SAD - U3.1. Seguridad lógica

Descargar estos apuntes

Índice

1. Seguridad lógica

La **seguridad lógica** es una disciplina que se encarga de proteger la información y los sistemas informáticos de posibles amenazas. Para ello, se utilizan técnicas y herramientas que permiten garantizar la confidencialidad, integridad y disponibilidad de la información.

La seguridad lógica es una parte fundamental de la seguridad informática, ya que protege los sistemas de posibles ataques y evita que la información sensible caiga en manos de personas no autorizadas.

1.1. Políticas de seguridad corporativa

La primera medida de seguridad lógica que debe adoptar una empresa es establecer unas normas claras en las que se indique qué se puede y qué no se puede hacer al operar con un sistema informático. Estas normas marcan las pautas generales de utilización del sistema y configuran el marco de actuación de todos los usuarios.

En sentido genérico, el conjunto de normas que definen las medidas de seguridad y los protocolos de actuación a seguir en la operativa del sistema reciben el nombre de **políticas de seguridad corporativa** en materia informática.

Estas normas son aplicables a toda la empresa, por lo que todos los departamentos de la misma deben estar implicados en su elaboración, ya que todos van a tener que cumplirlas. Además, la política genérica engloba, a su vez, las distintas normas específicas aplicables a cada sector de la empresa, que estarán adaptadas, en cada caso, a los niveles específicos de seguridad de cada sector.

Algunas de las medidas o mecanismos establecidos en las políticas de seguridad
son las siguientes:

- **Autenticación de usuarios**: sistema que trata de evitar accesos indebidos a la información a través de un proceso de identificación de usuarios, que en muchos casos se realiza mediante un nombre de usuario y una contraseña.
- **Listas de control de acceso**: mecanismos que controlan qué usuarios, roles o grupos de usuarios pueden realizar qué cosas sobre los recursos del sistema operativo.
- **Criptografía**: técnica que consiste en transformar un mensaje comprensible en otro cifrado según algún algoritmo complejo para evitar que personas no autorizadas accedan o modifiquen la información.
- **Certificados digitales**: documentos digitales, identificados por un número de serie único y con un periodo de validez incluido en el propio certificado, mediante los cuales una autoridad de certificación acredita la identidad de su propietario vinculándolo con una clave pública.

- **Firmas digitales**: es el conjunto de datos, en forma electrónica, consignados junto a otros o asociados con ellos que pueden ser utilizados como medio de identificación del firmante. Ejemplo: DNI electrónico.
- **Cifrado de unidades de disco o sistemas de archivos**: medidas que protegen la confidencialidad de la información.

1.2. Acceso a sistemas operativos y aplicaciones

Como hemos visto, para acceder a la información almacenada en un sistema informático en primer lugar hay que superar las barreras físicas de acceso. Una vez superadas estas barreras, el siguiente paso en materia de seguridad será establecer unas barreras lógicas que impidan el acceso a nuestros datos.

La primera barrera lógica que se puede establecer es la creación de **mecanismos de control de acceso** a la información. Para ello, en vez de que al encender los equipos se pueda acceder directamente a todos los datos almacenados en los mismos, una primera medida sería la creación de usuarios para organizar la información, de forma que cada usuario únicamente pudiera acceder a la información de la cuenta para la que dispone de autorización.

Las **cuentas de usuario** permiten asignar a cada uno de ellos unos derechos y privilegios que restringirán las operaciones que este va a poder realizar dentro de un sistema informático, así como la posibilidad de rastrear dichas operaciones. Como sistema de verificación de la identidad de cada uno de los usuarios se suele establecer la combinación entre un nombre identificativo (usuario, user, etc.), con la de una contraseña o password.

Si se trabaja en un entorno de red, es posible que, para acceder a algún recurso de la misma, se exijan unas credenciales determinadas, establecidas a través de las **listas de control de acceso (ACL, Access Control List)** que . Además, en las redes, los dispositivos de red, como los routers, pueden servir de barrera lógica impidiendo el acceso a determinadas zonas de la red para algunos usuarios (asignándoles un rango restrictivo de direcciones IP).

1.2.1 Contraseñas

En el ámbito informático podemos, por tanto, decir que `una contraseña es un sistema de autenticación de usuarios` compuesto por una combinación de símbolos (números, letras y otros signos).

En determinados supuestos, basta con conocer la contraseña para controlar un dispositivo informático, como por ejemplo un teléfono móvil. Sin embargo, lo habitual es que un mismo sistema pueda ser usado por diferentes usuarios, por lo que cada contraseña va asociada a un usuario del sistema.
De esta forma, para acceder al mismo, el usuario debe proporcionar su código identificador y la contraseña asociada a este y el sistema comprueba si ambos datos son correctos y si se corresponden entre sí, en cuyo caso habilita el acceso.

