Informe de incidentes de seguridad

IRIS-CERT <cert@rediris.es>

$Id : informe.tex, v1.52002/06/0700 : 05 : 45 pacoExp$

Índice General

1 Introducción

Este informe de incidentes de seguridad pretende reflejar los aspectos más relevantes que han ocurrido en la gestión de incidentes de seguridad gestionados por el grupo de seguridad de RedIRIS, IRIS-CERT durante el periodo de tiempo comprendido entre Octubre del año 2001 a Mayo del 2002.

Es nuestra intención que este informe actualizado sea presentado regularmente de manera ordinaria en la lista de coordinación de seguridad de RedIRIS, de forma que se pueda informar detalladamente de los problemas de seguridad a los responsables de las instituciones afiliadas y presentar una evolución continua de los incidentes de seguridad.

Además de las estadísticas se presenta en este informe un breve resumen de las posibles soluciones a los problemas de seguridad más frecuentas que se han producido y una descripción de los procedimientos y herramientas que con más frecuencia se han detectado a lo largo de este periodo.

Con toda seguridad este informe presenta bastantes lagunas que esperamos ir solucionando a lo largo del tiempo, hasta que refleje de una forma fiable los problemas de seguridad existentes.

2 Estadísticas

La carencia de recopilación de datos a la hora de gestionar los incidentes de seguridad hace que no podamos presentar unas estadísticas completas sobre los incidentes de seguridad, sino solamente unos ligeros esbozos de los principales problemas de seguridad que se han detectado.

Por otro lado en estas estadísticas solamente aparecen reflejados aquellos problemas de seguridad de los que tenemos directamente noticia , ya sea porque los administradores de las redes atacadas se han puesto en contacto con nosotros (casi siempre una red externa que denuncia un escaneo o acceso ilegal), o porque los administradores de una institución afiliada nos comunican un ataque que han sufrido.

Algunos de los datos más significativos son:

- El número de incidentes atendidos durante estos ocho meses (octubre 2001 a Mayo 2002 ha sido de 764 incidentes).
- Mediante notificaciones externas, sobre todo por parte de uno o dos centros afiliados se tiene constancia de al menos 38 incidentes de se-

guridad adicionales, además se han recibido correos informativos, en los que la dirección de contacto de IRIS-CERT aparece como copia (CC), de diversos grupos de seguridad internacionales.

- el 66% de los incidentes (509) han involucrado a equipo de fuera de España, sobre todo han sido situaciones en las que se ha recibido una denuncia desde el exterior relativa a un equipo Español, (428 incidentes).

- Aunque la mayoría de los incidentes que se han gestionado corresponden a equipos de la red académica (468 incidentes, 61%), se han gestionado también 296 incidentes en los cuales el equipo español involucrado no pertenencia a la red académica.

  Los principales incidentes de este tipo han sido debidos a:

  - Notificaciones , de servidores WWW atacados, sobre todo gracias al uso de la información de http://www.alldas.orgAlldas, http://www.alldas.org, donde se noticia vía correo-e de los ataques a servidores WWW.
  - Notificaciones de grupos de seguridad de FIRST y TI, donde intentan contactar con algún grupo de seguridad Español y nos envían el mensaje a nosotros[1]

- Se ha avisado un total de 53 veces a equipos de fuera de la red académica de posibles ataques desde RedIRIS. Esto ha sido posible gracias al análisis de los ficheros encontrados en máquinas atacadas donde se ha podido determinar el origen del ataque o encontrar evidencias de equipos atacados desde los españoles.

2.1 Evolución de los incidentes

En la figura 1, se observa la evolución de los incidentes de seguridad desde principios de 1999, el punto álgido en verano del año 2001 corresponde a la aparición de los problemas de seguridad en los servidores IIS de Microsoft.

