**Bastion walkthrough**

# **Index**

[Index 1](#_Toc184488015)

[List of pictures 1](#_Toc184488016)

[Disclaimer 2](#_Toc184488017)

[Reconnaissance 2](#_Toc184488018)

[Initial foothold 2](#_Toc184488019)

[User flag 4](#_Toc184488020)

[Privilege escalation 5](#_Toc184488021)

[Personal comments 6](#_Toc184488022)

[References 6](#_Toc184488023)

# **List of pictures**

[Figure 1 - nMap scan results 2](#_Toc184488005)

[Figure 2 - SMB null session connection 3](#_Toc184488006)

[Figure 3 - Possible username 3](#_Toc184488007)

[Figure 4 - Note.txt file found 3](#_Toc184488008)

[Figure 5 - Virtual Hard Disks (VHD) found 4](#_Toc184488009)

[Figure 6 - Hashed user passwords 4](#_Toc184488010)

[Figure 7 - Password cracked 4](#_Toc184488011)

[Figure 8 - User flag 5](#_Toc184488012)

[Figure 9 - Password found 5](#_Toc184488013)

[Figure 10 - Administrator password cracked 6](#_Toc184488014)

# **Disclaimer**

I do this box to learn things and challenge myself. I’m not a kind of penetration tester guru who always knows where to look for the right answer. Use it as a guide or support. Remember that it is always better to try it by yourself. All data and information provided on my walkthrough are for informational and educational purpose only. The tutorial and demo provided here is only for those who are willing and curious to know and learn about Ethical Hacking, Security and Penetration Testing.

Just to say: I am not an English native person, so sorry if I did some grammatical and syntax mistakes.

# **Reconnaissance**

The results of an initial nMap scan are the following:

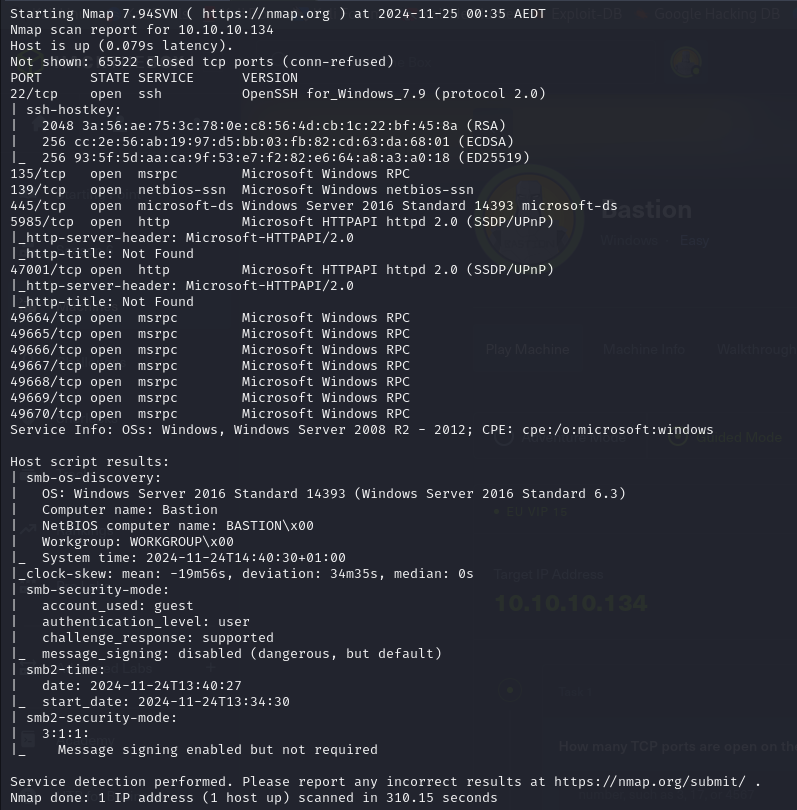


Figure 1 - nMap scan results

Open ports are 22, 135, 139, 445, 5985, 47001, 49664, 49665, 49666, 49667, 49668, 49669 and 49670. So, it seems to be SSH (port 22) service enabled, Microsoft RPC (ports 135, 49664, 49665, 49666, 49667, 49668, 49669 and 49670) service enabled, NetBios (port 139) service enabled, SMB (port 445) service enabled and two web application running on ports 5985 and 47001. Also, it seems to be a Windows target.

