Metasploit Framework

Material extraído de http://www.offensive-security.com

Traducido con Google Chrome

Editado con Libreoffice, Calibre, Sigil y Gimp.

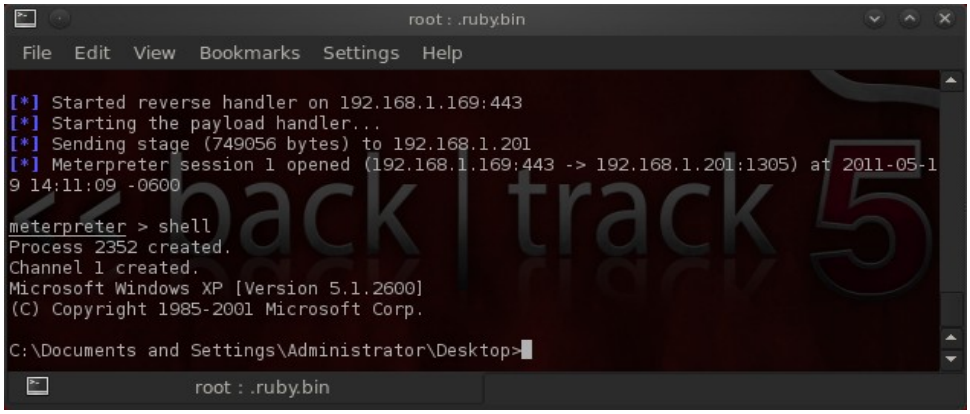
siriusinfoblog.blogspot.com

sirius.infoblog[at]gmail[dot]com

Introducción #01

"Si tuviera ocho horas para cortar un árbol, me pasaría las primeras seis de ellos afilar mi hacha".

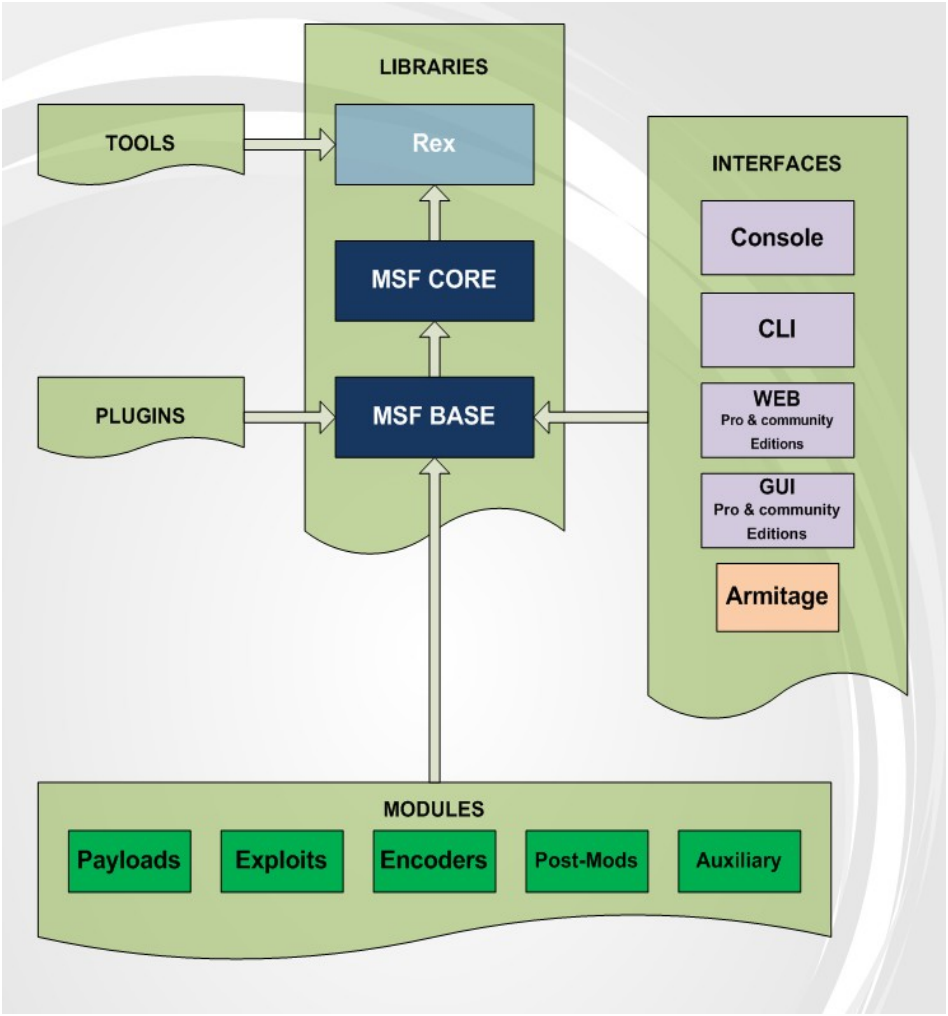
-Abraham Lincoln



Esta frase me ha seguido durante muchos años, y es un recordatorio constante de que me acerca a un problema con el conjunto adecuado de herramientas es imprescindible para el éxito. Entonces, ¿qué significa esta apertura semi filosófico tiene que ver con el Metasploit Framework? Antes de acercarse a una prueba de penetración o una auditoría, yo cuido a "afilar mis herramientas" y actualizar nada actualizable en BackTrack. Esto incluye una reacción de cadena corta, que siempre comienza con un mensaje "msfupdate" del marco de Metasploit. Considero que la MSF para ser una de las herramientas de auditoría individuales más útiles libremente disponibles para los profesionales de seguridad actuales. A partir de una amplia gama de comerciales hazañas de grado y un entorno de desarrollo de explotación extensiva, hasta llegar a las herramientas de la red de recolección de información y plugins web de vulnerabilidad. El Metasploit Framework

