

CURSO PARA LA OBTENCIÓN DEL

DIPLOMA DE INFORMÁTICA MILITAR

(59130)

Teoría de Sistemas Operativos

Capítulo 10. Preguntas y ejercicios

Índice

[1. Preguntas 3](#_Toc147863992)

# Preguntas

## ¿Cuál de los siguientes NO es un factor de autenticación comúnmente utilizado?

a) Contraseña

b) Huella dactilar

c) Color favorito

d) Tarjeta de acceso físico

## ¿Qué factor de autenticación se basa en algo que el usuario sabe?

a) Biometría

b) Token de seguridad

c) Contraseña

d) Tarjeta de acceso

## ¿Qué factor de autenticación se basa en algo que el usuario posee?

a) Contraseña

b) PIN

c) Certificado digital

d) Tarjeta de acceso físico

## ¿Qué factor de autenticación utiliza características físicas únicas del usuario, como su rostro o su voz?

a) Contraseña

b) Token de seguridad

c) Biometría

d) Tarjeta de acceso físico

## ¿Para qué se utiliza comúnmente una contraseña de BIOS o UEFI en una computadora?

a) Para cifrar el disco duro

b) Para proteger el sistema de ficheros de ataque por desbordamiento

c) Para evitar que se realicen cambios en la configuración del sistema

d) Para autenticar al usuario cuando accede al sistema operativo

## ¿Dónde se almacena típicamente la contraseña de BIOS o UEFI en una computadora?

a) En el disco duro

b) En un chip de memoria flash en la placa madre

c) En la memoria cache próxima a la RAM

d) En un servidor de contraseñas del sistema operativo

## . ¿Cuál de las siguientes contraseñas se consideraría más débil desde el punto de vista de la seguridad?

a) "P@ssw0rd"

b) "Choc0late!"

c) "Tr0ub4dor&3"

d) "S3cur3P@ssw0rd!"

## ¿Cuál de estas contraseñas es más difícil de adivinar por fuerza bruta? (k=longitud de la contraseña y n=números de símbolos utilizados)

a) k=4; n=26

b) k=6; n=26

c) k=4; n=36

d) k=8; n=26

## ¿Qué hace que una contraseña sea más fuerte desde el punto de vista de la seguridad?

a) Su longitud y total de alfanúmericos con símbolos utilizados

b) Su facilidad de memorización del algoritmo

c) Su uso de caracteres alfabéticos solamente

d) Su relación con datos personales, como nombres o fechas de nacimiento

## ¿Cuál de las siguientes contraseñas se consideraría más fuerte?

a) "123456"

b) "P@$$w0rd!"

c) "C0ffeeL0v3rs#2023"

d) "MyName123"

## ¿Se debe utilizar una contraseña única para diferentes cuentas en línea?

a) Si, facilita recordar las contraseñas

b) Si, se tiene menos riesgo de suplantación de identidad

c) No, se corre un riesgo de que un ataque en una cuenta comprometa a las otras

d) Si, para mejor compartir la contraseña con amigos y familiares

## ¿Qué deberías evitar al crear una contraseña?

a) Usar tu nombre o apellido

b) Hacerla lo más larga posible

c) Usar una combinación de letras y números

d) Cambiarla cada vez que inicies sesión

## ¿Qué tipo de información se almacena comúnmente en el archivo `/etc/passwd`?

a) Contraseñas de usuario cifradas

b) Nombres de usuario y contraseñas

c) Nombres de usuario y otra información de cuenta

d) Historial de inicio de sesión

## ¿Dónde se encuentra generalmente el archivo `passwd` en sistemas Unix y Linux?

a) En la carpeta de inicio de cada usuario

b) En la carpeta `/etc`

c) En la carpeta `/var`

d) En la carpeta `/home`

## ¿Cuál es el propósito del archivo `/etc/passwd`?

a) Almacenar las contraseñas de usuario en texto claro y cifrado

b) Almacenar información de grupos de usuarios del sistema

c) Proporcionar información sobre las cuentas de usuario del sistema

d) Registrar el historial de inicio de sesión de los usuarios

## ¿Cuál de las siguientes afirmaciones es cierta acerca del archivo `/etc/shadow`?

a) Sustituye a /etc/passwd en computadores modernos

b) Contiene contraseñas cifradas de usuarios

c) Hay un archivo de esa clase por cada grupo de usuarios

d) Contiene información sobre grupos de usuarios

## ¿Qué es el hashing de contraseñas?

a) Almacenar contraseñas en texto claro en el segmento hash de la memoria

b) Cifrar contraseñas con una clave secreta que el sistema operativo guarda en cache

c) Convertir contraseñas en una cadena de caracteres aleatoria.

d) Aplicar una función criptográfica para convertir una contraseña en un valor hash.

