1. Datos Generales de la asignatura

Nombre de la asignatura:	Hacking Ético
Clave de la asignatura:	CID2603
SATCA[1]:	2 -3 – 5
Carrera:	• Ingeniería en Sistemas Computacionales • Ingeniería en Tecnologías de la Información y Comunicaciones • Ingeniería en Inteligencia Artificial • Ingeniería en Ciencia de Datos • Ingeniería en Desarrollo de Aplicaciones. • Ingeniería en Informática

2. Presentación

Caracterización de la asignatura

La asignatura de **Hacking Ético** en la especialidad de *"Ciberseguridad para Industrias Clave y Servicios Estratégicos"* es clave para el perfil de egreso al formar profesionales capaces de:

- Identificar y mitigar amenazas cibernéticas de manera ética y efectiva.
- Contribuye a la capacidad de realizar pruebas de penetración, evaluación de vulnerabilidades y elaboración de informes, habilidades esenciales para proteger infraestructuras críticas y sistemas de sectores estratégicos como la agroindustria, energía, logística, entre otros.
- La asignatura se enfoca en la planificación, ejecución y post-explotación de pruebas de penetración, cubriendo tanto la seguridad en redes como en la nube, dispositivos móviles e IoT, lo que la convierte en un pilar de la ciberseguridad avanzada.
- Su importancia radica en su enfoque hacia la vanguardia tecnológica y su compromiso con la responsabilidad social, dado que el hacking ético contribuye al bienestar general al proteger activos clave para la sociedad.
- Esta asignatura se relaciona estrechamente con Ciberseguridad Empresarial en la gestión de riesgos y cumplimiento, y con Auditoría de Ciberseguridad, ya que ambas comparten competencias en análisis, seguridad y creación de informes, lo que permite la integración de proyectos transversales.
- Además, fomenta la inclusión, la equidad de género y la innovación social, promoviendo que estudiantes de diversos contextos participen activamente en un ámbito tan crítico como la ciberseguridad.
- La evaluación y mejora continua se basará en la generación de proyectos que promuevan la excelencia y reflejen el compromiso con una interculturalidad que

[1] Sistema de Asignación y Transferencia de Créditos Académicos

©TecNM 2025

integre diversas perspectivas en la solución de problemas complejos del ámbito tecnológico.
Intención didáctica
Como docente de Hacking Ético, la asignatura debe abordarse de forma progresiva, iniciando con fundamentos teóricos y avanzando hacia prácticas aplicadas en laboratorios y simulaciones. El enfoque debe ser práctico y basado en problemas, destacando la ética profesional en todo momento. Los contenidos deben equilibrar la teoría y la práctica, profundizando en la planificación de pruebas de penetración y el análisis de vulnerabilidades. Las actividades de los estudiantes, como simulaciones, estudios de caso, y la presentación de informes, fomentan competencias genéricas como el pensamiento crítico, la comunicación efectiva, la colaboración y el profesionalismo. El docente debe actuar como facilitador, guiando a los estudiantes en la aplicación práctica de los contenidos, promoviendo un entorno colaborativo y evaluando su progreso con retroalimentación constante.

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Tecnológico Nacional de México, campus Tuxtla Gutiérrez del 18 septiembre al 26 de octubre de 2024	Representantes de los Institutos Tecnológicos de: Tuxtla Gutiérrez, Tapachula y Frontera Comalapa. Jesús Carlos Sánchez Guzmán Ezequiel Cruz Wong Carlos Alberto López Escobar Brenda Guadalupe Pinto Vázquez	Foro Estatal Actualización Curricular para la Consolidación de Proyectos Estratégicos del TecNM en el Estado de Chiapas

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura

©TecNM 2025

El estudiante, al finalizar la asignatura “Hacking Ético” será capaz de planificar y ejecutar pruebas de penetración (pentesting) de manera ética, identificando y explotando vulnerabilidades en sistemas informáticos, redes, dispositivos móviles, IoT y entornos en la nube. Además, será competente en el análisis de resultados, aplicando técnicas de post-explotación y elaborando informes claros y precisos, comunicando los hallazgos y recomendaciones a audiencias técnicas y no técnicas para mejorar la seguridad de infraestructuras críticas en las organizaciones.

