Capítulo 3.
SEGURIDAD LÓGICA

Autor: Jesús Costas Santos

SEGURIDAD LÓGICA

Índice de contenidos

SEGURIDAD LÓGICA

3.1 PRINCIPIOS DE LA SEGURIDAD LÓGICA

- *Aplicación de barreras y procedimientos que resguarden el acceso a los datos y solo se permita acceder a ellos a las personas autorizadas*.
  - Capítulo 3: seguridad de acceso lógico a sistemas y políticas de privilegios a usuarios y grupos.
  - Capítulo 4: software *antimalware.*
  - Capítulo 5: Criptografía.

SEGURIDAD LÓGICA

3.1 PRINCIPIOS DE LA SEGURIDAD LÓGICA

- *En este tema estudiaremos:*
- **Control y medidas que impidan: Acceso y modificaciones no autorizadas a datos y aplicaciones**.
- Administración basada en el control de: identificación, autenticación y autorización de accesos.

SEGURIDAD LÓGICA

3.1 PRINCIPIOS DE LA SEGURIDAD LÓGICA

- ***Principio básico: todo lo que no está permitido debe estar prohibido.***

SEGURIDAD LÓGICA

3.2 CONTROL DE ACCESO LÓGICO

- Controlar el acceso conlleva 2 procesos:
  - Identificación: usuario se da a conocer en el sistema
  - Autenticación: verificación que realiza el sistema sobre esta identificación.
- Control a varios niveles:
  - Arranque: BIOS y gestor de arranque.
  - Sistema operativo y/o servidor de autenticación.
  - Datos, Aplicaciones y comunicaciones.

SEGURIDAD LÓGICA

3.2 CONTROL DE ACCESO LÓGICO

- Ataques:
  - Fuerza bruta: todas las combinaciones con un determinado conjunto de símbolos.
  - Diccionario: conjunto acotado a palabras y variaciones de éstas, con significado y utilizadas.
- Protección:
  - Máximo número de intentos.
  - Máxima Longitud de contraseña.
  - Ampliar el conjunto de símbolos posibles a utilizar.

SEGURIDAD LÓGICA

3.2.1 Política de contraseñas

- Recomendaciones contraseñas:
  - No incluir secuencias, palabras o nombres de usuario conocidos.
  - No dejar en blanco.
  - Variar entre servicios.
  - No revelarla, ni usarla en entornos poco seguros o públicos.
  - Modificarla con periodicidad.

SEGURIDAD LÓGICA

3.2.1 Política de contraseñas

- Configuración de políticas por administrador:
  - No dejar la seguridad en manos de usuario.
  - Disponer configuraciones que controle la configuración de contraseñas seguras.
  - Windows:
    - Directivas de seguridad local / Directivas de cuenta.
    - Visor de sucesos. Activar previamente auditorías.
  - GNU/Linux:
    - Módulo PAM_cracklib.
    - Control de intentos de login: **/var/log/auth.log**

SEGURIDAD LÓGICA

3.2.2 Control de acceso en la BIOS y gestor de arranque

- Peligros en el arranque:
  - Recuperación y modificación de contraseñas: arranque con distribuciones Live o gestor de arranque vulnerable.
- Seguridad en BIOS:
  - Protección de acceso físico a placa base.
  - Configuración (setup)→ contraseña.
  - Arranque (system)→ 1º dispositivo de arranque disco duro.

SEGURIDAD LÓGICA

3.2.2 Control de acceso en la BIOS y gestor de arranque

- Seguridad en gestor de arranque:
  - Ejemplo GRUB:
    - Contraseña a la edición del menú.
    - Contraseña al modo de recuperación.

SEGURIDAD LÓGICA

3.2.3 Control de acceso en el sistema operativo

- Auditoría de contraseñas de acceso:
  - Recuperación:
    - Windows: Ophcrack
    - GNU/Linux: John the ripper.
  - Modificación:
    - Windows: Arranque Live UBCD o acceso a consola y ejecución de control userpasswords2
    - GNU/Linux: acceso y modificación a /etc/shadow

SEGURIDAD LÓGICA

3.3 POLÍTICA DE USUARIOS Y GRUPOS

- Tarea fundamental del administrador de sistemas:
- Determinar nivel de seguridad de los datos y aplicaciones → **clasificar la información**, determinar el riesgo.
- Diversos niveles de la información requerirán diferentes medidas y niveles de seguridad.
- Definición de cuentas y su asignación a perfiles determinados, grupos o roles, así como asignación de privilegios sobre los objetos del sistema.

SEGURIDAD LÓGICA

3.3 POLÍTICA DE USUARIOS Y GRUPOS

- Permisos de acceso a cada objeto del sistema. Gestión en red LDAP / Active Directory.
  - Windows: Directivas de seguridad local: **Directiva de auditoría**, **Asignación de derechos de usuario** u **Opciones de seguridad.**
  - GNU/Linux: chmod (modificar), chown (propietario), chgrp (grupo) permisos sobre archivos.
- Listas de control de acceso (**ACL**): permite asignar permisos a un usuario, sin tener en cuenta el grupo al que pertenece.
  - Windows: cacls.
  - GNU/Linux: **getfacl** (ver) y **setfacl** (modificar-asignar) información de permisos sobre un archivo.

