Manual de Seguridad de Debian

Javier Fernández-Sanguino Peña <jfs@debian.org>

Version: 2.4 (revisión de traducción 3), Tue, 26 Apr 2005 04:11:41 +0200

Resumen

Este documento describe el proceso de asegurar y fortalecer la instalación original de Debian. Cubre algunas de las tareas más comunes al configurar un ambiente de red seguro usando Debian GNU/Linux y también muestra información adicional acerca de las herramientas de seguridad disponibles, así como el trabajo desarrollado por el equipo de seguridad de Debian.

Nota de Copyright

Traducción inicial al español realizada bajo la coordinación de Igor Tamara, actualmente en estado de revisión por Jaime Robles y Javier Fernández-Sanguino. *NOTA:* esta traducción aún no ha sido revisada por completo y puede tener aún muchos fallos ortográficos y de traducción. Si encuentra alguno, no dude en enviarlo al autor del documento.

Índice general

Capítulo 1

Introducción

Una de las cosas más dificiles sobre los documentos de seguridad es que cada caso es único. Dos cosas a las que se debe prestar atención son la amenaza del entorno y las necesidades de seguridad, tanto de cada parte individual como del servidor o de la red. Por ejemplo, las necesidades de seguridad de un usuario local son completamente diferentes a las de la red de un banco. Mientras que un usuario local necesita defenderse contra el cracker *script-kiddie*, un banco tiene que preocuparse de ataques dirigidos. Además, el banco tiene que proteger los datos de sus clientes con precisión milimétrica. En resumen, todo usuario debe considerar el equilibrio entre utilización y seguridad/paranoia.

Observe que este manual solamente trata de asuntos relacionados con el software. Ni el mejor software del mundo podría protegerlo si alguien tuviera acceso físico a la máquina. Usted puede colocarla bajo su mesa o puede ponerla en un búnker con un ejército que la protega. Sin embargo, un ordenador de escritorio puede ser muchísimo más seguro (desde el punto de vista del software) que un sistema protegido físicamente si el primero de ellos se configura de la manera apropiada y el segundo está lleno de agujeros de seguridad. Lógicamente, usted debe considerar ambos casos.

Este documento da una apreciación global de lo que usted puede hacer para incrementar la seguridad de su sistema Debian GNU/Linux. Si usted ha leido otros documentos con respecto a la seguridad en Linux, encontrará que describen problemas comunes, los cuales pueden solaparse con este documento. Sin embargo este documento no intenta ser la única fuente de información que usted debería usar, sólo intenta adaptar esa misma información para su aplicación sobre un sistema Debian GNU/Linux. La forma de trabajar de distintas distribuciones es diferente (el ejemplo habitual es la forma de arrancar y para los demonios del sistema); aquí usted encontrará material apropiado para los procedimientos y herramientas utilizadas por Debian.

Si vd. tiene algún comentario o sugerencia, por favor escriba un correo a Javier Fernández-Sanguino (`mailto:jfs@computer.org`) (dirección alternativa jfs@debian.org) y lo incorporará dentro de este manual.

Igualmente, si detecta alguna errata en la traducción de este manual, contacte con él.

1.1. Obtención del manual

Usted puede leer u obtener la última versión del manual de seguridad de Debian del Proyecto de documentación de Debian (http://www.debian.org/doc/manuals/securing-debian-howto/). También puede obtener las fuentes de la versión de cvs a través del Servidor CVS (http://cvs.debian.org/ddp/manuals.sgml/securing-howto/?cvsroot=debian-doc).

En el servidor del proyecto de documentación de Debian no podrá leer el documento en otros formatos (como PDF o txt). Sin embargo puede obtener o instalar el paquete harden-doc (http://packages.debian.org/harden-doc) el cual proporciona este mismo documento en formatos HTML, texto y PDF. Tenga en cuenta que este paquete puede no estar actualizado a la última versión disponible en Internet (¡pero siempre puede utilizar el paquete fuente para compilarse una nueva versión!).

1.2. Notas/Retroalimentación/Organización

Ahora, la parte oficial. Tanto Alexander Reelsen como Javier Fernández-Sanguino escribieron la mayoría de párrafos de este manual, pero en opinión de ambos éste no debería ser el caso. Ambos han crecido y vivido con el software libre, es algo que usan a diario y supongo que usted también. Por eso animamos a todo el mundo a enviar todo tipo de retroalimentación, añadidos o cualquier otra sugerencia que usted pueda tener.

Si desea mantener una cierta sección o mejor un párrafo, escriba a quien mantiene el documento y será bien recibido. Especialmente si encuentra una sección marcada como ARREGLAME, lo que significa que los autores no tienen el tiempo para hacerlo o el conocimiento total necesario sobre el tema, escríbales un correo inmediatamente.

Por el tema de este manual está claro que es muy importante mantenerlo actualizado y usted puede hacer su parte. Por favor, contribuya.

1.3. Conocimiento previo

La instalación de Debian GNU/Linux no es muy difícil y usted mismo debe haber sido capaz de instalarlo. Si tiene algún conocimiento sobre Linux u otro Unix y está familiarizado con la seguridad básica, le será más fácil entender este manual, dado que este documento no puede explicar cada pequeño detalle o característica (de lo contrario hubiera sido un libro en lugar de un manual). Si usted no está tan familiarizado, probablemente debería mirar 'Estar enterado de los problemas de seguridad generales' en la página 15 para saber como encontrar información más detallada.

1.4. Lo que falta escribir (ARREGLAME/PORHACER)

- Escribir sobre herramientas de monitorización remota (para comprobar la disponibilidad del sistema) como «monit», una herramienta para monitorizar los demonios. Consultar la página: `http://linux.oreillynet.com/pub/a/linux/2002/05/09/sysadminguide.html`.
- Considerar si escribir una sección sobre como construir aplicaciones de red basadas en Debian (con información como el sistema básico `equivs` y FAI).
- Buscar en `http://rr.sans.org/linux/hardening.php` información relevante que no ha sido tenida en cuenta.
- Añadir información sobre como configurar un portátil con herramientas de seguridad en Debian: `http://rr.sans.org/linux/debian_laptop.php`.
- Añadir información de como se configura un cortafuegos usando Debian GNU/Linux. La sección con respecto al cortafuegos actualmente está orientada hacia un solo sistema (no protegiendo otros...).
- Añadir información sobre como configurar un cortafuegos proxy con Debian GNU/Linux, estipulando qué paquetes específicos proporcionan servicios proxy (como `xfwp`, `xproxy`, `ftp-proxy`, `redir`, `smtpd`, `nntp-cache`, `dnrd`, `jftpgw`, `oops`, `pdnsd`, `perdition`, `transproxy`, `tsocks`). Debería dirigirse al manual para cualquier otro tipo de información. Además observe que zorp no está aún disponible como un paquete Debian, pero *es* un cortafuegos proxy (los desarrolladores oficiales proporcionan paquetes Debian).
- Información sobre la configuración de servicio con file-rc.
- Revisar todos los enlaces y URLs y arreglar/eliminar los que ya no están disponibles.
- Añadir información sobre sustitutos disponibles (en Debian) para servidores comunes que son útiles para el funcionamiento limitado. Ejemplos:
  - ¿lpr local cups (paquete)?
  - lpr remoto con lpr
  - bind con dnrd/maradns
  - apache con dhttpd/thttpd/wn (¿tux?)
  - exim/sendmail con ssmtpd/smtpd/postfix
  - squid con tinyproxy
  - ftpd con oftpd/vsftp
  - ...
- Más información referente a parches del núcleo relacionados con la seguridad en Debian, incluyendo los mostrados anteriormente y hablando específicamente de como habilitar estos parches en un sistema Debian GNU/Linux.

  - Linux Intrusion Detection (`lids-2.2.19`)
  - Linux Trustees (en el paquete `trustees`)
  - NSA Enhanced Linux (`http://www.coker.com.au/selinux/`)
  - kernel-patch-2.2.18-openwall (`http://packages.debian.org/kernel-patch-2.2.18-openwall`)
  - `kernel-patch-2.2.19-harden`
  - Linux capabilities (en el paquete `lcap`)
  - `kernel-patch-freeswan, kernel-patch-int`

- Detalles sobre como parar servicios innecesarios de red (al margen de `inetd`). Estos se encuentran parcialmente en el procedimiento de bastionado, aunque podrían ampliarse un poco más.
- Información con respecto a rotación de contraseñas, relacionado estrechamente con la política de seguridad.
- Política de seguridad, y sobre la educación de los usuarios sobre la política.
- ¿Más sobre tcpwrappers y wrappers en general?.
- `hosts.equiv` y otros agujeros de seguridad.
- Temas relacionados con servidores de ficheros tales como Samba y NFS.
- suidmanager/dpkg-statoverrides.
- lpr y lprng.
- Elimininar cosas de IP en GNOME.
- Hablar sobre pam_chroot (consultar `http://http://lists.debian.org/debian-security/2002/debian-security-200205/msg00011.html`) y su utilidad para limitar a los usuarios. Introducir información relacionada con `http://online.securityfocus.com/infocus/1575`. `Pdmenu`, por ejemplo, está disponible en Debian (mientras que flash no lo está).
- Hablar sobre enjaular servicios (chroot). Información adicional en `http://www.linuxfocus.org/English/January2002/aritcle225.shtml`, `http://www.networkdweebs.com/chroot.html` y `http://www.linuxsecurity.com/feature_stories/feature_story-99.html`.
- Hablar sobre los programas para hacer jaulas (chroot). `Compartment` y `chrootuid` están en la cola de entrada. Además, algunos otros (makejail, jailer) podrían ser introducidos en el futuro.
- Añadir información suministrada por Karl Hegbloom con respecto a enjaular BIND 9. Consultar `http://people.pdxlinux.org/~karlheg/Secure_Bind9_uHOWTO/Secure_Bind_9_uHOWTO.xhtml`.

- Añadir información suministrada por Pedro Zornenon con respecto a enjaular BIND 8 aunque únicamente para la versión potato :(. Consultar `http://people.debian.org/~pzn/howto/chroot-bind.sh.txt` (includo todo el título).
- Más información con respecto a los programas de análisis de bitácoras (ie. logcheck y logcolorise).

1.5. Listado de cambios/Historia

1.5.1. Versión 2.4

Cambios por Javier Fernández-Sanguino Peña.

- Reescrita la parte de la sección BIOS.

1.5.2. Versión 2.3

Cambios por Javier Fernández-Sanguino Peña.

- La mayoría de los archivos se encuentran marcados con la etiqueta file.
- Fallo de ortografía observado por Edi Stojicevi.
- La sección de herramientas de auditoría remota se ha modificado ligeramente.
- Se añadieron algunas piezas de PORHACER.
- Se añadió más información con respecto a impresoras y los archivos de configuración de cups (tomado de un hilo en debian-security).
- Se añadió un parche suministrado por Jesus Climent relacionado con el acceso de usuarios válidos del sistema en Proftpd cuando se ha configurado como servidor anónimo.
- Pequeños cambios sobre divisiones de esquemas para el caso especial de servidores de correo.
- Se añadió Hacking Linux Exposed para la sección de los libros.
- Error en directorio notificado por Eduardo Pérez Ureta.
- Error ortográfico /etc/ssh en la checklist notificado por Edi Stojicevi.

1.5.3. Versión 2.3

Cambios por Javier Fernández-Sanguino Peña.

- Cambio de ubicación del fichero de configuración de dpkg.
- Alexander eliminado de la información de contacto.
- Se añadieron direcciones de correo alternativas.
- Se arregló la dirección de correo de Alexander (aún entre comentarios).
- Se arregló la ubicación de la llave publicada de la distribución (gracias a Pedro Zorzenon por señalarlo).

1.5.4. Versión 2.2

Cambios por Javier Fernández-Sanguino Peña.

- Se arreglaron errores ortográficos gracias a Jamin W. Collins.
- Se añadió una referencia a la página de manual de apt-extracttemplate (documenta la configuración APT::ExtracTemplate).
- Se añadió la sección sobre SSH restringido. Información basada en los correos enviados por Mark Janssen, Christian G. Warden y Emmanuel Lacour en la lista de correo debian-security.
- Se añadió información sobre programas antivirus.
- Se añadió un FAQ: las bitácoras de *su* debido al cron que se ejecuta como root.

1.5.5. Versión 2.1

Cambios por Javier Fernández-Sanguino Peña.

- Se eliminó el ARREGLAME de lshell gracias a Oohara Yuuma.
- Se agregó un paquete para sXid y se eliminaron comentarios desde que éste se encuentra disponible.
- Se corrigieron algunos fallos ortográficos descubiertos por Oohara Yuuma.
- ACID está ahora disponible en Debian (en el paquete acidlab). Gracias a Oohara Yuuma por notificarlo.
- Se arreglaron los URLs de seguridad de Linux (gracias a Dave Wreski por comentarlo).

1.5.6. Versión 2.0

Cambios por Javier Fernández-Sanguino Peña. Quise cambiar la versión 2.0 cuando todos los ARREGLAMEs estaban cambiados, pero los eliminé de los números 1.9X :(

- Se convirtió el HOWTO a un manual (ahora puedo decir apropiadamente LEJM).
- Se añadió más información con respecto a los tcpwrappers y a Debian (ahora muchos servicios están compilados con soporte para ellos, así que ya no es problema de `inetd`).
- Se aclaró la información sobre como deshabilitar el servicio rpc para hacerlo más consistente (la información rpc hacía referencia a update-rc.d).
- Se añadieron pequeñas notas sobre lprng.
- Se agregó alguna información sobre servidores comprometidos (aún muy rústico).
- Se corrigieron fallos ortográficos detectados por Mark Bucciarelli.
- Se añadieron algunos pasos en la recuperación de password para proteger los casos en que el administrador tiene paranoid-mode=on.
- Se añadió información para colocar paranoid-mode=on cuando el login está en la consola.
- Nuevo párrafo para introducir las configuraciones de servicios.
- Se reorganizó la sección *Después de la instalación*. Además ésta se descompone en varios temas más, facilitando la lectura.
- Se escribió información sobre como montar un cortafuegos con el montaje estándar de Debian 3.0 (paquete iptables).
- Un pequeño párrafo explicando por qué la instalación estando conectado a Internet no es buena idea y cómo evitar esto usando las herramientas Debian.
- Un pequeño párrafo referenciando a un trabajo publicado en el IEEE sobre como aplicar a tiempo parches de seguridad.
- Un apéndice sobre como montar una máquina snort Debian basada en lo que Vladimir envió a la lista de seguridad de debian-security (3 de septiembre de 2001).
- Información sobre como logcheck se monta en Debian y como puede ser usado en el sistema HIDS.
- Información sobre la contabilidad del usuario y los beneficios de los análisis.
- Se incluyó la configuración apt.conf para leer únicamente /usr copiado del correo de Olaf Meeuwissen a la lista de correos debian-security.

- Nueva sección en VPN con algunas indicaciones y paquetes disponibles en Debian (se necesita contenido de como establecer VPNs y problemas específicos de Debian), basado en los envíos de Jaroslaw Tabor y Samuli Suonpaa a la lista debian-security.
- Una corta nota con respecto a algún programa que automáticamente construye jaulas para el cambio de directorio raíz.
- Nuevo artículo FAQ con respecto a identd basado en una discusión en la lista de correo debian-security (febrero 2002, empezado por Johannes Weiss).
- Nuevo artículo FAQ con respecto al inetd basada en una discusión en la lista de correo debian-security (febrero 2002).
- Se introdujo una nota en rcconf en la sección "deshabilitar servicios".
- Varió el enfoque con respecto a LKM, gracias a Philipe Gaspar.
- Se añadieron enlaces a documentos del CERT y fuentes de información de Couterpane.

1.5.7. Versión 1.99

Cambios por Javier Fernández-Sanguino Peña.

- Se añadió un nuevo FAQ con respecto al tiempo de arreglo de vulnerabilidades de seguridad.
- Secciones FAQ reorganizadas.
- Se comenzó a escribir la sección con respecto al firewalling en Debian GNU/Linux (podría ser ampliado un poco).
- Eliminados errores ortográficos detectados por Matt Kraai.
- Cambiada la información de DNS.
- Se agregó información sobre whisker y nbtscan para la sección de auditoría.
- Se modificó algún URL erróneo.

1.5.8. Versión 1.98

Cambios por Javier Fernández-Sanguino Peña.

- Se añadió una nueva sección con respecto a la auditoría usando Debian GNU/Linux.
- Se añadió información con respecto al demonio finger tomada de la lista de correo de seguridad.

1.5.9. Versión 1.97

Cambios por Javier Fernández-Sanguino Peña.

- Se cambió el enlace a Linux Trustees.
- Se corrigieron fallos ortográficos (parches de Oohara Yuuma y Pedro Zorzenon).

1.5.10. Versión 1.96

Cambios por Javier Fernández-Sanguino Peña.

- Se reorganizó el servicio de instalación y se añadieron y eliminaron algunas notas.
- Se añadieron algunas notas con respecto al uso de sistemas de comprobación de integridad como herramientas de detección de intrusos.
- Se añadió un capítulo con respecto firmas de paquetes.

1.5.11. Versión 1.95

Cambios por Javier Fernández-Sanguino Peña.

- Se añadieron notas con respecto a la seguridad de Squid enviadas por Philipe Gaspar.
- Cambios de enlaces sobre rookits gracias a Philipe Gaspar.

1.5.12. Versión 1.94

Cambios por Javier Fernández-Sanguino Peña.

- Se añadieron algunas notas con respecto a Apache y Lpr/lpng.
- Se añadió alguna información con respecto a noexec y particiones de acceso aleatorio.
- Reescritura de como puede el usuario ayudar en los asuntos de seguridad Debian (FAQ).

1.5.13. Versión 1.93

Cambios por Javier Fernández-Sanguino Peña.

- Se arregló el sitio donde se encuentra el programa de correo.
- Se añadieron algunos nuevos elementos a las FAQ.

1.5.14. Versión 1.92

Cambios por Javier Fernández-Sanguino Peña.

- Añadió una pequeña sección de como se maneja la seguridad en Debian.
- Clarificación sobre las contraseñas MD5 (gracias a 'rocky').
- Añadida un poco más de información con respecto a harden-X de Stephen Egmond.
- Añadió algunos artículos nuevos al FAQ.

1.5.15. Versión 1.91

Cambios por Javier Fernández-Sanguino Peña.

- Añadida un poco de información forense enviada por Yotam Rubin.
- Añadió información de como construir una red trampa con Debian GNU/Linux.
- Añadidas unas cosas a hacer más.
- Corrección de más errores ortográficos (gracias a Yotam).

1.5.16. Versión 1.9

Cambios por Javier Fernández-Sanguino Peña.

- Se añadió un parche para arreglar errores de ortografía y un poco de nueva información (contribuido por Yotam Rubin).
- Se añadieron referencias a otra documentación en línea (y no en línea) tanto en una única sección (vea 'Estar enterado de los problemas de seguridad generales' en la página 15) como dentro de algunas secciones.
- Añadida alguna información sobre como configurar opciones de bind para restringir el acceso al servidor de DNS.
- Agregada información de como bastionar un sistema de Debian automáticamente (con respecto al paquete harden y bastille).
- Eliminados algunos PORHACER hechos y añadidos otros nuevos.

1.5.17. Versión 1.8

Cambios por Javier Fernández-Sanguino Peña.

- Se añadió la lista de usuario/grupo por defecto proporcionada por Joey Hess (enviada a la lista de correo debian-security).
- Se añadió información sobre los rootkits LKM ('LKM - Loadable Kernel Modules (módulos cargables en el núcleo)' en la página 88) contribuida por Philipe Gaspar.
- Se agregó información sobre Proftp contribuida por Emmanuel Lacour.
- Se recuperó el apéndice checklist de Era Eriksson.
- Se añadieron algunos artículos nuevos al PORHACER y se arreglaron otros.
- Se incluyeron manualmente los parches de Era dado que no se habían incluido en la versión anterior.

1.5.18. Versión 1.7

Cambios por Era Eriksson.

- Se arreglaron errores ortográficos y se cambiaron algunas palabras.

Cambios por Javier Fernández-Sanguino Peña.

- Cambios menores de las etiquetas para seguir removiendo las tt, y sustituirlas por las etiquetas de prgn/package.

1.5.19. Versión 1.6

Cambios por Javier Fernández-Sanguino Peña.

- Se añadió el enlace al documento como se publicó en el DDP (debería reemplazar el original en el futuro cercano).
- Comenzó un mini-FAQ (debería extenderse) con algunas preguntas recuperadas de mi buzón.
- Se añadió información general a considerar cuando se está bastionando.
- Se añadió un párrafo con respecto al envío de correo local (entrante).
- Se añadieron enlaces de información.

- Se añadió información con respecto al servicio de impresión.
- Se añadió una lista de chequeo de bastionado.
- Se reorganizó información de NIS y RPC.
- Se añadieron algunas notas tomadas mientras está leyendo este documento en mi nuevo visor :)
- Se arreglaron algunas líneas mal formateadas.
- Se corrigieron algunos errores ortográficos.
- Se añadieron ideas Geniales/Paranoícas contribuidas por Gaby Schilders.

1.5.20. Versión 1.5

Cambios por Josip Rodin y Javier Fernández-Sanguino Peña.

- Se añadieron párrafos relacionados con bind y algunos ARREGLAMEs.

1.5.21. Versión 1.4

- Se revisaron algunos setuid pequeños.
- Cambios menores.
- Se averiguó como usar `sgml2txt -f` para la versión txt.

1.5.22. Versión 1.3

- Se añadió una actualización de seguridad después del párrafo de la instalación.
- Se añadió un párrafo del proftpd.
- En ésta ocasión se escribió algo sobre XDM, disculpas por el anterior.

1.5.23. Versión 1.2

- Muchas correcciones de gramática por James Treacy, nuevo párrafo de XDM.

1.5.24. Versión 1.1

- Errores ortográficos, cambios varios.

1.5.25. Versión 1.0

- Versión inicial.

1.6. Créditos y agradecimientos

- Alexander Reelsen escribió el documento original.
- Javier Fernández-Sanguino añadió aún más información al documento original.
- Robert van der Meulen aportó los párrafos de quota y muchas buenas ideas.
- Ethan Benson corrigió los párrafos de PAM y sugirió buenas ideas.
- Dariusz Puchalak hizo contribuciones a muchos capítulos.
- Gaby Schilders contribuyó a una buena idea de Genio/Paranoia.
- Era Eriksson resolvió problemas de idioma en muchos lugares y contribuyó al apéndice de la lista de comprobaciones.
- Philipe Gaspar escribió la información de LKM.
- Yotam Rubin contribuyó a los ajustes de muchos fallos ortográficos así como a la información con respecto a las versiones de bind y las contraseñas md5.
- Todas las personas que hicieron sugerencias que, eventualmente, se incluyeron aquí (consulte 'Listado de cambios/Historia' en la página 5).
- (de Alexander) A todas las personas que me animaron a escribir, este COMO (El cual posteriormente se convirtió en el manual) .
- La totalidad del proyecto Debian.

Capítulo 2

Antes de empezar

2.1. ¿Para qué quiere usted este sistema?

Asegurar Debian no se diferencia mucho de asegurar otro sistema; para hacer esto apropiadamente primero usted debe decidir lo que pretende hacer con éste. Luego tenga en cuenta que las siguientes tareas necesitan ser tomadas con cuidado si usted quiere un sistema de seguridad verdadero.

Usted encontrará que este manual está escrito de abajo hacia arriba, lo cual significa que usted leerá alguna información sobre tareas para hacer antes, durante y después de que la instalación de su sistema Debian esté hecha. Algunas tareas pueden ser pensadas así, tales como:

- Decidir cuáles servicios usted necesita, y limitar su sistema para ellos. Esto incluye desactivación/desinstalación de servicios innecesarios, y la adición de filtros como cortafuegos, o tcpwrappers.
- Limitar usuarios y permisos en su sistema.
- Asegurar los servicios ofrecidos, de tal forma que, en caso de un servicio comprometido, el impacto a su sistema sea minimizado.
- Usar las herramientas apropiadas para garantizar que el uso desautorizado se detecte, de tal manera que usted pueda tomar las medidas oportunas.

2.2. Estar enterado de los problemas de seguridad generales

El siguiente manual (por lo general) no entra en detalles del por qué algunos asuntos son considerados riesgos de seguridad. Sin embargo, usted debería tener una mayor información en lo que se refiere a UNIX en general y (en particular) a la seguridad de Linux. Tome algo de tiempo para leer acerca de la seguridad en documentos relacionados para poder tomar decisiones cuando usted se encuentre con diferentes opciones. Debian GNU/Linux está basado

en el núcleo de Linux, por lo que la mayor parte de la información referente a Linux, así como de otras distribuciones y en general la seguridad en UNIX también es aplicable aquí (incluso sí las herramientas usadas, o los programas disponibles, difieren).

Algunos documentos útiles incluyen:

- El Linux Security HOWTO (http://www.linuxdoc.org/HOWTO/Security-HOWTO.html) (también disponible en LinuxSecurity (http://www.linuxsecurity.com/docs/LDP/Security-HOWTO.html)) es una de las mejores referencias en lo que se refiere a la seguridad de Linux en general.
- El Security Quick-Start HOWTO for Linux (http://www.linuxsecurity.com/docs/LDP/Security-Quickstart-HOWTO/) es también un buen punto de arranque para usuarios novatos (para ambos, Linux y la seguridad).
- El Linux Security Administrator's Guide (http://seifried.org/lasg/) (proporcionado en Debian a través del paquete `lasg`) es una guía completa que conecta todos los asuntos relacionados con la seguridad en Linux, desde la seguridad del núcleo hasta VPNs. Esto es algo obsoleto (sin actualizar desde 1999) y ha sido reemplazado por la base del conocimiento de la Seguridad de Linux (actualmente no está disponible en línea, pero usualmente está en http://www.securityportal.com/Lksb/) (sin embargo en este momento no está ahí). Esta documentación también es proporcionada en Debian a través del paquete `lksb`.
- En Securing and Optimizing Linux: RedHat Edition (http://www.linuxdoc.org/links/p_books.html#securing_linux) usted puede encontrar un documento similar a este manual pero relacionado con RedHat. Algunos de los asuntos no son específicos de la distribución y también se aplican a Debian.
- IntersectAlliance ha publicado un documento que puede ser usado como una carta de referencia sobre como fortalecer los servidores de Linux. Esto está disponible en http://www.intersectalliance.com/projects/index.html.
- Para administradores de red, una buena referencia para construir una red segura es el Securing your Domain HOWTO (http://www.linuxsecurity.com/docs/LDP/Securing-Domain-HOWTO/).
- Si quiere evaluar los programas que usted va a usar (o quiere reforzar uno de los nuevos) debería leer el Secure Programs HOWTO (http://www.linuxdoc.org/HOWTO/Secure-Programs-HOWTO.html).
- Si usted está considerando instalar las capacidades de cortafuegos, usted debe leer el Firewall HOWTO (http://www.linuxdoc.org/HOWTO/Firewall-HOWTO.html) y el IPCHAINS HOWTO (http://www.linuxdoc.org/HOWTO/IPCHAINS-HOWTO.html).
- Finalmente, una buena carta para tener acceso es la Linux Security RefenceCard (http://www.linuxsecurity.com/docs/QuickRefCard.pdf).

De todos modos, usted puede adquirir más información con respecto a los servicios aquí explicados (NFS, NIS, SMB) en muchos de los HOWTOs del Linuxdoc Project (http://www.linuxdoc.org/). Algunos de estos documentos hablan sobre la parte de seguridad de un servicio dado, por lo que asegúrese de echarles un vistazo.

Los documentos HOWTO del proyecto de Documentación están disponibles en Debian GNU/Linux por medio de la instalación del `doc-linux-text` (versión texto) o `doc-linux-html` (versión html). Después de la instalación estos documentos estarían disponibles en `/usr/share/doc/HOWTO/en-txt` y en los directorios `/usr/share/doc/HOWTO/en-html`, respectivamente.

Otros libros de Linux recomendados:

- Seguridad Máxima de Linux: Una guía de Hacker para proteger su servidor Linux y la red. Anónimo. Libro de bolsillo - 829 páginas. Publicación Sams. ISBN: 0672313413. Julio 1999.
- Seguridad Linux por John S. Flowers. Nuevos viajeros: ISBN: 0735700354. Marzo 1999.
- Hacking Linux Exposed (http://www.linux.org/books/ISBN_0072127732.html) por Bryan Hatch. McGraw Hill educación superior. ISBN: 0072127732. Abril 2001.

Otros libros (también relacionados con los temas generales de UNIX y la seguridad, y no exclusivamente con Linux):

- Practical Unix and Internet Security (2nd Edition) (http://www.ora.com/catalog/puis/noframes.html) Garfinkel, Simpson y Spafford, Gene. O'Reilly Asociados. ISBN 0-56592-148-8. 1004pp. 1996.
- Firewalls y la Seguridad de Internet. Cheswick, William R. y Bellovin, Steven M. Addison Wesley. ISBN 0-201-63357-4. 320pp.

Algunos sitios Web útiles para mantenerse al tanto con respecto a la seguridad:

- Security Focus (http://www.securityfocus.com) el servidor que contiene la base de datos y las listas de vulnerabilidad de Bugtraq. Proporciona información general de seguridad, noticias y reportes.
- Linux Security (http://www.linuxsecurity.com/). Información referente a la seguridad de Linux en general (herramientas, noticias...). La más útil es la página main documentation (http://www.linuxsecurity.com/resources/documentation-1.html).
- Linux firewall and security site (http://www.linux-firewall-tools.com/linux/). Con información general con respecto a los cortafuegos en Linux y las herramientas para controlarlos y administrarlos.

2.3. ¿Cómo maneja Debian la seguridad?