5. Competencias previas

- Identificar Vulnerabilidades y Controles de Seguridad
- Administrar y Proteger Redes Inalámbricas
- Aplicar Legislación y Ética en Ciberseguridad
- Implementar Técnicas de Criptografía

6. Temario

No.	Temas	Subtemas
1	Hacking ético, planificación y alcance del pentesting	1.1 Introducción al hacking ético y las pruebas de penetración 1.2 Comprensión del hacking ético y las pruebas de penetración 1.3 Exploración de las metodologías de pruebas de penetración 1.4 Creación de su propio laboratorio 1.5 Planificación y alcance de una evaluación de pruebas de penetración 1.6 Comparación y contraste de conceptos de gobernanza, riesgo y cumplimiento 1.7 Importancia del alcance y los requisitos organizacionales o del cliente 1.8 Mentalidad de hacker ético al mantener el profesionalismo y la integridad
2	Recopilación de información y análisis de vulnerabilidades	2.1 Realización de reconocimiento pasivo 2.2 Realización de reconocimiento activo 2.3 Comprender el arte de realizar análisis de vulnerabilidades 2.4 Comprender cómo analizar los resultados de los análisis de vulnerabilidades 2.5 Ataques de ingeniería social 2.6 Pretextos para un acercamiento y suplantación de identidad 2.7 Ataques de ingeniería social 2.8 Ataques físicos 2.9 Herramientas de ingeniería social 2.10 Métodos de influencia
3	Explotación	3.1 Explotación de redes cableadas e inalámbricas

©TecNM 2025

		3.1.1 Explotación de vulnerabilidades basadas en red 3.1.2 Explotación de vulnerabilidades inalámbricas 3.2 Explotación de vulnerabilidades basadas en aplicaciones 3.2.1 Descripción general de los ataques basados en aplicaciones web para profesionales de seguridad y el Top 10 de OWASP 3.2.2 Cómo crear su propio laboratorio de aplicaciones web 3.2.3 Comprensión de las fallas de lógica empresarial 3.2.4 Comprensión de las vulnerabilidades basadas en inyección 3.2.5 Explotación de vulnerabilidades basadas en autenticación 3.2.6 Explotación de vulnerabilidades basadas en autorización 3.2.7 Descripción de las vulnerabilidades de secuencias de comandos entre sitios (XSS) 3.2.8. Comprensión de los ataques de falsificación de solicitud entre sitios (CSRF/XSRF) y falsificación de solicitud del lado del servidor 3.2.9 Comprensión del secuestro de clics 3.2.10 Explotación de vulnerabilidades de inclusión de archivos 3.2.11 Explotación de prácticas de código inseguro
4	Seguridad en la nube, dispositivos móviles, IoT y técnicas de post-explotación	4.1 Seguridad en la nube, dispositivos móviles e IoT 4.2 Vectores de ataque y ejecución de ataques a las tecnologías en la nube 4.3 Ataques y vulnerabilidades comunes contra sistemas especializados 4.4 Ejecución de técnicas de post-explotación 4.5 Creación de un punto de apoyo y mantenimiento de la persistencia después de comprometer un sistema 4.6 Comprensión de cómo realizar movimientos laterales, evitar la detección y enumeración
5	Informes y comunicación	5.1 Informes y comunicación 5.2 Comparación y contraste de componentes importantes de informes escritos 5.3 Análisis de los hallazgos y recomendación de la solución adecuada dentro de un informe 5.4 Explicación de la importancia de la comunicación durante el proceso de prueba de penetración 5.5 Explicación de las actividades posteriores a la entrega del informe 5.6 Herramientas y análisis de código 5.6.1 Comprensión de los conceptos básicos de desarrollo de software y scripts 5.6.2 Comprensión de los diferentes casos de uso de las herramientas de pentesting y análisis del código de exploits