## ¿Cuál es el propósito principal de utilizar el hashing de contraseñas?

a) Aumentar la longitud de las contraseñas

b) Facilitar la recuperación de contraseñas olvidadas.

c) Proteger las contraseñas de los ataques de fuerza bruta

d) Proteger las contraseñas almacenando versiones irreversibles y seguras.

## ¿Cuál es la ventaja de usar un "salt" (sal) en el hashing de contraseñas?

a) Reduce la longitud de las contraseñas

b) Protege contra ataques de fuerza bruta.

c) Facilita la recuperación de contraseñas olvidadas.

d) Añade un bit de control a las contraseñas.

## ¿Qué es el salting en el contexto de la seguridad de contraseñas?

a) Agregar sal al agua para cocinar contraseñas.

b) Agregar un valor aleatorio único a una contraseña antes de aplicar el hashing.

c) Generar una contraseña a partir de la contraseña del grupo de usuarios

d) Eliminar las contraseñas del fichero passwd y generar otra con hashing en shadow

## . ¿Cuál es el propósito principal de agregar sal a las contraseñas antes de hashearlas?

a) Hacer que las contraseñas sean más fáciles de recordar.

b) Aumentar la longitud de las contraseñas hasta el límite del desbordamiento

c) Prevenir ataques de fuerza bruta y tablas arcoíris.

d) Cambiar la contraseña actual por una generada por hashing.

## ¿Cuál de las siguientes afirmaciones es cierta acerca del salting?

a) El mismo valor de sal se utiliza para todas las contraseñas en una base de datos.

b) El valor de sal es secreto y se almacena en el kernel del sistema operativo.

c) El salting solo es necesario para contraseñas largas.

d) El salting agrega un valor único a cada contraseña antes de hashearla.

## ¿Cuál es una ventaja del salting en la seguridad de contraseñas?

a) Facilita la recuperación de contraseñas olvidadas.

b) Hace que las contraseñas sean más cortas.

c) Protege contra ataques de diccionario y tablas arcoíris.

d) Aumenta la velocidad de autenticación.

## ¿Qué tipo de sistema de autenticación es el método de Lamport?

a) Basado en contraseñas

b) Basado en tokens de seguridad

c) Basado en firmas digitales

d) Basado en biometría

## ¿Cómo se genera una contraseña Lamport?

a) A través de una tarjeta de acceso físico.

b) Se calcula aplicando raleatoriamente una función hash a una contraseña cifrada.

c) Se calcula aplicando recusivamente función heap a una contraseña en texto claro.

d) Se calcula aplicando reiteradamente una función hash a una contraseña en texto claro.

## Una técnica común de ingeniería social online en la que los atacantes envían correos electrónicos o mensajes que parecen provenir de fuentes legítimas, pero las víctimas son dirigidas a estos sitios falsos, donde se les solicita que ingresen sus contraseñas y otra información confidencial. ¿De qué tipo de ataque estamos hablando?

1. De fuerza bruta
2. De Fishing
3. De Vishing
4. De botnet

## A la acción de la figura se le suele llamar:

1. Shoulder fishing
2. Fishing
3. Vishing
4. Visoning

## ¿Qué es un ataque de desbordamiento de búfer?

a) Un ataque que sobrecarga el búfer de impresión de una impresora con excesivos trabajos

b) Un ataque en el que un proceso sobrepasa el límite de memoria asignado a un búfer y sobrescribe la memoria adyacente.

c) Un ataque en el que un hacker sobrecarga el almacenamiento en búfer de una base de datos.

d) Un ataque que causa la pérdida de datos en un servidor por desbordamiento de la cache L3

