SEGURIDAD

SEGURIDAD LÓGICA

Santiago Candela Solá
Universidad de Las Palmas de Gran Canaria

Índice.

- Seguridad Informática.
- Controles de Seguridad.
- Políticas de Seguridad.
- Estudios de la Seguridad.
- Seguridad Lógica.
  - Seguridad en la Bios y en el Cargador.
  - Seguridad Contraseña de Usuarios.
  - Accesos y Permisos como Root.
  - Servicios Disponibles a través de Red.
  - Cortafuegos.
  - Archivos de administración relacionados con la seguridad.
- Políticas y Planes de Seguridad.

Bibliografía:

- **Red Hat Linux Security Guide, 2002**
- **Administración de Red Hat Linux, Thomas Schenk, Prentice Hall, 2001**
- **Linux Security Basics, Aron Hsiao, Sams, 2001**

SEGURIDAD INFORMÁTICA.

Seguridad Informática ¿Qué es?

- La información junto con los servicios que presta el sistema informático es un bien, que al igual que otros importantes activos económicos, tiene un valor crucial para una organización, por esto, necesita ser adecuadamente asegurada.

- La Seguridad Informática protege esta información de un variado rango de amenazas, de manera de afirmar la continuidad de los negocios, minimizar el daño a estos, y maximizar utilidades y oportunidades.

- La Seguridad Informática es el conjunto de reglas, planes y acciones que permiten asegurar la información y los servicios contenidos en un sistema informático.

- Es curioso ver que la Seguridad informática es un conjunto de soluciones técnicas a problemas no técnicos.

Principales tópicos que se estudian en seguridad

- **SEGURIDAD LÓGICA**
- **MÓDULOS DE AUTENTICACIÓN PAM**
- **CONSOLA**
- **SEGURIDAD EN SISTEMA DE FICHEROS**
- **SEGURIDAD FÍSICA**
- **RAID**
- **SERVICIOS NFS+SAMBA**
- **SERVICIOS APACHE+FTP+SMTP**
- **SSH**
- **INTRUSIÓN Y RESPUESTA**
- **LOGS Y AUDITORIAS**
- **INTEGRIDAD DEL SISTEMA**
- **ATAQUES A CONTRASEÑAS**
- **SF CRIPTOGRAFIADO**
- **FILTROS**

¿Por qué es importante?

- La información es un activo con valor económico para las empresas, ya que sustenta la toma de decisiones. Pero además, se sabe que hay millones de equipos en el mundo enlazados a través de Internet, que son susceptibles de ataques.

- Estos equipos pueden ser usados como escudo y plataforma para atacar a otros, ocultándose así los verdaderos responsables.

- De manera creciente, las organizaciones junto a sus sistemas informáticos y de redes se enfrentan a un gran rango de amenazas, que incluyen:
  - Fraudes Computacionales
  - Espionaje Industrial
  - Sabotajes
  - Vandalismo
  - Inhabilitación de Servicios
  - Abuso de la Red
  - Virus

- Estas fuentes de daños se han tornado cada vez más comunes y sofisticadas.

Hacia la estandarización.

- Con motivo de lo anterior, las empresas e industrias reclaman ciertas reglas y regulaciones tanto al IEEE como a la AMA (American Medical Association), las cuales se describieron como la famosa CIA (en ingles o CID en español) de Confidentiality (Confidencialidad), Integrity (Integridad) y Availability (Disponibilidad). Este modelo está ampliamente aceptado para acceder a información “sensible” y el establecimiento de políticas de privacidad.

- Mantener la confidencialidad, integridad y disponibilidad de la información son esenciales para mantener un margen competitivo, rentabilidad e imagen comercial.

Los modelos sobre Políticas de Seguridad se basan en:

- Confidencialidad – La información solo debe ser leída, escrita o ejecutada por un conjunto predeterminado de usuarios del sistema. Los servicios deben ser utilizados por los usuarios autorizados.

- Integridad – La información no debe perderse o alterarse ni los servicios alterarse.

- Disponibilidad – La información y los servicios debe estar disponible en cualquier instante que se precise a los usuarios autorizados.

CONTROLES DE SEGURIDAD

- Controles Físicos
- Controles Técnicos
- Controles Administrativos

Controles Físicos

Técnicas de prevención:

- Uso de recintos con llaves o tarjetas.
- Uso de cámaras.
- Sistemas de alarma.
- Guardas de seguridad.
- Autentificadores por imágenes.

