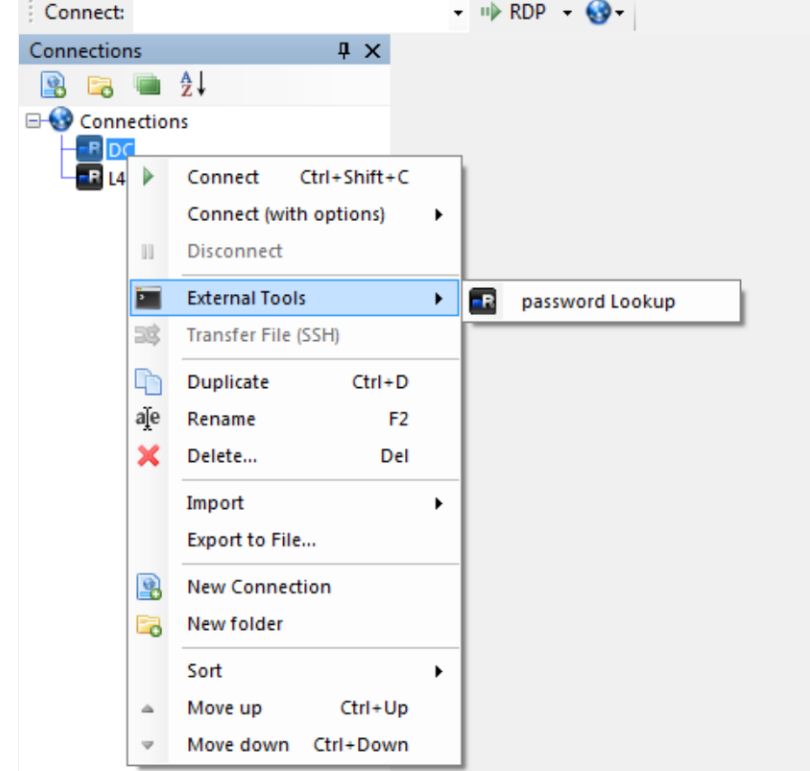


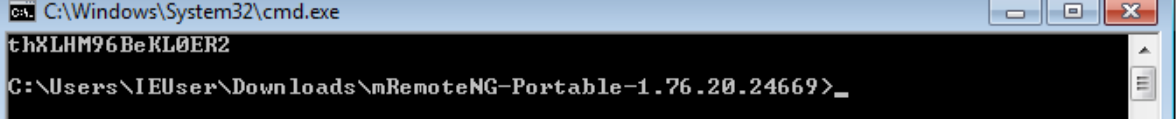
After launching mRemoteNG on the Windows seven machine you should be able to view the file without entering a password. 

To view the passwords, create a new mRemoteNG tool.



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





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