GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-610)

CONFIGURACIÓN SEGURA RED HAT LINUX 7

DICIEMBRE 2006

Edita:

NIPO: 076-06-216-8

Tirada: 1000 ejemplares
Fecha de Edición: diciembre de 2006

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

PRÓLOGO

Entre los elementos más característicos del actual escenario nacional e internacional figura el desarrollo alcanzado por las Tecnologías de la Información y las Comunicaciones (TIC), así como los riesgos emergentes asociados a su utilización. La Administración no es ajena a este escenario, y el desarrollo, adquisición, conservación y utilización segura de las TIC por parte de la Administración es necesario para garantizar su funcionamiento eficaz al servicio del ciudadano y de los intereses nacionales.

Partiendo del conocimiento y la experiencia del Centro sobre amenazas y vulnerabilidades en materia de riesgos emergentes, la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional en su artículo 9.2.f).

Una de las funciones más destacables que, asigna al mismo, el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración.

La serie de documentos CCN-STIC se ha elaborado para dar cumplimiento a esta función, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Diciembre de 2006

Alberto Sáiz
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

ANEXOS

1. INTRODUCCIÓN

1. El presente documento contiene una guía para la configuración segura del sistema operativo Red Hat Linux, en máquinas en las que posteriormente se instala aplicaciones que requieren un nivel óptimo de seguridad.

2. La configuración deberá realizarse en máquinas con el sistema operativo recién instalado, si bien también se deben llevar a cabo periódicamente sobre cualquier máquina para comprobar el estado de seguridad de la misma.

3. En un anexo final se incluye un cuadro con cada uno de los chequeos que deben realizarse, de forma que se facilite la labor de securizar la máquina.

2. PROCEDIMIENTO DE SECURIZACIÓN

4. A continuación se detallan los chequeos que deben realizarse en cada máquina para reforzar la seguridad del sistema operativo de la misma, tanto en máquinas con el sistema operativo recién instalado como en aquellas que necesiten una revisión posterior.

2.1. BIOS

5. Se recomienda colocar una contraseña de Arranque para deshabilitar el arranque desde disquetes y configurar correctamente las características de la BIOS. De esta forma se bloquea el acceso indeseado al arranque del sistema Linux con un disco especial y proteger la configuración de la BIOS.

2.2. POLÍTICAS DE SEGURIDAD

6. Antes de implementar seguridad, hay que definir perfectamente qué es lo que se quiere securizar. Para ello es necesario configurar una lista con que se considera permitido o no permitido, y determinar cómo se debe actuar en caso de violación de esa seguridad:

   - Cómo se clasifica la información como confidencial o delicada
   - El sistema contiene información confidencial o delicada
   - Exactamente de quién hay que guardarse
   - Los usuarios remotos tienen realmente necesidad de acceso
   - Las contraseñas o la encriptación proporcionan suficiente seguridad
   - Se necesita acceso a Internet
   - Que tipo de acceso es necesario desde el sistema a Internet
   - Que acciones se llevarán a cabo en el caso de brecha en la seguridad…..

2.3. ELECCIÓN DE LA CLAVE CORRECTA

7. El primer punto de la configuración de la Seguridad en un Sistema Linux, es la elección de una Clave o contraseña correcta.

8. La ejecución semanal de un crackeador de contraseñas, es un buen método para comprobar la fortaleza de las mismas. También sería deseable un mecanismo que detectara una contraseña débil cuando se introduce por primera vez o se cambie una antigua. Texto plano o palabras usuales de un diccionario, que no contengan números ni caracteres especiales, son contraseñas que no deberían ser permitidas.

9. Las siguientes reglas son un buen principio a seguir para la elección de una contraseña:

   - Deben tener al menos una longitud de 8 caracteres, incluyendo al menos 1 carácter numérico o especial.
   - No deben ser triviales, contraseñas triviales que sean fácilmente adivinables, basadas en el nombre de usuario, características personales…etc.
   - Deben tener un período de caducidad, requiriendo la elección de una nueva contraseña cuando haya pasado un período de tiempo especificado.
   - Se debe revocar el acceso después de un número determinado de intentos fallidos.

10. Por defecto el número mínimo de caracteres de la contraseña en el Sistema Linux es de 5, por lo que sería conveniente modificar el fichero correspondiente y cambiar este valor a 8, editando

    /etc/login.defs

    y cambiando la línea

    PASS_MIN_LEN 5

    a lo siguiente:

    PASS_MIN_LEN 8

11. El fichero */etc/login.defs* es el fichero de configuración de login del sistema. Se debe revisar este fichero para la configuración de cada sistema, ya que contiene algunos de los parámetros de la política de seguridad a instaurar.

2.4. LA CUENTA DE ROOT

12. La cuenta de root, es la cuenta con más privilegios del sistema, ya que no tiene ninguna restricción de seguridad impuesta. Así el sistema asume que el superusuario sabe lo que está haciendo.