Controles Técnicos

Técnicas de prevención:

- Sistemas de encriptación.
- Uso de tarjetas inteligentes.
- Sistema de autentificación de red.
- Listas de Control de Acceso.

Controles Administrativos

Técnicas de prevención:

- Definición y control de cuentas.
- Estrategias de división y separación de usuarios y grupos.
- Planes de actuación y prevención para recuperar al sistema.
- Actualizaciones.

POLÍTICAS DE SEGURIDAD

¿Qué son?

- Las Políticas de Seguridad son las reglas y procedimientos que regulan la forma en que una organización previene, protege y maneja los riesgos de daño sobre:
  - los computadores de sus sistemas y los elementos físicos asociados con éstos (edificación, impresoras, discos, cables, dispositivos de interconexión, etc.),
  - el software y la información almacenada en tales sistemas.
  - los usuarios del sistema.

- Sus principales objetivos:
  - Informar al mayor nivel de detalle a los usuarios, empleados y gerentes de las normas y mecanismos que deben cumplir y utilizar para proteger los componentes de los sistemas de la organización.
  - Proporcionar los criterios para adquirir, configurar y auditar los sistemas de computación y redes para que estén en concordancia con la política de seguridad.

Componentes

- Una política de privacidad
- Una política de acceso
- Una política de autenticación
- Una política de contabilidad
- Planes para satisfacer las expectativas de disponibilidad de los recursos del sistema
- Una política de mantenimiento para la red y los sistemas de la organización
- Directrices para adquirir tecnología con rasgos de seguridad requeridos y/o deseables
- Sanciones para quien infrinjan la política de seguridad
- Una política de reporte de incidentes y de divulgación de información

Estudio de la Seguridad

En la Red.

En los Servidores.

En las Estaciones de Trabajo.

Seguridad en la red

Estudia aspectos como:

- Diseño y configuración de arquitecturas para que sean seguras.
- Uso y configuración de hubs y routers para transmisión de información por la red segura.
- Distribución de servidores frente a un sistema centralizado.
- Uso de protocolos y aplicaciones de comunicación seguras.

Seguridad en los Servidores

Estudias aspectos como:

- Seguridad de los servicios y aplicaciones.
- Que servicios son necesarios.
- Que puertos hay que mantener abiertos y con que protocolos.
- Actualizaciones de seguridad de los servicios y aplicaciones.
- Autentificaciones de los servicios.

Seguridad en las Estaciones de Trabajo

Estudia aspectos como:

- Definición y administración de cuentas.
- Autentificación y contraseñas.
- Copias de seguridad.

Seguridad Lógica

SEGURIDAD EN LAS ESTACIONES DE TRABAJO

Aspectos de seguridad en una estación de trabajo, un nodo de la red.

- Seguridad en la BIOS de la placa base y el cargador del sistema operativo.
- Seguridad en la contraseña de usuarios.
- Acceso y permisos como root.
- Servicios disponibles a través de la red.
- Seguridad en la comunicación en la red.

La BIOS, nuestro primer punto de seguridad

- La BIOS (Sistema de entrada/salida básico) es una memoria ROM, EPROM o FLASH-Ram la cual contiene las rutinas de más bajo nivel para arrancar.

- Además, se apoya en otra memoria, la CMOS ,que almacena todos los datos propios de la configuración del ordenador.

La BIOS

- Las BIOS viejas tiene fama de tener claves universales, hay que asegurarse que la BIOS es reciente y que no contiene semejante puerta trasera.

- Desde la BIOS se puede limitar la secuencia de arranque al disco duro, con lo cuál impedimos el arranque desde cualquier otro dispositivo: floppy, cd-rom, etc.

  - También podemos controlar los puertos, serie y paralelo.

  - Con habilitar los puertos para ratón y teclado tenemos suficiente y evitamos puertas abiertas para usuarios malintencionados.

Seguridad en la Bios

- Un usuario que puede acceder de modo físico al sistema puede hacer que el sistema arranque desde un disquete o un CDROM y entrar en modo single o en modo rescue y acceder al sistema como root sin contraseña.

La Bios suele tener la posibilidad de colocar dos **contraseñas**. Depende del fabricante y la versión.

- **Contraseña para cambiar parámetros de la Bios**. (hacer que se pueda arrancar desde disquete).
- **Contraseña para que se cargue** el sistema operativo.