Al dar un vistazo general sobre la seguridad en Debian GNU/Linux usted debería tomar nota de los diferentes temas que Debian usa para proveer un sistema de seguridad en conjunto:

- Los problemas de Debian siempre son manejados abiertamente, inclusive los relacionados con la seguridad. Como dice en Debian Social Contract (http://www.debian.org/social_contract): *Nosotros no encubriremos los problemas, mantendremos el reporte de la base de datos abierto para el público todo el tiempo. Los reportes que los usuarios envíen en línea se colocarán inmediatamente para que sean visibles por otros.* Los temas de seguridad son discutidos abiertamente en la lista de correo debian-security. Los avisos de seguridad de Debian son enviados a listas de correo públicas (a las dos, internas y externas) y son colocadas en el servidor público.
- Debian sigue los asuntos de seguridad atentamente. El equipo de seguridad vigila muchas fuentes de seguridad relacionadas, siendo la más importante Bugtraq (http://www.securityfocus.com/cgi-bin/vulns.pl), a la búsqueda de paquetes con problemas de seguridad que puedan estar incluídos en Debian.
- Las actualizaciones de seguridad son la principal prioridad. Cuando surge un problema de seguridad en un paquete Debian, la actualización de seguridad es preparada tan rápido como es posible y distribuída para nuestras publicaciones estables e inestables, incluyendo todas las arquitecturas.
- La información referente a la seguridad es centralizada en un solo punto: http://security.debian.org/.
- Debian siempre está tratando de mejorar en conjunto la seguridad de la distribución empezando nuevos proyectos, como los mecanismos de verificación automática de firmado de paquetes.
- Debian trata de proveer una cantidad útil de herramientas relacionadas con la seguridad para la administración y monitorización del sistema. Los desarrolladores tratan de relacionar estrechamente estas herramientas con la distribución para hacerlas mejores y así reforzar las políticas locales de seguridad. Las herramientas incluyen: controladores de integridad, herramientas de auditoría, herramientas de firewall, herramientas para detectar intrusiones, etc.
- Los mantenedores del programa están enterados de los temas de seguridad. Esto conduce a muchos servicios "seguros por defecto" en la instalación, que puede imponer ciertos límites, algunas veces, para su uso normal. Sin embargo, Debian trata de balancear los asuntos de seguridad y la facilidad de administración, por ejemplo, los sistemas no son instalados desactivados, como en las distribuciones de la familia BSD. De cualquier modo, algunos asuntos especiales de seguridad, como programas setuid, forman parte de Debian Policy (http://www.debian.org/doc/debian-policy/).

Este mismo documento trata de hacerse valer, tanto como la mejor de las distribuciones seguras, publicando información de seguridad específica de Debian la cual complementa otros

documentos de información de seguridad relacionados con las herramientas usadas por Debian o por el sistema operativo en sí mismo (ver 'Estar enterado de los problemas de seguridad generales' en la página 15).

Capítulo 3

Antes y durante la instalación

3.1. Escoger una contraseña BIOS

Antes de instalar algún sistema operativo en su computador, establezca una contraseña BIOS. Después de la instalación (una vez se haya posibilitado la entrada desde el disco duro) regrese a la BIOS y cambie la secuencia de arranque del sistema para impedir el arranque desde el disco flexible, el CD-ROM y otros dispositivos desde los que no se debería arrancar. De otro modo un cracker solo necesitaría acceso físico y un disco de arranque para tener acceso a la totalidad de su sistema.

Inhabilitar El ingreso al programa sin una contraseña es mejor. Este puede ser muy efectivo si usted está administrando un servidor, porque éste no es reiniciado muy frecuentemente. El inconveniente para esta táctica es que el ingreso requiere intervención humana la cual puede causar problemas si la máquina no es de fácil acceso.

3.2. Escoger inteligentemente un esquema de partición

Un esquema de partición inteligente depende de cómo sea usada la máquina. Una buena regla para torpes es ser completamente tolerante con sus particiones y prestar atención a los siguientes factores:

- Cualquier jerarquía de directorios en la cual un usuario tiene permiso de escritura, así como `/home` y `/tmp`, debería estar en una partición separada. Esto reduce el riesgo de un DoS por parte de un usuario, al llenar su punto de montaje de "`/`" y tornar el sistema inservible. (Nota: esto no es estrictamente cierto, dado que siempre hay algún espacio reservado para el administrador, el cual un usuario normal no puede llenar).
- Cualquier partición que pueda variar, p.e. `/var` (especialmente `/var/log`) también debería estar en una partición separada. En un sistema Debian, usted debe crear `/var` un poco más grande de lo normal, debido a que los paquetes descargados (el apt cache) son guardados en `/var/cache/apt/archives`. Esto es mucho más importante para los

servidores del correo (`/var/mail` y/o `/var/spool/mail`) ya que los usuarios remotos pueden llenar la cola del correo (intencionada o no intencionadamente).

- Cualquier partición donde usted quiera instalar un software fuera de la distribución debe estar en una partición separada. De acuerdo con la jerarquía estándar de archivos, serían `/opt` o `/usr/local`. Si estos directorios están en particiones separadas, no serán borrados si usted tiene que reinstalar Debian.
- Desde el punto de vista de seguridad, tiene sentido intentar mover los datos estáticos a su propia partición y luego montar la partición en modo sólo lectura. Mejor aún, ponga los datos en un medio de sólo lectura. Ver más detalles a continuación.

3.3. No se conecte a Internet hasta que este listo

El sistema que usted va a instalar no debe ser conectado inmediatamente a Internet durante la instalación. Esto puede sonar estúpido pero usualmente se hace. Ya que el sistema instalará y activará servicios inmediatamente, si el sistema es conectado a Internet y los servicios no están correctamente configurados, usted está abierto a sufrir un ataque.

También verifique si algún servicio tiene nuevas vulnerabilidades de seguridad no arregladas en los paquetes que usted está utilizando para la instalación. Normalmente esto es cierto si usted está instalando desde un medio antiguo (como CD-ROMs) . En este caso, ¡puede estar comprometido antes de que la instalación se haya terminado!.

Como la instalación y las actualizaciones de Debian pueden ser realizadas desde Internet, usted debe pensar que es una buena idea usar esta característica en la instalación. Si el sistema va a ser conectado directamente a Internet (y sin estar protegido por un cortafuegos o NAT), es mejor instalar sin conexión a Internet, utilizando un espejo local de paquetes tanto para los fuentes de los paquetes de Debian como para las actualizaciones de seguridad. Usted puede configurar los espejos de paquetes usando otro sistema conectado a Internet con herramientas específicas de Debian (si es un sistema Debian) como `apt-move` o `apt-proxy`, u otras herramientas comunes para espejos que provean los archivos para el sistema instalado.

3.4. Colocar una contraseña de root (Administrador de Linux)

Colocar una buena contraseña a root es el más básico requerimiento para tener un sistema seguro.

3.5. Activar contraseñas shadow y md5

Al final de la instalación se le preguntará si las contraseñas shadow deben ser habilitadas. Responda con un SI a esta pregunta, y así las contraseñas se mantendrán en el archivo `/etc/shadow`. Solo el usuario root y el grupo shadow tienen acceso de lectura a este archivo, así

que los usuarios no estarán autorizados a realizar una copia de este archivo con el objeto de ejecutar un decodificador de contraseñas. Usted puede cambiar entre las contraseñas shadow y las contraseñas normales en cualquier momento utilizando `shadowconfig`. Además, durante la instalación se le preguntará si quiere usar las contraseñas con una función MD5 aplicada. Esto es generalmente una muy buena idea, ya que permite unas contraseñas más extensas y una mejor encriptación.

Lea más acerca de las contraseñas shadow en Shadow Password (`http://www.linuxdoc.org/HOWTO/Shadow-Password-HOWTO.html`) (`/usr/share/doc/HOWTO/en-txt/Shadow-Password.txt.gz`).

3.6. Ejecute el mínimo número de servicios requeridos

Los servicios son programas tales como los servidores de ftp y los servidores web. Ya que ellos deben estar *escuchando* las conexiones entrantes que requieren el servicio, computadores externos podrán conectarse con usted. Los servicios son algunas veces vulnerables (i.e. puede estar comprometido bajo un ataque dado) y por lo tanto son un riesgo de seguridad.

Usted no debería instalar servicios innecesarios para su máquina. Todo nuevo servicio instalado, quizás sin evidencia (o evidentemente), puede crear fallas de seguridad en su computador.

Como es bien sabido, cuando usted instala un servicio dado, el comportamiento erróneo es activarlo. En una instalación por defecto de Debian, sin servicios instalados, la huella de los servicios recorridos es lenta y es aun más lento cuando se habla acerca de los servicios ofrecidos en la red. La huella en Debian 2.1 no era tan difícil como la 2.2 (algunos servicios inetd fueron permitidos por descuido) y en el Debian 2.2 el Rpc PORTMAPPER se permite para la instalación. Rpc es instalado por descuido porque este es necesitado por muchos servicios, por ejemplo NFS, para recorrer en un sistema dado. Esto puede ser removido fácilmente, sin embargo, vea 'Deshabilitar los demonios' en esta página para saber como desactivarlo.

Cuando usted instale un nuevo servicio relacionado con la red (demonio) en su sistema Debian GNU/ Linux, éste puede ser habilitado de dos formas: a través del superdemonio de inetd (i.e una línea será añadida a `/etc/inetd.conf`) o a través de un programa automático que se ratifica a si mismo con el conector de unidades del sistema. Los programas automáticos son controlados a través de los archivos `/etc/init.d` , los cuales son llamados al momento de entrar a través del mecanismo SysV (o una alternativa mas) por usar conexiones del sistema en `/etc/rc?.d/*` (para mas información sobre como hacer la lectura `/usr/share/doc/sysvinit/README.runlevels.gz`).

Si usted aun desea tener algunos servicios para usarlos de vez en cuando, use los comandos de update, e.g. 'update-inetd' y 'update-rc.d' para eliminarlos del proceso de inicio.

3.6.1. Deshabilitar los demonios

Incapacitar un demonio (o servicio) es muy sencillo. Hay diferentes métodos:

- Eliminar las conexiones de `/etc/rc${runlevel}.d/` o renombrar las conexiones (así que ellos no empezarán con 'S')
- Mover el archivo de escritura (`/etc/init.d/_service_name_`) a otro nombre (por ejemplo `/etc/init.d/OFF._service_name_`)
- Eliminar la marca de ejecución del archivo `/etc/init.d/_service_name_`.
- Editar el fichero `/etc/init.d/_service_name_` para que éste se pare nada más ejecutarse.

Usted puede eliminar estas conexiones de `/etc/rc${runlevel}.d/` manualmente o usando `update-rc.d` (ver `update-rc.d(8)`). Por ejemplo, Usted puede inhabilitar un servicio de ejecución en los niveles haciendo:

```
update-rc.d stop XX 2 3 4 5 .
```

Por favor note que, si usted no *está* usando `file-rc`, `update-rc.d -f _service_ remove` no trabajara adecuadamente, ya que *todas* las conexiones son removidas, cuando se realice la reinstalación o crezca el paquete, estas conexiones estarán regeneradas (probablemente no como usted quería). Si usted piensa que esto no es intuitivo probablemente usted estaría en lo cierto (vea Bug 67095 (`http://bugs.debian.org/67095`). Del manual de paginas:

```
Si algunos archivos /etc/rcrunlevel.d/[sk]??nombre ya existen entonces
update-rc.d no hace nada. Esto ocurre porque el sistema administrador
puede reorganizar las conexiones, permitiendo que ellos dejen la
ultima conexión que queda, sin tener su configuración sobrescrita.
```

Si usted esá usando `file-rc` toda la información relativa a los servicios de entrada está manejada por un archivo de configuración común y es mantenido aun sí los paquetes son removidos del sistema.

Usted puede usar el TUI (Texto Interfaces del Usuario) proporcionado por `rcconf` para hacer todos estos cambios fácilmente (`rcconf` trabaja de dos formas por file-rc y el sistema normal V runlevels).

Otros métodos (no recomendables) de servicios inhabilitados son: `chmod 644 /etc/init.d/_demonio_` (pero éste provocará un mensaje de error cuando usted entre al sistema) o modificar la escritura de `/etc/init.d/_demonio_` (añadiendo una línea con `exit 0` al comienzo o comentando la parte `start-stop-daemon`). Ya que los archivos init.d son archivos de configuración, éstos no serán sobrescritos al actualizar programas.

Desafortunadamente, a diferencia de otros sistema operativos (UNIX), los servicios en Debian no pueden ser desactivados al modificar los archivos en `/etc/default/_servicename_`.

ARREGLAME: Proporcionar mas información sobre el manejo de demonios usando file-rc.

3.6.2. Deshabilitar los servicios inetd

Usted debe parar todos los servicios innecesarios en su sistema, como echo, chargen, discard, daytime, time, talk, ntalk y r-services (rsh, rlogin y rcp) los cuales son considerados ALTAMENTE inseguros (en cambio use ssh). Después de inhabilitarlos, usted debe revisar si realmente necesita el demonio inetd. Mucha gente prefiere usar los demonios en lugar de servicios de llamada via inetd. En los ataques de Denial of service existen posibilidades en contra de inedt, las cuales pueden incrementar la carga de la máquina tremendamente. Si usted aun quiere ejecutar algún tipo de servicio inedt, utilize un demonio de inet más configurable como xinetd o rlinetd.

Usted puede inhabilitar directamente los servicios por la edición de `/etc/inetd.conf`, pero Debian proporciona una mejor alternativa para hacer esto:`update-inetd` (el cual comenta los servicios de una forma que este pude fácilmente ser reactivado de nuevo). Usted podría eliminar el demonio telnet ejecutando estos comandos para cambiar el archivo de configuración y reiniciar el demonio (en este caso el servicio telnet es inhabilitado):

```
/usr/sbin/update-inetd --disable telnet
```

Si usted quiere tener servicios escuchando, pero no quiere que escuchen todas las direcciones IP de su host, usted podría usar una característica no documentada de inetd.. O usar un demonio inetd alterno como `xinetd`.

3.7. Lea las listas de correo de seguridad de Debian

Nunca es malo dar un vistazo en cualquier lista de correo de los anuncios de seguridad de Debian, donde son anunciados avisos y correcciones para promocionar paquetes por el equipo de Debian, o en debian-security@lists.debian.org, donde usted puede participar en discusiones acerca de cosas relacionadas a la Seguridad de Debian.

Para recibir alertas importantes de la seguridad de update. Envíe un e-mail a debian-security-announce-request@lists.debian.org (`mailto:debian-security-announce-request@lists.debian.org`)con la palabra 'suscribir' en la línea "subject". Usted también puede suscribirse a esta lista e-mail moderada en la pagina Web `http://www.debian.org/MailingLists/subscribe`

Estas listas de correo tienen un muy bajo volumen, y al suscribirse a esta usted será inmediatamente alertado de los asuntos de seguridad de la distribución Debian. Esto le permite rápidamente cargar nuevos paquetes con correcciones en la seguridad, lo cual es muy importante en el mantenimiento de un sistema seguro. (Vea'Ejecute una actualización de seguridad' en la página 32 para mas detalles sobre como hacer esto.)

Capítulo 4

Después de la instalación

4.1. Colocar una contraseña a lilo o grub

Es muy fácil entrar a una shell con el usuario root y cambiar las contraseñas simplemente tecleando "<name-of-your-bootimage> init=/bin/sh". Luego de cambiar las contraseñas y reingresar al sistema, la persona ha tiene acceso ilimitado (como root) y puede hacer cualquier cosa que el/ella quiera en el sistema. Después de este procedimiento, usted no tendrá acceso a su sistema, porque usted no conoce la contraseña de root.

Asegúrese que esto no pueda suceder, usted debería colocar una contraseña para el cargador de linux. Usted puede escoger entre una contraseña global y una contraseña para una imagen.

Para LILO usted necesita editar el archivo `/etc/lilo.conf` y agregar una contraseña y restringirlo como en el siguiente ejemplo:

```
image=/boot/2.2.14-vmlinuz
 label=Linux
 read-only
 password=hackme
 restricted
```

Cuando haya terminado, ejecute LILO. Omitir la línea `restricted` produce que LILO siempre pida una contraseña, aun si no se le pasan parámetros a LILO.Los permisos defectuosos de `/etc/lilo.conf` para que el gran root lea yescriba, y se habilite el acceso de solo lectura para el grupolilo.conf's de root.

Si usted usa GRUB en lugar de LILO, edite `/boot/grub/menu.lst` y agregue las siguientes dos líneas al inicio (sustituyendo, por supuesto 'hackme' con la contraseña deseada). Esto previene a los usuarios de editar los ítems de entrada. 'timeout3' especifica tres segundos antes del arranque del sistema por defecto.

```
timeout 3
password hackme
```

Para asegurar mas la integridad de la contraseña, usted podría guardarla una forma encriptada. La utilidad de grub-d5-crypt es que genera una contraseña la cual es compatible con el algorítmo (md5) de encripción de grub. Para especificar en GRUB que el formato de la contraseña md5 será usado, use la siguiente instrucción:

```
timeout 3
password --md5 $1$bw0ez$tljnxxKLfMzmnDVaQWgjP0
```

El parámetro –md5 fue agregado para instruir a grub a realizar el proceso de autenticación. La contraseña proporcionada es la versión encriptada en md5 de “hackme”. Usar el método de encripción md5 es preferible a su contraparte en solo texto. Mas información acera de la contraseña GRUB puede ser encontrada en el paquete de grub-doc.

4.2. Eliminar el prompt de root del núcleo

Los núcleos de Linux 2.4 proporcionan una forma para tener acceso a la línea de comandos del administrador que será presentada justo después de cargar el sistema de archivos cramfs. Un mensaje aparecerá para permitir al administrador entrar en una línea de comandos con permisos de root, esta línea de comandos puede ser usada manualmente para cargar módulos cuando la autodetección falla. Este comportamiento es el predeterminado para initrd’s linuxrc. El siguiente mensaje aparecerá:

```
Press ENTER to obtain a shell (waits 5 seconds)
```

Para eliminar este comportamiento usted necesita cambiar `/etc/mkinitrd/mkinitrd.conf` y colocar:

```
# DELAY The number of seconds the linuxrc script should wait to
# allow the user to interrupt it before the system is brought up
DELAY=0
```

Luego regenera su imagen del disco RAM. Usted puede hacer esto por ejemplo con:

```
o
# cd /boot
# mkinitrd -o initrd.img-2.4.18-k7 /lib/modules/2.4.18-k7
```

O hacer (preferir):

```
# dpkg-reconfigure kernel-image-2.4.x-yz
```

Note que DEBIAN 3.0 WOODY permite a los usuarios instalar 2.4 kernels (seleccionando*flavors*), *sin embargo* el defecto de kernel es de 2.2 (salvo para algunos artífices, para los cuales Kernel 2.2 no estaba en la entrada). Si usted considera esto un BUG considere el Bug 145244 (`http://bugs.debian.org/145244`) antes de enviar este.

4.3. Deshabilitar el arranque desde diskette

El MBR defectuoso en Debian antes de la versión 2.2 no actúa como un registro dominante en la entrada y deja abierto un método para quebrar fácilmente el sistema:

- Presione shift al momento de entrar, y de inmediato un MBR aparece.
- Luego presione F, y su sistema entrará desde un disquete. Esto puede ser usado para tener un acceso de ROOT al sistema.

Este comportamiento puede ser cambiado totalmente por:

```
lilo -b /dev/hda
```

Ahora LILO es puesto dentro del MBR. Este también puede ser archivado agregando "boot=/dev/hda" para lilo.conf. Hay otra solución la cual inhabilita rápidamente el MBR, completamente:

```
install-mbr -i n /dev/hda
```

De otra forma, esta "puerta trasera" desde la cual mucha gente no está enterada, puede salvar su pellejo si usted esta en aprietos con su instalación por cualquier razón.

ARREGLAMEcheck whether this really is true as of 2.2 or was it 2.1? INFO: Thebootdisks as of Debian 2.2 do NOT install the mbr, but only LILO

4.4. Restricción del acceso a la consola

Algunas políticas de seguridad quieren forzar a los administradores para registrarse en el sistema a través de la consola con su usuario/contraseña y luego llegar a ser un superusuario (con`su` o `sudo`). Esta política es implementada en Debian al editar el archivo `/etc/login.defs` o `/etc/securetty` cuando se usa PAM. En:

- `login.defs`, edite el la variable CONSOLE , que define un archivo o lista de terminales sobre las cuales la entrada de root es permitida.
- `securetty` agregando/removiendo las terminales desde las cuales el acceso a root es permitido.

Cuando use PAM se hacen otros cambios para el proceso de registro, los cuales pueden incluir restricciones para usuarios y grupos a tiempos dados, puede ser configurado en `/etc/pam.d/login`. Una interesante característica que puede ser incapacitada es la posibilidad de registrar con contraseñas sin efecto (nulas). Esta característica puede ser limitada removiendo el *nullok* de la linea:

```
auth required pam_unix.so nullok
```

4.5. Montando particiones de manera correcta

cuando se monta una partición ext2, usted tiene varias opciones adicionales para aplicar a el llamado montaje o a `/etc/fstab`. Por ejemplo, este fstab entra por la partición `/tmp`: /dev/hda 7 /tmp ext2 defaults .nosuid.noexec.nodev 0 2

```
/dev/hda7 /tmp ext2 defaults,nosuid,noexec,nodev 0 2
```

usted ve la diferencia a las secciones de opciones . La opción `nosuid` ignora los bits setuid y setgid completamente , mientras que `noexec` prohibe la ejecución de programas en ese punto de montaje, y `nodev`, ignora los dispositivos.Esto suena grandioso , pero esto

- únicamente se aplica a archivos del sistema ext2
- puede ser evitado fácilmente

La opción `noexec` previene los binarios de ejecutarse directamente, pero se engaña fácilmente:

```
alex@joker:/tmp# mount | grep tmp
/dev/hda7 on /tmp type ext2 (rw,noexec,nosuid,nodev)
alex@joker:/tmp# ./date
bash: ./date: Permission denied
alex@joker:/tmp# /lib/ld-linux.so.2 ./date
Sun Dec 3 17:49:23 CET 2000
```

Sin embargo, muchos “script kiddies” cuentan con “xploits” que intentan crear y ejecutar los archivos en `/tmp`.Si ellos no tienen una pista, ellos entrarán en esta trampa. En otros términos, un usuario no puede engañarse en ejecutar un binario troyanizado en `/tmp` e.g. por ejemplo cuando él agrega a propósito `/tmp`dentro de su PATH.

También se previene de algún programa que podría depender en que `/tmp` sea ejecutable. Más notablemente, Debconf tiene (¿tenía?) algunos problemas que consideran esto, para más información vea Bug 116448 (`http://bugs.debian.org/116448`).

Lo siguiente es un ejemplo más completo. Una nota, sin embargo: `/var` podrían ponerse en noexec, pero algún software como Smartlist contiene sus programas en / var. El mismo aplicado a la opción nosuid.

```
/dev/sda6 /usr ext2 defaults,ro,nodev 0 2
/dev/sda12 /usr/share ext2 defaults,ro,nodev,nosuid 0
2/dev/sda7 /var ext2 defaults,nodev,usrquota,grpquota
 0 2/dev/sda8 /tmp ext2
defaults,nodev,nosuid,noexec,usrquota,grpquota 0 2/dev/sda9
/var/tmp ext2 defaults,nodev,nosuid,noexec,usrquota,grpquota 0
 2/dev/sda10 /var/log ext2 defaults,nodev,nosuid,noexec 0
```

```
 2/dev/sda11 /var/account ext2 defaults,nodev,nosuid,noexec 0
 2/dev/sda13 /home ext2
rw,nosuid,nodev,exec,auto,nouser,async,usrquota,grpquota 0
2/dev/fd0 /mnt/fd0 ext2 defaults,users,nodev,nosuid,noexec
0 0/dev/fd0 /mnt/floppy vfat
defaults,users,nodev.nosuid,noexec 0 0/dev/hda /mnt/cdrom
iso9660 ro,users,nodev.nosuid,noexec 0 0
```

4.5.1. Serie /tmp noexec

Tenga cuidado si esta poniendo `/tmp`y usted quiere instalar el nuevo software, desde que alguno podría usarlo para la instalación. Apt es uno de esos programas (vea http://bugs.debian.org/116448) si no configuró propiamente `APT::ExtractTemplates::TempDir` (vea `apt-extracttemplates(1)`). Usted puede poner esta variable en `/etc/apt /apt.conf` a otro directorio con privilegios exec que no sea `/tmp`

Con respecto al noexec, por favor sea consciente que no podría ofrecerle tanta seguridad.Considere esto:

```
$ cp /bin/date /tmp
$ /tmp/date
(does not execute due to noexec)
$/lib/ld-linux.so.2 /tmp/date
(works since date is not executed directly)
```

4.5.2. Serie /usr leer-únicamente

Si usted pusiera `/usr` leer - únicamente usted no podrá instalar los nuevos paquetes en su Debian GNU / sistema Linux. Usted tendrá, primero que remontar leer -escribir, instale los paquetes y entonces remóntelo leer-únicamente. La última versión apt (en Debian 3.0´woody´) puede configurarse para ejecutar las órdenes antes y después de instalar los paquetes, para que usted pueda propiamente querer configurarlo.

Hacer esto modifica `/etc/apt/apt.conf` y agrega:

```
DPkg
{
Pre-Invoke { "mount /usr -o remount,rw" };
Post-Invoke { "mount /usr -o remount,ro" };
};
```

Note que el Post-invoke puede fallar con un "/usr busy" error en el mensaje. Esto pasa principalmente cuando usted está usando los archivos durante la actualización en que se puso al día. Incomodando pero no realmente una cantidad grande. Sólo hacerlo seguro que ésto ya no se use y ejecute Post - Invoke manualmente.

4.6. Ejecute una actualización de seguridad

En cuanto generalmente se revelen los nuevos bugs de seguridad en los paquetes, mantenedoras de debian y autores upstream generalmente dentro de días o incluso en horas. Después de que el bug es fijo, un nuevo paquete se proporciona en http://security.debian.org.Ponga la línea siguiente en sus fuentes. la lista y usted conseguirá la seguridad que se pone al día automáticamente, siempre que usted ponga al día su sistema.

```
deb http://security.debian.org/debian-security stable/updates main contrib
non-free
```

La mayoría de las personas que no viven en un país que prohibe la importación o usa la criptografía fuerte, debe agregar esta línea también:

```
deb http://security.debian.org/debian-non-US stable/non-US main contrib non-f
```

Si le gusta, usted puede agregar las líneas del deb-src también a apt. Vea `apt(8)` para detalles extensos.

Usted debe dirigir la seguridad frecuentemente que se pone al día, la inmensa mayoría de resultado de explotaciones de vulnerabilidades conocidas que no se han remendado a tiempo, cuando un nombre de http://www.cs.umd.edu/~waa/vulnerability.html name="papel por Bill Arbaugh">(presentó en el 2001 Simposio de IEEE en Seguridad y Retiro) explica.

ARREGLAME:Añade info cómo la firma de paquetes que se hace para que esto pueda hacerse automáticamente a través de un trabajo del cron (engaña grandemente :DNS).

4.7. Acceso de acuerdo a las necesidades del usuario

4.7.1. Uso de la autenticacion: PAM

PAM (modulos de autenticación de enchufes) permiten a los administradores de sistema elegir como usar la aplicaciones autenticadas . Note que PAM puede hacer nada a menos que una aplicación es compilada con soporte para PAM . La mayor parte de las aplicaciones que son enviadas con Debian 2.2 tienen este soporte construido . Ademas , Debian no tiene soporte PAM antes del 2.2. Cada aplicación con soporte PAM provee un archivo de configuración en `/etc/pam.d/` el cual puede ser usado para modificar este comportamiento. La siguiente descripción está lejos para completarla, para mas información usted podria querer leer la guia de el sistema administrador Linux -PAM http://www.kernel.org/pub/linux/libs/pam/Linux-PAM-html/pam.html (en la principal distribución ubicada de PAM http://www.kernel.org/pub/linux/libs/pam/)

PAM le ofrece a usted la posibilidad a ir por varios pasos de autenticación una vez, sin el uso de conocimientos .Usted puede autenticar de nuevo una base de datos Berkeley y de nuevo el

archivo de password normal y el uso únicamente de registros en si correctamente autenticos en ambos. Usted puede limitar a muchos con PAM , así como usted puede abrir sus puertas del sistema muy extensamente. Así que tenga cuidado. Una línea de la típica configuración tiene un campo de mando como su segundo elemento. Generalmente debe ponerse a " requisito", el cual devuelve un fracaso del login si hay una falta en el módulo.

La primera cosa que me gusta hacer, es agregar soporte MD5 a las aplicaciones de PAM, desde que esto ayuda, protege contra los cracks (passwords del diccionario que puede ser más largo usando MD5). Lo siguiente debe agregarse dos líneas a todos los archivos en `/etc/pam.d/` ese acceso de concesión a la máquina, como `login` and `ssh`.

```
# Be sure to install libpam-cracklib first or you will not be able to log in
password required pam_cracklib.so retry=3 minlen=12 difok=3
password required pam_unix.so use_authtok nullok md5
```

¿Así, qué hace esta maravilla? Las primeras cargas de la línea en el cracklib módulo de PAM que proporciona la contraseña strenght-checking (fuerza-verificando) las sugerencias para una nueva contraseña con una longitud mínima de 12 carácteres, una diferencia de por lo menos 3 carácteres de la contraseña vieja, y permite 3 reintentos. La segunda línea introduce el módulo de la autenticación normal con las contraseñas de MD5 y permite una cera de contraseña de longitud. El director use_authtok es necesario para entregar la contraseña del módulo anterior.

Para asegurarse que el root (administrador de Linux) del usuario sólo puede anotarse en el sistema de los términos locales, la línea siguiente debe habilitarse en `/etc/pam.d/login`:

```
auth requisite pam_securetty.so
```

Entonces usted debe agregar los términos que el root del usuario puede anotar en el sistema en `/etc/security/access.conf`. Último pero no menor a la línea siguiente debe ser los anabled si usted quiere preparar los límites del usuario.

```
session required pam_limits.so
```

Esto restringe los recursos del sistema que se permiten a los usuarios (vea en la siguiente pagina 'Los límites de el archivo.conf' en la página 35. Por ejemplo, usted podría restringir el número de logins coexistente (de un grupo dado de usuarios, o sistema-ancho) usted puede tener, el número de procesos, el tamaño de memoria.....