## ¿Cuál es el objetivo principal de un ataque de desbordamiento de búfer?

a) Robar contraseñas del usuario

b) El desbordamiento intencional del espacio de una variable para inyectar código maligno

c) Aumentar la velocidad de procesamiento de una aplicación para llevarla fuera de control del kernel del sistema operativo

d) Aumentar el almacenamiento el búfer de la ALU en un sistema multicore

## ¿Qué tipo de vulnerabilidad de software es explotada típicamente en un ataque de desbordamiento de búfer?

a) Vulnerabilidad de seguridad física mediante tarjetas inteligentes

b) Vulnerabilidad de ingeniería social a través de botnet

c) Vulnerabilidad de software de programación deficiente.

d) Vulnerabilidad de hardware en cuanto se produce Rowhammer

## ¿Cuál es una consecuencia común de un ataque exitoso de desbordamiento de búfer?

a) la disminución del rendimiento del sistema en beneficio del proceso principal

b) La eliminación de malware.

c) La ejecución de código malicioso.

d) La mejora de la seguridad de la red.

## ¿Qué es un "Canario de Pila" en el contexto de la seguridad informática?

a) Es un desbordamiento del buffer no controlado por el sistema

b) Una técnica de ataque en la que se coloca un valor aleatorio en la pila y produce desbordamiento de buffer

c) Un valor aleatorio colocado en la pila de una función para detectar desbordamientos de búfer.

d) Un tipo de ataque de denegación de servicio.

## ¿Cuál es el propósito principal de un Canario de Pila?

a) Proteger la información encriptada en la pila.

b) Evitar que los atacantes accedan al heap del proceso en curso usando la técnica de Rowhammer

c) Detectar y prevenir desbordamientos de búfer y ataques de ejecución de código malicioso.

d) Detectar y prevenir los ataque mediante hashing de contraseñas controladas por diccionario.

## ¿Cómo funciona un Canario de Pila?

a) Encripta todos los datos en la pila para evitar cualquier ataque de tipo desbordamiento de contraseña

b) Registra las actividades del sistema operativo para calcular una estadística de los ataques recibidos.

c) Coloca un valor aleatorio en la pila antes de la dirección de retorno de una función y verifica su integridad antes de que la función retorne.

d) Desactiva la caché de la CPU.

## . ¿Cuál es uno de los problemas a resolver en la implementación de Canarios de Pila?

a) Requiere acceso físico al hardware de la computadora.

b) Puede causar conflictos de memoria en el sistema operativo.

c) Puede tener un impacto en el rendimiento de las aplicaciones.

d) Solo es efectivo contra amenazas de red.

## ¿En qué tipo de programas y sistemas operativos es común encontrar la implementación de Canarios de Pila?

a) Solo en sistemas macOS.

b) Solo en sistemas Unix/Linux.

c) En sistemas Windows y otros sistemas operativos.

d) Solo en servidores web.

## ¿Qué sucede si un atacante intenta desbordar un búfer en un programa que utiliza un Canario de Pila?

a) El atacante obtiene acceso a la memoria RAM y limpia las memorias caché

b) El Canario de Pila detecta el desbordamiento y detiene la ejecución del programa.

c) El Canario de Pila borra todos las variables dinámicas de la pila

d) El programa se bloquea y muestra un mensaje de error.

## ¿Cuál es uno de los beneficios clave de los Canarios de Pila en términos de seguridad?

a) Protege contra todos los tipos de amenazas informáticas.

b) Aumenta la velocidad de ejecución de programas.

c) Dificulta la explotación de vulnerabilidades de seguridad que facilitan desbordamientos de búfer.

d) Dificulta la explotación de vulnerabilidades de seguridad que dificultan el hashing de contraseñas

## . ¿Qué significa la sigla DEP en el contexto de seguridad informática?

a) Data Entry Point.

b) Digital Encryption Protocol.

c) Data Execution Prevention.

d) Dynamic Encryption Process.

