Recuperación ante ataques

IRIS-CERT <certrediris.es>

14 de Noviembre de 2000

Resumen

Otro documento, mezcla de varios para contar con toda la información en conjunto sobre como buscar evidencias de que se ha sufrido un ataque.

Índice General

1 Introducción

En anteriores grupos de trabajo se han ido tratando diversos aspectos relacionados con la gestión de incidentes de seguridad[1] y este suele ser uno de los puntos más comentados en casi todos las reuniones. Para estas jornadas hemos preparado un pequeño documento

[1] Búsqueda de puntos de contacto, GGTT Oviedo 1999

donde se comentan los pasos a seguir para que un administrador de una máquina atacada pueda recopilar la información del ataque para su posterior análisis.

Lo primero hay que hay que indicar es que los procedimientos que se mencionan a continuación están pensados para situaciones en las que se requiere que los equipos atacados vuelvan a funcionar adecuadamente. En caso de que se considere más oportuno una investigación legal del incidente lo más conveniente sería acudir a los servicios jurídicos de la organización y contactar con las autoridades.

Por otro lado se hará una breve descripción del conjunto de utilidades "Colonel Toolkit" que se puede emplear en algunos casos para intentar averiguar que es lo que ha hecho un atacante en un equipo.

2 Un incidente de seguridad típico

Gran parte de los ataques que acaban con el acceso por parte del atacante a un equipo con permisos de root, suelen seguir el siguiente patrón de comportamiento:

1. El atacante realiza un escaneo buscando equipos vulnerables que estén ejecutando un servidor con algún fallo de seguridad conocido y que se ha comentado ampliamente en listas de seguridad, por ejemplo los fallos de desbordamiento de buffer en el servidor de FTP wuftp o del proceso rpc.statd.

2. El atacante emplea un exploit contra el equipo, consiguendo instalar una puerta de acceso en el sistema, muchas veces el exploit genera directamente un interprete de comandos con privilegios de root, o añade una linea en el /etc/inetd.conf para lanzar una shell en un puerto dado.

3. El atacante instala o compila un "rootkit", conjunto de programas de nombre y comportamiento similar al de comandos del sistema operativo, que sin embargo no muestran información sobre determinados estados del sistema[2]

4. El atacante instalará y/o compilara algunas herramientas de ataque, para escanear y atacar otros equipos y redes empleando la maquina recién atacada como puente.

Esta situación se produce hasta que alguien detecta un comportamiento anómalo en el equipo, algunas veces esta detección se realiza por el propio administrador del equipo debido a una carga de procesamiento anormal, accesos extraños, etc. pero en la mayoría de los caso la detección del equipo atacado se produce desde el exterior: Llega un correo a la organización indicando que el equipo en cuestión esta escaneando o ha sido empleado para atacar otros sistemas y al contactar con el administrador del equipo se descubre que la maquina ha sido a su vez atacada.

Sin entrar en el grave problema que es la ausencia de administración y actualización de estos equipo, los pasos a seguir suelen ser también siempre los mismos y es lo que se conoce como "recuperación ante un incidentes de seguridad.

3 Recuperación ante incidentes de seguridad

Una vez que el administrador ha sido apercibido del problema los pasos que se deben hacer son:

1. Desconexión de la red o apagado del equipo, para evitar que el atacante pueda seguir accediendo al equipo, evitando que recupera la información que haya podido obtener sobre otras redes o intente borrar sus huellas, o inutilice (borrado o formateo) el equipo atacado.

[2]Así la versión modificada del comando "ls" no listará los ficheros creados por el intruso, "ps" no mostrara determinados procesos o "netstat" no mostrara las conexiones del atacante

2. Realizar una copia de seguridad a bajo nivel. Siempre que sea posible es conveniente realizar una copia de los datos del equipo a bajo nivel, de forma que se tenga la información completa del estado del sistema cuando se detecto el ataque. Si es posible el análisis posterior de los datos se debería realizar sobre la copia (con el equipo apagado/desconectado).

3. Averiguar, examinando los datos disponibles toda la información posible sobre el ataque: vulnerabilidad empleada por el atacante, logs que muestren los ataques, escaneos y conexiones del atacante, programas instalados, logs y datos que las herramientas que el atacante ha instalado, etc. Estos datos deben ser después analizados para poder avisar a otros equipos que se han podido ver involucrados.

