Recomendaciones de seguridad

Chelo Malagón Poyato (chelo.malagon@rediris.es)
Francisco Monserrat Coll (francisco.monserrat@rediris.es)
David Martínez Moreno (david.martinez@rediris.es)

15 de diciembre de 2000. Versión 0.1

Índice General

Capítulo 1

Introducción

Cada vez son más frecuentes los incidentes en los que se ven involucradas las instituciones afiliadas a RedIRIS. El tiempo necesario para la atención de estos incidentes es cada vez mayor, ya que suelen involucrar a varias instituciones y muchas veces lo único que se puede conseguir es parar al intruso, sin llegar a menudo a conocer la identidad del atacante o los motivos por los cuales se produjo.

Con el incremento de usuarios en Internet, y en la comunidad RedIRIS en particular, es cada vez más fácil obtener información sobre vulnerabilidades de un equipo o sistema operativo, pudiendo atacar con facilidad y total impunidad equipos situados en cualquier organización . Además, son cada vez más los equipos conectados permanentemente a Internet que no disponen de un responsable de administración y gestión, y que están configurados por defecto para ofrecer una serie de servicios que no se suelen emplear.

Estos motivos nos han llevado a plantear unas recomendaciones generales de seguridad, al igual que se hace en otras áreas, para tratar de limitar el número y alcance de estos incidentes.

Somos conscientes de que estas recomendaciones no se podrán implantar en su totalidad, que llevarán algo de tiempo y que se deberán debatir antes de ser de uso común en RedIRIS, pero esperamos que este borrador aporte su "granito de arena" a este proyecto.

No creemos que la seguridad tenga que ser algo perteneciente a un área determinada dentro de los servicios informáticos de las organizaciones, sino que prácticamente depende de todos los niveles de servicio.

Nosotros a la hora realizar este borrador lo hemos clasificado en diversos niveles:

Directivas generales: Lo primero que creemos que se echa en falta en gran parte de las organizaciones afiliadas son unas directivas generales sobre seguridad, indicando a los usuarios internos y externos de la organización cuáles son los servicios y recursos que se están ofreciendo, los métodos de acceso, etc, y hasta formas de organización de los servicios que proporcionen más seguridad a las organizaciones.

Seguridad en nivel de Red: En esta sección trataremos sobre todo las medidas para evitar los ataques desde el exterior de una organización, comentando los filtros que se deberían instalar en los routers externos de las mismas para evitar diversos ataques típicos que se producen.

Seguridad en nivel de Sistema: Comentaremos aquí diversos aspectos de configuración de los equipos, centrándonos sobre todo en aquellos equipos multiusuario (equipos de correo, servidores de ficheros, etc).

Capítulo 2

Recomendaciones Generales

En esta sección trataremos aspectos generales organizativos que creemos pueden ayudar a la hora de aumentar la seguridad de las instituciones afiliadas.

El primero de estos aspectos, que creemos que se echa en falta en gran parte de las organizaciones afiliadas, es el relativo a las políticas de seguridad. Muchas organizaciones no tienen establecida una política de seguridad en la que se indiquen los derechos y obligaciones, o las sanciones en las que pueden incurrir los usuarios. En las páginas del CERT (http://www.rediris.es/cert/docs/poliseg.es.html) se indican los aspectos que debería contemplar una política de seguridad.

En organizaciones pequeñas todavía es frecuente emplear el mismo equipo como servidor de Internet (DNS, FTP, WWW, correo, etc) y como equipo multiusuario. Sin embargo, los problemas que pudieran derivarse de un robo de claves de usuario o de las acciones de los propios usuarios de la organización serían fácilmente evitables si los mencionados servicios de Internet estuvieran instalados en un equipo al que sólo tuvieran acceso un grupo reducido de usuarios.

Otro aspecto en el que creemos que se debe hacer un énfasis especial es en la definición de los puntos de contacto de cada organización. NO EXISTE ahora mismo en muchas instituciones un responsable definido para el área de seguridad, o incluso una dirección de correo a la que se pudieran enviar los avisos y notificaciones de seguridad. Por lo tanto nos parece muy importante el que exista un alias de correo, redirigido después a cuentas de usuarios finales, para poder contactar con los responsables de seguridad de cada institución, al igual que debe existir el alias de correo *postmaster* para tratar los asuntos relacionados con el correo electrónico.

En aquellas organizaciones en las que por su complejidad interna existan varios responsables de "área", es evidente que también deberían contar con este tipo de dirección. Así se evitaría tener que contactar con el PER de una institución por teléfono para advertirle de un incidente, y que éste lo tenga que reenviar al responsable de un equipo, el cual despúes vuelve a notificarlo al PER, con lo que al final no existe un seguimiento real del incidente.

Si una organización delega en un grupo la gestión de los servicios de comunicaciones para una sección, es lógico pensar que el personal de RedIris tiene que conocer esta situación para poder contactar con los responsables de este departamento cuando sea preciso.

Por último hay que destacar las dificultades que están surgiendo en las instituciones que disponen de aulas o espacios de uso compartido, desde donde surgen ataques de denegación de servicio y barridos de puertos y redes hacía otras localizaciones, sin que muchas veces exista un control sobre quién ha sido el usuario que ha realizado la acción. Creemos que el acceso a estas instalaciones debe realizarse de una forma más controlada.

Capítulo 3

Seguridad en nivel de red

Los ataques a nivel de red siguen siendo bastante frecuentes. Aunque las pilas TCP/IP de los distintos sistemas operativos son cada vez más robustas, todavía son frecuentes los ataques de denegación de servicio en servidores NT y Unix debidos al empleo de generadores de datagramas IP erróneos o complicados de procesar.

Es también frecuente el empleo de herramientas automatizadas de escaneo y comprobación de vulnerabilidades en redes, así como la utilización de programas especifícos que explotan una determinada vulnerabilidad de un servidor o servicio concreto para atacarlo.

En esta sección vamos a tratar sobre todo las medidas que creemos que se deben establecer en las organizaciones mediante el filtrado de diversos protocolos en los routers de acceso, para así evitar el acceso desde fuera a estos servicios. Estas medidas no serán efectivas contra ataques internos, salvo que se apliquen medidas internas concretas en aquellas organizaciones que tienen un direccionamiento plano de red para su red física, pero permitirán como mínimo reducir ciertos problemas como el SPAM o los ataques contra servicios bien conocidos como NFS, NetBios, etc. Además permitirán que incluso si los usuarios finales activan esos servicios en sus máquinas, éstos no serán accesibles desde el exterior, evitando así múltiples problemas.

3.1 Filtrado de paquetes

Aunque la seguridad a nivel de sistema sigue teniendo una importancia vital, los fallos en varios servicios TCP/IP y la existencia de protocolos defectuosos hace imprescindible el uso de filtros en el nivel de red, que permitan a una organización restringir el acceso externo a estos servicios. De esta forma, sólo aquellos servicios que deban estar accesibles desde fuera del área local serán permitidos a través de filtros en los routers. Además es importante que estos filtros determinen las condiciones de acceso a los servicios permitidos. Aunque el filtrado es difícil de implementar correctamente, queremos dar algunos consejos que ayudarán a las organizaciones a implementar sus propios filtros en función a sus necesidades y a su topología de red concreta. En particular, se recomienda encarecidamente que se filtren los siguientes servicios si no es necesario su acceso desde fuera de una organización concreta:

Nombre	Puerto	Tipo de conexión	Servicio
echo	7	tcp/udp	Eco: Devuelve los datos que se reciben
systat	11	tcp	Información del sistema
netstat	15	tcp	Información sobre la red
chargen	19	tcp/udp	Generador de caracteres continuo
SMTP	25	tcp	Puerto de correo
domain	53	tcp/udp	Servidor de Nombres (DNS)
bootp	67	udp	Arranque de estaciones remotas sin disco
tftp	69	udp	Arranque de equipos remotos, carga de configuraciones
link	87	udp	
supdup	95	udp	
sunrpc	111	tcp/udp	Servicio de RPC (portmapper)
news	119	tcp	Servidores de News (deberían estar ya filtrados en todos los routers de las organizaciones afiliadas a RedIRIS)
NetBios	137-139	udp/tcp	Servicios NetBios sobre TCP/IP (Windows)
snmp	161	udp	Gestión remota de equipos mediante SNMP
xdmpc	177	udp	Llegada de correo
exec	512	tcp	Ejecución remota de comandos (rexec)
login	513	tcp	Acceso remoto a un sistema (rlogin)
shell	514	tcp	Shell remoto
biff	512	udp	
who	513	udp	Información sobre los usuarios que hay conectados en un equipo remoto
syslog	514	udp	Almacenamiento de los logs de los sistemas en remoto
uucp	540	tcp	Envío de ficheros y mensajes mediante uucp, actualmente en desuso
route	520	udp	Información sobre enrutamientos
openwin	2000	tcp	
NFS	2049	tcp/udp	Sistema de ficheros remotos de Sun y Unix en general
X-Windows	6000 +n	tcp	Servidor X-Windows

CHARGEN y ECHO: Puertos 11 y 19 (TCP/UDP) Es muy importante para evitar ataques de denegación de servicio por puertos UDP (http://www.cert.org/advisories/CA-96.01.UDP_service_denial.html), filtrar a nivel de router o firewall los servicios "chargen"y "echo"y en general todos los servicios UDP que operen por debajo del puerto 900, con excepción de aquellos que se necesiten explícitamente.

Sistema de nombres de dominio (DNS): Puerto 53 (TCP/UDP) Es necesario filtrar el acceso desde el exterior a todos los equipos excepto a los servidores de DNS primarios y secundarios establecidos en una organización. [1]

TFTPD: Puerto 69 (UDP) En general cualquier servicio UDP que responde a un paquete de entrada puede ser víctima de un ataque de denegación de servicio (DoS). Un acceso no restringido al servicio TFTP permite a sitios remotos recuperar una copia de cualquier fichero "wordreadable", entre los que se pueden incluir ficheros críticos como ficheros de configuración de routers y ficheros de claves. Es por ello, que aquellas organizaciones que no necesiten usar este servicio deberían filtrarlo y aquellas que necesiten usarlo, lo configuren adecuadamente teniendo en cuenta las medidas de seguridad a nivel de aplicación.

Comandos r de BSD UNIX: Puertos 512, 513 y 514 (TCP) Los comandos r incrementan el peligro de que sean interceptados contraseñas en texto plano cuando se presenta un ataque utilizando sniffers de red, pero lo más importante es que son una fuente bastante frecuente de ataques y vulnerabilidades. Filtrando los puertos 512, 513 y 514 (TCP) en el hardware de red se evitará que personas ajenas a su organización puedan explotar estos comandos, pero no lo evitará a personas de su propia organización. Para ellos, aconsejamos el uso de otras herramientas como el ssh, uso de versiones seguras de los comandos "r" (Wietse Venema's logdaemon), uso de tcp_wrapper para proporcionar una monitorización del acceso a estos servicios, etc...

SunRPC y NFS: Puertos 111 y 2049 (TCP/UDP) Filtrar el tráfico NFS evitará que sitios ajenos a su organización accedan a sistemas de archivos

[1] Consultar la documentación relativa a la configuración del servidor de DNS en la seguridad de sistemas

exportados por máquinas de su red, pero como ocurría en el caso anterior, no se evitará que se realicen ataques desde dentro del área local. La mayoría de las implementaciones NFS emplean el protocolo UDP, por lo que es posible, en algunos casos, el envío de peticiones NFS falsificando la dirección origen de los paquetes (IP-spoofing http://www.cert.org/advisories/CA-1996-21.html. Es por tanto muy aconsejable la instalación de las últimas versiones actualizadas de los servidores y clientes NFS que tienen en cuenta estas características.

SMTP Puerto 25 (TCP) Es importante configurar el router de manera que todas las conexiones SMTP procedentes de fuera de una organización pasen a una estafeta central y que sea desde ésta desde donde se distribuya el correo internamente. Este tipo de filtros permitirá que no existan puertos 25 descontrolados dentro de una organización, ya que suelen ser foco de importantes problemas de seguridad, además de un registro centralizado de información, que podrá ayudar a la hora de detectar el origen de intentos de ataque. El administrador del sistema o el responsable de seguridad sólo se tendrá que preocupar de tener actua lizado este servidor para evitar ataques aprovechando vulnerabilidades o fallos bien conocidos en los mismos. Para obtener más información sobre diseño de un servicio de correo electrónico puede consultar la siguiente página:
http://www.rediris.es/mail/coord/sendmail/estafeta.html.

NetBios. Puertos 137, 138 y 139 (TCP/UDP) Estos puertos son los empleados en las redes Microsoft (Windows para Trabajo en Grupo, dominios NT, y LANManager), tanto para la autenticación de usuarios como para la compartición de recursos (impresoras y discos). Es frecuente el permitir el acceso global a uno de estos dispositivos, ignorando que es posible el acceso a estos recursos desde cualquier dirección de Internet.

SNMP Puerto 161 (UDP/TCP) Muchos equipos disponen en la actualidad de gestión SNMP incorporada. Dado que estas facilidades de gestión no suelen necesitar accesos externos, se deben establecer filtros a nivel de router que eviten que se pueda obtener información sobre los dispositivos (routers, hubs, switches) desde el exterior o incluso se gestionen los equipos en remoto.