## ¿Cuál es el objetivo principal de DEP?

a) Acelerar la velocidad de ejecución de programas.

b) Proteger datos almacenados en el disco duro.

c) Evitar que se ejecute código malicioso en regiones de memoria marcadas como no ejecutables.

d) Evitar que se ejecute código malicioso en regiones de memoria marcadas como ejecutables mediante la alteración del contador de programa

## ¿Cómo funciona DEP para prevenir la ejecución de código malicioso?

a) Desactiva por completo la memoria RAM.

b) Marca ciertas regiones de memoria como no ejecutables y evita que el procesador ejecute código en esas áreas.

c) Requiere que todos los programas se ejecuten en modo kernel ya que es más seguro que el modo usuario

d) Cifra y descifra todo el contenido de la memoria en tiempo real

## ¿En qué tipo de sistemas operativos es común encontrar la función DEP?

a) Solo en sistemas macOS.

b) Solo en sistemas Unix/Linux.

c) En sistemas Windows y otros sistemas operativos.

d) Solo en sistemas móviles.

## ¿Cuál de las siguientes afirmaciones es cierta sobre DEP?

a) DEP es una técnica de ataque con código malicioso en regiones de memoria marcadas como no ejecutables.

b) DEP solo protege contra virus y malware conocidos.

c) DEP es efectivo para prevenir la ejecución de código malicioso en regiones de memoria marcadas como no ejecutables.

d) DEP solo es necesario en servidores, no en computadoras personales.

## . ¿Cuál es uno de los beneficios clave de DEP en términos de seguridad?

a) Aumenta la velocidad de ejecución de programas porque la CPU trabaja en forma especulativa

b) Dificulta la explotación de vulnerabilidades de seguridad que permiten descifrar las contraseñas.

c) Dificulta la explotación de vulnerabilidades de seguridad que permiten la ejecución de código malicioso.

d) Protege contra ataques de phishing cuando el ordenador está conectado a WIFI

## ¿Qué significa la sigla ROP en el contexto de seguridad informática?

a) Ransomware Oriented Programming.

b) Return-Oriented Programming.

c) Randomized Operating Procedures.

d) Read-Only Protection.

## ¿Cuál es el objetivo principal de un ataque de ROP?

a) Robar contraseñas en texto claro.

b) Explotar vulnerabilidades en el cifrado de datos.

c) Ejecutar código malicioso utilizando fragmentos existentes de código ejecutable en el programa.

d) Atacar sistemas operativos.

## ¿Qué hace que ROP sea una técnica de ataque efectiva?

a) Utiliza solo código escrito por el atacante.

b) Utiliza solo lenguaje ensamblador.

c) Requiere acceso físico a la computadora objetivo.

d) Utiliza fragmentos de código legítimo en el programa.

## . ¿Cómo funciona un ataque de ROP?

a) Inyecta código malicioso en el programa objetivo.

b) Modifica el sistema de archivos del sistema operativo.

c) Utiliza instrucciones de retorno (ret) para saltar a fragmentos de código existentes en el programa y ejecutar operaciones maliciosas.

d) Cifra los datos en el disco duro.

## ¿Cuál es uno de los desafíos clave para un atacante en un ataque de ROP?

a) Encontrar una vulnerabilidad de día cero en el programa objetivo.

b) Tener acceso físico al hardware de la computadora objetivo.

c) Conocer el lenguaje ensamblador a nivel experto.

d) Escanear la red en busca de vulnerabilidades.

## . ¿En qué tipo de programas y sistemas operativos es más común encontrar ataques de ROP?

a) Solo en programas antivirus.

b) En una amplia variedad de programas y sistemas operativos.

c) Solo en sistemas macOS.

d) Solo en sistemas Unix/Linux.

## ¿Qué medida de seguridad puede ayudar a mitigar los ataques de ROP?

a) Utilizar un antivirus actualizado.

b) No permitir que los programas ejecuten código en absoluto.

c) Implementar técnicas de protección de memoria, como DEP (Data Execution Prevention) o ASLR (Address Space Layout Randomization).

d) Utilizar un firewall de red.

## . ¿Qué significa la sigla ASLR en el contexto de seguridad informática?

a) Address Space Layout Randomization.

b) Advanced Security and Log Retrieval.

c) Application Security and Logging Routine.

d) All System Logs Randomized.

## . ¿Cuál es el propósito principal de ASLR?

a) Aumentar la velocidad de ejecución de programas.

b) Proteger la dirección IP de un sistema.

c) Dificultar la explotación de vulnerabilidades de seguridad al aleatorizar la ubicación de la memoria.

d) Encriptar el tráfico de red.