©TecNM 2025

7. Actividades de aprendizaje de los temas

1. Hacking ético, planificación y alcance del pentesting	
Competencias	Actividades de aprendizaje
Específica(s): asignatura Desarrolla la capacidad de planificar y definir el alcance de pruebas de penetración éticas aplicando metodologías estructuradas y considerando los requisitos organizacionales o del cliente, mientras mantiene el profesionalismo, la integridad y el cumplimiento de normas y regulaciones de seguridad. **Genéricas:** - Capacidad de análisis y síntesis - Comunicación oral y escrita en su propia lengua - Conocimiento de una segunda lengua - Habilidades de gestión de información (habilidad para buscar y analizar información proveniente de fuentes diversas) - Capacidad crítica y autocrítica - Trabajo en equipo - Compromiso ético - Habilidades de investigación - Búsqueda del logro	1. Lectura guiada sobre los conceptos fundamentales de hacking ético y pruebas de penetración 2. Discusión en clase sobre las diferentes metodologías de pruebas de penetración y su aplicación en escenarios reales 3. Taller práctico para la creación de un laboratorio virtual de pruebas de penetración, donde los estudiantes configuren redes y sistemas simulados. 4. Estudio de caso en el que los estudiantes planifiquen el alcance de una evaluación de pentesting para una organización ficticia, teniendo en cuenta los objetivos del cliente 5. Comparación y análisis de estudios sobre gobernanza, riesgo y cumplimiento en el contexto de ciberseguridad, destacando su importancia en el pentesting. 6. Debate ético donde los estudiantes discutan casos de pentesting reales, evaluando los dilemas éticos y profesionales enfrentados por los hackers éticos. 7. Simulación grupal donde los estudiantes asuman el rol de consultores de ciberseguridad y presenten un plan de alcance a una "empresa cliente", considerando los requisitos y limitaciones del negocio.
2. Recopilación de información y análisis de vulnerabilidades	
Competencias	Actividades de aprendizaje

©TecNM 2025

Específica(s): Realiza reconocimientos pasivos y activos, identificando y analizando vulnerabilidades utilizando herramientas y técnicas especializadas, y ejecutar ataques de ingeniería social en el contexto de pruebas de penetración manteniendo un enfoque ético, con el fin de identificar debilidades de seguridad en sistemas y usuarios. **Genéricas:** - Capacidad de análisis y síntesis - Comunicación oral y escrita en su propia lengua - Conocimiento de una segunda lengua - Habilidades de gestión de información (habilidad para buscar y analizar información proveniente de fuentes diversas) - Capacidad crítica y autocrítica - Trabajo en equipo - Compromiso ético - Habilidades de investigación - Búsqueda del logro	1. Lectura y análisis de artículos sobre técnicas de reconocimiento pasivo y activo, enfocándose en su aplicación en investigaciones forenses. 2. Taller práctico donde los estudiantes realicen análisis de vulnerabilidades utilizando herramientas específicas, aplicando los conceptos aprendidos. 3. Estudio de caso en el que se analicen los resultados de un análisis de vulnerabilidades real, identificando y discutiendo las implicaciones forenses. 4. Simulación de ataques de ingeniería social donde los estudiantes practiquen la identificación de pretextos y técnicas de suplantación de identidad, reflexionando sobre las consecuencias forenses. 5. Role-playing para experimentar y entender la dinámica de los ataques físicos y cómo pueden comprometer la seguridad de la información. 6. Demostración y uso de herramientas de ingeniería social en un entorno controlado para comprender su funcionamiento y aplicabilidad en investigaciones forenses. 7. Debate en clase sobre métodos de influencia y su papel en el contexto de la ingeniería social, analizando casos de éxito y fracaso 8. Proyecto final donde los estudiantes diseñen un plan de respuesta forense a un ataque simulado, integrando los conocimientos adquiridos sobre vulnerabilidades, ingeniería social y análisis de resultados.
3. Explotación	
Competencias	Actividades de aprendizaje