proporciona un entorno de trabajo realmente impresionante. El MSF es mucho más que una simple colección de exploits, es una infraestructura que se puede aprovechar y utilizar para sus necesidades personalizadas. Esto le permite concentrarse en su ambiente único, y no tener que reinventar la rueda. Este curso se ha redactado de forma que abarque no sólo los frontales de "usuario" aspectos del marco, sino más bien darle una introducción a las capacidades que ofrece Metasploit. Nuestro objetivo es dar una mirada en profundidad a las muchas características de la MSF, y le proporcionará las habilidades y la confianza para utilizar esta herramienta increíble para sus capacidades extraordinario. Haremos lo posible para mantener este curso al día con todos los nuevos y emocionantes Metasploit tiene como su incorporación. Cierto grado de conocimiento previo que se espera y exige a los estudiantes antes de que el contenido proporcionado en este curso será útil. Si usted encuentra que usted no está familiarizado con un determinado tema, se recomienda pasar el tiempo dedicados a la investigación propia sobre el problema antes de intentar el módulo. No hay nada más satisfactorio que resolver problemas por sí mismo, por lo que se le animo a Try Harder ™

Metasploit Arquitectura



Sistema de Archivos y Bibliotecas

El sistema de ficheros MSF se presenta de una manera intuitiva y está organizado por el directorio.

- •datos: archivos editables utilizadas por Metasploit
- •documentación: proporciona documentación para el marco
- •código fuente y las bibliotecas de terceros: externo
- •lib: la "carne" de la base de código marco

•módulos: los módulos actuales de MSF
•plugins: plugins que se pueden cargar en tiempo de ejecución
•scripts: Meterpreter y otros scripts
•diversas herramientas: útiles utilidades de línea de comandos

Bibliotecas

Rex

•La biblioteca básica para la mayoría de tareas
•Maneja sockets, protocolos, transformaciones de texto y otros
•SSL, SMB, HTTP, XOR, Base64, Unicode

MSF :: Core

•Proporciona la «base» API
•Define el Metasploit Framework

MSF :: Base

•Proporciona el «amigo» API
•Proporciona APIs simplificado para el uso en el Marco

Módulos y Localizaciones

Metasploit, tal como se presenta al usuario, se compone de módulos.

Exploits

- Definido como los módulos que utilizan cargas útiles
- Una hazaña sin una carga útil es un módulo auxiliar

Cargas útiles, los codificadores, Nops

- Cargas útiles consisten de código que se ejecuta remotamente
- Encoders asegurar que las cargas útiles llegan a su destino
- Nops mantener los tamaños de carga constante.

Módulos Ubicaciones

Árbol módulo primario

- Se encuentra en / opt/metasploit/msf3/modules /

Especificado por el usuario Módulo Tree

- Situado bajo ~ / / .msf4/modules
- Esta ubicación es ideal para los conjuntos de módulos privados

Carga de árboles adicionales en tiempo de ejecución

- Pasa la opción-m cuando se ejecuta msfconsole (msfconsole-m)
- Utilice el comando loadpath dentro msfconsole

Metasploit Object Model

En el Metasploit Framework, todos los módulos son clases de Ruby.

•Módulos de heredar de la clase de tipo específico
•Los tipos específicos de clase hereda de la clase del módulo Msf ::
•Hay una API común compartido entre los módulos

Las cargas útiles son ligeramente diferentes.

•Las cargas útiles son creados en tiempo de ejecución de los distintos componentes
•Encolar teatralizadores con etapas

Mixins y Plug-ins

Una derivación rápida a Ruby.

- Cada clase tiene un solo padre
- Una clase puede incluir varios módulos
- Los módulos pueden añadir nuevos métodos
- Los módulos pueden sobrecargar los métodos antiguos
- Módulos Metasploit heredar MSF :: Módulo e incluyen mixins para agregar características.

Metasploit Mixins

Mixins son, sencillamente, la razón por rocas Ruby.

- Mixins "incluir" una clase a otra
- Esto es a la vez diferente y similar a la herencia
- Mixins pueden reemplazar los métodos de una clase '

Mixins puede añadir nuevas funciones y permite a los módulos tienen diferentes "sabores".

- Protocolo específico (por ejemplo: HTTP, SMB)
- Comportamiento específico (es decir: la fuerza bruta)
- conectar () está implementado por el mixin TCP
- connect () está sobrecargado y luego a través de FTP, SMB, y otros.

Mixins puede cambiar el comportamiento.

- El escáner mixin sobrecargas run ()
- Cambios escáner run () para run_host () y run_range ()
- Se llama a estos en paralelo en función del valor HILOS
- La fuerza bruta es similar mixin

```
clase myparent
     def woof
          puts "guau!"
     final
final

clase MyClass <myparent
final

objeto = MyClass.New
object.woof () => "guau!"

================================================ ==============

módulo MyMixin
     def woof
          pone "secuestrado el método guau!"
     final
final

clase MyBetterClass <MyClass
     incluir MyMixin
final
```

Metasploit Plugins

Plugins trabajar directamente con la API.

- Ellos manipulan el marco en su conjunto
- Plugins conectar en el subsistema de eventos

- Ellos automatizar tareas específicas que sería tedioso hacerlo manualmente

Plugins sólo funcionan en la msfconsole.

- Los plugins pueden añadir nuevos comandos de consola
- Se extienden la funcionalidad Marco general