1. Datos Generales de la asignatura

Nombre de la asignatura:	Tópicos de Ciberseguridad
Clave de la asignatura:	SCD-2004
SATCA[1]:	*2-3-5*
Carrera:	Ingeniería en Sistemas Computacionales

2. Presentación

Caracterización de la asignatura

Esta asignatura aporta al perfil del Ingeniero en Sistemas Computacionales la capacidad de utilizar tecnologías y herramientas actuales y emergentes acordes a las necesidades del entorno. Además de las siguientes capacidades:

- Implementa aplicaciones computacionales para solucionar problemas de diversos contextos, integrando diferentes tecnologías, plataformas o dispositivos.
- Diseña, desarrolla y aplica modelos computacionales para solucionar problemas, mediante la selección y uso de herramientas matemáticas.
- Evalúa tecnologías de hardware para soportar aplicaciones de manera efectiva.

Su importancia radica en que permitirá al estudiante utilizar herramientas digitales de seguridad que puedan contribuir a enfrentar de una mejor manera los ciberataques y vulnerabilidades, así como poner controles que ayuden a mitigar el riesgo en una organización.

La asignatura permite reconocer diversos escenarios de pruebas de seguridad disponibles en el mercado, para el reforzamiento de la protección de la información en el contexto de administración de sistemas a través de las metodologías relevantes de la seguridad para el reconocimiento de tecnologías de cómputo de manera pasiva y activa.

Esta asignatura requiere de los conocimientos previos obtenidos en las asignaturas de Ingeniería de Software, Sistemas operativos II, Lenguajes de Interfaz y Seguridad en la infraestructura tecnológica.

[1] Sistema de Asignación y Transferencia de Créditos Académicos

Intención didáctica

La asignatura está integrada por cinco temas, dentro de los cuales el alumno deberá realizar investigación y desarrollo de prácticas.

En las actividades sugeridas se propone la formalización del aprendizaje y utilización de herramientas digitales que contribuyan a la seguridad en dispositivos y aplicaciones.

Se organiza el temario como a continuación se describe.

En el primer tema, se refiere a la conexión segura a servidores en la nube, en el cual el estudiante realizará las configuraciones necesarias lograr este fin. También se abordarán las principales vulnerabilidades que afectan a las aplicaciones en la nube, en la cual el estudiante tendrá la oportunidad de codificar sus soluciones propuestas con el fin de mitigar estos a ataques. mediante el análisis de archivos logs el estudiante podrá detectar intentos de accesos fallidos o posibles ataques de la aplicación.

En el segundo tema, se abordarán los elementos del proceso de ingeniería inversa, comenzando con una introducción donde se sintetizan los conceptos básicos. Posteriormente se aprenderán las metodologías específicas, además de las principales herramientas de cracking. El estudiante analizará diferentes tipos de binarios, con el objeto de decidir qué métodos y codificación de crackeo son los más adecuados para un problema en específico.

En el tercer tema se estudiará desde los conceptos básicos del malware, definición, clasificación y propagación. Pasando por el impacto económico del mercado negro del malware y crimeware, donde se le orientará en las precauciones necesarias en el momento de investigar estos tipos de subtemas. Se revisará brevemente las etapas de desarrollo de algunos tipos de malware. Así como la existencia del mercado gris, donde si bien lo que se compra es legal, no lo es moralmente. Se abordará la postura ética desde la óptica de la ingeniería acerca de estos temas. Para finalizar con la implementación en equipos de un laboratorio de análisis de malware donde se el estudiante podrá analizar y estudiar el comportamiento de varias muestras de malware.

En el cuarto tema, conocerá las configuraciones necesarias para protegerse de posibles ataques físicos o de hardware en servidores, mediante la instalación y configuración del sistema operativo como servicios, protocolos de red y opciones de acceso remoto. Así mismo se realizará un mantenimiento correcto y revisión de los sistemas operativos instalados.