Específica(s): Desarrolla la capacidad de explotar vulnerabilidades en redes cableadas e inalámbricas, así como en aplicaciones web y empresariales, utilizando técnicas avanzadas como ataques de inyección, XSS, CSRF y explotación de fallas de autenticación y autorización, aplicando metodologías de hacking ético para identificar fallos críticos de seguridad y proponer soluciones que fortalezcan la infraestructura tecnológica. **Genéricas:** - Capacidad de análisis y síntesis - Comunicación oral y escrita en su propia lengua - Conocimiento de una segunda lengua - Habilidades de gestión de información (habilidad para buscar y analizar información proveniente de fuentes diversas) - Capacidad crítica y autocrítica - Trabajo en equipo - Compromiso ético - Habilidades de investigación - Búsqueda del logro	1. Lectura y análisis de artículos sobre la explotación de redes cableadas e inalámbricas, incluyendo ejemplos de vulnerabilidades comunes. 2. Taller práctico para la explotación de vulnerabilidades en redes, donde los estudiantes realicen pruebas de penetración simuladas en entornos controlados. 3. Desarrollo de un laboratorio de aplicaciones web donde los estudiantes configuren un entorno de prueba para Prácticar la explotación de vulnerabilidades. 4. Estudio de caso sobre el Top 10 de OWASP, analizando cada vulnerabilidad y discutiendo técnicas de explotación. 5. Simulaciones de ataque en las que los estudiantes practiquen la explotación de vulnerabilidades basadas en autenticación y autorización. 6. Demostración y análisis de ataques de inyección y XSS, permitiendo a los estudiantes experimentar y comprender su impacto en aplicaciones web. 7. Análisis de vulnerabilidades de CSRF/XSRF y su explotación en aplicaciones web, a través de ejercicios prácticos y estudios de caso. 8. Práctica sobre secuestro de clics donde los estudiantes aprendan a identificar y explotar esta técnica en entornos de prueba. 9. Revisión de prácticas de código inseguro, analizando ejemplos reales de código y proponiendo mejoras para mitigar vulnerabilidades.

©TecNM 2025

	10. Proyecto en el que los estudiantes diseñen y ejecuten un ataque controlado, documentando el proceso de explotación y presentando sus hallazgos y recomendaciones para mitigar riesgos.
4. Seguridad en la nube, dispositivos móviles, IoT y técnicas de post-explotación	
Competencias	Actividades de aprendizaje
Específica(s): Desarrolla la capacidad de identificar y explotar vulnerabilidades en entornos de nube, dispositivos móviles e IoT, ejecutando ataques y técnicas de post-explotación para establecer persistencia y realizar movimientos laterales en sistemas comprometidos, aplicando estrategias avanzadas de evasión y enumeración, con el fin de proteger y fortalecer infraestructuras tecnológicas críticas. **Genéricas:** - Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social. - Solución de problemas - Compromiso ético	1. Lectura y análisis de materiales sobre criptografía aplicada a la informática forense, discutiendo su importancia en la protección de datos y la integridad de la evidencia. 2. Taller práctico donde los estudiantes realicen una adquisición lógica de datos en dispositivos móviles y sistemas en la nube, utilizando herramientas forenses adecuadas. 3. Simulación de escenarios para la adquisición física de dispositivos, donde los estudiantes practiquen técnicas de recuperación de datos de forma segura y respetando la cadena de custodia. 4. Ejercicio práctico sobre adquisición directa e indirecta, permitiendo a los estudiantes aplicar diferentes métodos para recopilar evidencias digitales según el contexto de la investigación. 5. Demostración de herramientas de adquisición por hardware, donde los estudiantes aprendan a utilizar dispositivos forenses especializados para la recuperación de datos. 6. Estudio de caso sobre incidentes de seguridad en la nube y dispositivos IoT, analizando las técnicas de post-explotación utilizadas y las medidas de mitigación implementadas.

