EXAMEN NO. 2 - PROYECTO

VALOR 15%

Este trabajo se realizará en grupos y se deberá entregar un documento estructurado por secciones donde se explique el trabajo realizado.

Adicionalmente, cada miembro del grupo deberá llenar una coevaluación de sí mismo y de cada uno de los miembros del equipo.

Especificaciones:

1. **(10 puntos)** Despliegue del equipo de trabajo
    a. Crear una máquina virtual con el Sistema Operativo de preferencia (Linux o Windows).
    b. Instalarle una versión de MySql
    c. Instalarle un servidor Web, dependiendo del lenguaje en que van a querer programar (IIS si van a programar en .Net, un Apache normal si van a programar en PHP o HTML y un Apache Tomcat si van a programa en Java Web).

    Entregable: Sección 1: Especificaciones técnicas del equipo

    Nota: si para otros cursos ya se tiene una máquina con esas condiciones la pueden usar.

2. **(10 puntos)** Descargar Nessus de https://www.tenable.com/downloads/nessus . Se recomienda descargar la versión 8.11.1, para Windows o Linux (según su preferencia). Debe obtener un código de activación gratuito en el mismo sitio. Instale Nessus en la computadora que se preparó en el punto anterior.
    a. Se recomienda desactivar las actualizaciones automáticas de Nessus (el proceso de actualización consume mucho CPU por un lapso alto, y se activa sin previo aviso). Sin embargo, asegúrese de actualizarlo antes de iniciar el escaneo.
    b. Inicie sesión en Nessus y configure un escaneo avanzado dirigido hacia la propia máquina. Provea a Nessus las credenciales de la máquina para obtener un resultado más preciso.
    c. Genere un reporte con las vulnerabilidades detectadas.

    Entregable: Sección 2: Reporte de las vulnerabilidades detectadas

3. **(15 puntos)** Aplicar las actualizaciones (parches) que faltan al equipo según el resultado del punto anterior.

    Entregable: Sección 3: Listado de las actualizaciones aplicadas, incluyendo código de actualización (KB….), el nombre y una pequeña descripción de lo que corrige

4. **(5 puntos)** Volver a correr el escaneo de vulnerabilidades y generar el reporte de vulnerabilidades detectadas. Verificar que el equipo no tenga vulnerabilidades, **críticas ni altas.**

    Entregable: Sección 4: Reporte de las vulnerabilidades post aplicación de parches

    Nota: No deberían mostrarse vulnerabilidades críticas ni altas.

5. **(25 puntos)** Ejecutar un ejercicio de Hardenización al equipo desplegado, para lo cual deberán basarse en las guías de benchmark provistas por CIS. Seleccione un enfoque sobre el cual quiera aplicar la hardenización.

    a. Correr el benchmark para identificar los elementos de seguridad faltantes en el equipo (de acuerdo el enfoque escogido)

    Entregable: Sección 5A: Informe de los resultados del benchmark

    b. Del informe de resultados del benchmark, seleccionar al menos 10 recomendaciones para fortalecer la seguridad y aplicar las guías de hardenización para esas recomendaciones

    Entregable: Sección 5B: Hardenización. Documentar los pasos de hardenización con pantallazos del antes y después

    c. Correr el benchmark nuevamente para identificar las mejoras que fueron implementadas.

    Entregable: Sección 5C: Informe de los resultados del benchmark donde se demuestre que se aplicaron mejoras.

6. **(25 puntos)** Desarrollar una aplicación Web que pida login y contraseña y cuya funcionalidad consista en el registro de datos personales (los datos a pedir son decisión de los estudiantes).

    La página Web debe tener certificado TLS para autenticar; además, la aplicación web debe programarse de forma segura, de forma que no sea vulnerable a los 10 ataques de Owasp. También, se debe programar el almacenamiento seguro de la contraseña.

    Entregable:

    Sección 6A: Pantallazos de la pantalla de login y de registro de información.

    Sección 6B: Explicación de cómo se programó de forma segura para evitar cada uno de los 10 ataques de OWASP con los pantallazos del código que programaron.

7. **(10 puntos) COEVALUACIÓN:** Llenar el formulario adjunto de coevalucación y autoevaluación.

8. **PUNTOS EXTRA (15 puntos):** En la aplicación Web del punto 7, programar un API, con autenticación para su consumo.

    Entregable: Explicación y pantallazos de la forma en que se programó la autenticación del API