Ahora revise `/etc/pam.d/passwd` y cambie la primera línea. Usted debe agregar el "md5" de la opción para usar las contraseñas de MD5, cambie el lenght mínimo de contraseñas de 4 a 6 (o más) y ponga un legth máximo, si usted desea. La línea resultante mirará algo como:

```
password required pam_unix.so nullok obscure min=6 max=11 md5
```

Si usted quiere proteger su (un comando), para que sólo algunas personas puedan usarlo para volverse a root en su sistema, usted necesita agregar uno nuevo para agregar un nuevo "wheel" de grupo a su sistema (ésa es la manera más limpia, desde que ningún archivo tiene tal un permiso de grupo todavía). Agregue el root y los otros usuarios que deberian ser capaces de ejecutar `su` a el usuario de root a este grupo. Entonces agregue la línea siguiente a `/etc/pam.d/su`:

```
auth requisite pam_wheel.so group=wheel debug
```

Esto asegura que sólo personas de el grupo wheel pueden usar `su` para volverse root. Otros usuarios no seran capaces de volverse root. De hecho ellos conseguirán un mensaje negado si ellos intentan volverse volverse root.

Si usted quiere que sólo ciertos usuarios autentiquen a un servicio de PAM, esto es bastante fácil de lograr usando los archivos dónde los usuarios que son permitidos al login (o no) se guarden. Sólo imagine que usted quiere permitirle el login de ´ref´to al usuario vía ssh. Así que usted lo pone en `/etc/sshusers-allowed` y le escribe lo siguiente en `/etc/pam.d/ssh`:

```
auth required pam_listfile.so item=user sense=allow
file=/etc/sshusers-allowed onerr=fail
```

Por último, pero no menos importante, cree `/etc/pam.d/other` y coloque las líneas siguientes:

```
auth required pam_securetty.so
auth required pam_unix_auth.so
auth required pam_warn.so
auth required pam_deny.so
account required pam_unix_acct.so
account required pam_warn.so
account required pam_deny.so
password required pam_unix_passwd.so
password required pam_warn.so
password required pam_deny.so
session required pam_unix_session.so
session required pam_warn.so
session required pam_deny.so
```

Estas líneas mantendrán una buena configuración predefinida en todas las aplicaciones que apoyan PAM (se niega el acceso por el valor predeterminado).

4.7.2. Los límites de el archivo.conf

Usted realmente debe hacer una mirada seria en este archivo. Aquí usted puede definir los límites de recurso del usuario. Si usted usa PAM, el archivo `/etc/limits.conf` se ignora y usted debe usar en cambio `/etc/security/limits.conf`.

ARREGLAME: Adquirir unos buenos limites.conf concluidos aquí.

4.7.3. Editar /etc/login.defs

El próximo paso es revisar la configuración básica y acción en el login del usuario.

```
FAIL_DELAY 10
```

Esta variable debe ponerse a un valor más alto, para hacerlo más difícil usar el término para anotar usando la fuerza bruta. Si una contraseña mala se teclea en, el posible asaltador (o el usuario normal!) tiene que esperar por 10 segundos para conseguir un nuevo login que incite realmente el tiempo que se consume cuando usted prueba las contraseñas.Preste atención al hecho que esta escena es inútil si se usa el programa de otra manera que el getty, como el mingetty por ejemplo.

```
FAILLOG_ENAB yes
```

Si usted habilita esta variable, se anotarán los logins fallados. Es importante guardar huella de ellos para coger a alguien que pruebe un ataque de fuerza bruta.

```
LOG_UNKFAIL_ENAB yes
```

Si usted pusiera la variable “FAILLOG_ENAB” asi, entonces usted también deberia poner esta variable a sí. Esto grabará el usernames desconocido si los login fallaron. Si usted hace esto, asegúrese de que los logs tienen por ejemplo permisiones (640 por ejemplo, con una escena de grupo apropiada como el adm), porque los usuarios entran en su contraseña a menudo accidentalmente como el username y usted no quiere otro para verlo.

```
SYSLOG_SU_ENAB yes
```

Este uno habilita el logging de la pueba `su` a syslog. Bastante importante en serias maquinas pero note que esto puede crear el retiro de los resultados a medida que esten bien.

```
SYSLOG_SG_ENAB yes
```

Igual que SYSLOG_SU_ENAB pero lo aplica al programa `sg`.

```
MD5_CRYPT_ENAB yes
```

Como lo expuesto anteriormente, MD5 suma grandemente las contraseñas que reducen el problema de ataques del diccionario, desde que usted puede usar las contraseñas más largas. Si usted está usando slink, lea los documentos sobre MD5 antes de habilitar esta opción.Por otra parte esto esta fijo en PAM.

```
PASS_MAX_LEN 50
```

Si se activan las contraseñas de MD5 en su configuración PAM, Entonces esta variable debería ser ajustada al mismo valor que se uso allí.

4.7.4. Usar su

Si usted realmente necesita que los usuarios se vuelvan el super usuario en su sistema,e.g. por instalar los paquetes o agregar usuarios, usted puede usar el comando `su` para cambiar su identidad. Usted debe intentar evitar cualquier login como root del usuario y en cambio usar `su`. Realmente, la mejor solución es quitar su y cambiar a `sudo`, como él tiene más rasgos que `su`. Sin embargo,`su` es más común como se usa en muchos otro Unixes.

4.7.5. Usar sudo

`sudo` le permite al usuario ejecutar los comandos definidos bajo la identidad de otro usuario, así como root. Si el usuario agrega a `/etc/sudoers` y se autentica correctamente, él es capaz de avanzar comandos en que se ha definido `/etc/sudoers`. Las Violaciones, como las contraseñas incorrectas o intentos de ejecutar un programa usted no tienen permiso para ser anotado y mandado por correo a root.

4.7.6. Restringiendo usuarios

A veces usted podría pensar que necesita tener los usuarios creados en su sistema local para proporcionar un servicio (pop3 manda por correo el servicio o ftp). Antes de hacer eso, primero recuerde que la aplicación de PAM en Debian GNU/Linux le permite validar a los usuarios con una variedad ancha de el servicio de directorio externo (el radio, el ldap, etc.) con tal de que por el ,el libpam sea empacado.

Si los usuarios necesitan ser creados y el sistema puede ser remotamente de acceso tome en cuenta que los usuarios sean capaces al login al sistema. Usted puede arreglar esto dando a los usuarios una nula (`/dev/null`) interfaz de comandos (él necesitaría ser listada en `/etc/shells`). Si usted quiere permítales a los usuarios acceder a el sistema pero limitar sus movimientos, usted puede usar el `/bin/rbash`, equivalente a agregar la opción `-r` en bash (*RESTICTED SHELL* ver `bash(1)`). Por favor note que incluso con la interfaz de comandos

restringido, un usuario que entra en acceso a un programa interactivo (eso podría permitirle la ejecución de un subshell) podría poder desviar los límites de el shell.

Debian no es proporcionado actualmente (pero puede serlo en el futuro) el módulo del `pam_chroot`. Una alternativa a este chroot es el servicio que proporciona el logging remoto (ssh, telnet).

Si usted desea restringirlo *when* los usuarios pueden acceder a el sistema que usted quiere tener personalizado `/etc/security/access.conf` para sus necesidades.

Restringiendo ssh para los usuarios

Los sshd de Debian no le permitirán restringir el movimiento del usuario a través del servidor desde que le falte la función de Chroot que el anuncio (sshd2) el programa tiene (uso de 'ChrootGroups' o 'ChrootUsers', vea `sshd2_config(5)`). Sin embargo,hay un parche disponible eso le permitirá hacer esto, el parche, puede recuperarse del informe Bug report 139047 (`http://bugs.debian.org/139047`) o `http://www.cag.lcs.mit.edu/~raoul/` (y podría aplicarse en el paquete de OpenSSH en el futuro). Emmanuel Lacour tiene los paquetes del ssh con este rasgo a `http://debian.home-dn.net/woody/ssh/`, yendo a través de el paso de la recopilación se recomienda, sin embargo. Una descripción de todos los pasos necesitados puede encontrarse en `http://mail.incredimail.com/howto/openssh/` (casi todos son aplicables a Debian aun cuando habla sobre RedHat 7.2). Después de aplicar el parche simplemente usted modifica lo que necesita el `/etc/passwd` cambiando el camino de la casa de los usuarios (con la especial ficha `/./`):

```
joeuser:x:1099:1099:Joe Random User:/home/joe/./:/bin/bash
```

Esto restringirá *both* accesos de el interfaz de comandos remoto así como la copia remota a través del canal ssh.

Asegúrese para tener todos los binarios necesitados y bibliotecas en el el camino del chrooted para los usuarios. Estos archivos deben poseer por root evitar ser manoseados por el usuario (para terminar el chrooted encarcelado). Una muestra podría incluir:

```
./bin:
total 660
drwxr-xr-x 2 root root 4096 Mar 18 13:36 .
drwxr-xr-x 8 guest guest 4096 Mar 15 16:53 ..
-r-xr-xr-x 1 root root 531160 Feb 6 22:36 bash
-r-xr-xr-x 1 root root 43916 Nov 29 13:19 ls
-r-xr-xr-x 1 root root 16684 Nov 29 13:19 mkdir
-rwxr-xr-x 1 root root 23960 Mar 18 13:36 more
-r-xr-xr-x 1 root root 9916 Jul 26 2001 pwd
-r-xr-xr-x 1 root root 24780 Nov 29 13:19 rm
lrwxrwxrwx 1 root root 4 Mar 30 16:29 sh -> bash
```

```
./etc:
total 24
drwxr-xr-x 2 root root 4096 Mar 15 16:13 .
drwxr-xr-x 8 guest guest 4096 Mar 15 16:53 ..
-rw-r--r-- 1 root root 54 Mar 15 13:23 group
-rw-r--r-- 1 root root 428 Mar 15 15:56 hosts
-rw-r--r-- 1 root root 44 Mar 15 15:53 passwd
-rw-r--r-- 1 root root 52 Mar 15 13:23 shells

./lib:
total 1848
drwxr-xr-x 2 root root 4096 Mar 18 13:37 .
drwxr-xr-x 8 guest guest 4096 Mar 15 16:53 ..
-rwxr-xr-x 1 root root 92511 Mar 15 12:49 ld-linux.so.2
-rwxr-xr-x 1 root root 1170812 Mar 15 12:49 libc.so.6
-rw-r--r-- 1 root root 20900 Mar 15 13:01 libcrypt.so.1
-rw-r--r-- 1 root root 9436 Mar 15 12:49 libdl.so.2
-rw-r--r-- 1 root root 248132 Mar 15 12:48 libncurses.so.5
-rw-r--r-- 1 root root 71332 Mar 15 13:00 libnsl.so.1
-rw-r--r-- 1 root root 34144 Mar 15 16:10
libnss_files.so.2
-rw-r--r-- 1 root root 29420 Mar 15 12:57 libpam.so.0
-rw-r--r-- 1 root root 105498 Mar 15 12:51 libpthread.so.0
-rw-r--r-- 1 root root 25596 Mar 15 12:51 librt.so.1
-rw-r--r-- 1 root root 7760 Mar 15 12:59 libutil.so.1
-rw-r--r-- 1 root root 24328 Mar 15 12:57 libwrap.so.0

./usr:
total 16
drwxr-xr-x 4 root root 4096 Mar 15 13:00 .
drwxr-xr-x 8 guest guest 4096 Mar 15 16:53 ..
drwxr-xr-x 2 root root 4096 Mar 15 15:55 bin
drwxr-xr-x 2 root root 4096 Mar 15 15:37 lib

./usr/bin:
total 340
drwxr-xr-x 2 root root 4096 Mar 15 15:55 .
drwxr-xr-x 4 root root 4096 Mar 15 13:00 ..
-rwxr-xr-x 1 root root 10332 Mar 15 15:55 env
-rwxr-xr-x 1 root root 13052 Mar 15 13:13 id
-r-xr-xr-x 1 root root 25432 Mar 15 12:40 scp
-rwxr-xr-x 1 root root 43768 Mar 15 15:15 sftp
-r-sr-xr-x 1 root root 218456 Mar 15 12:40 ssh
-rwxr-xr-x 1 root root 9692 Mar 15 13:17 tty

./usr/lib:
```

```
total 852
drwxr-xr-x 2 root root 4096 Mar 15 15:37 .
drwxr-xr-x 4 root root 4096 Mar 15 13:00 ..
-rw-r--r-- 1 root root 771088 Mar 15 13:01
libcrypto.so.0.9.6
-rw-r--r-- 1 root root 54548 Mar 15 13:00 libz.so.1
-rwxr-xr-x 1 root root 23096 Mar 15 15:37 sftp-server
```

4.7.7. Manual de auditoría del usuario

Si usted es paranoico usted podría querer agregar a los usuarios una definición `.profile` que pone el ambiente en cierto modo tal que ellos no pueden retirar las capacidades de la auditoría de la interfaz de comandos (los comandos son descargas a `$HISTFILE`. El `.profile` podría ponerse como sigue:

```
HISTFILE=/home/_user_/.bash_history
HISTSIZE=100000000000000000
HISTFILESIZE=100000000000000000
set -o HISTFILE
set -o HISTSIZE
set -o HISTFILESIZE
export HISTFILE HISTSIZE HISTFILESIZE
```

Note: el - o atribuye colocar una variable leer-únicamente en bash.

Para trabajar esto el usuario no pueden modificar el `.profile` o `.bash_history` pero debe poder primero leer uno y escribe uno en el segundo. Usted puede hacer esto fácilmente cambiando éstos archivos y el directorio dónde ellos residen para ser poseídos por otro usuario (root), y da escritura a los permisos del grupo de usuarios a la historia del archivo. Otra opción está terminando el uso del programa `chattr`.

Si usted es completamente paranoico y quiere intervenir en el comando de cada usuario,usted podría tomar bash a el código de la fuente, revise este y haga envío a todos de que el usuario tecleó en otro archivo. O tiene `ttysnoop` constantemente algun nuevo monitor ttys y dump en el rendimiento en un archivo. Otro programa útil es Snoopy (`http://sourceforge.net/project/?group_id=2091`) el cual es un programa usuario-transparente que engancha como en una bibliotecaproporcionando una envoltura alrededor del execve llamadas (), cualquier comando ejecuta el estar anotado a syslogd usando la facilidad del `authpriv` facility (usualmente storead a `/var/log/auth.log`.

Note que usted no puede usar el comando `script` por esto desde que este no funcionará como una interfaz de comandos (aun si usted agrega esto a `/etc/shells`.

4.7.8. Completa auditoría del usuario

El ejemplo anterior es una manera simple de configurar el usuario interviniendo el cual no podría ser útil para los sistemas complejos. Si éste es su caso, usted necesita mirar a `acct`, la

contabilidad de utilidades. Éstos anotarán todos los comandos corridos por usuarios o procesos en el sistema, al gasto de espacio del disco.

Al activar la contabilidad, toda la información sobre los procesos y el usuario se guarda bajo `/var/account/`, más específicamente en el `pacct`. El paquete de contabilidad incluye algunas herramientas (`sa` y `ac`) para analizar estos datos.

4.7.9. Repasando los perfiles del usuario

Si usted quiere normalmente *see* a los usuarios qué están haciendo, cuando esten ellos conectándos usted pueden usar la base de datos de `wtmp` que incluye toda la información del login. Este archivo puede procesarse con varias utilidades, entre ellos `sac` el cual puede hacer un profile en cada usuario que muestra en que estructura de tiempo ellos normalmente anotan adelante en el sistema.

En caso de que usted tiene la contabilidad activada, usted también puede usar las herramientas con tal de que por esto en el comando determine cuando los usuarios acceden a el sistema y qué ellos ejecuten.

4.8. Proporcionando acceso seguro a los usuarios

4.8.1. Limitando lo que los usuarios pueden ver/hacer

Limitando el acceso a la información de otros usuarios

4.9. Usando tcpwrappers

Las envolturas de TCP se desarrollaron cuando no había ningún filtro del paquete real disponible y el control de acceso fue necesitado. Las envolturas de TCP permiten permitir o negar un servicio para un organizador o un dominio y defina un valor permitido o niegue la regla. Si usted quiere que más informaciones de una mirada a `hosts_access(5)`.

Muchos servicios instalados en Debian son cualquiera de estos dos:

- lanzó a través del servicio del tcpwrapper (`tcpd`)
- compiló con el soporte libwrapper incorporado.

En la primera mano, de servicios son configurados en `/etc/inetd.conf`, esto incluye telnet,ftp,netbios,swat and finger (usted verá que el archivo de la configuración se ejecute primero `/usr/sbin/tcpd`. Por otro lado, aun cuando un servicio no se lanza por el superdemonio del `inetd` ,en cualquier caso,sujetó las reglas de envolturas de tcp compilando su soporte en él. Los servicios compilados con las envolturas del tcp en Debian incluyen ssh,portmap, in.talk, rpc.statd, rpc.mountd,gdm,oaf (el demonio activador de GNOME), Nessus y muchos otros.

Tenga en cuenta esto cuando el `tcpchk` está avanzando. Usted puede agregar servicios en que se unen a la biblioteca de la envoltura de los archivos `host.deny` y `hosts.allow` pero los `tcpchk` advertirá que este no puede encontrar esos servicios desde que parece para ellos en `/etc/inetd.conf` (el manpage no es totalmente exacto aquí).

Ahora, aquí viene un truco pequeño, y probablemente la intrusión más pequeña del sistema de descubrimiento disponible. En general, usted debe tener una política decente del cortafuego como una primera línea, y envolturas del tcp como la segunda línea de defensa. Un truco pequeño es poner un comando SPAWN [1]en /etc/hosts.deny que envía correos a root siempre que hay un servicio negado en las envolturas de los gatillos:

```
ALL: ALL: SPAWN ( \
 echo -e "\n\
 TCP Wrappers\: Connection refused\n\
 By\: $(uname -n)\n\
 Process\:%d (pid%p)\n\
 User\:%u\n\
 Host\:%c\n\
 Date\: $(date)\n\
" | /usr/bin/mail -s "Connection to%d blocked" root) &
```

Beware(tenga cuidado): El ejemplo anterior impreso puede fácilmente ser DoSed por estar haciendo las muchas conexiones en un período corto de tiempo. Muchos correos electrónicos significan mucho del archivo I/O para enviar únicamente unos correos.

4.10. La importancia de logs y alarmas

Cómo las bitácoras y alarmas son tratadas es un problema importante en un sistema seguro. Es fácil ver que, aun cuando el sistema está perfectamente configurado y, supuestamente, 99 % asegurado. Si el 1 % sucede, y no hay seguridad midiendo en tales situaciones, primero, descubra esto y, segundo, las alarmas del aumento, el sistema no está en absoluto seguro.

Debian GNU/Linux proporciona algunas herramientas para hacer el análisis de bitácoras, la mayoría, notablemente el `logcheck`. Sin embargo, allí se está considerando mucho análisis del log que no puede cubrirse totalmente aquí, un recurso bueno para la información es Couterpane's Log Analysis Resources (`http://www.counterpane.com/log-analysis.html`).

4.10.1. Configurando el sitio donde las alertas son enviadas

Debian viene con una configuración de syslog estándard dentro de (etc/syslog.conf)que anota mensajes para apropiar archivos dependiendo de la facilidad del sistema. Usted debería familiarizarse con ésto, debe mirar el archivo `syslog.conf` o sino la documentación. Si usted

[1]beware of the case here since *spawn* will not work

pretende mantener un sistema seguro usted podrá estar precavido de a dónde se mandan los mensajes de registro de manera que no pasen inadvertidos.

Por ejemplo, enviar mensajes a la consola es una configuración interesante ya que es útil para muchos sistemas de nivel de producción. Pero para muchos sistemas también es importante añadir una nueva máquina que podría servir como servidor de registro (i.e. esto recibe los registros desde todos los otros sistemas).

El correo de Root también deberia ser considerado, muchos controles de seguridad como `snort`) envían alarmas al buzón de Root. Este buzón normalmente apunta al primer usuario que se creó en el sistema (compruebe `/etc/aliases`). Tenga cuidado de enviar correo de root a cualquier lugar donde pueda ser leído (ya sea local ó remotamente)

Hay otros informes y alianzas en su sistema. En un pequeño sistema, ésto probablemente lo más simple para asegurarse de que todas las alianzas apunten hacia la cuenta de root, y que el correo para root este dispuesto para el sistema de buzón personal del administrador.

ARREGLAME: it would be interesting to tell how a Debian system can send/receive SNMP traps related to security problems (jfs). Check: `snmptraglogd`, `snmp` and `snmpd`.

4.10.2. Usar un servidor de registro

Un servidor de regiastro es un servidor que recoge remotamente datos syslog de la red. Si una de sus máquinas es craqueada, el intruso no puede cubrir sus huellas, a menos de que también altere el servidor de registro. Así el servidor de registro deberá ser especialmente seguro. Convertir una máquina en servidor de registro es simple. Simplemente lance syslogd con 'syslogd -r' y nace un nuevo servidor de registro. Seguidamente, congifure las otras máquinas para que envíen datos al servidor de registro, Para hacer ésto permanentemente en Debian edite `/etc /init.d/sysklogd` y cambie la línea:

```
SYSLOGD=""
```

to

```
SYSLOGD="-r"
```

Luego, configure las otras máquinas al enviar los datos al servidor de registro. Agrege una entrada como la siguiente `/etc/syslog.conf`:

```
facility.level @your_loghost
```

Mire la documentación para saber que usar en lugar de *facility* y *level* (ellos no deben ser introducirse de forma literal como se hace aquí). Si usted quiere registrar todo remotamente, escriba:

```
*.* @your_loghost
```

dentro de su syslog.conf. Registrar tanto remota como localmente es la mejor solución (el atacante creerá haber cubierto sus pasos después de eliminar los archivos locales de registro). Para información adicional consulte el manual de paginas `syslog(3)`, `syslogd(8)` y `syslog.conf(5)`.

4.10.3. Permisos para el archivo de registro

No sólo es importante decidir como son usadas las alertas, sino también quienes tiene acceso a éstas, i.e. puede leer o modificar los archivos de registro (si no se está usando un servidor remoto de registros). Las alertas de seguridad que el atacante pueda cambiar o inhabilitar no son de mucho valor en el momento de la invasión.

Algunos permisos para el achivo de registro no son perfectos despúes de la instalación. Primero `/var/log/lastlog` y `/var/log/faillog`no necesitan tener un permiso de lectura para un usuario normal. En el archivo lastlog usted puede ver quien entró recientemente y en faillog usted mira un resumen de las entradas fallidas. El autor recomienda cambiar permisos a 660.Haga una breve revisión en sus archivos de registro y decida muy cuidadosamente cuales logfile deben tener permiso de lectura y escritura para un usuario con UID distinto a 0 y un grupo aparte de 'adm' o 'root'.

Quiero enfatizar que los permisos del archivo de registro apache son realmente malos debido al hecho de que el usuario apache tiene los registros del archivo apache. Si un ususario obtiene un interfaz de comandos con una puerta trasera de apache, ellos pueden eliminar fácilmente los archivos de registro.

4.11. Uso del cambio de directorio raíz

`chroot` es una de las posibilidades más poderosas para restringir un demonio, un ususario u otro servicio. Sólo imagine una cárcel alrededor de su objetivo, del cual no puede escapar (normalmente, hay sin embargo muchas condiciones que permiten un escape fuera de su cárcel). Si usted no confía en un usuario, puede crear un cambio en el ambiente. Ésto puede usar un pequeño espacio adicional de disco, puesto que se necesita copiar todos los ejecutables necesarios, así como las biblioteca dentro de la cárcel. Aún si el usuario hace algo malicioso, el alcance de un daño es limitado al aseguramiento.

Un buen ejemplo de este caso,es,si usted no autentica en contra de `/etc/passwd`puede usar LDAP o MySQL. Así que su demonio ftp únicamente necesita un binario y quizá un poco de biblioteca. Un cambio de directorio raíz seria un excelente seguro del mejoramiento de condiciones externas; si una nueva vulneración es conocida para este demonio ftp, entonces solamente el atacante puede vulnerar el UID del usuario de demonio ftp y nada más.

Por supuesto, muchos otros demonio también podrán beneficiarse desde este modo de arranque.

Sin embargo, esté prevenido que el seguro `chroot` puede estar dañado si el usuario entra en éste es el superusuario. Así que usted necesita que el servicio corra como un usuario no privilegiado. Límitando su ambien usted está límitando la palabra leíbles que el servicio de archivos ejecutables puede acceder, así, usted límita las posibilidades de una subida del privilegio por el uso de vulnerabilidades de seguridad de los sistemas locales. Incluso en ésta situación usted no puede estar copmpletamente seguro de que no hay ninguna manera para que un atacante hábil se escape de algún modo del aseguramiento. Usando solamente un servidor de programa, el cual tiene una reputación de medida de aseguramiento que es buena. Incluso la cavidad minusiosa de archivos manuales puede ser abierta por un atacante hábil interrumpiendo el sistema por dentro. Despues de todo, `chroot` no fue diseñado como una herramienta de comprobación.

Como una nota adicional, Demonios omite BIND (Internet nombra el servicio) esto no viene con un cambio de directorio raíz, de hecho demonios no viene con un cambio de directorio raíz. Éste debe cambiar en el woody (3.0) release.

También hay algún software (no actualmente en Demonios pero el cual podría estar disponible en el futuro) que puede ayudar al arreglo del ambiente del cambio de directorio raíz. Por ejemplo, `makejail` puede crear y poner al día un aseguramiento del cambio de directorio raíz con la canfiguración de pequeños archivos. También intenta suponer e instalar dentro del aseguramiento todos los archivos requeridos por demonios. Más información en `http://www.floc.net/makejail/` `Jailer`. Es una herramienta similar la cual puede ser cobrada desde `http://www.balabit.hu/downloads/jailer/`.

4.11.1. Configuarción Kernel

4.11.2. Características de la red configurando kernel

ARREGLAME: Content missing

Muchas características de kernel pueden ser modificadas ya que actualmente se repiten algunas cosas dentro del sistema del arhivo `/proc` o usando el sistema ctl. Pra ingresar a `sysctl -A` puede mirar que debe configurar y que otras opciones hay. Solamente en algunas cosas usted necesita editar algunas cosas aquí, pero usted puede aumentar la seguridad que es un buen camino.

```
net/ipv4/icmp_echo_ignore_broadcasts = 1
```

Este es un 'emulador de windows' porque éste funciona como windows para que emita el sonido si uno de estos es establecido para 1. De otro modo, ésto no hace nada.

```
net/ipv4/icmp_echo_ignore_all = 0
```

Si usted no quiere bloquear ICMP sobre su cortafuego, permira ésto.

```
net/ipv4/tcp_syncookies = 1
```

Ésta opción es una espada de doble filo. Por otra parte su sistema está protegido contra la inundación de syn; por otra parte viola las normas definidas (RFCs). Esta opción es totalmente muda, como cuando usted inunda otro lado que está iniudado, así que el otro lado también está ocopado. Si usted quiere cambiar está opción usted también puede cambiar ésto dentro de `/etc/network/options` para colocar `syncookies=yes`.

```
/proc/sys/net/ipv4/conf/all/log_martians = 1
```

Los paquetes con direcciones imposibles (debido a las rutas incorectas) sobre el registro que obtuvo su red.

Este es un ejemplo del ajuste en otro material útil. Usted debería añadir ésta información dentro de la escritura de `/etc/network/interface-secure` (el nombre dado como un ejemplo) y es llamado desde `/etc/network/interfaces` como éste:

```
auto eth0
iface eth0 inet static
 address xxx.xxx.xxx.xxx
 netmask 255.255.255.xxx
 broadcast xxx.xxx.xxx.xxx
 gateway xxx.xxx.xxx.xxx
 pre-up /etc/network/interface-secure


# Script-name: /etc/network/interface-secure
# Modifies some default behaviour in order to secure against
# some TCP/IP spoofing & attacks
#
# Contributed by Dariusz Puchalak
#
echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
 # broadcast echo protection enabled
echo 0 > /proc/sys/net/ipv4/ip_forward # ip forwarding disabled
echo 1 > /proc/sys/net/ipv4/tcp_syncookies # TCP syn cookie protection enable
echo 1 >/proc/sys/net/ipv4/conf/all/log_martians
 # Log packets with impossible
addresses # but be careful with this on heavy loaded web
serversecho 1 > /proc/sys/net/ipv4/ip_always_defrag
 # defragging protection always
enabledecho 1 > /proc/sys/net/ipv4/icmp_ignore_bogus_error_responses
 # bad error message protection
enabled
# now ip spoofing protection
for f in /proc/sys/net/ipv4/conf/*/rp_filter; do
 echo 1 > $f
done
```

```
# and finally some more things:
# Disable ICMP Redirect Acceptance
for f in /proc/sys/net/ipv4/conf/*/accept_redirects; do
 echo 0 > $f
done

for f in /proc/sys/net/ipv4/conf/*/send_redirects; do
 echo 0 > $f
done

# Disable Source Routed Packets
for f in /proc/sys/net/ipv4/conf/*/accept_source_route; do
 echo 0 > $f
done

# Log Spoofed Packets, Source Routed Packets, Redirect Packets
for f in /proc/sys/net/ipv4/conf/*/log_martians; do
 echo 1 > $f
done
```

4.11.3. Configuarción de las características de los cortafuegos

Para tener la capacidad del cortafuego, para proteger el sistema local u otros *detrás* de este, el kernel necesita estar compidalo con las capacidades del cortefuego. El Debian normal 2.2 kernel (también 2.2) susmistra el paquete de filtro del cortafuego `ipchains`, el kernel normal de Debian 3.0 (kernel 2.4) suministra el *poderoso* paquete de filtros de cortafuegos `iptables` (filtro de la red). Las distribucines más viejas de Debian necesitan el parche apropiado del kernel (Debian 2.1 usa el kernel 2.0.34).

En todo caso, es bastante fácil usar un kernel diferente al suministrado por Debian. Usted puede encontrar paquetes de kernel pre-compilados que puede instalar fácilmente en el sistemas de Debian. Usted tambiém puede obtener las fuentes del kernel usando `kernel-source-X` y armar paquetes de kernel personalizados con `make-kpkg`.