Filtros de datagramas IP Por otro lado, para prevenir los ataques basados en bombas ICMP, se deben filtrar los paquetes de redirección ICMP y los paquetes de destino ICMP inalcanzables. Además, y dado que actualmente el campo de opciones de los paquetes IP apenas se utiliza, se pueden filtrar en la totalidad de las organizaciones los paquetes de origen enrutado (source routed packets). Estos paquetes indican el camino de vuelta que ha de seguir el paquete, lo cual es algo inseguro, ya que alguno de los puntos intermedios por los que pase el paquete puede estar comprometido.

Si una organización determinada no necesita proveer de otros servicios a usuarios externos deberían filtrarse igualmente esos otros servicios. Por poner un ejemplo, filtrar conexiones POP e IMAP a todos los sistemas excepto a los que deben ser accesibles desde el exterior. Esta misma regla es aplicable a otros servicios como WWW, SMTP, NTP, etc...).

Con el protocolo IP que actualmente está mayoritariamente en uso, es casi imposible eliminar el problema del IP-spoofing (falsificación de la IP). Sin embargo, se pueden tomar algunas medidas que reducirán el número de paquetes de este tipo que entran y existen en una red local. Actualmente, el mejor modo de realizar esto es restringir la entrada en el interfaz externo (filtro de entrada), no permitiendo que un paquete entre a nuestra red si tiene la dirección origen de la red interna. De la misma forma, se deberán filtrar los paquetes salientes que tengan una dirección origen distinta a la correspondiente a la red interna (con esto último se evitarán ataque de IP-spoofing originados desde nuestra red). La combinación de estos dos filtros prevendrán que un atacante de fuera de nuestra red envíe paquetes simulando hacerlo desde dentro de nuestra red, así como que paquetes generados dentro de nuestra red parezcan haber sido generados fuera de la mismas.

En la entrada al interfaz interno de una organización se deben filtrar los bloques de paquetes con las siguientes direcciones:

- Redes Broadcast: Para evitar que su organización sea utilizada como intermediaria en un ataque de denegación de servicio de tipo *smurf* (http://www.cert.org/advisories/CA-1998-01.html) es necesario bloquear el tráfico ICMP a las direcciones de broadcast (bits dedicados a hosts todos a uno) y de red (bits dedicados a hosts todos iguales a cero).

- Su área local.

- Números de red privada reservados: No se debe recibir tráfico desde o hacia las siguientes direcciones a través de los routers puesto que se trata de redes privadas reservadas:
  - 10.0.0.0 - 10.255.255.255 10/8 (reservada)
  - 127.0.0.0 - 127.255.255.255 127/8 (loopback)
  - 172.16.0.0 - 172.31.255.255 172.16/12 (reservada)
  - 192.168.0.0 - 192.168.255.255 192.168/16 (reservada)

3.2 Configuración de las pilas TCP/IP en equipos finales

Gran parte de los ataques de denegación de servicio (DoS) se producen debido a fallos en las implantaciones de las pilas TCP/IP en los sistemas operativos. Así, son famosos los ataques de denegación de servicio mediante el envío de datagramas IP con información ICMP errónea, que provocan el reinicio del equipo, o los ataques mediante inundación SYN y FIN, impidiendo el normal funcionamiento de los servidores. En la medida de lo posible, se debe revisar la configuración de estos sistemas, en especial la configuración de "reenvío de datagramas IP" (*ip-forwarding*), que permite que un sistema funcione como un router.

3.3 Monitorización de routers y equipos de acceso

Hace algunos años era frecuente el empleo de equipos de acceso (servidores de pools de módems, routers de acceso, etc.) para la conexión a los servidores de las organizaciones desde el domicilio de los usuarios. Con la aparición de Infovía y los proveedores de acceso a Internet, el uso de estos sistemas ha ido disminuyendo, aunque siguen estando operativos en muchas instituciones.

Tanto estos equipos como los routers de interconexión y cualquier dispositivo (switch, concentrador ATM, etc. que disponga de esta opción), deben estar monitorizados. Los syslog deben configurarse para ir enviando los mensajes de la consola a un equipo central donde se deben almacenar durante un periodo razonable de tiempo, de forma que se puedan comprobar los intentos de conexión no autorizados y las caídas que se producen en estos equipos. Esta monitorización es muchas veces muy sencilla de establecer y la recepción y almacenamiento de los registros no requiere mucha carga del procesador.

En instalaciones con mucho equipamiento de red puede ser recomendable el empleo de alguna herramienta de monitorización SNMP de los equipos, de forma que las incidencias que vayan ocurriendo sean notificadas en tiempo real a los administradores de la red.

Es necesaria la instalación de versiones recientes de los sistemas operativos de estos equipos, puesto que muchas instalaciones disponen de versiones antiguas susceptibles a ataques de denegación de servicio que pueden ser fácilmente evitables si se actualizan periódicamente los sistemas.

3.4 Separación de las redes y filtros anti-sniffing

Gran parte de los ataques que se producen son debidos a la obtención de las claves empleando un programa de sniffing en una red ethernet. En muchas ocasiones, la separación de las redes y el empleo de switches y routers hace falta para permitir una mayor descongestión del tráfico interno de una organización, pero además es muy necesario para lograr una mayor seguridad dentro de esta.

Las salas de acceso general (bibliotecas, salas de prácticas comunes, aulas de estudiantes, etc.) deben estar separadas mediante puentes (bridges) o conmutadores (switches) del resto de la red, para evitar que se puedan obtener, mediante sniffers, claves de acceso de otros grupos de usuarios. En general los equipos que necesiten el empleo de sistemas inseguros de transmisión de claves deberían estar aislados de la red, de forma que estas claves no se transmitan por toda la organización.

Hay que considerar además las posibilidades de gestión y consola remota que disponen muchos hubs y switches: hay que cambiar las claves por defecto que suelen tener estos equipos y deshabilitar la gestión remota de éstos si no se va a hacer uso de ella (SNMP, consolas remotas, servidor de HTTP...). Consulte la ponencia presentada en los Grupos de Trabajo de Barcelona "Implantación de un sistema de securización global a nivel de red", (http://www.rediris.es/rediris/boletin/46-47/ponencia8.html).

Hay que indicar que existen ya versiones de sniffers para los sistemas Windows, siendo posible muchas veces la obtención de contraseñas de acceso a sistemas de ficheros remotos de Netbios, pudiendo modificar fácilmente cualquier aplicación existente en estos servidores. Además en muchos servidores Samba la clave de conexión de Windows coincide con la clave del usuario, por lo que estas medidas anti-sniffing se deben aplicar a cualquier protocolo que circule por la red.

Capítulo 4

Recomendaciones en nivel de sistema

Las configuraciones establecidas por defecto en muchos sistemas operativos no son las más adecuadas desde el punto de vista de seguridad. Además, el desconocimiento y la desinformación de los responsables de estos equipos es motivo frecuente de problemas de seguridad. En este apartado vamos a comentar diversas medidas que se deberían adoptar en los sistemas para evitar gran parte de estos problemas.

4.1 Configuración de equipos Unix

4.1.1 Actualización y control de fallos

Los ataques con más éxito en los sistemas informáticos se basan en aprovechar vulnerabilidades en el software que no ha sido actualizado a la última versión facilitada por el fabricante, o que no ha sido parcheado convenientemente. Esto afecta tanto al software de red de grandes máquinas y sistemas operativos, como al software de PC de usuarios.

Esta tarea es laboriosa porque supone mantenerse al día de la evolución de los productos, así como conocerlos a fondo para poder configurarlos correctamente. La mayoría de los vendedores mantienen listas con los parches recomendados (Sun, IRIX, etc...). A la hora de instalar un parche, se recomienda comprobar la firma digital, si existiera, y el checksum para verificar que se trata de una copia válida. El MD5 comprueba la integridad y la no alteración del paquete, y la firma PGP la autenticidad de su autor.

Es muy importante estar al día y revisar el software que se utiliza, especialmente aquel que tenga que ver con la conectividad a Internet, administración de servicios de red, etc... y actualizarlo o parchearlo con las últimas actualizaciones disponibles. A menudo no resulta buena idea utilizar la última versión disponible, sino la penúltima, ya que al ritmo al que se lanzan nuevas versiones de productos, la última, con casi toda seguridad, no habrá sido puesta a prueba en su fase de diseño ni ha sido suficientemente validada por los usuarios. A veces, merece la pena esperar un período de tiempo, aunque eso sí, no con la primera versión del producto.

Por último, comentar que no es suficiente con instalar la última versión o actualización disponible, sino que es necesario configurarla convenientemente, de manera que se cierren los resquicios que puedan dejar las instalaciones por defecto. Esta corrección es importante no sólo en los sistemas operativos, sino también en el software en general.

4.1.2 Directivas generales

En esta sección, daremos algunas ideas a los administradores sobre la configuración de los equipos Unix. Algunas de las directivas generales a la hora de configurar un sistema teniendo en cuenta la seguridad se pueden sintetizar en los siguientes puntos:

- La presencia de archivos .rhosts y /etc/hosts.equiv merece especial cuidado, pues garantizan el acceso a la máquina sin necesidad de autenticación. Si no es necesario el uso de comandos *r* (aconsejado en capítulos anteriores, e insistentemente por IRIS-CERT), no se necesita la presencia de estos archivos al no ser una alternativa segura a telnet. Se recomienda usar clientes ssh, ampliamente descritos ya en este documento.

- Se puede establecer qué terminales son seguros, y por lo tanto desde qué terminales se puede conectar el usuario root. En los terminales declarados como no seguros el usuario antes de llegar a ser root, necesitará conectarse utilizando una cuenta sin privilegios en el sistema y después utilizar el comando "su"para cambiar a root, lo que añade un nivel extra de seguridad.

- Desactivar IP forwarding y source routing. Es especialmente importante en el caso de estar usando una Sun como host bastión o como "dual-homed".

- Es importante deshabilitar la posibilidad de ejecución de código en pila de usuario, lo que evitará algunos problemas de "buffer-overflow"(pero no todos). En el caso de máquinas Solaris lo podemos hacer incluyendo en el fichero de especificación del sistema "/etc/system"las líneas:

  ```
  set noexec_user_stack=1
  set noexec_user_stack_log=1
  ```

  y reiniciando a continuación.

- Evitar que el correo del root se almacene sin que nadie lo lea. Para ello establezca un archivo ".forward"en el home del root para redirigir el correo a una cuenta real en el sistema. Así mismo, sería necesario asegurarse que estos archivos, si existen en los directorios home de los usuarios, no ejecuten ningún comando.

- Desactivar la ejecución de comandos en los dispositivos montables por los usuarios.

- Separar las máquinas de los usuarios de aquellas que ofrecen algún servicio a la comunidad (servidores), y restringir en la medida de lo posible el acceso a las mismas.

- El administrador debe prevenir posibles escuchas en la red. Un "sniffer"escucha todo lo que pasa por una puerta ethernet, incluyendo contraseñas de cuentas de usuario, de superusuario, claves de POP, etc.. Para evitarlo, se recomienda el uso de Shell Seguro (ssh) (http://www.ssh.org/) u otros métodos de cifrado de contraseñas.

- Revisar el path de la cuenta root en los ficheros de inicio (.login, .cshrc, .profile, ...). El comando path o la variable de entorno PATH definen los directorios de búsqueda de los ejecutables. El directorio ".", es decir, el actual, nunca debe aparecer en el path del root.

4.1.3 Seguridad en sistemas de archivos

El aspecto más vulnerable en la protección de archivos son los modos de acceso SUID y SGID. Se aconseja realizar frecuentemente una auditoría de los mismos, monitorizando los cambios, puesto que son ficheros especialmente explotados por intrusos potenciales. Algunas sugerencias son:

- Los sistemas Unix/Linux proporcionan otras maneras de limitar el acceso a varios recursos del sistema a usuarios que no sean el usuario root, como las cuotas de disco, la limitación de los recursos del sistema por proceso y/o usuario, y la protección para los subsistemas restringiendo el acceso a las colas de procesos batch y de impresión para los usuarios no autorizados.

- Si no hay mas remedio que usar NFS, se debe configurar de la forma más restrictiva posible. En el fichero /etc/exports se especifica a quién se exporta y cómo se exporta un sistema de ficheros (de sólo lectura, sin permiso de escritura al root, etc.). El comando "showmount"permite verificar que el fichero de configuración /etc/exports es correcto.

- Establecer en el /etc/profile una umask para los usuarios lo más restrictiva posible (022, 033 ó incluso 077). La máscara del root debe ser 077.

- No usar Samba en la medida de lo posible. Si es necesaria su utilización, se debe configurar muy restrictivamente el fichero /etc/smb.conf.

- Asegúrese de que todos los ficheros que cuelgan del directorio /dev son ficheros especiales y que del mismo modo no existen archivos de dispositivo fuera de la estructura de /dev.

- Considere eliminar el acceso a lectura de todos aquellos archivos que no necesiten tener dicho acceso. También es aconsejable revisar los ficheros y directorios escribibles por todo el mundo.

- Asegúrese de que el usuario root es el propietario de los directorios /etc, /usr/etc, /bin, /usr/bin, /sbin, /usr/sbin, /tmp y /var/tmp. Además, los directorios /tmp y /var/tmp deben tener el *sticky bit* establecido.

