1. Datos Generales de la asignatura

Nombre de la asignatura:	Seguridad de Datos.
Clave de la asignatura:	IDB-2105
SATCA[1]:	1 – 4 - 5
Carrera:	Ingeniería en Sistemas Computacionales

2. Presentación

Caracterización de la asignatura
Esta asignatura aporta al perfil profesional del egresado de la carrera de Ingeniería en Sistemas Computacionales la capacidad de detectar agujeros de seguridad en aplicaciones web y redes de cómputo con la intención de solucionar o proteger las fallas de seguridad y mantener la integridad de la información en ambientes digitales. La asignatura viene a cubrir la necesidad que existe en la actualidad de proteger los sistemas de información de ataques, por parte de ciberdelincuentes, algo que se ha tornado muy común y que la sociedad exige profesionales con los conocimientos suficientes para abordar tales problemáticas en las redes e infraestructuras tecnológicas de las empresas e instituciones. La relación de esta materia está ligada con materias tales como Redes de Computadora, Conmutación y Enrutamiento en Redes de Datos, Administración de Redes, pero también con materias del corte de aplicaciones como, Programación Web, Tópicos Avanzados de Programación Web, Dispositivos Programables Inteligentes, Visualización Web y Procesamiento de Datos, esto derivado de la importancia de mejorar la seguridad en los productos desarrollados en las materias antes mencionadas.
Intención didáctica
La materia tiene la intención de proporcionar herramientas prácticas de hackeo al estudiante con la intención de descubrir fallas de seguridad y así tomar medidas para evitar violaciones de seguridad en redes de computadoras o a través de aplicaciones Web. La materia está dividida en 4 temas principales. El primer tema lleva al alumno a un conocimiento básico e introductorio sobre la actividad de los Hackers, así como la manera en que trabajan y lo que hacen o pueden hacer en una red de computadora o una aplicación web.

[1] Sistema de Asignación y Transferencia de Créditos Académicos

El segundo tema comienza con los métodos de recopilación de información, ya que muchos agujeros de seguridad se dan debido a la información disponible que puede obtener el ciberdelincuente a través de técnicas o programas especializados. El tercer tema viene a identificar las diferentes vulnerabilidades que pueden existir en un ámbito digital y con ello llevar a cabo ataques a estas vulnerabilidades en un ambiente virtual totalmente controlado, con la intención de poder llevar a cabo las modificaciones pertinentes en el ámbito real. Por último el cuarto tema trata sobre varios puntos adicionales que pueden servir al alumno en el ámbito profesional a la hora de aplicar los conocimientos en el ámbito laboral.

El docente desempeñará la labor como facilitadora de los contenidos teóricos y será un guía para la implementación de las prácticas realizadas en el entorno virtual en donde se deberán de realizar la detección de vulnerabilidades y los ataques, con el claro objetivo de conocer a fondo las debilidades y poder subsanar las mismas, será necesario evaluar los alumnos por medio de bitácoras, con la intención de observar y valorar el aprendizaje de los procesos a realizar.

Se debe de buscar el uso adecuado de herramientas gratuitas o de código abierto comerciales vigentes, para que puedan proponer en un futuro la adquisición de las herramientas en sus versiones empresariales en el ámbito virtual y para que de esta manera puedan actualizar su conocimiento con las versiones a surgir en un futuro.

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Instituto Tecnológico Superior de Jerez. Mayo del 2021.	Instituto Tecnológico Superior de Jerez. Mtro. Ricardo Saldivar Quezada.	Reuniones de Academia para el diseño de Especialidad

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
Aplicar técnicas de hackeo ético en los sistemas de información para detectar vulnerabilidades implementando soluciones para la prevención de ataques informáticos tanto en redes de cómputo como aplicaciones informáticas.

5. Competencias previas

Configura y administra servicios de red eficientes y confiables. Desarrolla aplicaciones web con diferentes tecnologías y lenguajes de programación. Entendimiento amplio de los diferentes protocolos de red.

6. Temario

No.	Temas	Subtemas
1	Introducción al Hacking Ético.	1.1. Fases del Hacking. 1.2. Tipos de Hackers. 1.3. Metodologías de Hacking Ético.
2	Métodos de Recopilación de Información.	2.1. Recopilación pasiva. 2.2. Recopilación semi-pasiva. 2.3. Recopilación activa.
3	Vulnerabilidades.	3.1. Vulnerabilidades en Hosts. 3.2. Vulnerabilidades en aplicaciones Web. 3.3. Vulnerabilidades en Redes.
4	Herramientas y temas adicionales para el Hacking Ético.	4.1. Machine Learning aplicado al hacking. 4.2. Activismo de seguridad informática. 4.3. Casos de Estudio sobre Hackeo. 4.4. Desarrollo de informes sobre Hacking Ético.