# **Initial foothold**

Since it seems to be a Windows target, one of my first task it is to connect to the SMB service via a null session, as shown in the following picture:

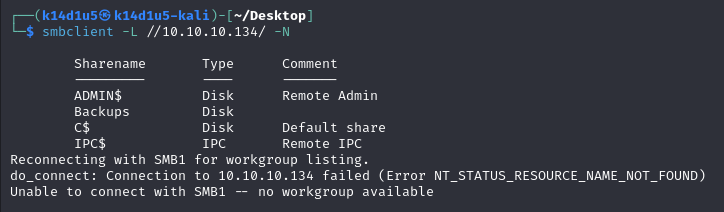


Figure 2 - SMB null session connection

Luckily, I was able to do it. So, I tried to browsing the shares, the one named in particular. In this share I found two interesting information:

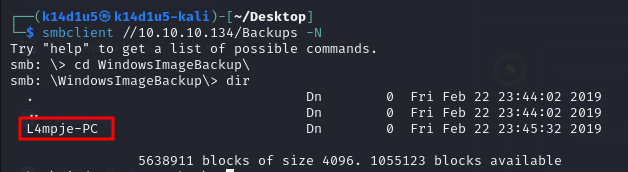


Figure - Possible username

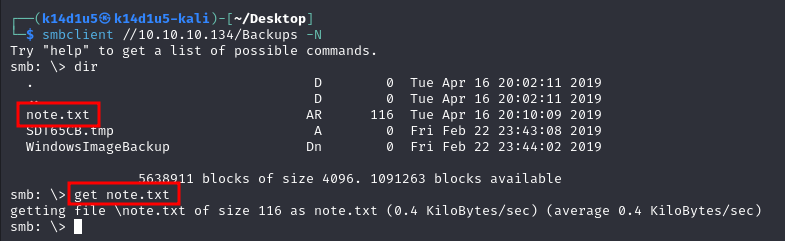


Figure 4 - Note.txt file found

In the first screenshot, I show I found a directory named as a hostname. So, it could be a username. In the second one, I show I found an interesting file. I forgot the screenshot of its content, but it advices me to not download the backups on my local machine because the VPN was too slow. I kept to search something useful and I found two virtual disks, as shown in the following picture:

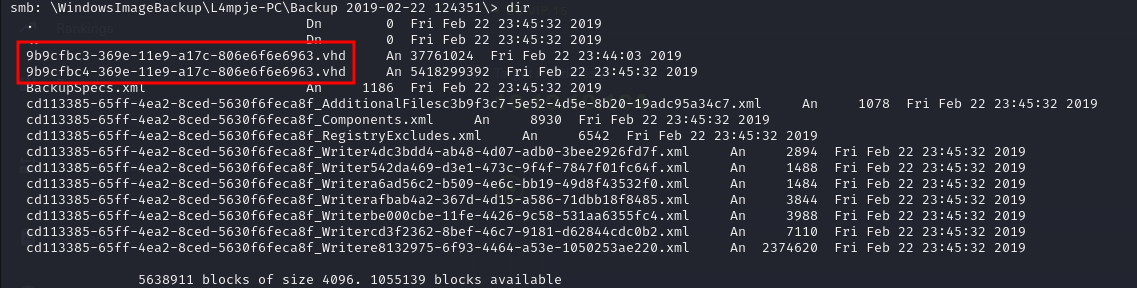


Figure 5 - Virtual Hard Disks (VHD) found

At this point I was curious to investigate these disks. To do it, I mounted the share on my local Kali Machine running the command: . At this point I extracted a list of all files contained in the bigger disk running the command: . In this way, I found out that it was the actual file system of a Windows machine. So, I thought that my next move would be to get the and files. I completed this task just running the following commands: and .

