Reto de Análisis Forense – RedIRIS

Diciembre 2003

- INFORME EJECUTIVO -

Román Medina-Heigl Hernández

-[http://www.rs-labs.com/]-

TABLA DE CONTENIDOS

1 Introducción.

El 21 de Agosto de 2002, a las 19:01:35 (CEST) un nuevo sistema ve la luz: un flamante Linux es instalado sobre un viejo Pentium 166 con 48 MB RAM. El administrador comete la imprudencia de no actualizar el sistema y habilita un servicio sin saber que éste contenía un agujero de seguridad públicamente conocido. Aproximadamente trece horas más tarde (22 Ago 08:17:24 CEST) el sistema había sido comprometido. Pero no será hasta pasada la media noche del día siguiente (23 Ago 00:21:04 CEST) cuando se produzca una nueva intrusión y comiencen las verdaderas muestras de actividad del atacante.

2 Objetivos.

El atacante –al parecer de origen rumano- pretende utilizar el sistema como plataforma para lanzar nuevos ataques. Para ello, descarga herramientas destinadas a comprometer otros sistemas de forma masiva e incluso tenemos evidencias de que llega a utilizarlas. También lanza un pequeño ataque de denegación de servicio contra algún enemigo. Busca afianzarse en la máquina y por ello instala varias puertas traseras junto a un "rootkit". Además trata de cerrar el agujero de seguridad que él mismo utilizó horas antes, para evitar nuevas intrusiones.

Se persigue también la creación de una base de operaciones para IRC. El atacante instalará un par de "IRC-bouncers" a través de los cuales se conectará a Undernet. Aprovechará por último para emplazar un bot de IRC.

3 Impacto.

Afortunadamente el compromiso fue detectado rápidamente y la máquina fue desconectada a las 15:36:30 (CEST) del 23 de Agosto de 2002. Hubo actividad en IRC y también algún pequeño intento de DoS[1] pero no tenemos indicios de que el atacante llegara a comprometer nuevas máquinas.

4 Análisis realizado.

Se ha invertido cerca de 40 horas de trabajo en la realización del presente estudio. Hemos hecho especial hincapié en el esbozo detallado de una posible cronología de los hechos ("time-line") y en tratar de encasillar cada una de las pruebas y evidencias que hemos ido obteniendo paulatinamente.

[1] DoS: "Denial of Service" (ataque de denegación de servicio).

Asimismo se ha estudiado en profundidad la causa del compromiso, esto es, la vulnerabilidad explotada, y las medidas que el administrador de la máquina podría haber adoptado para evitar la intrusión. También se ha tratado de caracterizar y localizar al atacante con un alto grado de detalle. Por último y no por ello menos importante, hemos querido dotar al estudio de un fuerte carácter didáctico por lo cual se ha hecho especial énfasis en explicar cada uno de los pasos empleados en el análisis forense del sistema comprometido.

5 Recomendaciones.

El sistema deberá ser reinstalado a partir de un medio seguro (por ejemplo, los CDs de instalación de Linux). Antes de conectar de nuevo a la red, deberemos asegurarnos de que está al día en parches de seguridad, es decir, no contiene ninguna vulnerabilidad conocida.

Otras buenas prácticas que aconsejamos seguir son:

- Deshabilitar todos los servicios innecesarios, incluído "portmap" y demás servicios RPC.
- Intentar enjaular los servicios que necesitemos realmente ("chroot").
- En caso de necesitar administración remota utilizar un servicio seguro como SSH.
- Monitorizar regularmente los registros ("logs") del sistema.
- Suscribirse a listas de distribución sobre seguridad como "Bugtraq"[2] así como a boletines de seguridad de la propia distribución Linux que estemos usando. Parchear nuestro sistema en cuanto se descubran nuevos fallos de seguridad.
- Utilizar algún sistema de verificación de ficheros basado en firmas como puede ser "Tripwire". Guardar las bases de datos de firmas en un lugar seguro, nunca en la propia máquina (preferiblemente en algún medio de sólo lectura, como un cdrom).
- Instalar un sistema de detección de intrusos (IDS) como "Snort" en el perímetro de la red.
- Aplicar parches de seguridad a nivel de núcleo del sistema, como "grsec"[3], para hacer más difícil la explotación de futuros agujeros de seguridad que puedan aparecer en un futuro.

[2] Sitio web de Bugtraq: http://www.securityfocus.com/archive/1.
[3] Grsec: http://www.grsecurity.net.