## ¿Cómo funciona ASLR en un sistema operativo?

a) Cambiando aleatoriamente la dirección IP del sistema.

b) Cambiando aleatoriamente la dirección de la puerta de enlace predeterminada.

c) Cambiando aleatoriamente la ubicación de la memoria de las aplicaciones y bibliotecas en el espacio de direcciones virtual.

d) Cambiando aleatoriamente la contraseña del administrador.

## ¿Cuál es uno de los beneficios clave de ASLR en términos de seguridad?

a) Acelerar la velocidad de carga de programas.

b) Facilitar la administración de contraseñas.

c) Dificultar la explotación de vulnerabilidades de desbordamiento de búfer y otros ataques.

d) Proteger los datos almacenados en la nube.

## ¿En qué tipo de sistemas operativos se encuentra comúnmente la implementación de ASLR?

a) Solo en sistemas Windows.

b) Solo en sistemas macOS.

c) En sistemas Unix/Linux, Windows y otros sistemas operativos.

d) En sistemas operativos móviles, pero no en sistemas de escritorio.

## ¿Qué tipo de ataque de seguridad puede dificultarse significativamente mediante la implementación de ASLR?

a) Ataques de fuerza bruta.

b) Ataques de denegación de servicio.

c) Ataques de phishing.

d) Ataques que aprovechan vulnerabilidades de desbordamiento de búfer.

## ¿Cuál es uno de los posibles desafíos al implementar ASLR?

a) Aumento de la velocidad de ejecución de programas.

b) Posible incompatibilidad con aplicaciones antiguas que dependen de direcciones de memoria fijas.

c) Mayor consumo de memoria RAM.

d) Dificultad para administrar contraseñas.

## . ¿Qué es un ataque de detección de canal lateral?

a) Un ataque que utiliza una contraseña débil para acceder a un sistema.

b) Un ataque que aprovecha las vulnerabilidades en el cifrado de datos.

c) Un ataque que explora las fugas de información involuntarias, como el consumo de energía o el tiempo de acceso a la memoria, para deducir información confidencial.

d) Un ataque que utiliza fuerza bruta para romper contraseñas.

## ¿Cuál es el objetivo principal de un ataque de detección de canal lateral?

a) Exponer claves públicas.

b) Exponer claves privadas.

c) Proteger datos encriptados.

d) Aumentar el rendimiento de un sistema.

## ¿Qué tipo de información se puede obtener a través de un ataque de detección de canal lateral?

a) Contraseñas en texto claro.

b) Datos encriptados.

c) Información sobre patrones de consumo de energía, tiempo de acceso a la memoria, u otros canales secundarios.

d) Información sobre la ubicación geográfica de un usuario.

## ¿Cuál de las siguientes afirmaciones es cierta sobre la mitigación de ataques de detección de canal lateral?

a) No existen medidas efectivas para mitigar estos ataques.

b) Desactivar por completo la caché de la CPU es la única solución.

c) Se pueden aplicar contramedidas como el enmascaramiento de datos, la aleatorización de tiempo o el ruido de potencia.

d) Estos ataques solo afectan a servidores y centros de datos.

## . ¿Cuál es uno de los desafíos de la mitigación de ataques de detección de canal lateral?

a) Requiere una gran cantidad de recursos de hardware.

b) Es una técnica que no se puede bloquear.

c) No afecta el rendimiento del sistema.

d) No es una amenaza real en la actualidad.

## ¿Qué es un ataque de detección de canal lateral en el contexto del algoritmo RSA?

a) Un ataque que utiliza contraseñas débiles para descifrar mensajes encriptados con RSA.

b) Un ataque que se enfoca en interceptar el tráfico de red.

c) Un ataque que explora las fugas de información, como el consumo de energía o el tiempo de ejecución, para deducir claves privadas.

d) Un ataque que apunta a descifrar mensajes encriptados utilizando la fuerza bruta.

## ¿Cuál es el objetivo principal de un ataque de detección de canal lateral en el contexto de RSA?

a) Exponer claves públicas.

b) Exponer claves privadas.

c) Proteger datos encriptados.

d) Acelerar el procesamiento de datos.