Configurando los cortafuegos en Debian se discute más a fondo en 'Añadir capacidades al cortafuegos' en la página 64.

4.12. Añadiendo parches al kernel ARREGLAME: More content

Debian GNU/Linux suministra algunos de los parches para el kernel de Linux que aumentan su aseguramiento. Estos incluyen:

- Detección de Intrusos en Linux (dentro del paquete `lids-2.2.19`)

- Capacidades de Linux (dentro del paquete `lcap`)
- Confianza en Linux (dentro del paquete `trustees`)
- Linux Aumentando con NSA (dentro del paquete `selinux` también disponible desde the developer's website (`http://www.coker.com.au/selinux/`))
- kernel-patch-2.2.18-openwall (`http://packages.debian.org/kernel-patch-2.2.18-openwall`)
- `kernel-patch-2.2.19-harden`
- Capacidades de Linux (dentro del paquete `lcap`
- soporte IPSEC en el kernel (dentro del paquete `kernel-patch-freeswan`)
- `kernel-patch-int`

4.13. Transferencia segura de archivos

Copiar los archivos de una manera segura desde un computador a otros puede ser logrados usando 'scp' que está incluido en el paquete ssh. Esto funciona como rcp pero es completamente encriptado, así los tipos malos ni siquiera pueden averiguar QUE copia usted.

4.14. Límites y control de los sistemas de archivos

4.14.1. Uso de Quotas

Tener una buena política de quotas es importante, esto abstiene a los usuarios de llenar el disco duro.

Usted puede usar dos sistemas diferentes de quotas: quota de usuario y quota de grupo. Como usted provablemente dedujo, la quota del usuario límita la cantidad de espacio del que un usuario puede disponer, la quota del grupo hace lo equivalente para los grupos. Tenga en cuenta ésto cuando esté organizando el tamaño de quotas.

Hay algunos puntos importantes para considerar acerca de la configuración del sistema de quotas:

- Mantener las quotas suficientemente pequeñas, para que los usuarios no ocupen el espacio de su disco.
- Mantener las quotas lo suficientemente grandes, para que los usuarios no se quejen o su quota de correo les impida aceptar un correo por un periodo de tiempo largo.
- Use las quotas para todas las áreas en las que los usuarios puedan escribir, en `/home` como también en `/tmp`.

Cada partición/directorio al que los usuarios tienen acceso completo de escritura deberían permitir el uso de quotas. Encuentre esas divisiones y directorios y calcule un tamaño de quota trabajable, que combine el uso y la seguridad.

Ahora que usted quiere usar quotas. Primero que todo usted necesita revisar que habilito el uso de quotas en el kernel. Si no, usted necesitará recompilarla. Después de ésto dése cuenta que el paquete 'quota' esté instalado. Si no está usted necesitará este.

Habilitar la quota para los respectivos sistemas de archivos es tan fácil como modificar la configuración `inicial` ajustándola a `defaults,usrquota` en su archivo `/etc/fstab` . Si usted necesita un quota para grupos, sustituya `usrquota` por `grpquota`. Puede usar ambos. Luego cree unos archivos quota.user y quota.group vacios en la raíz de los sistemas de archivos en los que usted quiera usar quotas (Ej. con `touch /home/quota.user /home/quota.group` para el sistema de archivos `/home`).

Reinicie la quota haciendo `/etc/init.d/quota stop;/etc/init.d/quota start`. Ahora la quota debería estar ejecuténdose, y los tamaños de las quoatas pueden establecerse.

Modificar quotas para un usuario específico (digamos 'ref') puede hacerse con `edquota -u ref`. Los grupos de quotas se pueden modificar con `edquota -g <group>`. Después establezca el límite suave y duro para las quotas y/o quotas de i-nodos cuando sea necesario.

Para más información acerca de las quotas, lea el manual de páginas sobre las quotas, y el mini-howto (`/usr/share/doc/HOWTO/en-html/mini/Quota.html`).

Usted puede o no gustar de `lshell`, el cual viola el FHS. También debe tener un cuenta que pam_limits. puede suministrar la misma funcionalidad que `lshell` el cual es huérfano actualmente. orphaned (http://bugs.debian.org/93894)

4.14.2. chattr/lsattr

Estos dos comandos son muy útiles, pero solo funcionan con el sistema de archivos ext2. Con 'lsattr' puede listar los atributos de un campo, y con 'chattr' puede cambiarlos. Note que los atributos no son l amisma cosa que los permisos. Hay muchos atributos, pero solamente menciono los más importantes para incrementar la seguridad. Hay dos flags los cuales solamente los puede establecer el superusuario.

En primer lugar está flag 'a'. Si se establece un archivo, este archivo puede ser abierto solamente para añadir. Este atributo es útil para algunos archivos en `/var/log/`,aunque se podría considerar que fuesen quitados algunas veces debido a la rotación de scripts de registro.

La segunda flag es 'i', en corto immutable. Si se establece un archivo, no puede ser modificado ni borrado o renombrado y no se creará ningún link hacia él. Si no quiere que los usuarios miren en sus archivos la configuración puede establecer este flag y quitar el permiso de lectura. Más aun, ésto puede darle un poco más de seguridad contra los atacantes, porque el cracker puede confundirse al no ser capaz de borrar un un archivo. De todos modos, nunca debería asumir que el cracker es ciego. Despeés de toso ha entrado en su sistema.

Note que lsattr y chattr estan disponibles solamente en los sistemas de archivos ext2.

4.14.3. Integridad de su sistema de archivos

¿Está usted seguro de que el `/bin/login` en su disco duro es todavía el binario que instaló allí hace unos meses? ¿Qué pasaría si es una versión hackeada, que guarda la contraseña introducida en un archivo oculto o la envía por un correo claro pro todoel internet?

El único método para tener alguna protección es comprobar sus archivos cada día/hora/mes (yo prefiero cada día) comparando la vieja md5sum y la actual. Dos archivos no pueden tener la misma md5sum, de modo que anda sobre seguro aquí, excepto alquien que hackeó el algoroitmo para crear md5sums un la máquina. Esto es bueno, extremadamente difícil y muy improbable. Realmente usted debería considerar que auditar sus binarios es muy importante, ya que es un modo fácil para reconocer los cambios en sus binarios. Las herramientas que comúnmente se uaan para ésto son `sXid`, `AIDE` (Ambientación Avanzada de Detección de Intrusos), `TripWire` (no es libre; la nueva versió será GPL), `integrit` y `samhain`.

Instalando `debsums` ayudará a revisar la integración de los archivos del sistema para comparar el md5sums de todos los archivos en contra de md5sums usado en el paquete del archivo Debian. Tenga cuidado con algunos archivos porque pueden ser fácilmente cambiados.

Además puede reemplazar `locate` por `slocate`. slocate es una versión mejorada para la seguridad de local de GNU. Cuando usa slocate el usuario solomante ve los archivos a los que el tiene acceso y puede excluir cualquier archivo o directorio del sistema.

4.14.4. Configuración de revisión de setuid

Debian sumunistra un trabajo cron que diariamente corre en `/etc/cron.daily/standard`. Este trabajo cron ejecutará el script `/usr/sbin/checksecurity` que almacenará la información de estos cambios.

Para que este chequeo sea hecho usted debe colocar `CHECKSECURITY_DISABLE="FALSE"` dentro de `/etc/checksecurity.conf`. Note, que este es el predeterminado, a menos de que usted haya cambiado algo, esta opción será colocada como "FALSE".

El comportamiento por defecto no manda la información al superusuario, pero en cambio guarda diariamente copias de los cambios dentro de `/var/log/setuid.changes`. Usted debe colocar el CHECKSECURITY_EMAIL (dentro de `/etc/checksecurity.conf`) a 'root'. Mire `checksecurity(8)` para mas información de configuración.

4.15. Otras recomendaciones

4.15.1. No use software que dependa de svgalib

SVGAlib es muy bueno para los amantes de la consola como yo, pero durante mucho tiempo se ha comprobado que esto ha sido muy inseguro. Han sido liberadas fallas en contra de `zgv` y era sencillo convertirse en root. Intente evitar el uso de programas que usen SVGAlib siempre que sea posible.

Capítulo 5

Asegurando los servicios que se ejecutan en su sistema

Los servicios que corren en su sistema pueden ser asegurados de dos maneras:

- Haciéndolos accequibles dentro de los puntos (interfaces) en los que tienen que estar.
- Configurándolos de una manera apropiada para que puedan ser debidamente usados por los usuarios legítimos de una manera autorizada.

Restringir los servicios de modo que solamente puedan ser accedidos desde un lugar dado puede ser hecho restringiendo el acceso al nivel del kernel (i.e. cortafuego), configúrelos sólo para escuchar en un interfaz dada (algunos servicios no pueden suministrar ésta característica) o usando otros métodos, por ejemplo el parche linux vserver (para 2.4.16) puede ser usado para forzar procesos de forma que usen solo una interfaz.

En cuanto a los servicios usados desde `inetd` (telnet, ftp, finger, pop3...) cabe notar que inetd no puede ser configurado de forma que los servicios solo escuchen en una interfaz dada. Sin embargo, su sustito el metademonio `xinetd` incluye un `bind` justamente para ste problema. Vea `xinetd.conf(5)`.

```
service nntp
{
 socket_type = stream
 protocol = tcp
 wait = no
 user = news
 group = news
 server = /usr/bin/env
 server_args = POSTING_OK=1 PATH=/usr/sbin/:/usr/bin:/sbin/:/bin
+/usr/sbin/snntpd logger -p news.info
 bind = 127.0.0.1
}
```

Laa siguientes secciones detallan como cada servicio determinado puede ser configurado debidamente dependiendo de los usos que se quieran dar.

5.1. Asegurando ssh

Si aún está usando telnet en vez de ssh, debe detener la lectura de este manual y cambiar esto. Ssh debería ser usado para todas las entradas remotas en vez de telnet. En una época donde es fácil husmear el tráfico de internet y obtener contraseñas en texto plano, debe usar sólo protocólos que usen criptografía. De una vez, ejecute un `apt-get install ssh` en su sistema.

Anime a todos los usuarios de su sistema para usar ssh en vez de telnet, o mejor aún, desinstale telnet/telnetd. Además, debe evitar las entradas al sistema usando ssh como root y use métodos alternativos en vez de root, como `su` o `sudo`. Finalmente, el archivo `sshd_config`, dentro de `/etc/ssh`, debe ser modificado para aumentar la seguridad así:

- `ListenAddress 192.168.0.1`

  Haga que ssh escuche solo la interfaz dada, sólo en un caso de que haya más de uno (y no necesite un ssh disponible sobre éste) o que en un futuro agrege una nueva tarjeta de red (y no necesite una conexión desde ssh en ésta).

- `PermitRootLogin No`

  Intente no permitir al Root entrar tanto como sea posible. Si alguien quiere volverse root por vía ssh, dos logins serán necesarios y la contraseña root no puede ser obtenida a fuerza bruta por vía SSH.

- `Listen 666`

  Cambie el puerto de escucha de tal manera que el intruso no pueda estar completamente seguro de si está corriendo un demonio de sshd. (Note que esto es seguridad por oscuridad).

- `PermitEmptyPasswords no`

  Las contraseñas en blanco convierten en broma la seguridad del sistema.

- `AllowUsers alex ref`

  Permita que solamente ciertos ususarios tengan acceso vía ssh a esta máquina.

- `AllowGroups wheel admin`

  Permita que solamente los miembros de ciertos grupos tengan acceso vía a ssh a esta máquina. AllowGroups y AllowUsers tienen directivas equivalentes para denegar el acceso a una máquina. Predeciblemente se llaman “DenyUsers” y “DenyGroups”.

- `PasswordAuthentication yes`

  Queda completamente a su elección lo que usted quiera hacer. Es más seguro permitir el acceso a la máquina solamente a usuarios con llaves ssh en el archivo ~/.ssh/authorized_keys. Si es lo que quiere déle el valor “no”.

Como nota final, dese cuenta que estas directivas son de los archivos de la configuración de OpenSSH. Ahora mismo hay tres demonios SSH usadados habitualmente, ssh1, ssh2, y el OpenSSH de la gente de OpenBSD. Ssh1 fue el primer domonio ssh diaponible y aún es el más comunmente usado (hay rumores de que existe incluso un porte a windows). Ssh2 tiene muchas ventajas sobre ssh1, pero se distribuye con una licencia mixta de código abierto-cerrado. OpenSSH es un demonio completamente libre que soporta tanto ssh1 como ssh2. La versión instalada en Debian cuando se escoge el paquete 'ssh' es OpenSSH.

Usted puede leer más información acerca de la configuración de SSH con PAM en el security mailing list archives (`http://lists.debian.org/debian-security/2001/debian-security-200111/msg00395.html`).

5.2. Asegurando Squid

Squid es uno de los servicios más populares de proxy/cache,y hay alunos problemas de seguridad que deben tenerse en cuenta. Por defecto Squid impide todas las solicitudes de los ususarios. Usted debe configurar Squid para permitir el acceso a los ususarios, servidores o redes confiables o redes definidas en una Lista de Control de Acceso en `/etc/squid.conf`, mire la guía del usuario de Squid en Squid User's Guide (`http://squid-docs.sourceforge.net/latest/html/book1.htm`) para más información acerca de la definición de las reglas ACL.

Además, si no configuró debidamente, algúien puede enviar correo a través de Squid, puesto que el diseño de los protocolos HTTP y SMTP es semejante. El archivo de configuración Squid niega por defecto el acceso al puerto 25. Si desea permitir las conexiones del puerto 25 adiciónelo a la lista Safe_ports. Sin embargo, esto *NO* is recomendado.

Ajustar y configurar debidamente el proxy/cache es solamente una parte para mantener su sitio seguro. Otra tarea necesaria es analizar los registros de Squid asegurándose que todas las cosas que están trabajando, deben hacerlo como se espera. Hay algunos paquetes en Debian GNU/Linux que pueden ayudar al administrador a hacer esto. Los siguientes paquetes estan disponibles en woody (Debian 3.0):

- `calamaris` - Analizar de las bitácoras de los proxy Squid y Oops.
- `modlogan` - Analizador modular de bitácoras.
- `sarg` - Generador de Reportes de Análisis de Squid.

ARREGLAME: Add more information about security on Squid Accelerator Mode

5.3. Asegurando FTP

Si realmente tiene que usar FTP (sin enmascararlo con sslwrap o dentro de un tunel ssl o ssh), debería hacer cambio del directorio raíz de FTP hacia el directorio de los usuarios ftp,

de modo que que el usuario sea incapaz de mirar cualquier otra cosa que su propio derectorio. De otra manera ellos pueden atravesar su sistema de archivos tal como si tuvieran una línea de comandos. Usted puede añadir la siguiente línea en su `proftpd.conf` en la sección global para habilitar esta característica del cambio de directorio raíz: feature:

```
DefaultRoot ~
```

Reinicie proftpd con `/etc/init.d/proftpd restart` y revise si puede escapar desde su directorio raíz ahora.

Para impedir los ataques de Proftp DoS use ../../.., y adicione la siguiente línea en `/etc/proftpd.conf`: `DenyFilter \*.*/`

No olvide que FTP envía login y contraseñas de autenticación en el texto plano (esto no es un problema si usted está proporcionando un servicio público anónimo) y hay buenas alternativas en Debian para ésto. Por elemplo, `sftp` (sumistrado por `ssh`). También hay implementaciones libres de SSH para otros sistemas operativos, por ejemplo: putty (http://www.chiark.greenend.org.uk/~sgtatham/putty/) y cygwin (http://www.cygwin.com).

Sin, embargo, si aún mantiene el servidor de FTP mientras los usuarios acceden a SSH podría encontrar un problema típico. Usuarios que acceden a los servidores Anónimos de FTP dentro de un sistema asegurado con SSH es el camino intentar entrar en el *servidor FTP*. Mientras el acceso se niegue, la contraseña nunca se enviará por la red en texto plano. Para evitar esto, el desarrollador de ProFTPd, TJ Saunders, creó un parche que impide a los usuarios anónimos del servidor FTP intentar contraseñas con cuentas SSH válidas. Más información y parches disponibles en: ProFTPD Patches (http://www.castaglia.org/proftpd/#Patches).

5.4. Asegurando el acceso al sistema X Window

Hoy en día, más y más empresas usan las terminales X cuando necesitan un servicio para muchas estaciones de trabajo, ésto puede ser peligroso porque necesita permitir que un servidor de archivos se conecte con los clientes (el servicio X, desde el punto de vista X. X intercambia la definición de cliente y servidor) Si sigue la (muy mala) sugerencia de muchos documentos, tecleé `xhost +` en su máquina. Esto permite conenctar con su sistema a cualquier cliente X. Para tener una seguridad ligeramente mejor, puede usar el comando `xhost +hostname` en vez de la anterior para permitir un acceso desde servidores específicos.

Una solucón mucho más segura es usar ssh como túnel de X y encriptar la sesión completa. Ésto se hace automáticamente cuando se hace ssh a otra máquina. Esto puede habilitarse en el archivo `/etc/ssh/ssh_config` colocando `X11Forwarding` a `yes`. Cuando use SSH, usted de suspender completamente el acceso basado de xhost.

Para mayor seguridad, si no necesita acceso a X desde otras máquinas, dehabilite el enlace con el puerto tcp 6000 tecleando simplemente: `startx -- -nolisten tcp`

Este es el comportamiento original en XFree 4.0 (el servidor X suministrado en Debian 3.0). Si está usando XFree 3.3.6 (i.e. tiene un Debian 2.2 instalado) puede editar `/etc/X11/xinit/xserverrcc` para que tenga unas líneas como las siguientes:

```
#!/bin/sh
exec /usr/bin/X11/X -dpi 100 -nolisten tcp
```

Si usted está usando XDM digite `/etc/X11/xdm/Xservers:0 local /usr/bin/X11/X vt7 -dpi 100 -nolisten tcp`

Lea mas sobre la seguridad X Window en XWindow-User-HOWTO (http://www.linuxdoc.org/HOWTO/XWindow-User-HOWTO.html) (`/usr/share/doc/HOWTO/en-txt/XWindow-User-HOWTO.txt.gz`).

ARREGLAME: Add info on thread of debian-security on how to change config files of XFree 3.3.6 to do this.

5.4.1. Revisar su administrador visual

Si usted solamente quiere tener un administrador visual instalado para el uso local (teniendo un bonito login grafico), asegurarse que el material seguro XDMCP (control de protocolo de administrador visual X) este inhabilitado. En XDM usted puede hacer esto con la siguiente linea. `/etc/X11/xdm/xdm-config`:

```
DisplayManager.requestPort: 0
```

Normalmente, todos los administradores visuales estan configurados para no iniciar los servicios de XDMCP por defecto en Debian.

5.5. Seguridad en el acceso de impresión (El asunto de lpd y lprng)

Imagine, que usted llega al trabajo, y la impresora está botando interminables cantidades de papel porque alguien está negando el servicio de linea de su demonio de impresión. ¿No es terrible?

En cualquier arquitectura de impresión Unix, tiene que haber la forma de enviar los datos de los clientes a los servidores de impresión. En el `lpr` y `lp` tradicional, el comando del cliente es copiado o se hace un enlace simbólico de los datos en el directorio de cola (por lo cual usualmente estos programas son SUID o SGID).

Para evitar algunos asuntos usted debe mantener seguros, los servidores de impresión. Esto significa que usted necesita configurar su servicio de impresión para que solo se permita la conexión del conjunto de servidores confiables. Para hacer esto es necesario, añadir los servidores a los que se les va a permitir imprimir en `/etc/hosts.lpd`.

Sin embargo, incluso si usted hace esto, el demonio `lpr` acepta las conexiones entrantes en el puerto 515 de cualquier interfaz. Deberia considerar hacer una regla de cortafuegos para las conexiones de red/servidor a las cuales no se permite la impresión (el demonio `lpr` no puede ser limitado a escuchar únicamente a una dirección IP dada).

`Lprng` se prefiere en lugar de `lpr` porque este puede ser configurado para hacer el control de acceso a IP, ademas se puede especificar cual interfaz va a emplear (aunque sea un poco extraño).

Si está usando el servicio de impresión de su sistema, pero solo localmente, no querrá compartir este servicio en la red. Puede considerar el uso de otros sistemas de impresión, como el servicio proporcionado en `cups` PDQ (`http://pdq.sourceforge.net/`) el cual se basa en el permiso de un usuario del dispositivo`/dev/lp0`

En `cups`, los datos de impresión se transfieren al servidor vía el protocolo http. Esto significa que el programa del cliente no necesita ningún privilegio especial, solamente requiere que el servidor esté escuchando sobre un puerto cualquiera.

Sin embargo, si usted quiere usar `cups`, pero solo localmente usted puede configurar esto para escuchar a la interfaz loopback cambiando `/etc/cups/cupsd.conf`:

```
Listen 127.0.0.1:631
```

Hay muchas otras opciones de seguridad, como por ejemplo permitir o negar redes y servidores en este archivo de configuración. Sin embargo si no los necesita, debería limitar posibilidad de escuchar el puerto. `Cups` también ofrece documentación a través del puerto HTTP, si no quiere revelar información potencialmente útil para agresores externos (estando abierto el puerto), también agregue:

```
<Location />
 Order Deny,Allow
 Deny From All
 Allow From 127.0.0.1
</Location>
```

Este archivo de configuración puede ser modificado para añadir muchas caracteristicas incluyendo certficados SSL/TLS y criptografía. Los manuales estan disponibles en http://localhost:631/ or at cups.org.

ARREGLAME: Add more content (the article on Amateur Fortress Building (`http://www.rootprompt.org`) provides some very interesting views).

ARREGLAME: Check if PDG is available in Debian, and if so,suggest this as the preferred printing system.

ARREGLAME: Check if Farmer/Wietse has a replacement for printer daemon and if it's available in Debian.

5.6. Asegurar el demonio de correo

Si su servidor no es un sistema de correo, usted realmente no necesita tener un demonio de correo escuchando conexiones entrantes, pero usted podría querer envío de correo local, por

ejemplo para recibir el correo del usuario Root desde cualquier sistema de alerta que usted tenga en algún lugar.

Para hacer esto en un sistema Debian, tendrá que eliminar el demonio smtp desde inetd:

```
$ update-inetd --disable smtp
```

y configurar el demonio de correo solo para escuchar en la interfaz loopback. En exim (el MTA por defecto) usted puede hacer esto añadiendo la siguiente línea editando: `/etc/exim.conf` y añadiendo la siguiente linea:

```
local_interfaces = "127.0.0.1"
```

Reinicie ambos demonios (inetd y exim) y estarán escuchando en el socket 127.0.0.1:25 solamente. Sea cuidadoso, y primero desconecte inetd, de lo contrario, exim no iniciara ya que el demonio inetd está manejando las conexiones entrantes.

Para usar postfix edite `/etc/postfix/main.conf`:

```
inet_interfaces = localhost
```

Si usted solo quiere un correo local, este metodo es mejor que usar la cubierta tcp-wrapping al demonio de correo o añadir las reglas del cortafuego para limitar el acceso de cualquier persona a este. Sin embargo, si necesita que escuche en otras interfaces, debería considerar lanzarlo desde inetd y añadir un tcp-wraping de forma que las conexiones sean revisadas contra `/etc/hosts.allow` y `/etc/hosts.deny` también será advertido cuando un acceso no autorizado está atentando en contra de su demonio de correo, usted debe instaurar un registrador apropiado para cualquiera de los metodos mencionados anteriormente.

5.7. Recibiendo Correo de forma segura

Leer/recibir correo es el protocolo más común de texto plano. Si usted usa POP3 o IMAP para obtener su correo, la contraseña es enviada en texto plano a través de la red, de modo que casi cualquiera podría leer su correo a partir de ahora. En lugar de esto, use SSL (Capa segura de Sockets) para recibir su correo. La otra alternativa es ssh, si tiene una cuenta shell en la máquina que actua como el servidor POP o IMAP. Este es un ejemplo básico `fetchmailrc` para demostrar esto:

```
poll my-imap-mailserver.org via "localhost"
 with proto IMAP port 1236
 user "ref" there with password "hackme" is alex here warnings 3600
 folders
 .Mail/debian
 preconnect 'ssh -f -P -C -L 1236:my-imap-mailserver.org:143 -l ref
 my-imap-mailserver.org sleep 15 </dev/null > /dev/null'
```

La preconexión es la línea más importante. Este lanza una sesión ssh y crea el tunel necesario, el cual automaticamente envía las conexiones para tener acceso a localhost puerto 1236 al servidor de correo IMAP, pero codificado. Otra posibilidad seria, usar el `fetchmail` con la caracteristica ssl.

Si usted quiere suministrar un servicio de correo codificado como POP e IMAP,`apt-get install stunnel` e inicie sus demonios de esta es la forma:

```
stunnel -p /etc/ssl/certs/stunnel.pem -d pop3s -l /usr/sbin/popd
```

Este comando encapsula al demonio proveido (-l) en el puerto (-d) y usa el certificado ssl especificado (-p).

5.8. Asegurando BIND

Hay diferentes consideraciones que puede implementar para asegurar el demonio de servidor de nombres, las cuales son similares a las mismas que cuando se asegura cualquier servicio dado:

- Configurar el demonio por si solo apropiadamente para que este no pueda ser afectado desde afuera. Esto abarca limitar las posibles dudas de los clientes: zona transferida y consultas recursivas.
- Limitar el acceso del demonio al servidor mismo, de modo que si este es usado para entrar, el daño en el sistema esté limitado. Esto incluye correr el demonio como un usuario no privilegiado y cambiarle el directorio raiz.

Deberia restringir alguna de la información que es dada por el servidor DNS para clientes externos para que no pueda ser usado para acceder a información valiosa de su organización que usted no quiere dar. Esto incluye añadir las siguientes opciones: *allow-transfer*, *allow-query*, *allow-recursive* y *version*.Puede limitar en una sección global (para que se aplica a todas las zonas presentes) o sobre una base por zona. Esta información esta documentada en el paquete `bind-doc`, lea más sobre esto en `/usr/share/doc/bind/html/index.html` una vez el paquete este instalado.

Imagine que su servidor está conectado a Internet y a su red interna (su IP interno es 192.168.1.2)(un servicio de multi domicilio basico). Usted no quiere dar ningun servicio para Internet y solo quiere permitir el lookups DNS desde su servidor interno. Usted podria restringir esto para incluirlo en: `/etc/bind/named.conf`:

```
options {
  allow-query { 192.168.1/24; } ;
  allow-transfer { none; } ;
  allow-recursive { 192.168.1/24; } ;
```

```
  listen-on { 192.168.1.2; } ;
  forward { only; } ;
  forwarders { A.B.C.D; } ;
};
```

La opción*listen-on*hace el bind DNS solo para la interfaz que tiene la dirección interna, pero si esta interfaz es la misma como la interfaz que se conecta a Internet (por ejemplo, si usted está usando NAT), las dudas seran solamente aceptadas si llegan desde su servidor interno. Si el sistema tiene multiples interfaces y el *listen-on* no está presente, solamente los usuarios internos podrian pregutar, ya que el puerto seria accesible para los atacantes exteriores, ellos podrian tratar de arrojarlo al servidor DNS (o explotar el amortiguador desbordandose agresivamente). Usted aun podría leer esto en 127.0.0.1 si usted no está dando el servicio DNS por ningun otro sistema que el de usted mismo.

El registro version.bind en la clase caos contiene la versión del proceso bind que se está ejecutando. Esta información es frecuentemente usada por dispositivos automaticos e individuos maliciosos que desean determinar si el bind de uno es vulnerable a un ataque específico. Para proporcionar falsa o negativa información en el registro de la version.bind, uno limita la probabilidad que un servidor pueda ser atacado basandonos en la versión publicitaria.Para suministrar su proia versión, utilice la *version* dirigida de la siguiente manera:

```
options {
 ... various options here ...
 version "Not available.";
};
```

Cambiar el registro de la version.bind que no proporciona una protección actual en contra de los ataques, pero este debería ser considerado un salva guardia útil. Con respecto a limitar los privilegios de BIND, usted debe darse cuenta que si un usuario del non-root recorre Bind, Bind no podra detectar las nuevas interfaces automaticamente. Como por ejemplo si usted pone en un portatil una tarjeta PCMCIA. Cambie el archivo README Debian en el directorio nombrado (`/usr/share/doc/bind/README.Debian`)para mas información acerca de este uso. Recientemente han habido muchos problemas de seguridad en lo que concierne a BIND, y por esto es necesario cambiar el usuario util cuando sea posible.

Para correr BIND bajo un usuario diferente, primero cree un usuario separado y un grupo para esto (no es buena idea usar,*not* nobody o nogroup para todo sevicio que no corra como raiz). En este ejemplo, el usuario y el grupo `named`serán usados. Usted puede hacer esto entrando a:

```
addgroup named
adduser --system --ingroup named named
```

Ahora edite `/etc/init.d/bind` con su editor favorito y cambie la linea comenzando con:

```
start-stop-daemon --start
```

a

```
start-stop-daemon --start --quiet --exec /usr/sbin/named -- -g named -u named
```

Todo lo que usted necesita hacer ahora es reiniciar Bind'/etc/init.d/bind, y luego cambiar su syslog por dos entradas como estas:

```
Sep 4 15:11:08 nexus named[13439]: group = named
Sep 4 15:11:08 nexus named[13439]: user = named
```

Gwow! su nombre ahora no corre como raíz. Para archivar la máxima seguridad de Bind, ahora contruya su aseguramiento del cambio de directorio raiz (ver'Uso del cambio de directorio raíz' en la página 43)alrededor de su demonio. Hay una forma fácil para hacer esto: la opción `-t` (ver el manual de pagina `named(8)`). Esto le permitirá por si mismo un cambio de directorio raiz Bind, dentro del directorio dado, sin que usted necesite instlar un aseguramiento en el cambio de directorio raiz y sin preocuparse por la dinamica de librerias. Los únicos archivos que necesitan estar en ese cambio de aseguramiento de directorio son:

```
dev/null
etc/bind/ - should hold named.conf and all the server zones
sbin/named-xfer - if you do name transfers
var/run/named/ - should hold the pid and the name server cache (if
 any) this directory needs to be writable by named
 user
var/log/named - if you setup logging to a file, needs to be writable
 for the named user
dev/log - syslogd should be listening here if named is configure to
 log through it
```

Para que su denmonio BIND trabeje apropiedamente, este necesita permiso en los archivos nombrados. Ésta es una tarea fácil ya que los archivos de configuarción estan siempre en `/etc/named/`. Tenga en cuenta que esto solamente necesita acceso de lectura para los archivos de la zona, a menos que este sea un secundario o un servidor llamado cache. Si este es su caso usted tendra que dar permiso de lecto-escritura a las zonas necesarias (asi como la zona transferida desde los tarbajos del servidor primario).

