Bastionado de Centos

Instalación

Siempe que sea posible hay que instalar el SO desde DVD sin que esté conectado a la red hasta que se hayan completado el bastionado. Descargarnos la imagen desde el sitio oficial y verificar la integridad de la misma.

En caso contrario el equipo debe de instalarse desde un segmento de la red aislado del resto, sin acceso desde el exterior y con un acceso a internet restringido.

Elegir siempre la instalación **mínima** y posteriormente añadir sólo los servicios o paquetes necesarios para la función a realizar.

Particionado

- las particiones deben realizarse sobre LVM y formateadas como ext4 de esta forma su tamaño puede variar en caliente.
- La carpeta home de los usuarios y en general cualquier otra donde los usuarios puedan escribir, deben de estar en particiones independientes, esto evita, entre otras cosas, la creación de links duros (hardlink) a programas con el setuid activado y permite un control granulado de las opciones de mount
- Se deben asignar los privilegios mínimos a través de las opciones de mount:
  - Noexec en todo lo posible (evita la ejecución de binarios, aunque no de scripts)
  - Nodev en todos los puntos de montaje excepto en la raíz "/" o "/dev" (evita el uso de dispositivos en el punto de montaje)
  - Nosetui en todos los puntos de montaje excepto en la raíz "/" (previene el uso del bit setuid en el punto de montaje)
  - Monta /var/tmp con la opción bind a /tmp o crea un enlace simbólico

Red

Para el bastionado de la red tenemos que tener en cuenta lo siguiente:

- Deshabilitar los protocolos que no se utilizen
- Verificar los puertos en los que escucha el servidor y deshabilitar los innecesarios
- Restringir el acceso a los puertos abiertos a direcciones concretas

En Centos para configurar la red ejecutar

```
system-config-network
```

o editando el fichero correspondiente a nuestra tarjeta, que se encuentra en la ruta **/etc/sysconfig/networking/devices**

Los DNS hay que especificarlos en el archivo /etc/resolv.conf

Deshabilitar IPV6 si no lo utilizamos

Para ver si tenemos IPV6 activo ejecutamos

```
ifconfig | grep inet6
```

Para deshabilitarlo sin reiniciar el sistema, ejecutar:

```
echo 1 > /proc/sys/net/ipv6/conf/all/disable_ipv6
echo 1 > /proc/sys/net/ipv6/conf/default/disable_ipv6
```

otra forma sería:

```
sysctl -w net.ipv6.conf.all.disable_ipv6=1
sysctl -w net.ipv6.conf.default.disable_ipv6=1
```

Deshabilitar Zeroconf

Comprobar si se está ejecutando Zeroconf

```
ps -e | grep avahi
```

Si devuelve algún resultado es que avahi está activo. Para deshabilitarlo: Añadir la línea **NOZEROCONF=yes** Al archivo /etc/sysconfig/network y eliminar el paquete

```
yum -y remove avahi
```

Detectar sevicios en escucha

Ejecutar

```
sudo netstat -tuanp | grep LISTEN
```

Si tenemos servicios innecesarios en /etc/init.d se encuentran los scripts de gestión del sistema SystenV tradicional y en /etc/init se encuentran los servicios adaptdos al sistema upstart. Para ver que servicios tenemos ejecutamos

```
ls -1 /etc/init.d > servicios
```

o bien

```
ls -1 /etc/init >> servicios
```

Para deshabilitar un servicio determinado

```
chkconfig <service> off
```

si es posible eliminar los paquetes

Otras mejoras de seguridad en la red

Se utilizarán algunos parámetros de control de **sysctl** para proteger al sistema ante situaciones que introducen riesgo en las comunicaciones.

El archivo /etc/sysctl.conf debe contener las siguientes líneas:

- net.ipv4.icmp_echo_ignore_broadcasts = 1 → Evita la respuesta a broadcast icmp para prevenir el ataque smurf
- net.ipv4.icmp_ignore_bogus_error_responses = 1 → Activa la protección ante mensajes icmp incorrectos
- net.ipv4.tcp_syncookies = 1 → Habilita syncookies como protección ante ataques de tipo SYN flood
- net.ipv4.conf.all.log_martians = 1net.ipv4.conf.default.log_martians = 1 → Activa el log para paquetes falsos (spoofed), encaminados en el origen (source routed) y redirigidos (redirect)
- net.ipv4.conf.all.accept_source_route = 0net.ipv4.conf.default.accept_source_route = 0 → Deniega paquetes encaminados en el origen (source routed)
- net.ipv4.conf.all.rp_filter = 1net.ipv4.conf.default.rp_filter = 1 → Habilita el filtrado de paquetes de camino inverso (reverse path)
- net.ipv4.conf.all.accept_redirects = 0net.ipv4.conf.default.accept_redirects = 0net.ipv4.conf.all.secure_redirects = 0net.ipv4.conf.default.secure_redirects = 0 → Impide la modificación de las tablas de rutas desde el exterior
- net.ipv4.ip_forward = 0net.ipv4.conf.all.send_redirects = 0net.ipv4.conf.default.send_redirects = 0 →Evita el encaminado de paquetes