[1] IRIS-CERT todavía figura como punto de contacto exterior para incidentes donde este implicado el dominio .es

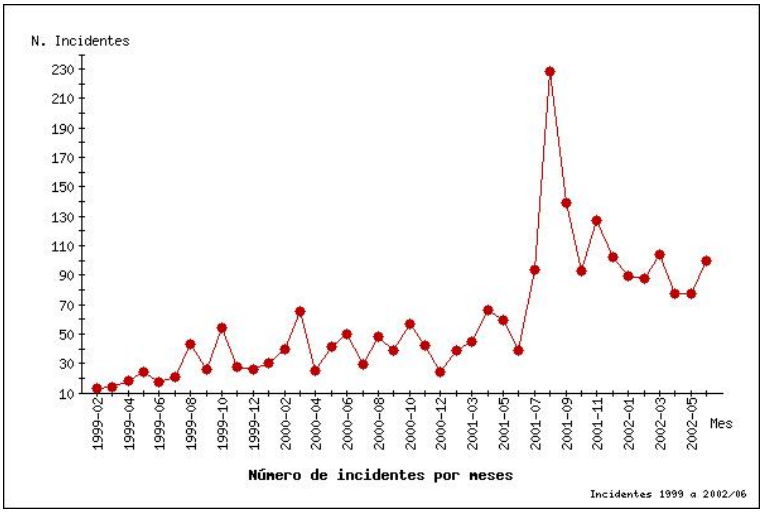

Figura 1: Evolución de incidentes por meses

El valor para el mes de Junio ha sido extrapolado a partir de los incidentes ocurridos desde principio del mes hasta el día 6 de Junio.

Se aprecia, sin embargo, como a partir de este incidente el número de incidentes ha tenido un gran incremento todos los meses, debido principalmente a un efecto que podríamos denominar de "ruido de fondo" que los equipos infectados por IIS provocan.

Hay que indicar además que gran la mayoría de los incidentes de seguridad se producen tras la recepción de un correo o queja de denuncia desde el exterior de las instituciones de RedIRIS, sobre todo debidas a escaneos de puertos o pruebas , por lo que los escaneos, sobre todo los provocados por este tipo de gusanos son los informes más numerosos.

Además la existencia de diversos mecanismos de denuncia automáticos, como http://www.dshield.org, o http://aris.securityfocus.com hacen que se reciban cada vez más denuncias automatizadas de este tipo de ataques.

En la siguiente tabla aparecen reflejada el porcentaje de cada uno de los incidentes clasificados a partir del primer mensaje que se recibe. Es decir, si inicialmente se recibe un mensaje indicando un escaneo de puertos, el incidente se clasifica como un escaneo, aunque posteriormente al investigar se observe que se trata de un acceso a un equipo y se proceda a investigar el

incidente.

Tipo de Incidente	**Cantidad**	%
Comunicación Ofensiva	3	0
Denegación de Servicio	21	2
Virus	1	0
Otros	17	2
Sondeos o escaneos de puertos	285	37
Acceso a cuentas privilegiadas	94	12
SPAM	20	2
Troyanos	11	1
Gusanos IIS	296	38
Usos no autorizados	10	1
Violaciones de Copyright	3	0

Las denuncias de usos no autorizados han sido debidas a malas configuraciones de los servicios, en especial el empleo de equipos Proxy para ocultar las conexiones a otros servidores en los incidentes de uso no autorizado de recursos, ya que los servidores permitían el uso del servidor por equipos externos a la organización.

En la figura 2, aparecen de una forma más clara los seis tipos más importantes de incidentes gestionados, se observa de una forma más clara como los incidentes debidos a escaneos y a los problemas de seguridad en IIS han sido un 75% de los incidentes gestionados.

Como se ha comentado antes, muchas veces los incidentes debidos a escaneos desde equipos Unix son en realidad accessos a cuentas privilegiadas del sistema, exigiendo un análisis de los ficheros enviados por los administradores para intentar determinar las acciones realizadas por los atacantes.

La diferenciación entre escaneos de servidores (puerto 80) y gusanos IIS es algo difusa, hemos procurado que todos los mensajes en los que se indicaba este puerto como destino del ataque sean clasificados directamente como gusanos, para así diferenciar este tipo de incidentes, sin embargo algunas veces por omisión o no ser muy precisos los primeros informes algunos incidentes

Figura 2: Porcentajes de incidentes

han sido clasificados dentro del grupo "genérico" de escaneos o pruebas, aunque después los administradores nos han indicado que se trataba de un equipo infectado por estos gusanos.

Sin poder ser muy estrictos, ya que muchas veces no guardamos la información referida al puerto escaneado, o se trata de escaneos a varios puertos, los servicios más atacados han sido.

Servicio	Puerto	veces
FTP	21/TCP	63
portmap/RPC	111/TCP	22
SSH	22/TCP	19

En la sección de incidencias más destacadas se hace mención a las vulnerabilidades existentes en estos los servidores que están escuchando en estos puertos.