Si usted quiere leer mas información sobre porque BIND no corre como el usuario non-root sobre los sistemas Debian, por favor revise el sistema Bug Tracking relacionado a BIND, específicamente Bug #50013: bind should not run as root (`http://bugs.debian.org/50013`).

Usted, también puede encontrar mas información con respecto al cambio de raiz de BIND. Chroot-BIND-HOWTO (`http://www.linuxdoc.org/HOWTO/Chroot-BIND-HOWTO.html`) (analizar Bind 9) y Chroot-BIND8-HOWTO (`http://www.linuxdoc.org/HOWTO/Chroot-BIND8-HOWTO.html`) (analizar Bind8). Estos mismos documentos deberian

estar disponibles a traves de la instalación de `doc-linux-text` (versión de texto) o `doc-linux-html` (versión html).

Si usted está instaurando un aseguarmiento del cambio de directorio raiz completo (i.e no solo `-t`)para BIND 8.2.3 en Debian (potato), asegurese de tener los siguientes archivos en:

```
dev/log - syslogd should be listening here
dev/null
etc/bind/named.conf
etc/localtime
etc/group - with only a single line: "named:x:GID:"
etc/ld.so.cache - generated with ldconfig
lib/ld-2.1.3.so
lib/libc-2.1.3.so
lib/ld-linux.so.2 - symlinked to ld-2.1.3.so
lib/libc.so.6 - symlinked to libc-2.1.3.so
sbin/ldconfig - may be deleted after setting up the chroot
sbin/named-xfer - if you do name transfers
var/run/
```

ARREGLAME, merge info from http://www.cryptio.net/~ferlatte/config/ (Debian-specific) and http://www.psionic.com/papers/whitep01.html.

5.9. Asegurando Apache

ARREGLAME. Add content.

Usted puede limitar el acceso a el servidor Apache si si usted quiere usar esto solo internamente (para objetivos de prueba, para tener acceso al archivo`doc-central` etc..) y si no quiere que extraños tengan esto. Para hacer esto use el `Listen` o `BindAddress` dirigidos en `/etc/apache/http.conf`.

Usando Listen:

```
Listen 127.0.0.1:80
```

Usando BindAddress:

```
BindAddress 127.0.0.1
```

Luego reinicie Apache con `/etc/init.d/apache restart` y vera que esto es de solo Audición en la interfaz `loopback`.

De todos modos, que usted no este usando todo lo funcionamiento suministrado por Apache, usted podria querer dar un vistazo a otro servicio de la web proporcionados en Debian como `dhttpd`.

La Apache Documentation (`http://httpd.apache.org/docs/misc/security_tips.html`) proporciona información relacxionada con las medidas de seguridad que deben ser tomadas en el servidor web del Apache (esta misma información está suministrada en Debian por el paquete`apache-doc`).

5.10. Asegurando finger

Si usted quiere recorrer el servicio de finger, primero preguntese si usted necesita realizar esto. Si lo hace, usted mismo descubrira que Debian proporciona muchos demonios finger (Puest fuera de `apt-cache search fingerd`):

- cfingerd - Demonio finger configurable
- efingerd - Es otro demonio finger para unix capaz de una fina-sintonización de su rendimiento.
- ffingerd - Un demonio seguro.
- fingerd - Remoto servidor de la información del usuario
- BSD- Demonio finger con soporte qmail.

`ffingerd` es el demonio finger recomendado para si usted va ausar esto para un servicio publico. De todos modos usted se fortalece, cuando establece este a traves de inetd, xinetd o tcpserver para: limitar el numero de procesos que estaran corriendo al mismo tiempo, limitar el acceso para el demonio finger a partir de un numero dado por los servidores (usando el wrappers tcp) y teniendo esto solamente por audición para la interfaz en la que usted necesita estar.

5.11. Cambio general de directorio raíz y paranoia suid

Es probablemente favorable decir que la complejidad de BIND es la razón por la cual este ha sido revelado a muchos atacantes en los años recientes (ver seguridad Bind en la pagina 52). (ver 'Asegurando BIND' en la página 58)

Otros programas con caracteristicas complejas y una larga base del usuario instalado incluyen Sendmail y algunos demonios (e.g. WUftpd). (Evidentemente un programa sin caracteristicas y sin satisfacer que pueden ser muy inseguros, e ineficacez).

De cualquier modo, usted recorre cualquiera de estos, considere los dispositivos similares para ellos -revocando los privilegios de root, corriendo en un aseguramiento del cambio de directorio raiz- reemplazandolos con una equivalencia mas segura.

5.12. Texto claro general con el password paranoia

Usted deberia tratar de evitar cualquier servicio de red el cual envia y recibe contraseñas en un texto claro sobre una red como FTP/Telnet/NIS/RPC. El autor recomienda para todos el uso de ssh en cambio de telnet y ftp.

Mantenga en mente que migrar de telenet a ssh pero usando otros protocolos de texto claro no aumentan su seguridad de NINGUNA forma! lo mejor seria eliminar ftp, telnet, pop, imap, http y suplantarlos con sus respectivos servicios codificados. Usted debe considerar moverse desde otros servicios hasta sus versiones SSL, ftp-ssl, telnet-ssl, pop-ssl, https...

Muchos de estas indicaciones numeradas en la parte superior se aplican a documentos en todo el sistema Unix (Usted los encontrara si lee cualquier otro hardening-related relacionado con lo que tiene que ver con Linux y otros Unix).

5.13. Incapacitar NIS

Es posible que usted no tenga que usar NIS, en el servicio de información de la red, porque este permite que la contraseña actue. Este puede ser demasiado inseguro si su organización está rota.

Si usted necesita que la contraseña actue entre maquinas, usted deberia considerar usar otras alternativas. Por ejemplo usted puede colocar un servidor LDAP y configurar PAM en su sistema para contactar el servidor LDAP para la autenticación del usuario. Usted puede encontrar una detallada organización en el LDAP-HOWTO (`http://www.linuxdoc.org/HOWTO/LDAP-HOWTO.html`) (`/usr/share/doc/HOWTO/en-txt/LDAP-HOWTO.txt.gz`).

Lea mas sobre la seguridad en NIS-HOWTO (`http://www.linuxdoc.org/HOWTO/NIS-HOWTO.html`) (`/usr/share/doc/HOWTO/en-txt/NIS-HOWTO.txt.gz`).

ARREGLAME (jfs): Add info on how to setup this in Debian

5.14. Desactivar los servicios RPC

Usted deberia desactivar donde quiera que sea posible. Muchas fallas seguras de este sevicio son conocidas y pueden ser fácilmente exploradas. Por otra parte los servicios NFS son totalmente importantes en algunas redes, de esta manera usted encontrara un balance de seguridad y utilidad en su red. El DDoS (distribución negativa del servicio)ataca el uso de RPC que son explotados para entrar en el sistema y actuar tanto como el llamado agente/manipulador. Lea mas sobre la seguridad NFS en NFS-HOWTO (`http://www.linuxdoc.org/HOWTO/NFS-HOWTO.html`) (`/usr/share/doc/HOWTO/en-txt/NFS-HOWTO.txt.gz`).

Inhabilitar el paquete `portmap` es super sencillo. Hay diferentes mátodos. Uno de los más sencillos en un sistema Debian 3.0 es hacer un desinstalamiento del paquete `portmap`. Si usted

está usando otra versión, tendrá que desactivar el servicio como se ve en 'Deshabilitar los demonios' en la página 23, esto es debido a el programa que forma parte del paquete `net-base` (el cual no puede ser desinstalado sin que el sistema se haya destruido).

Esto en realidad elimina toda conexión con el sistema relacionado a el `portmap` en `/etc/rc${runlevel}.d/`,lo cual es algo que usted también hacerlo manualmente. Otra posibilidad es `chmod 644/etc/init.d/portmap`, pero que da un mensaje de de error o cuando se entra a el sistema. Usted también puede deshacer `start-stop-daemon` en la parte `/etc/init.d/portmap` que es la cubierta del escrito.

5.15. Añadir capacidades al cortafuegos

El Sistema operativo Debian GNU/Linux que tiene capacidades built-in proporcionadas por Linux kernel. Esto significa que si usted instala un sistema potato (descargar Debain 2.2) (el Kernel defectuoso es 2.2) usted tendra el corta-fuegos `ipchains` disponible en el Kernel el cual seguramente estara instalado (debido a su prioriedad). Si usted instala instala un sistema woody (Descargar Debian 3.0) (el Kernel defectuoso es 2.4) usted tendra el corta fuegos `ipchains` disponible. `iptables`.

Algunos usuarios podrian colocar reglas a el corta-fuegos como fuente para este escrito. Sin embargo revise que programas o caracteristicas del corta fuegos usted debe usar ya que ellos pueden explorar otros archivos y cambiar las definiciones que usted agrego en el inicio. Por ejemplo, `firewalk`, para uno, usara otro archivo de configuración para colocar el corta fuegos.

5.15.1. Reglas Iptables

Si usted está usando Debian 3.0, usted notara que el paquete `iptables` lo tiene instalado. Este es el soporte para el 2.4.4+ de la implementación de un filtro de la red de Kernel. Ya que solo despues de la instalación el sistema no puede conocer ninguna regla corta-fuegos (reglas del corta-fuegos son también sistemas específicos) usted debe habilitar `iptables`.

Para hacerlo como se debe, es de la siguiente manera:

- edite `/etc/default/iptables` de tal manera que la variable. `enable_iptables_initd` este colocada para *true*
- Cree un estructura del corta fuegos usando Iptibles, usted puede usar la linea de comando (ver `iptables(8)`) o algunas herramientas proporcionadas por el paquete corta fuegos Debian (ver'Paquetes del Corta Fuegos' en la página 66). Debe crear una estructura de reglas del corta fuegos para ser usada cuando el cortafuego esté *activo* y otra cuando el corta fuegos esté *inactivo* (estas pueden ser reglas vacías).
- Salvar las reglas que usted creo usando `/etc/init.d/iptablessave_active` y `/etc/init.d/iptables save_active` para recorrer estos escritos con las reglas corta fuegos que usted quiera capacitar.

Una vez esté hecha la estructura del corta fuegos, ésta es almacenada en el directorio `/var /lib/iptables/` y será ejecutada cuando el sistema arranque (o cuando reinicie el script con los argumentios *start* y *stop*). Por favor tenga en cuenta que la configuración inicial de Debian carga el código del corta fuegos en los niveles del multiusos (2-5),muy pronto (10). Es detenido en el nivel monousuario (1), cámbielo si no es la política local.

Prevenga que algunos de los paquetes se encuentran fuera de la linea pueden intrducir escritos del corta fuegos para ser recorrido, esto afectara indudablemente a la estructura comun y a usted entoces tendra un efecto indeseado. Consulte la documentación del paquete de documentación y use algunas de estas organizaciones.

Si usted no tiene un indicio sobre como colocar sus reglas al corta fuegos consulte el *Paquete Filtrador HOWTO* proporcionado por `iptables` al leer fuera de la linea en `/usr/share/doc /iptables/html/`

5.15.2. El sistema local corta fuegos

Usted puede usar las reglas de corta fuegos cono una forma para asegurar el acceso en un sistema local, invluso para limitaer la salida de comunicación hecha por este. Las reglas corta fuegos pueden ser usadas también para protejer procesos que *no* pueden ser configurados apropiadamente ni proveer servicios para algunas redes, direcciones, IP, etc...

Sin embargo, este paso se presentara despues en el manual, basicamente porque es *mucho* mejor para no depender únicamente de la capacidad del corta fuegos para protejer un sistema dado. La seguridad en un sistema no puede ser hecho de cubiertas, el corta fuegos deberia ser el ultimo en incluirse, una vez todos los servicios hayan sido fortalecidos. Usted puede fácilmente imaginar un plan en el cual el sistema está protegido solamente por un corta fuegos incorporadoy un administrador blissfully que remueve las reglas del corta fuegos por cualquiera que sea la razón (problemas con la instalación, molestias, errores humanos...), este sistema abierto ampliamnete para un ataque.

5.15.3. Usar otros corta fuegos para proteger otros sistemas

Un corta fuegos de Debian también puede ser instalado para proteger, con reglas de filtración, el acceso a los sistemas *detras de este*, limitando sus exposición en Internet.

Usted aun puede colocar un buzon Debian GNU/Linux como un camino hacia el corta fuegos, i.e. un filtrador de corta fuegos completamente transparente a la red puede hacer falta en la dirección IP pudiendo ser atacado directamente.

Si usted no sabe mucho acerca del corta fuegos, lea el Cortar fuegos-howto que pueden ser encontrados en el `doc-linux-text` (otros formatos del documento también disponibles). Vea 'Estar enterado de los problemas de seguridad generales' en la página 15 para mas apuntes.

5.15.4. Paquetes del Corta Fuegos

Hay un software completo que pueden ser usados para colocar reglas de corta fuegos en un sistema Debian

- `fwbuilder`
- `mason`, el cual puede proponer reglas de corta fuegos basadas en el trafico de la red a su sistema "sees".
- `bastille` (En medio de los fuertes pasos que pueden hacer nuevas versiones de bastille, es la posibilidad de añadir reglas del corta fuegos del sistema para ser ejecutado en el sistema.)
- `ferm`
- `fwctl`
- `easyfw`
- `firewall-easy`
- `ipac-ng`
- `gfcc`
- `knetfilter`
- `firestarter`

Los ultimos paquetes: gfcc son administradores GUIS usados o bien en GNOME (los primeros dos) o en KDE (el último), están orientados a usuarios (i.e. para usuarios caseros) ya que los otros paquetes en la lista, están más orientados para administradores.

ARREGLAME: Add more info regarding this packages

ARREGLAME: Check Information on Debian firewalling and what/how does it change from other distributions.

ARREGLAME: Where should the custom firewalling code be enabled (common FAQ in debian-firewall?)

Capítulo 6

Fortalecimiento automático de sistemas Debian

Luego de haber leido toda la información en los capítulos anteriores usted puede estar pensando "tengo que hacer muchas cosas para fortalecer mi sistema, ¿no podrian ser automatizadas estas cosas?". La respuesta es si, pero tenga cuidado con las herramientas automatizadas. Algunas personas creen, que una herramienta de fortalecimiento no elimina la necesidad de una buena administración. Asi que no se sorprenda al pensar que usted puede automatizar todo el proceso y solucionar todos los problemas relacionados. La seguridad es un proceso constante en el cual el administrador debe participar y no puede alejarse y dejar hacer todo a las herramientas dado que ninguna herramienta sencilla lo puede afrontar: con toda la seguridad posible de las políticas de implementaciones, todos los ataques y todos los entornos.

A partir de Woody (Debian 3.0) existen dos paquetes específicos que son utiles para la seguridad del fortalecimiento. El `fortalecimiento` tomara un enfoque basado en las dependencias del paquete para rápidamente instalar paquetes valiosos de seguridad y removerá aquellos uqe tengan defectos, la configuración de paquetes debe estar hecha por el administrador. La `bastilla` que implementa unas políticas de seguridad proporcionadas por el sistema local basado en la cofiguración previa hecha por el administrador (la elaboración de la configuración puede ser un proceso guiado, hecho por preguntas sencillas de si y no).

6.1. Fortalecer (harden)

El `paquete` harden trata de hacer más fácil la instalación y administración de hosts que necesitan buena seguridad. Este paquete debería ser utilizado por gente que quiere una ayuda rápida para aumentar la seguridad del sistema. Para hacer esto el paquete se contradice con otros que poseen defectos conocidos incluyendo (pero ilimitadamente): defectos de seguridad conocidos (así como el buffer se desborda), uso de claves de texto plano, falta de control de acceso, etc. Además, este instala automáticamente algunas herramientas que deberían realzar la seguridad de cierta manera: herramientas de detección de intrusión, herramientas de análisis de

seguridad, etc. Harden instala los siguientes*paquetes* virtuales (en otras palabras, únicamente no satisface dependencias en otros):

- `harden-tools`: herramientas para realizar el sistema de seguridad (revisores deintegridad, detección de intrusión, los parches del kernel . . .)
- `harden-doc`: proporciona este mismo manual y otra documentación de seguridad relacionada con paquetes.
- `harden-environment`: Ayuda a configurar un entorno fortalecido (normalmente vacio).
- `harden-servers`: remueve a los servidores inseguros*poralguna* razón.
- `harden-clients`: removes clients considered insecure for some reason.
- `harden-remoteflaws`: removes packages with known security holes that could be used by a remote attacker to compromise the system (uses versioned *Conflicts:*).
- `harden-localflaws`: removes packages with known security holes that could be used by a local attacker to compromise the system (uses versioned *Conflicts:*).
- `harden-remoteaudit`: tools to remotely audit a system.

Tenga cuidado porque si usted tiene un software que necesite (y usted no desea desinstalarlo por ninguna razón) y este se contradice con alguno de los otros paquetes antedichos, usted no podrá usar totalmente el `harden`(fortalecimiento). Los paquetes "harden" no ejecutan ninguna acción (directamente). Sin embargo, ellos poseen un paquete de conflictos intencionales con paquetes inseguros conocidos. De esta forma, el sistema de embalaje de Debian no aprobará estos paquetes. Por ejemplo, cuando usted trata de instalar un demonio telnet con `harden-servers` apt mostrará:

```
# apt-get instalar telnetd
Los siguientes paquetes serán REMOVIDOS:
harden-servers
Los siguientes paquetes nuevos srán instalados:
telnetd
Desea continuar (y/n)
```

Esto podría causar algunas preocupaciones en la cabeza del administrador, quien debería reconsiderar sus acciones.

6.2. Bastilla Linux

Bastille Linux (`http://www.bastille-linux.org`) es una herramienta automática de fortalecimiento, originalmente orientada en torno a las distribuciones de Red Hat y Mandrake

Linux. Sin embargo, el paquete `bastille` proporcionado en Debian (desde woody) es arreglado para brindar la mima fucionalidad para el sistema GNU/ Linux.

Bastille puede ser utilizado con diferentes Frontends (todos son documentados en su propio manual de páginas en el paquete Debian) los cuales capacitan al administrador para:

- Responder las preguntas paso por paso considerando la seguridad deseada de su sistema (usando `InteractiveBastille(8)`)
- Usar un entorno por defecto para seguridad (en medio de tres: Lax, Moderar o Paranoia) en una seguridad dada (servidor o estación de trabajo) y dejar decidir a la Bastilla cual política de seguridad implementar (usando `BastilleChooser(8)`)
- Tomar un archivo predefinido de configuración (podría ser proporcionado por Bastilla o hecho por el administrador) e implementar una política de seguridad (usando `AutomatedBastille(8)`)

Capítulo 7

Firma de paquete en Debian

Este capítulo también podría ser titulado “como categotizar/ actualizar con seguridad a sus sitema Debian GNU/Linux” y este merece su propio capítulo básicamente porque no será acorde a algún otro capítulo.

A partir de hoy (diciembre 2001) Debian no proporciona paquetes firmados en cuanto a la distribución de y la publicación de woody (3.0) no integrará este artículo. Existe una solución para paquetes firmados que, según se espera, serán proporcionados en la próxima publicación.

7.1. El esquema propuesto para revisiones de firma de paquete

El esquema corriente (no implementado)para firma de paquete usando apt es:

- el archivo de publicación incluye el md5sum de Paquetes.gz (este contiene el md5sums de paquetes) y será firmado. La firma es algo que pertenece a una fuente de confianza.
- Este archivo de publicación firmado se baja por ’apt-get update’ y almacenado en todo el HD con paquetes.gz.
- Cuando un paquete va a ser instalado, primero se baja, luego el md5sum es generado.
- El archivo de publicación firmado es revisado (firma correcta) y este se extrae del md5sum para el archivo Paquetes.gz, el número de comprobación de Paquetes.gz es generado y (si es correcto) el md5sum del paquete que se bajó es extraido de este.
- Si el md5sum del paquete que se bajó es el mismo que el del archivo Paquetes.gz, el paquete será instalado o de lo contrario el administrador será alertado y el paquete será dejado en cache (asi el administrador puede decidir si se instala o no). Si el paquete no está en los Paquetes.gz y el administrador ha configurado el sistema para instalar únicamente los paquetes revisados, éste tampoco será instalado.

Adicional a esto, la cadena de Sums MD5 `apt` es capaz de verificar si un paquete se origina desde una publicación específica. Este es menos flexible que firmar paquete por paquete, pero puede ser combinado con este esquema también (véase más abajo).

La firma de un paquete ha sido discutida en Debian de vez en cuando, para mayor información usted puede leer: http://www.debian.org/News/weekly/2001/8/ y http://www.debian.org/News/weekly/2001/11/. `http://www.debian.org/News/weekly/2001/8/`y`http://www.debian.org/News/weekly/2000/11/`.

7.2. Alternativa firmar esquema por paquete

El esquema adicional de firmar cada uno y todos los paquetes, permite que estos sean revisados cuando no son tan referenciados por un archivo de Paquetes existentes, además, los paquetes tercera-persona donde nunca existieron Paquetes para que estos también puedan ser usados en Debian, sin embargo, no serán un esquema por defecto.

Este esquema de firma de paquetes puede ser implementado utilizando `debsig-verify`y `debsigs`. Estos dos paquetes pueden firmar y verificar firmas implantadas en el deb-itself. Debian ya tiene la capacidad de hacer esto ahora, pero el implementar esta política y las herramientas no será iniciado hasta después de la publicación de Woody (así como no retrasa su ciclo de publicación).

NOTA: Normalmente `/etc/dpkg/dpkg.cfg` se desmonta con “no-debsig” como por defecto.

7.3. Revisar publicaciones de paquete

En caso que usted desee implementar seguridad adicional, revise que pueda usar el script inferior, proporcionado por Anthony Thown. Este script puede hacer nuevas revisiones de seguridad automáticamente, para permitir al usuario, estar seguro que el software que él/ella está bajando une el software de distribución de Debian. Esto abstiene a los ralizadores de Debian de producir daños en el sistema de alguien sin la responsabilidad proporcionada cargando el archivo principal, o espejos reflejando algo casi, pero no del todo parecido a Debian, o espejos proporcionando copias atrasadas inestables con problemas de seguridad conocidos.

Esta muestra de código renombrada como `apt-release-check`, debería ser usada de la siguiente manera:

```
# apt-get update
# apt-release-check
(...resultados...)
# apt-get dist-upgrade
```

Primero usted necesita:

- pulsar las teclas de archivo software que suele firmar archivos de Publicaciones, `http://ftp-master.debian.org/ziyi_key_2002.asc` y las adiciona a `~/.gnupg/trustedkeys.gpg` (lo ucal es lo que `gpgv` se usa por defecto)
- remover algunas `/etc/apt/sources.list` líneas que no utilizanla estructura normal de distribuciones, o cambie el script de modo que este trabaje con ellas.
- estar preparado para ignorar que las actualizaciones de seguridad Debian no hayan firmado archivos de publicaciones, y que los archivos de Fuente no tengan la suma de comprobaciones en el archivo de Publicación (aun).
- prepárese para verificar que las fuentes apropiadas son firmadas con las llaves propicias.

```
#!/bin/bash
# This script is copyright (c) 2001, Anthony Towns
#
# This program is free software; you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation; either version 2 of the License, or
# (at your option) any later version.
#
# This program is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
# GNU General Public License for more details.

rm -rf /tmp/apt-release-check
mkdir /tmp/apt-release-check || exit 1
cd /tmp/apt-release-check

>OK
>MISSING
>NOCHECK
>BAD

arch=‘dpkg --print-installation-architecture‘

am_root () {
 [ ‘id -u‘ -eq 0 ]
}

get_md5sumsize () {
 cat "$1" | awk ’/^MD5Sum:/,/^SHA1:/’ |
 MYARG="$2" perl -ne ’@f = split /\s+/; if ($f[3] eq $ENV{"MYARG"}) {
print "$f[1] $f[2]\n"; exit(0); }’}
checkit () {
 local FILE="$1"
```

```
 local LOOKUP="$2"

 Y="‘get_md5sumsize Release "$LOOKUP"‘"
 Y="‘echo "$Y" | sed ’s/^ *//;s/ */ /g’‘"

 if [ ! -e "/var/lib/apt/lists/$FILE" ]; then
 if [ "$Y" = "" ]; then
 # No file, but not needed anyway
 echo "OK"
 return
 fi
 echo "$FILE" »MISSING
 echo "MISSING $Y"
 return
 fi
 if [ "$Y" = "" ]; then
 echo "$FILE" »NOCHECK
 echo "NOCHECK"
 return
 fi
 X="‘md5sum < /var/lib/apt/lists/$FILE‘ ‘wc -c <
/var/lib/apt/lists/$FILE‘" X="‘echo "$X" | sed ’s/^ *//;s/ */ /g’‘"
 if [ "$X" != "$Y" ]; then
 echo "$FILE" »BAD
 echo "BAD"
 return
 fi
 echo "$FILE" »OK
 echo "OK"
}

echo
echo "Checking sources in /etc/apt/sources.list:"
echo "~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~"
echo
(echo "You should take care to ensure that the distributions you’re downloadi
echo "are the ones you think you are downloading, and that they are as up to"
echo "date as you would expect (testing and unstable should be no more than"
echo "two or three days out of date, stable-updates no more than a few weeks"
echo "or a month)."
) | fmt
echo

cat /etc/apt/sources.list |
 sed ’s/^ *//’ | grep ’^[^#]’ |
 while read ty url dist comps; do
```

```
 if [ "${url%%:*}" = "http" -o "${url%%:*}" = "ftp" ]; then
 baseurl="${url#*://}"
 else
 continue
 fi
 echo "Source: ${ty} ${url} ${dist} ${comps}"

 rm -f Release Release.gpg
 wget -q -O Release "${url}/dists/${dist}/Release"

 if ! grep -q '^' Release; then
 echo " * NO TOP-LEVEL Release FILE"
 else
 origline=`sed -n 's/^Origin: *//p' Release | head -1`
 lablline=`sed -n 's/^Label: *//p' Release | head -1`
 suitline=`sed -n 's/^Suite: *//p' Release | head -1`
 codeline=`sed -n 's/^Codename: *//p' Release | head -1`
 dateline=`grep "^Date:" Release | head -1`
 dscrline=`grep "^Description:" Release | head -1`
 echo " o Origin: $origline/$lablline"
 echo " o Suite: $suitline/$codeline"
 echo " o $dateline"
 echo " o $dscrline"

 if [ "${dist%%/*}" != "$suitline" -a "${dist%%/*}" !=
"$codeline" ]; then echo " * WARNING: asked for $dist,
got $suitline/$codeline" fi

 wget -q -O Release.gpg "${url}/dists/${dist}/Release.gpg"
 sigline="`gpgv --status-fd 3 Release.gpg Release 3>&1 >/dev/null
2>&1 | sed -n "s/^\[GNUPG:\] GOODSIG [0-9A-Fa-f]* //p"`" if [
"$sigline" ]; then echo " o Signed by: $sigline"
 else
 echo " * NO VALID SIGNATURE"
 >Release
 fi
 fi
 okaycomps=""
 for comp in $comps; do
 if [ "$ty" = "deb" ]; then
 X=$(checkit "`echo
"${baseurl}/dists/${dist}/${comp}/binary-${arch}/Release" | sed 's,//*,_,g'`"
"${comp}/binary-${arch}/Release") Y=$(checkit "`echo
"${baseurl}/dists/${dist}/${comp}/binary-${arch}/Packages" | sed 's,//*,_,g'`
"${comp}/binary-${arch}/Packages") if [ "$X $Y" = "OK OK"
]; then okaycomps="$okaycomps $comp"
```

```
 else echo " * PROBLEMS WITH $comp ($X,
$Y)" fi elif [ "$ty" = "deb-src" ]; then
 X=$(checkit "‘echo
"${baseurl}/dists/${dist}/${comp}/source/Release" | sed ’s,//*,_,g’‘"
"${comp}/source/Release") Y=$(checkit "‘echo
"${baseurl}/dists/${dist}/${comp}/source/Sources" | sed ’s,//*,_,g’‘"
"${comp}/source/Sources") if [ "$X $Y" = "OK OK" ]; then
 okaycomps="$okaycomps $comp"
 else echo " * PROBLEMS WITH component $comp
($X, $Y)" fi fi
 done
 [ "$okaycomps" = "" ] || echo " o Okay:$okaycomps"
 echo
 done

echo "Results"
echo "~~~~~~~~"
echo

allokay=true

cd /tmp/apt-release-check
diff <(cat BAD MISSING NOCHECK OK | sort) <(cd /var/lib/apt/lists && find .
-type f -maxdepth 1 | sed ’s,^\./,,g’ | grep ’_’ | sort) | sed -n ’s/^> //p’
>UNVALIDATEDcd /tmp/apt-release-check
if grep -q ^ UNVALIDATED; then
 allokay=false
 (echo "The following files in /var/lib/apt/lists have not been validated."
 echo "This could turn out to be a harmless indication that this script"
 echo "is buggy or out of date, or it could let trojaned packages get onto"
 echo "your system."
 ) | fmt
 echo
 sed ’s/^/ /’ < UNVALIDATED
 echo
fi

if grep -q ^ BAD; then
 allokay=false
 (echo "The contents of the following files in /var/lib/apt/lists does not"
 echo "match what was expected. This may mean these sources are out of date,"
 echo "that the archive is having problems, or that someone is actively"
 echo "using your mirror to distribute trojans."
 if am_root; then
 echo "The files have been renamed to have the extension .FAILED and"
 echo "will be ignored by apt."
```

```
 cat BAD | while read a; do
 mv /var/lib/apt/lists/$a /var/lib/apt/lists/${a}.FAILED
 done
 fi) | fmt
 echo
 sed 's/^/ /' < BAD
 echo
fi

if grep -q ^ MISSING; then
 allokay=false
 (echo "The following files from /var/lib/apt/lists were missing. This"
 echo "may cause you to miss out on updates to some vulnerable packages."
 ) | fmt
 echo
 sed 's/^/ /' < MISSING
 echo
fi

if grep -q ^ NOCHECK; then
 allokay=false
 (echo "The contents of the following files in /var/lib/apt/lists could not"
 echo "be validated due to the lack of a signed Release file, or the lack"
 echo "of an appropriate entry in a signed Release file. This probably"
 echo "means that the maintainers of these sources are slack, but may mean"
 echo "these sources are being actively used to distribute trojans."
 if am_root; then
 echo "The files have been renamed to have the extension .FAILED and"
 echo "will be ignored by apt."
 cat NOCHECK | while read a; do
 mv /var/lib/apt/lists/$a /var/lib/apt/lists/${a}.FAILED
 done
 fi) | fmt
 echo
 sed 's/^/ /' < NOCHECK
 echo
fi

if $allokay; then
 echo 'Everything seems okay!'
 echo
fi

rm -rf /tmp/apt-release-check
```

Capítulo 8

Herramientas de seguridad en Debian

ARREGLAME: Se necesita más contenido.