Sincronización de la fecha y hora

Hay que configurar todos los servidores para que se sincronizen con el mismo servidor de tiempo, ya que es muy necesario a la hora de investigar acciones que suceden en más de una máquina

Para configurar un servidor de tiempo hay que seguir estos pasos:

- Instalar el paquete ntpd

```
yum install ntp
```

- Editar el archivo/etc/ntp.conf y poner nuestro servidor de tiempo el primero de la lista

```
server X.X.X.X
```

- chkconfig ntpd on

Control de acceso

Las acciones a realizar son las siguientes:

- Impedir el inicio de sesión al usuario root tanto en local como en remoto
- La limitación del uso del comando su,
- La configuración de sudo para mejorar el auditado del acceso como root
- Que cada administrador tenga su usuario y no lo comparta nunca
- Reemplazar el algoritmo MD5 por SHA512 para los hashes de las contraseñas
- Impedir el uso de contraseñas antiguas y realizar varias comprobaciones para asegurar que la nueva contraseña es diferente de la antigua (pam_unix)

Crear usuarios con privilegios de administrador

Ejecutar el siguiente comando para cada usuario que requiera privilegios de administrador

```
usermod -G wheel -a usuario
```

Editar el archivo /etc/pam.d/su y asegurarse de que contiene la línea

```
auth required pam_wheel.so use_uid
```

Limitar el uso de sudo a miembros de un grupo de administradores

Editando el archivo /etc/sudoers mediante el comando **visudo** y asegurarse de que contiene la línea

```
%wheel ALL=(ALL) ALL
```

A partir de ahora todos los usuarios que requieran la ejecución de los comandos su y sudo deben ser miembros del grupo **wheel**

Desactivar el inicio de sesión local al usuario root

Editar el archivo /etc/shadow y sustituir el campo de la contraseña de root por un ! los dos primeros campos de la línea deben ser iguales a los de la siguiente línea.

```
root:!:14698:0:99999:7:::
```

Mejorar el sistema de contraseñas

hash, recordar contraseñas antiguas y realizar comprobaciones a las nuevas cuando se cambie una de ellas. Editar el archivo /etc/pam.d/system-auth y asegurarse de que contiene la línea

```
password sufficient pam_unix.so obscure sha512 shadow nullok try_first_pass
use_authtok remember=10
```

Editar el archivo /etc/login.defs y asegúrar que contiene las siguientes líneas

```
MD5_CRYPT_ENAB noENCRYPT_METHOD SHA512
```

En RedHat el archivo /etc/libuser.conf debe contener la línea

```
crypt_style = sha512
```

También puede ser interesante el uso de algunos módulos pam (plugable authentication modules):

- Pam_tally2 desactiva una cuenta de usuario tras varios intentos consecutivos de autenticación fallidos
- Pam_limits limita el número de sesiones concurrentes
- Pam_inicio de sesiónuid impide el inicio de sesión si no está iniciado el servicio de auditoría auditd
- Pam_access impide el inicio de sesión por origen, consola o cuenta de usuario
- Pam_time impide el inicio de sesión por horario

Crear usuarios sin SHELL

Hay determinados casos en los que puede ser util tener usuarios que puedan iniciar sesión pero no tengan acceso a una SHELL, por ejemplo para usuarios de FTP.

Para crear usuario sin Shell hay que ejecutar el comando:

```
useradd -M -s /sbin/nologin usuario
```

Donde -M indica que no se creará el directorio HOME del usuario, si es necesario que tenga HOME hay que quitar este parámetro del comando, y -s indica la SHELL que se le asigna al usuario, al especificar /sbin/nologin se asigna una SHELL que impide el inicio de sesión en el sistema

Mesaje de inicio

Establecer el mensaje corporativo de inicio de sesión, para ello copiamos el texto en el archivo /etc/motd

Enviar los logs a un servidor remoto

En caso de usar syslogd el archivo /etc/syslog.conf debe contener la siguiente línea

```
auth.info,authpriv.info,user.crit           @X.X.X.X
```