- Estas contraseñas se pueden borrar quitando la pila de la placa base. Es bueno colocar una cerradura en la unidad central.

Seguridad en el Cargador

Contraseña en el cargador

Colocar contraseña en el cargador evita.

- **Acceso en modo linux single y hacerse root sin contraseña.**
- **Acceder a otros sistemas operativos que tengamos en el sistema cargados de forma dual.**
- **Vienen dos cargadores con la distribución de Red Hat LILO y GRUB.**

Contraseña en LILO

(Linux Loader), es el cargador mas estandar.

- Si no hay contraseña en el arranque con ctrl x, se entra en modo usuario single.

- También se puede evitar ejecutar el primer proceso **init** para que no solicite contraseña.
- En el arranque de Lilo pulsar la tecla Shift de la izquierda y entrar
- LILO boot: linux init = /bin/bash

LILO permite usar la directiva **password** en el fichero **/etc/lilo.conf** para realizar protecciones.

Contraseña en LILO

Colocar una contraseña para cargar cualquier sistema operativo.

- Antes de cualquier imagen colocar la directiva
  password = contraseña

- Punto débil, la contraseña no se codifica, el fichero puede ser leído por cualquier usuario y leer la contraseña.
- Desactivar permisos. (chmod 600 /etc/lilo.conf).

Contraseña en LILO

Se puede colocar contraseña para cargar un sistema operativo específico.

Colocando la directiva password seguidamente de la directiva image.

image = /boot/vmlinuz…

password = contraseña

Se puede hacer que se pida una contraseña solo para cambiar los parámetros con los que se arranca el núcleo, con la directiva **restricted**.

image = /boot/vmlinuz..

password = contraseña

restricted

Ejemplo de un lilo.conf con contraseña

```
boot=/dev/hda
map=/boot/map
install=/boot/boot.b
prompt
timeout=100
default=linux
image=/boot/vmlinuz-2.2.5
    label=linux
    root=/dev/hda1
    read-only
restricted
password=la_contraseña
```

Seguridad en el Cargador

- Configurando el lilo.conf adecuadamente junto con la seguridad de la BIOS, crearemos un sistema bastante seguro.

- El comando `chattr +i /etc/lilo.conf` permite proteger el lilo.conf

  – Sólo el root puede modificar este valor.

Contraseña en GRUB

Grub es otro cargador que viene con Red Hat, no es tan estandar pero es editable en línea de comandos y la contraseña se codifica.

En la línea de comandos escribir

/sbin/grub-md5-crypt

grub nos solicita una contraseña <contraseña>, cuando la introducimos nos devuelve la misma codificada <contraseña codificada>.

- en el fichero texto de configuración /boot/grub/grub.conf introducimos la directiva

  password –md5 <contraseña codificada>

- permite colocar contraseña en cada sistema operativo que se arranca.

Seguridad en la contraseña de usuarios

- Es la puerta para que un usuario entre en Linux.
- Utiliza /etc/shadow, para ocultar las contraseñas codificadas del fichero /etc/passwd.

- Utiliza /etc/gshadow, para ocultar las contraseñas codificadas del fichero /etc/group.

- Utiliza el codificador criptográfico MD5 Message Digest Algorithm, que permite introducir claves mayores de ocho caracteres con un nivel de codificación de 56 bits.

Recomendaciones par una buena contraseña.

- Utilizar mezcla de caracteres numéricos, alfabéticos con mayúsculas y minúsculas y no alfanuméricos.
- No utilizar palabras o sus invertidas que estén en un diccionario, español o extranjero. (programas como Crack las descubren)
- No utilizar información conocida, personal o de la empresa, fecha de nacimiento, teléfono, etc.
- Escribir contraseñas de mas de ocho caracteres.
- No escribir las contraseñas en papel que pueda ser leido.
- Utilizar frases que nos recuerden la contraseña.

Archivo de configuración de cuentas

- El archivo para configurar cuentas de usuario es /etc/passwd.
- Se pueden añadir nuevas cuentas de usuario editando directamente este archivo, pero para crear la contraseña se debe usar la utilidad /usr/bin/passwd
- Por cada usuario debe aparecer lo siguiente:
- candela:x:101:100:santiago candela:/home/candela:/bin/bash

Campos de /etc/passwd

candela:x:101:100:santiago candela:/home/candela:/bin/bash

1. Nombre del usuario, debe ser único.
2. Campo de contraseña. Una x indica que se usan contraseñas ocultas. Las contraseñas se almacenan en otro fichero shadow.
3. Uid, Identificador del usuario, debe ser único.
4. Gid,Identificador del grupo.
5. Campo de comentario.
6. Directorio de trabajo donde se sitúa el usuario al iniciar sesión.
7. Shell asignado al usuario.