# **User flag**

Since I obtained the SAM and SYSTEM files, I tried to extract the hashed user passwords running the script, as shown in the following figure:

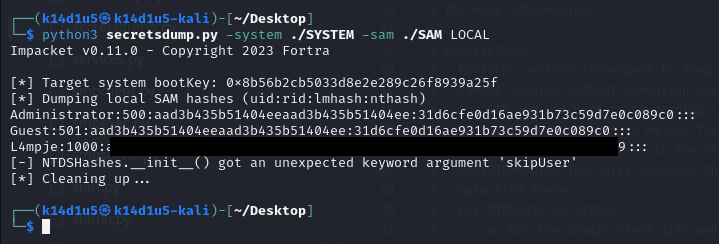


Figure 6 - Hashed user passwords

At this point I just need to crack the L4mpje’s password, so I copied his row in a file and I run John The Ripper tool (using my custom password wordlist):

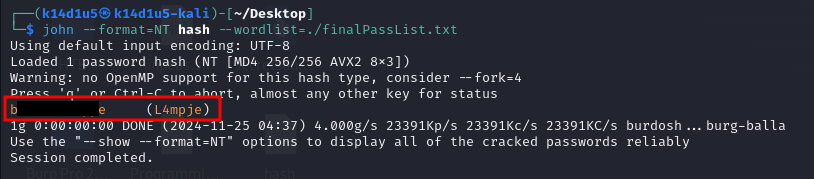


Figure 7 - Password cracked

Luckily, I was able to crack the password and I used these credentials to log in via SSH on the target and retrieve the user flag:

