25 consejos para aumentar la seguridad en Linux

TecMint 26-Ago-2013

Tweet
Compartir

Hoy en día, Linux es un software operativo libre y de código abierto que se distribuye bajo la licencia pública general GNU. Celebrando sus 22 años, TecMint publicó 25 consejos para aumentar la seguridad en estos sistemas.

En 1991, Linus Torvalds tuvo como objetivo crear un sistema operativo que funcionara igual que UNIX. Primero, bajo el nombre de Freax, el 26 de agosto de 1991, crea la versión 0.01 de Linux (renombrado así por Ari Lemmke). Después de varias pruebas y versiones, en marzo de 1994 se lanzó la versión 1.0.

Más adelante, en 1996 se eligió la mascota oficial, un pingüino que puede tener distintas versiones, siempre y cuando se reconozca la autoría del diseñador.

Criticado por falta de controladores y compatibilidad, paulatinamente Linux continúa mejorando y, actualmente, IBM, Intel Corporation, Hewlett-Packard, Dell o MIPS Technologies tiene programadores que emplean el sistema operativo para los equipos que fabrican.

A continuación te mostramos un resumen de los 25 consejos enlistados:

- **1 Seguridad física del sistema**

Configurar el BIOS para deshabilitar el arranque por CD/DVD, dispositivos externos y diskettes. Después, habilitar la contraseña del BIOS y proteger el archivo GRUB con contraseña para restringir el acceso físico al sistema.

- **2 Disco particionado**

Es importante contar con diferentes particiones para conseguir mayor seguridad de los datos en caso de que algún desastre ocurra. Al crear diferentes particiones, los datos pueden ser separados o agrupados según su tipo. Cuando un accidente ocurre, solo los datos de la partición afectada deberán ser remplazados, mientras que los datos en otras particiones no se verán afectados.

Asegúrate de tener las siguientes particiones e instalar todas las aplicaciones de terceros en la partición /opt

/
/boot
/usr
/var
/home
/tmp
/opt

- **3 Minimizar paquetes para minimizar vulnerabilidades**

¿Realmente necesitas todos los servicios instalados- se recomienda evitar instalar paquetes que no se utilizan para evitar las vulnerabilidades de esos paquetes. Esto minimiza el riesgo de que comprometan un servidor.

Identifica y elimina los servicios y programas innecesarios en el servidor para minimizar vulnerabilidades. Utiliza el comando "***chkconfig***" para identificar los servicios que están corriendo en runlevel3

```
# /sbin/chkconfig --list |grep '3:on'
```

Una vez identificado el servicio incensario, es posible deshabilitarlo con el siguiente comando

```
# chkconfig serviceName off
```

Utiliza el adiestrador de paquetes RPM, yum o apt-get, para listar todos los paquetes instalados en el sistema y remover aquellos que no son necesarios con el siguiente comando:

```
# yum -y remove package-name
```

```
# sudo apt-get remove package-name
```

- **4 verifica los puertos de red que escuchan conexiones**

Con la ayuda del comando "***netstat***" es posible listar todos los puertos abiertos y los programas que los utilizan. Es posible utilizar el comando "***chkconfig***" para deshabilitar todos los servicios de red no deseados en el sistema.

```
# netstat -tulpn
```

- **5 Utiliza Secure Shell (SSH)**

Los protocolos Telnet y rlogin utilizan texto plano para el envío de la información, en cambio, Secure Shell es un protocolo seguro ya que utiliza cifrado en todas las comunicaciones entre equipos.

Nunca inicies sesión directamente como root, a menos que sea sumamente necesario. Utiliza el comando "sudo" para ejecutar comandos que requieran permisos administrativos. Sudo está especificado en el archivo ***/etc/sudoers/*** y puede ser editado con el comando "visudo" a través de la interfaz del editor Vi.

También se recomienda cambiar el puerto predeterminado para el protocolo SSH, puerto 22, a un puerto no convencional.

Se recomienda modificar el archivo de configuración "***/etc/ssh/sshd_config***" con los siguientes parámetros para restringir el acceso a usuarios.

Deshabilitar inicio de sesión de root

```
PermitRootLogin no
```

Permitir solo usuarios específicos

```
AllowUsers username
```

Utilizar versión 2 del protocolo SSH

```
Protocol 2
```

Cambiar puerto para escuchar conexiones entrantes

```
Port 50221
```

- **6 Mantener actualizado el sistema**

Siempre se debe mantener actualizado el sistema y aplicar los parches, soluciones de seguridad y actualizaciones de kernel más recientes y tan pronto se encuentre encuentren disponibles.

```
# yum updates

# yum check-update

# sudo apt-get update
```