13. Una de las pocas medidas de seguridad que se pueden adoptar en cuanto al usuario root, es configurar en tiempo máximo de inactividad de la cuenta de root. Para ello hay que configurar una variable especial de Linux, llamada *TMOUT* (tiempo en segundos para la inactividad antes de abandonar el sistema).

14. En el fichero */etc/profile* hay que añadir la siguiente línea (después de la línea HISTFILESIZE):
    TMOUT=7200
15. Si decidimos incluir esta línea en el fichero indicado, todos los usuarios que superen los 7200 segundos (2 horas) de inactividad, serán automáticamente desconectados del sistema.

16. Si se prefiere configurar un tiempo de inactividad diferente para cada usuario, habría que configurar esta misma variable para cada usuario en el fichero .bashrc .

17. Para que los cambios tengan efecto, se debe salir y volver a entrar al sistema como root.

2.5. EL FICHERO /etc/exports

18. Si se están exportando ficheros de sistema utilizando el servicio NFS, hay que estar bien seguros de tener bien configurado el fichero /etc/exports con el acceso más restrictivo posible. Es decir que no hay que utilizar comodines, no permitiendo el acceso de escritura como root y configurando en lo posible como sólo lectura:

19. Editar el fichero /etc/exports y añadir las siguientes líneas:
    /dir/to/export host1.mydomain.com(ro,root_squash)
    /dir/to/export host2.mydomain.com (ro,root_squash)

    Donde:
    - /*dir/to/export* es el directorio que se quiere exportar
    - *host#.mydomain.com* es la máquina que tiene permiso para entrar en el directorio
    - La opción *ro*, significa sólo lectura
    - La opción *root_squah*, es para no permitir el acceso a escritura como root en este directorio

20. Para que estos cambios tengan efecto, es necesario ejecutar el comando siguiente en el terminal:
    [root@deep]# /usr/sbin/exportfs –a

Nota: Hay que estar totalmente seguros de necesitar el servicio NFS en el Sistema, ya que puede ser un grave problema de seguridad.

2.6. DESHABILITAR EL PROGRAMA DE ACCESO A CONSOLA

21. Hay que estar totalmente seguros que el acceso por consola está correctamente configurado, ya que desde la consola se pueden realizar operaciones como reseteo, reinicio...etc., entre otras. Para ello conviene deshabilitar ciertas opciones mediante el siguiente comando:

    [root@deep] /# rm –f /etc/security/consolo.apps/<servicename>

donde servicename, es el nombre del programa que se desea deshabilitar desde la consola. A menos que se utilice siempre xdm, hay que tener en cuenta que borrar el servicio xserver, conlleva que ningún usuario podrá ejecutar X server (excepto root).

22. Un ejemplo de los servicios típicos que se suelen deshabilitar:

```
[root@deep] /# rm –f /etc/security/consolo.apps/halt
[root@deep] /# rm –f /etc/security/consolo.apps/poweroff
[root@deep] /# rm –f /etc/security/consolo.apps/reboot
[root@deep] /# rm –f /etc/security/consolo.apps/shutdown
[root@deep] /# rm –f /etc/security/consolo.apps/xserver
```

2.7. DESHABILITAR TODOS LOS ACCESOS A CONSOLA

23. La librería PAM de Linux, instalada por defecto en el sistema , permite al administrador del sistema, elegir que aplicaciones autentifican a usuarios (como la consola de acceso…etc). Para deshabilitar el acceso todos esos accesos a usuarios, se deben comentar las siguientes líneas que se refieren a pam_console en el fichero /etc/pam.d.

24. El siguiente script realizará esta tarea automáticamente. Creando el script disabling.sh como root, (touch disabling.sh) que incluyan las siguientes líneas:

```
# ¡/bin/sh
cd /etc/pam.d
for i in * ; do
sed ´/[^#]. *pam_consle.so/s/^/#/´< $i > foo && mv foo $i
done
```

25. Para realizar el script ejecutable:

```
[root@deep] /# chmod 700 disabling.sh
[root@deep] /# ./disabling.sh
```

26. Este script comentará todas las líneas referentes a pam_console.so de todos los ficheros situados en el directorio /etc/pam.d . Una vez ejecutado el script, se puede eliminar del sistema.

2.8. EL FICHERO INETD /etc/inetd.conf

27. El fichero inetd.conf dice qué puertos deben estar escuchando y que servicio debe estar escuchando en dichos puertos.

28. Lo primero que hay que hacer es definir los servicios que van a ser necesarios y cuales no, para habilitar o deshabilitar dichos puertos, y así evitar posibles agujeros de seguridad.

29. Para ello basta con comentar (#) los servicios que no se vayan a utilizar y mandar un SIGHUP para actualizar dicho fichero de configuración.