Además Debian suministra un numero de herramientas de seguridad que pueden hacer en un equipo con Debian instalado adecuadamente para los propositos de analisis de seguridad. Algunos de ellos son suministrados cuando se instala el paquete `harden-remoteaudit`

8.1. Evaluación de herramientas de vulnerabilidad remota

Las herramientas suministradas por Debian para ejecutar la evaluación de vulnerabilidad remota son:

- nessus
- raccess
- whisker
- nikto (reemplazo de whisker)
- bass (no libre)
- satan (no libre)

La herramienta más completa y actualizada es `nessus`la cual está compuesta de un cliente (`nessus`) usado como un GUI y un servidor (`nessusd`)los cuales lanzan los ataques programados. Nessus incluye vulnerabilidades remotas para varios sistemas, incluyendo dispositivos de red, servidores ftp, servidores www, etc. Las últimas liberaciones son igual de capaces de analizar un sitio web y tratar de descubrir páginas interactivas diponibles y que podrían ser atacadas. También hay clientes Java y Win32 (no incluido en Debian) los cuales pueden ser usados para contactar el administrador

`Whisker` es un scaner de evaluación de vulnerabilidad orientada a la web incluyendo tácticas anti-IDS (la mayoria de ellas no son mas *anti-IDS*).Este es uno de los mejores cgi-scanners disponibles,son capaces de detectar servidores de www y lanzar únicamente un conjunto de ataques dados en contra de este. La base de datos usada para revisar, puede ser modificada fácilmente para suministrar nueva información.

`Bass` (Bulk Auditing Security Scanner) [1] y `Satan` (Security Auditing Tool for Analysing Networks)[2] deben ser pensados más como programas de "conceptos de prueba" que como herramientas que serán usadas mientras se ejecutan las auditorías. Ambos son absolutamente antiguos y no se mantienen hasta la fecha. Sin embargo,SATAN fue la primera herramienta para el suministro de una evaluación de vulnerabilidad que una simple herramienta (GUI) y Bass se mantiene como una herramienta de evaluación de alto desempeño.

8.2. Herramientas de revisión de redes

Debian suministra algunas herramientas usadas para revisiones de servidores remotos (pero sin evaluación de vulnerabilidad). Estas herramientas son, en algunos casos, usadas por revisores de evaluación de vulnerabilidades como el primer tipo de ataque que corre en contra de los servidores remotos que intentan determinar los servidores remotos disponibles. Actualmente Debian suministra:

- nmap
- xprobe
- queso
- knocker
- hping2
- isic
- icmpush
- nbtscan

Mientras `queso`y `xprobe` suministran únicamente detección remota de sistemas operativos.(usando revisión de huellas TCP/IP) `nmap` y `knocker` pueden detectar el sistema operativo de detención y pueden revisar puertos de servidores remotos. De otro lado `hping2` y `icmpush` pueden ser usados para técnicas remotas de ataque ICMP.

Diseñado específicamente para redes Netbios, `nbtscan` puede ser usados para revisar redes IP y para traer informacióne de nombres desde los servidores de SMB, incluyendo nombres de usuario, nombres de red, direcciones MAC...

[1] N.T. : Revisor en masa de Auditoría de seguridad
[2] N.T.:herramientas de seguridad de auditoría para analisis de redes

8.3. Auditorías internas

Actualmente, solamente la herramienta `tiger` es usada en Debian para ejecutar auditorias internas (también llamadas white box) del servidor para determinar si el sistema de archivos son montados apropiadamente, cuyos procesos están escuchando en el servidor, etc.

8.4. Auditoría de códigos fuente

Debian suministra dos paquetes que pueden ser usados para auditar programas escritos en C/C++ y encuentran errores de programación que pueden conducir a fallas potenciales de seguridad.

- flawfinder
- rats

8.5. Redes privadas virtuales

ARREGLAME:Contenido necesario

Debian suministra bastantes paquetes para montar redes virtuales privadas encriptadas:

- `vtun`
- `tunnelv`
- `cipe`
- `vpnd`
- `tinc`
- `secvpn`
- `pptp`
- `freeswan`

IPsec (i.e. FreeSWAN)es probablemente la mejor opción dado que esta promete interoperar con más que cualquiera otra que use IPsec, pero estos otros paquetes pueden ayudarlo a tener un tunel seguro en un momento de prisa. PPTP es un protocolo de Microsoft para VPN. Este es soportado bajo Linux, pero se conoce que tiene serios problemas de seguridad.

para más información dirígase a VPN-Masquerade HOWTO (`http://www.linuxdoc.org/HOWTO/VPN-Masquerade-HOWTO.html`) (cubre IPsec y PPTP) VPN HOWTO (`http://www.linuxdoc.org/HOWTO/VPN-HOWTO.html`) (cubre PPP sobre SSH), y Cipe mini-HOWTO (`http://www.linuxdoc.org/HOWTO/mini/Cipe+Masq.html`), PPP and SSH mini-HOWTO (`http://www.linuxdoc.org/HOWTO/mini/ppp-ssh/index.html`).

8.6. Public Key Infrastructure (PKI). Infraestructura de claves públicas

Cuando se considera un PKI usted está confrontandolo con una amplia variedad de herramientas:

- Un Autoridad de certificados que puede distribuir certificados y puede trabajar bajo una jerarquia dada.
- Un directorio para apoyar los certificados de los usuarios públicos.
- Una base de datos (?) para mantener listas de certificados revocados.
- Dispositivos que pueden operar con CA para mantener smartcards/usb tokens/o lo que sea para almacenar certificados seguramente.
- Aplicaciones que tienen en cuenta los certificados dados que pueden certificarse por un CA para llevar a cabo una comunicación encriptada y revisar certificados dados contra CRL (para la autenticación y soluciones de firma completa sencilla).
- Un reloj fechador que autoriza firmar los documentos digitalmente.
- Una consola de administración desde el cual todos pueden ser usados apropiadamente (certificado de generación, lista de control de revocación, etc.).

Usted puede usar algunos de los programas disponibles en Debian GNU/Linux que cubre algunas de sus herramientas, este incluye open SSL (para generación de certificados) Open LDAP (como un directorio para apoyar los certificados) soporte gnupg y freeswan (con x.509). Sin embargo, el sistema operativo no suministra (hasta la versión woody 3.0)cualquiera de los certificados libremente disponibles tales como pyCA, Open CA, OpenCA (`http://www.openca.org`) o los ejemplos de CA de OpenSSL. Para más información lea Open PKI book (`http://ospkibook.sourceforge.net/`).

8.7. Herramientas antivirus

No hay muchas herramientas de antivirus en Debian, probablemente por que los usuarios de GNU/Linux no son regularmente plagados por los virus. Este ha tenido, sin embargo, gusanos y virus para GNU/Linux incluso si no ha habido (aún esperanzadoramente) algún virus que se haya podido extender ampliamente sobre cualquier distribución de Debian. En cualquier caso, los administradores deben buscar abrir una salida de antivirus o protejerse contra ellos.

Debian actualmente suministra las siguientes herramientas para la construcción de ambientes de antivirus:

- sanitizer (`http://packages.debian.org/sanitizer`), una herramienta que puede ser usada para filtrar emails desde procmail y eliminar virus.

- amavis-postfix (http://packages.debian.org/amavis-postfix),un script que suministra una interfaz desde el agente de transporte de correo hacia uno o más revisores de virus (este paquete lo suministra la versión postfix).

Como usted puede ver, Debian no sumninistra actualmente ningún programa de antivirus por si mismo. Hay, sin embargo, proyectos libres de antivirus los cuales (en el futuro) podrían ser incluidos en Debianopenantivirus (http://sourceforge.net/projects/openantivirus/) (pocas oportunidades para este dado que está basado completamente en Java). Debian nunca suministrará software de antivirus comerciales como: jvirus (http://sourceforge.net/projects/jvirus/) Panda Antivirus (http://www.pandasoftware.com/com/linux/linux.asp), NAI Netshield (uvscan) (http://www.nai.com/naicommon/buy-try/try/products-evals.asp), Sophos Sweep (http://www.sophos.com/), TrendMicro Interscan (http://www.antivirus.com/products/), RAV (http://www.ravantivirus.com).... para mas enlaces vea Linux antivirus software mini-FAQ (http://www.computer-networking.de/~link/security/av-linux_e.txt).

Para más información sobre como montar un sistema detector de virus lea el artículo de Dave Jones construyendo un sistema detector de virus en su correo para su red. Building an E-mail Virus Detection System for Your Network (http://www.linuxjournal.com/article.php?sid=4882)

Capítulo 9

Antes del compromiso

9.1. Montar el descubrimiento de intrusión

Debian incluye algunas herramientas para detectar intrusiones, las cuales usted quisiera configurar para montar la defensa de su sistema local (si es verdaderamente paranoico o si su sistema es realmente crítico) o para defender otros sistemas en la misma red.

Siempre debe darse cuenta que para mejorar realmente el sistema de seguridad con la introducción de algunas de estas herramientas, usted necesitara tener un mecanismo de alerta+respuesta, pero no use el descubrimiento de intrusión si usted no va a alertar a nadie (i.e. no malgaste su tiempo configurando cosas que mas tarde no usara).

La maryoría de herramientas de descubrimiento de intrusión sera también registrada bajo syslog o enviará mensajes hacia el usuario root. (muchos de ellos pueden ser configurados para enviar correo a otros usuarios) con respecto al particualar ataque que ha sido detectado. Un administrador tiene que configurarlos apropiadamente, para que los falsos-positivos no envíen alertas y a las alertas también se tengan en cuenta apropiadamente. Las alertas pueden indicar un ataque en curso y puede no ser útil, por ejemplo, que un dia mas tarde, después del ataque exitoso este sea descubierto. Para estar seguro que una política es apropiada sobre la dirección de alertas y para que los mecanismos técnicos se puedan implementar y estén en su sitio.

Una interesante fuente de información es CERT's Intrusion Detection Checklist (`http://www.cert.org/tech_tips/intruder_detection_checklist.html`)

9.1.1. Detección de intrusos basadas en Red

`snort` es un flexible paquete de sniffer o logger el cual detecta ataques usando un ataque de asignatura. Este detecta una variedad de ataques y examinaciones, tales como buffer overflows, stealth pot scans, ataques CGI, examinaciones SMB y más. Snort tiene la capacidad de alertar en tiempo real. Esta es una herramienta la cual debe ser instalada sobre toda ruta para mantener un ojo sobre su red. Ya instalado `apt-get install snort`,siga las preguntas y obseve su registro.

Snort en Debian está habilitado con muchos chequeos de seguridad los cuales usted debe solicitar, sin embargo, usted debe personalizar el montaje para tomarlo dentro de las consideraciones de servicios particulares en donde usted avanza sobre su sistema. Usted también tiene que solicitarlo para recuperar los chequeos adicionales y asi especificar estos servicios.

Usted también puede usar ambos `snort` para establecer detención de red para un rango de servidor en su red como también detecta ataques de red sobre su propio servidor.

Hay otras herramientas que pueden ser usadas para detectar ataques de red (aunque mas simples). `Portsentry` es otro interesante paquete que puede sugerir su aislamiento cuando una examinación es hecha hacia su site. Otras herramientas como `ippl` `iplogger` también detectaran ataques de IP (TCP Y ICMP), igual que si ellos no suministraran técnicas avanzadas para la detención de ataques de red. (como lo hace snort).

Usted puede evaluar cualquiera de estas herramientas con el programa `idswakeup`, un generador falso-positivo que alerta los NIDSs con plenitud de considerar ataques comunes disponibles en Debian.

9.1.2. Servidores basados en la detención

`Tiger` es una vieja herramienta de intrusión de detención la cual ha sido soportada por Debian desde la distribución de woody. Tiger suministra la forma de revisar asuntos comunes relatados para los rompimientos de seguridad, passwords, problemas en archivos del sistema, procesos de comunicación ... La versión de Debian incluye nueva seguridad específica para Debian: MDSsums da suministros binarios y también revisa los ya instalados y los paquetes vulnerables. La falta de instalación hace que `tiger` avance cada día y génere un reporte el cual es enviadao hacia el super usuario. Los reportes generados pueden darse a través de la información de un cuidadoso compromiso del sistema.

Hay también un número de registros de auditorias de herramientas, en el site, como logcheck. Estas herramientas pueden ser absolutamente usables si se garantiza propiamente para alertar al administrador sobre eventos inusuales en el sistema de archivos locales. `logcheck`. pude ser enteramente garantizado, pude enviar mensajes desde eventos recuperados y desde los registros que son meritorios de atención. El abandono de instalación incluye perfiles para eventos ignorados y violaciones políticas para tres diferentes montajes (estación de trabajo, servidor y paranoia). Los paquetes de Debian incluyen un archivo de configuración `/etc/logcheck/logcheck.conf`, dirigido por el programa, que define al usuario y que también revisa sus envios. También suministra una forma de paquete que provee servicios para implementar nuevas políticas en los directorios: `/etc/logcheck/hacking.d/_packagename_`, `/etc/logcheck/violations.d/_packagename_`, `/etc/logcheck/violations.ignore.d/_packagename_`, `/etc/logcheck/ignore.d.paranoid/_packagename_`, `/etc/logcheck/ignore.d.server/_packagename_`, and `/etc/logcheck/ignore.d.workstation/_packagename_`. Sin embargo, no muchos paquetes lo hacen actualmente. Si usted tiene una política que puede ser útil para otros usuarios , por favor envielo como un pequeño reporte para los paquetes apropiados, mire mas información en `/usr/share/doc/logcheck/README.Debian`

también algunos de los chequeadores de archivo de sistemaintegrados (mire en 'Integridad de

su sistema de archivos' en la página 49) puede ser absolutamenetutil para montar la detención de anomalias en un medio asegurado. Unaintrusión efectiva, muy seguramente, modificara los archivos en el sistema de archivos locales en orden para salvar las políticas de seguridad local. Instala troyanos, crea usuarios... Este evento puede ser detectado con ellos.

9.2. Parches útiles del núcleo

ARREGLAME: Las secciones necesitan como cubrir los parches específicos que pueden ser instalados en Debian usando el paquete del kernel-2.x.x-patch-XXX.

Hay algunos parches de núcleos, las cuales incrementan significativamente los sistemas de seguridad. Aqui hay algunos de ellos:

- OpenWall patch de Solar Designer. Ésta es una serie útil de restricciones de parches, como enlaces, FIFOs in `/tmp`, restringidos `/proc`,un archivo manejado por descriptor especial, sin el área de un grupo de usarios y otros mas. homepage:`http://www.openwall.com/linux/`
- *LIDS — Intrusión de detención del sistema Linux por Huagang Xie & Philippe Biondi*. Este parche hace que el proceso duro de creación de Linux sea mas fácil. Usted puede restringir todos los procesos, dar lo adecuado para escrbir o leer archivos, o remover, por fallas, y para tener la habilidad de leer archivos. Además usted también puede capacitarlos para procesos certeros. Aunque este permenece en la fase beta, este es casi uno de los sistemas de administrador paranoico. The Homepage: `http://www.lids.org`
- *POSIX Control a acceso de listas. Access Control Lists (ACLs) para Linux* este parche se suma al control de acceso de listas, un avanzado metodo para restringir accso de listas, hacia el núcleo de Linux Homepage: `http://acl.bestbits.at/`
- *Consejo de administrador en linux*. Este parche se suma al decente avance de permisos del sitema para su núcleo de Linux. Todos los objetos son surtidos en la memoria del núcleo. Homepage: `http://trustees.sourceforge.net/`
- *Parches internacionales del núcleo*. Ésta es una cripta orientada a los parches del núcleo. Ademas usted tiene que prestar atención a sus leyes locales con respecto al uso de la criptografia. Basicamente se suma la posibilidad de usar sistemas de archivos encriptados. Homepage: `http://www.kerneli.org`
- *SubDomain*. Es una extención del núcleo para crear mas seguridad y fácilidades para montar chroot en su medio. Usted puede especificar los archivos necesarios para el servicio manual de chrooted y para no compilar los servicios estaticamente. Homepage: `http://www.immunix.org/subdomain.html`
- *UserIPAcct*. Este no es realmente un parche de seguridad relatado, pero le permite crear cuotas para el tráfico sobre su servidor por usuario. Y usted puede traer estadisticas acerca del tráfico del usuario. Homepage: `http://ramses.smeyers.be/useripacct`.

- *FreeS/WAN*. Si usted quiere usar IPSec con Linux usted necesita este parche. Usted puede crear VPNs con esta facilidad, igual para las máquinas de windows, como IPSsec el cual es un estandard común. Homepage: `http://www.freeswan.org`

9.3. Evitando rootkits

9.3.1. LKM - Loadable Kernel Modules (módulos cargables en el núcleo)

LKM (Loadable Kernel Modules) son archivos que contienen dinamicamente modulos caragables del núcleo. Ellos son dinámicamente cargables en el núcleo para avanzar en tareas asignadas. SobreGNU/Linux son usadas para expandir la funcionalidad del núcleo. se pueden tomar grandes ventajas usando LKMs, como habiamos dicho, ellospueden ser dinamicamente cargables sin la recopilación del núcleo total, puede ser usado para especificar dispositivos de drivers (o archivos del sistema) y otros drives de hardware como tarjetas de sonido, tarjetas de red. Pero algunos crackers deben usar LKMs para rootkits (knark y adore) para instalar puertas traseras en los sistemas de GNU/Linux.

LKM rootkits pueden esconder procesos, archivos, directorio y las mismas conexiones sin modificar el origen de códigos binarios. Porejemplo, `ps` puede tomar procesos de información desde`/proc`, un malicioso LKM puede derrocar el núcleo paraesconder el proceso especifico desde procfs, pero no siempre una buenacopia de binarios `ps` deben alistar todos los procesos correctos de información.

9.3.2. Detector de rootkits.

El trabajo detector puede ser simple y doloroso, o difícil y agotador, depende de la medida que escoja. Hay dos medidas de defensa con respecto a la seguridad LKM, la proactiva y reactiva.

Defensa proactiva.

La ventaja de esta defensa es que previene algunos daños lkm rootkit del sistema. La defensa proactiva mas usada es “obteniendo el primero”, este está caragando un diseño LKM para proteger los daños de un sistema ocasionados por un diseño malicioso. Hay otra medida para eliminar las capacidades en el núcleo, haciendo el sistema mas seguro. Por ejemplo, usted remueve la capacidad para detener la carga y la descarga del módulo del núcleo.

Sobre el sistema de Debian usted puede encontrar algunos paquetes los cuales son una herramienta proactiva mas segura.

- `kernel-patch-2.4-lsm` - LSM son los modulos de seguridad de la estructura Linux.
- `lcap` - Remueve las capacidades en el núcleo, haciendo del sistema mas seguro.

Si usted realmente no necesita muchas caracteristicas del núcleo sobre su GNU/Linux usted tiene que solicitar modulos de soporte caragables incapacitados durante la configuración del núcleo. Este previene LKM rootkits, pero usted no debe usar las caracteristicas del modulo del núcleo sobre su GNU/Linux. Fijese que indiscapacitando los modulos caragables usted puede sobrecargar el núcleo, en ocasiones no es necesario.

Para indiscapacitar los modulos de soporte cargables, solo valla a CONFIG_MODULES=n on `.config`.

Defensa Reactiva.

La ventaja de la defensa reactiva es que tiene una sobrecarga en los recursos del sistema. Este trabaja comparando el sistema de llamadas tabulando con una copia limpia conocida en el archivo de un diskette. La mas obvia desventaja es llamada para el único administrador cuando el sistema no ha sido comprometido.

El detector de rootkits en Debian puede ser consumado con `chkrootkit`. Este programa revisa signos de rootkits sobre el sistema local y si el objetivo del computador es infectado con un rootkit.

Usted también puede usar SKAT (`http://s0ftpj.org/en/site.html`). SKAT revisa el area de memoria del núcleo a (`/dev/kmem`) para información acerca del objetivo del servidor, esta información incluye la instalación de modulos cargables del núcleo.

ARREGLAME: información adicional sobre como compilar el soporte del nrúucleo w/o lkm.

9.4. Ideas geniales/paranóicas — qué debe hacer

Ésta es probablemente la más inestable y divertida sección, ya que espero que algunas de de los "duh. ideas locas del sonido" puedan ser realizadas. Siguiendo aqui usted debera encontrar algunas ideas —esto depende del punto de vista en donde usted observe si ellos son genios, paranóicos, locos o si pueden dar una garantía — para incrementar su seguridad rápidamente usted no deberá venir y sacarlo ileso.

- Jugando alrededor con PAM. Como se dijo en el articulo phrack 56 PAM , lo agradable con PAM es que "usted está limitado únicamente por lo que pueda pensar" es verdad, imagine la raíz del inicio de sesión únicamente posible con revisión de impresión o eyescan o cryptocard (porque yo aqui hago una conjunción OR y no AND).
- Iniciación de sesión fascista. Yo diria que que todo lo que nosotros hemos hablado acerca de login es "un sueve inicio de sesión". si usted quiere ejecutar una sesión real, tome una impresora con papel fanfold y registre todo lo complicado para imprimir sobre el.Los sonidos divertidos, son confiables y no pueden ser removidos.
- Distribución de CD. Esta idea es muy fácil de realizar y ofrece muy buena seguridad. Crear una distribución de un endurecido Debian, con propias reglas de barrera, hace

imagenes ISO de este y surgen sobre un CD. lo hace iniciable. Ésta es una lectura única de distribución con cerca de 600 MB para servicios, y es imposible para introductores y asi poder empezar a leer/escribir el acceso sobre el sistema. Solo asegurese siempre de los datos los cuales deben escribirse sobre "wires". De todas formas, el introductor no puede cambiar las reglas de barreara, distribuyendo entrdas o iniciar propios demonios. (el tiene la capacidad, ya que reinicia y tiene que manejar su sitema de nuevo para cambiarlos)

- El Switch de capacidad del modulo apagado. Cuando desconecta el uso de modulos del núcleo en un tiempo compilado del núcleo, muchos núcleo se basan en puertas traseras imposibles para poder implementarlas, ya que muchos de ellos estan basados en la instalación de modulos modificados del núcleo.

- Entrando a través del cable serial (contribuido por Gaby Schilders). Dado que que los servidores aun tienen puertos en serie, imagínese tener una máquina de registro de bitácoras desconectada de su red en la mitad con un puerto serial multiplexor (antiquisimo o algo similar). Ahora todos sus servidores registrando a sus puertos seriales. Con sólo escritura. la máquina de registo únicamente acepta texto plano como entrada sobre sus puertos seriales y únicamente escribe en un archivo de registro. Enganche un cd/dvd writer. Cuando el registro del archivo está cerca de 600 MB lo copia al cd-rom. Ahora si pudieran hacer quemadoras con auto-cambiadores ... No copia tan dura como la impreosra, pero que puede manejar largos volúmenes y los cd no toman mucho espacio de almacenamiento.

- Haga que todo sea inmutable (tomado desde Tips-HOWTO, escrito por Jim Dennis). Despues de que usted instale y configure su sitema dirigase a través de `/bin`, `/sbin/`, `/usr /bin`, `/usr/sbin` y `/usr/lib` (y un poco de otros inusuales sospechosos) y hagalo en uso liberal de `chattr +i command`. también se suma en la raiz de archivos del núcleo. Ahora `mkdir /etc/.dist/` copia todo desde `/etc/` de la parte interior (Lo hago en dos pasos usando `/tmp/etcdist.tar` para evitar la recurrencia) dentro del directoro (opcionalmente usted puede crear `/etc/.dist.tar.gz`) y marquelo como inmutable.

  La razón para todo es limitar el daño que usted pueda ocasionar cuando se registyra como root. Usted no podra sobreescribir archivos con un desviado operador de redirecciones, usted no podra hacer del sitema algo inusual con un desviado espacio dentro de un comando `rm -fr` (usted puede permancer haciendo lo suficiente con los daños de sus datos —: pero sus libs y bins estaran seguros).

  Ésta también emplea una variedad de seguridad y rechazo de servicios de cualquier imposible explosión o algo de mayor dificultad (ya que muchos de ellos confian en sobre copiar archivos a través de las acciones de algun programa SUIDque *no suministra arbitrariamente una interfase de comandos*)

  El único inconveniente de este es cuando se construye y se hace su `make install` sobre varias clases de sistemas binarios. Sobre la otra mano también previene la instalación desde los archivos sobre escritos. Cuando usted olvida leer el Makefile y chattr -i los archivos que pueden ser sobre escritos fallan con el make (y los directorios para los cuales usted necesita para añadir archivos), usted solo use el comando chattr y regrese. Usted también puede tener la oportuinidad de mover sus viejos bins, libs o lo que sea dentro de un old/directory o puede renombrar, marcar o lo que sea.

Note que esto lo previene de hacer una actualización de los paquetes de su sistema. Dado que los archivos que ellos suministran no pueden ser sobre escritos, y usted debe tener un mecanismo para desactivar la bandera de inmutable sobre todos los binarios antes de un `apt-get update`.

9.4.1. Construyendo un equipo trampa

ARREGLAME. Mas contenido específico necesario para Debian

Si usted desea (y también puede implementarlo y dedicarle tiempo) usted puede mintar todo un equipo trampa (del inglés, *honeypot* [1]) usando un sistema de Debian GNU/Linux. Usted tiene todas las herramientas necesarias en orden para montar toda la red trampa (N.T. del inglés *honeynet*, el *honeypot* es sólo el servidor falso): el cortafuegos, los detectores de intrusión y el servidor falso. Sea cuidadoso. Sin embargo, tiene que estar bien seguro de que sea alertado a tiempo (vea "la importancia del registro y las alertas" en la pagina 36 'La importancia de logs y alarmas' en la página 41), usted debe tomar la medida apropiada y terminar el compromiso tan pronto como haya visto suficiente. Los siguientes paquetes le pueden ser de utilidad:

- la tecnología del cortafuegos usted la debera necesitar (suministrado por Linux Kernel).
- `syslog-ng` para enviar el registro desde el honeypot hacia una máquina de servidor remota.
- `snort` para montar la captura de todo la llegada del trafico de red para honeypot y para detectar ataques.
- `osh` el cual puede ser usado para montar una restricción de comandos de interfase con el inicio de sesión (mire el bajo Lnce Spitzener).
- Claro que si, todos los servidores para su falso servidor honeypot usted se los puede imaginar (pero no haga duro el *not* honeypot)).
- y también los falsos servicios, suministrados por `dtk` si usted necesita usar el honeypot también como un servicio de detección de intrusión.
- Chequeadores integrales (vea 'Integridad de su sistema de archivos' en la página 49) y los toolkit de Coroners y (`tct`) para hacer una auditoria de post ataque.

Usted puede leer más acerca de la construcción de honeypots en el excelente artículo de Lanze Spitzner para construir un honeypotTo Build a Honeypot (`http://www.net-security.org/text/articles/spitzner/honeypot.shtml`) (desde las serie conocidad de su enemigo), o la construcción de su propio honeypot de David Raikow Building your own honeypot (`http://www.zdnetindia.com/techzone/resources/security/stories/7601.htm`). también el proyecto de honeynet Honeynet Project (`http://project.honeynet.org/`) es dedicado para la construcción de honeypots y auditorias de ataques hechos para ellos, ésta es una información valios sobre como montar un honeypot y resultados de auditoría de un ataque (mire el concurso).

[1] N.T. es un equipo fácil de acceso el cual permite al acceso de crackers

Capítulo 10

Después del compromiso

10.1. Conducta general

Si usted se encuentra presente fisicamente cuando un ataque está sucediendo si al hacer lo siguiente, no afecta las transacciones de negocios, simplemente desconecte el NIC hasta que pueda descifrar lo que el intruso quiere hacer y asegure el computador,inhabilitando la capa uno de la red, es la única vía verdadera de mantener al atacante alejado del equipo comprometido (consejo prudente de Phillip Hofmeister).

Si realmente usted quiere arreglar el compromiso rápidamente, usted deberá eliminar el servidor comprometido de su red y reinstalar el sistema operativo desde el comienzo. Esto no debería tener ningún efecto si usted no sabe como el intruso se volvió root. En este caso, debe chequear todo: firewall/file integrity/loghost logfiles y así sucesivamente. Para más información sobre que hacer y seguir una intrusión, observe Sans'Incident Handling Guide (`http://www.sans.org/y2k/DDoS.htm`) o pasos del CERT para recuperarse de un compromiso en sistema UNIX o NT (`http://www.cert.org/tech_tips/root_compromise.html`).

