CONTROL DE PERMISOS DE ARCHIVOS Y ATRIBUTOS

Monitorear los permisos del sistema de archivos, es crucial para mantener la integridad del sistema.

Revise el sistema periódicamente, en busca de permisos "setuid" o "setgid", no autorizados o innecesarios. Considere que los programas con "setUID root", se corren como superusuario independientemente de quién los ejecute, y son causa frecuente de "buffer overflows". SetUID root se usa normalmente, para permitir que cualquier usuario pueda realizar ciertas acciones, que de otro modo sólo podrían ser ejecutadas por el administrador. Busque programas sospechosos, y quíteles setuid o setgid, usando chmod:

```
root# find / -type f -perm +6000 -ls
59520 30 -rwsr-xr-x 1 root root 30560 Apr 15 2001 /usr/bin/chage
59560 16 -r-sr-sr-x 1 root lp 15816 Jan 6 2001 /usr/bin/lpq
root# chmod -s /usr/bin/chage /usr/bin/lpq
root# ls -l /usr/bin/lpq /usr/bin/chage
-rwxr-xr-x 1 root root 30560 Apr 15 2001 /usr/bin/chage
-r-xr-xr-x 1 root lp 15816 Jan 6 2001 /usr/bin/lpq
```

Los archivos con atributos de escritura para todos, pueden ser alterados o borrados con facilidad, búsquelos todos:

```
root# find / -perm -2 ! -type l –ls
```

En el transcurso de la operación, verá varios archivos; entre ellos varios dentro de /dev/, e incluso el directorio /tmp. Busque e identifique los archivos que no tienen un dueño o pertenecen a un grupo. Podrían haber sido creados por algún intruso:

```
root# find / -nouser -o –nogroup
```

Si utiliza los comandos lsattr y chattr, el superusuario puede modificar las características de archivos y directorios, incluyendo su alteración o borrado, mejor que al usar chmod. Utilizar los atributos "appendonly" (sólo agregar contenido) e immutable, pueden ser bastante efectivos para proteger los logs (registros de actividad) de ser borrados, o evitar que pueda incorporarse código malicioso, a los binarios críticos del sistema. Aunque esto no garantiza que los archivos no puedan ser modificados, exige al menos que se tenga cuenta de root para hacerlo. El comando chattr se usa para fijar o quitar estos atributos, mientras que lsattr se usa para listarlos. Fijando el modo "append-only"a los logs del sistema, los datos que se agregan, no se podrán borrar. Aunque esta práctica requiere modificar los scripts de rotación de logs, puede ayudar a evitar que un eventual intruso, borre sus huellas. Una vez que se rotan los logs, deberían ponerse en *modo* "immutable". Es util modificar en este sentido, aquellos archivos que no se cambian a menudo, como /bin/login, /bin/rpm o /etc/shadow.

```
# chattr +i /bin/login
# chattr +a /var/log/messages
# lsattr /bin/login /var/log/messages
----i--- /bin/login
-----a-- /var/log/messages
```

Ningún usuario, debiera poder correr programas con setuid, desde su directorio home. Utilice la opcion nosuid en el archivo /etc/fstabs, para las particiones que puedan ser escritas por usuarios distintos de root. Puede usar tambien nodev y noexec, en particiones que contengan homes de usuarios, o incluso en /var, lo cual impide la ejecución de programas y la creación de dispositivos de caracteres o de bloques, lo cual nunca debiera ser necesario. Consulte las páginas del manual de mount, para obtener más información.

SERVICIOS INNECESARIOS

Una de las mejores maneras de evitar compromisos remotos de seguridad, es deshabilitar los servicios que no es necesario proveer. Muchos de los servicios que se dejan habilitados por defecto en la configuración del metademonio inetd, no se usarán casi nunca. Desactive los que no necesite, comentando la línea correspondiente en el archivo /etc/inetd.conf

Encontrará scripts de ejecución de servicios por runlevel, en `/etc/rc*.d` o en `/etc/rc.d/rc*` -según la distribución-. Mueva esos enlaces, renombre o borre, o incluso desinstale el paquete correspondiente. En RedHat puede usar `/sbin/chkconfig --list` para ver qué servicio corre en cada runlevel. Para quitarlos, use `/sbin/chkconfig --del servicio`. Válgase de `netstat -a -p --inet`, de `ps`, y de los port scanners, para determinar qué servicios corre.

USO DE RPM Y DPKG

El uso de /bin/rpm en RedHat u otras basadas en aquella, y de /usr/bin/dpkg en Debian y derivadas, es la clave en la administración de los paquetes de software del sistema. Sea cauto al utilizar las correspondientes herramientas de actualización automática, como AutoRPM, AptRPM, Up2date o AptGet.