En el quinto tema, se conocerán las diferentes técnicas de pentesting realizando un entorno controlado de pruebas. En dicho entorno se analizarán diversas vulnerabilidades y sus principales vectores de ataque. Del mismo modo se evaluarán algunos de los ataques más comunes a contraseñas. En el subtema de post explotación, se identificarán aquellos agujeros de seguridad encontrados y se realizará la investigación del ¿Por qué? y los ¿cómo? de dichos fallos de seguridad. Para finalizar en el los subtemas de “hacking

de servidores y aplicaciones web" y "ataques de denegación de servicio". Donde tras evaluar un sistema existe se gestionará en una propuesta de un programa de seguridad y aplicar las diferentes pruebas mediante una metodología.

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Tecnológico Nacional de México campus San Juan del Río. Junio del 2020.	M.G.T.I. Cuevas Carrillo Elsa Lic. Flores Rosales José Amisadai Ing. Medina Varela Wilfrido M.G.T.I. Rodríguez Nieto Elvia Ing. Sánchez Orduña Govani Gregorio Ing. Valdes Arteaga Leonardo	Reunión de Academia Carrera de Ingeniería en Sistemas Computacionales para el diseño de Módulo de Especialidad y elaboración de programas de estudio.

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
Aplicar técnicas y herramientas de ciberseguridad como una medida para mitigar los riesgos y vulnerabilidades informáticas, y que a su vez contribuyan al aseguramiento e integridad de la información y tecnologías de la organización.

5. Competencias previas

Desarrolla soluciones de software, considerando la metodología y herramientas para la elaboración de un proyecto aplicativo en diferentes escenarios. Conoce, identifica, selecciona y administra diferentes sistemas operativos con el fin de resolver problemáticas reales, así como aplicar procedimientos de interoperabilidad entre diferentes sistemas operativos. Desarrollar software para establecer la interfaz hombre-máquina y máquina-máquina. Identificar las diferentes vulnerabilidades en los sistemas de información y seguridad perimetral evaluando servicios y mecanismos necesarios para implementar una estrategia en la seguridad de la infraestructura tecnológica, de acuerdo a los requisitos de la organización.

6. Temario

No.	Temas	Subtemas
1	Desarrollo de aplicaciones seguras en la nube	1.1 Introducción a la seguridad en la nube. 1.1.1. Conexión segura a servidores 1.2 Seguridad en el desarrollo de software 1.2.1 Vulnerabilidades comunes en el software 1.2.2 Archivos logs
2	Ingeniería inversa	2.1 Introducción a la Ingeniería Inversa 2.2 Metodología 2.3 Herramientas de Ingeniería Inversa (Cracking) 2.3.1 Desensamblador. 2.3.2 Depuradores. 2.3.3 Decompiladores. 2.3.4 Monitoreo. 2.4 Métodos y codificación de Crackeo
3	Análisis de malware	3.1 Conceptos Fundamentales. 3.2 Clasificación del Malware. 3.3 Crimeware. 3.3.1 Crimeware y Mercado del Malware. 3.3.2 Desarrollo de malware. 3.3.3 Línea Gris (Botnets legales). 3.4 Laboratorio de Análisis de malware. 3.4.1 Metodologias de Analisis. 3.4.2 Obtención de muestras 3.4.3 Tipos de Análisis 3.4.4 Identificación de registros y persistencia. 3.4.5 Reporte Técnico.
4	Hardening de servidores	4.1 Protección en sistemas Windows 4.1.1 Políticas de cuenta 4.1.2 Políticas locales y de grupos 4.1.3 Event log 4.1.4 Servicios del sistema 4.1.5 Registros 4.1.6 Sistema de archivos 4.1.7 Firewall 4.2 Protección en sistemas GNU/Linux Unix 4.2.1 Configuración inicial 4.2.2 Servicios 4.2.3 Configuración de red