- AUSCERT recomienda que todos los archivos ejecutados por el usuario root deben ser propiedad de dicho usuario, no ser escribibles ni por el grupo ni por otros (es decir, con modo 755 o mejor) y localizados en un directorio donde cada directorio en el path sea propiedad del usuario root. En este sentido, una práctica general consistiría en examinar la protección de los ficheros y directorios antes y después de instalar software o de ejecutar utilidades de verificación.

- Es recomendable comparar las versiones de programas en el sistema con una copia válida de las mismas (por ejemplo del CD-ROM). Hay que tener especial cuidado con las copias de seguridad, pues pueden contener ficheros alterados o Caballos de Troya.

- Los Caballos de Troya pueden tener el mismo "standard checksum"y timestamp que la versión original. Por esto, el comando de UNIX sum(1) y el timestamp asociado a los programas no es suficiente para determinar si estos han sido alterados o reemplazados. El uso de cmp(1), MD5, Tripwire y otras utilidades para generar un checksum criptográfico son necesarios para detectar estos caballos de troya.

4.2 Filtrado de servicios en equipos Unix

Para evitar riesgos innecesarios, se deben configurar TODAS las máquinas de una organización para que ofrezcan únicamente los servicios que se tenga en mente ofrecer y no otros. Esto disminuirá considerablemente el riesgo de que estas máquinas sean atacadas aprovechando servicios completamente descuidados y que en muchas ocasiones no se es consciente que se están ofreciendo.

Es necesario asegurarse de que no existen debilidades en los archivos de configuración de los servicios ofrecidos y que los servicios se ofrezcan sólo al conjunto de usuarios para los cuales se diseñó.

4.2.1 Servicios dependientes de inetd

El archivo inetd.conf contiene una lista con todos los servicios que el demonio inetd[1] invoca cuando recibe una petición sobre un socket.

[1] El proceso inetd es un "superservidor configurable", empleado para escuchar en varios puertos simultáneamente y lanzar el programa adecuado para cada servicio. Para más información, consulte las páginas de manual de este comando.

Por defecto, a la hora de instalar el sistema operativo, se establece un archivo inetd.conf con gran cantidad de servicios activados por defecto, que en la grandísima mayoría de los casos no son necesarios. Es completamente necesario revisar este archivo con el fin de comentar las líneas de todos aquellos servicios que no sean necesarios explícitamente, y que en muchas ocasiones son causa de ataques y vulnerabilidades.

Nuestra recomendación es comentar todos los servicios que se lanzan desde el inetd.conf anteponiendo un carácter #äl principio de cada una de las líneas. Una vez hecho esto, se pueden descomentar (quitando el carácter "#") aquellos servicios que sean necesarios en esa máquina en concreto.

Para que los cambios realizados en este archivo de configuración tengan efecto, recuerde reiniciar el proceso inetd.

Puesto que en muchos casos, cuando se ofrece un servicio, éste está dirigido a un sector de la comunidad de Internet, es muy útil contar con algún mecanismo que permita rechazar conexiones dependiendo de su origen y/o de su ident, y que proporcione además, una monitorización del acceso. En este contexto, recomendamos la instalación de *tcp_wrapper* (http://www.rediris.es/cert/doc/docu_rediris/wrappers.es.html), que se puede descargar en el FTP de RedIRIS. El tcp_wrapper (tcpd) actúa de intermediario transparente en las conexiones TCP, añadiendo un nivel extra de registro de conexiones, control de acceso y acciones configurables por conexión.[2]

4.2.2 Servicios dependientes de RPC

En general, los clientes de los servicios dependientes de RPC (Remote Procedure Control) hacen una llamada al gestor de RPC (rpcbind en Solaris, portmap en Linux, pero siempre el puerto 111/tcp), para averiguar donde están los servicios de cada procedimiento.

Esta información se puede ver como usuario, con el comando "rpcinfo -p", que implementa una llamada al procedimiento remoto 'dump'. Si alguno de los servicios que aparecen al ejecutar este comando no son necesarios, será imprescindible desactivarlos en los scripts de inicialización del sistema, lugar desde donde son lanzados.

En cuanto al tcp_wrapper, no puede usarse para controlar el acceso a estos servicios, pero si se puede usar para controlar y registrar el acceso al

[2] En servidores que generan una carga elevada y que tienen su propio sistema de control de acceso y de históricos no es necesario el empleo de tcp_wrapper.

gestor RPC. Para hacerlo, es necesario tratar rpcinfo/portmap como un servidor independiente que implementa un servicio en el puerto 111. En Linux, portmap ya está compilado de esta manera, por lo que el acceso se puede controlar directamente con los archivos hosts.allow y hosts.deny. En Solaris, se requiere compilar una versión especial del rpcbind y enlazarlo con la biblioteca libwrap.a (Solaris: /usr/local/lib/libwrap.a, Linux: /usr/lib/libwrap.a).

4.2.3 Servicios arrancados en los scripts de inicio del sistema operativo

Aparte de los servicios dependientes de RPC y de los dependientes de inetd, comentados con anterioridad, en el proceso de instalación del sistema operativo en una máquina se activan una serie de servicios por defecto que se ejecutan desde el /etc/rc* correspondiente (por ejemplo el smtp, o el domain) que en la mayoría de los casos no son necesarios. Si éste es el caso, recomendamos que sean desactivados y que se modifiquen los scripts de inicio para que en subsiguientes arranques de la máquina no se vuelvan a lanzar.

4.3 Política de contraseñas

Sin duda, uno de los métodos más habituales usados por los hackers para comprometer un sistema es el robo de contraseñas. Robando un nombre de usuario y su contraseña correspondiente, un intruso puede, reduciendo las probabilidades de ser detectado, ganar acceso a un sistema, modificarlo, y usarlo como lanzadera para atacar a otros sistemas. La mayoría de los sistemas no tienen ningún mecanismo de control de las contraseñas que utilizan sus usuarios y en la mayoría de los casos existe por lo menos una contraseña en el sistema que puede ser fácil de descubrir, comprometiendo la seguridad del sistema completo.

La protección de las contraseñas es uno de los principios más importantes en seguridad, por lo que es necesario que las organizaciones posean una política de contraseñas bien definida.

Las técnicas utilizadas por los crackers para obtener contraseñas ajenas son muy variadas (desde aprovechar vulnerabilidades en ciertas aplicaciones hasta utilizar "Caballos de Troya", usualmente enmascarados en el programa /bin/login). Si un intruso obtiene un fichero passwd de una máquina ajena, normalmente realiza una copia del mismo a otra máquina y ejecuta programas crackeadores contra él, que son relativamente rápidos y que realizan ataques de fuerza bruta, de diccionario o híbridos sobre las contraseñas robadas.

A continuación daremos algunas directivas a tener en cuenta por los administradores de sistemas o responsables de seguridad para implementar una política de contraseñas adecuada en sus organizaciones.

4.3.1 Contraseñas débiles

- La primera directiva, y en nuestra opinión la más importante, es desarrollar una guías que ayuden a los usuarios a la hora de escoger contraseñas lo suficientemente robustas para que no sean vulnerables a los ataques de diccionario o de fuerza bruta que suelen realizar la mayoría de las utilidades diseñadas para romper contraseñas. Estas medidas vienen ampliamente descritas en multitud de documentos por lo que no creemos necesario que sean repetidas aquí, pero a modo de ejemplo: no se deben escoger palabras del diccionario, palabras de estén relacionadas con el usuario (nombre de la mujer o marido, domicilio, fecha de nacimiento, etc...), utilizar contraseñas con una longitud mínima de 8 caracteres, no usar el nombre de usuario o una variante, como el nombre de usuario al revés, etc.

- Informar a los usuarios de que no almacenen información sobre su cuenta/contraseña en archivos de texto en ningún sistema.

- Si se tiene más de una cuenta en distintos sistemas no es aconsejable utilizar la misma contraseña en todas, pues si la contraseña quedara comprometida en una máquina, lo quedaría igualmente en el resto.

- Cuando se utiliza el servicio de finger (puerto 79 tcp/udp) para interrogar a un servidor, a menudo éste revela más información sobre sí mismo y sus usuarios de la que sería deseable (el shell que está utilizando cada usuario, su directorio personal, el grupo al que pertenece, y lo que en este caso es más importante, el nombre del usuario en la máquina, con lo que el atacante ya poseería la mitad de la información que necesita para entrar en un sistema). Debido a que además suele proporcionar información sobre la hora del último login, un atacante podría confeccionar patrones de trabajo de los distintos usuarios. En definitiva, se trata de información demasiado valiosa para distribuirla sin control, por lo que es aconsejable eliminar este servicio de las máquinas si no es estrictamente necesario su uso.

- Utilizar con cierta frecuencia programas tipo crack para chequear la robustez de las contraseñas del sistema y de esta forma encontrar claves débiles forzando el cambio de las mismas. Es mejor que nosotros conozcamos antes que el atacante la debilidad de nuestras contraseñas.
- Establecer un política de cambios periódicos de contraseñas (sobre todo en las máquinas más importantes y las de cuentas privilegiadas). Además es aconsejable no reutilizar contraseñas antiguas.

4.3.2 Cuentas sin contraseña o contraseñas por defecto.

- Cambiar todos las contraseñas instalados por defecto en el proceso de instalación del sistema operativo.
- Escanear el fichero de contraseñas (/etc/shadow o /etc/passwd) periódicamente en busca de cuentas con UID igual a 0 (reservada para el usuario root).
- Revisar el fichero de contraseñas en busca de cuentas nuevas de las que no se tiene conocimiento y que en la mayoría de los casos son indicativo de intrusión.
- No permitir la existencia de cuentas sin contraseña.
- Eliminar cuentas de usuarios que se hayan dado de baja en la organización o que no se estén utilizando.
- Es aconsejable el uso de programas como "noshell" (ftp://ftp.rediris.es/mirror/coast/tools/unix/noshell) que permiten al administrador obtener información adicional sobre intentos de conexión a cuentas canceladas o bloqueadas en una máquina. Utilizando este mecanismo, cada intento de conexión queda registrada, mediante correo electrónico o syslogd, dando información sobre el usuario remoto, la dirección IP, el día y la hora del intento de login y el tty utilizado en la conexión.

4.3.3 Contraseñas reutilizables

- Reducir o eliminar la transmisión de contraseñas reutilizables en texto claro sobre la red. De esta forma se evitará que las contraseñas sean capturadas por lo que se denomina "packet sniffers"[3].

  Utilice contraseñas de un sólo uso (one-time passwords)(S/Key, Secure Net Key, Secure ID, etc...) para el acceso autenticado desde redes externas o para acceder a recursos sensibles como routers, servidores de nombres, etc.

- Si se trata de sistemas UNIX, recomendamos el uso del fichero /etc/shadow, o lo que es igual, un segundo fichero que contiene las contraseñas cifradas y es sólo accesible por el usuario root, quedando el /etc/passwd con una "x"en el lugar donde deberían aparecer las contraseñas cifradas. La mayoría de sistemas Linux, por ejemplo, vienen con PAM configurado. PAM (Pluggable Authentication Modules) es un método mucho más potente de gestión de seguridad y contraseñas que se adapta perfectamente a cualquier entorno UNIX.

- Si su sistema tiene la posibilidad de aplicar una serie de reglas en la introducción de palabras clave, es aconsejable que lo utilice. Por ejemplo, en el caso de un sistema Solaris, en el archivo /etc/default/passwd, o en un sistema con PAM, en el fichero /etc/pam.conf, se pueden establecer algunos valores por defecto, como son el número mínimo de caracteres que debe tener un contraseña, el máximo período de tiempo en el cual es válida, el mínimo período antes de que la contraseña pueda cambiarse, etc.

4.4 Política de cuentas

Desde el punto de vista de la seguridad, el fichero /etc/passwd tiene una importancia vital. Si tiene acceso a este archivo, lo puede alterar para cambiar el contraseña de cualquier usuario, o incluso tener privilegios de superusuario cambiando su UID a 0.

[3]Herramientas de monitorización y de red que permiten leer toda la información que circula por un segmento de la red, pudiendo así obtener las claves de acceso a las sesiones de terminal(telnet), ftp, http y servicios más comunes

Entre las recomendaciones que podemos dar para establecer una política adecuada de cuentas y grupos en un sistema podemos destacar:

4.4.1 Administración

- Del mismo modo que alentamos a las organizaciones para que posean una política de contraseñas bien definida, es necesario que también dispongan de un formulario para el registro de usuarios bien definido, donde se incluya una sección, que deberá ser firmada por el beneficiario, aceptando las condiciones y responsabilidades que supone tener una cuenta en el sistema. Se deberá contemplar también la posibilidad de acreditación por parte de los mismos.

- Asegurarse de que existen copias de seguridad del área de disco de usuarios siempre que esto sea posible y se dispongan de los medios para hacerlo.

- Considere el agrupar los directorios de los usuarios de una forma lógica, especialmente si espera tener muchos usuarios en el sistema.

- Monitorice los registros en busca de intentos "su"no autorizados o fallidos.

- Compruebe frecuentemente los intentos de conexión no autorizados.

- Establezca una política de asignación de cuotas de disco a usuarios y grupos, así como la preparación de procedimientos de comprobación de los mismos con el fin de controlar que ningún usuario sobrepase el límite de espacio asignado.

4.4.2 Cuentas especiales

- Evitar la existencia de cuentas compartidas.

