

CURSO PARA LA OBTENCIÓN DEL

DIPLOMA DE INFORMÁTICA MILITAR

(59130)

Teoría de Sistemas Operativos

Capítulo 10. Preguntas y ejercicios

Índice

[1. Preguntas 3](#_Toc147130027)

[1.1. ¿Qué función realiza un controlador de dispositivo en un sistema operativo? 3](#_Toc147130028)

[1.2. ¿Qué es la E/S por bloques en sistemas operativos? 3](#_Toc147130029)

[1.3. ¿Qué es una interrupción de hardware en un sistema operativo? 3](#_Toc147130030)

[1.4. ¿Qué significa DMA en el contexto de E/S en sistemas operativos? 3](#_Toc147130031)

[1.5. ¿Cuál de las siguientes no es una función de un controlador de dispositivo? 3](#_Toc147130032)

[1.6. ¿Qué es el pooling de E/S en sistemas operativos? 3](#_Toc147130033)

[1.7. ¿Cuál es el propósito principal de las interrupciones de software en un sistema operativo? 3](#_Toc147130034)

[1.8. ¿Qué tipo de interrupción es generada por dispositivos de hardware para notificar eventos como la finalización de una transferencia de datos? 4](#_Toc147130035)

[1.9. ¿Cuál es el propósito de una tabla de vectores de interrupción en un sistema operativo? 4](#_Toc147130036)

[1.10. ¿Qué beneficio proporcionan las interrupciones en un sistema operativo? 4](#_Toc147130037)

[2. Ejercicios 4](#_Toc147130038)

[2.1. Comando para ver interrupciones 4](#_Toc147130039)

[2.2. Comando para ver una lista de interrupciones 4](#_Toc147130040)

[2.3. Comando para ver la afinidad 4](#_Toc147130041)

[2.4. Lista de los núcleos de CPU a los que se puede asignar una interrupción 5](#_Toc147130042)

[2.5. Dispositivos PCI en el sistema 5](#_Toc147130043)

[2.6. Módulos kernel cargados en el sistema 5](#_Toc147130044)

[2.7. Lista de los dispositivos en el directorio /dev 5](#_Toc147130045)

[2.8. Lista de dispositivos USB conectados al sistema 5](#_Toc147130046)

[2.9. Detección y carga de controladores de dispositivos 6](#_Toc147130047)

[2.10. Configuración de hardware del sistema, incluyendo la lista de dispositivos y controladores asociados 6](#_Toc147130048)

[2.11. Información sobre un módulo del kernel, incluyendo detalles sobre el controlador de dispositivo 6](#_Toc147130049)

[2.12. Información sobre los dispositivos de bloque 6](#_Toc147130050)

# Preguntas

## ¿Cuál de las siguientes características hace que una contraseña sea más segura?

a) Una contraseña corta

b) Una contraseña larga

c) Una contraseña basada en el nombre del usuario

d) Una contraseña que contiene solo letras minúsculas

## ¿Por qué es importante cambiar regularmente las contraseñas?

a) Para aumentar la complejidad de las contraseñas

b) Para evitar el bloqueo de la cuenta

c) Para hacer que las contraseñas sean más fáciles de recordar

d) No es necesario cambiar regularmente las contraseñas

## ¿Cuál de las siguientes afirmaciones es cierta con respecto a las contraseñas seguras?

a) Deben contener al menos un número y una letra en mayúscula

b) Deben ser iguales a la dirección de correo electrónico del usuario

c) Deben ser compartidas con amigos y colegas

d) No importa si se comparten con otros, siempre que sean fuertes

## ¿Cuál de las siguientes es una recomendación importante para crear contraseñas seguras?

a) Utilizar palabras comunes y fáciles de recordar

b) Utilizar la misma contraseña para todas las cuentas

c) Evitar el uso de caracteres especiales como símbolos y números

d) Utilizar una combinación de letras mayúsculas, minúsculas, números y símbolos

## . ¿Cuál es un ejemplo de una contraseña segura?

a) "password123"

b) "miapellido"

c) "P@$$w0rd!"

d) "123456789"

## . ¿Por qué es importante no compartir sus contraseñas con nadie?

a) Para mantener la privacidad y la seguridad de sus cuentas

b) Porque es una práctica común y segura compartirlas

c) Para facilitar el acceso de otros a su cuenta

d) No importa si se comparten, siempre que confíe en la persona con la que las comparte

