Cómo se hizo fácil el hacking

METASPLOIT

Cuando de seguridad se trata, la revelación pública de vulnerabilidades y del código de explotación que funciona son hoy en día una cosa habitual. Vemos por qué esto puede ser tanto perjudicial como útil para asegurar nuestros sistemas. **POR KURT SEIFRIED**

El pasado mes escribí acerca de los problemas DNS de seguridad, e incluí ejemplos de cómo explotarlos antes de que la revista se imprimiera [1]. Desde entonces, un amigo y yo mismo estuvimos discutiendo cómo era realmente de explotable el problema del DNS – personalmente dije que era relativamente fácil hacerlo, pero él discrepaba, alegando que no sería nada trivial.

Los dos nos mantuvimos en nuestras trece hasta que dijo, "Si piensas que es tan fácil, escribe el código de explotación." Mi respuesta fue "¿Para qué molestarme? Alguien escribirá ese código o un módulo Metasploit dentro de unos cuantos días o semanas y lo lanzará públicamente." Y así fue.

Esto supone un interesante cambio de eventos – hace años hubiera intentado crear un exploit que funcionara o bien intercambiar un favor con alguien que supiera de un tipo que conociera a otro que hubiera explotado código. Ahora estoy dispuesto a esperar unos cuantos días o semanas hasta que alguien cree y lance públicamente código de explotación, probablemente en cualquier forma fácil de usar, como puede ser un módulo Metasploit.

A pesar de que los atacantes volverán a crear nuevos ataques y los usarán en secreto, la tendencia es a que se incrementen la revelación pública de vulnerabilidades y el código de explotación que funcione, lo cual es tanto malo como bueno.

Código de Explotación

La explotación de código es muy parecido a una palanca – es una herramienta muy útil si necesitas derribar una pared para ver las tuberías de debajo, o es una buena manera de entrar en una casa para robar.

Los códigos de explotación, especialmente los bien empaquetados, como los módulos Metasploit, son una herramienta inestimable para profesionales de la seguridad. Las usamos para evaluar la seguridad de nuestros sistemas y para generar información de manera que podamos escribir luego firmas de ataque. (Escribir una firma de ataque sin una captura de red es posible, aunque a menudo doloroso). Sin código de explotación nuestros trabajos podrían ser más difíciles, si no completamente imposibles en algunas situaciones.

Los atacantes usan código de explotación en virtualmente idénticas maneras, pero con el objetivo de entrar y comprometer a los sistemas, por ejemplo, para crear botnets u obtener acceso a información sensible.

Metasploit a Escena

La gente no sólo ha comenzado a compartir código de explotación, la calidad de este código también ha aumentado. Atrás quedan las explotaciones del pasado basadas en prueba y error y sólo para arquitecturas y sistemas específicos que a menudo fallaban al compilar si no se les arreglaban algunos errores serios. Los scripts de la shell, antaño frecuentemente llenos de fallos, utilizados para ejecutar código o comandos hostiles después de que el ataque tuviera éxito, también han evolucionado. Las infraestructuras para la

Anatomía de un Exploit

Típicamente, un exploit comprende dos elementos: el ataque en sí mismo y el programa shell. El ataque puede ser cualquier número de cosas: un underflow de entero, un desbordamiento de búfer, etc. El fin de la mayoría de estos ataques es permitir al atacante modificar los contenidos de la memoria del sistema, dejándoles controlar la ejecución del programa y, en última instancia, la ejecución de código arbitrario. A menudo a este código se le conoce como código shell, la punta de lanza que nos da acceso a un shell o acceso remoto y control del sistema en cuestión. El código de la shell es clásicamente específico del sistema operativo y de la arquitectura, y a veces tiene restringido los caracteres e instrucciones que puede usar (a causa de la presencia de problemas específicos de programas o de sistemas de seguridad, por ejemplo).

creación de exploits, de las cuales Metasploit es la opción de código abierto más conocida, han simplificado el trabajo a los desarrolladores de exploits, profesionales de la seguridad, así como a los chicos malos.

Metasploit proporciona interfaces de línea de comandos, gráficas y web con más de 300 módulos de exploit a lo largo de una extensa variedad de programas, servicios y sistemas operativos.

Además, simplifica el proceso de forma importante y lo hace mucho más repetible, lo cual es bueno nuevamente tanto para los chicos buenos como para los malos.