    1. Cambiar los permisos de dicho fichero a 600: *[root@deep] /#chmod 600 /etc/inetd.conf*
    2. Asegurarse que el propietario de dicho fichero es root: *[root@deep] /#stat /etc/inetd.conf*
    3. Editar el fichero con vi, y deshabilitar los servicios no necesarios como podrían ser: ftp, telnet, shell, login, exec, talk, ntalk, imap, pop-2, pop-3, finger, auth
    4. Matar el demonio con el que corre el fichero: *[root@deep] /# killall –HUP inetd*
    5. Otra posibilidad de securizar el fichero, es hacerlo inmutable con el comando chattr:
    6. [root@deep] /#chattr +i /etc/inetd.conf

30. Esto evitará cambios accidentales en el fichero, ya que un fichero inmutable, no podrá ser borrado, modificado o renombrado y no se podrán crear enlaces a este fichero (el único que podrá cambiar esta situación es el superusuario root).

2.9. TCP_WRAPPERS

31. Por defecto Red Hat Linux permite todas las peticiones de servicios. La utilización de TCP_Wrappers permitirá securizar los servidores contra intrusiones externas.

32. TCP_Wrappers utiliza los ficheros /etc/hosts.allow y /etc/hosts.deny, para permitir el acceso desde otros servidores.

33. Editar el fichero hosts.deny (*vi /etc/hosts.deny*) y añadir las siguientes líneas (acceso denegado por defecto):

    # Deny access to everyone
    ALL: ALL@ALL, PARANOID

    Que significa que todos los servicios, todos los destinos, que no estén especificados serán bloqueados hasta que no estén permitidos en el fichero de habilitación (hosts.allow).

34. Editar el fichero hosts.allow (*vi /etc/hosts.allow*) y añadir la dirección Ip y el nombre correspondiente al host, al cual se le va a permitir el acceso.

35. El programa *tcpdchk*, es el tcpd wrapper que chequea la configuración. Examina la configuración tcp wrapper y reporta todos los problemas reales y potenciales que encuentre.

    [root@deep] /# tcpdchk

2.10. EL FICHERO /etc/hosts.conf

36. Linux suele utilizar una librería para resolver la equivalencia entre nombre del host y su dirección IP. El fichero /etc/host.conf especifica cómo se resuelven los nombres de los hosts. Las entradas en este fichero especifica qué servicios se deben utilizar y en qué orden para resolver los nombres.

37. Se editará este fichero (vi /etc/hosts.conf) y se añadirán las siguientes líneas:

    #Lookuop names via DNS first then fall back to /etc/hosts.
    order bind, hosts
    #We have machines with multipl IP addresses.
    multi on
    #Check for IP address spoofing.
    nospoof on

38. La opción order indica el orden de los servicios. Se recomienda configurar la librería para que compruebe en primer lugar el nombre del servidor (bind) y luego el fichero de hosts (hosts). (Se deberá tener instalado el software DNS/BIND, o esta configuración no funcionará correctamente).

39. La opción multi, indica que un host que aparece en el fichero /etc/hosts puede tener múltiples direcciones IP o múltiples interfaces ethN.

40. La opción nospoof indica que no se debe permitir el spoofing en esa máquina.

2.11. EL FICHERO /etc/services

41. Los números de los puertos están definidos en la RFC 1700. El fichero /etc/services, permite a los programas servidor y cliente, convertir los nombres de servicio en el número de puerto correspondiente. Esta lista permanecerá en cada host y se guarda en /etc/services. Sólo el usuario root está autorizado a realizar modificaciones en este fichero, y se debería inmunizar el fichero utilizando la opción chattr +i.

2.12. EL FICHERO /etc/securetty

42. El fichero /etc/securetty permite especificar a que dispositivos TTY puede el superusuario root “loguearse”. Este fichero es leído al iniciar la conexión por /bin/login. Su formato es una lista de los nombres de los dispositivos TTY permitidos. Para deshabilitar cualquiera de estas líneas , simplemente hay que comentarla (#). La recomendación es que root sólo se pueda conectar a un tty, y que se tenga que utilizar el comando su para pasar a ser root en otro tty.

2.13. CUENTAS ESPECIALES

43. Es muy importante deshabilitar todas las cuentas que crea por defecto el sistema operativo y no se usan en el sistema. Todo esto se debe comprobar cada vez que se realiza una actualización o se instala un nuevo software.

44. Se da por asumido que se está utilizando shadow password. Esto se puede habilitar bajo la opción de Configuración de Autentificación.

45. Para borrar esos usuarios innecesarios, basta con ejecutar el comando:
    [root@deep] /# userdel username

46. Para borrar un grupo del sistema, ejecutar el comando:
    [root@deep] /# groupdel username

47. Usuarios que normalmente no deben existir: Adm, lp, sync, shutdown, halt, news, uucp, operator, gopher, games (si no se usa el X Window Server), ftp (si no se usa un servidor anónimo de ftp). Si además se quiere borrar el directorio propio de cada usuario, hay que añadir la opción –r al comando userdel.