10.2. Haciendo copias de seguridad del sistema

Recuerde que si usted está seguro de que el sistema ha sido comprometido, no puede confiarse del software o de alguna otra información que esté en ese momento. Las aplicaciones podrían haber sido troyanizadas, y módulos del kernel estar instalados, etc.

Lo mejor es sacar una copia completa de seguridad (usando `dd`) después de haberlo cargado desde un medio seguro. Los discos compactos de Debian GNU/Linux pueden ser usados correctamente por éste dado que ellos suministran a una interfaz de comandos en la consola 2 cuando la instalación haya iniciado (presione Alt 2 y luego Enter). La interfaz de comando puede ser usada para sacar una copia de seguridad a un lugar diferente (a lo mejor un servidor de archivos en red vía NFS/FTP ...) para hacer un análisis mientras el sistema está fuera de línea (o siendo reinstalado).

Si usted está seguro que solamente hay un módulo del kernel troyano, usted puede intentar lanzar la imagen del kernel desde el disco compacto en *modo* rescue. Asegúrese de iniciar en *modo* single o si no, de modo que otros procesos troyanos no correrán después del kernel.

10.3. Análisis forense

Si usted desea recopilar mas información, el `tct` (El juego de herramientas del instructor de Dan Farmer y Wietse Venema) contiene paquetes de utilidad que ejecuta un "post mortem" de un sistema. El `tct` permite al usuario recopilar información acerca de archivos borrados, procesadores en funcionamiento y más. Observe la documentación incluída para más información.

Los análisis forense siempre se deben hacer en la copia de seguridad de datos, *nunca* en los mismos datos, ya que estos podrían ser falsificados a través de este análisis (y perderse).

ARREGLAME. De este párrafo se espera que suministre mas información acerca de la legalidad en el sistema Debian en un futuro venidero.

ARREGLAME: hablar sobre como va a hacer un debsums en un sisema estable con el disco compacto md5sums, con la recuperación de un sistema de archivo restaurado en una distribución separada.

Capítulo 11

Preguntas Frecuentes

Este capítulo introduce algunas de las preguntas más comunes de la lista de seguridad de Debian. Debería leerlas antes de preguntar o la gente posiblemente le diga RTFM (N.T. Read The Fucking Manual - Lea el P*to Manual).

11.1. La seguridad en el sistema operativo Debian

11.1.1. ¿Es más seguro Debian que X?

Un sistema es sólo tan seguro como su administrador es capaz de hacerlo. La instalación predeterminada de Debian de servicios trata de ser *segura*, pero puede no ser tan paranoica como la de otros sistemas operativos que instalan todos los servicios *deshabilitados de manera predeterminada*. En cualquier caso, el administrador del sistema necesita adaptar la seguridad del sistema a su política de seguridad local. Para ver una recopilación de datos acerca de vulnerabilidades de seguridad de muchos sistemas operativos mire en `http://securityfocus.com/vulns/stats.shtml`. ¿Le son útiles estos datos? El servidor lista varios factores a considerar cuando se interpretan los datos y avisa de que los datos no pueden usarse para comparar las vulnerabilidades de un sistema operativo frente a otro.[1] Tenga también en mente que alguna de las vulnerabilidades de BugTraq que afectan a Debian se aplican sólo a la rama *unstable*.

¿Es Debian más segura que las otras distribuciones de Linux (como RedHat, SuSE...)?

No hay realmente muchas diferencias entre las distribuciones de Linux más allá de la instalación base y el sistema de gestión de paquetes. La mayoría de las distribuciones comparten las mismas aplicaciones con diferencias fundamentalmente en las versiones de esas aplicaciones que se distribuyen en esa distribución estable. por ejemplo, el núcleo, Bind, Apache, OpenSSH, XFree, gcc, zlib, etc, todas son comunes en las distribuciones Linux.

[1] Por ejemplo, teniendo en cuenta los datos de Securityfocus, puede parecer que Windows NT es más seguro que Linux, lo que es una afirmación cuestionable. Después de todo, las distribuciones de Linux proporcionan habitualmente muchas más aplicaciones comparadas con Windows NT de Microsoft.

Por ejemplo, RedHat se distribuyó desafortunadamente cuando era actual la versión 1.2.3 de foo en la que más tarde se encontró un agujero de seguridad. Debian, por otro lado, tuvo la suerte de distribuir foo 1.2.4 que incorporaba el parche al fallo. Ese fue el caso en el problema con rpc.statd (`http://www.cert.org/advisories/CA-2000-17.html`) Hace varios años.

Hay mucha colaboración entre los equipos de seguridad de las distribuciones de Linux más grandes. Las actualizaciones de seguridad raramente se dejan sin actualizar en una distribución. El conocimiento acerca de una vulnerabilidad nunca se esconde a otras distribuciones así que los arreglos se suelen hacer coordinados, o por el CERT (`http://cert.org`). Como resultado, las actualizaciones de seguridad necesarias suelen liberarse al mismo tiempo y la seguridad relativa entre las diferentes distribuciones es muy similar.

Una de las mayores ventajas de Debian en relación a la seguridad es la facilidad del sistema de actualización a través de del uso de `apt`. Aquí hay algún otro aspecto a considerar acerca de la seguridad de Debian:

- Debian proporciona más herramientas de seguridad que otras distribuciones, mire en 'Herramientas de seguridad en Debian' en la página 79.
- La instalación estándar de Debian es más pequeña (con menos funcionalidad) y por lo tanto más segura. Otras distribuciones, en favor de la usabilidad, tienden a instalar muchos servicios demanera predeterminada y algunas veces, no están bien configurados (recuerde los gusanos Ramen o Lion (`http://www.sans.org/y2k/lion.htm`)). La instalación de Debian no está tan limitada como OpenBSD (donde no hay demonios activados de forma predeterminada), pero es un buen compromiso. [2]
- Debian documenta las mejores prácticas de seguridad en documentos como este.

11.1.2. Hay muchos errores de Debian en Bugtraq. ¿Significa eso que es muy vulnerable?

La distribución Debian contiene un gran y creciente número de paquetes de programas y probablemente más que los proporcionados por muchos sistemas operativos propietarios. Cuantos más paquetes se instalen, mayor será el riesgo potencial de tener problemas de seguridad para un sistema dado.

Más y más personas están examinando el código fuente en busca de debilidades. Hay muchos avisos acerca de auditorías del código fuente de los componentes más importantes de Debian. Cuando esas auditorías de código fuente descubren vulnerabilidades, se solucionan y se envía un aviso a las listas y a Bugtraq.

Los errores que están presentes en la distribución Debian tambien afectan habitualmente a otros fabricantes y distribuciones. Revise la sección "Debian specific: yes/no" al comienzo de cada aviso DSA).

[2] Sin descontar el hecho de que algunas distribuciones como RedHat o Mandrake, están tomando en serio la seguridad de sus instalaciones predeterminadas haciendo que el usuario seleccione *perfiles de seguridad*, o mediante asistentes para ayudar en la configuración de *cortafuegos personales*.

11.1.3. ¿Tiene Debian alguna certificación relacionada con la seguridad?

Respuesta corta: no.

Respuesta larga: las certificaciones cuestan dinero y nadie ha dedicado los recursos para certificar a Debian GNU/Linux a ningún nivel de, por ejemplo, el "Common Criteria". Si está interesado en obtener una distribución certificada, pruebe a proporcionar los recursos para que ello sea posible.

11.1.4. ¿Hay algún programa de securización para Debian?

Sí. Bastille Linux (`http://www.bastille-linux.org`), originalmente orientado hacia otras distribuciones de Linux (RedHat y Mandrake), actualmente funciona para Debian. Los pasos están siendo tomados para integrar los cambios hechos a la versión original al paquete Debian llamado `bastille`.

Sin embargo, algunas personas creen que una herramienta de securización no elimina la necesidad de una buena administración.

11.1.5. Quiero ejecutar el servicio XYZ, ¿cuál debería elegir?

Una de las mayores fortalezas de Debian es la gran variedad de elecciones posibles entre paquetes que proporcionan la misma funcionalidad (servidores de DNS, servidores de correo, servidores de FTP, servidores WEB, etc.). Eso puede resultar confuso para el administrador novel al tratar de determinar que paquete es el adecuado. La mejor opción para una situación concreta se basa en el compromiso entre su funcionalidad y los requerimientos de seguridad. Hay algunas preguntas que debe contestar antes de decidir entre paquetes similares:

- ¿Se mantiene el programa original? Cuando fué su última versión?
- ¿Está el paquete maduro? El número de versión realmente *no* no informa acerca de su madurez. Trate de indagar acerca de la historia del programa.
- ¿Está el programa libre de errores? ¿Han salido avisos de seguridad relacionados con él?
- ¿Proporciona el programa todas las funcionalidades que necesita? ¿Proporciona más de lo que realmente necesita?

11.1.6. ¿Cómo puedo hacer el servicio XYZ más seguro en Debian?

Puede encontrar información en este documento acerca de cómo hacer algunos servicios (FTP, Bind) más seguros en Debian GNU/Linux. Para los servicios que no se cubran aquí, mire la documentación del programa o información general sobre Linux. La mayoría de las guías de seguridad para sistemas Unix también se aplican a Debian. En la mayoría de los casos, securizar un servicio X en Debian es como securizar ese mismo servicio en cualquier otra distribución de Linux (o Un*x).

11.1.7. ¿Cómo puedo eliminar todos los mensajes de los servidores?

Si no le gusta que los usuarios se conecten a su servidor POP4, por ejemplo, y obtengan información sobre sus sitema, puede querer eliminar (o cambiar) el mensaje que los servidores muestran a los usuarios. [3] El hacer eso depende del programa que esté ejecutando para un servicio determinado. Por ejemplo, en `postfix`, puede configurar el mensaje de SMTP en `/etc/postfix/main.cf`:

```
smtpd_banner = $myhostname ESMTP $mail_name (Debian/GNU)
```

Otros programas no son tan fáciles de cambiar. `OpenSSH` tiene que ser recompilado para poderse cambiar la versión que muestra. Tenga cuidado con no eliminar la primera parte (`SSH-2.0`) del mensaje, que muchos clientes usan para identificar qué protocolo(s) soporta su paquete.

11.1.8. ¿Son seguros todos los paquetes de Debian?

El equipo de seguridad de Debian no puede analizar posiblemente todos los paquetes incluidos en Debian en busca de vulnerabilidades potenciales porque simplemente, no tienen recursos suficientes para auditar todo el código fuente del proyecto. De todas formas Debian se beneficia de la auditoría de código hecha por los desarrolladores de los proyectos originales y de otros proyectos como Proyecto de auditoría de seguridad del kernel de Linux (`http://kernel-audit.sourceforge.net/`), o el Proyecto de auditoría de seguridad de Linux (`http://www.lsap.org/`).

De todas formas un desarrollador Debian podría distribuir un troyano en un paquete y no habría forma posible de comprobarlo. Incluso si se introduce en una rama de Debian, podría ser imposible cubrir todas las posibles situaciones en las que un troyano puede ejecutarse. Esa es la razón por la que Debian tiene una cláusula de *"no garantías"* en su licencia.

Aun así, los usuarios de Debian tiene confianza en el hecho de que el código estable tiene una gran audiencia y la mayoría de los problemas pueden descubrirse con el uso. Instalar programas no probados no es recomendable en un sistema crítico (si no puede hacer la auditoría de código necesaria). En cualquier caso, si se introduce una vulnerabilidad de seguridad en una distribución, el proceso que se usa para incluir paquetes (usando firma digital) asegura que el problema puede seguirse hasta el desarrollador. El proyecto Debian no se ha tomado a la ligera este tema.

11.1.9. ¿Por qué algunos archivos de registro/configuración tienen permiso de lectura para todos? ¿No es eso inseguro?

Por supuesto que puede cambiar los permisos predeterminados de Debian en sus sistemas. La política actual acerca de los archivos de registro y configuración es que tienen permisos de lectura para todos *salvo* que tengan información sensible.

Sea cuidadoso si hace cambios porque:

[3] Dese cuenta que eso es 'seguridad por oscuridad', y que probablemente no tenga un buen efecto a largo plazo.

- Los procesos pueden no ser capaces de escribir en los archivos de registro si restringe los permisos.
- Algunas aplicaciones pueden no funcionar si no pueden leer el archivo de configuración. Por ejemplo, si elimina los permisos de lectura para todos de `/etc/samba/smb.conf`, el programa `smbclient` no funcionará cuando lo ejecute un usuario normal.

ARREGLAME: Comprobar si esto está escrito en la Política. Algunos paquetes (p.e. demonios ftp) parece que usan permisos diferentes.

11.1.10. ¿Por qué /root/ (o usuarioX) tiene permisos 755?

La mismas preguntas, de hecho, se aplican a cualquier otro usuario. Como la instalación de Debian no pone *ningún* archivo en ese directorio, no hay información sensible que proteger. Si piensa que esos permisos son demasiado permisivos para su sistema, considere en asegurarlos a 750. Para los usuarios lea 'Limitando el acceso a la información de otros usuarios' en la página 40.

Este hilo de discusión (`http://lists.debian.org/debian-devel/2000/debian-devel-200011/msg00783.html`) de la lista de seguridad de Debian tiene más información acerca de ésto.

11.1.11. ¡Tras instalar un grsec/cortafuegos he empezado a recibir muchos mensajes de consola! ¿Cómo puedo eliminarlos?

Si está recibiendo mensajes de consola y tiene configurado `/etc/syslog.conf` para enviarlos a archivos o a un TTY especial, puede estar viendo los mensajes que se envían directamente a la consola.

El nivel de log predeterminado de la consola para cualquier núcleo es 7, lo que significa que cualquier mensaje con una prioridad menor aparecerá en la consola. Habitualmente, los cortafuegos (la regla LOG) y algunas otras herramientas de seguridad usan prioridades menores, que por lo tanto, se envían directamente a la consola.

Para reducir los mensajes que se envían a la consola puede usar la opción `dmesg` (`-n`, mire `dmesg(8)`), que examina y *controla* el anillo del buffer del kernel. Para solucionar esto en el próximo inicio, cambie `/etc/init.d/klogd` de:

```
KLOGD=""
```

a:

```
KLOGD="-c 4"
```

Use un número menor en `-c` si aun así los ve. Puede encontrar una descripción de los diferentes niveles de log en `/usr/include/sys/syslog.h`:

```
#define LOG_EMERG       0       /* sistema no usable */
#define LOG_ALERT       1       /* se debe actuar inmediatamente */
#define LOG_CRIT        2       /* condiciones críticas */
#define LOG_ERR         3       /* condición de error */
#define LOG_WARNING     4       /* condición de aviso */
#define LOG_NOTICE      5       /* condiciones normales pero significativas
#define LOG_INFO        6       /* informativo */
#define LOG_DEBUG       7       /* mensajes de depuración */
```

11.1.12. Usuarios y grupos del sistema operativo

¿Son necesarios todos los usuarios del sistema?

Si y no. Debian viene con algunos usuarios predeterminados (id de usuario (UID) < 99 como está descrito en la Política de Debian (`http://www.debian.org/doc/debian-policy/`) o `/usr/share/doc/base-passwd/README`) para facilitar la instalación de algunos servicios que requieren que se ejecute bajo el usuario/UID adecuado. Si no tiene intención de instalar nuevos servicios puede eliminar los usuarios que no tengan ningún archivo en su sistema y no ejecuten ningún servicio tranquilamente. En cualquier caso, el comportamiento predeterminado es que los UIDs del 0 al 99 se reservan en Debian y los UIDs del 100 al 999 se crean por los paquetes cuando se instalan (y se eliminan cuando el paquete se elimina completamente).

Para encontrar fácilmente los usuarios que no tienen ningún archivo ejecute el comando (como root ya que un usuario común puede no tener permisos para ir por algunos directorios sensibles):

```
cut -f 1 -d : /etc/passwd | \
while read i; do find / -user "$i" | grep -q . && echo "$i"; done
```

Estos usuarios son del paquete `base-passwd`. Mire en su documentación si quiere más información acerca de cómo se gestionan estos usuarios en Debian. La lista de usuarios predeterminados (con su grupo correspondiente) es la siguiente:

- root: Root es (típicamente) el super usuario.
- daemon: Algunos demonios sin privilegios que necesitan escribir en archivos del del disco se ejecutan como daemon.daemon (p.e., `portmap`, `atd`, y probablemente otros). Los demonios que no necesitan tener ningún archivo corren como nobody.nogroup, algunos otros demonios más complejos se ejecutan con usuarios dedicados. El usuario del demonio es también útil para demonios instalados localmente.
- bin: mantenido por razones históricas.
- sys: igual que bin. Aun así, /dev/vcs* y `/var/spool/cups` son del usuario y grupo sys.

- sync: La shell del usuario sync es `/bin/sync`. Aun así si su contraseña se pone fácil de adivinar (como “”), cualquiera puede sincronizar el sistema en la consola incluso si no tiene cuenta.
- games: Muchos juegos tienen SETGID de manera que puedan escribir sus propios archivos de puntuación más alta. Se explica en la política.
- man: El programa man (a veces) se ejecuta con el usuario man, para que pueda escribir páginas en `/var/cache/man`.
- lp: Usado por los demonios de impresión.
- mail: los buzones de `/var/mail` son del grupo mail, como se explica en la política. El usuario y grupo se usan también con otros propósitos por varios MTAs.
- news: Varios servidores de noticias y programas asociados (como `suck`) usan el usuario y grupo news de varias formas. Los archivos en la cola news son habitualmente del usuario y grupo news. Programas como `inews` que pueden usarse para enviar noticias son típicamente noticias con SETGID.
- uucp: El usuario y grupo uucp es usado por el subsistema UUCP. Tiene su propia cola y archivos de configuración. Los usuarios en el grupo uucp pueden ejecutar uucico.
- proxy: Como daemon, este usuario y grupo lo usan algunos demonios (especialmente demonios de proxy) que no tienen usuarios dedicados y necesitan tener archivos. Por ejemplo el grupo proxy lo usan `pdnsd`, y `squid`.
- majordom: `Majordomo` tiene un UID estático en sistemas Debian por razones históricas. No se instala en sistemas nuevos.
- postgres: Las bases de datos de `Postgresql` son de este usuario y grupo. Todos los archvos de `/var/lib/postgresql` son de este usuario para reforzar la seguridad.
- www-data: Algunos servidores web corren como www-data. El contenido *no* debe ser de este usuario o un servidor comprometido podría reescribir el web. Los datos escritos por el servidor web incluyendo los archivos de registro, deben ser de www-data.
- backup: Muchas funciones de copia/restauración pueden ser delegadas a alguien sin privilegios completos de root.
- operator: Operator es históricamente (y prácticamente) el único ’usuario’ que puede acceder al sistema de forma remota y no depende de NIS/NFS.
- list: Los archivos de listas de correo y sus datos son de este usuario y grupo. Algunos programas de listas de correo pueden ejecutarse también con este usuario.
- irc: Usado por demonios de IRC. Un usuario determinado se necesita únicamente por un error de `ircd`, que hace SETUID()s de si mismo a un UID determinado en el arranque.
- gnats.

- nobody, nogroup: Los demonios que no necesitan ningún archivo se ejecutan con el usuario nobody y grupo nogroup. Así que no debería existir ningún archivo de este usuario o grupo en el sistema.

Otros grupos que no tienen un usuario asociado:

- adm: El grupo adm se usa para tareas de monitorización del sistema. Los miembros de este grupo pueden leer muchos de los archivos de `/var/log`, y pueden usar xconsole. Históricamente `/var/log` eran `/usr/adm` (y más tarde `/var/adm`), del mismo grupo.
- tty: Los dispositivos TTY son de este grupo. Lo usan write y wall para escribir en los TTYs de otras personas.
- disk: Acceso directo a disco. Mayormente equivalente al acceso de root.
- kmem: /dev/kmem y archivos similares son accesibles en modo lectura por este grupo. Esto es, mayormente, una reliquia de BSD pero algunos programas siguen necesitando acceso directo de lectura a la memoria del sistema que se hace con SETGID kmem.
- dialout: Acceso directo y completo a los puertos serie. Los miembros de este grupo pueden reconfigurar el módem, llamar a cualquier parte, etc.
- dip: El nombre del grupo viene de "Dial-up IP", y ser de ese grupo le permite usar herramientas como `ppp`, `dip`, `wvdial`, etc. para comenzar una conexión. La mayoría de los usuarios de este grupo no pueden configurar el módem, pero pueden ejecutar programas que lo usa.
- fax: Permite a los miembros usar el programa de fax para enviar / recibir faxes.
- voice: Voicemail, usado por sistemas que usan módems como contestadores.
- cdrom: Este grupo puede ser usado localmente para dar acceso al CDROM a los usuarios.
- floppy: Este grupo puede ser usado localmente para dar acceso a la disquetera a los usuarios.
- tape: Este grupo puede ser usado localmente para dar acceso a la cinta a los usuarios.
- sudo: Los miembros de este grupo no necesitan teclear la contraseña cuando usen el programa `sudo`. Mire `/usr/share/doc/sudo/OPTIONS`.
- audio: Este grupo puede ser usado localmente para dar acceso a los usuarios al dispositivo de audio.
- src: Este grupo tiene el código fuente incluyendo los archivos de `/usr/src`. Puede usarse para darle al usuario la capacidad de gestionar el sistema de código fuente.
- shadow: `/etc/shadow` es de lectura para este grupo. Algunos programas que necesitan acceso a este archivo tienen SETGID shadow.

- utmp: Este grupo puede escribir en `/var/run/utmp` y archivos similares. Los programas que necesitan escribir ahí tienen SETGID utmp.
- video: Este grupo puede ser usado para dar a los usuarios acceso al dispositivo de video.
- staff: Permite a los usuarios añadir modificaciones locales al sistema (`/usr/local`, `/home`) sin necesidad de tener privilegios de root. Comparar con el grupo "adm", que está más relacionado con monitorización/seguridad.
- users: Mientras los sistemas Debian usan el sistema de usuarios privados de forma predeterminada (cada usuario tiene su propio grupo), algunos prefieren un sistema de grupos más tradicional, en el que cada usuario es miembro de este grupo.

¿Qué diferencia hay entre el grupo adm y el staff?

El grupo 'adm' son habitualmente administradores y los permisos de este grupo permiten leer los archivos de registro son tener que usar `su`. El grupo 'staff' es útil en soporte, administradores junior porque les permite trabajar en `/usr/local` y crear directorios en `/home`.

11.1.13. ¿Por qué se crea un nuevo grupo cuando añado un nuevo usuario? (O ¿Por qué Debian crea un grupo para cada usuario?)

El comportamiento predeterminado de Debian consiste en que cada usuario tiene su grupo privado. El esquema tradicional de UN*X asigna todos los usuarios al grupo *users*. Los grupos adicionales se creaban y se usaban para restringir el acceso a los archivos compartidos asociados a directorios de proyectos diferentes. La gestión de archivos era difícil cuando un usuario trabajaba en múltiples proyectos porque cuando alguien creaba un archivo, este se asociaba al grupo principal al que perteneciera (ej. 'users').

El esquema de Debian soluciona este problema asignando a cada usuario su propio grupo; así que con la máscara adecuada (0002) y el bit SETGID habilitado en un directorio dado, el grupo correcto se asigna adecuadamente para los archivos creados en ese directorio. Eso hace más fácil para la gente que trabaja en múltiples proyectos porque no tienen que cambiar grupos o umasks cuando trabajan o comparten archivos.

Puede, como siempre, cambiar este comportamiento modificando `/etc/adduser.conf`. Cambiar la variable *USERGROUPS* a 'no', de tal forma que no se cree un grupo cuando se cree un usuario. También poner *USERS_GID* al GID del grupo de usuarios al que pertenecerán los usuarios.

11.1.14. Preguntas acerca de servicios y accesos abiertos

¿Por qué están todos los servicios activados tras la instalación?

Es una aproximación al problema de, por una parte la seguridad y por otra la usabilidad. Al contrario que como OpenBSD, deshabilita los servicios a no ser que los habilite el administrador, Debian GNU/Linux habilitará todos los servicios instalados a no ser que se desactiven

(mire en 'Deshabilitar los demonios' en la página 23 para ver más información). Después de todo usted instaló el servicio ¿no es así?

Han habido muchas discusiones con las listas del correo en Debian (las dos, Debian-devel y debian-security) acerca de cual sería una mejor aproximación en la instalación predeterminada. Sin embargo, mientras se escribía este documento (marzo 2002) no se ha alcanzado un consenso.

¿Puedo eliminar inetd?

`Inetd` no es fácil de eliminar porque `netbase` depende del paquete que lo provee (`netkit-inetd`). Si quiere deshabilitarlo (mire 'Deshabilitar los demonios' en la página 23 o elimine el paquete usando el paquete `equivs`).

¿Por qué tengo abierto el puerto 111?

El puerto 111 es el portmapper de sunrpc y se instala de manera predeterminada como parte del sistema base de Debian porque no se sabe cuando un programa de usuario necesitará usar RPC para funcionar correctamente. En cualquier caso, se usa mayormente en NFS. Si no lo necesita, elimínelo tal y como se explica en 'Desactivar los servicios RPC' en la página 63.

¿Cual es el uso de `identd` (puerto 113)?

El servicio identd es un servicio de autenticación que identifica al usuario de una conexión TCP/IP concreta al servidor remoto que acepta la conexión. Típicamente cuando un usuario se conecta a un servidor remoto, `inetd` del servidor remoto le manda de vuelta una consulta al puerto 113 para encontrar la información del usuario. Esto se usa habitualmente en servidores de correo, FTP e IRC, también puede usarse para conocer qué usuarios de sus sistema local están atacando un sistema remoto.

Han habido discusiones extensas acerca de la seguridad de `identd` (mire los archivos de las listas de correo (`http://lists.debian.org/debian-security/2001/debian-security-200108/msg00297.html`)). Por lo general, `identd` es más útil en un sistema multi-usuario que en una estación de trabajo de un sólo usuario. Si no tiene por qué usarlo, deshabilítelo de tal forma que no deje un servicio abierto para el resto del mundo. Si decide cerrar con el cortafuegos el puerto identd, *por favor* hágalo usando una política de rechazo (reject) en vez de ignorar (drop) los paquetes, de otra forma la conexión al servidor que usa `identd` tendrá que expirar y se colgará hasta que lo haga (mire rechazar o ignorar (`http://logi.cc/linux/reject_or_deny.php3`)).

¿Yo he chequeado y tengo el siguiente acceso (xyz) y puedo cerrarlo?

Por supuesto que puede, usted puede ir dejando los portales abiertos en su sitio de política, fortaleciendo los servicios públicos disponibles para otros sistemas. Revise si estos son abiertos por inetd (observe 'Deshabilitar los servicios inetd' en la página 25) o por otros paquetes

instalados y tómelo en medidas apropiadas (configure inetd, remueva el paquete, anule el funcionamiento en bootup...).

¿He removido los servicios desde `/etc/services`,estoy en lo cierto?

No, `/etc/services` solo suministra un mapping desde un nombre virtual a un acceso numérico dado, removiendo nombres desde (usualmente) donde no haya que impedir servicios al ser iniciados. Algunos demonios no podrán funcionar si `/etc/services` ha sido modificado, pero ésta no es la norma y no es la vía recomendable para hacerlo, observe 'Deshabilitar los demonios' en la página 23.

11.1.15. ¡¡He perdido mi password y no puedo tener acceso al sistema!!

Usted necesita seguir unos pasos para recuperar su password y este depende desi usted ha aplicado o no el procedimiento para limitar el acceso a Lilo y BIOS.

Si usted ha limitado a ambos. Necesita desactivar las características de BIOS (hágalo solo desde el disco duro) antes de proceder, además, si usted olvida el password de BIOS, tendrá que abrir el sistema y eliminar la batería BIOS manualmente.

Si usted tiene un bootup en la unidad de cd-rom o en un disco habilitado, usted puede:

- inicie desde un disco de rescate e inicie el kernel.
- desplácese hasta la consola virtual (Alt+F2)
- monte el disco duro, en donde está su /root
- edite (El disco de rescate Debian 2.2, viene con `ae`, Debian 3.0 viene con `nano-tiny`, el cual es similar a `vi`) `/etc/shadow` y modifique la línea:

  ```
  root:asdfjl290341274075:XXXX:X:XXXX:X::: (X=cualquier número)
  ```

  para:

  ```
  root::XXXX:X:XXXX:X:::
  ```

Este removerá la clave del administrador. Usted puede iniciar el sistema y entrar como root desde el login: entre como root (con una clave vacía). Esto funcionará, a menos que usted haya configurado el sistema más firmemente, por ejemplo, si usted ha permitido usuarios con claves nulas y el administrador puede entrar puede entrar al sistema desde la consola.

Si usted ha introducido también estas características, usted necesitará entrar en el modo single. LILO no necesita ser limitado si usted ha hecho esto también, necesitará reiniciar `lilo` justo después que el administrador lo reajusta. Esto es totalmente difícil desde que su `/etc/lilo.conf` necesite ser atrapado por tener un / sistema de archivo, que es un disco de la memoria ram y no del verdadero disco duro.

Una vez que LILO no sea restringido, usted puede:

- Presionar Alt, shift o la tecla Control, antes que el sistema BIOS finalice, usted debería obtener la entrada LILO.
- Escribir "Linux single", linux init=/bin/sh ó como "linux 1" en la entrada.
- usted debería obtener una entrada a interfaz de comando en el modo singleuser (este solicitará la clave, aunque usted ya la conozca).
- vuelva a montar read/write the/ partition

```
mount -o remount,rw /
```

- Cambiar la clave del superusuario con `passwd` (desde que usted sea el superusuario, no se le solicitará la clave anterior).

11.2. ¡Mi sistema es vulnerable!

11.2.1. He sufrido una interrupción, ¿qué debo hacer?

Lea este documento y tome las medidas necesarias descritas aquí. Si necesita asistencia, usted puede usar debian-security@lists.debian.org para solicitar consejos sobre cómo recuperar /parche y arreglar su sistema.

11.2.2. ¿Cómo puedo encontrar el origen de un ataque?