4. Proceder a restaurar el equipo. Volver a configurar el equipo, reinstalando el Sistema Operativo si es preciso, y aplicando los parches y configuraciones adecuadas para evitar que el ataque se vuelva a producir. En caso de existan cuentas de usuarios en el equipo es conveniente que se avise a todos los usuarios y que estos cambien sus cuentas, ya que el atacante puede haberse copiado el fichero de claves y proceder después en su equipo a buscar claves débiles para volver a entrar.

5. Avisar a los responsables de los equipos atacados o fuente del ataque, así mismo notificar toda la información a los responsables de la organización (servicio de informática, centro de calculo, etc.) para que ellos se pongan en contacto. En la actualidad los ataques son "aleatorios" ya que los ataques se producen buscando equipos que presenten una determinada vulnerabilidad, por lo tanto el atacante puede haber conseguido entrar en otros equipos situados en la misma red.

Veamos con más detenimiento algunos de estos pasos, teniendo en cuanta que se debería documentar cada una de las actuaciones que se van realizandoen el equipo de forma que se pueda averiguar que comandos se han ejecutado para localizar los ficheros, donde se encontraban, etc.

4 Copia de los datos

Aunque existan copias de seguridad del equipo, es conveniente hacer una copia con la información que hay en el sistema cuando se detecta el ataque. Dependiendo de la situación puede ser conveniente incluso hacer una "copia" de los procesos que se están ejecutando en ese momento en el equipo, espacio de intercambio (swap) conexiones activas, etc, sin embargo normalmente basta con realizar una copia, a ser posible a bajo nivel, de los datos del sistema.

En equipos Unix se puede realizar una copia de las particiones del sistema de ficheros, empleando el comando dd, y volvar los contenidos a otra partición o fichero,

sin embargo es preferible volver los contenidos a otro equipo empleando por ejemplo el programa Netcat[3].

Lo más conveniente es arrancar el equipo desde un CDROM o cinta de instalación y realizar la copia en modo monousuario, de forma que no se empleen los programas que están instalados en el equipo. Algunos ejemplos de esta copia serían:

```
dd if=/dev/sda4 of = - | nc equipo remoto -p 100
```

y en el equipo remoto hacer:

```
nc -s -p 1000 > sda4
```

O bien enganchar los discos a un equipo y realizar la copia a bajo nivel, empleando discos duros de iguales características (mismo modelo) y haciendo de nuevo una copia a bajo nivel con dd.

```
dd if=/dev/sda of=/dev/sdb
```

NT no dispone de un procedimiento de backup a bajo nivel con las herramientas del sistema, aunque se puede emplear el procedimiento empleado para sistemas Unix, arrancar el equipo desde un disco de rescate o instalación de Linux/Unix y proceder a realizar la copia de los dispositivos a bajo nivel.

En cualquier caso es conveniente realizar estas copias a bajo nivel para poder restaurar los datos en caso de que ocurra algún problema al analizar los ficheros, además esto permitirá el análisis de los ficheros, buscando las fechas de modificación de ficheros.

5 Análisis de la intrusión

La primera acción que hay que realizar es comprobar todos los programas y ficheros de configuración instalados en el equipo.

En Muchos ataques lo primero que hace el atacante es modificar los programas y herramientas del sistema para ocultar su acceso, además suelen modificar los ficheros de configuración para crear nuevos usuarios , permitir accesos desde determinadas máquinas, etc, de forma que puedan acceder de una forma más cómoda con posteridad al equipo.

[3] http://dondeesta

Dado que los atacantes pueden modificar también los programas que vamos a comentar a continuación es conveniente que no se empleen los programas instalados en el propio equipo atacado, sino versiones que se tengan compiladas estáticamente y se acceda a ellas, El motivo de emplear ficheros compilados estáticamente es debido a que no emplean llamadas a las librerías del sistema, que pueden también ser modificadas por los atacantes. Por esa misma razón no es conveniente que se emplee el sistema operativo de la máquina atacada, ya que hasta el propio sistema operativo puede ser modificado mediante módulos en varios sistemas Unix, para ocultar los procesos y ficheros a determinados comandos.