48. Grupos que normalmente no deben existir: Adm, lp, news, uucp, games (si no se usa el X Window Server), dip, pppusers, popusers (si no se usa un servidor pop para el mail), slipusers.

49. Si es necesario añadir un nuevo usuario al sistema, hay que utilizar el siguiente comando:
    [root@deep] /# useradd username

50. Para añadir o cambiar una contraseña en el sistemas, hay que utilizar el siguiente comando:
    [root@deep] /# passwd username

51. Se pueden securizar estos archivos para prevenir borrados o modificaciones accidentales de estos ficheros (/etc/passwd, /etc/shadow, /etc/group, /etc/gshadow) con la opción ya mencionada chattr +i

2.14. BLOQUEAR su

52. El comando *su* (Substitute User), permite pasar a ser otro de los usuarios existentes en el sistema. Para evitar que cualquiera puede utilizar este comando para pasar a ser root o restringir el comando a ciertos usuarios se deben añadir las siguientes líneas en el fichero su del directorio */etc/pam.d/*. Se recomienda limitar este comando a la cuenta de root.

53. Editar el fichero su (*vi /etc/pam.d/su*) y añadir las siguientes líneas al principio del fichero:
    auth sufficient /lib/security/pam_rootok.so debug
    auth required /lib/security/pam_wheel.so group=wheel

54. Lo que significa que sólo los miembros del grupo wheel puede acceder a su para hacerse root, incluyendo el login (este grupo sería una cuenta especial creada a este efecto).

55. Una vez que está definido el grupo wheel, se deben añadir un usuario permitidos para realizar la operación su y acceder a los privilegios de root:
    [root@deep] /# usermod –G10 admin

- Donde *G* significa la lista de grupos suplementarios
- Donde el usuario es miembro del grupo identificado por el número *10 (wheel)*
- Donde *admin* es el nombre del usuario que queremos añadir al grupo wheel.

2.15. LÍMITE DE RECURSOS

56. El fichero */etc/security/limits.conf* es usado para controlar y limitar los recursos de los usuarios en el sistema. Es importante limitar los recursos de los usuarios para evitar en lo posible ataques de denegación de servicio, por el elevado número de procesos o gasto innecesario de memoria. Estos límites tendrán efecto cuando el usuario entre al sistema.

57. Editar el fichero (*vi /etc/security/limits.conf*) y añadir o cambiar las líneas:

    **hard core 0*
    **hard rss 5000*
    **hard nsproc 20*

58. Estas líneas prohíbe la creación de ficheros de core *-core 0*, restringir el número de procesos *–nsproc 20*, y restringir el uso de memoria a 5megas *-rss 5000*, para cualquiera excepto para el usuario root. (El * indica que aplica a todos los usuarios que entren en el servidor).

59. También hay que editar el fichero */etc/pam.d/login* y añadir la siguiente línea al final del fichero:
    session required /lib/security/pam_limits.so

60. Finalmente editar el fichero */etc/profile* y cambiar la siguiente línea:
    ulimit –c 1000000
    por
    ulimit –S –c 1000000 > /dev/null 2<&1

61. Esta modificación es necesaria para evitar los mensajes de error como: "Unable ro reach limit during login"

2.16. CONTROL DEL MONTAJE DEL SISTEMA DE FICHEROS

62. Se puede lograr mayor control sobre el sistema de ficheros *(/home, /tmp*) con algunas opciones como *noexec, nodev y nosuid*. Esto se puede configurar en el fichero */etc/fstab*, el cual contiene información descriptiva sobre varias opciones de montaje del sistema de *ficheros (defaults, noquota, nosuid, nodev, noexec, quota, ro, rw, suid…*).

63. Después de realizar las modificaciones oportunas en función de nuestras necesidades, se deben ejecutar los siguientes comandos para que tengan efecto las modificaciones (por ejemplo):

    [root@deeep] /#mount –oremount /home/
    [root@deeep] /#mount –oremount /tmp/

2.17. OCULTACIÓN RPM BINARIOS

64. Una vez instalado todo el software necesario en el sistema Linux con el comando RPM, es buena idea mover todo a un lugar seguro como un disco especial…etc. Esto tiene la intención de evitar la instalación de software malicioso (troyanos) vía RPM. Si en un futuro se necesita reinstalar nuevo software, es necesario volver a colocar el RPM binario en su fichero original. Para mover el RPM binario a un disquete, utilizar:

    [root@deep] /# mount /dev/fd0 /mnt/floppy
    [root@deep] /# mv /bin/rpm /mnt/floppy
    [root@deep] /# umount /mnt/floppy

65. Nunca se debe desinstalar el programa RPM completamente del sistema (no habrá forma de instalar nada). Otra opción es modificar los permisos del comando rpm, de 755 a 700. De esta forma un usuario que no sea root, no tendrá forma de instalar ningún paquete rpm:
    [root@deep] /# chmod 700 /bin/rpm

2.18. SHELL LOGGING

66. Para facilitar el uso de los comandos, la shell bash, mantiene un fichero con el histórico de las últimas 500 entradas efectuadas para cada usuario en */.bash_history* (en el directorio de cada usuario). Reduciendo este número de comandos, se puede limitar la posibilidad de descubrir passwords introducidas por error en texto plano, almacenadas por mucho tiempo en este archivo.