2.2 Comentarios sobre estas estadísticas

2.2.1 Ataques contra servidores IIS

Los gusanos CodeRed y Nimda siguen siendo uno de los problemas más notificados desde el exterior,

Entre los motivos por los cuales se sigue produciendo este tipo de ataques, casi 10 meses después de su inicio se encuentran las siguientes circunstancias:

1. Es muy difícil a nivel administrativo el filtro del servicio de HTTP a la entrada de las instituciones, ya que en muchos departamentos o grupos de investigación es frecuente el mantenimiento de un servidor HTTP propio, escasamente o mal administrado.

2. Falta de concienciación entre los usuarios / administradores de servidores IIS, de la necesidad de aplicar los parches de seguridad a este servidor, por lo que muchas veces se procede directamente a la reinstalación del equipo volviendo a ser este vulnerable tras un cierto tiempo de inactividad.

3. Falta de una actualización completa del servidor IIS, o de un conjunto de parches completo[2], del sistema, que permita al administrador instalar el servidor de una forma segura, sin tener que recurrir a la obtención de los parches uno a uno.

4. Dificultad en las organizaciones para el filtrado de equipos una vez que se notifica el problema, lo que permite la propagación del ataque.

En la sección dedicada a este tipo de ataque aparecen algunas indicaciones que se pueden tomar en las instituciones para evitar este tipo de ataques, aunque es un problema difícil de solucionar, debido al número de equipos que emplean este servidor HTTP, y la no existencia de una versión actualizada de este servidor que evite todas estas vulnerabilidades.

[2]También llamado service packs ;-)

2.2.2 Ataques contra plataformas Linux

En la mayoría de las ocasiones en las que se ha producido un acceso a una cuenta privilegiada del sistema en equipos Linux los servicios que se han empleado para obtener este acceso han sido los servicios de SSH y FTP, y en menor medida las vulnerabilidades existentes en diversos servicios de RPC.

La repercusión de estos ataques ha sido bastante elevada, sobre todo en el caso de los ataques contra servidores FTP, aunque la aparición de nuevas versiones no vulnerables de estos servidores en las ultimas versiones de las distribuciones Linux más importantes ha hecho que muchos usuarios al actualizar o reinstalar su máquina a la ultima versión no sean vulnerables a estos ataques.

De ambos tipos de ataques y los distintos tipos de rootkit detectados, aparece una reseña en una sección posterior.

2.3 Ataques contra plataformas Solaris

Debido a las vulnerabilidades descubiertas en diversos servicios RPC, servidores auxiliares de los procesos de entorno gráfico (dtspcd, cmsd, ttdserver) y servidor de impresión se han producido diversos ataques contra equipos Solaris.

En la mayoría de los casos se trataba de servidores sin actualizar desde hace tiempo, no dependientes directamente de los servicios de informática, sino pertenecientes a grupos pequeños de investigación que en algunas situaciones no disponían de personal encargado de la administración de estos equipos.

Aunque el número de ataques se ha visto reducido, estos equipos se siguen empleando para la realización de ataques de denegación de servicio, al disponer en la mayoría de los casos de una buena conectividad de red, y la falta de administración.

En general, se observa que los equipos pertenecientes a los servicios de informática presentan una menor incidencia de ataques, debido seguramente a la progresiva concienciación de los administradores y a la puesta en marcha de medidas (separación de redes, cortafuegos y filtros en router,etc.) para evitar estos ataques.

2.4 Balanceadores de carga

En algunas instituciones afiliadas han empezado a instalar sistemas de balaceo de carga en el tráfico saliente, teniendo contratada una linea alternativa con otro proveedor y empleando el sistema de balanceo de carga para calcular la ruta optima hacía un equipo.

Estos sistemas de balanceo de carga realizan conexiones DNS o HTTP hacia los equipos destino por cada una de las rutas que disponen y redirigen el tráfico por el interface correspondiente.

Sin embargo las consultas que realizan no son correctas y son detectadas por bastantes sistemas de detección de intrusos como escaneos del programa "nmap", llegandonos continuamente quejas sobre estos equipos. Como ejemplo sobre un mismo equipo hemos recibido ya más de 25 denuncias provocadas por este sistema de balanceo de carga.

Seguramente si el empleo de estos sistemas de balanceo de carga para el tráfico se popularizán es muy posible que los problemas debidos a este tipo de equipos sigan en aumento.