©TecNM 2025

	7. Discusión en grupo sobre los retos y mejores prácticas en la adquisición de datos en entornos de nube y dispositivos móviles, considerando aspectos legales y éticos. 8. Proyecto en el que los estudiantes diseñen un plan de adquisición de datos para un caso simulado, eligiendo las técnicas más adecuadas y justificando sus decisiones en función del contexto forense.
5. Informes y comunicación	
Competencias	Actividades de aprendizaje
Específica(s): Elabora informes claros y detallados sobre los hallazgos de pruebas de penetración, analizando vulnerabilidades y recomendando soluciones adecuadas, y comunicando de manera efectiva los resultados a diferentes audiencias, tanto técnicas como no técnicas, durante y después del proceso, utilizando herramientas especializadas y análisis de código para respaldar los hallazgos y garantizar la mejora continua de la seguridad. **Genéricas:** - Capacidad de análisis y síntesis - Comunicación oral y escrita en su propia lengua - Conocimiento de una segunda lengua - Habilidades de gestión de información (habilidad para buscar y analizar información proveniente de fuentes diversas) - Capacidad crítica y autocrítica - Trabajo en equipo - Compromiso ético - Habilidades de investigación - Búsqueda del logro	1. Lectura y análisis de ejemplos de informes de pruebas de penetración, destacando su estructura y componentes clave. 2. Taller de escritura donde los estudiantes redacten un informe de prueba de penetración simulado, incorporando los hallazgos, análisis y recomendaciones adecuadas. 3. Actividad de comparación y contraste de diferentes tipos de informes, identificando componentes importantes como resumen ejecutivo, metodología, hallazgos y recomendaciones. 4. Debate en clase sobre la importancia de la comunicación efectiva durante el proceso de prueba de penetración y la relación con los stakeholders. 5. Simulación de presentación de informes, donde los estudiantes presenten sus hallazgos a una audiencia ficticia (ej., directivos o técnicos), Prácticando la comunicación clara y efectiva. 6. Análisis de las actividades posteriores a la entrega del informe, discutiendo cómo

©TecNM 2025

	implementar las recomendaciones y la importancia del seguimiento. 7. Demostración y práctica en el uso de herramientas de análisis de código y pentesting, donde los estudiantes aplican conceptos básicos de desarrollo de software y scripts. 8. Estudio de caso sobre un informe de incidentes de seguridad, analizando cómo se presentan los hallazgos y qué mejoras se recomiendan. 9. Proyecto final donde los estudiantes elijan un caso práctico de pentesting, realicen la prueba, redacten el informe correspondiente y presenten sus resultados y recomendaciones a la clase.

8. Práctica(s)

Prácticas Tema1- Hacking ético, planificación y alcance del pentesting	
Práctica1: Investigación de carreras de PenTesting	En esta Práctica, completará los siguientes objetivos: • Realizar una búsqueda de empleos para un evaluador de penetración • Analizar los requisitos del puesto de evaluador de penetración • Descubra recursos para impulsar su carrera
Práctica2: Comparación de metodologías de PenTesting	En esta Práctica completarás los siguientes objetivos: • Comparar distintas metodologías de pentesting • Realizar investigaciones sobre metodologías de pentesting populares
Práctica3: Implementación de una máquina virtual (VM) Kali Linux preconstruida	En esta Práctica, completará los siguientes objetivos: • Parte 1: Implementación de una máquina virtual Kali Linux personalizada en una computadora con chip AMD o Intel • Parte 2: Implementación de una máquina virtual Kali Linux personalizada en una computadora MacOS basada en ARM M1/M2 • Parte 3: Explorando Linux
Práctica4: Investigación de Kali Linux	En esta Práctica, completará los siguientes objetivos: • Familiarícese con la GUI de Kali Linux. • Familiarícese con el shell de Kali Linux.