En un caso ideal, el administrador del sistema debería disponer de una base de datos de integridad en un dispositivo de almacenamiento externo al equipo, para poder comprobar los ficheros empleando productos como Tripwire o un sistema antivirus en Windows, para más información sobre el tripwire, consultar las Recomendaciones de seguridad[4]

Aunque no se disponga de esta Tripwire se pueden emplear otras técnicas para verificar la integridad de los ficheros, como:

- Comparar los binarios con los existentes con los de la instalación original (cuando no están empaquetados) o con lo que hay en otro equipo con la misma revisión del sistema operativo y parches, empleando el comando "cmp". Algunos vendedores mantienen una lista de hash MD5 de los programas binarios que distribuyen, se puede emplear el comando md5sum[5] para comprobar si la huella de los ficheros corresponde con la información del fabricante.

- Muchos sistemas Operativos disponen de un sistema de verificación de los paquetes instalados, la base de datos se mantiene en el propio equipo (por lo que el atacante puede modificarla) pero de todas maneras puede ser empleada muchas veces para comprobar que ficheros se han modificado. Para algunos sistemas Operativos el comando sería:

  RedHat Linux y otros linux basados en rpm : "rpm -Va"

  Debian falta por ver.

  Solaris y otros Unix con el comando pkgchk : "pkgchk -v"

  Hay que tener en cuenta que es habitual que algunos ficheros cambien de permisos o de contenido, por ejemplo al añadir usuarios al fichero de password, algunas instalaciones cambian los formatos, etc. Sin embargo no suele ser habitual que el comando "/bin/ls" sea modificado.

- Por ultimo caso se puede examinar los ficheros "sospechosos" y buscar cadenas que delaten que se trata de un troyano, aunque este método no suele dar buenos resultados si no se conoce los ficheros originales.

[4] http://www.rediris.es/cert/doc/docurediris/recomendaciones/
[5] ftp://ftp.rediris.es/mirror/dfncert/tools/crypt/md5sum/

Es conveniente examinar los ficheros de configuración y ficheros en cuantas de usuarios:

- /etc/passwd y /etc/shadow
- /etc/inetd.conf
- comprobar que no existen ficheros ".rhosts, .shosts, etc." que permitan accesos no deseados desde el exterior no deseados.
- hosts.allow y hosts.deny
- Ficheros con suid de root o de administrador nuevos, que puedan permitir a un usuario acceder rápidamente a root[6] Se puede emplear el siguiente comando para listar los ficheros setuid/guid:

```
find / \( -perm 0040000 -o perm 0020000 \) -type f -print
```

- Buscar ficheros y directorios que empiecen por punto, pero que el contenido no sea el habitual. Los ficheros que empiezan por punto no suelen aparecer con el comando ls (salvo que se indique la opción "-l") y se suelen emplear para almacenar la configuración de los programas en el directorio raíz de cada usuario. Algunas veces los atacantes instalan los programas en un directorio home ocultándolo.
- Buscar directorios y ficheros con caracteres de control y/o espacios: Igual que antes para ocultar la información, se crean directorios espacios o con nombre el carácter de espacio, o " .." para así ocultarlos ficheros.
- Buscar ficheros ASCII y ficheros en directorios como "/dev/", "/devices", etc. empleados muchas veces por los programas instalados por los atacantes para instalar ahí los programas, logs de las herramientas de ataque, etc.

Hay que examinar también los ficheros de logs, ya que aunque los atacantes suelen borrarlos otras veces el borrado no es completo, por lo quedan rastros de la intrusión, es conveniente tener los logs de todos los equipos centralizados, empleando el syslog[7].

La información de los ficheros de logs dependerá de como este configurado el syslog de cada equipo y de los rastros que haya borrado el atacante, se debe buscar información en:

[6]Por ejemplo, el comando vi con setuid de root, podría permitir la edición de ficheros, pero además al salir a un shell con ":!" este se ejecutaría como root.

[7]consultar las recomendaciones de seguridad

- utmp, utmpx: Información sobre los usuarios que están conectados en un momento dado en un equipo, es un fichero binario, aunque se puede emplear el comando who para analizarlos. El fichero utmpx aparece en Solaris y otros Unix. Muchas veces los programas de rotación de logs dejan una copia de estos ficheros con extensión ".1" o ".bak".

- wtmp y wtmpx: Información sobre los accesos con éxito al equipo, usuario que se conecta, protocolo que emplea, maquina origen de la conexión, etc. se puede emplear el comando "last" para examinarlo.

