**Chatterbox walkthrough**

# **Index**

[Index 1](#_Toc202777724)

[List of pictures 1](#_Toc202777725)

[Disclaimer 2](#_Toc202777726)

[Reconnaissance 2](#_Toc202777727)

[Initial foothold 2](#_Toc202777728)

[User flag 3](#_Toc202777729)

[Privilege escalation 4](#_Toc202777730)

[Personal comments 5](#_Toc202777731)

[References 5](#_Toc202777732)

# **List of pictures**

[Figure 1 - nMap scan results 2](#_Toc202777737)

[Figure 2 - User shell 3](#_Toc202777738)

[Figure 3 - User flag 3](#_Toc202777739)

[Figure 4 - Credentials found 4](#_Toc202777740)

[Figure 5 - NT AUTHORITY SYSTEM shell 4](#_Toc202777741)

[Figure 6 - Root flag 5](#_Toc202777742)

# **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:

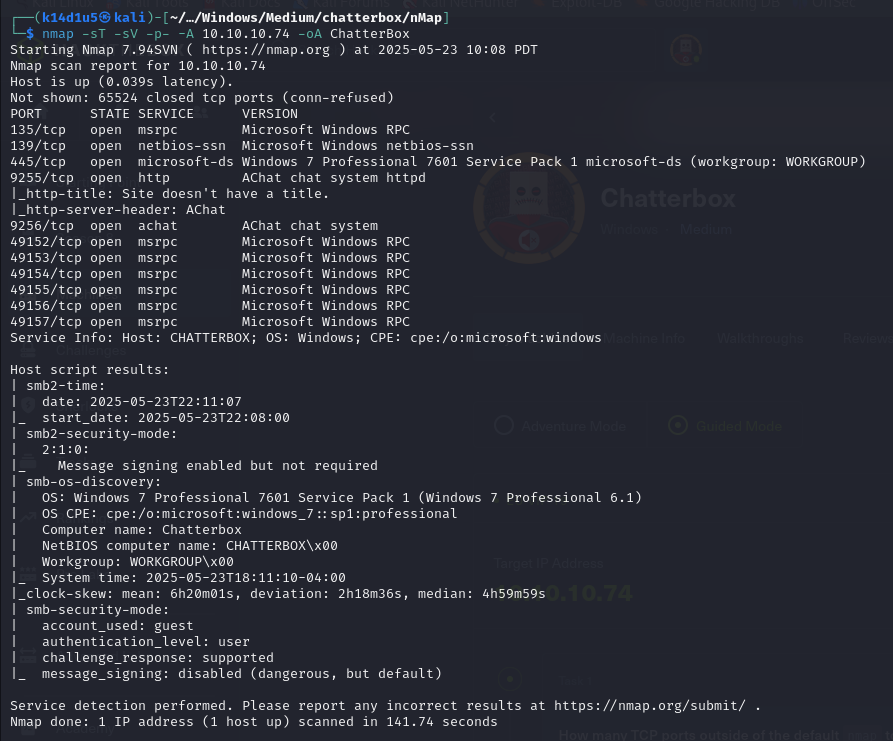


Figure - nMap scan results

Open ports are 135, 139, 445, 9255, 9256, 49152, 49153, 49154, 49155, 49156 and 49157. Therefore, enabled services are MSRPC (135, 49152, 49153, 49154, 49155, 49156 and 49157), NetBIOS (139), SMB (445) and a web application running on ports 9255 and 9256. Also, nMap recognized Windows as operative system.

# **Initial foothold**

As my usual, I started to analyze the web application. However, I was not able to have data and information browsing it via browser. Therefore, I tried to analyze some interesting named pipe to exploit. I found some interesting, but I needed credentials I haven’t. At this point I came back on the AChat web application and I found a public exploit.

# **User flag**

I download the AChat public exploit I found and generated an MSFVenom payload to force the application to download and execute a PowerShell script. I let the application to download the Invoke-PowerShellTcp PowerShell script in which I added the command line to open a reverse shell at the end of the file. When I run the Achat exploit with an opened listener, I obtain the user shell:

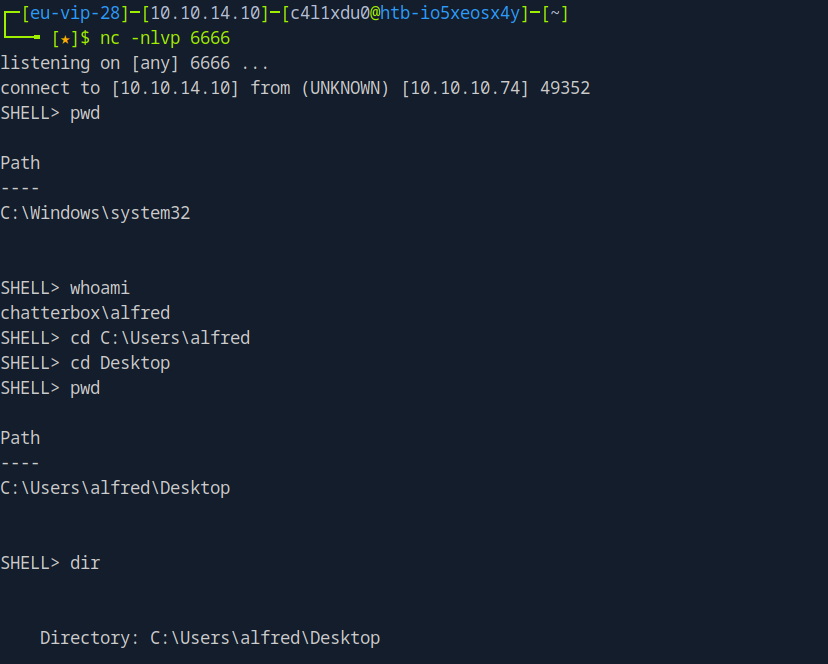


Figure 2 - User shell

Using this shell, I was able to retrieve the user flag:

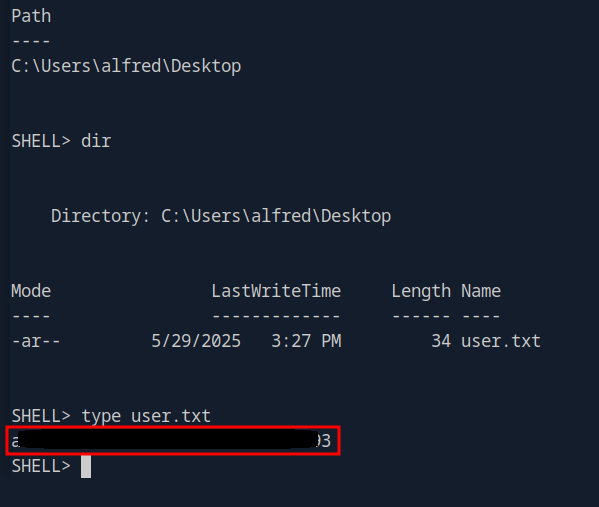


Figure 3 - User flag

# **Privilege escalation**

At this point I needed to escalate my privileges. I tried to upload WinPeas, but its results weren’t useful in this case. Therefore, I tried to look for some interesting information. After a little while, I found some credentials in registry, as shown in the following picture:

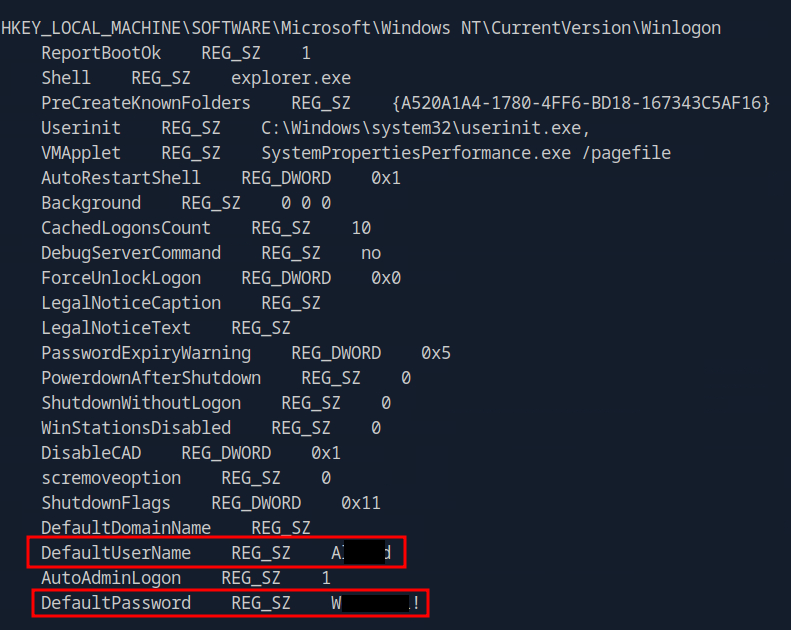


Figure 4 - Credentials found

Again, after a while I tried to use these credentials to login as Admin and, luckily, they worked. In particular, I used psexec to connect as Administrator:

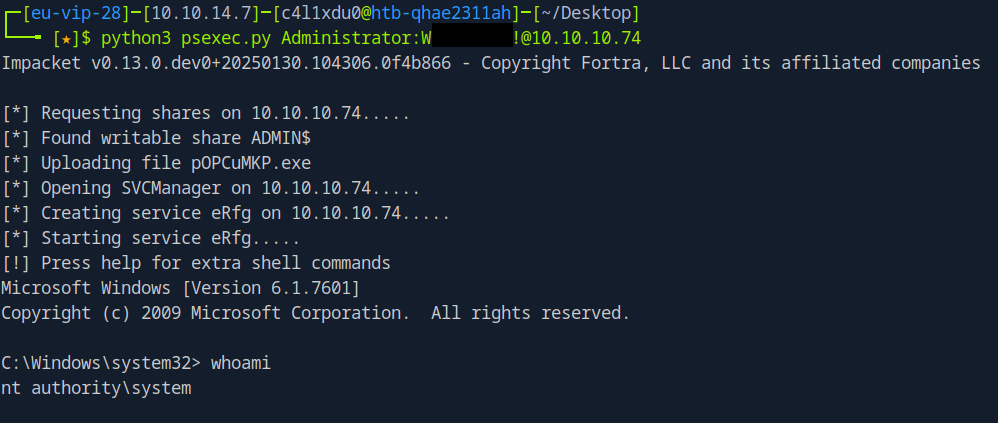


Figure 5 - NT AUTHORITY SYSTEM shell

Even I had a privileged shell, I was not able to retrieve the root flag. To do it, I opened the RDP protocol running the following two commands:

1. reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG\_DWORD /d 0 /f
2. netsh firewall add portopening TCP 3389 "Remote Desktop"

At this point, I connected as Administrator via RDP and I retrieved the root flag:

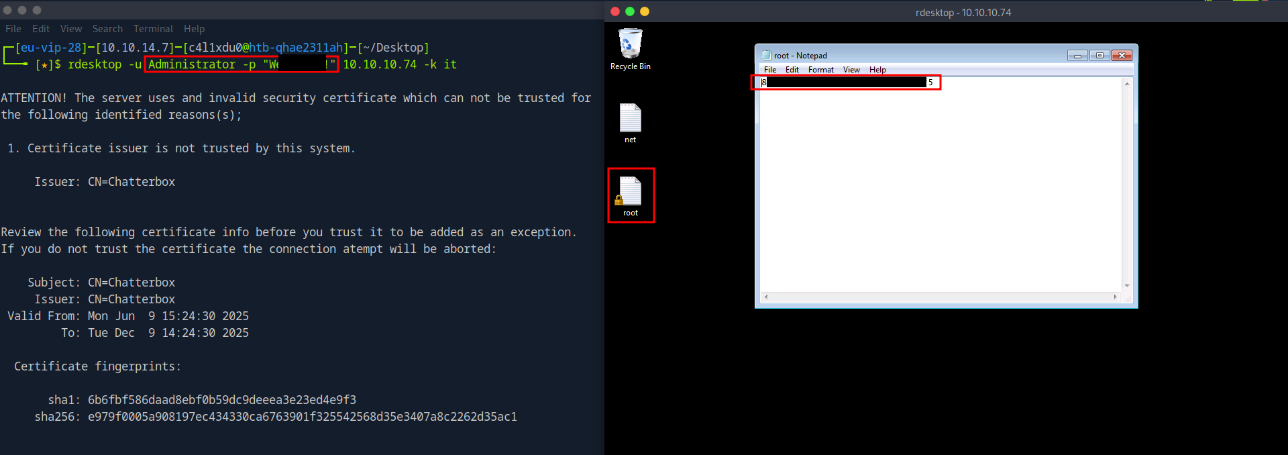


Figure 6 - Root flag

# **Personal comments**

This box was overall pretty simple. However, I was experienced a very bad user experience and I still don’t understand why. For this reason, I was forced to use the Parrot Pwnbox provided by HackTheBox platform to complete it. I was very annoyed about it. Also, it was interesting to check the AutoLogOn registry. Lastly, it was very strange that when I obtained the Administrator shell, I wasn’t able to retrieve the root flag and I needed to use RDP to do it. In my opinion, it was a good and interesting box overall.

# **References**

1. AChat exploit: <https://github.com/mpgn/AChat-Reverse-TCP-Exploit>.