1. Datos Generales de la asignatura

Nombre de la asignatura:	Pruebas de Intrusión
Clave de la asignatura:	CBB-2426
SATCA[1]:	1-4-5
Carrera:	Ingeniería en Ciberseguridad.

2. Presentación

Caracterización de la asignatura

El programa de la asignatura está diseñado para contribuir en la formación integral de las y los estudiantes del Tecnológico Nacional de México (TecNM), ya que proporciona las competencias necesarias para:

- Utiliza sistemas operativos, lenguajes de programación, redes y entornos tecnológicos para integrar soluciones de seguridad con responsabilidad e inclusión social en las organizaciones.
- Dirige el monitoreo, análisis y control de la información utilizando herramientas y marcos de referencia, con perspectiva ética, de respeto por la persona y de responsabilidad social.
- Evalúa riesgos de seguridad y vulnerabilidad en aplicaciones o instalaciones de tecnologías de la información con apoyo de herramientas de vanguardia automatizadas de acuerdo a metodologías, normas y estándares de excelencia.
- Diseña políticas de seguridad informática para establecer controles de seguridad pertinentes atendiendo los principios de no discriminación, Inclusión y equidad social.
- Gestiona incidentes y eventos de seguridad de informática para reducir la afectación negativa de la seguridad de la información y dar continuidad a las operaciones de la organización, atendiendo los principios de no discriminación, Inclusión y equidad social.
- Emplea métodos criptográficos para establecer protocolos de seguridad en el transporte de datos seguros a nivel de aplicación, usando herramientas de seguridad basadas en dichos protocolos integrando excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano.
- Propone soluciones para proteger la transmisión y almacenamiento de información sensible dentro de un área funcional o técnica, a partir de marcos de referencia con excelencia, vanguardia e innovación social aplicando mejores prácticas del mercado.
- Gestiona planes y proyectos de seguridad de la información de acuerdo con las necesidades del negocio, considerando riesgos y contingencias, promoviendo el cumplimiento de los principios de no discriminación, inclusión, equidad social, políticas, normas y acuerdos de nivel de servicio.
- Aplica procedimientos y técnicas de auditoría informática para detectar si se protegen los activos y recursos de la organización, si se mantiene la integridad de los datos, si se utiliza

[1] Sistema de Asignación y Transferencia de Créditos Académicos

eficientemente los recursos, si se atienden los principios de no discriminación, inclusión y equidad social y si se cumple con las leyes y regulaciones establecidas.

- Implementa soluciones metodológicas y controles de seguridad en el ciclo de vida del desarrollo de software que permitan la reducción de vulnerabilidades y la inclusión de mejores prácticas de seguridad, con una perspectiva de responsabilidad social.

Intención didáctica

El estudiante aprenderá los beneficios al utilizar el hacking ético para evaluar y reforzar sus sistemas de seguridad.

- Descubrir vulnerabilidades uno de los beneficios de la ciberseguridad y el hacking ético, es que con los ciberataques realizados por profesionales del hacking ético se pueden identificar las debilidades del sistema y, de esta manera, aplicar acciones correctivas para eliminarlas y evitar los riesgos que suponen en materia de ciberseguridad.
- Refuerza las políticas de ciberseguridad, otro de los beneficios de la ciberseguridad y el hacking ético, se puede medir si la política de ciberseguridad de la empresa es la adecuada y si los usuarios la están cumpliendo de forma correcta, y poder garantizar un alto nivel de ciberseguridad en el negocio.
- Aporta valor a la ciberseguridad, gracias al hacking ético, la empresa puede dar valor a la ciberseguridad, ya que empiezan a ser conscientes de la importancia que tiene la seguridad de sus sistemas.
- Reduce los costes de inversión, también destaca como beneficio, que la información que aporta el Hackeo Ético permite definir de forma eficiente las medidas necesarias para eliminar vulnerabilidades e implementar las herramientas y sistemas de defensa más eficaces.