Por lo tanto, cuanto más robusta sea una contraseña más difícil resultará acceder a la información protegida por la misma. Una contraseña muy difícil de averiguar por alguien que no la conozca aporta seguridad a un sistema, pero no basta. En efecto, de nada sirve tener una contraseña muy difícil de averiguar si la guardamos de forma que sea fácilmente accesible, si la revelamos indiscriminadamente a terceras personas o si la comunicamos sin tomar medidas de seguridad que impidan que otras personas puedan interceptar nuestra comunicación y obtenerla.

Por tanto, como administradores de un sistema informático, hay que ser estrictos a la hora de controlar las contraseñas de acceso al sistema desde todos los puntos de vista: fortaleza, almacenamiento y comunicación de las mismas.

> **John The Ripper**
>
> John The Ripper es una herramienta originalmente diseñada para averiguar contraseñas a través de ataques de fuerza bruta.

Debido a esto, se suele utilizar por los administradores de sistemas para comprobar la robustez de las contraseñas de los mismos y su vulnerabilidad a ataques de hackers utilizando las mismas herramientas que estos.

1.2.2. Amenazas para las contraseñas

Si alguien intenta acceder a un sistema informático protegido con contraseña, previamente deberá averiguar esta. Cuanto más robusta sea una contraseña, más difícil será averiguarla. Una combinación de cifras, números y otros caracteres hace que sea más fuerte, pero hay que tener en cuenta que los usuarios son seres humanos y tienden a establecer contraseñas fáciles de recordar, por lo que es habitual que los sistemas establezcan restricciones que obliguen a los usuarios a cumplir unas determinadas normas a la hora de seleccionar sus contraseñas.

Ahora bien, por muy sencilla que sea la contraseña, los intrusos deben poner en práctica algún sistema para averiguarla. Existen diversos sistemas para tratar de averiguar las contraseñas, los más habituales son los siguientes:

- Utilización de **sniffers**: programas que registran la actividad de un equipo informático y pueden interceptar las comunicaciones “escuchando” para obtener datos como las contraseñas.
- Uso de **keyloggers**: son programas o dispositivos cuyo fin es capturar las pulsaciones en un teclado, con lo que se pueden obtener las contraseñas que han sido escritas con ese teclado.
- Ataques por fuerza bruta: consisten en probar todas las combinaciones posibles de caracteres hasta encontrar la clave que permite acceder al sistema. Por esto, cuanto más larga sea la cadena de caracteres que tenga la clave más se dificulta el acceso, pues más tiempo requiere averiguar la contraseña: por ejemplo, `e345Tj6k3L9934pR` es más difícil de averiguar que `x4jT`.
- Ataques por diccionario: consisten en generar diccionarios con términos relacionados con el usuario y probar todas esas palabras como contraseñas para acceder a ese sistema. Suelen ser más eficaces que los ataques por fuerza bruta, ya que los usuarios tienden a establecer como contraseñas palabras de su idioma, pues son más fáciles de recordar. Por eso, a igualdad de longitud de la cadena de caracteres de la contraseña, cuanto menos significado y más caracteres tenga esta, más difícil será de hallar: por ejemplo, `hola` es mucho más fácil de averiguar que `x4jT`.
- Ataques por ingeniería social: consisten en engañar a los usuarios para que proporcionen sus contraseñas a los intrusos, haciéndose estos pasar por amigos, empleados de un banco, técnicos, etc.

Rockyou y la importancia de las contraseñas seguras

En 2009, un hacker consiguió acceder a un servidor de la empresa Rockyou y robar un archivo con más de 32 millones de contraseñas. Este archivo, conocido como `rockyou.txt`, se convirtió en una de las mayores filtraciones de contraseñas de la historia y puso de manifiesto la importancia de utilizar contraseñas seguras para proteger la información y los sistemas informáticos.

RockYou.txt: El archivo de contraseñas que cambió la ciberseguridad

Contraseñas seguras

Actividad 1.1 Descarga e instala la versión gratuita de Revealer Keylogger de teclado SO Windows.

- ¿Para qué actividades maliciosas puede utilizarse este software?
- ¿Puede considerarse este software un tipo de spyware?
- ¿Qué estrategias pueden emplearse para evitar el efecto del software de este tipo?

Actividad 1.2 Ataques a contraseñas

> Esta actividad se puede realizar en grupos de dos alumnos.

