Incidentes de seguridad en equipos Linux

Francisco Jesús Monserrat Coll

Centro de Comunicaciones del CSIC RedIRIS

francisco.monserrat@rediris.es

A pesar de la seguridad que pueden ofrecer los sistemas operativos Unix y Linux, sigue aumentando significativamente el número de equipos con estos sistemas operativos que son atacados con éxito de forma remota, consiguiendo el atacante acceder como administrador al equipo.

Esta situación se ha visto agravada esta año con la reaparición de los programas gusano para equipos Unix, que consiguen acceso automáticamente a los equipos vulnerables, dejando algunas veces puertas abiertas para posteriores accesos.

1. Introducción

Con el aumento de popularidad de los sistemas Unix para plataformas Intel, y sobre todo de Linux en sus distintas distribuciones, el número de incidentes de seguridad en los que son atacados este tipo de sistemas ha aumentado considerablemente en los ultimos tiempos.[1]

En la mayoría de las ocasiones los atacantes no realizan un ataque diriguido hacia un servidor concreto, sino que van buscando equipos vulnerables ante determinado conjunto, limitado, de vulnerabilidades hasta que encuentran un equipo vulnerable, que es atacado.

Una vez que el atacante ha obtenido acceso al sistema suele instalar y modificar varios ficheros del equipo para ocultar su presencia. Muchas veces la forma más segura de

solucionar el problema es reinstalar el sistema operativo y datos desde una copia de seguridad anterior a la fecha en la que se produjo el ataque.

Este año han aparecido diversos programas y scripts de ataque que combinados formaban un gusano, es decir un programa que buscaba y atacaba automáticamente otros equipos replicándose sin requerir ninguna interacción con el usuario.

Así a finales del año pasado y principio de este año aparecerieron diversos Gusanos, Ramen (http://www.cert.org/incident_notes/IN-2001-01.html)o Li0n (http://www.cert.org/incident_notes/IN-2001-03.html), para equipos Linux y sadmin/IIS (http://www.cert.org/advisories/CA-2001-11.html) que infectaba a equipos Solaris y atacaba simultaneamente servidores IIS de Microsoft.

Estos gusanos empleaban vulnerabilidades conocidas y solucionadas bastante antes de la aparición del gusano, pero al no haber sido actualizado el equipo víctima se producía un ataque exitoso. Una de las ventajas de los gusanos es que es posible analizar cuales son las acciones que ejecutan en el sistema, por lo que si no ha habido accesos posteriores al equipo y se conoce exactamente qué gusano ha sido el causante del ataque es posible solucionar el problema con más rapidez que en el caso de un ataque “manual”.

Dado que estos gusanos son un caso específico de los incidentes de seguridad, se tratarán indistintamente al resto de accesos no autorizados a los equipos.

Hay que indicar que los procedimientos mencionados a continuación están pensados para situaciones en las que se requiere que los equipos atacados vuelvan a funcionar rápidamente y en los que no ha habido un perjuicio serio.

En caso de que sea más conveniente una investigación judicial del ataque lo más conveniente sería acudir a los servicios jurídicos de la organización y contactar con las autoridades, ya que la manipulación del sistema pueda invalidar las posibles pruebas existentes en el 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 Administrador, suelen seguir el siguiente patrón de comportamiento:

1. El atacante realiza un barrido de puertos (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 FTPwuftp, el servidor bind de DNS o en el proceso **rpc.statd**.

Estos fallos de seguridad son anunciados en diversas listas de seguridad de proposito general, como Bugtraq (http://securityfocus.com/archive/1)

La mayoría de los vendedores de distribuciones Linux disponen de listas de anuncios, donde indican las actualizaciones por motivos de seguridad, de los programas que componen su distribución.

En algunas listas de seguridad, aparecen incluso programas que demuestran esta vulnerabilidad y que pueden ser empleados por los atacantes, estos programas se suelen denominar “exploits”.

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 fichero `/etc/inetd.conf` para lanzar una shell en un puerto dado. El método puede variar, aunque el objetivo del ataque suele ser siempre el mismo, obtener un acceso a una sesión interactiva o “shell remoto” en el equipo desde el cual proseguir el ataque.
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]

   Estos rootkit han ido evolucionando, siendo cada vez más complejos. Existen módulos del kernel que permiten ocultar diversos procesos, de forma que el atacante pueda ocultar su acceso sin modificar los binarios instalados en el equipo.