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Tecnológico Nacional de México del 4 al 6 de marzo del 2024.	Representantes de los Institutos Tecnológicos de: Aguascalientes, Cerro Azul, Ciudad Juárez, La Paz, Jiquilpan, Mérida, Morelia, Tuxtla Gutiérrez, Villa Hermosa. Institutos Tecnológicos Superiores de La Región Carbonífera, Las Choapas	Propuesta sintética de la carrera de Ingeniería en Ciberseguridad.
Tecnológico Nacional de México del 22 al 26 de abril del 2024.	Representantes de los Institutos Tecnológicos de: Aguascalientes, Cerro Azul, Ciudad Juárez, La Paz, Jiquilpan, Mérida,	Diseño y/o desarrollo curricular de la carrera de Ingeniería en Ciberseguridad

	Morelia, Tuxtla Gutiérrez, Villa Hermosa. Institutos Tecnológicos Superiores de La Región Carbonífera, Las Choapas. Representante de Ciencias Básica de los Institutos de: Celaya, Morelia CENIDET y CIIDET.	
Tecnológico Nacional de México del 27 al 31 de mayo del 2024.	Representantes de los Institutos Tecnológicos de: Aguascalientes, Cerro Azul, Jiquilpan, Mérida, Villahermosa. Institutos Tecnológicos Superiores de La Región Carbonífera, Las Choapas	Consolidación curricular de la carrera de Ingeniería en Ciberseguridad.

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
• Comprende, aplica y evalúa técnicas de hacking ético. • Diseña sistemas y técnicas específicas para asegurar los sistemas informáticos de la empresa y diversos dispositivos.

5. Competencias previas

- Analiza los requerimientos, manipula bases de datos para brindar soluciones al tratamiento de información basándose en modelos y estándares; de igual modo, implementa bases de datos para apoyar la toma de decisiones considerando las reglas de negocio.
- Conoce, selecciona y administra la seguridad de un sistema operativo en plataformas cliente-servidor, para resolver problemáticas reales y aplicar procedimientos de configuración de seguridad en plataformas de software.
- Desarrollar habilidades para diseñar, implementar y asegurar aplicaciones web mediante la integración de fundamentos del desarrollo web, la creación de interfaces interactivas en el front-end, la programación robusta en el back-end, y la aplicación de medidas de seguridad para proteger la integridad de los datos y la privacidad de los usuarios.
- Dominar los principios de la criptografía simétrica y asimétrica.
- Aplicar algoritmos de cifrado y técnicas de autenticación de forma eficiente y segura para proteger la información.
- Diseñar y desarrollar soluciones criptográficas para garantizar la confidencialidad, integridad y autenticidad de la información.

6. Temario

No.	Temas	Subtemas
1	Ethical Hacking.	1.1. Definición y objetivos 1.2. Penetration Testing 1.2.1. Terminología 1.2.2. Equipos Rojo y Azul 1.3. Importancia de la prueba de intrusión 1.4. Metodologías y enfoque comunes 1.5. Consideraciones éticas en la realización de pruebas de intrusión 1.6. Acuerdo de confidencialidad y consentimiento del cliente
2	Pruebas de Intrusión	2.1. Fases 2.1.1. Recopilación de la información 2.1.2. Modelado de Amenazas 2.1.3. Exploración 2.1.4. Análisis de vulnerabilidades 2.1.5. Explotación 2.1.6. Escalada de privilegios 2.1.7. Eliminación de huellas digitales 2.2. Obtención de Información 2.2.1. Utilizando Internet 2.2.2. Google hacking 2.2.3. OSINT 2.3. Herramientas de software 2.4. Social Engineering toolkit 2.5. Herramientas para encontrar vulnerabilidades 2.5.1. Explotación 2.5.2. Metasploit framework 2.5.3. Creación de troyanos 2.5.4. Escalando privilegios 2.5.5. Exploit-DB 2.5.6. Rapid7 2.5.7. 0day.today
3	Ataques a Contraseñas	3.1. Introducción 3.2. Diccionarios 3.3. Ataques offline 3.4. Ataques Online
4	Informes y Resultados.	4.1. Documentación de hallazgos 4.2. Evaluación e impacto de vulnerabilidades 4.3. Recomendaciones y propuestas para la resolución de huecos de seguridad 4.4. Presentación y entrega de informe