2.5 Respuesta ante los correos

Uno de los principales problemas que nos encontramos en la gestión de los incidentes de seguridad es la falta de respuesta ante los avisos de seguridad, lo que nos exige muchas veces el enviar periodicamente recordatorios para consultar si el problema de seguridad ha sido solucionado.

En el último periodo, ha mejorado algo la respuesta por parte de algunos proveedores Españoles, indicandonos que como mínimo van a proceder a contactar con el usuario para indicarles lo que ha pasado y/o tomar las medidas oportunas. Desgraciadamente, todavía hay algunos ISP y lo que es más grave instituciones Afiliadas a RedIRIS de los que muchas veces no tenemos ninguna comunicación en los incidentes de seguridad, por lo que no sabemos si se toma alguna medida para solucionar los problemas.

Para las instituciones afiliadas a RedIRIS el procedimiento general es enviar el correo, a las direcciones que podemos obtener, en orden de importancia de:

1. Información de contactos de seguridad proporcionada por las propias instituciones a IRIS-CERT

2. Base de datos de las "Personas de Enlace con RedIRIS, PER", muchas veces desactualizada cuando un PER deja sus funciones en unan institución y no se comunica a RedIRIS el cambio de PER.

3. Información de contacto de las bases de datos públicas sobre las direcciones IP y Dominios de DNS, también muchas veces desactualizada.

Hace falta un esfuerzo desde algunas instituciones por actualizar los datos, contactando con la Secretaría de RedIRIS para los puntos de contacto y Base de datos de PER y siguiendo los procedimientos del esNIC y RIPE , de forma que los puntos de contactos estén actualizados y se pueda contactar con los responsables rápidamente.

Además es importante que se responda al recibir una notificación relativa a un incidente de seguridad, para que en el grupo de seguridad tengamos constancia de que el incidente como mínimo ha sido leido por alguien de la institución y se van a tomar las medidas oportunas para solucionarlo.

3 Incidentes Significativos

3.1 Ataques contra servidores IIS

A mediados del año pasado surgieron varios ataques de tipo gusano[3] contra servidores IIS de Microsoft.

Estos ataques se aprovechaban de diversas vulnerabilidades existentes en este servidor para conseguir que se ejecutase el código del gusano, causando la "infección" del equipo y propagación del ataque a otros servidores.

Durante los primeros meses de la propagación, se llegaron a producir denegaciones de servicio y cortes en algunos de los centros afiliados a RedIRIS, debido al tráfico generado por estos gusanos y a los escaneos que producirán. Esta situación fue particularmente grave en aquellas organizaciones que tenían un direccionamiento de varias clases C agregadas, dándose casos de denegación de servicio externa (equipos infectados en otras Universidades que escaneaban a la red de la organización atacada).

Este ataque también genero ataques de denegación de servicio contra ciertos dispositivos de red (router, switchs, servidores de impresión,etc), que tenían habilitado el servidor HTTP para tareas de administración.

[3]Programas que se ejecutan y atacan a otros servidores automáticamente, sin intervención del atacante

El fabricante proporciono, aún antes de la aparición de este gusano parches que permitían solventar este problema, sin embargo todavía hoy los gusanos de este tipo representan gran parte de las alertas de seguridad existentes, como se ha visto en la sección de dedicada a las estadísticas de incidentes.

Dependiendo de las versión del gusano este solamente se dedicaba a infectar otros equipos (CodeRed) o también modificaba la configuración del equipo atacado, haciendo posible que un atacante accediera con posterioridad al equipo, gracias a la instalación de diversas puertas falsas en el equipo atacado (Nimda), empleando además otros medios como correo-e, sistemas de ficheros compartidos, etc, para su propagación.

Información adicional sobre este problema se puede encontrar en:

- http://www.cert.org/advisories/CA-2001-23.html Aviso generado por el CERT/CC sobre CodeRed, con la descripción de este problema y un análisis desde que surgió este problema en Julio del 2001 a Enero del 2002.
- http://www.microsoft.com/technet/security/bulletin/MS01-044.asp Parches de Microsoft relativos al CodeRed.
- http://www.cert.org/advisories/CA-2001-26.html Aviso del CERT/CC sobre el problema de seguridad de Nimda.
- http://www.microsoft.com/technet/security/bulletin/MS01-020.asp Información sobre el gusano NIMDA y parches que se deben aplicar. Hay que tener en cuenta que este gusano se puede propagar por otros medios (corre-e, navegador, etc), por lo que los usuarios que empleen estos productos debe tener actualizado los programas de acceso a Internet (Internet Explorer, Outlook, etc.) y el antivirus de escritorio.