67. Las líneas *HISTFILESIZE* y *HITSIZE* del fichero */etc/profile*, determinan el tamaño de estos comandos antiguos. Se recomienda para todos los usuarios cambiar estos tamaños a un valor de 20. Editando el fichero (*vi /etc/profile*) podremos cambiara las líneas correspondientes:
    HISTFILESIZE=20
    HISWTSIZE=20
68. El administrador debería añadir en el fichero */etc/skel/.bash_logout* una línea como
    rm –f $HOME/.bash_history
    para que cada vez que un usuario salga del sistema se borre el historial de comandos utilizados.

69. Todo esto sería efectivo para los nuevos usuarios que se crearan, para los usuarios que ya están creados, se debería editar su propio .bash_logout e incluir la línea indicada manualmente.

2.19. EL FICHERO LILO.CONF

70. LILO es el sistema de arranque más utilizado en Linux, puede manejar los procesos de arranque y puede arrancar imágenes del kernel desde disquete, discos duros o incluso arrancar otros sistemas operativos.

71. El fichero de configuración del LILO es */etc/lilo.conf* . Se deben añadir algunas líneas para mejorar su seguridad:

    - Añadir la siguiente línea:
      timeout=00

      Indica cuantos segundos tiene que esperar el sistema antes de reiniciar el sistema después de la selección por defecto. (Requisito C2).

    - Añadir la siguiente línea:
      restricted

      Esta opción pregunta por la contraseña si se requieren parámetros en la línea de comandos.

    - Añadir la siguiente línea:
      password=<password>

      Esta opción pregunta al usuario la contraseña cuando intenta cargar Linux. Las contraseñas son sensibles a mayúsculas. Además hay que asegurar que el fichero */etc/lilo.conf* no es legible por todo el mundo, ya que la línea password, contiene una contraseña sin encriptar, por lo que sólo debe ser visible por el superusuario.
      [root@deep] /# chmod 600 /etc/lilo.conf

72. Ahora se debe actualizar la configuración de lilo para que los cambios tengan efecto:

    [root@deep] /# /sbin/lilo –v

73. Una medida adicional de seguridad sobre este archivo es hacerlo inmutable (mediante el comando ya mencionado *chattr +i*)

2.20. DESHABILITAR CTRL+ALT+SUPRIMIR

74. Para deshabilitar este comando, basta con comentar la línea correspondiente en el fichero */etc/inittab*.

75. Esta opción es muy importante si no se dispone de seguridad física suficiente. Para realizarlo editar el fichero (*vi /etc/inittab*) y cambiar la siguiente línea:

    ca::*ctrlaltdel* : /sbin/shutdown –t3 –r now

    y comentarla.

    #ca::ctrlaltdel : /sbin/shutdown –t3 –r no w

76. Para que los cambios tomen efecto es necesario ejecutar el siguiente comando:

    [root@deep] /# /sbin/init q

2.21. COPIAS DE SEGURIDAD DE LOGS

77. Una de las consideraciones más importantes de seguridad es la integridad del sistema de logs en */var/log*.

78. Una de las opciones en colocar estos ficheros en un lugar seguro, pero cualquier intruso puede conseguir privilegios y conseguir el acceso a los mismos. Otra opción es obtener un copia física (papel) de estos archivos (*/dev/lp0*), modificando el fichero */etc/syslog.conf* añadiendo la siguiente línea:
    authpriv.;mail.*;local17.*;auth.*;daemon.info /dev/lp0*

79. Y resetear el demonio del syslog para que los cambios tengan efecto:

    [root@deep] /# /etc/rc.d/init.d/syslog restart

80. Por defecto el demonio del syslog no recibe ningún mensaje desde la red, se debe habilitar esta facilidad. Para ello hay que añadir la opción –r al script del demonio syslog (*vi +24 /etc/rc.d/init.d/syslog*) y cambiar :

    daemon syslogd –m 0

    por

    daemon syslogd –r –m 0

81. Luego se debe reiniciar el demonio para que los cambios tengan efecto:
    [root@deep] /# /etc/rc.d/init.d/syslog restart

2.22. SCRIPTS /etc/rc.d

82. Al fijar los permisos de los scripts, se deben arrancar y parar todos los procesos normales necesarios a la hora de arranque del sistema.

