Máster Ciberseguridad y Privacidad

Seguridad y pentesting de servidores de datos

Prueba de Evaluación Continua, PEC 1

1. Para dudas y aclaraciones sobre el enunciado, debéis dirigiros al consultor responsable de vuestra aula.
2. La actividad es completamente individual y se podrá calificar con suspenso todas aquellas entregas que sean susceptibles de haber realizado una copia.
3. Hay que entregar la solución en un fichero PDF y enviarlo al área **Entrega y registro de EC**.

Enunciado

1. Responsables de la seguridad de los datos (5 puntos)

La compañía ACME tiene, entre otras, una base de datos corporativa en la que almacena los datos de sus empleados, incluyendo sus datos personales y sus sueldos. Mediante un proceso automático, se realiza una copia de seguridad mensual de la base de datos que se almacena en una cinta en un lugar seguro. Por otro lado, existe un proceso mensual que extrae un subconjunto de datos y lo envía a un sistema de archivos en un servidor para preparar el proceso de nóminas.
Teniendo en cuenta este escenario, contesta de manera argumentada las siguientes cuestiones:

1.1. Describe que roles o individuos tendrían alguna responsabilidad en la seguridad (no sólo privacidad) de dichos datos y cuales serían sus funciones principales.
1.2. ¿Qué medidas básicas de seguridad crees que deberían implementar cada uno de los responsables mencionados en el apartado anterior?
1.3. La compañía ha planteado contratar un servicio de *Cloud Computing* que permita la gestión remota de todos los datos de la compañía. De este modo, se accederá mediante un *web-service* para la inserción y modificación de todos los datos, y una interfaz permite la gestión de estos. La compañía que ofrece

el servicio dice ocuparse de la seguridad de los datos, así como de realizar las copias de seguridad.
Lectura recomendada para solucionar este ejercicio (área de ficheros):

Database security in a cloud computing environment.pdf

1.3.1. ¿Cómo cambia este nuevo planteamiento el anterior esquema (explica cómo cambian los roles y las responsabilidades de cada uno)?
1.3.2. Comparado con el escenario anterior, ¿qué riesgos y oportunidades crees que han aparecido?
1.3.3. ¿Qué nuevas medidas de seguridad debería implantar o exigir la compañía ACME?
1.3.4. ¿En qué circunstancias crees que no sería aceptable un escenario de este estilo, es decir, la compañía no podría plantearse el externalizar este tipo de servicios?

1.4. Crea una instancia *cloud* de MongoDB (Atlas) y da de alta usuarios ficticios implementando los diferentes roles que has definido en el apartado 1.1. Incluye una captura de pantalla de dichos usuarios en tu respuesta a esta pregunta. ¿Cuáles de las medidas de seguridad propuestas en el apartado 12 puedes implementar en la instancia de Cloud MongoDB?

2. Arquitecturas de bases de datos (5 puntos)

En primer lugar, es necesario instalar una versión de Oracle 12c. La descarga es gratuita y puede realizarse desde este enlace:

http://www.oracle.com/technetwork/database/enterprise-edition/downloads/index.html

Tras la instalación, contestad a las siguientes cuestiones:

2.1. ¿Qué bases de datos (*tablespaces*) hay creadas por defecto?
2.2. ¿Dónde se encuentran los metadatos del sistema de base de datos? ¿Qué tablas destacarías?
2.3. ¿Qué usuarios de base de datos crea por defecto? ¿Qué permisos tienen dichos usuarios?
2.4. ¿Qué puertos tiene a la escucha? ¿Cuál es la función de cada uno de los procesos a la escucha? ¿Cómo pueden desactivarse?
2.5. ¿En qué directorio se encuentran los binarios? ¿Y los archivos de datos?
2.6. ¿Con qué permisos se ejecuta el proceso de base de datos en el sistema?
2.7. ¿Qué opciones de configuración, en cuanto a seguridad, se ofrecen durante la instalación?

En segundo lugar, vamos a instalar Mongo DB Community Server. Podéis descargarlo desde este link:

https://www.mongodb.com/try/download/community

2.8 Compara las opciones de seguridad disponibles durante la instalación de Mongo DB con las que has descrito en la pregunta 2.7.

2.9 ¿Qué puertos tiene por defecto a la escucha? ¿Cuál es la función de cada uno de los procesos a la escucha? ¿Cómo pueden desactivarse?

2.10 ¿Con qué permisos se ejecuta Mongo DB en el sistema?

2.11 ¿En qué directorio se encuentran los binarios? ¿Y los archivos de datos?

2.12 Por último, veamos cuales deberían ser los criterios para decantarse por uno u otro tipo de base de datos. Para ello, completa la siguiente tabla:

Base de Datos	Principales características	¿En qué casos deberíamos considerar su uso?	Aspectos de seguridad más relevantes a tener en cuenta
Oracle			
Mongo DB			
HP Vertica			
Neo4j			
Elastic Search			
MariaDB			
MSSQL			
Redis			
PosgreSQL			