Algunas medidas que se deberían tomar para evitar la propagación y ataque de este tipo de programas son:

1. Si el equipamiento de Red lo permite, es posible filtrar en los router de acceso el tráfico generado por estos y otros gusanos, empleando la característica de filtrado de tráfico NBAR, como se comenta en http://www.cisco.com/warp/public/63/nbar_acl_codered.shtml. Este técnica ha sido empleada en algunas instituciones con éxito, y aunque

no es perfecta (una versión del gusano emplea tráfico fragmentado y permite saltarse el filtro), es muy efectiva.

2. Detección interna. Muchas veces los equipos infectados generan en primer lugar intentos de acceso a otros equipos situados en la misma subred. Es conveniente que se comprueben periódicamente los logs de los servidores HTTP de las organizaciones y como mínimo se notifique a los usuarios internos la existencia de este gusano, de forma que disminuya el número de posibles equipos infectados a partir de este.

3. Facilitar a los administradores de estos sistemas información sobre el problema, así como mantener un repositorio interno con los parches que se deben aplicar una vez instalado el servidor, de forma que se facilite la instalación segura de estos equipos.

3.2 Ataques contra servicios SSH1

A principios de octubre apareció un programa que implementaba un ataque contra diversas implementaciones de SSH, y que afectaba a diversos fabricantes. Este ataque tuvo en principio una gran repercusión, ya que afectaba a varias versiones de este programa y el uso de SSH como alternativa segura a las conexiones de terminal hacía que en muchos equipos Unix estuviera habilitado con permisos de acceso desde cualquier dirección.

El CERT/CC genero una nota, http://www.cert.org/incident_notes/IN-2001-12.html donde se comentaba los problemas que estaban apareciendo.

Por otro lado, David Dittrich, de la Universidad de Washington realizó un informe preliminar sobre este ataque, que se puede encontrar en http://staff.washington.edu/dittrich/misc/ssh-analysis.txt

El problema empleado en este tipo de ataque afecta a los servidores SSH 1 de diversas arquitecturas, incluyendo el servidor SSH incluido en las versiones recientes de IOS de los equipos CISCO, aunque no se han detectado versiones del exploit que consigan tener éxito con sistemas operativos distintos de Linux, se provoca una provoca denegación de servicio por bloqueo o interrupción del servidor en otras arquitecturas como pueden ser las algunas versiones de IOS.

Desde entonces el uso de este programa de ataque se ha generalizado bastante, habiéndose encontrado en algunos equipos atacados estos programas, junto con scripts para facilitar el ataque a otras redes, aunque ultimante el número de ataques se ha reducido en los últimos meses.

En la mayoría de los ficheros que se han podido recuperar se empleaba el programa de ataque "X2,o X4", estos programas presentan algunas peculiaridades que han impedido un análisis detallado de los mismos:

- El programa esta encriptado, de forma que no existe ninguna cadena visible al comando "strings", además la cabecera del fichero ha sido modificada para evitar que pueda ser depurado mediante un depurador de código.
- El programa esta enlazado estáticamente, sin símbolos de depuración, por lo que tampoco se puede ver que llamadas al sistema emplean, salvo que se ejecute el programa dentro de un entorno controlado donde se monitoricen las llamadas al sistema.
- El programa requiere una clave para su ejecución.

Esta ultima característica debió estar pensada en principio para evitar su uso indiscriminado y evitar su propagación, sin embargo hemos encontrado diversos scripts que solucionan este problema, vía un módulo del núcleo que permite la ejecución del programa sin conocer la clave, además esta clave ha sido publicada en diversas páginas de Internet.

Las versiones X2 y X4, presentan como característica adicional el emplear un fichero de configuración donde se indican los valores que deben emplearse para cada versión del servidor SSH, de forma que se pueda emplear para mas o menos sistemas este ataque , en función de los valores que se encuentran en el fichero de configuración.

La versión comentada en el análisis de David Diettrich, permite atacar a un reducido número de equipos y requiere que el atacante se conecte después a determinado puerto del equipo víctima donde esta ejecutándose un interprete de comandos.