©TecNM 2025

Práctica5: Requisitos de cumplimiento y restricciones locales	En esta Práctica, completará los siguientes objetivos: • Investigue los servicios de pruebas de penetración proporcionados por consultores de seguridad para marcos de cumplimiento. • Realizar una búsqueda de empresas de pruebas de penetración.
Práctica6: Alcance y planificación previos al compromiso	Llegar a un acuerdo sobre las reglas de actuación que se aplican a una prueba de penetración o una auditoría de seguridad es el primer paso en cualquier relación con un cliente. Es importante dedicar tiempo a garantizar que tanto su empresa como el cliente comprendan claramente los términos y el alcance de la prueba. • Cree un documento de alcance y plan de pruebas de penetración que aborde los requisitos para los servicios de pruebas de penetración que se recopilaron del cliente. • Determinar las reglas de los elementos del compromiso.
Práctica7: Creación de un acuerdo de PenTesting	En esta Práctica, completará los siguientes objetivos: • Complete un acuerdo de prueba de penetración simple.
Práctica8: Código de conducta personal	En esta Práctica, completará los siguientes objetivos: • Enfoques de investigación para la toma de decisiones éticas • Código de ética de la investigación • Desarrolle su propio código personal de conducta ética

Practicas Tema 2 - Recopilación de información y análisis de vulnerabilidades	
Práctica9: Uso de herramientas OSINT	En esta práctica, explorará varias herramientas OSINT que los pentesters suelen utilizar. • Examinar los recursos OSINT. • Utilice SpiderFoot • Investigar Recon-ng • Encuentra archivos interesantes con Recon-ng
Práctica10: - Búsquedas DNS	En esta práctica, explorará herramientas comunes que se utilizan para recopilar información sobre un objetivo a través del Sistema de nombres de dominio (DNS). • Utilice **nslookup** para obtener información de dominio y dirección IP. • Utilice el comando **whois** para encontrar información de registro adicional.

©TecNM 2025

	• Compare la salida de las herramientas Nslookup y Dig. • Realizar búsquedas DNS inversas.
Práctica11: Búsquedas Shodan	En esta práctica, completará los siguientes objetivos: • Cree una cuenta de usuario de Shodan y regístrese para obtener una clave API • Utilice el sitio web de Shodan para buscar dispositivos IoT vulnerables • Utilice Shodan desde la CLI para realizar una búsqueda
Práctica12: Laboratorio - Enumeración con Nmap	En esta práctica, completará los siguientes objetivos: • Investigar Nmap • Realizar exploraciones básicas de Nmap
Práctica13: - Creación de paquetes con Scapy	En esta práctica, utilizará Scapy, una herramienta de manipulación de paquetes basada en Python, para crear paquetes personalizados. Estos paquetes personalizados se utilizarán para realizar un reconocimiento en un sistema de destino. Parte 1: Investigar la herramienta Scapy. Parte 2: Usar Scapy para rastrear el tráfico de la red. Parte 3: Crear y enviar un paquete ICMP. Parte 4: Crear y enviar paquetes TCP SYN.
Práctica14: - Detección de redes con Wireshark	En esta práctica, utilizará la utilidad Linux tcpdump para capturar y guardar el tráfico de red. Luego, utilizará Wireshark para investigar la captura de tráfico. • Prepare el host para capturar el tráfico de red. • Capture y guarde el tráfico de red. • Vea y analice la captura de paquetes.
Práctica15: - Escaneos de vulnerabilidades con herramientas Kali	En esta práctica, explorará las herramientas de escaneo de vulnerabilidades de red y las usará para realizar un escaneo de vulnerabilidades en un host de destino. • Realice escaneos de red con Nmap. • Utilice Greenbone Vulnerability Management para realizar un escaneo de vulnerabilidades.

©TecNM 2025

Práctica16: - Investigar fuentes de información de vulnerabilidades	En esta práctica, utilizará múltiples fuentes útiles para investigar más a fondo las vulnerabilidades. • Parte 1: Investigar vulnerabilidades y exposiciones comunes (CVE) • Parte 2: Explorar las enumeraciones de debilidades comunes (CWE) • Parte 3: Investigar los recursos de vulnerabilidad del Instituto Nacional de Estándares y Tecnología (NIST) • Parte 4: Investigación de vulnerabilidades en el Sistema de puntuación de vulnerabilidades común (CVSS)
Práctica17: - Explorar el kit de herramientas de ingeniería social	En esta práctica, completará los siguientes objetivos: • Parte 1: Lanzamiento de SET y exploración del conjunto de herramientas • Parte 2: Clonación de un sitio web para obtener credenciales de usuario • Parte 3: Captura y visualización de credenciales de usuario
Práctica18: - Usar el marco de explotación del navegador (BeEF)	En esta práctica, completará los siguientes objetivos: • Cargar el entorno GUI de BeEF • Conectar el navegador local para simular un ataque del lado del cliente • Investigar las capacidades de explotación de BeEF