- Evitar la existencia de cuentas "guestº de invitados. En este sentido, como varios sistemas instalan cuentas para invitados por defecto, será pues necesario desactivar o eliminar del sistema este tipo de cuentas.

- Usar grupos específicos para restringir qué usuarios pueden utilizar el comando "su".

- Comprobar el archivo de contraseñas del sistema una vez haya terminado el proceso de instalación del sistema operativo a fin de asegurarse de que todas las cuentas predeterminadas tienen contraseñas inválidas o han sido desactivadas o eliminadas.
- Eliminar todas las cuentas que permiten únicamente la ejecución de un comando (por ejemplo "sync"). Si se permiten este tipo de cuentas, el administrador deberá cerciorarse de que ninguno de los comandos que ejecutan acepta entradas de línea de comandos y de que no permiten ningún tipo de escape al shell que pueda permitir acceder a un shell de forma externa.

4.4.3 Usuario root

- La contraseña de root ha de ser especial, por lo que es necesario seleccionarla con cuidado, guardarla en lugar seguro y modificarla a menudo.
- Restringir el número de usuarios en el sistema que tienen acceso a esta cuenta.
- Evitar la existencia de archivos .rhosts en el directorio base del usuario root (normalmente /, o en Linux, /root/).
- Evitar la existencia del "."en el path de búsqueda del usuario root y de los administradores.
- Hacer uso de rutas completas para ejecutar órdenes como root.
- Evitar entrar por telnet como root a las máquinas, para así evitar la intercepción del contraseña en texto en claro, que daría a un intruso acceso total al sistema. Queda entonces doblemente marcado como importante el uso de ssh como herramienta indispensable para entrar en las máquinas remotamente.

4.5 Configuración de servicios más usuales

En este apartado vamos a comentar la configuración de algunos de los servicios más usuales que son ofrecidos por las organizaciones, sin entrar en detalle, pues estos temas ya se tratan en los Grupos de Trabajo correspondientes.

4.5.1 Configuración del sistema de correo

El servicio de correo es uno de los más fáciles de configurar en la actualidad, aunque paradójicamente sigue siendo uno de los más problemáticos en lo que a seguridad se refiere. En principio podemos clasificar los equipos en función de su papel en la transferencia del correo, en:

Equipos de usuario : Sistemas que leen y almacenan localmente el correo de uno o varios usuarios. Estos equipos suelen ejecutar un "lector de correo" o agente de usuario para obtener los correos. Suelen ser Pc's con Eudora, Outlook, Netscape o sistemas multiusuarios Unix con mh, pine, mutt, etc. En cualquier caso, para la lectura y almacenamiento de los correos en equipos Unix no es necesario que exista un proceso escuchando en el puerto 25 (SMTP), ni en los puertos de lectura de correo (110 (POP3) o 141(IMAP)).

Equipos de almacenamiento de correo : Equipos en los que se almacena el correo a la espera de ser leído desde los equipos de usuario. Para ello suelen emplear el protocolo pop3 (puerto 110), y en algunos casos emplean imap (141). Para la recepción de correo suelen ejecutar el programa sendmail en el puerto 25, aunque también es posible emplear otros programas, como smap/smapd del fwtk (firewall-toolkit), para no tener que ejecutar sendmail.

Equipos de intercambio de correo : Son los encargados de transferir el correo entre Internet y las organizaciones. Estos equipos deben tener un registro MX en el DNS, y tener establecido su direccionamiento inverso. Además en el router se debe filtrar el tráfico de la organización para que sólamente se produzcan accesos al puerto 25 de las servidores que están definidos en el DNS como MX (Mail eXchanger). Deben ejecutar sendmail, Postfix o un programa similar escuchando continuamente en el puerto 25.

La configuración de este servidor es crucial para el buen funcionamiento del servicio de correo. Se debe instalar la versión más actual del programa sendmail (el suministrado en muchos S.O., salvo Linux o FreeBSD, suele ser bastante antiguo) y configurarlo adecuadamente para que no pueda ser empleado para la distribución de correo basura (SPAM).

Consulte http://www.rediris.es/mail para más información sobre como configurar el servicio de correo en las organizaciones afiliadas a

RedIRIS.

En los equipos de almacenamiento, procure que las cuentas de correo no estén vinculadas directamente a una cuenta del sistema, o que ésta esté bloqueada salvo que sea necesaria. Evite la circulación de las claves en claro mediante el uso de APOP, desactive las cuentas de los usuarios que han dejado de pertenecer a la organización, sustituyendo las cuentas por alias a sus nuevas direcciones de correo.

4.5.2 Configuración del DNS

El servicio de DNS es crucial para la conexión a Internet. Sin embargo en muchas organizaciones no está configurado adecuadamente. Como en el correo, la configuración de este servicio ha sido explicada en el Grupo de Trabajo correspondiente, pero sin embargo creemos que se debe destacar:

1. Tener una versión actualizada del servidor de nombres: Es conveniente actualizar a una versión moderna del servidor. Las últimas versiones son más seguras y permiten establecer filtros y limitaciones en las transferencias de zonas, actualizaciones no solicitadas de datos, etc.

2. Tener configurado el direccionamiento inverso: Muchas instituciones no tienen establecido el direccionamiento inverso para los equipos, lo que dificulta muchas veces el acceso a determinados servicios o la monitorización en los registros.

3. Denegar el acceso a las zonas a otros servidores: Es conveniente que los servidores DNS estén configurados para permitir las transferencias de zona solamente a los servidores que estén definidos como secundarios; así se evita el que se pueda obtener información sobre la topología y configuración de la red desde el exterior.

4. No poner configuraciones de equipos en el DNS: Es posible indicar en los registros de DNS qué sistema operativo, arquitectura hardware, e incluso qué servicios se están ejecutando en la máquina. Esta información se puede emplear para atacar desde fuera de la organización.

5. Configuración en los clientes: En los filtrados de puertos (con tcp_wrapper) o en listas de acceso (en ficheros hosts.allow y hosts.deny), emplear nombres cualificados por completo y no sólo el nombre del equipo,

para evitar que un equipo de otra organización que se llama igual pueda tener acceso al sistema.

6. Aspectos generales de configuración: Como norma general, se debe cumplir que:

   - No se deben configurar los servidores de DNS para que reenvíen las peticiones (hagan "forward") a equipos de RedIRIS.
   - No se deben configurar DNS como secundarios de otra organización, salvo autorización explícita de la otra parte.
   - A ser posible se deben tener dos servidores, primario y secundario, en una misma organización, y por tanto tener especificados ambos equipos como servidores de nombres en la configuración de todos los equipos.

4.5.3 Configuración de los servidores WWW

Los equipos servidores WWW son susceptibles a varios tipos de ataques. Algunas medidas para evitarlos:

1. Dimensione el equipo adecuadamente, para evitar que se produzcan ataques de denegación de servicio (DoS).

2. Instale una versión actualizada del servidor WWW.

3. Salvo que sea necesario, deniegue el uso de CGI's que no sean los empleados por los administradores, elimine los CGI's de prueba, que suelen tener vulnerabilidades de seguridad, y desactive las extensiones del servidor (PHP, Server-Side Includes, servlets de java, etc.) salvo que sean necesarios.

4. En caso de que los usuarios deban programar CGI's, adviértales de los fallos más comunes que pueden existir y como solucionarlos (ftp://ftp.cert.org/pub/techtips/cgimetacharacters).

5. No comparta las páginas de los servidores mediante un sistema de ficheros; emplee un sistema de replicación (wget, mirror, etc.) para realizar el intercambio de las páginas.

4.5.4 Configuración de los servidores FTP

Lo servidores de FTP se han empleado en muchas ocasiones para el almacenamiento de software ilegal, propiciando el abuso de este servicio y muchas veces la sobrecarga de procesamiento de los servidores. Unas recomendaciones generales sobre este servicio son:

1. Instalar una versión del servidor actualizada, y fiable: Las versiones del servidor FTP que vienen con los sistemas operativos comerciales suelen tener pocos parámetros de configuración, y también varios fallos de seguridad. Aún en el caso de que no se vaya a emplear el equipo como servidor de FTP, instale una versión actual de ProFTPd o wuFTPD, que proporcionan bastantes opciones a la hora de configurar el número máximo de conexiones, orígenes de la conexión,etc.

2. En caso de que no se emplee el servicio de FTP anónimo, deshabilitarlo. En caso de que se emplee, salvo que sea necesario no permitir que el usuario FTP tenga permisos de escritura en ningún directorio, y en caso de que tenga que escribir, mantener este directorio en otro sistema de ficheros y evitar que el usuario tenga permisos de lectura y/o creación de directorios, para evitar la creación de repositorios de programas pirateados (http://www.rediris.es/cert/doc/docu_rediris/ftpconfig.es.html).

3. No emplear el servicio de FTP para la transmisión de documentos o ficheros importantes entre equipos, pues las claves de conexión se transmiten en claro. Use en su lugar scp, un reemplazo de rcp que viene con el paquete ssh.

4.5.5 Servidores de ficheros

Hace algunos años era frecuente el empleo de servidores de ficheros en los sistema Unix para la compartición de software entre las diversas estaciones de trabajo. En la actualidad es frecuente encontrar sistemas de ficheros en red, de los que el más conocido es el soporte de NetBios sobre IP (Windows 3.11/9x/ME/NT/2000 principalmente, pero también Unix con Samba). Su incorporación a la red se debe hacer tomando algunas medidas de seguridad.

Servidores NFS

El acceso NFS es frecuente en entornos Unix puros, aunque existen clientes y servidores para Windows 9x/NT/2000 y Novell Netware. Algunos puntos que hay que comprobar a la hora de configurar un servidor NFS deben ser:

1. Emplear servidores/clientes de NFS recientes. Inicialmente los servidores de NFS empleaban UDP como protocolo de transporte, pudiendo alterarse fácilmente las conexiones y realizar ataques simulando ser tanto el origen como el destino de las conexiones. La versión 3 del protocolo NFS permite usar TCP y emplea claves criptográficas para evitar la suplantación de los equipos.

2. No exportar directorios con permisos de escritura. Salvo que sea estrictamente necesario, exportar los sistemas de ficheros con permisos de sólo lectura, de forma que no se pueda escribir en ellos. En caso de que se tengan que exportar sistemas de ficheros con permisos de escritura (directorios personales de usuarios, por ejemplo), no exporte jerarquías de directorios que contengan binarios. En las estaciones clientes evitar montar sistemas de ficheros con permiso de ejecución.

3. Restringir los accesos. No exportar ficheros de configuración, indicar en las opciones de exportación qué equipos son los que pueden montar los recursos, y emplear para ello las direcciones IP o los nombres DNS **COMPLETOS**, para evitar suplantaciones de los equipos.

Servidores NetBios

NetBios se puede emplear sobre diversos protocolos de transporte. Su utilización original empleaba un protocolo denominado NetBEUI, que no permite el enrutado de los paquetes. Sin embargo, ahora mismo NetBios se emplea sobre TCP/IP, en servidores Windows y Unix. Algunos problemas de seguridad que tiene este protocolo son:

- Recomendamos, con toda rotundidad, que Windows 9x/ME se considere comprometido desde el mismo momento en que se arranca. Ninguna versión de Windows 9x/ME debería ser jamás utilizada en cualquier ordenador de una red donde algún recurso necesite ser asegurado.

- En sistemas NT/2000 es preciso tener instaladas las últimas versiones de los parches existentes (Service Packs), ya que las primeras implementaciones de los servidores tienen diversos problemas que abren la puerta a ataques de denegación de servicio (DoS).

- Evitar la exportación de sistemas de ficheros que contengan ejecutables con permisos de escritura, tanto para evitar la suplantación de los binarios como para evitar la proliferación de virus.

- En los servidores NT/2000 tener restringido y especificado siempre el acceso al grupo *Todos* y después permitir los accesos en función de los grupos de usuario. Hay que tener en cuenta que si estos servicios están abiertos a todo el mundo es posible acceder a ellos desde cualquier dirección IP.

- En servidores NT/2000 emplear como sistema de ficheros NTFS, ya que permite especificar derechos individuales a los usuarios. Por ello recomendamos no emplear FAT.

- En el caso de exportar directorios particulares de usuarios, emplear un sistema de cuotas en el servidor, ya sea mediante la instalación del parche correspondiente (Service Pack 4 o superior en NT), empleando las utilidades de Windows 2000, o empleando un equipo Unix con Samba y cuotas de disco, para evitar que un usuario pueda llenar la partición.

- Si se emplea Samba, procurar que las claves de acceso no sean las mismas que las de las cuentas de usuarios en los equipos. Emplear, si es posible, un servidor de autenticación externo (PDC) para evitar que las claves puedan ser obtenidas mediante un sniffer de red o por alguno de los virus y troyanos que estén apareciendo cada vez con más frecuencia en entornos Windows.

4.6 Monitorización de archivos de registro

En Unix existen diversos mecanismos para que quede constancia de toda la actividad de un proceso. El más simple de estos mecanismos es que el proceso en cuestión vaya escribiendo una especie de registro de todo lo que hace en un fichero (lo normal es llamar a estos registros "logs", aunque hay palabras en castellano de sobra, como "registrosº "históricos").