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

Esta situación se reproduce 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, [3] 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, en lineas generales los pasos a seguir serian:

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

   Dado que el apagado del equipo pude provocar la perdida de información sobre el ataque (procesos que se están ejecutando, sesiones abiertas, etc.) muchas veces es preferible el filtrado completo/desconexión del equipo de la red, para así proceder al análisis de estos datos.

   No sólo esto, el sistema puede haber sido modificado para que un apagado no esperado (o una desconexión de la red) borre todo el sistema de forma completa

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).

   La copia debe hacerse siempre que sea posible empleando binarios compilados estáticamente en otro equipo “fiable”, para evitar que se empleen programas modificados por el atacante.

   Estos datos se pueden enviar a los responsables de seguridad de la organización para que procedan a su análisis si el administrador no puede realizarlos.

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 existir 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.)

   En la actualidad los ataques son “aleatorios” ya que éstos 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.

   Suele ser conveniente además contactar con los responsables de la red desde donde se produjo el ataque, ya que muchas veces se trata de equipos “trampolín”, si estos equipos son “limpiados” se consigue que la red sea “un equipo” más segura.

4. Ejemplo de actuación

Veamos con más detenimiento algunos de estos pasos, teniendo en cuanta que se debería documentar cada una de las actuaciones que se van realizando en el equipo de forma que se pueda averiguar que comandos se han ejecutado para localizar los ficheros, donde se encontraban, etc.[4]

4.1. 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, [5] 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

Lo más conveniente es arrancar el equipo desde un disquete de rescate, 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. Un ejemplo de esta copía sería:

```
victima# dd if=/dev/particion of = - | gzip -9 | nc equipo remoto -
p 100
```

y en el equipo remoto hacer:

```
analisis$ nc -s -p 1000 > particion.dd.gz
```

Esta acción habría que repetirla con cada una de las particiones del equipo atacado, incluyendo la partición de SWAP.

Otra posibilidad es conectar 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, aunque así tenemos que apagar el equipo.

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

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 éstos.

4.2. 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 nuchos 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 posterioridad al equipo.

En caso de que el análisis se realize en el mismo disco hay que tener en cuenta que el atacante ha podido modificar algunos de los binarios y librerías del sistema, por lo que conviene emplear, si es posible, comandos compilados estaticamente en otro equipo, o montar / copiar los comandos desde una máquina de confianza, para evitar que los programas modificados por el atacante nos oculten la información del equipo.

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, AIDE, VipperDB, etc. que realizan una firma digital de los ficheros instalados en los equipos.

Aunque no se disponga de alguna de estas herramientas 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 (ftp://ftp.rediris.es/mirror/dfncert/tools/crypt/md5sum/) 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** por ejemplo:

```
 victima$ rpm -Va | grep bin
SM5....T  /bin/ps
S.5....T  /usr/sbin/tcpd
S.5....T  /bin/netstat
S.5....T  /sbin/ifconfig
```

  - *Debian* El formato de paquetes empleado en Debian también incluye dentro de los todos los paquetes la información de las huellas MD5 de los ficheros. El comando **debsums -l -s** permite comprobar la integridad de los paquetes y ver que ficheros se han modificado.
  - *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. [6]

  La comprobación de la base de datos local no es del todo fiable, ya que el atacante ha podido modificarla tras la intrusión, por lo que es conveniente mantener una copia de

esta base de datos en un sistema aislado, aunque muchas veces no existe esta copia y se debe recurrir a la base de datos del sistema.

- 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.

El empleo de scripts de comprobación de integridad automáticos, que cada cierto tiempo comprueben que los ficheros no han sido modificados, ya sea empleando el sistema de gestión de paquetes o algún programa de los comentados antes, permite muchas veces detectar cuando se ha producido un ataque, Esto sucedió hace poco en un servidor de desarrollo del proyecto Apache [7] Es conveniente examinar los ficheros de configuración y ficheros en cuantas de usuarios:

- `/etc/passwd`y `/etc/shadow`
- `/etc/inetd.conf`
- Programas del arranque `rcX.d`
- Procesos ejecutados en el **crontab** del administrador.
- 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[8] Se puede emplear el siguiente comando para listar los ficheros setuid/guid:

```
victima # 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 ocultando los programas en directorios que comienzan con punto.
- 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 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.

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:

- `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 frecuentes y todo lo que se sale de lo habitual\footnote{Lo que implica que el administrador debería observar los logs de su equipo habitualmente ;-)}
- 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.

Muchas veces aunque los atacantes suelen borrar los ficheros de logs, es posible emplear el Coroner's Toolkit, mencionado en la bibiliografía para recuperar la información contenida en el espacio ocupado por los ficheros borrados y después análizar los resultados.

4.3. Análisis de los datos

Cuando se produce un incidente de seguridad en un equipo es siempre conveniente realizar un análisis del equipo o equipos atacados, siguiendo los pasos que se han comentado anteriormente, para así intentar averiguar desde donde se produjo el ataque, que vulnerabilidad empleo para acceder al equipo, que acciones realizó en el equipo, nivel de destreza del atacante, etc.

De esta forma se debe intentar determinar los motivos por los que el ataque tuvo exito, de forma que se puedan tomar las medidas oportunas para que no se vulva a producir

4.4. 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 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.

4.5. 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 los grupos de seguridad de diversos organismos, se solicita que se envié notificación de todos los incidentes de seguridad “sufridos” por los equipos, de forma que se pueda tener una visión global de los ataques que se están produciendo.

El procedimiento de actuación, en general, de los grupos de seguridad es intentar contactar con los responsables de las organizaciones origen del ataque, para avisarles de que hay un equipo que ha podido ser atacado, de esta forma se intenta evitar que existan equipos “trampolin” empleados para atacar impunemente otros equipos.

5. Conclusiones

En la actualidad la mayoria de los incidentes de seguridad reportados a IRIS-CERT en los que hay equipos Unix involucrados, no tienen como fin la manipulación o acceso a la información contenida en estos sistemas, sino que son escogidos aleatoriamente, sin embargo es posible que en el futuro los ataques sean más diriguidos hacia intereses concretos, aunque siempre usando equipos vulnerables como equipos "trampolin" desde los cuales atacar a estos sistemas.

Gran parte de los ataques son detectados debidos a las acciones que realizan los atacantes desde los equipos “víctima”, al buscar nuevos equipos vulnerables.

Por lo general es posible averiguar con bastante exactitud cómo se produjo el ataque y las acciones que realizó el atacante en el equipo, aunque muchas veces el coste en tiempo que requiere el análisis del equipo hacen que los sistemas sean reinstalados sin averiguar que sucedió normalmente.

Los equipos atacados suelen ser sistemas mal administrados donde hay funcionando servicios que no son necesarios y que están instalados con la configuración por defecto del equipo. Los responsables de estos equipos no suelen actualizar los paquetes instalados en los equipos, lo que provoca que sean vulnerables a equipos desde el exterior.

Muchas veces los equipos son reinstalados con versiones vulnerables del sistema operativo, empleando una copia en CDROM, y no son actualizados convenientes, permitiendo que los atacantes pueden volver a entrar en el equipo en poco tiempo,.

6. Herramientas

La lista de programas que se suelen utilizar a la hora de análizar un incidente de seguridad es muy extensa y depende de cada situación, muchas veces son comandos típicos del sistema operativo, por lo que el comentario que aparece es mínimo, y solo

hay que buscar en las páginas del manual para ver todas las opciones que pueden realizar.

- *grep* Comando del sistema operativo empleado para la busqueda de cadenas en ficheros
- *strings* Comando del sistema operativo que muestra los caracteres ASCII imprimibles de un fichero.
- *dd* Comando del sistema operativo empleado para hacer copias a bajo nivel de dispositivos.
- *lsof (ftp://ftp.rediris.es/mirror/dfncert/tools/admin/lsof)* Herramienta que permite análizar que ficheros o sockets están siendo usados en un equipo, con indicación de los procesos que los están empleando. Suele venir incorporada en los equipos Linux y *BSD.
- *rpm* Programa de gestión del software instalado en los equipos, empleado en las distribuciones RedHat, Suse, Mandrake,..., en debian el programa dselect realiza funciones similares.
