

Donar

 Ir Buscar01
Introducción

02 Requisitos

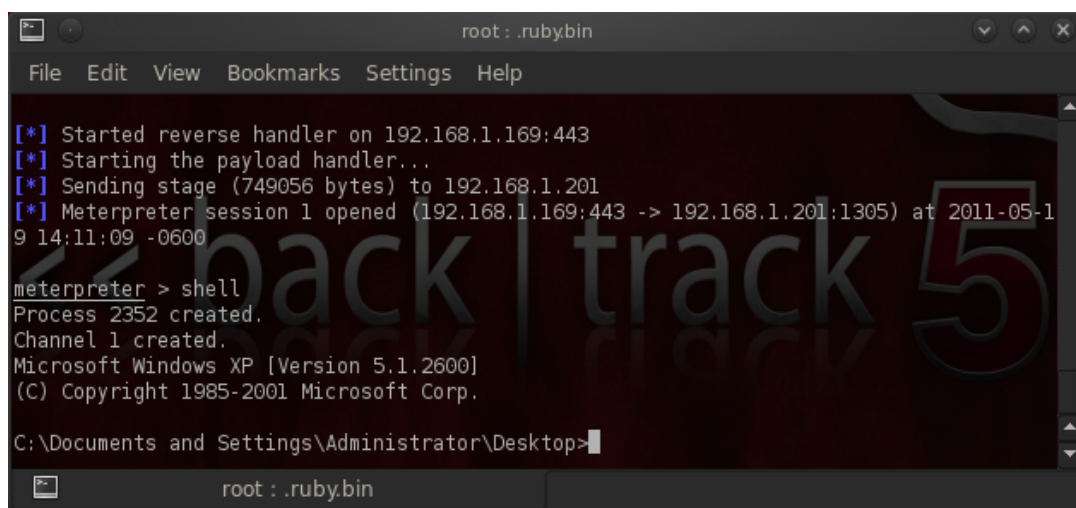
03
Fundamentos
de Metasploit04 Recopilación
de información05 Análisis de
Vulnerabilidad06 Escribir un
Fuzzer simple07 Exploit
Desarrollo08 Web App
Dev Explotar09 Los ataques
Client Side10 Explotación
MSF Mensaje11 Meterpreter
Scripting12 Acceso
mantenimiento13 MSF
extendido uso14 Metasploit
GUIs

Acerca de los

Introducción

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

-Abraham Lincoln



```
root : .rubybin
File Edit View Bookmarks Settings Help

[*] Started reverse handler on 192.168.1.169:443
[*] Starting the payload handler...
[*] Sending stage (749056 bytes) to 192.168.1.201
[*] Meterpreter session 1 opened (192.168.1.169:443 -> 192.168.1.201:1305) at 2011-05-19 14:11:09 -0600

meterpreter > shell
Process 2352 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator\Desktop>
```

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

autores

Publica Módulo
de referencia

Referencia del
módulo auxiliar

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. Cierta 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™**

Introducción

[Donar](#) | [Introducción](#) | [Materiales necesarios](#) | [Fundamentos Metasploit](#) | [Recopilación de información](#) | [análisis de vulnerabilidades](#) | [Escribir un Fuzzer simple](#) | [Exploit Desarrollo](#) | [Web App Exploit Dev](#) | [Los ataques Client Side](#) | [MSF Mensaje Explotación](#) | [Meterpreter Scripting](#) | [Acceso mantenimiento](#) | [Uso de MSF Extended](#) | [Metasploit GUIs](#) | [módulo de referencia](#) | [Sobre los autores](#)

Copyright © 2012 Offensive Security Ltd. Todos los derechos reservados.

