INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE COMPUTO

UNIDAD DE APRENDIZAJE: SISTEMAS OPERATIVOS

TAREA 06: “SEGURIDAD Y VIRTUALIZACIÓN”

NOMBRE: FARRERA MENDEZ EMMANUEL SINAI

NUMERO DE LISTA: 8

PROFESOR: ARAUJO DIAZ DAVID

GRUPO: 4CM3

FECHA DE ENTREGA: 20 DE JUNIO DEL 2023

(la respuesta estará en el siguiente formato: **respuesta**, en negritas y subrayado)

1.- ¿Cuáles son las dos facetas que tiene la seguridad?

Dos de las más importantes son la perdida de datos y los intrusos.

2.- Mencione tres causas comunes de perdida de datos.

- **Actos divinos: Incendios, inundaciones, terremotos, guerras, revoluciones o ratas que roen las cintas o discos flexibles.**
- **Errores de Hardware o Software: Mal funcionamiento de la CPU, discos o cintas ilegibles, errores de telecomunicación o errores en el programa.**
- **Errores Humanos: Entrada incorrecta de datos, mal montaje de las cintas o el disco, ejecución incorrecta del programa, perdida de cintas o discos.**

3.- ¿Cuáles son las dos clases de intrusos (descríbalos brevemente)?

Los intrusos pasivos solo desean leer archivos que no están autorizados a leer.

Los intrusos activos son más crueles: Desean hacer cambios no autorizados a los datos.

4.- ¿Cuáles son algunas categorías comunes de intrusos activos?

Curiosidad casual de usuarios no técnicos. Muchas personas tienen en sus escritorios terminales para sistemas con tiempo compartido y, por la naturaleza humana, algunos de ellos leerán el correo electrónico de los demás u otros archivos, si no existen barreras en frente de ellos. Por ejemplo, la mayoría de los sistema UNIS tienen predefinido que todos los archivos se pueden leer de manera pública.

Conocidos husmeando. Algunos estudiantes, programadores de sistemas, operadores y demás personal técnico consideran como un reto personal romper la seguridad del sistema de cómputo local. A menudo son muy calificados y están dispuestos a invertir una cantidad sustancial de su tiempo en este esfuerzo.

Un intento deliberado de hacer dinero. Algunos programadores en banco han intentado penetrar un sistema bancario con el fin de robarle al banco. Los esquemas han variado desde cambiar el software para truncar y no redondear el interés, para quedarse con una pequeña fracción de dinero, hasta sacar dinero de las cuentas que no se han utilizado en anos o el "correo negro" .

Espionaje comercias o militar. El espionaje indica un intento serio y fundamentado por parte de un competidor u otro país para robar programas, secretos comerciales, patentes, tecnología, diseño de circuitos, planes de comercialización, z etc. A menudo, este intento implica la cobertura de cables o el levantamiento de antenas hacia la computadora con el fin de recoger su radiación electromagnética.

5.- En qué consiste la seguridad física.

El nodo o nodos que contengan los sistemas informáticos deben dotarse de medidas de seguridad físicas frente a posibles intrusiones armadas o subrepticias por parte de potenciales intrusos.

6.- ¿Qué incluye la seguridad física?

Hay que dotar de seguridad tanto a las habitaciones donde las maquinas residan como a los terminales o estaciones de trabajo que tengan acceso a dichas maquinas.

7.- ¿Cuáles son los mecanismos de protección de la seguridad física?

Los mecanismos de seguridad física se relacionan con la protección del hardware del sistema.

En función del sistema que se trate, los mecanismos que se emplean son más o menos sofisticados. Así, en entornos sencillos las medidas de seguridad son simples y fáciles de aplicar. Sin embargo, es más común que los sistemas empresariales dispongan de un punto neurálgico llamado CPD (Centro de Proceso de Datos) Habitualmente este lugar es cuarto de telecomunicaciones, donde se alojan los servidores y electrónica de red base del sistema.

8.- ¿Qué trata de impedir la seguridad física?

Son los incendios, robos, secuestros, homicidios, suplantación y robo de información, que se analizan y designan según la probabilidad de amenaza (altamente probable, probable, poco probable y probabilidad desconocida)

9.- ¿En qué consiste la seguridad operacional?

La seguridad operacional en el área de informática pretende identificar las amenazas y reducir los riesgos al detectar las vulnerabilidades incapacitando o minimizando así el impacto o efecto nocivo sobre la organización.

10.- ¿Qué es la verificación de autenticidad de usuarios?

La autenticación consiste en la verificación de las credenciales con las que se identificó el usuario, es decir, se demuestra que realmente es quién dice ser. Estas credenciales son conocidas como factores de autenticación. La autorización son las acciones que se permiten realizar al usuario con dichas credenciales.

11.- ¿Cómo funciona y que problemas existen al emplear una contraseña como medida de seguridad?