- *Tripwire (http://www.tripwire.org)* Programa que genera diversas huellas criptográficas de los ficheros instalados en los equipos, pudiendo así verificar después que ficheros han sido modificados. la antigua versión académica se puede encontrar en ftp://ftp.rediris.es/mirror/coast/tools/unix (ftp://ftp.rediris.es/mirror/coast/tools/unix)
- *nc (netcat) (http://www.l0pth.com/~weld/netcat)* Herramiente para la conexión de conexiones TCP/UDP entre equipos, se suele emplear para transmitir por la red los contenidos de los particiones/equipos atacados fácilmente.
- The Coroner's Toolkit (tct) (http://www.porcupine.org/forensics/) Conjunto de herramientas para realizar análisis en sistemas atacados, permiten recuperar ficheros borrados siempre que no hayan sido sobreescritos, calcular la integridad de los ficheros existentes en el equipo, consultar que ficheros han sido accedidos desde una determinada fecha, etc.
- Ldasm (http://www.geocities.com/rmaxdx/ldasm.htm) Desensamblador de binarios Unix, genera un código ASM bastante "legible", indicando las llamadas al sistema que emplea un programa, lo que permite seguir la ejecución de algunos programas usados en diversos ataques.

Bibliografía

Wietse Venema, Dan Farmer, *Computer Forensic Analysis class : http://www.porcupine.org/forensics/handouts.html (http://www.porcupine.org/forensics/handouts.html)* , Trasparencias sobre una sesión impartida por Dan Farmer y Wiete Venema en Verano de 1999 sobre análisis forense en equipos Unix, con referencias a la herramiente TCT. .

Dave Dittrich, *Información de David Diettrich sobre análisis forense : http://www.cac.washington.edu/People/dad/ (http://www.cac.washington.edu/People/dad/)* , Página WWW con información de David Diettrich sobre diversos aspectos de la seguridad informática, incluyendo diversas presentaciones realizadas en Sans (http://www.sans.org/) así como bastante documetnación sobre análisis forense en equipos Unix. .

Equipo de seguridad de RedIRIS, *Recomendaciones de seguridad: http://www.rediris.es/cert/docs/docsiris/recomendaciones (http://www.rediris.es/cert/doc/docsiris/recomendaciones)* , Breve guia de configuración segura de equipos Unix/Linux en Red .

CERT/CC, *Documentos de seguridad del CERT/CC: http://www.cert.org/tech_tips (http://www.cert.org/tech_tips)* , Documentos publicados por el CERT/CC, cubriendo diversos aspectos de seguridad en equipos Unix, detección de las intrusiones, limpieza de sistemas, configuraciónes seguras de servicioes, programación segura de CGI, etc, incluyendo una guia con información sobre como volver a la normalidad (http://www.cert.org/tech_tips/win-UNIX-system_compromise.html) tras un acceso a una cuenta privilegidada. .

Antonio Villalón Huerta, *Seguridad en Unix y Redes: http://www.rediris.es/cert/doc/unixsec (http://www.rediris.es/cert/doc/unixsec)* , Libro muy completo sobre la seguridad en equipos Unix y redes, configuración de equipos, cortafuegos, etc. incluye una extensa bibliografía sobre seguridad. .

Notas

1. estadísticas del CERT/CC (http://www.cert.org/stats/) muestran la evolución de incidentes de cualquier tipo gestionados por el CERT/CC, además en en los informes anuales de este organismo (http://www.cert.org/annual_rpts/) aparecen año tras año las vulnerabilidades más empleadas por los atacantes para acceder a

los equipos, en la mayoria de las veces servicios ejecutandose sobre plataformas Unix

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}

   Además con el rootkit se suelen instalar “puertas traseras” en el equipo, programas que permitan acceder de fácilmente en otras ocasiones al equipo. Así una modificación en el programa **tcpd** de los tcpwrapper, cuando el programa **tcpd** recibía una conexión con origen un puerto determinado (421/TCP), se ejecutaba un interprete de comandos, teniendo acceso al equipo.

3. Pocas usuarios instalan algún programa como Cops (ftp://ftp.rediris.es/rediris/cert/mirrors/dfncert/tools/admin/Cops/) , System Scanner de ISS (http://www.iss.net/eval/specs4.html) o Nessus (http://www.nessus.org) para comprobar las posibles vulnerabilidades de sus equipos.

4. Se puede emplear el comando **script** para ir generando un fichero con todos los programas que se ven ejecutando.

5. Esto es especialmente importante en el caso de que se este realizando un análisis con vista a un proceso judicial, en, ya que si se ha operado directamente sobre los datos originales, los datos obtenidos serán invalidados

6. Este es uno de los motivos por los cuales siempre que sea posible se debe realizar la instalación de los programas mediante el sistema de paquetes del sistema operativo, de forma que se tenga información fiable sobre los programas instalados en el equipo.

7. Consultar la lnota de prensa del 19 de Mayo del 2001 (http://www.apache.org/info/20010519-hack.html)

8. 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.