7. Actividades de aprendizaje de los temas

1. Ethical Hacking.	
Competencias	Actividades de aprendizaje
Específica(s): • Analizar y detectar técnicas de ocultación de ataques a sistemas y redes en casos reales. • Conocer las tendencias actuales en técnicas de ciberataque. • Analizar sistemas para encontrar evidencias digitales de ciberataques y adoptar las medidas para mantener la cadena de custodia de dichas evidencias. • Comprender, aplicar y evaluar técnicas de hacking ético. • Conocer requisitos y procedimientos avanzados de certificación de sistemas seguros. • Comprender, aplicar y evaluar las técnicas de seguridad en el desarrollo y uso de aplicaciones web y en los servicios basados en ellas. • Analizar e identificar las vulnerabilidades de un sistema informático, y ser capaz de desarrollar métodos de protección de la información.	• Conocer los papeles en los que operan los equipos Rojo y Azul. • Formar dichos equipos con no discriminación, Inclusión y equidad social. • Hacer mucho énfasis en el compromiso del Hacking Ético. • Realizar instalaciones de los entornos controlados para realizar el pentesting. • Realizar la instalación de herramientas para el pentesting. • Investigar sobre los diferentes acuerdos de confidencialidad y consentimiento del cliente tanto estatales, nacionales e internacionales.

• Comprender y saber aplicar técnicas criptográficas avanzadas. *Genérica(s):* • Capacidad de análisis, síntesis y abstracción. • Capacidad de comunicación oral y escrita. • Habilidad en el uso de tecnologías de información y comunicación. • Trabajo en equipo. • Conocer la normativa técnica y disposiciones legales de aplicación en la materia de ciberseguridad, sus implicaciones en el diseño de sistemas y en la aplicación de herramientas de seguridad. *Transversal(es):* • Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social. • Usa comunicación oral y escrita atendiendo los principios de no discriminación, Inclusión y equidad social. • Diseña e implementa soluciones a problemas propios de ámbito de su área de aplicación integrando aprendizajes, rasgos y capacidades de excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano.	
2. Pruebas de intrusión.	
Competencias	Actividades de aprendizaje
Específica(s): • Analizar y detectar técnicas de ocultación de ataques a sistemas y redes en casos reales.	• Formar dichos equipos con no discriminación, Inclusión y equidad social. • Conocer las diferentes técnicas de obtención de información, ya sea referente a un dispositivo o a una persona.

• Conocer las tendencias actuales en técnicas de ciberataque. • Analizar sistemas para encontrar evidencias digitales de ciberataques y adoptar las medidas para mantener la cadena de custodia de dichas evidencias. • Comprender, aplicar y evaluar técnicas de hacking ético. • Conocer requisitos y procedimientos avanzados de certificación de sistemas seguros. • Comprender, aplicar y evaluar las técnicas de seguridad en el desarrollo y uso de aplicaciones web y en los servicios basados en ellas. • Analizar e identificar las vulnerabilidades de un sistema informático, y ser capaz de desarrollar métodos de protección de la información. • Comprender y saber aplicar técnicas criptográficas avanzadas. • Conocer la normativa técnica y disposiciones legales de aplicación en la materia de ciberseguridad, sus implicaciones en el diseño de sistemas y en la aplicación de herramientas de seguridad. *Genérica(s):* • Capacidad de análisis, síntesis y abstracción. • Capacidad de comunicación oral y escrita. • Habilidad en el uso de tecnologías de información y comunicación. • Trabajo en equipo. *Transversal(es):*	• Utilizar las herramientas de uso público y privado para la obtención de información y vulnerabilidades de equipos y personas. • Conocer las diferentes técnicas de ingeniería social. • Se sugiere el uso de herramientas como Shodan, Maltego, OpenVas, Nmap, WireShark, tcpdump, etc. • Se recomienda utilizar la herramienta SET incluida en kali linux con el fin de generar clones de sitios web y obtener credenciales, generar códigos QR para redirección, etc. • Para encontrar vulnerabilidades se sugiere el uso de las siguientes herramientas: Nmap con Scrypting, OpenVas, Nessus, Explioit DB, Google Hacking, etc • De igual forma para las pruebas de intrusión se sugiere el uso de Rapid7 y 0day.today etc.

• Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social. • Usa comunicación oral y escrita atendiendo los principios de no discriminación, Inclusión y equidad social. • Diseña e implementa soluciones a problemas propios de ámbito de su área de aplicación integrando aprendizajes, rasgos y capacidades de excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano.	