La versiones X2-X4, han sido más usadas ya que generaban directamente la conexión con el interprete de comandos en el ataque, lo que permitía su uso dentro de programas de escaneo de ataque, o autoroot, que son lo que más hemos encontrado en los equipos atacados. Estos autoroot, suelen consistir en una serie de scripts que se van ejecutando secuencialmente y emplean algunos de estos programas:

1. pscan, pscan2 , se trata de un scanner bastante rápido utilizado para buscar el banner identificativo de la versión del servidor SSH que esta corriendo en un equipo.

2. Un pequeño script, basado en awk, que compara la salida de pscan2 con determinados valores, para analizar que parámetro se debe emplear en el ataque.

3. Un script que ejecuta el ataque contra el servidor, empleando la información obtenida en el paso anterior

La principal diferencia entre estos autoroot y los gusanos que aparecieron hace algún tiempo contra servidores Unix, es que estos autoroot no suelen ser activados automáticamente, para evitar una propagación excesiva que alertaría del ataque.

Por otro lado los rootkit que se han ido encontrando han ido evolucionado y se han encontrado versiones bastante recientes de Adore (rootkit, como módulo del núcleo) y del T0rn, así como combinaciones de varios rootkit en uno.

La solución ante este tipo de ataques es la actualización del software de SSH que se este empleando en el equipo, y la limitación mientras no se procede a la actualización a mecanismos de control de acceso (filtros en los núcleos, router o en los ficheros de control del tcpdwrapper), para evitar las conexiones desde equipos desconocidos y el forzar el empleo en el servidor SSHD del protocolo SSH2 que no es vulnerable a este ataque.

Afortunadamente las ultimas versiones de las distribuciones Linux más importantes incorporan las nuevas versiones de estos servidores SSH, por lo que en los últimos meses la repercusión de este tipo de ataque ha sido mínima.

3.3 Ataques al servidor FTP

Los servidores FTP, sobre todo los basados en el distribuido por la Universidad de Washington, wu-ftpd han tenido diversas vulnerabilidades en los últimos tiempos, que han ido apareciendo al poco de salir una nueva versión de este servidor, lo que ha provocado que haya sido uno de los métodos más empleados para acceder al equipo.

La ultima versión, de este ataque, permite atacar servidores vulnerables a las versiones 2.6.0, 2.6.1, 2.4.2, existente en las distribuciones Linux

- Suse, 6.0 a 7.2
- RedHat 5.2 a 7.2

- Slackware 7.1
- Mandrake 6.0 a 8.1
- Immunix 6.2 y 7.0
- Debian potato y sid
- Caldera OpenLinux 2.3

Esta variedad de distribuciones Linux, combinado con un sistema de autoroot similar al comentado en el caso de los ataques a servidores SSH ha provocado la proliferación de ataques con éxito a estos servidores.

En algunos de las situaciones en las que los administradores nos han enviado los ficheros instalados por los atacantes, hemos podido comprobar que los scripts de instalación proceden a actualizar la versión del servidor FTP, para evitar que este vuelva a ser atacado.

3.3.1 Rootkit en Linux

En los equipos analizados se ha encontrado varios diversos rootkit, advirtiéndose una mayor complejidad en los mecanismos empleados para ocultar su funcionamiento:

- Empleo del comando "chattr" para evitar que los binarios modificados sean borrados al actualizar los paquetes.
- Cambio completo de los atributos de los ficheros, para evitar que el comando "find" indique que son ficheros recientes.
- Ocultación de los ficheros de configuración y claves, mediante concatenación de caracteres, para evitar que la salida del comando "strings" delate la presencia del de los ficheros.
- Encriptación mediante compresores de los binarios, evitando así que el comando strings presente cualquier información.

Sin embargo, y por lo general los scripts de instalación todavía no modifican la base de datos del software de instalación, por lo que una comprobación, ("rpm -Va", en sistemas basados en RPM) permite detectar con facilidad los binarios modificados.

Se han detectado algunas instalaciones de rootkit de núcleo, que ocultan a nivel de núcleo los ficheros y procesos , evitando modificar los binarios, pero en los equipos analizados, este sistema venía acompañado de modificaciones en los binarios (comprobación adicional de los atacantes), o bien el módulo fallaba en la instalación inicial en el arranque del equipo delatando la presencia de los scripts.

Los atacantes han dejado de utilizar puertas traseras basadas directamente en servidores telnetd, o el comando login, para emplear servidores SSHD escuchando en determinado puerto y compilados para emplear un password precompilado como clave de acceso. De esta forma evitan que los administradores puedan monitorizar sus actividades fácilmente una vez que se ha descubierto el ataque. Estos servicios suelen ser lanzados en los scripts de arranque , con nombres que suelen hacer referencia al servidor cache de nombres (nscd) o a los servidores de tiempo (ntpd).