Este método tendría sus limitaciones:

- si dos procesos escriben sus informes simultáneamente al mismo fichero el resultado final puede ser confuso.
- no nos sirve de mucho si queremos almacenar, a medida que se producen, copias de estos informes en otra máquina distinta.
- en algunos casos no nos basta con llevar un registro: hay situaciones de emergencia que deben avisarse inmediatamente.
- lo ideal es que estos ficheros no puedan ser modificados por cualquiera (o poco valor tendrían como registro fiable), pero interesa que cualquier programa tenga capacidad de generarlos, lo cual es una contradicción.

Para solucionar estas limitaciones se creó el sistema 'syslog' de Unix. Está compuesto por lo siguiente:

- Un proceso privilegiado (syslogd), capaz de generar ficheros de log y avisos bassándose en determinadas configuraciones hechas por el administrador.
- Un servicio TCP/IP (514/udp), que permite enviar mensajes syslog de una máquina a otra.
- Un fichero de configuración (/etc/syslog.conf).

4.6.1 Configuración

El fichero /etc/syslog.conf permite especificar qué acciones se llevan a cabo cuando un determinado programa solicita registrar una actividad. Syslog clasifica las actividades a registrar según dos parámetros: subsistema (facility) y severidad.

El subsistema depende de quién ha generado el informe: el núcleo, sistema de correo, news, etc. La severidad indica la prioridad que se le asigna a cada uno de los mensajes, desde los de depuración (debug) hasta los de emergencia y/o pánico. Consulte la página de manual de "syslogd.conf" para más información.

El fichero de configuración permite asignar acciones por subsistema y severidad. Por ejemplo:

```
mail.info /var/log/mail
mail.err /var/log/mail-errores
kern.crit root
kern.emerg *
auth.info /var/log/auth
auth.info @otramaquina
```

Esto significa:

- Los informes relacionados con correo, que tengan severidad "informativa" o mayor se almacenan en el fichero /var/log/mail.
- Si tienen severidad "error" o mayor, se almacenan en otro fichero /var/log/mail-errores.
- Si se produce un mensaje crítico del sistema, no esperamos a almacenarlo en ningún sitio; se escribe inmediatamente un mensaje a 'root' donde quiera que esté, para que sepa lo que pasa.
- Si ese mensaje es además del tipo "emergencia", no sólo avisaremos a root sino a todos los usuarios (es lo que pasa cuando se hace un shutdown, por ejemplo).
- Los informes de seguridad, de severidad "info" o mayor, no sólo se guardan en el fichero /var/log/auth sino que además se mandan a la máquina "otramaquina" (ésto asume que hay un syslog corriendo en "otramaquina", que el puerto 514/udp de la misma está accesible y que ese syslog está a su vez configurado).

4.6.2 Particularidades

- Se deben utilizar tabuladores y no espacios en el fichero /etc/syslog.conf.
- Si se genera un informe que no esté previsto en el fichero de configuración, syslog lo volcará a la consola.

- Los ficheros donde vamos a volcar estos logs deben estar creados de antemano, aunque estén vacíos.
- El valor de severidad 'notice' no se puede combinar con otros, debe aparecer solo en una línea.
- El comodín * equivale a todos los subsistemas excepto 'mark'.

4.6.3 Uso desde programas

Los programas en C usan llamadas al sistema para acceder a syslog. Sin embargo, los scripts también pueden hacerlo. Si son en Perl, la forma más fácil es usar el módulo Perl Sys::Syslog (man Sys::Syslog).

Tanto en Perl como desde el shell se puede usar el programa logger:

```
logger -p mail.err Error entregando mensaje.
```

que enviará dicho informe como subsistema 'mail' y severidad 'err'.

Existen otras opciones (ver man logger).

4.6.4 Rotación de ficheros de registro

El problema de almacenar registros históricos o logs es que éstos crecen, y tarde o temprano llenan el disco. Para evitar esto, se recurre a la rotación de logs.

Ejemplo de fichero rotado mensualmente:

1. Antes de empezar:
    - /var/log/milog se crea vacío.
2. Al primer mes:
    - /var/log/milog se renombra como /var/log/milog.1
    - /var/log/milog se "vacía" de nuevo (se copia /dev/null sobre él).
3. Al segundo mes:
    - /var/log/milog.1 se renombra como /var/log/milog.2
    - /var/log/milog se renombra como /var/log/milog.1

- /var/log/milog se ”vacía”de nuevo.

Por supuesto, almacenaremos un número limitado de meses (o semanas, o días), o ésto no serviría de nada. Además, los registros de meses (semanas, días) anteriores se pueden comprimir.

Hacer esto tiene su truco. No se puede borrar impunemente un fichero que está abierto por un proceso (syslogd, en este caso), mejor dicho, no se debe, ya que los resultados no serán los que nos imaginamos.

La manera correcta de vaciar un fichero abierto es:

```
cp /dev/null <fichero>
```

4.6.5 Otros aspectos relacionados

Algo más sobre los aspectos de seguridad: cuando se almacenan registros con finalidad informativa (estadísticas, etc) suele bastar con almacenarlos en la misma máquina donde se generan. Cuando se almacenan por motivos de seguridad, sin embargo, nos interesa preservar una copia en otra máquina. El motivo es que si hay una intrusión en la primera máquina podrán borrar o modificar los registros, pero esas mismas actividades quedarán registradas en la segunda, avisando así a los operadores.

Normalmente, la máquina que reciba los logs (loghost) no debe recibir otra cosa (para no ser susceptible de ataques) ni debe poder recibir logs desde fuera de la red local (para evitar ataques por saturación). Para evitar consultas al DNS cada vez que se genere un informe, la dirección IP de esta máquina debe estar en el fichero /etc/hosts de las máquinas que manden informes.

4.7 Comprobación de integridad

Una vez que se ha accedido a un sistema es frecuente modificar los binarios de algunos servicios y programas del sistema operativo para permitir su acceso posterior. Así mismo se pueden modificar los ficheros de configuración de los servicios para hacerlos más vulnerables. Para evitar esto se suele emplear herramientas de comprobación de integridad. Estos programas funcionan en dos fases; primero se crea la base de datos de integridad, empleando varios algoritmos criptográficos para obtener una “huella dactilar” de cada uno de los ficheros. En una fase posterior se comprueban periódicamente los ficheros existentes en el sistema de ficheros con las firmas que ha generado este programa, pudiendo así averiguar si se ha producido alguna modificación en los mismos.

Existen varias herramientas que permiten realizar esta comprobación de integridad. La más conocida es quizá Tripwire. Este programa permite emplear varios algoritmos criptográficos a la hora de generar la base de datos (MD2, MD4, MD5, SHA, Snefru, CRC-32), para evitar que un atacante pueda modificar los ficheros. La ultima versión de Tripwire disponible de uso general es la versión 1.3, disponible en el servidor FTP de Rediris. Desde el año pasado la Universidad de Purdue transfirió la licencia a la empresa Tripwire Security System, que ha desarrollado una nueva versión, la 2.0 disponible también para entornos Windows NT. Sin embargo, y dado que las diferencias son mínimas con respecto a la versión 1.3, emplearemos ésta como referencia.

4.7.1 Instalación de Tripwire

Tripwire está disponible en el repositorio de programas de seguridad de RedIRIS (ftp.rediris.es/soft/rediris/cert) en código fuente para los sistemas Unix. Así mismo está compilado en formato de paquete para algunas distribuciones Linux. La compilación no suele dar problemas y una vez instalado se emplea el fichero de configuración /usr/local/bin/tw/tw.config para indicar qué ficheros se deben comprobar.

4.7.2 Configuración de Tripwire

Un ejemplo sería:

```
/root                   R
/                       R
/vmlinuz                R
/boot                   R
/etc                    R
/etc/inetd.conf         R
/etc/rc.d               R
/etc/exports            R
/etc/mtab               L
/etc/motd               L
```

```
/etc/group              R
/etc/passwd             L
/usr                    R
/usr/local              R
/dev                    L-am
/usr/etc                R
=/home                  R
/var/spool              L
/var/log                L
/var/spool/cron         L
/var/spool/mqueue       L
/var/spool/mail         L
/sbin                   R
=/proc                  E
=/tmp
=/cdrom
```

Como se ve, cada una de las entradas está formada por un identificador del directorio o fichero que se debe monitorizar y despues una serie de flags. Tripwire por defecto viene con una serie de identificadores predefinidos (R, L, E, etc.) para indicar distintas situaciones, como por ejemplo el que los ficheros sean de sólo lectura (R), ficheros de log (L), o ficheros que se deben excluir (E), etc. Consulte la página del manual para ver las distintas opciones de Tripwire.

Una vez definido el fichero de configuración se debe ejecutar el comando tripwire con la opción de crear la base de datos (tripwire -initialize). De esta forma Tripwire calculará los hash (las huellas) de cada uno de los ficheros y almacenará la información en los ficheros de la base de datos. Una vez generada la base de datos se debe almacenar en un dispositivo de sólo lectura (como un CD-ROM) o copiada a otro equipo para evitar que un intruso pueda modificarla. En sistemas con dispositivos removibles donde se pueda bloquear físicamente la escritura (disquetes), se puede copiar ahí la base de datos y después protegerlos contra escritura (en las unidades ZIP el bloqueo se realiza a nivel software, por lo que esta medida no es válida).

De esta forma es posible lanzar un proceso periódicamente que compruebe la integridad de los ficheros para evitar modificaciones, y actualizar manualmente la base de datos cuando se actualice el sistema operativo o se apliquen parches a éste.

4.8 Seguimiento de procesos

En gran parte de los sistemas Unix es posible ejecutar procesos de "accounting" o "contabilidad" para ir registrando el uso de los recursos de los equipos por parte de los usuarios y los procesos. La forma de configurar el sistema para que realize estos métodos de "accounting" suele depender mucho del sistema operativo del equipo, ya que suele realizarlo el núcleo (kernel) de éste, volcándose a ficheros cada cierto período de tiempo y realizando un procesamiento estadístico de estos datos. Antiguamente los procesos de accounting solían requerir bastante tiempo de procesamiento y eran difíciles de configurar y administrar. Sin embargo en la actualidad, la activación del accounting se suele realizar por la ejecución de un script en el arranque del sistema y la utilización de otro script para realizar las estadísticas durante la noche.

Las principales ventajas que tiene este sistema es poder analizar qué procesos se están ejecutando en el sistema, así como los usuarios que los realizan, pudiendo ver si algún usuario está ejecutando algún proceso en segundo plano o se ha producido algún ataque de saturación contra un servidor. Consulte la documentación del sistema operativo para ver cómo activar estos procesos de "accounting".

4.9 Actualizaciones de software

Sería conveniente dar algunas recomendaciones que permitan a los administradores disponer de un sistema automatizado para la recogida, instalación y notificación de parches. Algunas de estas recomendaciones se pueden resumir en los siguientes puntos:

- Actualización de los sistemas, tan pronto sea posible, a la última versión facilitada por el fabricante.

- Aplicación de todos los parches "recomendados" hasta el momento para esa versión del sistema operativo. Sería aconsejable la utilización de un script que se conectase al servidor FTP del fabricante concreto y aplicase los parches necesarios de forma automática.

Mantenga correctamente parcheados los sistemas utilizando algunos de los siguientes métodos:

1. Parcheado incremental. Utilización de un script que periódicamente aplique los parches necesarios desde la última aplicación, sin intervención humana y con notificación al administrador.
2. Obtener una lista de parches necesarios (incremental), después decidir qué parches son realmente necesarios para el sistema concreto y aplicarlos. Hay parches que aunque se recomiendan para una versión de un sistema operativo concreto, si no se posee un determinado software o paquete instalado, no es necesario aplicarlo. También ocurre al contrario, hay parches necesarios para una determinada versión de software instalado que no se incluyen en los parches recomendados para esa versión del S.O.

Para aquellos administradores que dispongan de máquinas Solaris, se puede obtener un sistema de recogida automática de parches en:
http://www.um.es/alfonso/

Capítulo 5

Recomendaciones para usuarios finales

5.1 Introducción

Los administradores de red preocupados por la seguridad de sus sistemas deben estar continuamente informados de las nuevas versiones de los productos instalados en sus máquinas. Pero no sólo los profesionales deben preocuparse de estos detalles, los usuarios finales también se pueden ver afectados por múltiples problemas si no actualizan su software.

Muchos pueden pensar que el problema de la seguridad sólo atañe a los administradores, informáticos y profesionales del sector: nada más lejos de la realidad. El usuario final también debe preocuparse por la integridad de su sistema doméstico.

Desde el clásico antivirus, perfectamente actualizado, hasta el propio navegador, hay programas imprescindibles dentro del PC y que deben actualizarse con regularidad.

George Guninski y Juan Carlos Cuartango descubren continuamente nuevos fallos de seguridad para Windows que dejan los datos del disco duro accesibles a través del navegador.

Una configuración incorrecta del sistema operativo puede dejar abierto el sistema a cualquier intruso. Un virus puede inutilizar todo nuestro ordenador, o un troyano puede desvelar todas nuestras cuentas de acceso a Internet. Por todo ello, la seguridad también afecta a los usuarios domésticos.

En esta sección, vamos a dar unas guías básicas de seguridad para distintos sistemas operativos dirigidas a los usuarios finales.

5.2 Guía Básica de Seguridad para Windows 95/98/ME

Windows 95/98/ME son sistemas operativos que están principalmente diseñados para trabajar como clientes, por lo que su uso y configuración será más facil que cuando hablamos de un servidor (Linux, Windows NT/2000, etc.), pero no los libera de que tengan serios problemas de seguridad.

