Situación Evaluativa
Al estudiante FORMA A

Sigla	Nombre Asignatura	Horas semana
ASY6131	Seguridad en Sistemas computacionales	4 h semana 18

Ítem	Puntaje	% Ponderación
Competencia Especialidad	**77 puntos**	**100%**

1.-<u>INSTRUCCIONES GENERALES:</u>

- En esta oportunidad deberá desarrollar un proyecto de seguridad para la organización con las herramientas vistas durante el desarrollo de la asignatura que contemple:
  - Propuesta de plan y política de ciberseguridad a la organización
  - Identificación de potenciales vulnerabilidades
  - Propuesta de plan de mitigación
- Para la resolución del examen, NO se considera una presentación del producto.
- Los trabajos entregados fuera de plazo obtendrán la calificación mínima.
- Para esta evaluación puede usar herramientas locales o remotas.
- Máquinas virtuales a usar:

  1. Kali Linux
  2. Metasploitable

CONTENIDO DEL INFORME

- Información del proyecto
- Propósito y justificación del proyecto
- Todo lo abarcado en los requisitos específicos
- Conclusiones para apoyar la toma de decisiones, de acuerdo con las necesidades de la organización.

Formatos de entrega:

- Hoja tamaño carta o A4
- Tipo de letra: Títulos Arial 14 Negrita, Contenido Arial 12
- Interlineado: 1,5.
- Párrafo: Justificado.

PRESENTACIÓN ORAL

- Tendrá una duración de 15 minutos por cada equipo (10 de presentación y 5 de preguntas).
- La presentación debe contener:
  - Características y análisis del caso
  - Una demostración sobre vulnerabilidades detectadas (Puede ser video o en vivo).
  - Resumen de la política de seguridad a implementar
  - Conclusiones del análisis.

Situación Evaluativa
Al estudiante FORMA A

2.-CONTEXTO:

"Resolver las vulnerabilidades sistémicas para asegurar que el software construido cumple las normas de seguridad exigidas por la industria"

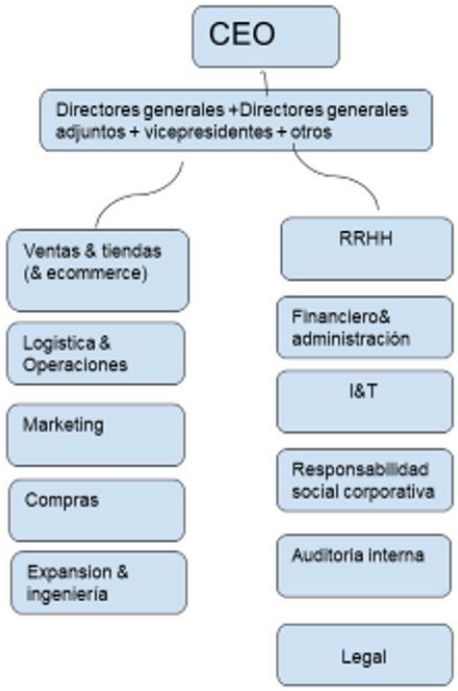
Actualmente usted forma parte del personal de especialistas de seguridad de la empresa "La segura LTDA". El equipo de expertos está conformado por 4 especialistas del área, con altos conocimientos sobre temas de desarrollo de código seguro, por lo que de manera cotidiana debe hacer tareas relacionadas a ejecución de pruebas, recibe y visualiza una serie de eventos e incidentes relacionados a la seguridad de los activos de información. Su tarea es analizar estos eventos, aprender más sobre ellos y decidir si indican actividad maliciosa. Para ello, se realiza investigación en diversas fuentes por medio de motores de búsqueda tales como Google, con la finalidad de obtener más información sobre estos eventos. Las siguientes tareas están diseñadas para proporcionar alguna orientación a través del proceso de análisis. Las habilidades que deberá evidenciar serán las siguientes:

- Realizar un levantamiento e identificación de activos de información y procesos de negocio relacionados a la organización, identificando los objetivos a los cuales la organización desea llegar en términos de ciberseguridad. (Ítem I).
- Evaluar las diferentes rutas para lograr los objetivos planteados por la organización en términos de ciberseguridad. (Ítem I).
- Realizar políticas de seguridad en desarrollo de código seguro y el uso del mismo, que le permita sensibilizar al cliente o usuario respecto del marco de trabajo para la organización. (Ítem I).
- Analizar y evaluar los mecanismos y herramientas utilizados para proporcionar los niveles de seguridad que requiere la organización. (Ítem I).
- Aplicar técnicas de escaneo de vulnerabilidades para garantizar la seguridad de la solución requerida por la organización, detectando las potenciales vulnerabilidades del software para proporcionar una solución en los niveles de seguridad que requiere la organización. (Item II).
- Priorizar las vulnerabilidades identificadas del software a fin de desarrollar un plan de mitigación. (Item II).
- Explotar las vulnerabilidades críticas mediante técnicas de Ethical hacking, a fin de verificar el grado de impacto que ellas puedan causar. (Item II).
- Elaborar un plan de mitigación de vulnerabilidades y amenazas identificadas como críticas con posibilidad de explotación para garantizar la seguridad de la solución requerida por la organización, aplicando controles de ciberseguridad para garantizar los principios de la seguridad informática en la aplicación de software desarrollado. (Ítem III).