- **7 Controlar las tareas programadas**

El demonio ***cron*** tiene una característica incluída en la cual se puede especificar los usuarios que pueden y no pueden ejecutar tareas programadas. Esto se controla con el uso de los archivos llamados ***/etc/cron.allow*** y ***/etc/cron.deny***. Para bloquear a un usuario, basta con añadir su nombre de usuario en el archivo ***cron.deny*** y para permitir un usuario que ejecute tareas, se añade su nombre en el archivo ***cron.allow*.** Si se desea deshabilitar a todos los usuarios del uso de tareas, se añade la palabra ***ALL*** a una línea del archivo ***cron.deny***.

```
# echo ALL >> /etc/cron.deny
```

- **8 Deshabilitar puertos USB**

Muchas veces pasa que se desea restringir a los usuarios para que no puedan conectar memorias USB en lo equipos, con la finalidad de proteger contra robo la información que almacenan. Para lograr esto, se debe crear el archivo ***/etc/modprobe.d/no-usb*** y agregarle la siguiente línea, con la cual no se detectarán dispositivos de almacenamiento por USB.

```
install usb-storage /bin/true
```

- **9 Activar SELinux**

El módulo SELinux (Security Enhanced Linux o Seguridad Mejorada de Linux, en español) es un mecanismo de seguridad y control de acceso que se incluye en el kernel. Deshabilitar esta característica, significa quitar los mecanismos de seguridad del sistema. Piensa dos veces y de forma cuidadosa antes de quitarlo, incluso si tu equipo está conectado a Internet y provee servicios públicos.

SELinux provee tres modos básico de operación:

  - Enforcing (Restrictivo): Este es el modo habilitado por defecto y que habilita y aplica las políticas de seguridad en el equipo.
  - Permissive (Permisivo): En este modo, SELinux no forzará el uso de políticas en el sistema, solo advertirá y registrará las acciones. Este modo es muy útil para la resolución de problemas relacionados con SELinux.
  - Disabled (Deshabiltado): SELinux está apagado.

Si SELinux está deshabilitado, se puede habilitar con el siguiente comando:

```
# setenforce enforcing
```

Se puede saber el estado de SELinux desde la línea de comandos escribiendo los siguientes comandos:

```
# sestatus

# system-config-selinux

# getenforce
```

- **10 Deshabilitar los escritorios gráficos KDE o GNOME**

No existe la necesidad de ejecutar escritorios gráficos basados en X, como KDE o GNOME, dentro de un servidor de producción. Se pueden desinstalar o deshabilitar para aumentar la seguridad y rendimiento del servidor. Para hacerlo, únicamente edita el archivo ***/etc/inittab*** y ajusta el nivel de ejecución en 3. Si deseas quitarlo por completo, utiliza el siguiente comando:

```
# yum groupremove "X Window System"

# sudo apt-get remove --purge xserver-xorg
```

- **11 Deshabilitar IPv6**

Si no se utiliza ningún protocolo de IPv6 en el sistema, entonces de debería deshabilitar, puesto que ninguna de las aplicaciones, políticas y protocolos de IPv6 se requieren. Edita el archivo de configuración de red y añade las siguientes líneas para deshabilitarlo:

```
NETWORKING_IPV6=no

IPV6INIT=no
```

- **12 Evitar que los usuarios reutilicen contraseñas**

Esta es una medida muy útil en caso de que se requiera evitar que los usuarios reutilicen contraseñas viejas. Para lograrlo se debe utilizar el módulo de autenticación de usuarios PAM y el archivo ***/etc/security/opasswd***.

En sistemas Red Hat Enterprise Linux, CentOS o Fedora se edita el archivo ***/etc/pam.d/system-auth.*** En sistemas Debian, Ubuntu o Linux Mint, editar el archivo ***/etc/pam.d/common-password***. En estos archivos se debe añadir la siguiente línea a la sección **auth:**

```
auth    sufficient    pam_unix.so likeauth nullok
```

También se debe agregar la siguiente línea a la sección **password** para evitar que un usuario reutilice las últimas 5 contraseñas usadas en el sistema:

```
password    sufficient    pum_unix.so nullok use_authtok md5 shadow remember=5
```

- **13 Revisar el tiempo de validez de contraseñas de usuarios**

En Linux, las contraseñas de los usuarios son almacenadas de forma cifrada en el archivo ***/etc/shadow.*** Para ajustar la fecha de expiración de la contraseña de un usuario, se necesita utilizar el comando ***chage.***

Para saber el tiempo de uso, vigencia o días desde el último cambio de contraseña, se utiliza el comando:

```
# chage -l nombre_de_usuario
```

Algunas opciones del comando son:

  - -M Para indicar el máximo número de días de vigencia de la contraseña.
  - -m Para indicar el mínimo número de días de vigencia de la contraseña.
  - -W Para indicar cuantos días antes de que la contraseña expire, se mande una advertencia.

- **14 Bloqueo y desbloqueo manual de cuentas**

Esta característica es muy útil para evitar borrar cuentas de usuario, ya que sirve para especificar un periodo de tiempo en el cual se bloquearán las cuentas de usuario. Esto se realiza con el comando:

```
# passwd -l nombre_de_usuario
```

Para desbloquear al usuario se utiliza el comando:

```
# passwd -u nombre_de_usuario
```

Cabe mencionar que si el usuario **root** inicia sesión como algún usuario bloqueado, si podrá iniciar sesión.