- Para quitar un paquete:

```
#rpm -e <paquete>
#dpkg -r <paquete>
```

- Listar los contenidos del paquete:

```
#rpm -qvl <paquete.rpm>
#dpkg -c <paquete.deb>
```

- Listar los paquetes con su información:

```
#rpm -qvia
#dpkg –l
```

- Ver la información de un paquete:

```
#rpm -qpi <paquete.rpm>
#dpkg -I <paquete.deb>
```

- Verificación básica de integridad:

```
#rpm -Va
#debsums –a
```

- Averiguar a qué paquete pertenece un archivo:

```
#rpm -qf </trayecto/al/archivo>
#dpkg -8 </trayecto/al/archivo>
```

- Instalar un nuevo paquete:

```
#rpm -Uvh <paquete.rpm>
#dpkg -i <paquete.deb>
```

CONFIGURACIÓN DE TCP WRAPPERS

Estas reglas se usan a menudo para monitorear y controlar, el acceso a los servicios listados en el archivo /etc/inetd.conf. Si algún servicio se corre como "standalone", sin depender del superdemonio, tcpwrapers no podrá controlar su actividad. Si necesita por ejemplo, "recubrir" (horrible traducción de wrapear :) su in.ftpd:

```
ftp tcp nowait root /usr/sbin/tcpd in.ftpd -l -L -i –o
```

Antes de que un demonio de servicios sea invocado ante una petición, tcpd se asegurará de verificar que el origen del paquete, es un host permitido. Los intentos de conexión, se envían al syslogd. Todos los servicios deben estar deshabilitados en el archivo *host.deny*:

```
ALL:ALL
```

Para enviar un mail al administrador del sistema cada vez que se note un intento fallido de conexión:

```
ALL: ALL: /bin/mail -s "%s intento de conexión de %c"
admin@sudominio.com
```

Habilite servicios en específico en /etc/host.allow usando el nombre del servicio, seguido por la información del host:

```
sshd: clienta24.seguros.com, ripper.seguros.com
in.ftpd: 192.168.1.
```

El punto al final, indica que toda esa red estará autorizada. Use `tcpdchk` para verificar sus archivos de acceso. El control de acceso funciona asi:

1- El acceso a un servicio se garantiza, si el host encaja en las definiciones de `host.allow`.

2- Si el servicio está especificamente denegado para el host en cuestión, se rehusará la conexión

3- De otro modo, se garantizará el acceso al servicio.

Si en su sistema no se han creado archivos de control de acceso, se interpretará su contenido como vacío, de modo que el control de acceso al host, quedará desactivado!!!

CONFIGURACIÓN DE SYSLOG

El syslogd, es un demonio encargado de capturar y llevar registro, de los mensajes generados por los diferentes procesos durante su ejecución, mientras que por su parte, klogd es el responsable de hacer lo propio, pero con los mensajes generados por el kernel. Los registros de actividades (también puede encontrarlos como bitácoras, cuadernos, o nombres peores ;) serán en la mayoría de los casos, indicadores primarios de los problemas que pudieran presentarse en su sistema. Incluso hay quienes guardan sus logs... en /dev/lp0.

Ajuste su archivo de configuracion de syslogd, /etc/syslog.conf, para que envíe información de tipo específico a archivos específicos, para que pueda ser leída y analizada con más sencillez y velocidad.

```
#monitorear intentos de autentificación
auth.*; authpriv.* /var/log/authlog

#auditar todos los mensajes del kernel
kern.* /var/log/kernlog

#monitorear todas las advertencias y mensajes de error
*.warn; *.err /var/log/syslog

#enviar una copia a un host de logs remoto. Configure el script #de
inicio de syslogd para que corra con las opciones -r -s
#dominio.com en su servidor de logs. Asegúrese de que el nivel #de
seguridad en su servidor de logs, sea bueno, cuando menos.
*.info @loghost
auth.*; authpriv.* @loghost
```

Restrinja el acceso a los directorios de logs y de syslog a sus usuarios normales, usando:

```
#chmod 751 /var/log /etc/logrotate.d
#chmod 640 /etc/syslog.conf /etc/logrotate.conf
#chmod 640 /var/log/*.log
```

SEGURIDAD EN DNS

Las transferencias de zona, sólo debieran permitirse en servidores maestros que actualizan la información de zona (dominio), es sus servidores esclavos. No hacerlo de ese modo, puede permitir que hosts no autorizados, obtengan información de nombres de hosts e Ips. Restrinja las peticiones sólo a dominios públicos. Configuración para un servidor con zonas públicas y privadas:

```
<Directory />
Options None
// Permite trasnferencias solo a su servidor de nombres esclavo.
// Solo permite peticiones de la red 192.168.1.0.
zone "midominio.com" {
type master;
file "master/db.midominio.com";
allow-transfer {192.168.1.6; };
allow-query {192.168.1.0/24; };
};
```

Rechaze y guarde un registro, de las peticiones de versión que se le hagan, excepto desde su propio host. Obtener el número de versión de BIND que corre, ayudará a los intrusos a determinar qué tipo de ataque dará buenos resultados con su servidor de nombres:

```
// Impide saber qué versión de BIND está usando
zone "bind" chaos {
type master;
file "master/bind";
allow-query {localhost; };
};
```

El archivo *.master/bind*, deberá contener entonces:

```
$TTL 1d
@ CHAOS SOA localhost. root.localhost. (
1 ; serial
3H ; refresh
15M ; retry
1W ; expire
1D ) ; minimum
NS localhost.
```

