Reto de Análisis Forense de RedIris

INFORME EJECUTIVO

Reto_rediris_eje V.10. Rev. 30/Dic/2003

Motivos de la intrusión

El atacante, un "cracker" de nacionalidad rumana que utiliza el nick NeRoD, utilizó el sistema comprometido para instalar y ejecutar unos bots IRC que le permitían mantenerse permanentemente activo en distintos servidores IRC de undernet. Además, mediante este ataque añadía un nuevo ordenador a la lista de sistemas bajo su control, para lanzar nuevos ataques (incluso tendría la posibilidad de realizar ataques coordinados si está integrado en un grupo de "hackers"). De hecho, se ha detectado una tentativa de ataque lanzado desde el ordenador comprometido. Finalmente, señalar que tiene la posibilidad de utilizar el ordenador atacado como "puente" para acceder a otros ordenadores de la misma red, obtener nombres de usuario y password a partir del escaneo de la misma, etc, con el objetivo de obtener el control de nuevos sistemas.
Del análisis realizado en el sistema, no parece que la finalidad del intruso sea la de causar daños en el sistema atacado o la del robo o alteración de información. Las motivaciones, en este caso van más bien dirigidas al terreno del prestigio y reconocimiento entre los grupos de "hackers".

Análisis realizado

El análisis de ha realizado con fines principalmente didácticos, por lo que se ha decidido utilizar herramientas comunes y disponibles en cualquier sistema. Así, se ha optado por usar únicamente órdenes habituales del Sistema Operativo en cuestión (Linux) y seguir una secuencia lógica partiendo de un "desconocimiento" de las técnicas habituales de los "hackers". Así, se decidió no utilizar herramientas del estilo de *chkrootkit,* que habrían acelerado considerablemente la tarea, pero dejarían muchas "técnicas" ocultas.

El análisis se ha llevado a cabo en cuatro fases, en un orden de complejidad creciente:

1.- En una fase preliminar, se ha recopilado información básica sobre el ordenador, interfaces de red, números IP, tipo y versión del Sistema Operativo, servicios instalados, etc, con el objetivo de situar un escenario de partida. Una parte importarte de esta fase consiste en determinar qué servicios se encontraban activos, qué versiones de los "daemons" se estaban utilizando para dar esos servicios, y obtener una lista de las vulnerabilidades para esos servicios. A partir de las vulnerabilidades conocidas, se puede realizar una evaluación de los riesgos que se estaban asumiendo para cada uno de esos servicios y establecer la vía de entrada más probable.

2.- En una segunda fase se ha procedido a estudiar los ficheros de "log", el primer paso que debe darse para tratar de hacerse una idea de cómo estaba funcionando el sistema y qué puede haber ocurrido (aunque si el intruso es hábil, posiblemente quede poca información que recopilar). En este caso, el estudio sí ha sido bastante fructífero, llegándose a determinar la IP que se utilizó para lanzar el ataque (concretamente una IP correspondiente a Perú), y confirmando la vía de entrada que se consideró más probable en la Fase 1. También se detectó que los sistemas de "log" dejaron de funcionar poco después de uno de los intentos de ataque, lo que prácticamente confirma que el sistema ha sido comprometido.
Dentro de esta misma fase, se realizó un estudio detallado de la configuración del sistema, teniendo en cuenta fechas y horas para tratar de estimar qué modificaciones se habían realizado. Una breve investigación reveló que se había descargado e instalado un "rootkit".

3.- Después de la inspección a nivel básico, y tras confirmar que se había instalado un "rootkit", la tercera fase se dedicó a estudiar en profundidad el contenido del mismo, y su proceso de instalación, para determinar el nivel de compromiso del sistema. En esta fase ya son necesarios conocimientos avanzados (hay que analizar scripts de instalación, conocer en profundidad la estructura del sistema operativo, etc), aunque se puede llevar a cabo con órdenes tan simples como *grep*, *find*, *more*, *vi*, etc..
Tras este estudio, se pueden determinar qué ficheros del sistema han sido sustituidos o modificados, y qué nuevo software se ha instalado desde el "rootkit". No obstante, aún falta información de las acciones que el intruso ha realizado en el sistema al margen del "rootkit".