Shadow, Contraseñas ocultas

- Cuando no existían contraseñas ocultas, la contraseña, se almacenaba (cifrada) en /etc/passwd.
- Esto podía ser leído por cualquier usuario del sistema, aunque sólo modificado por el root.
- Actualmente las contraseñas cifradas se guardan en /etc/shadow, accesible sólo por el root.

Campos de /etc/shadow

candela:RB3mAtGdwFMDE:10568:0:-1:7:7:-1

1. Nombre de la cuenta de usuario.
2. Campo de contraseña cifrado.
3. Fecha contada como días transcurridos desde 1 enero 1970 en que se creo o cambio la contraseña.
4. Número de días que deben transcurrir hasta que la contraseña se pueda volver a cambiar.
5. Número de días maximo tras los cuales si no se cambia la contraseña la cuenta expira.
6. Días antes de la expiración de la contraseña en que se avisará al usuario al inicio de cesión.
7. Días después de la expiración de la contraseña en que la cuenta se inhabilita si la contraseña no se ha cambiado.
8. Días transcurridos desde la fecha en que la cuenta se inhabilitará (independiente de cambio en la contraseña).

inhabilitar usuarios

- Para inhabilitar una cuenta de usuario basta con modificar la entrada en /etc/passwd
  - candela:x12:100:100:santiago candela:/home/candela:/bin/bash
- Al añadir algo después de la x las utilidades de shadow ya no buscará la contraseña en el archivo /etc/shadow.
- Para habilitarla basta con quitar el “12”.

Eliminar sí, pero con seguridad

- Para eliminar el usuario, eliminamos las entradas que hace referencia a él.
- Si se elimina la cuenta del usuario y alguno de sus archivos permanece en el sistema, un nuevo usuario añadido con el nuevo identificador puede acceder a dicho archivo.
- El comando find /-nouser –exec rm –Rf {}\;
- Borrará todos los archivos y directorios cuyo propietario no se encuentre en /etc/passwd.

Crear contraseñas en un sistema multiusuario.

Cuando el administrador crea una nueva cuenta existen varias posibilidades.

- Crear la cuenta con el usuario y preguntar a este la contraseña.
- Crear una contraseña conocida por el usuario (DNI) y obligar al usuario a cambiarla con el comando passwd.

Crear contraseñas en un sistema multiusuario

- El administrador tiene que verificar que las contraseñas de los usuarios no son débiles.

- Como el comando passwd es PAM (Plugable Autentification Module), el administrador puede endurecer los requisitos de la contraseña con los módulos pam_cracklib.so, pam_passwdqc.
  (www.kernel.org/pub/linux/libs/pam/modules.html).

- El comando **change** permite especificar la caducidad en días de una contraseña.

  change –M 30

  el usuario se ve obligado a cambiar sus contraseña todos los meses. El valor 99999 indica que la contraseña no expira.

Acceso y Permisos como root

En las estaciones de trabajo hay que realizar tareas como root para

- Colocar los parámetros de red
- Montar un servicio de red
- Montar dispositivos
- Configurar nuevos dispositvos

Un usuario normal puede ser root o adquirir privilegios de root con programas que tengan el bit SETUID tales como su o sudo.

- Que un usuario tenga privilegios de root puede cargarse la seguridad del sistema.
- El administrador del sistema tiene que decidir a que usuarios le da privilegios de root.

Prohibir acceso como root

Quitarle al root el procesador de comandos Shell, para no ejecutar comandos.

Esto se realiza editando el fichero /etc/passwd

- sustituyendo el último campo de la línea de root /sbin/shell por /sbin/nologin

  que no permite login, su, ssh, sftp.

- Programas que no requieren el shell todavía tienen acceso a la cuenta del root. sudo, email.

No permitir entrar en el sistema como root

Esto se realiza editando o eliminando el fichero **/etc/securetty**

- contiene todos los dispositivos donde el root puede hacer login.
- Aún estando el fichero securetty en blanco el root puede entrar con un SSH, o utilizando el comando **su**.