Controle a qué interfaces escucha su named, para evitar exponerlo a interfaces en los que no es necesario:

```
listen-on { 192.168.1.1; };
```

Use Listas de Control de Acceso, para agrupar hosts, según criterios de confiabilidad. La etiqueta de ACL "internal", permite un mayor grado de acceso a la información por parte de los hosts que incluye. Para usarla, debe estar definida:

```
acl "internal" {
{192.168.1.0/24; 192.168.2.11; };
};
```

Luego, puede ser usada en declaraciones de zona o en las opciones:

```
zone "inside.mynet.com" {
type master;
file "master/inside.mynet.com";
allow-query {"internal"; };
};
```

SEGURIDAD DE APACHE

Limitar Apache para que atienda sólo la interface local, agregando en `/etc/httpd/httpd/conf` la linea:

```
Listen 127.0.0.1:80
```

Usar las siguientes líneas para desactivar el acceso al sistema de archivos por defecto, a menos que sea expresamente permitido. Esto desactiva la impresión del índice de contenidos si no existe el archivo index.html, Server Side Include y links simbólicos. Desactivar los links simbólicos puede impactar en la performance de sitios grandes:

```
<Directory />
Options None
AllowOverride None
Order deny,allow
Deny from all
</Directory>
```

Use las siguientes líneas para restringir el acceso al servidor solo a direcciones determinadas:

```
<Directory /home/httpd/html>
# Deny all accesses by default
Order deny,allow
# Allow access to local machine
Allow from 127.0.0.1
# Allow access to entire local network
Allow from 192.168.1.
# Allow access to single remote host
Allow from 192.168.5.3
# Deny from everyone else
Deny from all
</Directory>
```

Asegúrese de reiniciar Apache para probar los cambios

ARCHIVOS CRÍTICOS DEL SISTEMA

Archivo/Directorio	Perm.	Descripción
/var/log/	751	Dir. conteniendo todos los archivos log
/var/log/messages	644	Mensajes del sistema
/etc/crontab	600	Archivo crontab de todo el sistema
/etc/syslog.conf	640	Configuración del demonio syslog
/etc/logrotate.conf	640	Controla la rotación de los archivos log
/var/log/wtmp	660	Quien está loggeado ahora, use who
/var/log/lastlog	640	Quién se ha loggeado anteriormente. Use last
/etc/ftpusers	600	Listado de usuarios excluidos del ftp
/etc/passwd	644	Listado de las cuentas del sistema
/etc/shadow	600	Contiene los passwords de las cuentas
/etc/pam.d/	750	Archivos de configuración de PAM
/etc/hosts.allow	600	Archivo de control de acceso
/etc/hosts.deny	600	Archivo de control de acceso
/etc/lilo.conf	600	Archivo de configuración del gestor de arranque
/etc/securetty	600	Interfaces tty que permiten logins de root
/etc/rc.d/init.d/	750	Archivos de inicio en sistemas RedHat
/etc/init.d/	750	Archivos de inicio en sistemas Debian
/etc/sysconfig/	751	Configuración del sistema y la red en RedHat.
/etc/inetd.conf	600	Archivo de configuración del superservidor Inetd
/etc/cron.allow	400	Listado de usuarios que pueden usar cron
/etc/cron.deny	400	Listado de usuarios que no pueden usar cron
/etc/ssh/	750	Archivos de configuración de Secure Shell
/etc/sysctl.conf	400	Opciones de optimización del kernel en RedHat

RECURSOS EN LA WEB.

Apache: directorios y protección con passwords
http://www.apacheweek.com/features/userauth
http://www.apache-ssl.org/

BastilleLinux
http://www.bastille-linux.org

Bugtraq:
http://www.securityfocus.com/forums/bugtraq/intro.html

CERT: Módulos para mejoras de seguridad
http://www.cert.org/security-improvement

Detección de Intrusos
http://www.linuxsecurity.com/intrusion-detection

Introducción a la seguridad en Linux
http://www.linux-mag.com/1999-10/security_01.html

John the Ripper, el destripador de passwords
http://www.openwall.com/john

Linux Security
http://www.linuxsecurity.com

Nmap, escaneador de puertos
http://www.insecure.org/nmap

OpenSSH: herramienta segura de acceso remoto
http://www.openssh.com

Proyecto de seguridad OpenWall
http://www.openwall.com

Protocolo NTP (Network Time Protocol)
http://www.ntp.org

Utilidad de Transferencia Incremental de Archivos
http://rsync.samba.org

Herramienta de control de acceso a root sudo
http://www.courtesan.com/sudo

Snort, sistema de detección de intrusos
http://www.snort.org

Tripwire, herramienta de integridad de archivos
http://www.tripwiresecurity.com

Uso de Snort
http://www.linuxsecurity.com/using-snort.html

DMIRE

RedULA

La intención principal de esta Referencia Rápida, es constituirse en un punto de partida para mejorar la seguridad de su sistema y buscar información más profunda al respecto. No puede reemplazar de modo alguno, la lectura exhaustiva de la abundante documentación ya existente, sobre la seguridad de los sistemas Linux.