CAI 1. CONSULTA SOBRE CUMPLIMIENTO DE DIFERENTES POLÍTICAS DE SEGURIDAD EN ENTIDAD FINANCIERA

Una entidad financiera dispone de una **Política de Seguridad** que indica que los **mecanismos de autenticación** se basan en la existencia de contraseñas, y especifica un conjunto de condiciones que éstas deben cumplir:

1. **Debe tener como mínimo 8 caracteres.**
2. **Debe tener al menos un carácter de cada uno de los siguientes tres grupos:**
    a. **Letras (mayúsculas y minúsculas): A, B, C, … a, b, c …**
    b. **Caracteres numéricos: 0, 1, 2, 3,.., 8, 9**
    c. **Símbolos: ! @ # $ % & *^( ) - = { } [ ] \ : ; < > ? , . /**

No disponen de mecanismo alguno que controle el cumplimiento de esta Política de Seguridad en dicha empresa.

La base de datos de control de acceso a los sistemas de información de dicha empresa contiene una tabla con el nombre de los usuarios, su ***username,*** la contraseña cifrada mediante un ***algoritmo de hashing seguro*** para evitar que si alguien accede a dicha tabla no puede conocer dicha contraseña y tiene también un campo **salt** que podría ser añadido como prefijo o sufijo a dicha contraseña para el almacenamiento seguro de la misma.

Se sospecha por parte de la Dirección de la empresa que las cuatro contraseñas de la tabla siguiente no cumplen con la Política de Seguridad de dicha organización,

Nombre usuario	Username	Contraseña	Salt
Ivan Toreman Gerto	ivtorto	----------	40
José A. Pearse Mariso	japeama	----------	53
Rafael ConseryTamper	raconta	----------	17
Pedro Marteis Poncio	pmarpo	----------	29

(Las contraseñas no aparecen pues el cliente nos informará de ellas en la sesión de trabajo del próximo lunes día 17 de Febrero)

Las sospechas se fundamentan en que el primer usuario ha indicado a alguno de sus compañeros de trabajo que "***no me he complicado la vida y he puesto como contraseña una palabra de la lengua inglesa***", el segundo ha comentado en los pasillos de trabajo que "***no me ha quebrado la cabeza y he puesto una contraseña de las más comunes que se ponen seguida de un punto y dos números***", el tercero ha dicho que ***"tiene puesta una contraseña jugando con algunas de las letras de mi nombre y apellidos"*** y el último está comentando que ha puesto como contraseña ***"la fecha de nacimiento de uno de sus hijos"***. Consideren también que podrían estar diciendo alguna mentira o tirarse un farol.

También, de acuerdo con la estrategia de aseguramiento de la información ***Security by design u open security*** la entidad financiera publica en su página Web que la integridad de las

transferencias financieras, a través de la aplicación para móviles que se pueden descargar los clientes, se hará de **"forma segura"** usando **Códigos de Autenticación de Mensajes (MAC)** de los mensajes realizados por el cliente al servidor del banco con **claves secretas de un tamaño de 32 bits.** Dicha entidad entrega a los clientes cada año un dispositivo físico (*pendrive, smartcard*, …) que contiene dicha clave para realizar todas las gestiones financieras que deseen durante el año.

La **Política de Seguridad propuesta por el Gobierno de la Seguridad de la Información (GSI)** de la entidad especifica **que todas las transmisiones de información de la entidad con los clientes deben ser íntegras (no hay todavía preocupación por la confidencialidad),** evitando los posibles ataques. No obstante, el GSI de la entidad que nos ha contratado, tiene dudas razonables sobre la **robustez del algoritmo de generación de MAC y las claves usadas para los MAC por dicha aplicación para dispositivos móviles**. Durante la sesión de Consultoría del próximo día 17 de Febrero recibiremos de la entidad financiera tres mensajes de diferentes clientes y su correspondiente MAC (algo parecido a lo siguiente):
Mensaje: `34567891 987654 300`
MAC: `ada141975ed739fe27e50cab4b5dd5a7c96553b1`
Y en este caso se ha empleado para el MAC una clave de 32 bits, que si fuera fácil derivar, sería necesario tomar medidas para evitar estos posibles ataques de ***Key Replication***.

Las consultas que nos presenta el cliente **(Informe Ejecutivo**) consisten en:

1. **Informar al cliente cuál o cuáles de los usuarios incumple la Política de Seguridad de contraseñas mediante la correspondiente comprobación por la técnica seleccionada**. **Además, el cliente nos solicita que se le indique las reglas de la Política que podrían estar violando cada una de las contraseñas analizadas. (Valoración 30%)**
2. **Recomendar una solución organizativa y/o tecnológica al cliente (oportunidad de negocio) para evitar todos estos problemas de incumplimiento de la Política de Seguridad de contraseñas y mejorar la misma. (Valoración 20%)**
3. **Informar al cliente si es seguro el tamaño de clave que está usando para asegurar la integridad de las transmisiones**. **Indicar razonadamente,** en caso que el tamaño no sea suficiente, **qué tamaño recomendarían (nos** solicita **el cliente calcular el tamaño exacto de clave** que sería conveniente **48 bits??, 64 bits??,...)** teniendo en cuenta que la capacidad de computación de un posible atacante **desde un punto de vista pesimista es 100.000 veces mayor que los equipos que hacen la experimentación los Equipos de Trabajo**. El cliente nos comunica que valora muy positivamente **TODAS LAS PRUEBAS EMPÍRICAS QUE SE APORTEN PARA AVALAR TAL TAMAÑO DE CLAVE. (Valoración 30%)**
4. **¿Cuáles podrían ser las mejoras del modelo de proceso de negocio que tiene la entidad bancaria actualmente para la entrega de la clave a los clientes (se añade en un documento aparte)?**. Presente **detalladamente** en el informe el nuevo modelo de proceso de negocio que propone **y todos y cada uno de los aspectos técnicos que deberían ser considerados para ejecutar el proceso de negocio modelado**. **(Valoración 20%)**

El presupuesto económico de la consultoría acordado con el cliente ha sido de **1290€+IVA**

Normas del entregable

- El plazo de entrega de dicha consultoría se ha acordado con el cliente que finalizará el próximo **día 20 de Febrero de 2020 a las 19:30 horas.**
- Se debe realizar la entrega al CISO por parte del ingeniero ***Consultor Jefe*** a través de la Plataforma de Enseñanza Virtual (opción Herramientas -> Mensajes de Curso) un

archivo InfEj*ETnum*CAI1.pdf que contenga todos los detalles (No se debe indicar en los documentos los ingenieros que han participado en el Equipo de Trabajo Consultor, **pero si en el mensaje enviado**).