No permitir al root SSH login

En el fichero /etc/ssh/sshd_config desabilitar la línea

PermitRootLogin no

Utiliar módulos PAM para limitar al root

- Utilizando el módulo /lib/security/pam_listfile.so se puede especificar los usuarios que no pueden utilizar un determinado servicio.

- Se puede denegar el servicio vsftpd FTP a un grupo de usuarios cuyos nombres aparecen en un fichero /etc/vsftpd.ftpusers

  Editando el fichero /etc/pam.d/vsftpd asociado al servicio FTP con:

  auth required /lib/security/pam_listfile.so item=user sense=deny file=/etc/vsftpd.ftpusers onerr=succeed

- Línea similar se puede colocar en otros servicios que admitan PAM.

Limitar acceso como root

- Acceder como root a través de los comandos **su** y **sudo**.

- Un usuario normal puede acceder como root a traves del comando su, que le solicitará la contraseña del root.
- Se puede volver a pasar a un usuario normal con su pero el sistema no preguntará contaseña.
- Se puede limitar el uso de **su** a un conjunto de usuarios:
- Adicionando usuarios al grupo predefinido **wheel** en /etc/grup, bien siendo root editando el fichero o mediante el comando

  usermod –G wheel <nombre de usuario>

  y seguidamente editar el fichero PAM /etc/pam.d/su y colocar la línea

  auth required /lib/security/pam_wheel.so use_uid
- Hace que solo los miembros del grupo **wheel** puedan utilizar el commando **su**.

El comando **sudo**

- Ejecuta un comando como root.

  sudo <comando>

- Cuando un usuario normal utiliza sudo se le pregunta por su contraseña.

- El fichero **/etc/sudoers** contiene la lista de usuarios que pueden utilizar sudo.

- Este fichero se edita y modifica con el comando **visudo**.

Cuentas para Acceso a una aplicación o a datos compartidos

- Se crea una cuenta como a un usuario normal pero en el campo shell se coloca /bin/false.

- Esto limita el acceso solo a los usuarios del sistema que conocen la contraseña. Los usuarios pueden acceder a la cuenta con el comando su.

Bloqueo de pantalla

- Programa de bloqueo de pantalla que no pueda ser desactivado por el usuario, que se active al cabo de un cierto tiempo (5 minutos) y exija contraseña para desbloquearse.

Servicios Disponibles a través de la Red

Cada vez que se permite un servicio de red en el computador:

- se abre uno o varios puertos
- se activa un programa (daemond) con su usuario propietario que permanece a la escucha en esos puertos.
- Por esos puertos pueden venir ataques desde el exterior.

- Todos los servicios que no se usan deben estar desactivados.
- El fichero **inetd.conf** controla los servicios ofrecidos por **inetd** (demonio que escucha peticiones que vienen de la red). Colocando # al principio de una línea, deshabilita el servicio.
- Para ver servicios y desactivarlos existen comandos como ntsysv, chkconfig.

Servicios disponibles a través de la red

- También hay que ver que puertos están abiertos y asociados a servicios **/etc/services**.

- Los login y shell remotos (rlogin, rsh, y telnet) deben evitarse y utilizar SSH, protocolo de comunicación de red que utiliza técnicas de Autentificación Criptográfica y Encriptación y es mas seguro.

Tiene tres aplicaciones como cliente.

- ssh – un acceso remoto seguro.
- scp – un copiador remoto.
- sftp – permite transferencia de ficheros remoto.

Cortafuegos Personales

- Un cortafuegos protege a los usuarios y a la información de ataques externos. Todo el tráfico se recibe en el cortafuegos.
- Cuando llega un paquete a un puerto, el cortafuegos lo analiza según una regla y filtra su acceso o lo desecha.
- **ipchains** es el software de filtrado de paquetes que se compila en el núcleo.
- Se puede programar el cortafuegos y colocar reglas para los puertos abiertos con el comando **iptables**.
- Básicamente existen dos tipos de cortafuegos en Linux:
  - Filtro de paquetes
  - Cortafuegos proxy

Cortafuegos

- En el filtro de paquetes, la información que se necesita para tomar la decisión sobre que hacer con ese paquete está en la cabecera.

- En la cabecera hay un total de trece campos:
  - Dirección de origen y destino.
  - El protocolo.
  - Etcétera.