		4.2.4 Logging 4.2.5 Mantenimiento del sistema
5	Herramientas de Pentesting	5.1. Introducción y entorno de pruebas 5.2 Ataque de las contraseñas 5.3 Análisis de las vulnerabilidades 5.4 Post Explotación 5.5 Hacking Servidores y Aplicaciones Web 5.6 Ataques de denegación de servicio

7. Actividades de aprendizaje de los temas

1. Desarrollo de aplicaciones segura en nube	
Competencias	Actividades de aprendizaje
Específica(s): Implementa las configuraciones necesarias para establecer una conexión segura sobre SSL y SSH con el servidor. Realiza un código seguro para la mitigación de las vulnerabilidades más comunes. Identifica accesos fallidos o no autorizados mediante el análisis de archivos log. Genéricas: ● Capacidad de análisis y síntesis. ● Capacidad de organizar y planificar. ● Habilidad para buscar y analizar información proveniente de fuentes diversas ● Capacidad de aplicar los conocimientos. ● Solución de problemas	● Realiza las configuraciones necesarias para realizar conexiones seguras al servidor de mediante Certificados SSL y SSH ● Evalúa y mitigar las principales vulnerabilidades en el software mediante el desarrollo de código seguro, validando las vulnerabilidades más comunes (OWASP). ● Desarrollar código para el análisis de archivos log, en busca de errores e intentos fallidos/no autorizados u otra información que pudiera ser una señal en contra de la seguridad del sistema e información.
2. Ingeniería inversa	
Competencias	Actividades de aprendizaje
Específica(s): Aplicar métodos y técnicas a un producto de software para identificar características y comportamiento del mismo.	● A partir de un archivo sin extensión, identificar su formato. ● Obtener el código fuente a partir de un archivo binario. ● Auditar un software vulnerable desarrollado por el estudiante para

Genéricas: ● Capacidad de análisis y síntesis. ● Solución de problemas. ● Habilidad para trabajar en forma autónoma. ● Capacidad para tomar decisiones. ● Capacidad para aplicar conocimientos en la práctica.	identificar las características de dicha vulnerabilidad. (Se sugiere stackover flow, Inyección o XSS)
3. Análisis de malware	
Competencias	Actividades de aprendizaje
Específica(s): ● Implementa un laboratorio de análisis de malware para comprender y estudiar muestras de malware. ● Desarrollar técnicas efectivas de mitigación y prevención de ataques a partir de muestras estudiadas. Genéricas: ● Capacidad de análisis y síntesis. ● Compromiso ético ● Capacidad de trabajo en equipo ● Capacidad para tomar decisiones. ● Habilidades para buscar, procesar y analizar información procedente de fuentes diversas	● Realiza una Infografía Tipos de Malware. ● Desarrolla un software no dañino que ejemplifica la propagación de un malware. ● Implementa un laboratorio de análisis de malware dinámico o estático. ● Realiza una evaluación del ataque o comportamiento de un malware. ● Elaboración de un Reporte técnico de daños.
4. Hardening de servidores	
Competencias	Actividades de aprendizaje
Específica(s): Aplicar las mejores prácticas para realizar una configuración endurecida, una instalación segura, un adecuado manejo de usuarios y logs y un, aseguramiento de servicios. Genéricas: ● Capacidad de aplicar conocimientos en la práctica ● Habilidades de investigación	● Buscar sobre las actividades propias de un proceso de hardening ● Instalar Windows Server 2016/2019 ● Aplicar las mejores prácticas que indique el facilitador ● Instalar Ubuntu Server/CentOS/Debian ● Aplicar las mejores prácticas que indique el facilitador