    *[root@deep] /# chmod –R 700 /etc/rc.d/init.d/**

83. De esta forma se limita a que sólo el superusuario puede ver, ejecutar y modificar los scripts.

84. Por defecto cuando se inicia Linux, se puede ver la versión de distribución, versión de kernel y nombre del servidor (demasiada información). Para evitar esto, se debe ocultar la información que deseemos comentado las líneas deseadas del fichero */etc/rc.d/rc.local*

85. A continuación se deben borrar los siguientes ficheros (issue.net e issue) de */etc*:

    [root@deep] /# rm – f /etc/issue
    [root@deep] /# rm –f /etc/issue.net

Nota: el fichero */etc/issue.net*, es el banner de login que se muestra a los usuarios que se conectan vía telnet, SSH.

2.23. BITS DE PROGRAMS DE ROOT

86. Un usuario normal puede ejecutar programas como root, si es capaz de poner el SUID de root en dichos programas. (-rwsr-xr-x SUID o –r-xr-sr-x SGID). Por ello es necesario eliminar los bits de estos programas propietarios de root (*chmod a-s file_name*), pero hay programas o ficheros que necesitan tener estos privilegios.

87. Para encontrar los ficheros que tienen estos bits activos, podemos utilizar:

    [root@deep]/# find / -type f \ (-perm –04000 –o –perm –02000 \) \-exec

88. Algunos de los ficheros en los que se deben quitar estos bits en :

/usr/bin:
chage, gpasswd, wall, chfn, chsh, newgrp, write

/usr/sbin:
usernetctl, traceroute

/bin:
mount, umount, ping
/sbin:
netreport

2.24. PARÁMETROS DEL KERNEL

89. A partir de la versión 6.2 de Red Hat, todos los parámetros del kernel se encuentran en */proc/sys*, pero también se puede utilizar el archivo */etc/sysct1.conf* para modificar y configurar estos parámetros. Este fichero es leído y cargado cada vez que el sistema se inicia, por lo que las modificaciones a realizar en */proc/sys*, se harán por medio del fichero */etc/sysct1.conf*, porque se tiene mayor control y se ejecuta antes del rc.local u otros scripts de usuario.

2.25. CONFIGURACIÓN DEL SISTEMA ANTE PETICIONES PING

90. Prevenir al sistema de la ejecución externa de ping y que nuestros sistema no responda , es una medida más de seguridad. El protocolo TCP/IP realiza diferentes saltos antes de llegar a su objetivo, que puede proporcionar mucha información a un atacante. Para ello:

    [root@deep] /#echo 1 > /proc/sys/netipv4/icmp_echo_ignore_all

91. También se debe añadir esta línea en el fichero */etc/rc.d/rc.local* , para que se ejecute cada vez que se inicia el sistema.

Nota. Esto es para la versión 6.1

92. Para la versión 6.21, se debe editar el fichero */etc/sysctl.conf* y añadir la siguiente línea:

    # Enable ignoring ping requets
    net.ipv4.icmp_echo_ignore_all = 1

93. Para que los cambios tengan efecto se debe reiniciar la red:

    [root@deep] /# /etc/rc.d/init.d/network restart

2.26. RESPUESTA ANTE PETICIONES DE BROADCAST

94. Como a la petición de ping, es necesario deshabilitar la respuesta a una petición de broadcast. Cuando llega un paquete a la dirección de broadcast de una red (***.***.***.255), el paquete es reenviado a todas las máquinas de la red. Entonces las máquinas de la red, responderían con un paquete ICMP echo request y puede producir una congestión de la red (DOS).

    [root@deep] /# echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcast

95. Se debería añadir esta línea en el fichero */etc/rc.d/rc.local* , para que se ejecute cada vez que el sistema reinicie.

Nota: Esto es para la versión 6.1.

96. Para la versión 6.2, también se editará el fichero */etc/sysctl.conf* y se añadirá la siguiente línea:

    #enable ignoring broadcasts requets
    net.ipv4.icmp_echo_ignore_broadcasts = 1

97. Para que los cambios tengan efecto, se debe reiniciar la red:

    [root@deep] /# /etc/rc.d/init.d/network restart

2.27. PROTOCOLOS DE ROUTING

98. Los protocolos de routing pueden generar serios problemas de seguridad. Por ello se recomienda la deshabilitación del IP routing, para ello hay que ejecutar el siguiente comando:

    [root@deep] /# for f in /proc/sys/net/ipv4/conf//accept_source_routing*
    >echo 0 > $f
    >done

    [root@deep] /#

99. Se pueden añadir los comandos indicados en el script */etc/rc.d/rc.local* , para poder automatizar esta opción.

Nota: Esto es para la versión 6.1.