7. Actividades de aprendizaje de los temas

1. Introducción al Hacking Ético	
Competencias	Actividades de aprendizaje
Específica(s): Conoce los conceptos iniciales sobre el Hackeo Ético y las metodologías principales que se emplean en la actualidad. Genéricas: • Capacidad de análisis y síntesis. • Capacidad de organizar y planificar.	Exposición y discusión sobre las diferentes fases del Hacking Ética. Investigar y analizar los diferentes tipos de Hackers en diversas fuentes. Investigar y analizar sobre las diferentes metodologías que implementan los Hackers en sus ataques y plasmar lo encontrado de manera clara y objetiva ya

• Habilidad para buscar y analizar información proveniente de fuentes diversas. • Habilidades de investigación. • Capacidad de generar nuevas ideas. Liderazgo. • Habilidad para trabajar en forma autónoma. • Habilidad de redactar de manera clara y objetiva las ideas.	sea en un reporte de investigación o algún recurso didáctico.
2. Métodos de Recopilación de Información.	
Competencias	Actividades de aprendizaje
Específica(s): Comprende y aplica métodos para la recopilación de la información de diferentes medios para la preparación de ataques o en la detección de vulnerabilidades de los sistemas informáticos. Genéricas: • Capacidad de análisis y síntesis. • Habilidad para buscar y analizar información proveniente de fuentes diversas. • Capacidad de aplicar los conocimientos en la práctica. • Habilidades en el uso de las tecnologías de la información y de la comunicación. • Habilidades de investigación. • Capacidad de generar nuevas ideas. • Solución de problemas.	Investigar sobre los diferentes tipos de métodos de recopilación de la información en metodologías de Hackeo. Llevar a cabo la instalación y configuración del laboratorio virtual con software gratuito o de prueba, junto con sistemas operativos de código libre para aplicar las diferentes metodologías de recopilación de información. Usar diferentes programas para la obtención de información del usuario o de las redes de computadoras.
3. Vulnerabilidades.	
Competencias	Actividades de aprendizaje

Específica(s): Detectar vulnerabilidades para efectuar ataques a los diferentes sistemas informáticos de una red para hacer las correcciones pertinentes y evitar ataques de personas externas. Genéricas: • Capacidad de análisis y síntesis. • Habilidad para buscar y analizar información proveniente de fuentes diversas. • Capacidad de aplicar los conocimientos en la práctica. • Habilidades en el uso de las tecnologías de la información y de la comunicación. • Habilidades de investigación. • Capacidad de generar nuevas ideas. • Solución de problemas.	Investigar y discutir sobre los diferentes tipos de vulnerabilidades existentes en los sistemas informáticos. Instalar software usado para realizar ataques y detección de vulnerabilidades en un ambiente virtual encapsulado. Realizar prácticas sobre ataques a vulnerabilidades de tipo host. Realizar prácticas sobre ataques a páginas Web. Realizar prácticas sobre ataques hacia redes de computadoras.
4. Herramientas y temas adicionales para el Hacking Ético.	
Competencias	Actividades de aprendizaje
Específica(s): Conocer y aplicar herramientas adicionales para el Hacking Ético y el diseño de informes completos para las auditorías de seguridad. Genéricas: • Capacidad de análisis y síntesis. • Habilidad para buscar y analizar información proveniente de fuentes diversas. • Conocimientos sobre el área de estudio y la profesión. • Capacidad de aplicar los conocimientos en la práctica.	Aplicar técnicas de Machine Learning en ataques de Hackeo en una práctica controlada. Exponer diferentes casos de estudio sobre Hacking Ético y discutir en el grupo sobre las posibles herramientas usadas y las maneras en que se puede contrarrestar los ataques. Investigar sobre la ética que se debe de llevar en los trabajos del Hacking Ético y el activismo internacional que se lleva a cabo en esta área.

• Habilidades en el uso de las tecnologías de la información y de la comunicación. • Habilidades de investigación. • Capacidad de generar nuevas ideas. • Capacidad de identificar, plantear y resolver problemas. • Capacidad creativa.	Llevar a cabo un documento de auditoria de los resultados encontrados en el análisis de alguna red.