Aunque ya lo hemos citado en el apartado de servidores NetBios, no vendrá mal repetir una frase que resuma la capacidad de Windows 95/98/ME en red:

Recomendamos, con toda rotundidad, que Windows 9x/ME se considere comprometido desde el mismo momento en que se arranca. Ninguna versión de Windows 9x/ME debería ser jamás utilizada en cualquier ordenador de una red donde algún recurso necesite ser asegurado.

No debemos olvidar, que al tener un equipo conectado a la red de una institución, la persona responsable de ese equipo es, así mismo, el responsable de la seguridad del mismo. Si un hacker se cuela en ese equipo y ataca, por ejemplo, a un equipo de la NASA, usted tendrá parte de responsabilidad por el hecho de que el ataque provenga de su máquina.

Este documento pretende dar unas recomendaciones sobre la configuración y uso adecuado que debemos hacer de nuestro ordenador cuando tenemos instalado Windows 95/98/ME.

5.2.1 Seguridad en red

Si tenemos el PC con Windows conectado a una red, lo más probable es que tengamos configurada la red para Trabajo en Grupo de Microsoft. Esta red nos permite intercambiar información entre los distintos ordenadores que integran la red, de manera que podamos compartir recursos (directorios, impresoras, etc...) para que el resto de los equipos tengan acceso a ellos. Si esto es así, deberemos tener en cuenta algunas medidas de seguridad:

1.No comparta recursos si no es necesario.

2.Si necesita compartirlos, hágalo siempre con una buena contraseña y aseguresé de que el recurso se comparte con las personas que lo necesitan y no éste accesible para todo el mundo.

3.Siempre que sea posible, compártalos como de "sólo lectura". Así evitará que, accidentalmente o por maldad, le borren información o le llenen el disco duro escribiendo en el directorio compartido.

4.NUNCA comparta su disco duro con privilegios de escritura ni siquiera con contraseña. Aunque comparta con contraseña, hay programas que realizan diversos tipos de ataque (de fuerza bruta, diccionario, etc..) hasta que dan con la contraseña correcta. Un hacker tiene todo el tiempo del mundo para probar, y Windows no le avisa que que lo está haciendo.

En general, le recomendamos que no comparta información importante de forma permanente por este método, pues no proporciona demasiada seguridad.

5.2.2 Antivirus, virus y caballos de troya.

Uno de los problemas más graves de seguridad en los Windows son los virus y últimamente los troyanos:

Virus. Son programas hechos por alguien y su función es muy diversa, pero básicamente todos tienen la capacidad de reproducirse y una estrategia de propagación. Lo más peligroso del virus es su "payload$^{\underline{o}}$ efecto, que puede ir desde mostrar una pelotita rebotando en los bordes de la pantalla hasta el formateo del disco.

Caballos de Troya. Son programas que tras una función aparentemente inocente encierran en su interior otra función. Por ejemplo, un troyano típico puede presentarnos una pantalla igual a aquella en la que tenemos que escribir nuestro login y nuestra contraseña. Cuando los introduzcamos, los almacenará. Lamentablemente los troyanos en Windows están muy de moda desde que aparecieron los ya famosos BackOriffice o Netbus, que tras instalase en el equipo, permiten el acceso y control remoto del ordenador desde Internet. Periódicamente aparecen más troyanos de este tipo.

Algunas soluciones para evitar este tipo de problemas son:

1. Antivirus. Buscan virus (y troyanos) en nuestro ordenador y los eliminan. En la actualidad muchos no sólo se limitan a buscar en nuestro disco duro y memoria, sino también en los mensajes que nos llegan por correo o los que nos bajamos de Internet. Sin embargo, la eficacia de un antivirus depende de su actualización, por lo que es importantísimo actualizarlo al menos una vez al mes. Diariamente aparecen en Internet decenas de virus que podrán atacarnos hasta que, primero, los antivirus

los detecten, y segundo, nosotros actualicemos el antivirus en nuestro PC. Por lo tanto, un antivirus no protege totalmente contra los virus nuevos, por lo que es necesario tomar otro tipo de medidas:

2. Si le llega un ejecutable por correo que no haya solicitado, NO LO EJECUTE, incluso aunque venga de una persona conocida. Los últimos virus como el conocido Melissa usaban la agenda del equipo infectado para mandar correos con el virus contenido en un gracioso fichero adjunto. Lo más recomendable es borrarlo (si no lo ejecuta no le infectará) o en todo caso, comprobar si el remitente realmente se lo ha enviado conscientemente. En caso contrario, bórrelo definitivamente.

3. Abra los documentos de Office (Word, Excel...) sin macros: si cuando abre un fichero de este tipo, le avisa que el fichero tiene macros, ábralo sin macros; probablemente sea un virus.

5.2.3 Algunos apuntes más

Windows 9x/ME no es un sistema operativo que se hiciera pensando en la seguridad y al margen de la red debemos tener en cuenta algunas cosas más:

Vigile el acceso físico a su equipo. Si alguien tiene acceso a su PC, puede encender el ordenador y ya tendrá a su disposición toda la información que en él está contenida. Windows no provee ningún mecanismo para validar usuarios, para conseguir esto, deberemos recurrir a software de terceros.

La contraseña que Windows nos pide al arrancar no es ninguna medida de seguridad: con pulsar "Cancelarº la tecla ESC entraremos igualmente. Por tanto, cierre las puertas con llave cuando se ausente, no permita que nadie desconocido se siente en su PC, etc.

Su Ordenador Personal debe ser Personal. Aunque teóricamente Windows es un sistema operativo multitarea y multiusuario, esto no es del todo cierto. En realidad es más un entorno monousuario, ya que no distingue realmente entre usuarios. Por eso es totalmente desaconsejable compartir un PC entre varias personas. Cualquiera por error o maldad puede ver, modificar o borrar sus datos.

Capítulo 6

Guía básica de seguridad de Windows NT

6.1 Introducción

Windows NT fue, según Microsoft, diseñado y desarrollado con la seguridad en mente; por lo tanto, podríamos pensar, "no tengo que preocuparme de su seguridad". Esto es falso.

Lo primero es que ningún programa nos va dar solución a la seguridad definitiva y total (y el que lo prometa miente). Todos tienen fallos y vulnerabilidades que para cuando son parcheados, el programa será tildado de obsoleto. Lo segundo es que la seguridad de un sistema depende en gran medida de nuestras políticas y de la configuración del sistema.

Esta guía trata las recomendaciones de configuración que se deben tener en cuenta si está usando Windows NT. No es objetivo de esta guía enseñarle a usar Windows NT, aunque sí se hace una pequeña introducción de los conceptos básicos para unificar términos.

6.2 Conceptos Básicos

6.2.1 Dominio

Es un grupo lógico de máquinas que comparten cuentas de usuarios y seguridad de los recursos. Un dominio está integrado por una máquina NT servidor de dominio que administra las cuentas y recursos del dominio en cuestión, y/o servidores y/o estaciones de trabajo. Los usuarios de un mismo dominio tendrán un inicio de sesión único en el servidor del dominio para acceder a los recursos de cualquier parte de la red, una cuenta única para acceder a las máquinas del dominio, etc.

6.2.2 Cuentas de usuarios

En las cuentas de los usuarios se establecen datos como el propietario de la misma, contraseña de acceso, localización de su directorio de inicio de sesión, grupo al que pertenece, etc. Windows NT distingue las cuentas locales y las cuentas de dominio:

Cuenta local de usuario: pertenecen a una única estación Windows NT. El procedimiento de *login* de las mismas se valida en una base de datos local de la estación. La herramienta administrativa de la estación para crearlas, modificarlas, borrarlas y establecer políticas de seguridad es el *Administrador de usuarios* o el *Administrador de usuarios para dominios.*

Cuenta de dominio: pertenecen al dominio en cuestión. El procedimiento de *login* requiere, además del nombre de usuario y contraseña, el dominio al que se está haciendo *login*. La validación se hace en una base de datos existente en el servidor de dominio. La herramienta administrativa del servidor para crearlas, modificarlas, borrarlas y establecer políticas de seguridad del dominio es el *Administrador de usuarios para dominios.*

Tanto si se hace *login* en un tipo de cuenta u otro, para acceder al menú de seguridad de la estación o el servidor (para cambiar el password, bloquear el terminal, o cierre de sesión e incluso del sistema) se debe teclear la siguientes combinación de teclas CTRL+ALT+SUPR.

Las cuentas que por defecto crea NT son la de *Invitado* (Guest), deshabilitada por defecto, y la de *Administrador*, para configuración y control de usuarios y recursos.

6.2.3 Cuentas de grupos

Las cuentas de usuarios se organizan en grupos. Cuando se añade un usuario a un grupo, el usuario tendrá los derechos y permisos asignados a ese grupo.

Windows NT distingue dentro del concepto de grupo, dos categorías: grupos locales y globales.

Grupo local: lo forman cuentas locales de usuarios y grupos globales de otros dominios. Se usan para asignar a grupos de usuarios permisos para acceder a un recurso.

Grupo global: lo forman únicamente cuentas de dominio. Aunque los grupos globales pueden usarse para asignar permisos a los recursos, su funcionalidad principal es agrupar las cuentas de un dominio. Para lo primero es mejor añadir los grupos globales como locales.

NT crea por defecto ciertos grupos locales, globales y de sistema con ciertos derechos ya adquiridos. Los grupos locales que existen por defecto en cualquier máquina NT son:

Usuarios: Usuarios normales con cuenta.

Administradores: Usuarios con derechos para administrar el sistema.

Invitados: Usuarios sin cuentas que tienen derechos muy limitados.

Operadores de copia de seguridad: Usuarios con derechos de copia de seguridad y restauración de archivos.

Si la máquina es servidora de dominio, además de los anteriores grupos locales, NT crea:

Operadores de cuentas: Usuarios con derechos para administrar cuentas de usuarios.

Operadores de servidores: Usuarios con derechos para administrar servidores.

Operadores de impresión: Usuarios con derechos para administrar impresoras

y además crea los siguientes grupos globales:
Admins. de dominio Usuarios de dominio Invitados de dominio
Los usuarios se convierten en miembros de los grupos del sistema automáticamente al acceder a la red. Los grupos de sistema en cualquier máquina NT son:

Todos: incluye a todos los usuarios que acceden a la red. No se puede controlar quién pertenece a este grupo, pero sí los permisos y derechos de este grupo.

CREATOR OWNER (propietario): usuario que creó el recurso o es propietario del mismo.

Es conveniente revisar qué derechos tienen todos estos grupos por defecto dentro del menú de políticas de derechos de usuarios.

6.3 Políticas de passwords y cuentas

El administrador de la red debe establecer una política de passwords en la que se especifique:

- Una duración máxima de la contraseña (aconsejable unos 90 días).
- Una longitud mínima (aconsejable un mínimo de 8 caracteres).
- Un histórico de la contraseña (unas 5 contraseñas).
- Un bloqueo automático tras sucesivos fallos de *login* (unos 5 fallos).

La política se establece accediendo al menú del *Administrador de usuarios para dominios/Directivas/Cuentas/Plan de cuentas*

Para desbloquear una cuenta:

Administrador de usuarios para dominios/Usuario/Propiedades/Cuenta desactivada

También es útil establecer restricciones en el *Administrador de usuarios para dominios* como:

- Horas de entrada en una máquina del dominio.
- Estaciones desde las que se puede acceder al dominio.
- Tiempo de expiración de las cuentas.
- Restricción de acceso telefónico.

, así como templates para las cuentas de nueva creación.

6.4 Permisos y derechos de usuario

Los derechos de usuario definen qué pueden hacer los usuarios. Algunos de los derechos más comunes son:

- El derecho de inicio de una sesión local.
- Derechos de administración de auditoría.
- Derecho de apagar el equipo.
- Derecho de acceder al equipo desde la red (acceder a recursos compartidos).
- Derecho de hacer copias de seguridad o de restaurar ficheros desde copias de seguridad.

Para configurar los derechos de usuarios, se elige *Derechos de usuario* del menú *Directivas* del *Administrador de usuarios para dominios* y se autorizan para cada derecho los usuarios o grupos apropiados.

Hay que tener en cuenta que es conveniente eliminar al grupo *Todos* el derecho de *Acceder a este equipo desde la red.*

Los permisos definen qué recursos pueden usar los usuarios o grupos de usuarios, entendiendo por recurso un fichero, directorio o una impresora. Los permisos controlan el acceso a directorios y ficheros locales y compartidos en la red y son configurados por el administrador o por el propietario de los mismos. Hay permisos estándar y permisos individuales. Los permisos estándar son una combinación de los permisos individuales.

6.4.1 Permisos para directorios

Permisos estándar	Permisos individuales	Permisos para nuevos ficheros
Sin acceso	Ninguno	Ninguno
Listar	R, X	-
Lectura	R, X	R,X
Añadir	W, X	-
Añadir y Lectura	R, W, X	R, X
Cambio	R, W, X, D	R, W, X, D
Control total	Todo	Todo

6.4.2 Permisos para ficheros

Permisos estándar para archivos	Permisos individuales
Sin acceso	Ninguno
Lectura	R, X
Cambio	R, X, W, D
Control Total	Todos

En un sistema de ficheros NTFS, el administrador puede configurar los permisos de ficheros y directorios pulsando con el botón derecho del ratón sobre el fichero o directorio que se que desee proteger, y luego la secuencia *Propiedades/Seguridad/Permisos*.

