Máster Ciberseguridad y Privacidad

Seguridad y pentesting de servidores de datos

Prueba de Evaluación Continua, PEC 3

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. Implicaciones en las BBDD de *General Data Protection Regulation (3'5 puntos)*

Contesta las siguientes preguntas al respecto de la GDPR:

a) ¿Quién está obligado a cumplir con esta normativa?

b) Describe brevemente cuáles son los principios que rigen esta nueva normativa.

c) ¿Cuáles son los principales derechos que posee el sujeto de los datos?

d) En el escenario en el que una empresa que ha implementado una página de *e-commerce* almacena toda la base de datos con la información de sus clientes en el *cloud* público de Amazon; ¿cuál de los roles definidos por el GDPR estaría adoptando la empresa de e-commerce y cual le correspondería a Amazon?

e) En caso de que la empresa de *e-commerce* anterior tuviera constancia de tener comprometido los datos de sus clientes debido a un incidente de seguridad, ¿cuáles son sus obligaciones? ¿qué puede pasar si no cumple con dichas obligaciones?

f) ¿En qué casos será obligatorio designar a un Oficial de Protección de Datos?

g) Uno de los casos de uso que se barajan en la organización es realizar minería de datos aprovechando el gran volumen que datos alojados en las bases de datos con objeto de ofrecer a los clientes servicios personalizados. ¿qué aspectos legales deberían considerarse en éste supuesto?

h) Como responsable de seguridad de la información de una prestigiosa universidad online, el rector te ha pedido que prepares un *e-mail* para enviar a todo el personal técnico de la universidad poniendo en relieve los principales aspectos de la GDRP y cómo esta nueva normativa puede afectar a los procesos de la Universidad. Realiza un redactado corto y conciso con todas las afectaciones.

Fuentes a consultar:

Página con FAQs y otros recursos:
http://ec.europa.eu/justice/data-protection/reform/index_en.htm

Texto de la ley en PDF:
http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

2. BD NO-SQL (3'5 puntos)

En la organización en la que trabajas se están planteando el uso de *Elastic Search* para la persistencia y búsqueda de los datos de una nueva aplicación. Como responsable de la seguridad de las aplicaciones y bases de datos te han pedido que hagas un estudio de los riesgos que supone el uso de una BD NoSQL y que documentes los requisitos de seguridad que se deberán considerar en su implantación para prevenir o mitigar dichos riesgos.

Para ello debes acceder a la parte del material externo que se indica a continuación:

https://www.elastic.co/community/security

https://www.elastic.co/blog/found-elasticsearch-security

Ejemplo de posibles problemas por errores:

https://securityintelligence.com/news/pos-attacks-possible-as-different-types-of-malware-infect-4000-elasticsearch-servers/

3. Vulnerabilidades en bases de datos (3 puntos)

El pasado **27/10/2020** se publicaron una serie de vulnerabilidades que afectan a la base de datos oracle.

3.1. Explica brevemente (máximo en 15 líneas) **las 3 vulnerabilidades más graves publicadas** ese día para la **base de datos** Oracle.

Una de las vulnerabilidades que más frecuentemente podemos encontrar afectando a bases de datos son las inyecciones SQL.

3.2. Prepara una pequeña presentación (máximo 3 *slides*) en la que explicar porqué es necesario prevenir inyecciones SQL y qué impacto podría llegar a suponer este tipo de ataque para la organización. **Se trata de una presentación de concienciación para un directivo que no tiene ningún conocimiento técnico.**
Adjunta las slides como imágenes insertadas en tu respuesta a la PEC. Incluye algunas lineas indicando con qué explicación acompañarías cada una de las slides.

3.3. Describe qué pasos seguirías para **prevenir** ataques de inyección SQL. Debes identificar los puntos más vulnerables y posibles medidas de mitigación teniendo en cuenta la base de datos usada. Se permite el uso de cualquier técnica y herramienta externa.

3.4. Prepara un plan de detección ante un ataque SQLi. ¿Qué medidas pueden considerarse para **detectar** éste tipo de ataques?

3.5. Prepara un plan de mitigación ante un ataque SQLi. ¿Qué medidas consideras que pueden considerarse para **paliar y recuperarse** de los efectos de un ataque una vez éste se ha producido?