Observando las bitácoras (si ellas no han sido cambiadas), usando sistemas de detección de intrusión (observe 'Montar el descubrimiento de intrusión' en la página 85), `traceroute`, `whois` y herramientas similares (incluyendo análisis forense), usted puede encontrar un ataque a la fuente. La manera como usted debería reaccionar frente a esta información depende, solamente del uso apropiado que usted le de a la política de seguridad y que *usted* considere lo que es un ataque. ¿Es un scanner remoto un ataque? ¿Un ataque es una prueba de vulnerabilidad?

11.2.3. Cualquier programa en Debian es vulnerable ¿Qué debo hacer?

Tómese un momento. Primero, observe si la vulnerabilidad ha sido anunciada en listas de correo de seguridad pública (como Bugtraq) u otros foros, el equipo de seguridad Debian permanece actualizado con estas listas, de manera que ellos ya pueden estar enterados del problema. No ejecute ningunas acciones remotas si usted ya observa algún anuncio en `http://security.debian.org`.

Si no observa nada de lo anteriormente nombrado, por favor envíe un correo a los paquetes afectados, XXXtan bién como una descripción de la vulnerabilidad, tan detallada como sea posible (demuestre si el concepto de código también es correcto) para security@debian.org , el cual lo accederá a un análisis con el equipo de seguridad.

11.2.4. El número de versión para un paquete indica que todavía estoy corriendo una versión vulnerable

En lugar de actualizar una nueva descarga, podemos fijar la seguridad en backport, a la versión que fue enviada en la descarga establecida. La razón de esto es asegurarnos que una descarga cambie posiblemente un poco algunas cosas o que se interrumpan repentinamente, como un resultado de la seguridad fija. Usted puede chequear si está corriendo una versión segura de un paquete, observando el paquete changelog o comparando su número de versión exacta (versión upstream -slash- descargar debian)el número de la versión exacta con la versión indicada en el Asesor de seguridad Debian.

11.2.5. Encontré usuarios haciendo 'su' en mis bitácoras

Usted puede encontrar líneas en sus bitácoras como:

```
 Apr 1 09:25:01 server su[30315]: + ??? root-nobody
 Apr 1 09:25:01 server PAM_unix[30315]: (su) session opened for user nobody b
(uid=0)
```

No se preocupe tanto, revise si esto se debe a un trabajo en funcionamiento a través de cron (usualmente con `/etc/cron.daily/find` o `logrotate`):

```
$ grep 25 /etc/crontab
25 6 * * * root test -e /usr/sbin/anacron || run-parts --report
/etc/cron.daily
$ grep nobody /etc/cron.daily/*
find:cd / && updatedb --localuser=nobody 2>/dev/null
```

11.2.6. Software específico

Proftpd es vulnerable a un ataque en el servicio Denial.

Agregue `DenyFilter \*.*/` a su archivo de configuración, para más información observe http://www.proftpd.org/critbugs.html.

11.3. Preguntas con respecto al equipo de seguridad Debian

11.3.1. Lo que es una Advertencia de Seguridad Debian (DSA).

Ésta es una información enviada por el equipo de seguridad Debian (observe en la parte de abajo), informando acerca de un ajuste de una seguridad relacionada a la vulnerabilidad

disponible para el sistema operativo Debian. Los ASDs firmados, son enviados a las listas de correo público y anunciado en la página web de Debian (tanto en la página frontal como en el área de seguridad security area (http://www.debian.org/security/)).

Las DSA incluyen información acerca de el(los) paquete(s) afectado(s), el error descubierto y donde se pueden obtener los paquetes actualizados (y sus sumas MD5).

11.3.2. La firma sobre de la advertencia de Debian no es verificada correctamente.

Probablemente este sea un problema suyo. La lista de anuncios de seguridad de Debian tiene un filtro que solamente permite el envío de mensajes con una firma correcta de uno de los miembros del equipo de seguridad.

Probablemente alguna pieza de los programas de correo de su parte, hace cambios menores en los mensajes rompiendo la firma. Asegúrese que sus programas no no hacen ninguna codificación o decodificación MIME, o haya conversión de tabuladores a espacio.

Un posible culpable es fetchmail (con la codificación MIME habilitada) y formail (de procmail 3.14 únicamente).

11.3.3. Como se tratan los incidentes de seguridad en Debian?

Una vez el equipo de seguridad recibe una notificación de un incidente , uno o mas miembros lo revisan y consideran a Debian /estable vulnerable o no. Si nuestro sistema es vulnerable este es trabajado sobre el ajuste del problema. El paquete se mantiene en buen contacto siempre y cuando no haya contacto ahora con la seguridad del equipo. Finalmente el ajuste es probado y los nuevos paquetes son preparados, los cuales entonces son compilados sobre toda la arquitectura estable y son transferidos de un computador, de la periferia al centro, después de que toda esta labor se hace el asesor de la seguridad (DAS) es enviado a los correos de lista pública.

11.3.4. ¿Cuánto tiempo tomará Debian para ajustar la vulnerabilidad?

Analizando el tiempo que tarda la seguridad del equipo Debian , al enviar un acesor y producir paquetes ajustados es mínimo. Una vez es conocida la vulnerabilidad, ésta se ajusta a la distribución estable rápidamete.

Un reporte publicado published in the debian-security mailinglist (http://lists.debian.org/debian-security/2001/debian-security-200112/msg00257.html) mostró que en el año 2001, este tomó el equipo de seguridade Debian, un termino medio de 35 días para ajustar la seguridad vulnerable relacionada, Sin embargo, sobre el 50 % de las vulnerabilidades fueron ajustados en 10 días y el 15 % fueron ajustados *algunos días*los avisos que fueron registrados.

Sin embargo, cuando se formula está pregunta la gente se hace estas preguntas trata de no olvidar que:

- DSAS no es enviada hasta que:
  - los paquetes esten disponibles para *todas* las arquitecturas soportadas por Debian (este toma algun tiempo para paquetes, que son parte del sistema central considerando especialmente, el numero de la arquitectura soportadas en las publicaciones estables.
  - Nuevos paquetes evaluados completamente para asegurar que las imperfecciones no sean introducidas.
- El paquete sería obtenido antes de que el DSA sea enviado (a lafila de entrada, o de espejos).
- Debian es un proyecto conformado por voluntarios.
- Hay una claúsula "no hay garantías" que son parte de la licensia con la cual debian es otorgado.

11.4. ¿Cómo es manejada la seguridad para `prueba` e `inestable`?

la respuesta corta es:esto no es. La prueba y lo inestable, son rápidamente movidos objetivamente, y el equipo de seguridad no tiene los medios apropiados que necesita para soportarlos, si usted quiere tener un servicio seguro (y estable), usted está motivado a trabajar con lo estable.

Sin embargo, como un hecho real lo inestable, usualmente es arreglado rápidamente,para la seguridad de datos actualizada. Algunas veces estos son usualmente obstenidos en versiones rápidas (otra versiones posteriores que se necesitan usualmente son backported).

11.4.1. ¿Por qué no hay réplicas oficiales de security.debian.org?

A: el objetivo de seguridad.debian.org, es permitir actualizaciones de seguridad de la forma más rápida y fácil posible. Las réplicas añadirían complejidad extra innecesaria y pueden la causar frustraciones si no están actualizados.

11.4.2. ¿Cómo puedo buscar el equipo de seguridad?

A: La información de seguridad puede ser enviada a la seguridad Debian org, la cual es leída por todo el operador Debian. Si usted tiene información sensitiva , por favor use el equipo@ de seguridad Debian org, que solamente los miembros de seguridad del equipo pueden leer. Si desea correo puede ser codificado con la seguridad Debian contacte la clave (ID 363CCD95)

11.4.3. ¿Qué diferencia hay entre seguridad @ Debian org y la lista de seguridad Debian org?

Cuando usted envia mensajes a la seguridad @Debian org y Debian. Estos son enviados a los reveladores de la lista de correo (Debian-privada) todos estos están suscritos a los reveladores Debian, al enviar esta lista son guardados privadamente (i.e no son archivados en el web publico).Debian security@lists.debian.org es una lista de correos pública, a bierta para quien quiera inscribirse, y hay archivos disponibles en la página web.

11.4.4. ¿Cómo puedo contribuir con el equipo de seguridad Debian?

- Para contribuir a este documento ajustar ARREGLAME,proporcionando nuevos contenidos. La documentacón es importante y reduce la sobre carga de responder asuntos comúnes. La traduccón de este documento a otras lenguases de gran utilidad.
- Por las aplicaciones de empacar que son útiles para proporcionar /revisando la seguridad en el /usando un sistema Debian . Si usted no es un revelador, archive un WNPP bug (`http://www.debian.org/devel/wnpp/`) y solicite al sesoftware lo que usted considera útil y no es comúnmente proporcionado.
- Auditar aplicaciones en Debian o ayudar a resolver la seguridad de errores de programación y reportar asuntos a securiti@ debian.org.el proyecto de otros trabajos como Linux Kernel Security Audit Project (`http://kernel-audit.sourceforge.net/`) or the Linux Security-Audit Project (`http://www.lsap.org/`) incrementa la seguridad de Dbian GNU/linux desde contribuciones , que eventualmente ayudarán también.

En algunos casos por favor, revise cada problema antes de reportarlo para la security@ debian org. Si usted es capaz de proporcionar parches que agilisen el proceso sabiamente. No simplemente enviar mails bugtraq, desde que ellos todavía sean recibdos. Sin embargo es una buena idea proporcionar información adicional.

11.4.5. ¿Quiénes componen el equipo de seguridad debian?

Normalmente el equipo de seguridad Debian consta de cinco miembros y dos secretarios. El equipo de seguridad designa las personas para unirlas al equipo.

11.4.6. ¿La seguridad debian del equipo revisa los nuevos paquetes en debian?

No, la seguridad de los equipos Debian no revisa cada paquete nuevo ni hay un chequeo automático (lintian) para detectar defectos en los paquetes nuevos, desde esas revisiones es imposible detectarlos automáticamente . Sin embargo mantenerlos es completamente responsabilidad de el software que es introducido en Debian y no en software, y no un software que nisiquiera es asiganado por un revelador autorizado.Ellos estan encargados de analizar el software y mantenerlo en la seguridad de aviso.

11.4.7. ¿Yo tengo una antigua versión sobre Debian , está soportada la seguridad?

Infortunadamente no , la seguridad del equipo Debian no puede manejar la descarga estable de éste, (también inestable) y otras antiguas descargas . Sin embargo usted puede esperar la seguridad de la información actualizada por un periodo límite de tiempo justo , a un despues de que la distribución del nuevo Debian sea descargada.

Apéndice A

El proceso de fortalecimiento es manejado paso a paso

Un procedimiento siempre es útil, si le permite ver el proceso completo de fortalecimiento y le permita tomar desiciones. Una posibles aproximación para este procedimiento en Debian 2.2.GNU/linux es mostrado abajo. Este es un proceso post de instalación para una revición de la lista de medidas a ser tomadas, paso a paso, durante la configuración. vea 'Lista de chequeo de la configuración' en la página 117.también este procedimiento está (por el momento) más orientado hacia el fortalecimiento de servicios del sistema de redes.

- Haga una instalación del sistema (considere la información en este howto acerca de las particiones). Después que la instalación de base sea instalada, entre a la instalación por defecto , no seleccione paquetes de tareas, si no seleccione shadow passwords.
- Vaya através de `dselect` y remueva lo que no es necesario, si no selecciono paquetes antesv de ser (I)instalados. Deje la menor cantidad de programas necesarios en el servidor.
- Actualice todo el software desde los utimos paquetes disponibles en security.debian.org como se expuso previamente en 'Ejecute una actualización de seguridad' en la página 32.
- implemente las sugerencias presentadas en este manual , considerando las cuotas del usuario, definiciones de login y lilo.
- Para hacer un fortalecimiento del servicio haga una lista de servicios activos actualmente en el sistema.

  ```
  $ ps -aux
  $ netstat -pn -l -A inet
  # /usr/sbin/lsof -i | grep LISTEN
  ```

  Necesitará instalar `lsof-2.2` para que el tercer comando funcione (corralo como root). Debería ser consiente que `lsof` puede transladar la palabra LISTEN a su configuraciones de los locales.

- Para eliminar los servicios innecesario, primero determine como comienza y de que paquete proviene. Puede hacer esto fácil revisando el programa que escucha en ese puerto, el siguiente ejemplo le dice como hacer uso de estas herramientas y `dpkg`

```
#!/bin/sh
# ARREGLAME: this is quick and dirty; replace with a more robust script
for i in ‘sudo lsof -i | grep LISTEN | cut -d " " -f 1 |sort -u‘ ; do
 pack=‘dpkg -S $i |grep bin |cut -f 1 -d : | uniq‘
 echo "Service $i is installed by $pack";
 init=‘dpkg -L $pack |grep init.d/ ‘
 if [ ! -z "$init" ]; then
 echo "and is run by $init"
 fi
done
```

- Una vez que usted encuentre servicios no deseados, remueva el paquete (con `dpkg -purge`) o, si es útil, pero no debería estar habilitado al inicio, use `update-rc.d` (vea ‘Deshabilitar los demonios’ en la página 23) para removerlo del sistema de inicio.

- Para los servicios inetd (lanzado por el super demonio)usted podría revisar los servicios habilitados, por ejemplo con:

```
$ grep -v "^#" /etc/inetd.conf | sort -u
```

  e incapacitar aquellos que no sean necesarios, comentando la línea que los incluye, removiendo los paquetes o usando `update-inetd`

- Si se tienen servicios de cubierta (usando estos `/usr/sbin/tcpd`) revise que los `/etc/hosts.allow` y `/etc/hosts.deny` estén configurados acorde a su política de servicios.

- Si es posible y dependiendo de cada servicio usted puede tener un límite de servicios, si desea limitar cuando se usa más de una interfaz externa para escuchar solamente cada una de ellas. Por ejemplo, si usted desea el acceso interno a FTP, haga que el demonio escuche en su interfaz de administración solamente, no sobre todas las interfaces (i.e, 0.0.0.0:21).

- Reinicie la máquina, o cámbiela para entrar a single user y vuelva a multiusuario con

```
$ init 1
(....)
$ init 2
```

- Revise los servicios disponibles actualmente, y si es necesario repita estos pasos de nuevo.

- Instale, ahora los servicios necesarios, si usted todavia no lo ha hecho, y configurelos apropiadamente.
- Revise que usuarios son utilizados para correr los servicios deisponibles, por ejemplo con:

```
$ for i in '/usr/sbin/lsof -i |grep LISTEN |cut -d " " -f 1 |sort -u';
do user='ps -ef |grep $i |grep -v grep |cut -f 1 -d " "' ; echo
"Service $i is running as user $user"; done
```

  y considere cambiar estos servicios para un usuario o grupo dado, que pueden también ser cambiados de directorio raíz, para incrementar la seguridad. Puede hacer esto cambiando el script `/etc/init.d` donde el servicio se activa. La mayoría de servicios en Debian usan `start-stop-daemon` de tal forma que puede usar la opción –change-uid y la opción –chroot para configurar estos servicios. Cambiar el directorio raíz de los servicios está más allá del alcance de este documento, pero ofrecemos una palabra de advertencia: Usted podría necesitar poner todos los archivos instalados por el servicio de paquetes usando dpkg -L y los paquetes de los que dependen en el ambiente de cambio de directorio raíz.
- Repita los pasos anteriores para revisar que los solamente los servicios deseados corran, y que lo hagan como el usuario o grupo desea.
- Pruebe la instalación de servicios para saber si trabajan como se esperaba.
- Compruebe el sistema usando un revisor de aseguramiento de vulnerabilidades (como `nessus`) para determinar las vulnerabilidades del sistema (configuraciones erróneas, servicios viejos o innecesarios)
- Instale medidas de instrusión por red y medidas de intrusión por servidor (como `snort` y `logsentry`).
- Repita el paso del revisor de red y verifique que los sistemas de detección de intrusiónd trabajan correctamente.

para los verdaderos paranoicos, considere también lo siguiente:

- Agregar capacidades de cortafuegos al sistema, aceptando conexiones entrantes solamente para los servicios ofrecidos y limite conexiones salientes para los autorizados.
- Vuelva a revisar la instalación con una nueva herramienta de revisión de vulnerabilidades.
- Revise las conexiones salientes usando un revisor de red desde el sistema a un servidor externo y verificque que las conexiones indeseadas no encuentren vía de salida.

ARREGLAME: Este procedimiento considera el servicio de fortelecimiento, pero no el sistema de fortalecimiento a nivel de usuario, incluir informaciones con respecto al chequeo de permisos del usuario, archivos setuid y paros en el sistema usando el sistema de archivos.

Apéndice B

Lista de chequeo de la configuración

Este apéndice reitera puntos de otras secciones de este manual condensando en un formato de lista de chequeo. El propósito es ser un resumen para quienes ya han leído el manual. También hay otras buenas listas de chequeo disponibles, Kurt Seifried tiene una configuración basada en un curso en Securing Linux Step by Step (`http://seifried.org/security/os/linux/20020324-securing-linux-step-by-step.html`).

ARREGLAME: esto es basado en v1.4 del manual, y podría necesitar actualizarse.

- límitar la entrada para un acceso físico.
  - Capacitar la contraseña BIOS
  - incapacitar la entrada floppy/cdrom/...
  - enviar una contraseña LILO o GRUB (`/etc/lilo.conf` o `/boot/grub/menu.lst`, respectivamente); revisar que la configuración de los archivos LILO o GRUB sea de lectura-protegida.
  - desaprobar el disco flexible MBR para iniciar por el respaldo de la floppy booting back door by overwriting the MBR (maybe not?)
- partitura
  - Separe los datos del suscriptor, no sistema de datos, y cambiar rápaidamente los datos del tiempo de recorrido de sus datos de particón.
  - enviar `nosuid,noexec,nodev` montar opciones en `/etc/fstab` sobre la partición ext2 tal como `/tmp`.
- Higiene de las contraseñas y aseguramiento a la entrada
  - Defina una buena contraseña para el administrador
  - Habilite shadowing y MD5 en las contraseñas
  - Instale y use PAM

    - Agregue MD5 para soportar PAM y asegúrese que: (en términos generales) las entradas en el archivo `/etc/pam.d/` que permiten acceso a la máquina, tengan en el segundo campo del archivo pam.d definidoc com "requisite" o "required".
    - Cambie `/etc/pam.d/login` para permitir solamente entradas locales al administrador.
    - también marque las tty: atuorizadas en `/etc/security/access.conf` y generalmente configurar este archivo para limitar la entrada del administrador tanto como sea posible.
    - Agregue pam_limits.so si usted desea habilitar límites para usuarios.
    - Cambie `/etc/pam.d/passwd`: especifique un tamaño mínimo de contraseña.(podrían ser 6 caracteres) y habilite md5
    - agregue un grupo wheel a `/etc/group` si desea, agregue pam_wheel. para entrar a `/etc/pam.d/su`
    - para especificar controles por usuario iniciales, use pam_listfile cuando sea apropiado.
    - tenga un archivo `/etc/pam.d/other`y montarlo con seguridad alta.
  - ponga límites en `/etc/security/limits.conf` (note que `/etc/limits` no es usado si usted está utilizando PAM)
  - Restrinja `/etc/login.defs`; también, si usted habilita MD5 y/o PAM, asegurese que usted hace los cambios carrespondientes ahí también.
  - inhabilite el acceso a root por ftp en `/etc/ftpusers`
  - inhabilite la entrada vía red al root; use `su(1)` o `sudo(1)`. (considere instalar `sudo`)
  - Use PAM para hacer cumplir las restrinciones adicionales sobre logins?

- Otros asuntos de la seguridad local.

  - Cambios de Kernel (ver 'Características de la red configurando kernel' en la página 44)
  - Parches del Kernel (ver 'Parches útiles del núcleo' en la página 87)
  - restrinja los permisos de los archivos de bitácora (`/var/log/{last,fail}log`, Apache logs)
  - Verifique que la revisión de setuid está habilitada en `/etc/checksecurity.conf`
  - Considere hacer algunos archivos log append-only y configurar archivos inmutables usando chattr (ext2 filesystems únicamente)
  - Active integridad de archivos (vea 'Integridad de su sistema de archivos' en la página 49). instale `debsums`
  - Considere remplazar locate con slocate
  - Enviar bitácoras a una impresora local?
  - Queme su configuración sobre un CD de arranque y e inicie la máquina desde este?
  - incapacitar módulos del kernel?

- Limite el acceso a la red

- Instale y configure `ssh` (se sugiere PermitRootLogin No `/etc/ssh/sshd_config`, PermitEmptyPasswords No; note que hay otras sugerencias en este texto)
- Considere incapacitar o eliminar in.telnetd
- Generalmente, inhabilite los servicios gratuitos en `/etc/inetd.conf` usando `update-inetd --disable` (or inhabilite todo inetd, o use un reemplazo como xinetd or rlinetd)
- Inhabilite los otros servicios gratuitos de red; mail, ftp, DNS, www, etc no deben estar corriendo si usted no los necesita y monitoréelos regularmente.
- Para los servicios que necesite, no use solamente los programas comunes, busque más versiones seguras enviadas por Debian (o busque otros recursos). Para cualquier servicio que usted termine usando, asegúrese de entender los riesgos.
- Monte celdas de directorio raíz distintos para usuarios externos y demonios.
- Configure firewall y tcpwrappers (i.e. `hosts_access(5)`); revise `/etc/hosts.deny` en este texto.
- si usted corre ftp, monte su servidor ftpd y siempre corra chrooted para el directorio raíz del usuario
- Si usted corre X, inhabilite la autenticación xhost y use ssh a cambio, mejor aún, inhabilite X remoto si usted puede (adicione -nolisten tcp a X desde la línea de comandos y apague XDMCP en `/etc/X11/xdm/xdm-config` configurando requestPort a 0)
- Inhabilite el acceso externo a impresoras.
- Use tunel para sesiones de IMAP o POP a través de SSL o ssh; instale stunnel si usted quiere proporcionar este servicio a usuarios de correo remoto
- Monte un loghost y configure otras máquinas para enviar logs a ésta (`/etc/syslog.conf`)
- asegure BIND, Sendmail, y otros demonios complejos (Configure una celda de cambio de directorio ; corra como non-root pseudo-user)
- Instale snort o una herramienta de logging similar.
- Prescinda de NIS y RPC si usted puede (inhabilite portmap).

- Políticas

  - Eduque a los usuarios acerca de los porque y los como de sus políticas. Cuando usted ha prohibido algo que normalmente está disponible en otros sistemas, suministre documenteción que explique como conseguir resultados similares usando otros medios más seguros.
  - Prohiba el uso de protocolos que usa claves en texto plano (telnet, rsh y friends; ftp, imap, http, . . .).
  - Prohiba programas comoVGAlib.
  - Use quotas de disco.

- manténegase informado sobre asuntos de seguridad
  - Subscríbase a la lista de correo de seguridad
  - Subscríbase a las actualizaciones de seguridad, adicione a `/etc/apt/sources.list` una entrada (o entradas) a http://security.debian.org/debian-security
  - Además recuerde correr periódicamente `apt-get update ; apt-get upgrade` (tal vez instalar un cron job?) como se explicó en 'Ejecute una actualización de seguridad' en la página 32.

Apéndice C

Montar un IDS aislado

Usted puede montar fácilmente una máquina Debian como un Sistema de Detección de Instrusos usando `snort`.

Algunas pautas:

- Instale una base de sistema Debian y no seleccione paquetes adicionales.
- Baje e instale (con dpkg) manualmente los paquetes necesarios (vea los paquetes instalados en la lista de abajo).
- Baje e instale ACID (Analisis Consolado para Instrucciones para la Base de Datos).

ACID es un paquete corrientepara Debian con el `acidlab`, esto ocaciona un grafico WWW interfaz para sacar snort's . Esto pude obtenerse desde `http://www.cert.org/kb/acid/`, `http://acidlab.sourceforge.net` or `http://www.andrew.cmu.edu/~rdanyliw/snort/`. You might want to read the Snort Statistics HOWTO (`http://www.linuxdoc.org/HOWTO/Snort-Statistics-HOWTO/index.html`).

Usted puede montar este sistema con almenos dos interfaces: una interfaz conectada para un mantenimiento lan (para el acceso a los resultados y para mantener el sistema), una interfaz conectada con ip-direcciónagregada al sistema al segmento de la red para ser analizado .

Para configurar las tarjetas de red sin una ip-dirección usted no puede usar el standard's Debian `/etc/network/interfaces` desde el `ifup` y `ifdown` espere más informaciones que necesita. Usted tiene (simple `ifconfig eth0 up`)

Usted necesita tener puesta instalacióne Debian standard Apache, MySQL y PHP4 por ACID para trabajar. Downloaded paquetes (Nota:las versiones podrian variar dependiendo de cada distribución debian que usted usa, esto es desde Debian *woody* septiembre 2001):es

```
ACID-0.9.5b9.tar.gz
adduser_3.39_all.deb
apache-common_1.3.20-1_i386.deb
```

```
apache_1.3.20-1_i386.deb
debconf_0.9.77_all.deb
dialog_0.9a-20010527-1_i386.deb
fileutils_4.1-2_i386.deb
klogd_1.4.1-2_i386.deb
libbz2-1.0_1.0.1-10_i386.deb
libc6_2.2.3-6_i386.deb
libdb2_2.7.7-8_i386.deb
libdbd-mysql-perl_1.2216-2_i386.deb
libdbi-perl_1.18-1_i386.deb
libexpat1_1.95.1-5_i386.deb
libgdbmg1_1.7.3-27_i386.deb
libmm11_1.1.3-4_i386.deb
libmysqlclient10_3.23.39-3_i386.deb
libncurses5_5.2.20010318-2_i386.deb
libpcap0_0.6.2-1_i386.deb
libpcre3_3.4-1_i386.deb
libreadline4_4.2-3_i386.deb
libstdc++2.10-glibc2.2_2.95.4-0.010703_i386.deb
logrotate_3.5.4-2_i386.deb
mime-support_3.11-1_all.deb
mysql-client_3.23.39-3_i386.deb
mysql-common_3.23.39-3.1_all.deb
mysql-server_3.23.39-3_i386.deb
perl-base_5.6.1-5_i386.deb
perl-modules_5.6.1-5_all.deb
perl_5.6.1-5_i386.deb
php4-mysql_4.0.6-4_i386.deb
php4_4.0.6-1_i386.deb
php4_4.0.6-4_i386.deb
snort_1.7-9_i386.deb
sysklogd_1.4.1-2_i386.deb
zlib1g_1.1.3-15_i386.deb
```

Installed packages (dpkg -l):

```
ii adduser 3.39
ii ae 962-26
ii apache 1.3.20-1
ii apache-common 1.3.20-1
ii apt 0.3.19
ii base-config 0.33.2
ii base-files 2.2.0
ii base-passwd 3.1.10
ii bash 2.03-6
```

```
ii bsdutils 2.10f-5.1
ii console-data 1999.08.29-11.
ii console-tools 0.2.3-10.3
ii console-tools- 0.2.3-10.3
ii cron 3.0pl1-57.2
ii debconf 0.9.77
ii debianutils 1.13.3
ii dialog 0.9a-20010527-
ii diff 2.7-21
ii dpkg 1.6.15
ii e2fsprogs 1.18-3.0
ii elvis-tiny 1.4-11
ii fbset 2.1-6
ii fdflush 1.0.1-5
ii fdutils 5.3-3
ii fileutils 4.1-2
ii findutils 4.1-40
ii ftp 0.10-3.1
ii gettext-base 0.10.35-13
ii grep 2.4.2-1
ii gzip 1.2.4-33
ii hostname 2.07
ii isapnptools 1.21-2
ii joe 2.8-15.2
ii klogd 1.4.1-2
ii ldso 1.9.11-9
ii libbz2-1.0 1.0.1-10
ii libc6 2.2.3-6
ii libdb2 2.7.7-8
ii libdbd-mysql-p 1.2216-2
ii libdbi-perl 1.18-1
ii libexpat1 1.95.1-5
ii libgdbmg1 1.7.3-27
ii libmm11 1.1.3-4
ii libmysqlclient 3.23.39-3
ii libncurses5 5.2.20010318-2
ii libnewt0 0.50-7
ii libpam-modules 0.72-9
ii libpam-runtime 0.72-9
ii libpam0g 0.72-9
ii libpcap0 0.6.2-1
ii libpcre3 3.4-1
ii libpopt0 1.4-1.1
ii libreadline4 4.2-3
ii libssl09 0.9.4-5
ii libstdc++2.10 2.95.2-13
```

```
ii libstdc++2.10- 2.95.4-0.01070
ii libwrap0 7.6-4
ii lilo 21.4.3-2
ii locales 2.1.3-18
ii login 19990827-20
ii makedev 2.3.1-46.2
ii mawk 1.3.3-5
ii mbr 1.1.2-1
ii mime-support 3.11-1
ii modutils 2.3.11-13.1
ii mount 2.10f-5.1
ii mysql-client 3.23.39-3
ii mysql-common 3.23.39-3.1
ii mysql-server 3.23.39-3
ii ncurses-base 5.0-6.0potato1
ii ncurses-bin 5.0-6.0potato1
ii netbase 3.18-4
ii passwd 19990827-20
ii pciutils 2.1.2-2
ii perl 5.6.1-5
ii perl-base 5.6.1-5
ii perl-modules 5.6.1-5
ii php4 4.0.6-4
ii php4-mysql 4.0.6-4
ii ppp 2.3.11-1.4
ii pppconfig 2.0.5
ii procps 2.0.6-5
ii psmisc 19-2
ii pump 0.7.3-2
ii sed 3.02-5
ii setserial 2.17-16
ii shellutils 2.0-7
ii slang1 1.3.9-1
ii snort 1.7-9
ii ssh 1.2.3-9.3
ii sysklogd 1.4.1-2
ii syslinux 1.48-2
ii sysvinit 2.78-4
ii tar 1.13.17-2
ii tasksel 1.0-10
ii tcpd 7.6-4
ii telnet 0.16-4potato.1
ii textutils 2.0-2
ii update 2.11-1
ii util-linux 2.10f-5.1
ii zlib1g 1.1.3-15
```

FIXME: !!!!! Falta mucho aqui !!!!! ¿Dónde esta lo demás?