Así, los directorios %SystemRoot% (normalmente C:\Winnt), %SystemRoot%\System32 y %SystemRoot%\Temp, tienen respectivamente derechos de *Control total*, *Cambio* y *Control total*, para el grupo *Todos*.

Para corregirlo, una vez comprobado que el *Administrador* tiene Control total sobre los mismos, cambiar a sólo Lectura %SystemRoot% sin propagar estos cambios a los subdirectorios, y %SystemRoot%\System32 a sólo Lectura propagándolos, con la precaución de poner permiso de Cambio a *Todos* a %SystemRoot%\System32\RAS y %SystemRoot%\System32\spool\Printer.

De la misma manera, el volumen C: donde se encuentran ficheros relacionados con el arranque de la máquina, debería formatearse NTFS y los ficheros críticos deberían tener:

C:\boot.ini ⇒ Control total para *Administradores* y *Sistema*.

C:\ntdetect.com ⇒ Control total para *Administradores* y *Sistema*.

C:\autoexec.bat ⇒ Control total para *Administradores* y *Sistema* y Lectura a *Todos*.

C:\config.sys ⇒ Control total para *Administradores* y *Sistema* y Lectura a *Todos*.

Y muy importante, cuando se formatea un volumen con NTFS, el grupo *Todos* adquiere *Control total* del volumen. Cuidado con los permisos por defecto.

6.5 Compartición de recursos de red

Para compartir recursos de red sólo tendremos que pinchar con el botón derecho sobre un directorio o una impresora y veremos una opción que será Compartir. Nos aparecerá un menú desde donde podremos compartir el recurso.

Los recursos de la red se comparten de forma segura con los siguientes permisos:

Lectura: permite listar directorios, ficheros.

Cambio: permite crear directorios, añadir ficheros, modificar datos y permisos de éstos, borrar ficheros y directorios, y permisos de Lectura.

Control total: permite modificar permisos, toma de posesión, y permisos de Cambio.

Sin acceso: este permiso prevalece sobre cualquier otro y deniega el acceso al recurso.

A diferencia de lo que ocurre con los permisos NTFS, no se pueden asignar diferentes permisos a distintos ficheros de un mismo directorio compartido.

Cuando se combinan los permisos de recursos compartidos y los permisos del volumen NTFS, prevalecen los más restrictivos.

6.6 Seguridad del registro

El registro es una base de datos que mantiene información sobre la configuración hardware, software y de entorno de la máquina. Se puede ver con REGEDT32. Por defecto, Windows NT 4.0 no permite el acceso remoto al registro por defecto.

El Registro de NT es un arma muy poderosa para poder configurar correctamente determinados parámetros de nuestra máquina. Se ha de tener un especial cuidado a la hora de trabajar directamente con el editor del registro, ya que la introducción de valores erróneos puede acarrear problemas al sistema. El entorno ideal para estos casos sería contar con una máquina de pruebas, y tras comprobar que no existen problemas, proceder a la modificación del Registro en el resto de sistemas.

Es conveniente:

- Deshabilitar el acceso remoto al registro a los usuarios no autorizados, revisando la siguiente entrada en el registro:

  Nota: A partir de ahora se utilizará HKLM como abreviatura de HKEY_LOCAL_MACHINE.

```
HKLM\SYSTEM\CurrentControlSet\Control\SecurePipeServers\WinReg
```

Asegúrese de que sólo el grupo de *Administradores* tiene como permisos de seguridad *Control total* sobre esta clave. Puede ver los permisos que tiene una clave del registro situándose sobre ella y pulsando en el menú *Seguridad*, la opción *Permisos*.

La instalación del Service Pack 3 para Windows NT 4.0 desactiva la posibilidad de que un usuario anónimo se conecte al registro remotamente. Como un recordatorio, Windows NT 4.0 restringe el acceso remoto al registro a los usuarios de dominio usando las listas de control de acceso (los permisos) asociadas a esta clave de registro.

- Deshabilitar (poner a 0) si es necesario el apagado del equipo en la opción *ShutdownWithoutLogon* de:

  ```
  HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon
  ```

- Deshabilitar (poner a 0) la variable *AutoAdminLogon*:

  ```
  HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon
  ```

  Esta modificación, evitará saltarse el cuadro de diálogo de autenticación a través de los valores DefaultUsername, DefaultPassword y DefaultDomain. Esta característica es posible si se ha configurado el AutoAdminLogon para evitar tener que teclear la contraseña cada vez que se inicie la sesión (práctica a todas luces poco recomendable).

- Poner a 1 (verdadero) la variable *Parameters*:

  ```
  HKLM\SYSTEM\CurrentControlSet\Services\RemoteAccess
  ```

- Poner la variable *FullPrivilegeAuditing* a 1:

  ```
  HKLM\SYSTEM\CurrentControlSet\Control\LSA
  ```

En el primer caso estaremos habilitando la auditoría de los servicios de acceso remoto. Con la segunda variable, conseguiremos auditar todos los derechos de usuarios, que nos ayudará a poder controlar si algún usuario utiliza ciertos derechos administrativos para acceder a ficheros confidenciales o que conlleven riesgos al sistema.

- Poner a 1 *LegalNoticeCaption*:

  `HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon`

  e indicar el texto de advertencia en *LegalNoticeText*.

  Con estás dos entradas podremos habilitar que aparezca una ventana con un aviso cada vez que se inicie la sesión. Esta práctica se recomienda en entornos corporativos, y puede contener avisos legales, consejos, o normas internas, que pueden prevenir un mal uso de la red y reprimir intentos de sabotajes.

- Poner a verdadero *DontDisplayLastUserName* en:

  `HKLM\SOFTWARE\Microsoft\WindowsNT\Current\Version\Winlogon`

  Esta modificación evitará que el sistema muestre en la ventana de autenticación el nombre del último usuario. De sobra es conocido que los nombres de usuarios son pieza codiciada por los crackers a la hora de poder proceder a distintos tipos de ataque, como el de fuerza bruta. Es por ello que además de esta modificación, recomendamos renombrar las cuentas de usuarios que vienen por defecto en Windows NT, como pueda ser la de *Administrador*.

- Limpiar el fichero de paginación (swap) al apagar el equipo, poniendo a 1 la variable *ClearPageFileAtShutdown* en:

  `HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\MemoryManagement`

  Con este valor conseguiremos que el archivo que almacena la memoria virtual del sistema se borre automáticamente tras salir de una sesión. Esta característica evita que un posible atacante acceda a este archivo y recoja información confidencial.

- Poner a cero la variable *AllocateFloppies*, si se desea deshabilitar el acceso a las disqueteras:

  `HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon`

- Para deshabilitar el acceso al CDROM poner a 0 *AllocateCDROMS*:

  `HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon`

  Con estas dos entradas se consigue desactivar las disqueteras y las unidades de CD-ROM respectivamente. En determinados entornos se aconseja esta práctica, para impedir la grabación de datos, o la ejecución e instalación de software. Tampoco podemos olvidar que también suelen ser entrada habitual de los virus informáticos.

- Poner a cero la variable *AutoAdminLogon*:

  `HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon`

  Esta modificación, evitará saltarse el cuadro de diálogo de autenticación a través de los valores *DefaultUsername*, *DefaultPassword* y *DefaultDomain*. Esta característica es posible si se ha configurado *AutoAdminLogon* para evitar tener que teclear la contraseña cada vez que se inicie la sesión.

- Poner a cero la entrada *ShutdownWithoutLogon*:

  `HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon`

  Con este valor conseguiremos que no se pueda apagar un sistema NT sin iniciar una sesión. Esta posibilidad presenta un problema de seguridad que se agrava en el caso de los servidores cuya ubicación física no esté protegida. Si esta característica estuviera habilitada, cualquiera podría apagar el sistema desde el cuadro de diálogo de autenticación, con la consecuente pérdida de servicios y recursos para los clientes que estuvieran haciendo uso de ellos.

- NT por defecto comparte cada uno de las particiones que tengamos en nuestro sistema para el administrador. Para evitar este hecho, deberemos crear una variable de tipo DWORD llamada *AutoShareServer* con el Editor del registro, en:

  `HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters`

  y ponerle un valor de cero.

  Esta será la entrada correcta en el caso de que estemos en un NT Server. Para las versiones NT Workstation, la variable tendrá que llamarse *AutoShareWks*.

- Poner la variable RestrictAnonymous a 1 en:

  `HKLM\System\CurrentControlSet\Control\LSA`

  Iniciar una sesión nula, o sesión anónima, permite obtener información sensible sobre la máquina y el dominio en el que se encuentra, como pueden ser nombres de usuario, grupos, recursos compartidos, propiedades de las passwords, etc. Por defecto NT permite las credenciales nulas contra el recurso \\nombreservidor\IPC$, que toda máquina NT comparte para que otras máquinas usen recursos y se autentiquen en ellas (su nombre tecnico es InterProcess Communication, IPC's). Aunque es algo imprescindible en cualquier máquina NT, no es en absoluto adecuado que cualquier usuario no autenticado pueda acceder a información del dominio y/o la máquina.

  Esta misma vía se puede utilizar con malas intenciones, por ejemplo, a través del comando NET USE, para recopilar información de cara a un posterior ataque. Se puede forzar la autenticación en este tipo de sesiones mediante la activación de la variable RestrictAnonymous.

- Los sistemas NT permiten dos tipos de desafíos para lograr la autenticación ante el servidor. El más seguro es el sistema propietario de NT (MD4), y tenemos en el desafío LanManager (DES), para clientes Windows 95/98 y NetWare, el eslabón más débil. NT trabaja por defecto con ambos sistemas indistintamente, por lo que un atacante podría forzar un intercambio de contraseñas DES (LanManager) y a partir de ahí interceptar los paquetes durante el desafío para llegar a conseguir las contraseñas.

Para evitar dar facilidades en este sentido se pueden configurar nuestros sistemas para que únicamente utilicen el sistema de autenticación LanManager cuando se necesite. Para ello deberemos igualar la variable LMCompatibilityLevel a 1 en:

`HKLM\System\CurrentControlSet\Control\LSA`

- Proteger adecuadamente el registro de usuarios no autorizados.
- Hacer copias periódicas del mismo con la utilidad REGBACK.EXE. Obviamente, las copias deberían estar guardadas en un lugar seguro, pues en ellas va toda la información sensible de nuestra máquina.

6.7 Auditorías

El sistema de Auditoría de Windows NT permite rastrear sucesos que ocurren en una máquina NT, tanto servidor como estación de trabajo. Las auditorías son esenciales para mantener la seguridad de los servidores y redes. Además de permitir un seguimiento de las actividades realizadas por los usuarios.

La política de auditorías se establece en cada máquina NT. Se pueden realizar tres tipos de auditorías en NT:

6.7.1 Auditoría de cuentas de usuario

Rastrea los sucesos de seguridad y escribe apuntes en el registro de seguridad. Se activa en *Administrador de usuarios en dominios/ Directivas/Auditoría/Plan de auditorías.*

Los sucesos que se pueden auditar son:

- Inicio y cierre de sesión.
- Acceso a ficheros, directorios o impresoras.
- Ejercicio de los derechos de un usuario.
- Seguimiento de procesos.
- Inicio, reinicio y apagado del sistema.

6.7.2 Auditoría del sistema de archivos

Rastrea sucesos del sistema de archivos. Esta opción se activa en *Propiedades*, tras pulsar con el botón derecho sobre el fichero o directorio que se desee auditar y luego seleccionando *Seguridad/ Auditorías.*

Los sucesos que se pueden auditar son: *Lectura*, *Escritura*, *Ejecución*, *Eliminación*, *Cambio de permisos* y *Toma de posesión.*

Para auditar ficheros y directorios, éstos deben estar localizados en un volumen NTFS.

6.7.3 Auditoría de impresoras

Primero se establece la política de auditorías pinchando dos veces en la impresora en cuestión, dentro del menú *Impresoras*, y luego seleccionando *Seguridad/Auditorías.*

Algunos de los eventos que se pueden auditar son: *Uso de la impresora*, *Cancelar trabajos de impresión*, *Control total*, etc.

Se debe tener derechos de administrador para configurar propiedades de auditoría.

Una vez que se activa una auditoría se utiliza el Registro de seguridad del *Visor de sucesos* que se encuentra dentro del menú de Inicio *Herramientas administrativas*, para ver los eventos auditados.

Se debería tener cuidado y proteger los archivos de auditoría que están almacenados en el directorio %SystemRoot%\system32\config, en los archivos:

APPEVENT.EVT: Registro de sucesos de aplicaciones.

SECEVENT.EVT: Registro de sucesos de seguridad.

SYSEVENT.EVT: Registro de sucesos del sistema.

Algo muy importante a la hora de mirar los registros es que la máquina tenga la hora correcta, ya que si tenemos que comparar sus registros con los de otras máquinas: si ambas no están sincronizadas será muy difícil. Para esto debería usar NTP (Network Time Protocol) que sirve para poner en hora ordenadores y mantenerlos sincronizados (http://www.rediris.es/ntp/).