## 7. ¿Qué es un ataque de fuerza bruta en relación con las contraseñas?

a) Un ataque en el que un atacante adivina la contraseña correcta de inmediato

b) Un ataque en el que un atacante intenta todas las combinaciones posibles de contraseñas hasta encontrar la correcta

c) Un ataque en el que un atacante engaña al usuario para que revele su contraseña

d) Un ataque en el que un atacante intercepta el tráfico de red para obtener la contraseña del usuario

## 8. ¿Cuál de las siguientes afirmaciones es cierta acerca de la autenticación de dos factores (2FA)?

a) Es menos segura que una contraseña única

b) Requiere el uso de dos contraseñas

c) Agrega una capa adicional de seguridad al requerir dos formas diferentes de autenticación

d) No es necesario para la mayoría de las cuentas en línea

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

a) Un proceso para eliminar las contraseñas débiles.

b) La adición de información adicional aleatoria a una contraseña antes de almacenarla.

c) Un método para cifrar contraseñas en tiempo real.

d) La técnica de hashing de contraseñas más segura.

## ¿Cuál es el propósito principal del "salting" en la seguridad de contraseñas?

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

b) Aumentar la longitud de las contraseñas.

c) Fortalecer la seguridad almacenando contraseñas de manera más segura.

d) Encriptar las contraseñas antes de almacenarlas.

## ¿Cómo afecta el "salting" a las contraseñas almacenadas?

a) Las contraseñas se vuelven más fáciles de adivinar.

b) Las contraseñas se vuelven más largas.

c) Cada contraseña almacenada es única debido a la adición de información aleatoria.

d) Las contraseñas se vuelven más simples.

## ¿Cuál de las siguientes afirmaciones es verdadera acerca de las contraseñas salteadas?

a) Son vulnerables a ataques de fuerza bruta.

b) Son menos seguras que las contraseñas sin sal.

c) Son más seguras porque evitan el uso de caracteres especiales.

d) Son más resistentes a ataques de diccionario y tablas de hash precalculadas (rainbow tables).

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

a) Simplifica el proceso de autenticación.

b) Permite el almacenamiento de contraseñas en texto claro.

c) Protege contra ataques de diccionario y ataques con tablas de hash precalculadas.

d) Reduce la complejidad de las contraseñas.

## ¿Qué información se utiliza típicamente como "sal" en el "salting" de contraseñas?

a) La contraseña del usuario.

b) La dirección de correo electrónico del usuario.

c) Un valor aleatorio único para cada usuario.

d) El nombre de usuario del usuario.

## ¿Qué es una característica importante de un "sal" efectivo?

a) Debe ser la misma para todos los usuarios.

b) Debe ser secreto y no almacenado junto con las contraseñas.

c) Debe ser igual al nombre de usuario del usuario.

d) Debe ser una cadena de caracteres alfanuméricos fija.

## ¿Cuál de las siguientes afirmaciones es cierta con respecto al "salting" de contraseñas?

a) Es una práctica obsoleta y no se utiliza en la actualidad.

b) Aumenta la velocidad de autenticación.

c) Es una técnica efectiva para proteger las contraseñas almacenadas, especialmente en caso de filtraciones de bases de datos.

d) Solo se aplica a contraseñas cortas.

## . ¿Qué es el método de Lamport en seguridad informática?

a) Un método para almacenar contraseñas en texto claro.

b) Un algoritmo de cifrado simétrico.

c) Un método de autenticación basado en contraseñas de un solo uso.

d) Un algoritmo de compresión de datos.

## ¿Cuál es la característica principal de las contraseñas generadas por el método de Lamport?

a) Son contraseñas de texto claro.

b) Son contraseñas estáticas y permanentes.

c) Son contraseñas de un solo uso que cambian con cada autenticación.

d) Son contraseñas alfanuméricas.

## . ¿Cómo se almacenan las contraseñas en el método de Lamport?

a) En un servidor centralizado.

b) En una base de datos en línea.

c) Como una lista de hashes de contraseñas.

d) En texto claro.

## . ¿Cómo se genera una contraseña de un solo uso en el método de Lamport?

a) Mediante un algoritmo de cifrado asimétrico.

b) Seleccionando una contraseña de una lista predefinida.

c) Aplicando una función hash criptográfica a una contraseña principal.

d) Mediante un algoritmo de compresión de datos.

## 5. ¿Cuál es una desventaja potencial del método de Lamport?

a) Requiere una gran cantidad de almacenamiento para las contraseñas.

b) Es vulnerable a ataques de diccionario.

c) Las contraseñas de un solo uso pueden ser difíciles de generar.

d) No es adecuado para autenticación en línea.