## ¿Qué tipo de información se puede obtener a través de un ataque de detección de canal lateral en RSA?

a) Contraseñas en texto claro.

b) Datos encriptados.

c) Información sobre patrones de consumo de energía o tiempo de ejecución.

d) Direcciones IP de los servidores.

## . ¿Cuál es uno de los canales secundarios utilizados en un ataque de detección de canal lateral en RSA?

a) Canal de radio.

b) Canal de red.

c) Canal de tiempo.

d) Canal de almacenamiento.

## ¿Cuál de las siguientes afirmaciones es cierta sobre la mitigación de ataques de detección de canal lateral en RSA?

a) No hay medidas efectivas para mitigar estos ataques.

b) La desactivación de la caché de la CPU es la única solución.

c) Se pueden aplicar contramedidas como el enmascaramiento de datos o el ruido de potencia.

d) Estos ataques solo afectan a servidores y centros de datos.

## ¿Cuál es uno de los desafíos de la mitigación de ataques de detección de canal lateral en RSA?

a) Requiere una gran cantidad de recursos de hardware.

b) Es una técnica que no se puede bloquear.

c) No afecta el rendimiento del sistema.

d) Es una amenaza poco común.

## ¿Qué son los ataques de canal lateral a la caché?

a) Ataques que se dirigen a la memoria RAM de un sistema.

b) Ataques que aprovechan las debilidades en el cifrado de datos.

c) Ataques que explotan las filtraciones de información a través de canales secundarios, como el tiempo de acceso a la caché.

d) Ataques que utilizan la fuerza bruta para descifrar contraseñas.

## 2. ¿Qué tipo de información se puede obtener a través de un ataque de canal lateral a la caché?

a) Contraseñas en texto claro.

b) Información sobre la estructura interna de la CPU.

c) Patrones de acceso a la caché, revelando posibles claves o datos confidenciales.

d) Información sobre la ubicación geográfica del usuario.

## 3. ¿Cuál es uno de los canales secundarios utilizados en ataques de canal lateral a la caché?

a) Canal de radio.

b) Canal de red.

c) Canal de tiempo.

d) Canal de energía eléctrica.

## . ¿Qué es la "sincronización del reloj" en el contexto de un ataque de canal lateral a la caché?

a) El proceso de ajustar la hora en un dispositivo.

b) El proceso de sincronizar el reloj de la CPU con el reloj del sistema.

c) El uso de información de tiempo de acceso a la caché para inferir datos secretos.

d) El proceso de medir el rendimiento del procesador.

## . ¿Cuál es uno de los ejemplos más conocidos de ataque de canal lateral a la caché?

a) Ataque de fuerza bruta.

b) Ataque de diccionario.

c) Ataque Spectre.

d) Ataque de denegación de servicio.

## . ¿Cómo pueden mitigarse los ataques de canal lateral a la caché?

a) Utilizando un firewall.

b) Aplicando medidas de seguridad en el software y el hardware para minimizar las filtraciones de información.

c) Desactivando la caché en la CPU.

d) Aumentando la velocidad del reloj de la CPU.

## . ¿Cuál es uno de los desafíos de la mitigación de ataques de canal lateral a la caché?

a) Requiere una gran cantidad de recursos de hardware.

b) Es ineficaz y no tiene impacto en la seguridad.

c) No hay medidas efectivas para mitigar estos ataques.

d) Solo se pueden mitigar mediante medidas de seguridad física.

## 8 ¿En qué tipo de entornos o escenarios es más probable que ocurran ataques de canal lateral a la caché?

a) Entornos de redes sociales.

b) Entornos de servidor y centros de datos.

c) Entornos de juegos en línea.

d) Entornos de edición de video.

## ¿Qué es la "vulnerabilidad Meltdown" en relación con los ataques de canal lateral a la caché?

a) Una técnica de mitigación de ataques de canal lateral.

b) Un ataque que explota debilidades en el cifrado de datos.

c) Un tipo de ataque de canal lateral a la caché que afecta principalmente a procesadores Intel.

d) Un método de sincronización de relojes en la CPU.