6.8 Seguridad en Red

6.8.1 Protocolos de Red

Debemos instalar sólo los protocolos que vayamos a necesitar. En principio y salvo que tengamos necesidad de usar más protocolos, deberíamos usar uno de estos dos:

- NetBEUI
- TCP/IP

NetBEUI es un protocolo de red no enrutable, sólamente útil para redes de pequeño tamaño. TCP/IP es el líder indiscutible en cualquier tipo de red. Con cualquiera de estos dos protocolos el servicio que estamos ofreciendo a la red es el llamado SMB (Bloques de Mensajes de Servidor), de Microsoft, también conocido como *Cliente de redes Microsoft*, y que básicamente proveen servicios de archivos y red. Estos servicios están instalados por defecto normalmente.

Los servicios TCP/IP de Internet como servidores Web y FTP, se pueden instalar de modo opcional en Windows NT.

Puede verse un resumen de puertos TCP/IP junto con su descripción en la página 8.

Conviene tener abiertos el menor número de servicios posibles. Al ser estos opcionales, no vienen instalados por defecto y hay que instalarlos a posteriori. Salvo que se necesiten y que se sepa lo que se está haciendo, conviene no instalar ninguno.

También se pueden configurar las opciones de seguridad TCP/IP para permitir o bloquear la dirección del/los puerto/s que se necesiten según los servicios que se quieran utilizar. Para hacer esto, siga la siguiente secuencia:

1. *Panel de Control/Red/Protocolos/Protocolo TCP/IP/Propiedades/ Avanzadas*
2. Marque *Activar seguridad*
3. Pulse el botón *Configurar*
4. Seleccione el adaptador correspondiente y marque el número de puerto/s del servicio/s que quiera permitir.

6.9 Service Pack's

Los Service Pack (SP) no son más que un conjunto de parches que Microsoft saca de vez en cuando para solucionar fallos, dar nuevas funcionalidades, etc. Lo bueno de estos parches es que de una sola vez se aplican todos (a veces más de 100) rápida y fácilmente. El sistema es muy similar a los *clusters* de parches recomendados de Sun.

Todo NT debería tener instalado al menos el penúltimo SP. En el momento de escribir esta guía, el último Service Pack es el 6a. Microsoft se ha comprometido a sacar un Service Pack 7 que resuelva aún más fallos.

Los Service Pack's son independientes del tipo de NT 4.0 que haya instalado, por lo que son los mismos para Workstation, Server, Server Enterprise, etc.

Si después de instalar un Service Pack instala algún servicio, controlador o programa que altere de forma significativa Windows NT (Microsoft Office, sistemas de bases de datos, etc.), es muy recomendable que reinstale el Service Pack para asegurarse de que la aplicación no ha sobreescrito ningún fichero con una versión anterior.

Y para terminar, un consejo:

Nunca instale un SP en otro idioma que no sea el de la instalación del sistema operativo. Tendrá que reinstalar el sistema.

6.10 Cortafuegos

Cuando se conecta un sistema Windows a Internet existe el peligro potencial de los protocolos SMB. Si hay carpetas compartidas SMB en la red que conecta a Internet, potencialmente cualquiera de los usuarios de Internet puede acceder a las carpetas o secuestrar sesiones. Además, hay problemas de seguridad intrínsecos a los protocolos. A continuación se describe como desactivar estos servicios apropiadamente:

1. *Panel de Control/Red/Enlaces.*

2. Seleccione *Todos los servicios* en la caja de texto correspondiente a *Mostrar enlaces.*

3. Expanda las opciones TCP/IP bajo las cabeceras: *NetBIOS*, *Server* y *Workstation.*

4. Seleccione el adaptador a desactivar y pulsar el botón *Desactivar*.

6.11 Consideraciones generales

No conviene que NT esté instalado en una máquina con arranque dual, ya que esto haría que muchas de sus garantías de seguridad perdieran efectividad.

Es casi obligado que la partición del sistema sea NTFS. No hay ningún motivo por el que NT haya de instalarse en una partición FAT.

Conviene dar a cada uno de los usuarios del sistema unas ciertas normas sobre el uso de la máquina que podría empezar con la frase de "Todo lo que no esté explícitamente permitido, está prohibido"y continuar explicando todo lo que está permitido. Si se dejan las cosas claras desde un principio, nos ahorraremos muchos quebraderos de cabeza.

Administrador no hay más que uno. Aunque NT permite que haya varios administradores para tareas determinadas, es muy importante delimitar estas tareas al máximo si más de una persona administrará la máquina o dominio NT. A medida que el numero de administradores tiende a infinito, la funcionalidad en la máquina tiende a cero.

Los usuarios solo deben tener los privilegios necesarios para ser usuarios. En un exceso de celo, podemos cometer el error de limitar demasiado los privilegios de los usuarios. Esto hace que el usuario no pueda usar la máquina normalmente y perdamos de vista el objetivo por el que hacemos todo esto. Por otro lado, si los usuarios tienen excesivos privilegios (algunos administradores irresponsables lo permiten para no tener que hacer las cosas ellos y que las hagan los usuarios) nos podemos encontrar que por desconocimiento, experimentación o maldad se cause daño al sistema.

Apéndice A

Información de seguridad en Internet

A.1 Listas de distribución

A.1.1 Listas de RedIRIS

Puede encontrar información sobre las listas de seguridad en RedIRIS en la URL:

- http://www.rediris.es/cert/servicios/listas/listserv.es.html .

De estas listas queremos destacar la lista IRIS-CERT. Esta lista, restringida a responsables de la comunidad RedIRIS, tiene como objetivo tratar temas relacionados con la seguridad en las comunicaciones y en las máquinas de la Comunidad de RedIRIS, con el fin de coordinar servicios. Actualmente existen 133 suscriptores, pero desgraciadamente el tráfico es nulo. A partir de ahora deberá ser obligatoria la existencia de al menos una persona de cada institución en esta lista. Lo mismo ocurrirá con otras listas IRIS-*: IRIS-MAIL, IRIS-DNS y IRIS-IP. En el caso de que no se proporcionen puntos de contacto para esta lista, será el PER. Desde IRIS-CERT queremos hacer un trabajo de potenciación de esta lista, esperando tener respaldo de todos aquellos responsables de seguridad interesados en mejorar su labor diaria.

A.1.2 Otras

Podrá encontrar información útil sobre listas de distribución relativas a seguridad en las siguientes URLs:

- http://www.rediris.es/cert/links/listas.es.html
- http://www.cica.es/seguridad/INFORMACION_LISTAS/listas.es.html

A.2 Boletines

- Criptonomicón: http://www.iec.csic.es/criptonomicon/
- Kriptópolis (Criptogafía, PGP y Seguridad en Internet): http://www.kriptopolis.com/boletin.htm
- Una al día (Hispasec: Noticias diarias de seguridad informática): http://www.hispasec.com/

A.3 Áreas de Documentación

- Área de documentación de IRIS-CERT: http://www.rediris.es/cert/doc/
- Enlaces mantenidos por IRIS-CERT: http://www.rediris.es/cert/links/
- CERT/CC (CERT Coordination Center): http://www.cert.org/
- CERT-COORD: http://www.terena.nl/tech/projects/cert/
- EuroCERT: http://www.eurocert.org/
- esCERT-UPC: http://escert.upc.es/
- SecurityFocus: http://www.securityfocus.com/
- X-Force (Internet Security System): http://www.iss.net/
- The WC3 Security Resources: http://www.w3.org/Security/

A.4 Sitios de hackers

- Els Apostols : http://www.apostols.org/ Grupo Español
- HNN- HackerNewsNetwork : http://www.hackernews.com/
- HERT Computer Security (Hacker Emergency Response Team) : http://www.hert.org
- Cult of the Dead Cow (cDc) : http://www.cultdeadcow.com/ Página de los creadores de BackOriffice y otras herramientas.
- HackerShield : http://www.netect.com/hs_overview.html

A.5 Herramientas y software de Seguridad

- Herramientas de seguridad de RedIRIS : http://www.rediris.es/cert/tools
- Área de Seguridad de RedIRIS : ftp://ftp.rediris.es/rediris/cert/
- Nmap : http://www.insecure.org/nmap/ Herramienta para realizar escaneos de puertos y detección de Sistemas Operativos.
- Tucows (Sección Security) : http://tucows.uam.es/

A.6 Avisos de seguridad, parches, etc... de varias empresas de software

- Microsoft : http://www.microsoft.com/security/
- RedHat : http://www.redhat.com/corp/support/errata
- Debian : http://security.debian.org/
- Sun : http://sunsolve.sun.com/
- Suse : http://www.suse.de/e/patches/
- Mandrake : http://www.linux-mandrake.com/en/security/
- Enlaces mantenidos por IRIS-CERT : http://www.rediris.es/cert/links/

A.7 Herramientas de evaluación de la seguridad para Windows NT

- Herramientas para escanear los puertos TCP de un ordenador o conjunto de ordenadores dentro de una red (http://www.ipswitch.com/).

  Con esta herramienta se pueden escanear u obtener la lista de puertos que están abiertos en un ordenador o conjunto de ordenadores.

- Herramienta para descargar los permisos (ACLs) del sistema de ficheros, los registra, comparte e imprime en breve tiempo. También detecta algunos agujeros en el sistema de seguridad (http://www.somarsoft.com/).

- Kane Security Analyst es una herramienta de tasación de seguridad en red (permisos para los usuario y grupos en el dominio, seguridad C2, claves que puedan descubrirse fácilmente, particiones no seguras, violaciones de los inicios de sesión y seguridad en ellos, autenticaciones a bajo nivel, etc.), que analiza un dominio Windows NT Server o Workstation . Presenta los resultados detallados y fácilmente comprensibles (http://www.intrusion.com/product/ksa_nt.html).

- Para más información, consulte
  la sección de Tucows : http://tucows.uam.es/securitynt.html sobre herramientas de seguridad para NT.

A.7.1 Herramientas para escanear virus

- McAfee ViruScan : http://www.mcafee.com
- Panda Antivirus : http://www.pandasoftware.com
- Inoculan Antivirus for Windows NT : http://www.cheyenne.com/desktop/productinfo/
- Para más referencias, consultar la sección de Tucows : http://www.sdi.uam.es/tucows/virusnt

Apéndice B

Contribuciones

Además del personal de RedIRIS, las siguientes personas han contribuido al desarrollo de estas recomendaciones de seguridad:

- *Alfonso López Murcia (alfonso@fcu.um.es). Actualizaciones de software en equipos Unix.*
- Victor Barahona (victor.barahona@uam.es). Recomendaciones para usuarios.

B.1 Agradecimientos

Esta información ha sido suministrada por:
Area de Seguridad del CICA
mailto: sec-team@cica.es
http://www.cica.es/seguridad
Victor Barahona
Unidad Tecnica de Comunicaciones
Universidad Autonoma de Madrid
http://www.sdi.uam.es/comm/ss/
una_al_dia. Noticias HispaSec (http://www.hispasec.com)

Apéndice C

Registro de Cambios

Aunque no sea exhaustivo y tengamos que automatizarlo, nos parece adecuado ir poniendo un registro de los cambios entre las versiones. Este registro de cambios se publicará también aparte para que se puede consultar sin tener que recuperar el documento completo.

Futuras vías

Estas son algunas ideas sobre las posibles vías de desarrollo.

- Generación automática de los documentos.
- Contribución global mediante un repositorio (¿CVS?).
- Generar automáticamente la documentación en HTML.
- Probar el pdftex o similar para evitar los ficheros enormes que se generan con el ps2pdf de dominio publico.
- Separar las secciones, de forma que por un lado se traten los problemas de seguridad, con independencia del S.O. y despúes se comenten las soluciones y problemas para los distintos sistemas o partes de un diseño de servicios de red.
- Hacer la parte de referencias más dinámica, viendo la forma que las referencias se puedan incluir en el texto y se generen despues correctamente.

C.0.1 Versión 0.1

Generada el 15 de diciembre de 2000. Esta revisión esperamos que sea la última que reciba la guía con este formato. La próxima revisión tendrá por objeto separar en partes casi completamente independientes las recomendaciones (red, Unix, Windows, servicios, etc.) pero sin entrar a fondo en cada campo. ¡Tan sólo han de ser unas directivas, no un manual completo de actuación!

- Muchísimas correcciones ortográficas pendientes.
- Reescritura de algunos párrafos.
- Revisión completa de la información de las recomendaciones, y actualización de la información (Windows 2000, PAM, etc.).
- Eliminación de la gran parte de los enlaces del Apéndice 1. La fuente de enlaces será en general http://www.rediris.es/cert/links/ .
- Completa revisión del capítulo 6 sobre seguridad en Windows NT. Muchas claves de registro estaban mal escritas. Esperamos que no haya más que tocar en ella.

C.0.2 Versión 0.0.2

Generada el 14 de julio de 1999, una pequeña revisión, antes de las vacaciones.

- Cambios cosméticos y de redacción de algunas secciones.
- Incorporación de este documento de cambios.
- Incorporación de la sección de contribuciones.
- Incorporación de la sección de seguridad de usuarios.
- Incorporación de las notas de parcheado de S.O.

C.0.3 Versión 0.0.1

Primera versión, presentada en los Grupos de Trabajo de Mayo de 1999 de RedIRIS, primer borrador para intentar encontrar voluntarios que contribuyan a la realización de las recomendaciones.