## 6. ¿Cómo se verifica una contraseña de un solo uso en el método de Lamport?

a) Se compara con una lista de contraseñas almacenadas en texto claro.

b) Se aplica una función hash criptográfica y se compara con la contraseña almacenada.

c) Se envía al servidor central para su verificación.

d) Se cifra con una clave pública y se compara con la contraseña almacenada.

## ¿Qué hace que las contraseñas generadas por el método de Lamport sean seguras?

a) Su longitud, ya que son muy largas.

b) La complejidad de los caracteres utilizados en ellas.

c) El hecho de que son de un solo uso y cambian constantemente.

d) Su almacenamiento en un servidor centralizado.

## ¿Qué es la autenticación basada en lo que se tiene?

a) Un método de autenticación basado en conocimientos.

b) Un método de autenticación basado en una smartcard

c) Un método de autenticación basado en características físicas del usuario.

d) Un método de autenticación basado en la ubicación geográfica.

## ¿Cuál de las siguientes no es un ejemplo de factor de autenticación basado en lo que se tiene?

a) Contraseña.

b) Tarjeta de acceso físico.

c) Huella dactilar.

d) Pregunta de seguridad.

## ¿Qué factor de autenticación se basa en la posesión de un objeto físico?

a) Factor de autenticación basado en conocimientos.

b) Factor de autenticación basado en características físicas.

c) Factor de autenticación basado en posesión.

d) Factor de autenticación basado en ubicación.

## . ¿Qué tipo de factor de autenticación es más difícil de robar o duplicar?

a) Factor de autenticación basado en conocimientos.

b) Factor de autenticación basado en características físicas.

c) Factor de autenticación basado en posesión.

d) Factor de autenticación basado en ubicación.

## ¿Cuál es una ventaja de la autenticación basada en lo que se tiene?

a) Es fácil de recordar para los usuarios.

b) Puede proporcionar un nivel adicional de seguridad.

c) No requiere dispositivos adicionales.

d) Es vulnerable a ataques de fuerza bruta.

## . ¿Qué factor de autenticación se basa en conocimientos previos del usuario?

a) Factor de autenticación basado en posesión.

b) Factor de autenticación basado en ubicación.

c) Factor de autenticación basado en características físicas.

d) Factor de autenticación basado en contraseñas

## 2. ¿Cuál de las siguientes no es una característica biométrica comúnmente utilizada en sistemas de autenticación?

a) Huella dactilar.

b) Contraseña.

c) Reconocimiento facial.

d) Escaneo de retina.

## ¿Qué hace que la biometría sea una forma efectiva de autenticación?

a) La facilidad de robar o duplicar las características biométricas.

b) La falta de precisión en la identificación de las características biométricas.

c) La singularidad y la dificultad de falsificar las características biométricas.

d) La necesidad de dispositivos costosos.

## ¿Cuál de las siguientes afirmaciones es cierta con respecto a la autenticación por huella dactilar?

a) Es fácil de falsificar mediante impresiones en 3D.

b) Es una forma altamente precisa de autenticación biométrica.

c) Requiere que los usuarios proporcionen una contraseña junto con su huella dactilar.

d) No se utiliza en aplicaciones de seguridad debido a su falta de precisión.

## ¿Cuál es una consideración importante en la implementación de la autenticación por biometría?

a) La necesidad de recordar múltiples contraseñas.

b) La protección de los datos biométricos almacenados.

c) La facilidad de compartir características biométricas con otros usuarios.

d) La falta de precisión en la identificación biométrica.

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

a) Un ataque que sobrecarga el búfer de impresión de una impresora.

b) Un ataque en el que un programa o 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.

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

a) Robar contraseñas.

b) Exponer vulnerabilidades de software.

c) Aumentar la velocidad de procesamiento de una aplicación.

d) Aumentar el almacenamiento en búfer de un sistema.

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

a) Vulnerabilidad de seguridad física.

b) Vulnerabilidad de ingeniería social.

c) Vulnerabilidad de software de programación deficiente.

d) Vulnerabilidad de hardware.

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

a) El aumento del rendimiento del sistema.

b) La eliminación de malware.

c) La ejecución de código malicioso.

d) La mejora de la seguridad de la red.

## . ¿Cuál es una técnica común utilizada para mitigar ataques de desbordamiento de búfer?

a) Escanear el tráfico de red.

b) Implementar medidas de seguridad física en el servidor.

c) Utilizar lenguajes de programación que gestionen automáticamente la memoria.

d) Incrementar el tamaño del búfer de memoria.

# Ejercicios