solo el bloque que ha producido un fallo sino varios bloques contiguos a éste, en previsión de que próximamente se tenga que acceder a ellos. Solo resulta útil en archivos de acceso secuencial.

Preguntas de autoevaluación tema 10

10.1. ¿Cuáles son los objetivos, desde el punto de vista de la seguridad, que debe cumplir un sistema informático?

- ***Confidencialidad.*** Los datos solo deben ser leidos por aquellos usuarios autorizados o por el propietario de los datos.
- ***Integridad.*** El contenido de los datos únicamente pueden ser modificados por su propietario y usuarios autorizados por el.
- ***Disponibilidad.*** Los recursos del sistema deben encontrarse disponibles para los usuarios autorizados.

10.2. ¿Cuándo se considera que un sistema informático se encuentra en un estado seguro?

Cuando sus recursos hardware y software son accedidos y utilizados únicamente por los usuarios autorizados según una política de seguridad preestablecida.

10.3. ¿Qué afirma el principio del mínimo privilegio?

Cada usuario debe tener los mínimos derechos de acceso necesarios para completar tareas que está autorizado a realizar.

10.4. ¿En qué consisten las políticas de seguridad de control de acceso discrecional?

Son definidas por el propietario de un recurso y especifican cuáles son los derechos de acceso de los restantes usuarios a dicho recurso.

¿Y las políticas de control de acceso obligatorio?

Definidas a nivel de diseño del sistema, regulan el acceso y flujo de información dentro del mismo.

10.5. Señalar algunas técnicas de autenticación de usuarios.

Nombre de usuario y contraseña, objeto físico, rasgo fisiológico.

10.6. ¿Cómo se mide la eficacia de un mecanismo de autenticación?

Se mide por el porcentaje de intrusos a los que se les concede el acceso y el porcentaje de usuarios legítimos a los que se les deniega acceso.

10.7. ¿Qué técnicas se pueden emplear para reforzar la seguridad del mecanismo de autenticación por contraseñas?

Envejecimiento de contraseñas: Las contraseñas solo son validas durante un periodo de tiempo, transcurrido el cual expiran y deben ser cambiadas.

Contraseñas de un solo uso: La contraseña expira cuando finaliza la sesión de usuario, por lo que cuando inicia otra vez debe usar una nueva contraseña. Para ello posee un libro de contraseñas que se han de usar en orden.

Reto dinámico: El sistema presenta al usuario un reto que debe resolver para acceder o para poder continuar trabajando.

10.8. ¿Qué es el software malicioso?

Aquel diseñado para causar daños o utilizar recursos de un computador sin el conocimiento y consentimiento de sus usuarios legítimos.

10.9. ¿Qué es una bomba lógica?

Un fragmento de código insertado en un programa legítimo que únicamente se activa cuando se cumplen o dejan de darse unas condiciones prestablecidas, como por ejemplo, una fecha y hora determinadas. Una vez activada puede provocar diferentes acciones: modificar, encriptar o borrar los archivos del disco duro, detener el computador, mostrar un mensaje por pantalla, enviar correos electrónicos, reproducir una canción o un video, etc.

10.10. ¿Qué es una puerta secreta?

Un fragmento de código insertado en un programa o sistema con la finalidad de poder saltarse los procedimientos de autentificación o ganar privilegios. Se activa al introducir ciertas secuencias especiales de entrada o una determinada secuencia de eventos.

10.11. ¿Qué es un caballo de Troya?

Es un programa aparentemente inofensivo que aparte de realizar aparentemente la función para la que está diseñado realiza una función desconocida y no deseable por el usuario del programa,

como borrado de archivos, envío de información al intruso o permitir acceso remoto del intruso al sistema.

10.12. ¿Qué es un virus?

Un fragmento de código insertado dentro del código de un programa anfitrión que se ejecuta si el usuario abre el programa anfitrión. Un virus puede realizar diferentes funciones nocivas, como por ejemplo el borrado de archivos, funciones molestas como mensajes en pantallas. Además un virus se propaga insertando copias de su código en otros archivos entre usuarios. Un computador se infecta cuando el usuario ejecuta un programa infectado.

Tienen hasta cuatro fases: latente, propagación, activación y ejecución en este orden.

Otra forma de virus utilizada en los últimos años son los virus insertados en macros, que son programas ejecutables embebidos en un documento de un procesador de texto, hoja de cálculo u otro archivo.

10.13. ¿Qué es un gusano informático?

Es un programa capaz de reproducirse y propagarse a otros computadores, generalmente a través de una red informática. Básicamente provoca una denegación del servicio o un servicio deficiente ya que en su función de reproducción realiza un consumo desproporcionado de recursos de los computadores y del ancho de banda de la red por la que se propaga.

10.14. ¿Qué es un programa espía?

Es un programa que se instala de forma furtiva en el computador por un virus o troyano y que se dedica a recopilar información sobre la actividad de sus usuarios para enviárselas a terceros.

¿Qué tipo de información recopila?

Entre la información que recopila se encuentran datos de conexión a Internet, clave de e-mail, mensajes enviados y recibidos, páginas web visitadas, descargas e información intercambiada a través de formularios electrónicos.

