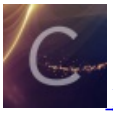
Hack The Box - Bastion Writeup

原创

ShinJoe 于 2019-08-29 15:51:04 发布 136 收藏
分类专栏： hackthebox

本文链接：https://blog.csdn.net/qq_23026851/article/details/90056238



- nmap 结果如下：

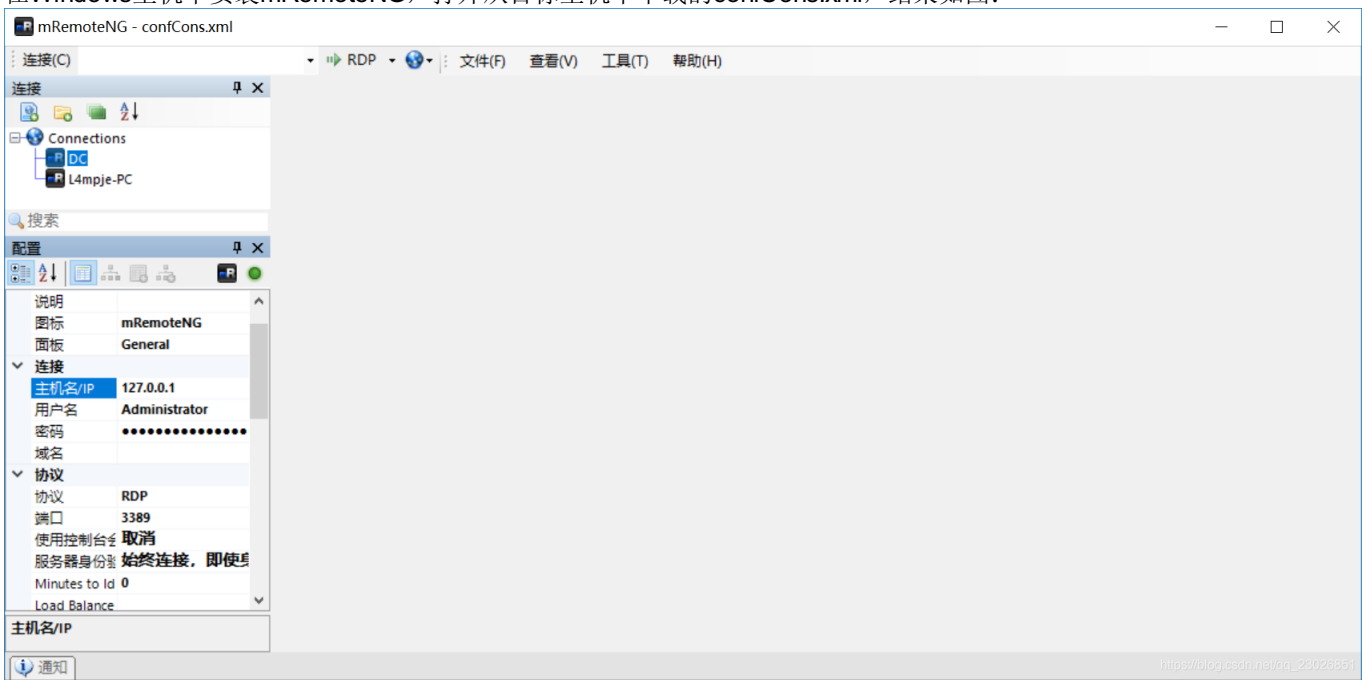
```
root@kali:~/HTB/Boxes/Bastion# cat nmap.out
# Nmap 7.70 scan initiated Sun Apr 28 22:49:29 2019 as: nmap -sV -sC -oN nmap.out 10.10.10.134
Nmap scan report for 10.10.10.134
Host is up (0.030s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE      VERSION
22/tcp  open  ssh          OpenSSH 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
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -50m21s, deviation: 1h09m15s, median: -10m23s
| 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: 2019-04-29T04:39:17+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: 2019-04-28 22:39:16
|_  start_date: 2019-04-28 02:54:28

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Apr 28 22:49:46 2019 -- 1 IP address (1 host up) scanned in 17.54 seconds
```


- 因为有RPC端口开放，因此我又进行了全端口扫描（nmap -p- -vvv 10.10.10.134），发现了一些其他的开放端口，其中5985端口运行着WinRM，说不定等会会用到。
- 用smbmap对445端口进行枚举，结果如下：