La seguridad de la contraseña es una medida de la efectividad de una contraseña contra ataques de adivinación o de fuerza bruta. En su forma habitual, estima cuántas pruebas necesitaría un atacante que no tiene acceso directo a la contraseña, en promedio, para adivinarla correctamente. La seguridad de una contraseña depende de la longitud, la complejidad y la imprevisibilidad.

12.- En que consiste la identificación física para seguridad.

La seguridad física identifica las amenazas, vulnerabilidades y las medidas que pueden ser utilizadas para proteger físicamente los recursos y la información de la organización.

13.- Mencione algunas medidas preventivas para seguridad.

1. **Controles de acceso a los datos más estrictos**
2. **Realizar copias de seguridad**
3. **Utilizar contraseñas seguras**

4. **Proteger el correo electrónico**
5. **Contratar un software integral de seguridad**
6. **Utilizar software DLP**
7. **Trabajar en la nube**
8. **Involucrar a toda la empresa en la seguridad**
9. **Monitorización continua y respuesta inmediata**

14.- Describa en qué consisten las matrices de protección para seguridad.

Una matriz de acceso es una representación abstracta del concepto de dominio de protección. Este modelo fue propuesto por Lampson como una descripción generalizada de mecanismos de protección en sistemas operativos. Es el modelo más utilizado, del que existen numerosas variaciones, especialmente en su implementación.

15.- ¿Qué son las listas de control de acceso?

Las listas de control de acceso (ACL) filtran el tráfico IP y protegen su red del acceso no autorizado. Una ACL es un conjunto de condiciones que el Citrix ADC evalúa para determinar si se permite el acceso. Por ejemplo, el departamento de Finanzas probablemente no quiera permitir que otros departamentos tengan acceso a sus recursos, como recursos humanos y documentación, y esos departamentos desean restringir el acceso a sus datos.

16.- ¿Qué es una lista de capacidades?

La otra posibilidad es almacenar la matriz por filas. En este caso, a cada proceso se le asocia una lista de capacidades. Cada capacidad corresponde a un objeto más las operaciones permitidas.

Cuando se usan capacidades, lo usual es que, para efectuar una operación M sobre un objeto O, el proceso ejecute la operación especificando un puntero a la capacidad correspondiente al objeto, en vez de un puntero al objeto. La sola posesión de la capacidad por parte del proceso quiere decir que tiene los derechos que en ella se indican. Por lo tanto, obviamente, se debe evitar que los procesos puedan "falsificar" capacidades.

17.- Describa el estándar de niveles de seguridad TCSEC Orange Book (TCSEC -Trusted Computer System Evaluation Criteria).

El TCSEC define cuatro divisiones de seguridad, a saber: D, C, B y A, donde la división A tiene la seguridad más alta. Cada división representa una diferencia significativa en la confianza que un individuo u organización puede colocar en el sistema evaluado. Además, las divisiones C, B y A se subdividen, a su vez, en una serie de grupos jerárquicos llamados clases (C1, C2, B1, B2, B3 y A1) que expanden o modifican los requisitos de la división o clase inmediatamente superior

18.- ¿Cuál es el objetivo de la virtualización?

El objetivo es poner a disposición estos recursos a nivel virtual para distribuirlos entre los diferentes clientes de forma flexible en función de las necesidades de cada uno.

19.- ¿Cómo se le denomina a un sistema operativo diferente opera en la parte superior del sistema operativo principal?

Cuando un sistema operativo diferente opera en la parte superior del sistema operativo principal mediante la virtualización, se le denomina máquina virtual (VM).

20.- ¿Qué es un gestor de máquinas virtuales?

Los gestores de máquina virtual son partes de software que crean, gestionan y supervisan las máquinas virtuales

21.- ¿Qué características de funcionamiento son importantes para la virtualización?

Cuando el entorno virtual se está ejecutando, y un usuario o programa emite una instrucción que requiere recursos adicionales del entorno físico, el hipervisor transmite la solicitud al sistema físico y almacena los cambios en la caché. Todo esto sucede prácticamente a la misma velocidad que habría si este proceso se realizara dentro de la máquina física (en especial, si la solicitud se envía a través de un hipervisor open source diseñado a partir de la máquina virtual basada en el kernel [KVM]).

22.- ¿Qué es la emulación de un sistema operativo?

La emulación nos permite modelar hardware y software viejos y recrearlos utilizando tecnología actual. La emulación nos permite utilizar una plataforma actual para acceder a aplicaciones antiguas, sistemas operativos o datos mientras que el software antiguo aun «piensa» que sigue corriendo en su ambiente original.

23.- ¿Qué permite realizar la virtualización asistida por hardware?

La virtualización sirve principalmente para compartir los recursos de un servidor y optimizar el uso de sus procesadores. Asimismo, su puesta en marcha aumentará la calidad y agilidad de la infraestructura informática y mejorará en todo momento los tiempos de respuesta del servidor.