SEGURIDAD LÓGICA

DIRECCIONES DE INTERÉS

- Sitio web sobre seguridad informática de Microsoft:
  - http://www.microsoft.com/spain/protect/
- Manual de administración segura de GNU/Linux:
  - http://es.tldp.org/Manuales-LuCAS/GSAL/gsal-19991128.pdf
- Seguridad en GNU/Linux:
  - http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/MonogSO/SEGLIN00.html
- Administración de aspectos de seguridad en GNU/Linux y Windows:
  - http://www.adminso.es/wiki/index.php/
- Cómo de fuerte es tu contraseña:
  - http://howsecureismypassword.net/
- Comprobador de contraseñas de Microsoft:
  - http://www.microsoft.com/latam/protect/yourself/password/checker.mspx
- Administración de usuarios en GNU/Linux:
  - http://www.linuxtotal.com.mx/index.php?cont=info_admon_008
- Comprueba la fortaleza y generador de claves. Password tools bund. Disponible en Sourceforge:
  - http://sourceforge.net/projects/pwdstr/
- Recomendaciones para la creación y uso de contraseñas seguras de Inteco.
  - http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Notas_y_Articulos/recomendaciones_creacion_uso_contrasenas

SEGURIDAD LÓGICA

SOFTWARE

- **Pam_cracklib**: Módulo PAM de control de autenticación de usuarios en sistemas GNU/Linux.
  - http://fferrer.dsic.upv.es/cursos/Linux/Avanzado/HTML/ch11.html
- Algunas **distribuciones** arrancables en modo **Live**, con aplicaciones de recuperación y modificación de contraseñas de sistemas:
  - **Ultimate Boot CD (UBCD)**: distribución entorno simulado Windows aplicaciones como antivirus, recuperación de datos, aplicaciones de recuperación y borrado de contraseñas de la BIOS (cmos_pwd), borrado y restitución de nuevas contraseñas de usuarios de sistemas Windows instalados en disco, incluso creación de nuevas cuentas de usuario administrador.
    - http://www.ultimatebootcd.com/
  - **Backtrack**: distribución específica con un conjunto de herramientas de auditorías de seguridad, entre otras algunas que permiten escalada de privilegios en sistemas Windows (ophcrack) y GNU/Linux (John the ripper).
    - http://www.backtrack-linux.org/
  - **Ophcrack**: Distribución específica que contiene la aplicación de mismo nombre con capacidad de extraer contraseñas de usuarios en sistemas Windows.
    - http://ophcrack.sourceforge.net/
  - **Slax**: Distribución basada en Slackware, muy ligera y arrancable desde USB. Permite el montaje y acceso a los sistemas de ficheros instalados en disco.
    - http://www.slax.org/
  - **Wifiway y Wifislax**: distribuciones orientadas a realizar auditorías wireless, como recuperación de contraseñas.
    - www.wifiway.org/ y http://www.wifislax.com/

SEGURIDAD LÓGICA

SOFTWARE

- **John the ripper**: software de recuperación de contraseñas. Especializado en contraseñas de sistemas GNU/Linux.
  - http://www.openwall.com/john
- **Generador de funciones hash-resumen**: Cifrado de texto plano mediante diversos algoritmos como MD5 o SHA.
  - http://www.hashgenerator.de/
- **Windows SteadyState:** control y administración de usuarios y seguridad de sistemas Windows de forma centralizada y sencilla.
  - http://www.microsoft.com/spain/protect/products/family/steadystate.mspx
- **Keepass Password Safe:** administrador de contraseñas de diversas cuentas como mail, bancos, etc.
  - keepass.info/
- **DeepFreeze: congelador de sistemas operativos. Permite arrancar el sistema siempre con una configuración predeterminada.**
  - www.faronics.com/

SEGURIDAD LÓGICA

NOTICIAS

- **Utilizando mapas como contraseñas de acceso, una nueva idea de seguridad informática**
  - http://noticias.lainformacion.com/ciencia-y-tecnologia/tecnologia-general/utilizando-mapas-como-contrasenas-de-acceso-una-nueva-idea-de-seguridad-informatica_Kt8uDQyuXZu27JJbyXmVr4/
- **Artículo sobre "Recomendaciones para la creación y uso de contraseñas seguras" de Inteco, disponible en la siguiente página web:**
  - **http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Notas_y_Articulos/recomendaciones_creacion_uso_contrasenas.**
- **Artículo sobre el uso de cuentas limitadas y administrador en sistemas Windows:**
  - **http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Notas_y_Articulos/cuenta_administrador_vs_limitada**