## ¿Qué es una "cola de almacenamiento" en una CPU y cómo puede estar relacionada con los ataques de canal lateral a la caché?

a) Una lista de instrucciones en espera de ejecución; puede ser un objetivo para ataques de canal lateral.

b) Un tipo de memoria RAM utilizada para almacenar caché de datos.

c) Un componente de hardware utilizado para proteger la CPU de ataques.

d) Una unidad de procesamiento dedicada a ejecutar instrucciones especulativas.

## ¿Cuál es uno de los métodos utilizados en la mitigación de ataques de canal lateral a la caché?

a) Aumentar la velocidad del reloj de la CPU.

b) Utilizar software de seguridad para detectar y bloquear ataques.

c) Desactivar completamente la caché de la CPU.

d) Implementar técnicas de sincronización de reloj más precisas.

## . ¿Cuál es el objetivo principal de un ataque de canal lateral a la caché?

a) Robar contraseñas en texto claro.

b) Obtener información sobre los patrones de acceso a la caché para deducir datos confidenciales.

c) Interceptar tráfico de red.

d) Explotar debilidades en el cifrado de datos en la RAM.

## ¿Cuál es una de las ventajas de la caché de la CPU que también puede ser aprovechada por los atacantes en ataques de canal lateral?

a) Acelera el procesamiento de datos sin ningún riesgo.

b) Almacena datos confidenciales de forma segura.

c) Permite el acceso más rápido a datos comunes, lo que puede revelar patrones de acceso.

d) Protege la CPU de cualquier tipo de ataque.

## ¿Cuál es uno de los efectos secundarios no deseados de las medidas de mitigación de ataques de canal lateral a la caché?

a) Aumento del rendimiento de la CPU.

b) Reducción del consumo de energía.

c) Pérdida de rendimiento en aplicaciones específicas debido a la desactivación de ciertas optimizaciones.

d) Aumento de la velocidad del reloj de la CPU.

## ¿Cuál es una técnica comúnmente utilizada en ataques de canal lateral a la caché para deducir información confidencial?

a) Ataque de fuerza bruta.

b) Ataque de diccionario.

c) Monitoreo de tiempos de acceso a la caché.

d) Ataque de negación de servicio.

## ¿Qué es el ataque de canal lateral a la caché conocido como "Prime+Probe"?

a) Un ataque que utiliza patrones de acceso a la caché para deducir información confidencial.

b) Un ataque que desactiva completamente la caché de la CPU.

c) Un ataque que explota vulnerabilidades en el sistema operativo.

d) Un ataque que intercepta el tráfico de red.

## 2. ¿Cuál es la fase "Prime" en el ataque Prime+Probe?

a) La fase de interceptación de datos.

b) La fase de preparación, donde se carga la caché con datos específicos.

c) La fase de extracción de datos confidenciales.

d) La fase de cifrado de datos.

## ¿Qué papel desempeña la fase "Probe" en el ataque Prime+Probe?

a) La fase de preparación de datos.

b) La fase de almacenamiento de datos en la caché.

c) La fase de monitoreo de los tiempos de acceso a la caché para deducir información confidencial.

d) La fase de encriptación de datos.

## . ¿Cuál es el objetivo principal del ataque Prime+Probe?

a) Robar contraseñas en texto claro.

b) Desactivar la caché de la CPU.

c) Obtener información sobre los patrones de acceso a la caché para deducir datos confidenciales.

d) Explotar debilidades en el cifrado de datos en la RAM.

## ¿Cuál de las siguientes afirmaciones es cierta sobre los ataques de canal lateral a la caché en general?

a) Son fácilmente detectables y bloqueables.

b) No tienen impacto en la seguridad de la información.

c) Pueden ser utilizados para revelar patrones de acceso a la caché y deducir datos confidenciales.

d) Solo afectan a las aplicaciones de oficina.

## ¿Cuál es uno de los desafíos de mitigar el ataque Prime+Probe?

a) Requiere una gran cantidad de recursos de hardware.

b) Es una técnica que no se puede bloquear.

c) No tiene efecto en el rendimiento del sistema.

d) No afecta a los servidores y centros de datos.

## ¿Qué es la CPU especulativa?

a) Una CPU que funciona a velocidades más lentas que las CPU convencionales.

b) Una CPU que realiza cálculos de manera más precisa que otras CPUs.

c) Una CPU que anticipa y ejecuta instrucciones antes de saber si son necesarias.

d) Una CPU que está diseñada exclusivamente para juegos.