3. Ataques a contraseñas.	
Competencias	Actividades de aprendizaje
Específica(s): • Analizar y detectar técnicas de ocultación de ataques a sistemas y redes en casos reales. • Conocer las tendencias actuales en técnicas de ciberataque. • Analizar sistemas para encontrar evidencias digitales de ciberataques y adoptar las medidas para mantener la cadena de custodia de dichas evidencias. • Comprender, aplicar y evaluar técnicas de hacking ético. • Conocer requisitos y procedimientos avanzados de certificación de sistemas seguros. • Comprender, aplicar y evaluar las técnicas de seguridad en el desarrollo y uso de aplicaciones web y en los servicios basados en ellas. • Analizar e identificar las vulnerabilidades de un sistema informático, y ser capaz de desarrollar	• Formar dichos equipos con no discriminación, Inclusión y equidad social. • Se sugiere el uso de herramientas de cracking de contraseñas como John the ripper, Hidra, Medussa, Hash cat, OphCrak y herramientas en línea como onlinehashcrack.com.

métodos de protección de la información. • Comprender y saber aplicar técnicas criptográficas avanzadas. *Genérica(s):* • Capacidad de análisis, síntesis y abstracción. • Capacidad de comunicación oral y escrita. • Habilidad en el uso de tecnologías de información y comunicación. • Trabajo en equipo. *Transversal(es):* • Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social. • Usa comunicación oral y escrita atendiendo los principios de no discriminación, Inclusión y equidad social. • Diseña e implementa soluciones a problemas propios de ámbito de su área de aplicación integrando aprendizajes, rasgos y capacidades de excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano	

4. Informes y Resultados.

Competencias	Actividades de aprendizaje
Específica(s): • Analizar y detectar técnicas de ocultación de ataques a sistemas y redes en casos reales. • Conocer las tendencias actuales en técnicas de ciberataque.	• Formar dichos equipos con no discriminación, Inclusión y equidad social. • Investigar sobre los informes de resultados de las pruebas de intrusión generados por empresas y personas independientes para tomarlos como ejemplo de cómo va un informe.

• Analizar sistemas para encontrar evidencias digitales de ciberataques y adoptar las medidas para mantener la cadena de custodia de dichas evidencias. • Comprender, aplicar y evaluar técnicas de hacking ético. • Conocer requisitos y procedimientos avanzados de certificación de sistemas seguros. • Comprender, aplicar y evaluar las técnicas de seguridad en el desarrollo y uso de aplicaciones web y en los servicios basados en ellas. • Analizar e identificar las vulnerabilidades de un sistema informático, y ser capaz de desarrollar métodos de protección de la información. • Comprender y saber aplicar técnicas criptográficas avanzadas. • Conocer la normativa técnica y disposiciones legales de aplicación en la materia de ciberseguridad, sus implicaciones en el diseño de sistemas y en la aplicación de herramientas de seguridad. *Genérica(s):* • Capacidad de análisis, síntesis y abstracción. • Capacidad de comunicación oral y escrita. • Habilidad en el uso de tecnologías de información y comunicación. • Trabajo en equipo. *Transversal(es):* • Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social.	• Utilizar los marcos y normas internacionales sobre la presentación de resultados como por ejemplo la ISO 27001, etc.

• Usa comunicación oral y escrita atendiendo los principios de no discriminación, Inclusión y equidad social. • Diseña e implementa soluciones a problemas propios de ámbito de su área de aplicación integrando aprendizajes, rasgos y capacidades de excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano	

8. Práctica(s)

1.- Instalación y configuración de los equipos a utilizar en el laboratorio.

- Instalar los servidores: Windows, Linux, Metasploitable, OWASP, etc.
- Instalar el equipo para penetración con Kali Linux.
- Utilizar Nmap para explorar la red y los equipos.
- Generar equipo de trabajo como son el Rojo y el Azul.

2.- Pruebas de Intrusión.

- Utilizando el laboratorio dentro de un entorno controlado:
  - Instalar y configurar un entorno de red de prueba con diferentes equipos tanto servidores, como portátiles, móviles etc.
  - Abrir intencionalmente pùertos en los servidores y servicios y equipos.
- Realizar búsquedas con Google dorks sobre un tema en específico.
- Utilizar la red OSINT para investigar a personas.
- Utilizar la red Shodan para encontrar MAC adress de diversos dispositivos.
- Realizar búsqueda avanzada con NMAP.
- Capturar y analizar tráfico de la red del laboratorio.
- Realizar Pretexting.
- Hacer una campaña de phising con las diversas herramientas disponibkles.
- Utilizar la herramienta incorporada SET en Kali Linux para realiar phising con emal y demás.
- Utilizar WifiPhiser para la obtencion de información del usuario, y capturar sus datos.
- Utilizar NMAP para encontrar las vulnerabilidades de los equipos de la red.
- Instalar OpenVas para detectar vulnerabilidades de los equipos.
- Instalar y configurar la herramienta Nessus para la detección de vulnerabiliades en los equipos del laboratorio.