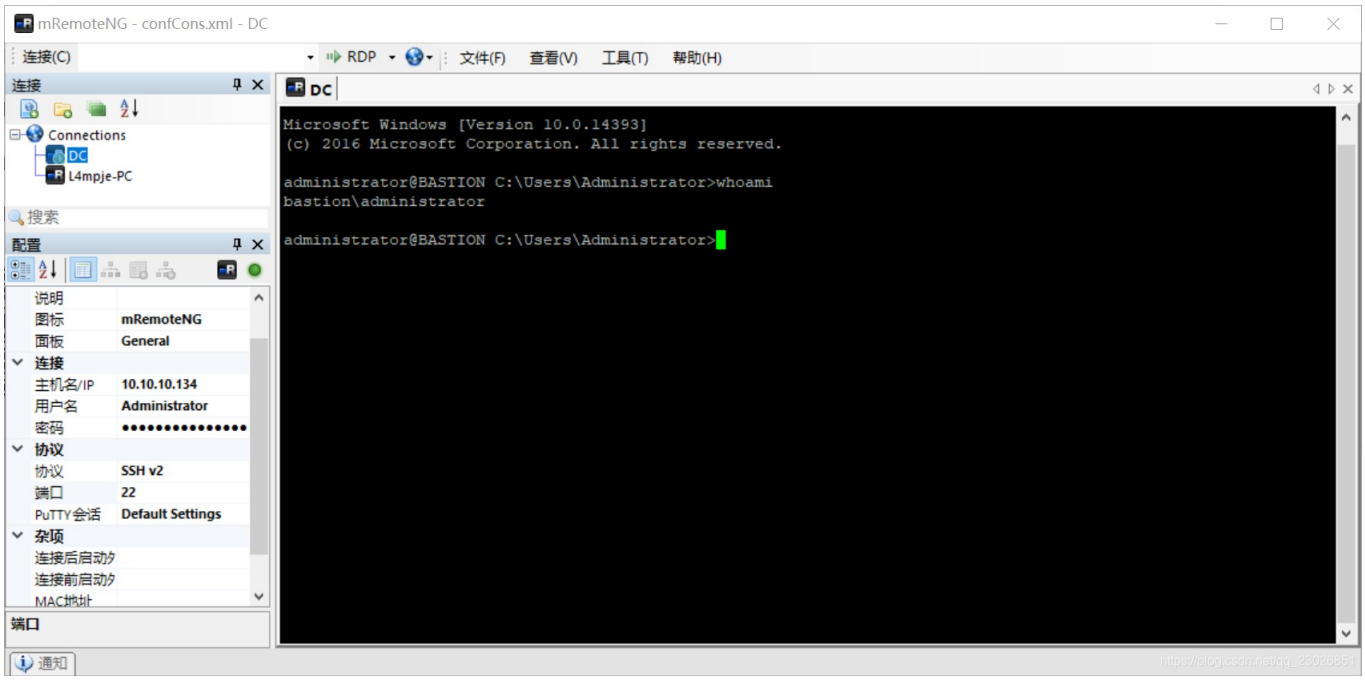
```
root@kali:~/HTB/Boxes/Bastion# smbmap -u guest -H 10.10.10.134
[+] Finding open SMB ports....
[+] User SMB session establishd on 10.10.10.134...
[+] IP: 10.10.10.134:445        Name: 10.10.10.134
        Disk                                                    Permissions
        ----                                                    -----------
        ADMIN$                                                  NO ACCESS
        Backups                                                 READ, WRITE
        [!] Unable to remove test directory at \\10.10.10.134\Backups\OgnQESsHeX, plreae remove manually
        C$                                                      NO ACCESS
        IPC$                                                    READ ONLY
```


- 我们对Backups这个共享有读的权限，可以用smbmap -u guest -H 10.10.10.134 -R Backups来进行目录遍历。其中可以看到vhd文件，vhd即virtual hard disk。
- 理论上可以远程挂载vhd文件进行操作，但我的Win10并没有自带Mount-VHD这一命令，HyperV的功能似乎也不开放，于是我索性把5G多的vhd直接下载下来了。
- 下载完之后，在Windows命令行中输入如下命令：
  - > diskpart
  - > select vdisk file="c:\a.vhd"
  - > attach vdisk
  - 结束后，> detach vdisk

- Windows的hash后的密码存储在C:\Windows\System32\config\SAM中，把SAM和SYSTEM文件复制到Kali中。使用samdump2把SAM提取成可破解的格式（samdump2 SYSTEM SAM > hash.txt）。
- 用John破解该hash：John --format=NT --wordlist=rockyou.txt hash.txt，得到一对用户名和密码。
- 凭借刚得的用户名和密码，通过ssh登录远程主机，此时可查看user.txt。
- 为了提升权限，可以跑Sherlock.ps1查看有无漏洞。然而这个box不需要我们这么做，因为它安装了一个叫mRemoteNG（https://github.com/mRemoteNG/mRemoteNG）的软件。该软件的confCons.xml中存储了远程连接的配置信息，我们只需要利用这个xml文件即可。
- 在Windows主机中安装mRemoteNG，打开从目标主机中下载的confCons.xml，结果如图：



- Administrator的密码已经被通过xml文件自动加载了，保持原样就好，至于具体是什么需要关心吗？修改IP和连接协议（RDP->SSHv2），右键连接，搞定。



这个box不是很难，但相当realistic。我在整个过程中学到了很多东西，比如smb enumeration，vhd如何挂载，mRemoteNG等等，非常有意思。