Practicas Tema3 - Explotación	
Práctica19: - Escaneo de vulnerabilidades SMB con enum4linux	En esta práctica, completará los siguientes objetivos: • Inicie enum4linux y explore sus capacidades. • Identificar computadoras con servicios SMB ejecutándose. • Utilice enum4linux para enumerar usuarios y recursos compartidos de archivos de red. • Utilice smbclient para transferir archivos entre sistemas.
Práctica20: - Ataques en ruta con Ettercap	En esta práctica, completará los siguientes objetivos: • Parte 1: Lanzamiento de Ettercap y exploración de sus capacidades • Parte 2: Realizar el ataque en ruta (MITM) • Parte 3: Utilice Wireshark para observar el ataque de suplantación de ARP
Práctica21: - Escaneo de vulnerabilidades web	En esta práctica, completará los siguientes objetivos: Parte 1: Iniciar Nikto y realizar un análisis básico Parte 2: Usar Nikto para analizar varios servidores web Parte 3: Investigar vulnerabilidades de sitios web Parte 4: Exportar resultados de Nikto a un archivo

©TecNM 2025

Práctica22: - Usar el escáner de vulnerabilidades GVM	En esta práctica, completará los siguientes objetivos: Parte 1: Analizar un host en busca de vulnerabilidades Parte 2: Aprovechar una vulnerabilidad encontrada por GVM Nota: El análisis llevará algo de tiempo y puede tardar más de 30 minutos en completarse.
Práctica23: - Ataques de inyección	En esta práctica, completará los siguientes objetivos: Parte 1: Explotar una vulnerabilidad de inyección SQL en DVWA Parte 2: Investigar la mitigación de la inyección SQL
Práctica24: - Usar herramientas de contraseñas	En esta práctica, completará los siguientes objetivos: Parte 1: Investigar ataques de contraseñas Parte 2: Descifrar hashes con ataques de diccionario Hashcat Parte 3: Descifrar hashes con John the Ripper mediante ataques de diccionario y de fuerza bruta Parte 4: Descifrar hashes con RainbowCrack y Rainbow Tables
Práctica25: - Cross Site Creación de scripts	En esta práctica, completará los siguientes objetivos: Parte 1: Realizar exploits de secuencias de comandos de sitios cruzados reflexivos Parte 2: Realizar exploits de secuencias de comandos de sitios cruzados almacenados
Práctica26: - Usar la guía de pruebas de seguridad web OWASP	En esta práctica, completará los siguientes objetivos: Parte 1: Investigar el WSTG Parte 2: Analizar un sitio web e investigar referencias de vulnerabilidades

Tema5-Informes y comunicación	
Práctica27: Exploración de informes de pruebas de penetración	En esta práctica, completará los siguientes objetivos: Parte 1: Revisar los informes de pruebas de penetración disponibles públicamente Parte 2: Desarrollar su propio formato de informe Parte 3: Crear su informe de pruebas de penetración
Práctica28: Recomendar medidas correctivas en función de los hallazgos	En esta práctica, completará los siguientes objetivos: • Identificar y priorizar las vulnerabilidades encontradas en el servidor DVWA. • Investigar y recomendar estrategias de mitigación.

©TecNM 2025

Práctica29: Análisis de código de explotación	En esta práctica, interpretará algunos scripts y comandos que se ingresan en el shell. Esto le ayudará a desarrollar su conocimiento sobre el software y las herramientas de pruebas de penetración. Es importante que pueda interpretar los comandos y scripts que encuentre como parte de nuestros acuerdos de pruebas de penetración con nuestros clientes.
Práctica30: Análisis de código de automatización	En esta práctica, completará los siguientes objetivos: • Parte 1: Escriba un script Bash para automatizar un escaneo de Nmap y almacenar los resultados. • Parte 2: Diferenciar entre scripts escritos en Bash, Python, Ruby y PowerShell.