Instalación de Metasploit

Hay dos maneras de instalar Metasploit: descargando el archivo tar empaquetado o sacando la última versión del repositorio del código fuente Subversion del proyecto. Personalmente prefiero esta última, ya que asegura que obtengamos los últimos exploits y el código actualizado. Los archivos tar empaquetados tienden a estar al menos unas cuantas semanas desfasados.

```
[root@victim log]# ls -la /tmp/
total 24
drwxrwxrwt  3 root     root     4096 2008-08-27 14:29 .
drwxr-xr-x 21 root     root     4096 2008-08-26 21:49 ..
drwxrwxrwt  2 root     root     4096 2008-08-26 21:49 .ICE-unix
-rw-------  1 root     root     1024 2008-08-26 20:59 .rnd
srwxrwxrwx  1 postgres postgres    0 2008-08-27 14:17 .s.PGSQL.5432
-rw-------  1 postgres postgres   25 2008-08-27 14:17 .s.PGSQL.5432.lock
-rw-r--r--  1 apache   apache     0 2008-08-27 14:28 the-awstats-exploit-worked
[root@victim log]#
```

Figura 2: ... y los resultados fáciles de verificar.

Obviamente, necesitaremos el software cliente Subversion, que puede instalarse con comandos como:

```
# yum install ➥
subversion
```

(sustitúyase por el comando oportuno de su sistema administrador de paquetes). Después de instalarlo, simplemente vamos al directorio en el que deseamos instalar Metasploit – por ejemplo, nuestro directorio home – e introducimos el comando:

```
# svn checkout➥
http://metasploit.➥
com/svn/hramework3/trunk/➥
metasploit
```

Esto grabará la más reciente infraestructura Metasploit y módulos exploit, y los colocará en un directorio llamado *metasploit*.

En este punto, Metasploit no funciona si no tenemos instalado Ruby, y dependiendo de cómo queramos acceder a él – por ejemplo, a través de la interfaz web o de la interfaz gráfica de usuario – también necesitaremos un número de paquetes Ruby:

```
# yum install ruby ruby-irb➥
ruby-libs ruby-rdoc ruby-devel➥
readline ruby-gtk2➥
ruby-libglade2 rubygems
```

Una vez instalado Ruby y las dependencias restantes, necesitaremos hacer lo propio con Ruby on Rails.

El comando siguiente instalará la versión 1.2.2:

```
# gem install -v=1.2.2➥
rails
```

Seguidamente podemos ir al directorio en el que se encuentra instalado Metasploit y ejecutar la consola basada en texto (*msfconsole*), la interfaz web (*msfweb*), o la interfaz gráfica (*msfgui*). Luego, simplemente elegimos un exploit – por ejemplo, el exploit de ejecución del comando remoto AWStats 6.1 y 6.2 – e introducimos la dirección IP o un rango de hosts, y el comando que queremos ejecutar. Como podemos ver en el ejemplo de la captura de pantalla, la GUI es bastante intuitiva y los resultados fáciles de verificar (Figuras 1 y 2).

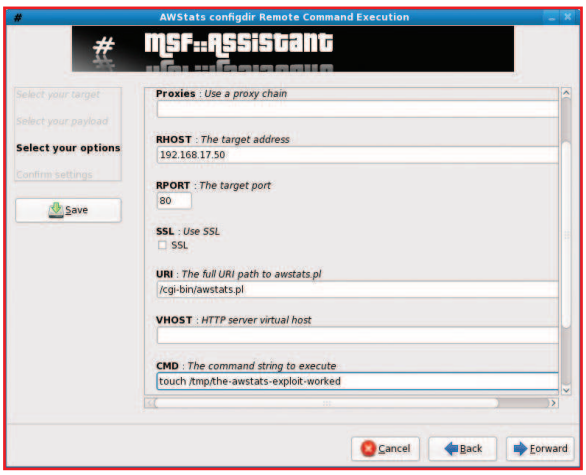

Figura 1: La GUI es bastante intuitiva...

Conclusión

Para proteger nuestros sistemas deberíamos familiarizarnos con las herramientas que se usarán contra ellos. Por ejemplo, el ataque contra AWStats se bloquea en Fedora Core 9 cuando SELinux está en modo de "cumplimiento" ("enforcing" – modo predeterminado). Metasploit no es el primer framework de explotación disponible, ni tampoco el más potente. Herramientas como *Core Impact* e *Inmunity Canvas*, las cuales incluyen exploits de actualización, también se encuentran disponibles con soporte comercial. Otros sitios, como Packet Storm y Miw0rm, poseen igualmente importantes cantidades de código de explotación disponible. La mejor defensa es un buen ataque. ■

RECURSOS

[1] "Ataques DNS" de Kurt Seifried, Linux Magazine, Edición en castellano, Nº 46.

[2] Metasploit: *http://www.metasploit.com/*

[3] Inmunity Canvas: *http://www.inmunitysec.com/products-canvas.shtml*

[4] Core Impact: *http://www.coresecurity.com/*

[5] Packetstorm: *http://packetstormsecurity.org/*

[6] Milw0rm: *http://www.milw0rm.com/*