3.4 Ataques a Equipos Solaris

Aunque el número de ataques a plataformas solaris no ha aumentado mucho, se han producido diversos incidentes en los cuales se ha visto implicados varios equipos Solaris.

Hemos detectado ataques contra servidores solaris, provocados desde equipos Linux, habiendo recuperado en uno de los equipos un conjunto de programas de ataque contra este sistema Operativo compilados para Linux, lo que permitía a los atacantes diversificar las plataformas y permite suponer que son programas bastante portables.

En un incidente un equipo Linux fue atacado y desde el se procedió a realizar ataques contra servidores dtspcd de Solaris, detectando en los logs de los scripts empleados por el atacante un total de 96 equipos posiblemente atacados.

Puestos en contacto con los administradores de la red implicada, se comprobó que efectivamente gran parte de estos equipos habían sido atacados con éxito.

Otros exploit encontrados y que afectan a servicios instalados en plataformas Solaris incluyen como se ha comentado ataques contra el servidor de impresión y contra diversos servicios de RPC. De este ultimo el mismo programa permitía atacar (con distinto código en cada caso), servicios RPC en Linux y Solaris.

3.4.1 Rootkit

En uno de los últimos incidentes analizados se encontró el ficheros comprimido con los ficheros de instalación y binarios de un rootkit empleado en varios ataques, en lineas generales este rootkit presenta las siguientes características.

- Este rootkit oculta el nombre de los ficheros de configuración de forma que no se pueden ver mediante el comando strings, ya que no ocupan posiciones consecutivas. El ocultamiento es muy sencillo, en C sería un código similar a este.

```
char fichero[20] ;
        fichero[0] = '/' ;
        fichero[1] = 'l' ;
        fichero[2] = 'i' ;
fichero[3] = 'b' ;
fichero[4] = '/' ;
        ....
        fichero[n-1] = 'q' ;
        fichero[n] = '\0' ;
```

- Emplea como directorios de configuración:

```
USRDIR="/usr/lib/locale/cz/..."
SUNRKDIR="/usr/lib/locale/tr/..."
```

- El script instala los siguientes programas "troyanizados"
  - du
  - find
  - login
  - ls
  - netstat
  - ps

- top

y un demonio de sshd, configurado al parecer para dar acceso a root con un passwd que se almacena en un fichero en los directorios de configuración.

- Además el rootkit incorpora los siguientes programas:

  fix : Programa para cambiar la fecha de los binarios del rootkit cuando se instalan y así ocultarlos.

  fresht : Script de borrado de logs

  resize : utilidad para hacer que los ficheros del rootkit tengan el mismo tamaño que los originales.

  srload : Binario encargado de ejectuar en el arranque los demonios de escaneo y demás del rootkit.

  sunsniff : Sniffer para Solaris

  syn : Demonio de denegación de servicio

  td : Demonio de control remoto stalchel

- Por ultimo, este rootkit deja los ficheros modificados con las mismas fechas y tamaños de los originales, por lo que no aparecen a simple vista como modificados. Emplea el programa srload, para lanzarlo en el arranque y ocultar así a los procesos del sniffer y sshd.

3.5 Denegación de Servicio

Los ataques de denegación de servicio se han reducido, aunque todavía ocupan un lugar significativo. La disponibilidad de mayores anchos de banda en algunos troncales ha permitido algunas veces que los atacantes disimularan su actividad, por lo que gran parte de los incidentes de este tipo se han detectado mediante alertas recibidas desde el exterior.

Dado que este tipo de incidentes se produce como consecuencia de un acceso a una cuenta privilegiada del sistema, el evitar este tipo de accesos es la mejor medida para evitar que se produzcan ataques de denegación de servicio desde las instituciones afiliadas.

Gran parte de los ataques siguen empleando ataques basados en el empleo de direcciones de broadcast, para amplificar los ataques por lo que es

conveniente filtrar este tipo de tráfico tanto en los router de acceso como en los Router internos de la organización. En http://www.cymru.com/řobt/Docs/Articles/secure-ios-template.html hay información sobre la configuración segura de un router cisco para evitar este y otro tipo de ataque.