## . ¿Cuál es el propósito principal de la ejecución especulativa en una CPU?

a) Aumentar la velocidad del reloj de la CPU.

b) Acelerar la velocidad de procesamiento de gráficos.

c) Reducir el consumo de energía.

d) Mejorar el rendimiento general al predecir y ejecutar instrucciones.

## . ¿Qué es un "branch prediction" en una CPU especulativa?

a) Una técnica para prevenir ataques de seguridad en la CPU.

b) Una técnica para anticipar el resultado de las instrucciones de salto condicional.

c) Una técnica para aumentar el tamaño de la caché de instrucciones.

d) Una técnica para dividir la CPU en múltiples núcleos.

## . ¿Cuál es uno de los posibles desafíos de la CPU especulativa relacionado con la seguridad?

a) La ejecución especulativa puede aumentar el rendimiento, pero no afecta la seguridad.

b) Vulnerabilidades de seguridad como Spectre y Meltdown que pueden exponer datos confidenciales.

c) Falta de compatibilidad con software existente.

d) Mayor consumo de energía en comparación con las CPU convencionales.

## . ¿En qué tipo de aplicaciones o escenarios es más beneficioso el uso de CPU especulativa?

a) Aplicaciones de oficina como procesamiento de texto y hojas de cálculo.

b) Aplicaciones de edición de video y diseño gráfico.

c) Aplicaciones de inteligencia artificial y aprendizaje profundo.

d) Aplicaciones de navegación web y correo electrónico.

## . ¿Cómo afecta la ejecución especulativa al rendimiento general de la CPU?

a) No tiene ningún efecto en el rendimiento.

b) Puede aumentar significativamente el rendimiento al ejecutar instrucciones de manera anticipada.

c) Disminuye el rendimiento al ralentizar la CPU.

d) Solo afecta el rendimiento de la GPU.

## ¿Cuál es un beneficio clave de la CPU especulativa en términos de rendimiento?

a) Aumenta la velocidad del reloj de la CPU.

b) Reduce la necesidad de almacenar caché.

c) Permite la ejecución de instrucciones fuera de orden.

d) Acelera la ejecución de instrucciones al predecir y anticiparlas.

adicionales sobre CPU especulativa:

## ¿Cuál es uno de los principales riesgos de seguridad asociados con la CPU especulativa?

a) Consumo excesivo de energía.

b) Rendimiento insuficiente.

c) Vulnerabilidades que podrían exponer datos confidenciales.

d) Incompatibilidad con software antiguo.

## . ¿Cuál es el propósito de la "ejecución fuera de orden" en una CPU especulativa?

a) Realizar cálculos de manera más precisa.

b) Ejecutar instrucciones en el orden en que se presentan en el programa.

c) Acelerar el procesamiento al ejecutar instrucciones de manera anticipada si es posible.

d) Reducir el tamaño de la caché de datos.

## . ¿Cuál es una de las ventajas de la CPU especulativa en términos de rendimiento de aplicaciones de cómputo intensivo?

a) Mayor consumo de energía.

b) Mayor compatibilidad con software antiguo.

c) Capacidad para ejecutar aplicaciones de manera más eficiente.

d) Reducción de la cantidad de RAM necesaria.

## . ¿Cuál es una de las desventajas de la ejecución especulativa en términos de consumo de energía?

a) Reduce significativamente el consumo de energía.

b) Aumenta el consumo de energía debido a la aceleración de instrucciones.

c) No tiene ningún efecto en el consumo de energía.

d) Solo afecta el consumo de energía de la GPU.

## . ¿Qué tipo de instrucciones en un programa de computadora pueden beneficiarse más de la ejecución especulativa?

a) Instrucciones de entrada/salida.

b) Instrucciones de cálculo intensivo.

c) Instrucciones de espera.

d) Instrucciones de RAM.

## . ¿Cómo puede mitigarse el riesgo de vulnerabilidades de seguridad asociadas con la CPU especulativa?

a) Apagar la CPU cuando no se está utilizando.

b) Aplicar parches de seguridad y actualizaciones del sistema operativo.

c) No utilizar CPUs especulativas en absoluto.

d) Utilizar una mayor cantidad de RAM.

temas operativos.