En caso de usar rsyslogd el archivo /etc/rsyslogd.conf debe contener la siguiente línea

```
auth.info,authpriv.info,user.crit           @@X.X.X.X:PUERTO
```

Si se ha denegado la salida del tráfico mediante reglas de iptables habrá que permitir la salida al puerto 514 UDP mediante el comando

```
iptables -I OUTPUT -p udp -d X.X.X.X –dport 514 -j ACCEPT
```

At y Cron

Permitir el uso de cron y at tan solo al usuario root ejecutando los siguientes comandos

```
rm /etc/{cron.deny,at.deny}echo root > /etc/cron.allowecho root >
/etc/at.allow
```

Bastionar el acceso por SSH

Para mejorar la seguridad del servicio SSH se deben realizar las siguientes acciones:

- Permitir tan solo el protocolo ssh2
- Si el servidor tiene más de una IP definir en cuantas debe escuchar
- Impedir el inicio de sesión como root
- Impedir el uso de contraseñas en blanco
- Impedir el uso de autenticación basada en host
- Establecer un límite de tiempo para el inicio de sesión
- Establecer un número máximo de intentos antes de bloquear la sesión
- Establecer un tiempo de sesión inactiva a 5 minutos
- Ignorar los archivos rhosts y shosts
- Limitar el inicio de sesión a un grupo de usuarios del sistema
- Separar los privilegios de los procesos de SSH
- Configurar el mensaje de inicio de sesión

Editamos el archivo /etc/ssh/sshd_config y añadimos o cambiamos las líneas:

```
LoginGraceTime 120
ClientAliveInterval 300
ClientAliveCountMax 0
Banner /etc/ssh/ssh_banner
AllowGroups wheel
ListenAddress ip_por_donde_escucha
```

Para configurar el mensaje de inicio de sesión hay que editar el archivo /etc/ssh/ssh_banner e insertar el texto

Auditar el sistema

Ojo activar el sistema de auditoria puede volver inutilizable el servidor más potente, así que hay que usarlo con precaución y planificación.

Los pasos genéricos que debemos seguir son:

- Instalar el paquete auditd

- Localizar los archivos críticos y/o de mayor riesgo para los servicios que ofrece el servidor
- Configurar auditd para que se inicie junto al sistema
- Configurar el núcleo para que audite procesos que se inician antes que el servicio auditd
- Añadir los archivos críticos al servicio auditd

Al configurar auditd hay que:

- Tener /var/log/audit en su una partición propia
- Ajustar max_log_file y num_logs para que usen el máximo posible del espacio de la partición de logs
- Ajustar space_left de forma que permita al administrador tener tiempo para liberar espacio ante una alerta de poco espacio disponible
- En el caso de que se llene el disco se ejecutará la acción definida por disk_full_action, todos los accesos deben ser terminados ya que no hay capacidad de auditar

Para instalar y arrancar auditd durante el inicio del sistema ejecutar estos comandos

```
yum install auditd
chkconfig auditd on
```

Una vez instalado y configurado hay que revisar el resultado del comando aureport regularmente

Una vez obtenido el listado de los archivo a auditar hay que agregarlos al archivo /etc/audit/audit.rules

Actualizar el sistema

Mantener el sistema actualizado con los últimos parches

Deshabiliar dispositivos innecesarios

Para ver los dispositivos ejecutar

```
lspci -v
```

```
lsusb
```

Una vez localizados, deshabilitar los módulos innecesarios

Deshabilitar servicios innecesarios

Algunos servicios que no deben existir en ningún caso son:

- rlogin
- rsh
- rexec
- rcp

- telnet → Usar ssh en su lugar
- talk

Scripts de bastionado

- http://www.eugeniabahit.com/proyectos/jackthestripper
- http://abdulet.net/?p=594

Referencias

- http://www.cyberciti.biz/tips/linux-security.html
- http://mundogeek.net/traducciones/odonovan.html
- http://www.cica.es/Seguridad/guia-de-seguridad-en-una-estacion-linux.html
- http://www.cica.es/Seguridad/seguridad-en-los-ficheros-protecciones.html
- www.sans.org/resources/policies
- http://abdulet.net/?p=591

Búsqueda de archivos con suid/sgid

```
find / -type t\ (-perm 04000 -o - perm -02000\) -exec ls -la {} \
```

Buscar otros archivos peligrosos

```
find / name -rhosts -name .netrc
```

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

Permanent link:
http://wiki.intrusos.info/doku.php?id=seguridad:asegurar_linux&rev=1429862707

Last update: **2023/01/18 13:57**