- messages, situado en /var/log o en /var/adm. contiene información diversa, dependiendo como se ha indicado antes de la configuración del syslog.

- secure: En muchas distribuciones Linux el fichero /var/log/secure almacena todos los eventos de seguridad, conexiones realizadas al equipo, cambios de usuario (su, etc.). Buscar conexiones a servicios poco frecuentes, direcciones IP de conexión poco habituales y todo lo que se sale de lo habitual[8]

- xferlog: Empleado por algunos servidores de ftp para registrar las transferencias de ficheros

- ficheros del servidor WWW: En los casos en los que el atacante ha realizado primero un escaneo de vulnerabilidades en el servidor WWW aparecen intentos de conexión a cgi que no están instalados.

- ficheros de historia ".bash_history", o similar en las cuentas del administrador y usuarios que se cree que han sido empleadas por el atacante.

Una vez que se disponne de todos los ficheros e información de los ficheros de logs es conveniente analizarla para intentar determinar el origen del ataque, averiguar como pudieron entrar en el equipo, si han tenido acceso a otros equipos, etc. Es conveniente empaquetar todos los ficheros, haciendo un "tar" de todos los ficheros y enviarlo con formulario de notificación de incidentes[9][10]

6 Reinstalación del equipo

Una vez que se ha determinado las causas del ataque se debe proceder a eliminar los rastros del ataque y configurar el equipo para que no se vuelvan a producir estos ataques. Si la versión del sistema operativo es algo antigua es un buen momento para instalar una versión mas actualizada del equipo. Igualmente si se disponen de copias de seguridad anteriores

[8] Lo que implica que el administrador debería observar los logs de su equipo habitualmente ;-)

[9] http://www.rediris.es/cert/servicios/iris-cert/incidentes/formulario.txt

[10] En caso de que los ficheros muy grandes se puede emplear el servidor de ftp anónimo de RedIRIS para dejar ahí los ficheros

al ataque se puede restaurar las copias (aunque convendría comprobar si los ficheros de la copia de seguridad no han sido modificados). o proceder a reinstalar solamente los ficheros o paquetes modificados.

Una vez que se tiene el sistema operativo "limpio" proceder a instalar los parches de seguridad que hayan salido para esta versión del equipo, eliminar los servicios de red que no sean precisos, etc. Existen diversas guias de configuración en este sentido, una de ellas las recomendaciones de seguridad[11] que hemos comentado anteriormente.

7 Notificación del ataque

Muchas veces los equipos atacados son empleados para lanzar ataques a otros sistemas, por lo que no necesariamente el equipo origen de un ataque es "culpable", muchas veces este equipo ha sido a su vez atacado y si se avisa al administrador se puede conseguir que este también corrija los problemas de seguridad que hay en este equipo.

Los atacantes muchas veces han realizado inicialmente un barrido buscando equipos vulnerables, por lo que una notificación a los administradores de la red en la organización del ataque puede ayudar a descubrir problemas de seguridad a nivel global. Este es uno de los motivos por los cuales desde RedIRIS se solicita que se envié notificación de todos los incidentes de seguridad "sufridos" por equipos de las organizaciones afiliadas, de forma que se pueda tener una visión global de los ataques que se están produciendo.

El procedimiento general de actuación de IRIS-CERT es intentar contactar con los responsables de las organizaciones origen del ataque, para avisarles de que hay un equipo que ha podido ser atacado. Sin embargo si el correo nos llega como copia (CC) procesamos el incidente para fines estadísticos, aunque no avisamos individualmente a la organización atacada.

8 Referencias y programas de utilidad

Comentario: Esta puesto con una macro que habrá que redefinir en la plantilla de documentación .

A. Documentación de seguridad

- Recomendaciones de seguridad de RedIRIS
- Documentación del CERT/CC (en Ingles)
- Libro en Castellano de Seguridad en Redes
- Ultima versión de este documento

B. Herramientas

[11] http://www.rediris.es/cert/doc/docrediris/recomendaciones/

- Lsof, para ver analizar que ficheros emplea un proceso
- Tripwire Existen nuevas versiones con una licencia mas restrictiva en la Pagina Oficial[12]
- Colonel's Toolkit herramienta realizada por Dan Farner y Wietse venema para el analisis de ataques.

9 Versiones y colaboraciones

Version inicial de este documento.

[12] http://www.tripwire.org