Cortafuegos

- Los Cortafuegos Proxy redirigen el tráfico permitido a través del cortafuegos rescribiendo sus cabeceras.

- La diferencia entre uno y otro es sutil: mientras el proxy reencamina el tráfico el filtro de paquetes no redirige el tráfico.

- Ambos, proporcionan un mismo nivel de seguridad cuando están correctamente configurados.

Archivos de administración relacionados con la seguridad

- Son archivos que limitan el uso de aplicaciones o servicios.
- Se pueden crear los archivos:
- /etc/host.allow, con el contenido:

  ALL:LOCAL
- /etc/host.deny, con el contenido:

  ALL:ALL

Con el fin de limitar servicios a determinados hosts o dominios.

Archivos de administración relacionados con la seguridad

- Ejemplo:
- Comando **at** – permite ejecutar tareas programadas.
- Los ficheros **/etc/at.allow** y **/etc/at.deny** permite especificar los usuarios que pueden o no utilizar el comando at.
- Si los ficheros no existen solo root puede ejecutar **at**.

Ejemplo: Comando **cron**

- permite ejecutar tareas programadas de forma repetitiva.

- Los ficheros **/etc/cron.allow** y **/etc/cron.deny** permite especificar los usuarios que pueden o no utilizar el comando **cron**.

Póliticas y Planes de Seguridad

Politicas y planes de seguridad

Cualquier política de seguridad deberá contemplar:

- A quién se le permite usar las cuentas de usuarios.
- Disciplina a la hora de asignar las palabras de paso.
- Políticas de uso de los recursos del sistema.
- Cómo evitar/controlar el uso indebido de las cuentas y recursos del sistema.
- Procedimientos de monitorización del sistema.

Elementos básicos de un plan de seguridad:

- Políticas de acceso al sistema: clases de usuarios y requerimientos, privilegios de éstos y grupos de usuarios.
- Niveles adicionales de seguridad: caducidad de cuentas, palabras claves cambiantes.
- Plan de monitorización: recursos a controlar y periodicidad de los controles.
- Plan de auditoría: cada cuanto tiempo y que elementos del sistema se auditan.

Puntos débiles del sistema

- Bios y cargador sin contraseñas.
- Usuarios sin palabra de paso.
- Cuentas de usuarios no utilizadas.
- Cuentas de usuario predeterminadas.
- Cuentas de invitados.
- Cuentas de acceso de aplicaciones.
- Cuentas de grupos.
- Archivos ejecutables con los bits SUID y GID activados.
- Permisos de acceso a los archivos.
- Conexiones con el exterior.

Tareas de supervisión

- Control de la cuentas de usuario.
- Control de las palabras de paso.
- Garantizar la protección adecuada de los archivos.
- Aumentar los niveles de seguridad mediante utilidades adicionales de autentificación.
- Limitar los sistemas que se pueden conectar.
- Registrar los intentos fallidos de entrada en el sistema.
- Limitar el acceso a los usuarios durante periodos de tiempo.
- Finalización automática de sesiones ociosas.
- Hacer uso de los grupos de usuarios (grupos efectivos).
- Evitar los archivos ejecutables con SUID y GID activos.

Tareas de supervisión

Minimizar los riegos del software libre:

- Probar el producto como usuario no privilegiado.
- Obtener los ejecutables a partir de la compilación del código fuente.
- Descomprimir con cuidado el software: examinar y realizar esta acción en un área segura.
- Examinar el código fuente si es posible.
- Examinar los archivos de construcción del código objeto y ejecutables (Makefile).
- Antes de proceder a la instalación definitiva, realizar una de prueba.
- Probar el funcionamiento del software.
- Si se generan archivos con los bits SUID y GUID activos, comprobar que tengan los privilegios mínimos necesarios.

Procedimientos

Monitorizar los archivos:

- Comprobar propietarios y permisos de los archivos importantes de configuración del sistema.
- Verificar la integridad de archivos binarios del sistema.
- Verificar la presencia o ausencia de ciertos archivos.
- Verificar la integridad interna de los sistemas de archivos.

Procedimientos

Monitorizar la actividad del sistema:

- Procesos.
- Intentos fallidos de entrada.
- Intentos de entrada del superusuario.
- Tareas realizadas por el superusuario.
- Lo que hacen los usuarios.
- Auditar los eventos importantes del sistema.

FIN