Metasploit Framework

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Informática Forense & GNU/Linux

Sitio Web: http://www.ReYDeS.com

e-mail: ReYDeS@gmail.com

Sábado 30 de Abril del 2016

Presentación

Alonso Eduardo Caballero Quezada es EXIN Ethical Hacking Foundation Certificate, LPI Linux Essentials Certificate, Brainbench Certified Network Security (Master), Computer Forensics (U.S.) & Linux Administration (General), IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling y Digital Forensics.

Ha sido Instructor en el OWASP LATAM Tour Lima, Perú del año 2014, y Conferencista en PERUHACK 2014. Cuenta con más de doce años de experiencia en el área y desde hace ocho años labora como Consultor e Instructor Independiente en las áreas de Hacking Ético & Informática Forense. Perteneció por muchos años al grupo internacional de Seguridad RareGaZz y al Grupo Peruano de Seguridad PeruSEC. Ha dictado cursos presenciales y virtuales en Ecuador, España, Bolivia y Perú, presentándose también constantemente en exposiciones enfocadas a Hacking Ético, Informática Forense, GNU/Linux y Software Libre.

@Alonso_ReYDeS www.facebook.com/alonsoreydes

pe.linkedin.com/in/alonsocaballeroquezada/

Metasploit Framework

Metasploit Framework (MSF) está lejos de ser sólo colección de exploits. Es un framework o estructura de trabajo completo, la cual puede ser construida y utilizada para necesidades específicas. Permite concentrar la atención en un único entorno, y no reinventar la rueda.

En la actualidad Metasploit Framework es considerado como la herramienta de auditoría libremente disponible más útil para los profesionales en seguridad.

Incluye un amplia diversidad de “exploits” de nivel comercial y un amplio entorno para el desarrollo de exploits, desde herramientas para la recopilación de información, hasta plugins para vulnerabilidades web.

En la actualidad existen dos productos comerciales basados en Metasploit Framework: Metasploit Express y Metasploit Pro. Así mismo dos versiones “Libres”. Metasploit Comunity y Metasploit Framework.

* Penetration Testing Software: http://www.rapid7.com/products/metasploit/editions-and-features.jsp
* Metasploit Editions Comparison Table: https://community.rapid7.com/docs/DOC-2287

Terminología

- **Exploit:** Medio por el cual un atacante aprovecha una falla dentro de un sistema, aplicación o servicio.
- **Payload:** Código a ejecutar en el sistema, el cual ha sido seleccionado y entregado por el Framework.
- **ShellCode:** Conjunto de instrucciones utilizados como un “Payload” o carga útil cuando ocurre la explotación.
- **Módulo:** Pieza de software el cual puede ser utilizado por Metasploit Framework.
- **Listener:** Componente dentro de Metasploit el cual espera por una conexión entrante de algún tipo.
- **Base de Datos:** Metasploit Framework incluye soporte para el sistema de bases de datos PostgreSQL.
- **Meterpreter:** Payload avanzado, ampliable dinámicamente.

Interfaces

MSFcli

MSFCli proporciona una poderosa interfaz en línea de comando para el Framework. Esto permite fácilmente añadir exploits de Metasploit dentro de cualquier Script (guiónes) los cuales pueden ser creados.

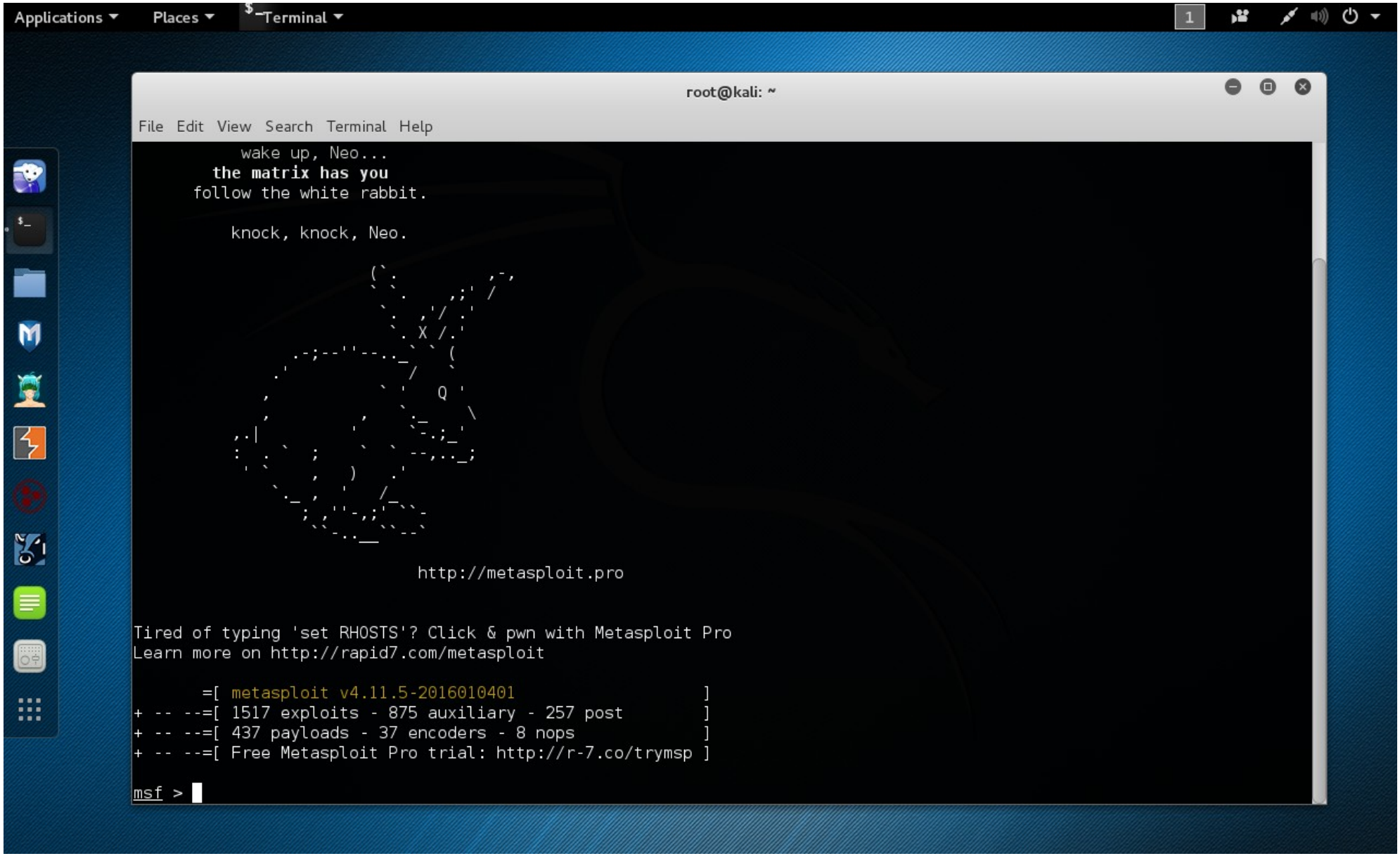
En el mes de Junio del año 2015 msfcli fue retirado. Se pueden obtener funcionalidades similares a través de “msfconsole” utilizando la opción “-x”.