El día de hoy, ha sido informado junto con su equipo que La empresa de retail OMICROM, ha contratado los servicios de la empresa y les ha sido asignado el proyecto. El cliente ha sufrido varios ataques a su sitio web en el último periodo, en los que le han extraído información crítica de la empresa e inyectado código en el mismo. El servicio Web se encuentra hospedado en un servidor Linux e implementado con apache.
La organización no ha desarrollado criterios de severidad, requerimientos de notificación o procesos de escalamiento para los eventos asociados con los ataques cibernéticos a la organización.

Situación Evaluativa
Al estudiante FORMA A

Adicionalmente, nos informan que su equipo de desarrollo iniciará un nuevo proyecto para migrar una aplicación muy antigua por lo que requieren contar con el marco de referencia, enmarcado en las buenas prácticas que deberán considerar los desarrolladores para la realización del proyecto bajo la premisa de "desarrollo de código seguro".
La empresa tiene el siguiente organigrama organizacional, en el que el área de I&T, tiene a su vez, al gerente del área TI, jefe de redes, jefe de desarrollo y sistemas.



3.-<u>REQUERIMIENTOS:</u>

Para el desarrollo de la entrega solicitada, los equipos de trabajo deben cumplir con los siguientes aspectos:

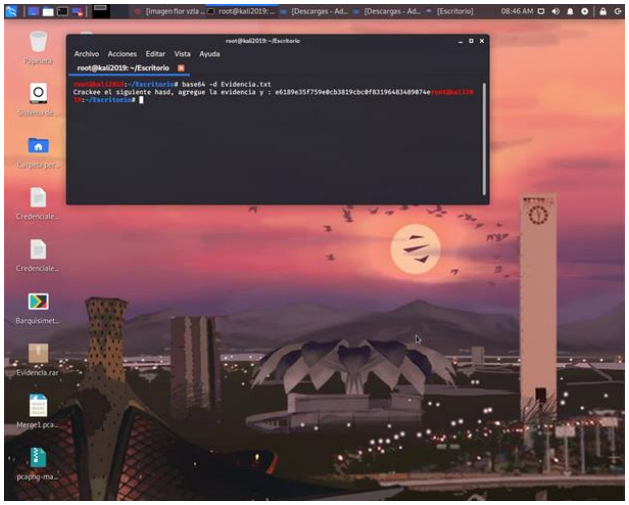
- Se deberá personalizar el fondo de escritorio de la máquina virtual Kali con la finalidad de demostrar que las capturas de pantalla se realizaron por usted y su equipo de trabajo. Para ello, descargue cualquier imagen de internet y defínala como fondo de escritorio.
- Utilizar Máquinas virtuales simulando los escenarios descritos en el caso, para implementar lo solicitado.

IMPORTANTE: Cuando guarde evidencia de lo realizado preocúpese de que se vea esta personalización ya que no serán consideradas las imágenes que no cumplan con este requerimiento.

- Todas las actividades realizadas deberán ser respaldadas o evidenciadas por medio de las correspondientes capturas de pantalla y su respectiva explicación.
- Verificar que tu máquina virtual se encuentre conectada a internet.

Situación Evaluativa
Al estudiante FORMA A

Ejemplo de personalización de pantalla:



Item I: Propuesta de plan y política de ciberseguridad a la organización

- Realice el levantamiento e identificación de activos de información y procesos de negocio relacionados a la organización, identificando los objetivos a los cuales la organización desea llegar en términos de ciberseguridad. (para ello puede incorporar supuestos al caso entregado inicialmente. Estos supuestos pueden basarse en empresas reconocidas del ramo retail)
- Evalúa las posibles rutas para lograr los objetivos planteados por la organización en términos de ciberseguridad, basándose en las buenas prácticas y estándares existentes.

Elabora el plan y la política de seguridad en desarrollo de código seguro y el uso de este, basado en OWASP. El plan debería considerar, entre otros:

  - Especificación de requerimientos de seguridad en etapa de análisis.
  - Especificación de requerimientos de seguridad en etapa de diseño del software.
  - Especificación de requerimientos de seguridad en etapa de codificación del software

- Analizar y evaluar 3 mecanismos y/o herramientas utilizadas para proporcionar los niveles de seguridad que requiere la organización.
- Proponga la estructura del gobierno corporativo para esta compañía

Ítem II: Gestión de vulnerabilidades

En este apartado, simularemos el servidor web utilizando la máquina virtual metaexplotaible. Como herramientas podrá utilizar el sofware local o remoto que se ha utilizado a lo largo del semestre para detección y análisis de vulnerabilidades.

Situación Evaluativa
Al estudiante FORMA A

- Haga un análisis de vulnerabilidades del sistema.
- En base a los resultados obtenidos, clasifique las vulnerabilidades identificadas según su criticidad.
- Explote las vulnerabilidades críticas mediante técnicas de Ethical hacking, a fin de verificar el grado de impacto que ellas puedan causar.
- Defina posibles soluciones a vulnerabilidades encontradas

Ítem III: Plan de mitigación

Elabore un plan de mitigación de vulnerabilidades y amenazas identificadas como críticas con posibilidad de explotación para garantizar la seguridad de la solución requerida por la organización, aplicando controles de ciberseguridad para garantizar los principios de la seguridad informática en la aplicación de software desarrollado.