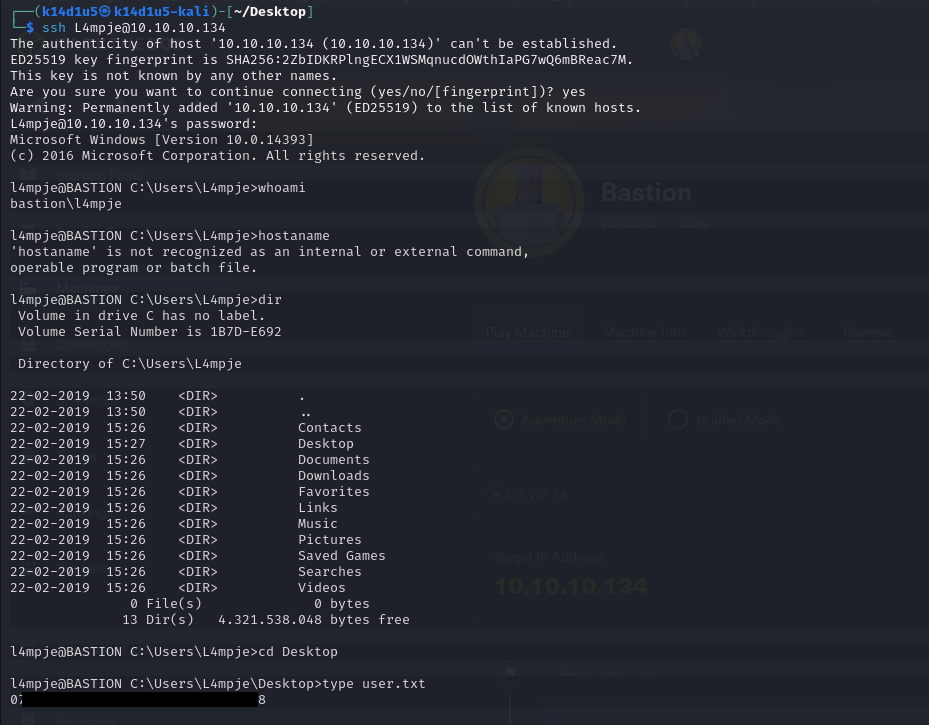


Figure 8 - User flag

# **Privilege escalation**

I just need to escalate my privileges. To do it, I initially run WinPeas, but I didn’t find anything useful. So, I looked for a clue on the file system. Browsing it, I found out that a program named is installed. Honestly, I didn’t know it. So, I looked for some information on the Internet. I learnt that it is a program to establish remote connection. Also, I found some interesting exploits against this program. However, the exploits I found were too newer than the box, so I decided to not use them because it was not the lesson I had to learn. I kept to look for some other information and I learnt that this program can store credentials in the file:

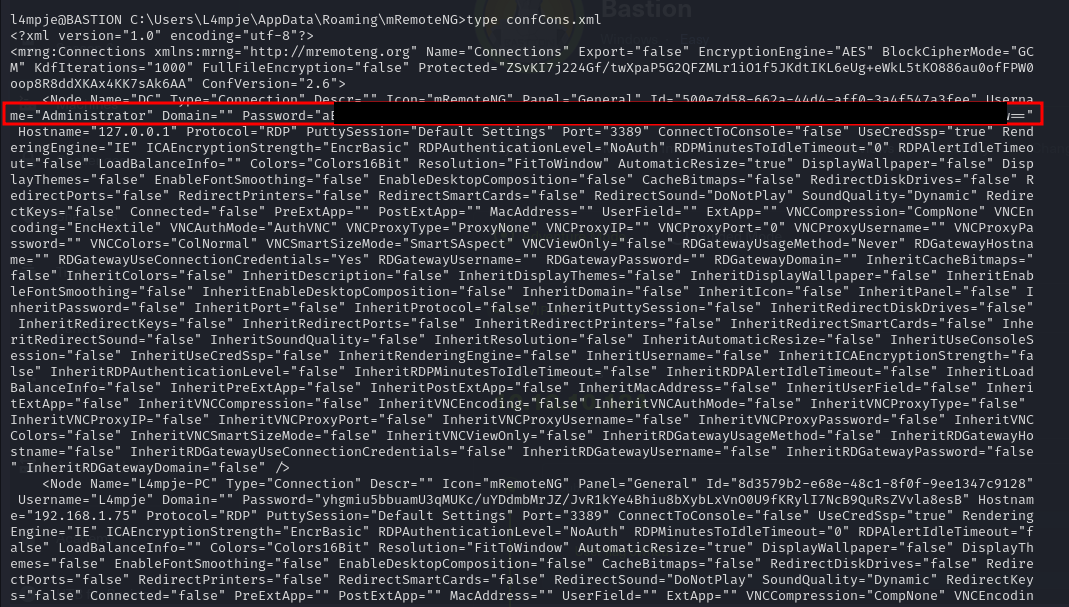


Figure 9 - Password found

It seems to be a base64 encoded password, but it was not. So, I looked again on the Internet and I found a python script to decrypt password. I run it and I obtained the Administartor password:

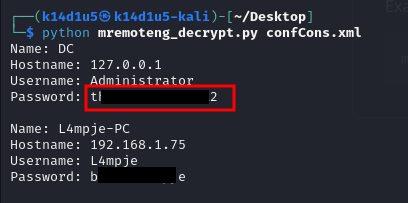


Figure 10 - Administrator password cracked

At this point, I just use them to log in on the target via SSH and I retrieved the root flag (I forgot the screenshots).

# **Personal comments**

This box was very interesting for me. I learnt new concepts about how to analyze a virtual hard disk (VHD) and I learnt about the program. However, the exploits were easy. I really enjoyed it. I evaluate it as Easy on the Hack The Box platform.

# **References**

<https://book.hacktricks.xyz/network-services-pentesting/135-pentesting-msrpc>

<https://github.com/gquere/mRemoteNG_password_decrypt>