El administrador de sistemas ha decidido comprobar la calidad de las contraseñas de su sistema operativo Linux utilizando las herramientas John The Ripper / Hashcat para auditar las contraseñas. De momento quiere probar la herramienta con tres usuarios, que son: **webmaster** (contraseña: admin), **plopez** (contraseña: pepe-el-decuentas), **mrobles** (contraseña: 123responda)

- Crea estos tres usuarios en tu sistema Linux. (Kali).
- Investiga cómo se utiliza John The Ripper y responde a las siguientes cuestiones:
  John The Ripper - Password Cracker / Cómo usar John The Ripper
  - ¿Qué es John The Ripper y para qué se utiliza?
  - ¿Qué tipos de ataques de contraseñas puede realizar John The Ripper?
  - ¿Cómo se instala y se utiliza John The Ripper en un sistema Linux?
  - ¿Qué resultados obtienes al utilizar John The Ripper con los usuarios creados?
- Investiga cómo se utiliza Hashcat y responde a las siguientes cuestiones:
  Hashcat - Advanced Password Recovery
  - ¿Qué es Hashcat y para qué se utiliza?
  - ¿Qué tipos de ataques de contraseñas puede realizar Hashcat?
  - ¿Cómo se instala y se utiliza Hashcat en un sistema Linux?
  - ¿Qué resultados obtienes al utilizar Hashcat con los usuarios creados?

1.3. Amenazas a la seguridad lógica

La seguridad lógica se enfrenta a diversas amenazas que pueden poner en peligro la información y los sistemas informáticos. Algunas de las amenazas más comunes son:

- **Virus y malware**: programas maliciosos que infectan los sistemas informáticos y pueden robar información o dañar los sistemas.
- **Ataques de denegación de servicio (DDoS)**: ataques que saturan los servidores con tráfico falso para impedir el acceso a los usuarios legítimos.
- **Phishing**: técnicas de engaño utilizadas para robar información confidencial, como contraseñas o datos bancarios.
- **Ingeniería social**: técnicas de manipulación utilizadas para engañar a las personas y obtener información confidencial.
- **Ataques de fuerza bruta**: ataques que intentan adivinar contraseñas probando todas las combinaciones posibles.
- **Ataques de inyección de código**: ataques que insertan código malicioso en las aplicaciones web para robar información o dañar los sistemas.
- **Ataques de suplantación de identidad (spoofing)**: ataques que falsifican la identidad de una persona o sistema para engañar a los usuarios.
- **Ataques de interceptación de comunicaciones**: ataques que interceptan las comunicaciones entre dos sistemas para robar información confidencial.
- **Ataques de explotación de vulnerabilidades**: ataques que aprovechan las vulnerabilidades de los sistemas para obtener acceso no autorizado
- **Ataques de ransomware**: ataques que cifran los datos de los sistemas y piden un rescate para recuperarlos.

Para prevenir y neutralizar este tipo de ataques, existen las llamadas herramientas antimalware, que pueden ser generales o orientadas a un cierto tipo específico de malware, por ejemplo, las herramientas antispyware. Los programas antimalware se distribuyen en diferentes modalidades: de escritorio, en línea, portátiles o en soporte Live. Además, soportan diferentes mecanismos y características para mejorar la protección.

Amezanas y ataques

Actividad 1.3 Define los siguientes tipos de atacantes:

Atacante	Descripción
a. Hacker	
b. Cracker	
c. Phreaker	
d. Sniffer	
e. Newbie	
f. Lamer	
g. Ciberterrorista	
h. Script kiddies	
i. Black-hat hacker	
j. White-hat hacker	
k. Troll	
l. Hacktivista	

Actividad 1.4 Define los siguientes términos:

Término	Descripción
a. Virus	
b. Gusano	
c. Troyano	
d. Spyware	
e. Adware	
f. Rootkit	
g. Ransomware	
h. Botnet	
i. Criptojacking	
j. Riskware	
k. Backdoor	

Actividad 1.5 Muchos fabricantes de software antimalware proporcionan versiones funcionales y gratuitas de sus productos. ¿Cuál es el modelo de negocio de estos fabricantes?

Actividad 1.6 Explica en qué consisten las siguientes características propias de herramientas antimalware actuales. Puedes consultar los sitios web de los principales fabricantes.

Característica	Descripción
a. Protección en tiempo real	
b. Protección planificada (o bajo demanda)	
c. Protección heurística (infecciones de malware de día cero)	
d. Actualización automática de base de datos	
e. Bloqueo de páginas web maliciosas conocidas o desconocidas (día cero)	
f. Sandbox	
g. Cuarentena	