10.15. ¿Qué establece un dominio de protección?

Establece para un subconjunto de objetos las operaciones emitidas o derechos de acceso de cada uno de ellos. De esta forma

un dominio queda definido por un conjunto de pares de la forma [objetos, derechos].

10.16. ¿Qué información contiene la matriz de acceso?

Cada fila i está asociada a un dominio Di, mientras que cada columna j a un objeto Oj. Cada elemento Aij contiene los derechos de acceso asociados al objeto Oj dentro del dominio Di.

10.17. Explicar la implementación de la matriz de acceso como listas de control de acceso.

Consiste en asociar con cada objeto una lista denominada lista de control de acceso (ACL). Cada entrada contiene pares de la forma [dominio, derechos].

Cuando un proceso va a acceder a un objeto, se consulta su ACL usando como parámetro de búsqueda el dominio de protección. Si un dominio Di no tiene una entrada en la lista eso significa que no tiene ningún derecho sobre el objeto y se produce una excepción. Si el dominio Di tiene una entrada en la lista, se comprueba que los derechos en el dominio Di sobre el objeto permiten realizar la operación solicitada. En caso contrario se deniega el acceso.

La ventaja es que permite fácilmente revocar derechos de forma selectiva sobre objetos que pueden estar en varios dominios. El inconveniente es que la ACL se comprueba en cada acceso al objeto. Si los accesos son frecuentes y la lista larga se pierde tiempo en la búsqueda. Se puede reducir el número de entradas de las ACL.

10.18. Explicar la implementación de la matriz de acceso como listas de capacidades.

Cada entrada de la lista contiene un identificador de objeto, que indica la localización del objeto o de una estructura de datos que contiene su localización, y sus derechos de acceso. A la dupla (objeto, derechos) se le denomina capacidad.

Una posible implementación es almacenarla en el espacio de direcciones del núcleo y asociar a cada capacidad un identificador numérico que coincide con su posición en la lista. Cuando un proceso está ejecutándose dentro de un cierto dominio desea realizar una cierta operación sobre un objeto, éste debe especificar

como parámetro en la correspondiente llamada al sistema el identificador de la capacidad.

¿Cuáles son sus ventajas e inconvenientes?

Una de las ventajas es que el acceso al contenido es muy rápido, ya que no se realizan búsquedas dentro de la lista puesto que el propio proceso indica al SO la posición de la capacidad en la lista. Otra ventaja es que permite encapsular a los procesos fácilmente, basta con asociarles un determinado dominio, algo que no es posible con las ACLs.

Un inconveniente de esta implementación es el coste que supone para el sistema la revocación de los permisos para un objeto en concreto, ay que requiere acceder a todas las listas de capacidades existentes, y buscar en cada una si existe la capacidad que se desea revocar.

10.19. ¿Cuándo se puede afirmar que un sistema es confiable?

Cuando cumple con los requerimientos de seguridad o política de seguridad que se había impuesto.

10.20. ¿Qué es una TCB?

Base de computador confiable (Trusted computer base) es un conjunto de elementos hardware y software que le permiten implementar los requisitos de seguridad establecidos.

¿Cuáles son las funciones del sistema operativo que debe incluir?

Entre las funciones que debe incluir se encuentran las relativas a creación de procesos, cambio de contexto, gestión de memoria y parte de la gestión de la E/S y del sistema de archivos.

10.21. ¿Qué función realiza el monitor de referencia de una TCB?

Se encarga de comprobar todas las llamadas al sistema que puedan comprometer la seguridad del sistema, como la creación de procesos o la apertura de archivos, y decidir si pueden ser procesadas o rechazadas. Nótese que el monitor de referencia toma las decisiones en base a la política de seguridad que se haya decidido seguir en el sistema que se plasma en el contenido de la matriz de acceso.

10.22. ¿Qué es un sistema de seguridad multinivel?

Un modelo que distingue varios niveles de seguridad. A cada objeto y usuario se le asigna un determinado nivel. El modelo debe

especificar un conjunto de reglas para establecer el acceso de los usuarios a la información (objetos).

10.23. ¿Qué reglas sigue el modelo de seguridad multinivel de Bell y La Padula?

- ***Imposibilidad de leer objetos de niveles superiores.***
- ***Imposibilidad de escribir objetos de niveles inferiores.***

Si se cumplen estas dos reglas se puede garantizar que no existirán fugas de información desde un nivel de seguridad superior hacia un nivel inferior.

10.24. Señalar los principios de diseño de sistemas operativos seguros propuestos por Saltzer y Sehr.

- ***El diseño debe ser público*.**
- ***El estado por defecto es el de no acceso.***
- ***Comprobación de los derechos de acceso.***
- ***Principio del mínimo privilegios.***
- ***Los mecanismos de protección deben ser simples y estar integrados en las capas más bajas del sistema.***
- ***Los mecanismos de protección deben ser aceptados por los usuarios.***
- ***Los mecanismos de protección deben ser aceptados por los usuarios.***
- ***Los mejores diseños son los más sencillos.***