La virtualización asistida por hardware consiste básicamente en emular mediante máquinas virtuales, los componentes de hardware. Con ello, el sistema operativo no se ejecuta sobre el hardware real, sino sobre el virtual.

24.- ¿Cómo se realiza la virtualización de almacenamiento?

La virtualización de almacenamiento se entiende como la agrupación de los recursos del almacenamiento físico y almacenamiento lógico, de manera que la gestión de múltiples dispositivos de almacenamiento en red se simplifica al reunirlos en un único almacén, administrado desde una única consola central.

25.- Describa la virtualización de memoria.

El sistema operativo invitado administra las direcciones virtuales a físicas del invitado. El hipervisor solo es responsable de traducir las direcciones físicas del invitado a direcciones de la máquina. La virtualización de memoria asistida por hardware utiliza la funcionalidad de hardware para generar las asignaciones combinadas con las tablas de páginas del invitado y las tablas de páginas anidadas que mantiene el hipervisor.

El diagrama muestra la implementación de ESXi de la virtualización de memoria.

26.- Mencione en qué consiste la virtualización de aplicaciones.

La virtualización de aplicaciones es un proceso que hace creer a una aplicación estándar que está interactuando directamente con un sistema operativo cuando, de hecho, no es así. Para completar esta maniobra, es necesario que haya una capa de virtualización insertada entre la aplicación y el sistema operativo.

27.- Enliste los beneficios de la virtualización.

- **Reduce riegos y costes**
- **Ofrece la posibilidad de monitorización**
- **Habilita la migración en caliente de máquinas virtuales**
- **Mejora los procesos de clonación y copias de seguridad**
- **Aporta una mayor disponibilidad y fiabilidad**

28.- ¿Qué es la paravirtualización?

La paravirtualización es una técnica de programación informática que permite virtualizar por software sistemas operativos. El programa para virtualizador presenta una interfaz de manejo de máquinas virtuales. Cada máquina virtual se comporta como un computador independiente, por lo que permite usar un sistema operativo o varios por computador emulado.

29.- ¿Qué es un contenedor?

Los contenedores son una forma de virtualización del sistema operativo. Un solo contenedor se puede usar para ejecutar cualquier cosa, desde un microservicio o un proceso de software a una aplicación de mayor tamaño.

30.- ¿Cuál es la forma de trabajo de un contenedor?

Las VM se ejecutan en un entorno de hipervisor en el que cada máquina virtual debe incluir su propio sistema operativo invitado dentro del mismo, junto con sus archivos binarios, bibliotecas y archivos de aplicaciones correspondientes. Esto consume una gran cantidad de recursos y genera mucha sobrecarga, especialmente cuando se ejecutan varias VM en el mismo servidor físico, cada una con su propio sistema operativo invitado.

Por el contrario, cada contenedor comparte el mismo sistema operativo host o kernel del sistema y tiene un tamaño mucho menor, a menudo de solo unos megabytes. Esto suele implicar que un contenedor puede tardar unos segundos en iniciarse (en comparación con los gigabytes y los minutos necesarios que requiere una VM típica).

REFERENCIAS

6.5 Concepto de seguridad - Materia SisOperativos. (s. f.). google. Recuperado 5 de junio de 2022, de https://sites.google.com/site/materiasisoperativo/unidad-6-proteccion-y-seguridad/6-5-concepto-de-seguridad

de Sistemas, A., & Perfil, V. T. M. (s. f.). Seguridad Operacional En el Area de Informatica. perfil. Recuperado 5 de junio de 2022, de https://seguridadseccion04.blogspot.com/p/seguridadoperacional-laseguridad.html

colaboradores de Wikipedia. (s. f.). Wikipedia, la enciclopedia libre. wikipedia. Recuperado 5 de junio de 2022, de https://es.wikipedia.org/wiki/Wikipedia:Portada

SEGURIDAD Y MECANISMO DE PROTECCION EN LOS S.O. - carlos2987. (s. f.). google. Recuperado 5 de junio de 2022, de https://sites.google.com/site/carlosraulsan2987/home/sistemas-operativos/unidad- 6/seguridad-y-mecanismo-de-proteccion-en-los-so

J. (2017b, abril 28). TCSEC, el libro naranja de la seguridad informática. teknoPLOF! Recuperado 5 de junio de 2022, de https://www.teknoplof.com/2017/04/28/tcsec-libro-naranja-la Seguridadinformatica/#:%7E:text=El%20TCSEC%20define%20cuatro%20divisiones,colocar%20en%20el%20sistema%20evaluado.

Limones, E. (2021, 5 abril). Virtualización: Qué es, para qué sirve y ventajas. OpenWebinars.net. Recuperado 5 de junio de 2022, de https://openwebinars.net/blog/virtualizacion-que-es-para-que-sirve-y-ventajas/