100. Para la versión 6.2, también se editará el fichero /etc/sysctl.conf y se añadirá la siguiente línea:

    # Disables IP source routing
    net.ipv4.conf.all.accept_source_route = 0

101. Para que los cambios tengan efecto se debe reiniciar la red:

[root@deep] /# /etc/rc.d/init.d/network restart

Nota: esto deshabilitará Source Routed Packets en todos los interfaces lo, ethN, pppN…etc.

2.28. PROTECCIÓN ANTE TCP SYN COOKIE

102. Un ataque de SYN, es un ataque de DoS que consume todos los recursos de la máquina, forzando al reinicio de la máquina.

[root@deep] /# echo 1 > /proc/sys/netipv4/tcp_syncookies

103. Se pueden añadir el comando indicado en el script */etc/rc.d/rc.lo*cal , para poder automatizar esta opción.

Nota: Esto es para la versión 6.1

104. Para la versión 6.2, también se debe editar el fichero /etc/sysctl.conf y añadir la siguiente línea:

 # Disables TCO SYN Cookie Protection
net.ipv4.tcp_syncookies = 1

105. Para que los cambios tengan efecto se debe reiniciar la red:

[root@deep] /# /etc/rc.d/init.d/network restart

106. Si se produce algún mensaje de error durante el reinicio, hay que comprobar que están habilitadas las TCP syncookies en la configuración del kernel.

2.29. DESHABILITAR LA REDIRECCIÓN ICMP

107. Cuando los host utilizan las rutas por defecto para llegar a un destino, la redirección de paquetes está habilitada, y los routers la utilizan para informar a los host de la ruta que deben seguir. Este es un agujero de seguridad que puede utilizar un atacante para modificar la tabla de rutas.

108. Por lo que se recomienda deshabilitar la Aceptación de la Redirección de Paquetes ICMP:

109. Se pueden añadir los comandos en el script */etc/rc.d/rc.local* , para poder automatizar esta opción.

[root@deep] /# for f in /proc/sys/net/ipv4/conf//accept_redirects;*
> echo 0 > $f
> done
[root@deep] /#

Nota: (versión 6.1)

110. Para la versión 6.2, también se debe editar el fichero */etc/sysctl.conf* y añadir la siguiente línea:

 # Disables ICMP Redirect Acceptance
net.ipv4.conf.all.accept_redirects = 0

111. Para que los cambios tengan efecto se debe reiniciar la red:

[root@deep] /# /etc/rc.d/init.d/network restart

Nota: esto deshabilitará Source Routed Packets en todos los interfaces lo, ethN, pppN…etc.

2.30. PROTECCIÓN DEFRAGGING

112. Para la versión 6.1, esta protección debe estar activa si el servidor actúa como gateway para enmascarar tráfico interno.

113. Se puede añadir el comando en el script */etc/rc.d/rc.local* , para poder automatizar esta opción.

[root@deep] /# echo 1 > /proc/sys/net/ipv4/ip_always_defrag

114. Para la versión 6.2, también se debe editar el fichero */etc/sysctl.conf* y añadir la siguiente línea:

 # Enable always defragging Protection
net.ipv4.ip_always_defrag = 1

115. Para que los cambios tengan efecto se debe reiniciar la red:

[root@deep] /# /etc/rc.d/init.d/network restart

2.31. HABILITAR LA PROTECCIÓN ANTE MENSAJES DE ERROR

116. Para la versión 6.1, esta protección avisará de la existencia de mensajes de error en la red.

117. Se puede añadir el comando en el script */etc/rc.d/rc.local* , para poder automatizar esta opción.

[root@deep] /# echo 1 > /proc/sys/net/ipv4/icmp_ignore_bogus_error_responses = 1

118. Para la versión 6.2, también se debe editar el fichero */etc/sysctl.conf* y añadir la siguiente línea:

 # Enable bad error message Protection
net.ipv4.icmp_ignore_bogus_error_responses = 1

119. Para que los cambios tengan efecto se debe reiniciar la red:

[root@deep] /# /etc/rc.d/init.d/network restart

2.32. HABILITAR LA PROTECCIÓN ANTE IP SPOOFING

120. Para la versión 6.1, esta protección previene de posibles ataques a la red de suplantación de la fuente que puede dar lugar a ataques de DoS.

121. Se puede añadir los comandos en el script */etc/rc.d/rc.local* , para poder automatizar esta opción.

[root@deep] /# for f in /proc/sys/net/ipv4/conf//rp_filter; do*
> echo 1 > $f
> done
[root@deep] /#

122. Para la versión 6.2, también se debe editar el fichero */etc/sysctl.conf* y añadir la siguiente línea:

 # Enable IP Spoofing protection, turn on Source Address Verification
net.ipv4.conf.all.rp_filter = 1

123. Para que los cambios tengan efecto se debe reiniciar la red:

[root@deep] /# /etc/rc.d/init.d/network restart

2.33. LOGS DE PAQUETES SUPLANTADOS, ENRUTAMIENTO Y PAQUETES REDIRIGIDOS

124. Para la versión 6.1, esta protección guardará un log de los paquetes suplantados, paquetes reenrutados de la fuente, y de paquetes redirigidos.