8. Práctica(s)

- Configurar un laboratorio de pruebas con alguna herramienta de virtualización de sistemas operativos y un sistema operativo con herramientas de hackeo o auditoría de redes.
- Llevar a cabo prácticas variadas con métodos pasivos de recopilación de información.
- Llevar a cabo prácticas variadas con métodos activos de recopilación de información.
- Llevar a cabo prácticas variadas con métodos semi-pasivos de recopilación de información.
- Utilizar software y técnicas de hackeo para realizar ataques de vulnerabilidades basadas en host o equipos de cómputo en una red virtualizada.
- Utilizar software y técnicas de hackeo para realizar ataques de vulnerabilidades en páginas web.
- Utilizar software y técnicas de hackeo para realizar ataques de vulnerabilidades en servidores.
- Aplicar técnicas de Machine Learning en metodologías de Hacking Ético.
- Diseñar un documento con los resultados de los ataques realizados a vulnerabilidades, con fines de auditoría de seguridad.

9. Proyecto de asignatura

El objetivo del proyecto que planteé el docente que imparta esta asignatura, es demostrar el desarrollo y alcance de la(s) competencia(s) de la asignatura, considerando las siguientes fases:

- **Fundamentación:** marco referencial (teórico, conceptual, contextual, legal) en el cual se fundamenta el proyecto de acuerdo con un diagnóstico realizado, mismo que permite a los estudiantes lograr la comprensión de la realidad o situación objeto de estudio para definir un proceso de intervención o hacer el diseño de un modelo.

- **Planeación:** con base en el diagnóstico en esta fase se realiza el diseño del proyecto por parte de los estudiantes con asesoría del docente; implica planificar un proceso: de intervención empresarial, social o comunitario, el diseño de un modelo, entre otros, según el tipo de proyecto, las actividades a realizar los recursos requeridos y el cronograma de trabajo.

- **Ejecución:** consiste en el desarrollo de la planeación del proyecto realizada por parte de los estudiantes con asesoría del docente, es decir en la intervención (social, empresarial), o construcción del modelo propuesto según el tipo de proyecto, es la fase de mayor duración que implica el desempeño de las competencias genéricas y especificas a desarrollar.

- **Evaluación:** es la fase final que aplica un juicio de valor en el contexto laboral-profesión, social e investigativo, ésta se debe realizar a través del reconocimiento de logros y aspectos a mejorar se estará promoviendo el concepto de “evaluación para la mejora continua”, la metacognición, el desarrollo del pensamiento crítico y reflexivo en los estudiantes.

10. Evaluación por competencias

Para evaluar las actividades de aprendizaje se recomienda solicitar: Infografías, Tablas Comparativas, Bitácoras de prácticas, Reportes de investigación, Videos tutoriales sobre el uso de alguna herramienta, Ensayos.

Cómo herramienta de verificación en el logro de las competencias del estudiante en cada una de las actividades de aprendizaje se recomienda usar: Rúbricas de evaluación, listas de cotejo y Guías de proyectos.

11. Fuentes de información

- Sabih, Z. (2018). Learn Ethical Hacking from Scratch. Packt Publishing.
- Maurushat, A. (2019). Ethical Hacking. University of Ottawa Press.
- Regalado, D., Harris, S., Harper, A., Eagle, C., Ness, J., Spasojevic, B., . . . Sims, S. (2015). Gray Hat Hacking: The Ethical Hacker's Handbook. Mc Graw-Hill Education.
- Rojas, M., & Ferney, E. (n.d.). Hacking Ético: Una herramienta para la seguridad informática.
- García-Moran, J. P. Fernández Hansen, Y. y Martínez Sánchez, R. (2014). Hacking y Seguridad en Internet: edición 2011. RA-MA Editorial. https://elibro.net/es/ereader/jerez/106415?page=13
- Bhardwaj, M., & Singh, G. (2011). Types of Hacking and their Counter Measure. *International Journal of Educational Planning & Administration.*, 43-53.
- Astudillo, K. (2018). Hacking Ético: ¡Cómo convertirse en hacker ético en 21 días o menos! 3ª Edición. Ra-Ma.
- Hoffman, H. (2020). Ethical Hacking with Kali Linux: Learn fast how to hack like a Pro.
- Baloch, R. (2015). Ethical Hacking and Penetration Testing Guide. CRC Press