- Utilizar la base de datos de la red Exploit DB para la interpretacion de los voletines de seguridad.
- Instalar y configurar la herramienta Metasploit
- Crear virus troyanos
- Utilizar las Vulnerabilidades encontradas de los equipos para hacer pruebas de penetración.
- Crear virus troyanos con encriptación a nivel de se indetectados por los antivirus y firewalls.
- Tomar control de los equipos y escalar los privilegios del usuario
- De ser posible instalar y configrar sistemas de videovigilancia.
- Realizar las pruebas de obtención de información y anotar los resultados

3.- Ataques a contraseñas.

- Realizar búsquedas con Nmap y diversas herramientas para descubrir la red
- Se sugiere el uso de herramientas como: John the ripper, Hidra, Medussa, Hash cat, OphCrak y herramientas en linea como onlinehashcrack.com; para descubrir las vulnerabilidades en los equipos.

3.- informes y resultados.

- De acuerdo a la información obtenida realizar los informes de resultados, tomando como base los formatos internacionales para ello.
- Buscar en internet sobre los informes de resultados de dominio púiblico.
- Formar equipo de trabajo para encontrar vulnerabilidades y emitir el informe de resultados, tomando en cuenta la no discriminación, Inclusión y equidad social.

9. Proyecto de asignatura

El objetivo del proyecto que planteé el docente que imparta esta asignatura, es demostrar el desarrollo y alcance del(los) logro(s) formativo(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 los saberes, habilidades y destrezas 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”, el desarrollo del pensamiento crítico y reflexivo en los estudiantes.

10. Evaluación de saberes, habilidades y destrezas

La evaluación de la asignatura debe de ser continua, sumativa y formativa, por lo que debe de considerarse el desempeño de cada una de las actividades de aprendizaje, haciendo especial énfasis en:

- Capacidad de análisis, síntesis, abstracción, de organizar y planificar, comprobado mediante las evidencias de aprendizaje tales como: Reportes, ensayos y prácticas, solución de ejercicios extra clase, actividades de investigación, elaboración de modelos o prototipos.
- Resolución de problemas con apoyo de software.
- Exámenes escritos y prácticos para comprobar la adquisición de conocimientos.

11. Fuentes de Información

1. R. MESSIER, CEH V11 CERTIFIED ETHICAL HACKER STUDY GUIDE. [S.l.]: WILEYSYBEX, 2021.
2. S. McClure, J. Scambray and G. Kurtz, Hacking exposed. Berkeley, Calif.: Osborne/McGraw-Hill, 1999.
3. R. Luppicini and B. Abu-Shaqra, The changing scope of technoethics in contemporary society. IGI Global, 2018.
4. Leonhardt F, "Auditing, Penetration Testing And Ethical Hacking". World Scientific Publishing Co, 2010. Available from: Scopus®, Ipswich, MA.
5. Himma K, Tavani H, "Ethical Issues Involving Computer Security: Hacking, Hacktivism, and Counterhacking". Handbook Of Information & Computer Ethics [serial online]. January 2008;:191. Available from: Complementary Index, Ipswich, MA.
6. Vignesh R, Rohini K. "Analysis to determine the scope and Challenging responsibilities of Ethical Hacking employed in Cyber Security". International Journal Of Engineering And Technology(UAE) [serial online]. January 1, 2018;7(3.27 Special Issue 27):196-199.
7. Berger H, Jones A. "Cyber security & ethical hacking for SMEs". ACM International Conference Proceeding Series [serial online]. July 25, 2016;Part F130520(Proceedings of the 11th International Knowledge Management in Organizations Conference on the Changing Face of Knowledge Management Impacting Society, KMO 2016.
8. Patil S, Jangra A, Bhale M, Raina A, Kulkarni P. "Ethical hacking: The need for cyber security". IEEE International Conference On Power, Control, Signals And Instrumentation Engineering, ICPCSI 2017 [serial online]. June 20, 2018;(IEEE International Conference on Power, Control, Signals and Instrumentation Engineering, ICPCSI 2017):1602-1606.
9. Asociación Nacional de Instituciones de Educación en Tecnologías de Información A.C. (2024). Modelo curricular por competencias. ANIEI.