- **15 Uso de contraseñas seguras**

Muchos usuarios utilizan contraseñas débiles que pueden ser descubiertas por medio de un ataque de fuerza bruta. Para evitar el uso de contraseñas débiles, el módulo PAM contiene una funcionalidad llamada **pam_cracklib** que obliga al usuario a utilizar contraseñas fuertes y seguras. Para habilitarlo basta con añadir al archivo ***/etc/pam.d/system-auth*** la siguiente directiva:

```
/lb/security/$ISA/pam_cracklib.so retry=3 minlen=8 lcredit=1 ucredit=-2 dcredit=-2 ocredit=-1
```

Las palabras reservadas significan:

  - lcredit = lower-case o minúsculas
  - ucredit = upper-case o mayúsculas
  - dcredit = digitos
  - other = otros

- **16 Activar Iptables (Firewall)**

Es áltamente recomendable habilitar el firewall de Linux para evitar accesos no autorizados a nuestro equipo. Se deben aplicar reglas para direcciones IP origen y destino y puerto UDP o TCP para paquetes entrantes, salientes y redirigidos.

- **17 Deshabilitar Ctrl+Alt+Supr en el archivo /etc/inittab**

En la mayoría de las distribuciones Linux, el presionar la combinación de teclas ***ctrl+alt+supr*** provocará un reinicio del sistema, por lo que no es muy recomendable tener habilitada dicha opción, específicamente en servidores de producción.

Esta acción se define dentro del archivo ***/etc/inittab*** en una línea similar a la siguiente:

```
# ca::ctrlaltdel:/sbin/shutdown -t 3 -r now
```

- **18 Verficar cuentas sin contraseñas**

Cualquier cuenta de usuario con una contraseña vacía significa una puerta abierta para acceso no autorizado desde cualquier parte del mundo. Se debe asegurar que todas las cuentas de usuario cuenten con contraseñas fuertes y seguras. Para revisar si existen cuentas con contraseñas vacías se puede utilizar el siguiente conjunto de comandos:

```
# cat /etc/shadow | awk -F : '($2=="") {print $1}'
```

> Este comando obtendrá toda la lista de usuarios en el sistema y mostrará a aquellos que su contraseña sea vacía.

- **19 Mostrar mensaje de SSH antes de iniciar sesión**

Es una buena práctica mostrar y contar con mensajes de seguridad o advertencias antes de realizar una autenticación por medio de SSH. Para mayor información leer el siguiente artículo.

- **20 Monitoreo de actividades del usuario**

Si se tienen muchos usuarios en el sistema, es muy importante recolectar información de la actividad y procesos de cada usuario, para después poder analizar esa información en caso de problemas de rendimiento o seguridad. Existen dos herramientas muy útiles llamadas **psacct** y **acct** que son utilizadas para monitorear los procesos y la actividad de los usuarios en el sistema. Estas herramientas se ejecutan en segundo plano y continuamente están registrando la actividad de los usuarios y los recursos del sistema que consumen servicios como Apache, MySQL, SSH, FTP, etc.

- **21 Revisión de bitácoras de forma regular**

Reasigna las bitácoras en un servidor dedicado de bitácoras, esto podría evitar que los intrusos puedan modificar las bitácoras locales. Los archivos de bitácoras más comunes se encuentran en la ruta ***/var/log/*** y son:

  - messages: Bitácoras del sistema
  - auth.log: Bitácoras de autenticación (Debian, Ubuntu, Linux Mint)
  - kern.log: Bitácoras del kernel
  - cron.log: Bitácoras del demonio crond
  - maillog: Bitácoras del servidor de correo del sistema
  - boot.log: Bitácoras del arranque del sistema
  - mysqld.log: Bitácoras del manejador de bases de datos, MySQL
  - secure: Bitácoras de autenticación (Red Hat, Fedora, CentOS)
  - utmp ó wtmp: Bitácora de inicio de sesión

Otros consejos:

- **22 Tener un respaldo de archivos importantes**
- **23 Unión de Tarjetas de Red**
- **24 Mantener /boot como solo lectura**
- **25 Ignorar ICMP o peticiones de Broadcast**

Fuente: TecMint MB

Últimas noticias

Usuarios de Skype afectados por ransomware en anuncios maliciosos 01-Abr-2017
Java y Flash encabezan la lista programas más obsoletos 31-Mar-2017
Apple soluciona error en Safari usado en ataques de ransomware 28-Mar-2017
Utilizan botnet GiftGhostBot para robar saldos de tarjetas de regalo 28-Mar-2017
Expertos señalan que hay archivos sensibles expuestos en Docs.com 28-Mar-2017
Spammers modifican archivos RTF para ocultar malware 27-Mar-2017
Estafas de bitcoins infestan las redes sociales 25-Mar-2017