Dado que el empleo de direcciones broadcast no se puede evitar para equipos situados dentro de la mismo subred, es conveniente de todas formas limitar la cantidad de tráfico ICMP que se puede enviar y recibir, como se comenta en ftp://ftp.rediris.es/rediris/red/ip/docs/ejem-cisco.txt, guia de procedimientos de conexión,

De todas formas se debe empezar a usar herramientas de monitorización de tráfico que permitan detectar cuando un equipo tiene un comportamiento anómalo y debe ser investigado. Esta monitorización debería ser realizada en las propias instituciones que son las que pueden tratar directamente con los administradores y comprobar cuando se trata de un ataque.

4 Información adicional

4.1 Envío de información a IRIS-CERT

Muchas veces la notificación que se envía relativa a un escaneo de puertos o ataque sin importancia se convierte en realidad en un incidente más serio en el cual un atacante exterior ha conseguido acceder a una cuenta privilegiada del sistema (tradicionalmente lo que se conoce como un "root compromise", en Unix) y posteriormente se instalan determinadas herramientas por el atacante para ocultar su acceso y atacar a otros equipos.

Desde IRIS-CERT creemos conveniente realizar un estudio detallado de este tipo de incidentes, para intentar averiguar en la medida de lo posible las acciones realizadas por los atacantes, herramientas empleadas, y así poder aconsejar a los responsables de la institución las medidas a emplear.

Así, si en el estudio se detecta la presencia de un programa captura de tráfico (sniffer), es aconsejable alertar a los usuarios de la organización en general y a aquellos usuarios que aparecen en el fichero resultados del sniffer en particular que deben cambiar sus claves de acceso, para evitar que el atacante emplee estas claves con posterioridad para otros accesos.

Además el estudio de las herramientas usadas por los atacantes nos permite aconsejar en otras situaciones similares a otros responsables sobre los

pasos a seguir para detectar un ataque.

Por ultimo muchas veces los programas utilizados para atacar a otros sitios mantienen un registro de los ficheros que se han atacado con éxito, pudiendo de esta forma avisar a los administradores de estos equipos del ataque, evitando así la propagación del ataque.

En los correos que se envían relativos a equipos posiblemente atacados se suele indicar una reseña a la

Guia de recuperacion de incidentes donde se indican los pasos a seguir.

Básicamente se le solicita a los administradores de los equipos que envíen:

1. Salida de la ejecución de comandos del sistema ("ps -aex","netstat -a",etc).
2. Ficheros de logs del equipo donde aparezcan los binarios instalados en el equipo.
3. Ficheros binarios (rootkit), instalados por el atacante para disimular el ataque.
4. Ficheros (logs, programas,código fuente, etc), instalados en directorios ocultos por los atacantes para atacar a otros equipos.

Esta información debe ser envíada al grupo de seguridad de RedIRIS, vía correo-e, cuando se trata de poca información o empleando uno de los siguientes medios:

- Por FTP, depositando el fichero en el directorio incoming del servidor FTP de RedIRIS
- vía HTTP, empleando el Servidor de ficheros de RedIRIS

En RedIRIS procederemos a analizar los ficheros que se nos envíen y enviar a los administradores la información que se pueda obtener de estos ficheros.

4.2 Recursos de coordinación de Seguridad

Como resumen, algunos enlaces que deben ser de sobre conocidos por todos aquellos que lean este documento, aunque no este de mas volver a citarlos:

- Lista de coordinación de seguridad, IRIS-CERT, en esta lista deberían estar como mínimo una persona o responsable de cada una de las instituciones afiliadas, de forma que puedan recibir la información y alertas de seguridad que vayan surgiendo, antes de que se produzcan.

  En la actualidad muchas organizaciones afiliadas a RedIRIS no cuentan con una dirección de contacto de seguridad, lo que provoca que muchas veces se envíe directamente al PER de la organización los avisos de seguridad.

- Formulario de atención de incidentes, disponible en el servidor FTP de RedIRIS con indicación de la información a enviar ante un incidente de seguridad.

- Documentación de seguridad en el servidor de RedIRIS, http://www.rediris.es/cert/doc Recopilación de información de seguridad para diversos aspectos, instalación segura de equipos, análisis de ataques, etc.

- Listado de grupos de seguridad Europeos, http://ti.terena.nl/, para la busqueda de grupos de seguridad en otros países.

- Lista pública de seguridad en castellano, CERT-ES@listserv.rediris.es, para consultas generales de seguridad.