125. Se puede añadir los comandos en el script */etc/rc.d/rc.local* , para poder automatizar esta opción.

```
[root@deep] /# for f in /proc/sys/net/ipv4/conf/*/log_martians; do
> echo 1 > $f
> done
[root@deep] /#
```

126. Para la versión 6.2, también se debe editar el fichero */etc/sysctl.conf* y añadir la siguiente línea:

```
# Log Spoofed Packets, Source Routed Packets, Redirect Packets
net.ipv4.conf.all.log_martians = 1
```

127. Para que los cambios tengan efecto se debe reiniciar la red:

```
[root@deep] /# /etc/rc.d/init.d/network restart
```

2.34. FICHEROS INUSUALES U OCULTOS

128. Es muy importante buscar en cualquier parte del Sistema, ficheros inusuales u ocultos que normalmente no suelen mostrarse con el comando ls, y pueden ser utilizados para ocultar información o programas de crakeo de contraseñas…etc. A veces se suelen guardar en directorios inusuales o con nombres raros como '..' o '..^G'. Se puede utilizar el programa find para buscar este tipo de ficheros ocultos.

```
[root@deep] /# find / -name ".. " –print -xdev
[root@deep] /# find / -name ".* " –print –xdev | cat –v
```

A veces incluso ficheros acabados con .xx o .mail (que aparentemente son normales).

129. Los Ficheros SUID o SGID, son potencialmente el principal objetivo de los atacantes, ya que pueden conseguir privilegios a través de ellos. Suelen aprovecharse de programas SUID y dejarlos como puertas traseras para una posterior entrada al sistema.

130. Se puede llevar un registro con los programas que tengan estos bits activos y su control de posibles cambios:

```
[root@deep] /# find / -type f \( -perm –04000 –o –perm –02000 \) \-exec ls –l
```

131. Otro de los agujeros de seguridad son los ficheros, directorios, abiertos a escritura por todos los usuarios o por todos los grupos, donde un atacante puede alojar sus programas, para encontrarlos:

[root@deep] /# find / -type f \(-perm –2 –o –perm –20 \) \-exec ls –l
[root@deep] /# find / -type d \(-perm –04000 –o –perm –02000 \) \-exec ls –l

132. No hay que permitir ningún fichero sin propietario, si existen es posible que un atacante haya entrado al sistema. Si se encuentra alguno, hay que verificar su integridad y o bien eliminar o bien asignarle un propietario (a veces se crean al desinstalar algún programa):

[root@deep] /# find /home –name .rhosts

2.35. PERMISOS DE FICHEROS CRÍTICOS

133. A continuación se detallan algunos de los ficheros críticos del sistema que deben tener permisos de escritura, lectura determinados:

Fichero	**Permisos**
/var/log	751
/var/log/messages	644
/etc/crontab	600
/etc/syslog.conf	640
/etc/logrotate.conf	640
/var/log/wtmp	660
/var/log/lastlog	640
/var/ftpusers	600
/etc/passwd	644
/etc/shadow	600
/etc/pam.d	750
/etc/hosts.allow	600
/etc/hosts.deny	600
/etc/lilo.conf	600
/etc/securetty	600
/etc/shutdown.allow	400
/etc/security	700
/etc/rc.d/init.d	750
/etc/init.d	750
/etc/sysconfig	751
/etc/inetd.conf	600
/etc/cron.allow	400
/etc/cron.deny	400
/etc/ssh	750
/etc/sysct1.conf	400

ANEXO A. LISTA DE COMPROBACIÓN

APARTADO	OK / NOK	OBSERVACIONES
Bios		
Elección de Clave Correcta		
Cuenta de root		
Fichero /etc/exports		
Programa Acceso a Consola		
Accesos a Consola		
Fichero /etc/inetd.conf		
TCP_Wrappers		
Fichero /etc/hosts.conf		
Fichero /etc/services		
Fichero /etc/securetty		
Cuentas especiales		
Bloqueo su		
Límite de Recursos		
Control de Montaje de Sistema de Ficheros		
Ocultación RPM Binarios		
Shell Logging		
Fichero lilo.conf		
Deshabilitación ctrl+alt+supr		
Bits de Programas		
Parámetros del Kernel		
Configuración ante peticiones PING		
Configuración ante peticiones BROADCAST		
Protocolos de Routing		
Protección ante TCP SYN Cookie		
Deshabilitación de redirección ICMP		
Protección Defragging		
Protección ante Mensajes de Error		
Protección ante IP Spoofing		

Logs de paquetes, suplantación y enrutamiento de paquetes		
Ficheros inusuales u ocultos		
Permisos de Ficheros Críticos		