4.- En la cuarta fase, se procede a un estudio de la partición de "swap", que debe contener parte de la memoria del sistema en las horas en las que estuvo conectado el intruso. La información que pueda obtenerse, como siempre, es parcial, pero puede revelar datos nuevos. Para el estudio de la partición de "swap" pueden utilizarse editores hexadecimales, pero, siguiendo el carácter didáctico del estudio, se puede usar el editor *vi* para ir buscando cadenas. El estudio de la partición de "swap" permitió conocer nuevos aspectos, como la existencia de la instalación de bots IRC, nuevas direcciones IP, o la coincidencia entre el nombre del "rootkit" (nerod) y el nick usado por el atacante en los canales IRC (NeRoD). La aparición de comentarios en rumano en el "rootkit", unido a conexiones desde IPs de Rumanía para acceder a los bots IRC hacen pensar que el intruso era el "autor" del "rootkit" (realmente es una modificación de otros rootkits), y que procedía de Rumanía. Puesto que el ataque inicial provino de un ordenador peruano, posiblemente el intruso utilizó ese ordenador, también bajo su control, para lanzar el ataque ocultando su verdadero origen.

En este caso, el análisis se ha dejado en este punto, aunque en general debe considerarse una quinta fase. La siguiente fase, esta ya mucho más laboriosa, consistiría en revisar en detalle las particiones en busca de información que quedara de ficheros borrados (por ejemplo, los ficheros que descargó el intruso y que al descomprimir dieron lugar a las instalaciones de los bots IRC), pero en este caso no se ha considerado necesaria.

Las direcciones IP implicadas, que se han ido obteniendo en las diferentes fases se han rastreado usando la utilidad whois que proporcionan las entidades NIC. Concretamente, se partió de la proporcionada por http://www.nic.com

Recomendaciones

Particularizando al caso en estudio las recomendaciones generales de seguridad, es conveniente hacer hincapié en lo siguiente:

- Nunca deben mantenerse servicios que no se estén utilizando, aunque se esté detrás de un firewall. En el ordenador atacado, estaban activas las nfs (que no se utilizan) y el sendmail. Sino son imprescindibles, estos servicios deben desactivarse siempre.
- Aunque se esté detrás de un firewall, deben tenerse siempre configurados los TCP-WRAPPERS. En este caso, habría sido conveniente que se filtrara el servicio sshd a través de tcp-wrappers.
- Siempre deben mantenerse actualizados los servicios que se vayan a dar. En este caso, estaban las versiones originales de la instalación del sistema, que suelen tener vulnerabilidades. Esto debe tenerse especialmente en cuenta si se va a dar un servicio público como es el caso de un FTP anonymous para internet.
- En el caso de dar un servicio público, aparte de tenerlo actualizado e instalar los últimos parches, no debe activarse hasta que esté completamente configurado. En el caso del ordenador atacado, el servicio FTP anonymous no estaba configurado del todo (se tenía la configuración por defecto tras instalar el paquete en el sistema).
- Siempre que se esté conectado de manera directa a Internet, debe hacerse a través de un firewall correctamente configurado.
- La seguridad no debe centrarse únicamente en el ordenador que hace de firewall. Los ordenadores de la red interna que tengan puertos de entrada abiertos a través del mismo deben mantener ese mismo nivel de seguridad. En este caso particular, el ordenador atacado tenía una IP perteneciente a una intranet, y ha sido comprometido. Una vez que el intruso está dentro de la misma, tiene acceso fácil a todo lo que circula por la red, y posiblemente se encuentre menos problemas para entrar a los ordenadores "más seguros"
- Debe usarse siempre ssh para abrir sesiones remotas, aunque se esté dentro de una intranet. Los intrusos suelen instalar "sniffers" en cuanto logran comprometer un sistema, con lo que accederán rápidamente a los nombres de usuario y passwords que circulen sin encriptar por la intranet.
- Deben revisarse con frecuencia los ficheros de log para dilatar lo menos posible el intervalo de tiempo entre la observación de "cosas extrañas" y el proceso de tomar acciones para detectar posibles intrusos.
- Debe disponerse de herramientas que detecten la modificación de los archivos básicos del sistema. Nos facilitará la detección de la instalación de cualquier rootkit o troyano. Un método sencillo es mantener una pequeña base de datos de las sumas MD5 de esos archivos (por supuesto, mantenida en lugar seguro...).

El informe técnico proporciona los detalles del análisis forense realizado para obtener la información aquí referenciada.