Guía Seguridad sobre máquinas con Centos

Guía CCN-STIC-619

Guía Seguridad

Contraseñas

Usar contraseñas seguras, especialmente para el usuario root.

Una contraseña segura tiene que tener al menos estas características:

- Tener una longitud mínima de 8 caracteres
- Mayúsculas y minúsculas alternadas
- Tantos signos de puntuación y números como sea posible
- Evitar palabras o frases comunes que puedan figurar en cualquier diccionario
- No tener relación evidente con datos personales del usuario: Nombre, fecha de nacimiento, etc

Política de caducidad de las contraseñas

Las definiremos en el fichero /etc/login.defs o a cada usuario manualmente con el comando **chage**

- El periodo máximo durante el que se puede mantener una contraseñaserá de 60 días
- La longitud mínima de la contraseña será de 8 caracteres.
- El período mínimo durante el que se debe mantener una contraseña será de 15 días
- El período durante el que el sistema avisará de una futura caducidad de la contraseñaserá de 15 días

Usuarios UID 0

Solamente root debería de ser el único usuario con el UID a 0

Particionado

- recomendable usar XFS o ext4
- Bloquear el acceso a la línea de comandos Grub. Sólo tiene que ser accesible por root y mediante contraseña

Las particiones se pueden montar de distintas formas para que limiten determinados permisos:

- Noauto: La partición no se montará automáticamente.
- Noexec: La partición no admitirá la ejecución de ficheros desde la misma.
- Nodev: La partición no admitirá la instalación de dispositivos.
- Permisos (ro), (rw):La partición se configurará con permisos read-only (ro, solo lectura), read-write (rw, lectura y escritura)

Recomendacionesde seguridad para las particiones:

- boot → noauto, noexec, nodev, nosuid, ro.

Si hay que actualizar el kernel habría que montar temporalmente la partición **boot** como **rw**

- /boot/efi. → umask=0077, shortname=winnt <dump> 0 <pass> 0
- /usr y /opt → nodev, ro

para actualizar o instalar una nueva aplicación habría que montar temporalmente la partición correspondiente como **rw**

- /var → defaults, nosuid
- /var/log → nodev, noexec, nosuid, rw.
- /var/log/audit → nodev, noexec, nosuid, rw.
- /var/www → nodev, noexec, nosuid, rw
- /home y /tmp → nodev, noexec, nosuid, rw
- /media/XXX → noauto, nodev,nosuid, rw
- swap → defaults,<dump> 0 <pass> 0.

Seguridad Red

- Direcciones ip fijas
- deshabilitar protocolos no utilizados : Zeroconf, ipv6 si no se utiliza,

Para prevenir ataques a algunos protocolos (dccp, sctp, rds, tipc)se añaden archivos **.conf** al directorio **/etc/modprobe.d** para que se ejecute la shell **/bin/false** en lugar de cargar el módulo del protocolo indicado

From:
http://wiki.intrusos.info/ - **LCWIKI**

Permanent link:
http://wiki.intrusos.info/doku.php?id=seguridad:ens:centos

Last update: **2023/01/18 14:37**