MSFconsole

MSFonsole es probablemente la interfaz más popular de Metasploit Framework. Proporciona una consola centralizada “todo en uno”, lo cual permite un acceso eficiente hacia virtualmente todas las opciones disponibles en el Framework. Podría resultar intimidatorio al inicio, pero una aprendida la sintaxis de los comandos se apreciará su poder.

* Armitage: http://www.fastandeasyhacking.com/
* https://www.offensive-security.com/metasploit-unleashed/msfconsole/

Demostraciones



Cursos Virtuales

Todos los Cursos Virtuales dictados están disponibles en Video.

Curso Virtual de Hacking Ético

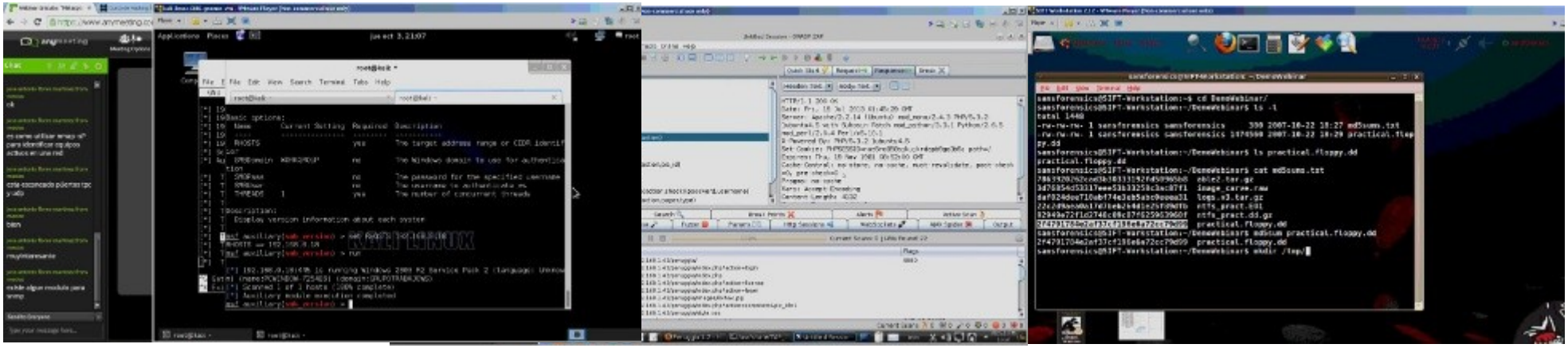
http://www.reydes.com/d/?q=Curso_de_Hacking_Etico

Curso Virtual de Hacking Aplicaciones Web

http://www.reydes.com/d/?q=Curso_de_Hacking_Aplicaciones_Web

Curso Virtual de Informática Forense

http://www.reydes.com/d/?q=Curso_de_Informatica_Forense



Más Contenidos

Videos de 30 Webinars Gratuitos sobre Hacking Ético, Hacking Aplicaciones Web e Informática Forense.

http://www.reydes.com/d/?q=videos

Diapositivas utilizadas en los Webinars Gratuitos.

http://www.reydes.com/d/?q=node/3

Artículos y documentos publicados

http://www.reydes.com/d/?q=node/2

Mi Blog sobre temas de mi interés.

http://www.reydes.com/d/?q=blog/1

¡Muchas Gracias!

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Informática Forense & GNU/Linux

Sitio Web: http://www.ReYDeS.com

e-mail: ReYDeS@gmail.com

Sábado 30 de Abril del 2016