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.

©TecNM 2025

©TecNM 2025

10. Evaluación por competencias

Son las técnicas, instrumentos y herramientas sugeridas para constatar los desempeños académicos de las actividades de aprendizaje.

- Análisis de casos.
- Análisis y solución de problemas.
- Entrevistas a expertos
- Solución de problemas realizados en forma individual o en equipo.
- Discusiones y debates en equipos.
- Paneles de presentaciones de temas.

- Reportes de proyectos, investigaciones, trabajos, etc.
- Solución de cuestionarios
- Ensayos y/o trabajos de diverso tipo
- Elaboración de controles de lectura
- Simulaciones y/o demostraciones.
- Resúmenes
- Juegos de roles.
- Esquemas gráficos (mapas conceptuales, mapas mentales, mapas procedimentales, cuadros sinópticos, diagramas de flujo, etc.)
- Fichas de observación para prácticas
- Investigaciones documentales o de campo.

11. Fuentes de información

1. Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems* (3rd ed.). Wiley.
- Este libro aborda conceptos fundamentales de seguridad en redes y sistemas distribuidos, con un enfoque en el análisis de vulnerabilidades y pruebas de penetración.

2. Kim, D., & Solomon, M. G. (2021). *Fundamentals of Information Systems Security* (4th ed.). Jones & Bartlett Learning.
- Una fuente esencial para comprender los conceptos básicos de ciberseguridad, incluyendo pruebas de penetración y análisis de vulnerabilidades.

3. Skoudis, E., & Liston, T. (2017). *Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses* (2nd ed.). Pearson IT Certification.
- Este recurso guía a los estudiantes en la práctica del hacking ético, cubriendo técnicas de ataque y defensa en entornos simulados.

4. Erickson, J. (2018). *Hacking: The Art of Exploitation* (2nd ed.). No Starch Press.
- Un libro altamente técnico que profundiza en la explotación de vulnerabilidades, con ejemplos prácticos y ejercicios para reforzar el aprendizaje de técnicas de hacking.

5. Simpson, W. R. (2020). *Ethical Hacking and Penetration Testing Guide*. Auerbach Publications.

©TecNM 2025

- Este texto cubre tanto los aspectos éticos como las técnicas prácticas para llevar a cabo pruebas de penetración en diferentes entornos, incluyendo redes y sistemas empresariales.

6. OWASP Foundation. (2023). *OWASP Top Ten*. https://owasp.org/www-project-top-ten/
- El informe OWASP Top Ten es un recurso fundamental para la comprensión de las vulnerabilidades más críticas en aplicaciones web y cómo mitigarlas, proporcionando ejemplos y prácticas recomendadas.

7. McClure, S., Shah, S., & Shah, S. (2018). *Web Hacking 101: How to Hack Legally and Earn Thousands of Dollars* (3rd ed.). O'Reilly Media.
- Este libro se enfoca en las pruebas de penetración de aplicaciones web, ofreciendo una perspectiva detallada de cómo identificar y explotar vulnerabilidades con un enfoque ético.

8. EC-Council. (2021). *Certified Ethical Hacker (CEH) v11: Study Guide & Lab Manual*. EC-Council Press.
- Un recurso indispensable para la certificación CEH, cubriendo todas las técnicas y herramientas que los estudiantes necesitan dominar para convertirse en expertos en hacking ético.

9. Mitnick, K. D., & Simon, W. L. (2017). *The Art of Deception: Controlling the Human Element of Security*. Wiley.
- Este libro analiza la ingeniería social como una herramienta clave en las pruebas de penetración, explicando cómo los atacantes explotan las debilidades humanas.

10. Grimes, R. A. (2019). *Cryptography Apocalypse: Preparing for the Day When Quantum Computing Breaks Today's Crypto*. Wiley.
- Un enfoque en la seguridad de datos y criptografía, cubriendo vulnerabilidades futuras en un mundo donde la computación cuántica será una realidad.