● Capacidad de aprender ● Capacidad de adaptarse a nuevas situaciones ● Búsqueda del logro	
5. Herramientas de Pentesting	
Competencias	Actividades de aprendizaje
Específica(s): Conocer las técnicas de pos-explotación y las tareas que puede realizar un pentester para elevar privilegios, buscar persistencia o eliminar el rastro. Genéricas: ● Capacidad de análisis y síntesis. ● Habilidades de gestión de información (habilidad para buscar y analizar información proveniente de fuentes diversas). ● Habilidades interpersonales. ● Habilidades de investigación. ● Trabajo en equipo. ● Capacidad de aplicar los conocimientos a la práctica.	● Realizar una investigación de las fases y al menos tres herramientas de pruebas y plasma sus resultados en un cuadro comparativo. ● Aplicar en un caso de estudio las teclas técnicas y herramientas para perpetrar ataques a las credenciales. ● Aplicar en un caso de estudio como se identifican y catalogan las vulnerabilidades de software. ● Aplicar en un caso de estudio como la herramienta metasploit ayuda al pentester en la labor de explotación de vulnerabilidades. ● Aplicar a un caso de estudio las técnicas de pos-explotación y las tareas que puede realizar en pentester para elevar privilegios, buscar persistencia o eliminar el rastro. ● Aplicar a un caso de estudio el Hacking Servidores y Aplicaciones Web ● Aplicar a un caso de estudio ataques de denegación de servicio ● Gestionar en una organización la propuesta de un programa de seguridad para aplicar las diferentes pruebas mediante una metodología.

8. Práctica(s)

1. Crear herramientas propias para la identificación de archivos binarios sin extensión.
2. Generación de certificados para la conexión segura.
3. Desarrollar un pequeño software que simule un malware, específicamente un joke (malware inofensivo), cuyo único propósito es ser una prueba de concepto del peligro de un malware.
4. Desarrollar un laboratorio de análisis de malware, con máquinas virtuales y herramientas opensource, donde se pueda estudiar las varias muestras controladas de malware.
5. Desarrollo e implementación práctica de un pentest mediante el uso de las herramientas y técnicas más conocidas para la consecución de cada fase.

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

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

Para evaluar las actividades de aprendizaje se recomienda solicitar: reportes de prácticas, estudios de casos, exposiciones en clase, reportes de visitas y portafolio de evidencias.

Para verificar el nivel del logro de las competencias del estudiante se recomienda utilizar: listas de cotejo, matrices de valoración, rúbricas, guías de observación, coevaluación y autoevaluación.

11. Fuentes de información

- Center for Internet Security. (2020). Cibersecurity Best Practices. USA: CIS. Recuperado de: https://www.cisecurity.org/cybersecurity-best-practices/.
- Weidman, G. (2014) Penetration Testing: A Hands-On Introduction to Hacking, San Francisco. No Starch Press, Inc.
- Faircloth, J. (2011). Penetration Tester's Open Source Toolkit, 3rd Edition, Waltham Syngress.
- Ligh, M., Adair, S., Hartstein, B., & Richard, M. (2010). Malware Analyst's Cookbook and DVD. John Wiley & Sons Inc.
- González, P., Sánchez, G. & Soriano de la Cámara, J.M. (2015). Pentesting con Kali 2.0, Mostoles: 0xWORD Computing S.L.
- Engebretson, P. (2013). The Basics of Hacking and Penetration Testing, 2nd Edition, Waltham: Syngress.
- Gonzalez, P.(2014). Ethical Hacking: teoría y práctica para la realización de un pentesting, Móstoles:0xWord Computing.
- Sikorski, M., Honig, A.(2012). Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. No Starch Press.
- Dang, B., Gazet, A., Bachaalany, E., & Josse, S. (2014). Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation.
- Yurichev, D. (2013-2019). Reverse Engineering for Beginners (Understanding Assembly Languaje).
- The Offensive Security Team, «Understanding Payloads in Metasploit,» 28 04 2016. [En línea]. Available: https://www.offensive-security.com/metasploit-unleashed/payloads/. [Último acceso: 2905 2016].
- Wilhelm, T. (2013). Professional Penetration Testing, 2nd Edition, Waltham: Syngress.

- «The Penetration Testing Execution Standard,» 16 08 2014. [En línea]. Available: http://www.pentest-standard.org/. [Último acceso: 20 02 2016].