1. Datos Generales de la asignatura

Nombre de la asignatura:	Análisis de vulnerabilidades II
Clave de la asignatura:	CSB-2403
SATCA[1]:	1 – 4 – 5
Carrera:	Ingeniería en Informática

2. Presentación

Caracterización de la asignatura
Esta asignatura aporta al perfil del egresado los conocimientos científicos y tecnológicos en la solución de problemas en el área informática con un enfoque interdisciplinario. También aplica normas, marcos de referencia y estándares de calidad y seguridad vigentes en el ámbito del desarrollo y gestión de tecnologías y sistemas de información. Así como también realizar actividades de auditoría y consultoría relacionadas con la función informática. Esta materia le sucede a la asignatura de Análisis de Vulnerabilidades 1, estudia cómo explotar las vulnerabilidades de un sistema informático para comprometer dicho sistema. Se enfoca en técnicas que permitirán desde encontrar puertos abiertos, hasta desarrollar código propio que aproveche una vulnerabilidad de buffer overflow y permita tomar control total del equipo objetivo. Así como también poder documentar de manera profesional los resultados del análisis de vulnerabilidades.
Intención didáctica
La asignatura se encuentra organizada en cuatro temas. En el primer tema se estudian las bases de los ataques de Cross-Site Scripting (XSS) que son un tipo de inyección donde los atacantes explotan la confianza que un usuario tiene en un sitio en particular. En el tema dos se estudian diferentes tipos de exploits, que son programas o códigos que se aprovechan de un agujero de seguridad (vulnerabilidad) en una aplicación o sistema, de forma que un atacante podría usar para provocar un comportamiento no intencionado o imprevisto en una aplicación, o en cualquier dispositivo electrónico.

[1] Sistema de Asignación y Transferencia de Créditos Académicos

El tercer tema es la siguiente fase a la explotación de un sistema, explora el ¿qué hacer después de conseguir acceso a un sistema informático? por ejemplo, el escalamiento de privilegios, transferencia de archivos y limpieza de huellas y rastros.

El tema cuatro concluye proporcionando el conocimiento para la documentación y la generación de reportes con las que concluyen las pruebas de penetración y suelen reflejar el trabajo completo por parte de quien lleva a cabo las pruebas de penetración o vulnerabilidad.

Los contenidos se abordarán de manera secuencial como los marca el programa, buscando la aplicación del conocimiento en el mundo real con un enfoque basado en actividades que promuevan en el estudiante el desarrollo de sus habilidades para trabajar de manera práctica.

La extensión y profundidad de los temas es suficiente para garantizar que el estudiante logre las competencias señaladas oportunamente. Por otro lado, el estudiante deberá comprometerse a trabajar permanentemente en el análisis y resolución de ejercicios y problemas a fin de que logre dichas competencias antes de concluir la materia.

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Revisión del 26 al 30 de abril del 2021 por parte del Tecnológico Nacional de México Campus Lerdo.	Representantes de los Institutos Tecnológicos Superiores de: Instituto Tecnológico Superior de Lerdo.	Reunión para el Análisis y Diseño por competencias de la Especialidad de "*Ciberseguridad*".

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
● Emplea el ciclo de vida de una prueba de penetración. ● Entiende lo que hace un exploit y cómo puede éste, ser modificado para adaptarse a un objetivo específico. ● Escala privilegios en sistemas Windows y Linux ● Aplica métodos de transferencia de archivos, limpieza de huellas y rastros. ● Realiza documentación y reportes con las que concluyen las pruebas de penetración.

5. Competencias previas

- Se recomiendan las competencias desarrolladas y adquiridas en las asignaturas de Análisis de vulnerabilidades 1 y Gestión de amenazas.

● Habilidades de gestión de información, en la búsqueda y análisis de información de diferentes fuentes. ● Habilidades cognitivas de abstracción, análisis, síntesis y reflexión. ● Capacidad de pensamiento lógico, analítico y crítico.

6. **Temario**

No.	Temas	Subtemas
1	Ataque de aplicaciones Web	1.1 Cross-site scripting 1.2 Inyección SQL 1.3 Inclusión Local y remota de archivos y navegación de directorios.
2	Explotación	2.1 Exploits públicos. 2.2 Buffer overflow. 2.3 Evasión de antivirus. 2.4 Ataques de contraseñas.
3	Post explotación	3.1 Teoría del escalamiento de privilegios. 3.2 Escalamiento en Windows. 3.3 Escalamiento en Linux. 3.4 Exploits disruptivos. 3.5 Métodos de transferencia de archivos 3.6 Creación de túneles con proxychains. 3.7 Limpieza de huellas y rastros.
4	Reportes y Documentación	4.1 Documentación de pruebas. 4.2 Documentando con Metasploit. 4.3 Reporte ejecutivo. 4.4 Reporte técnico.

7. Actividades de aprendizaje de los temas

Ataque de aplicaciones Web	
Competencias	Actividades de aprendizaje
Específica(s): ● Comprende cómo es un ataque a las aplicaciones web. ● Realiza ataques de secuencia de comandos en sitios cruzados. Genéricas:	● Identificar Cross-site scripting. ● Crear scripts para robar cookies de autenticación. ● Crear inyección SQL en aplicaciones web. ● Realizar inclusión tanto local como remota de archivos, y navegación de directorios.

● Capacidad de abstracción, análisis y síntesis. ● Capacidad de comunicación oral y escrita. ● Habilidades para buscar, procesar y analizar información procedente de fuentes diversas. ● Compromiso con la calidad.	
Explotación	
Competencias	Actividades de aprendizaje
Específica(s): ● Entiende lo que hace un exploit y cómo puede éste, ser modificado para adaptarse a un objetivo específico. ● Utiliza exploit públicos y aprovecha un agujero de seguridad. Genéricas: ● Capacidad de abstracción, análisis y síntesis. ● Capacidad de comunicación oral y escrita. ● Habilidades para buscar, procesar y analizar información procedente de fuentes diversas. ● Compromiso con la calidad.	● Utilizar exploit públicos. ● Utilizar la herramienta de Metasploit MSFVVenom para generar shellcodes utilizando diferentes cargas útiles disponibles en el framework. ● Ejecutar código en un equipo tomando como ventaja el buffer overflow. ● Recrear el exploit sobre el software SLMail5. ● Efectuar evasión de antivirus. ● Ejecutar ataques de contraseñas.
Post explotación	
Competencias	Actividades de aprendizaje
Específica(s): ● Realiza escalamiento de privilegios en diferentes sistemas operativos. ● Ejecuta transferencia de archivos. ● Realiza limpieza de huellas y rastros. Genéricas: ● Capacidad de abstracción, análisis y síntesis. ● Capacidad de comunicación oral y escrita. ● Habilidades para buscar, procesar y analizar información procedente de fuentes diversas. ● Compromiso con la calidad.	● Ejecutar escalamiento de privilegios en Windows. ● Ejecutar escalamiento de privilegios en Windows. ● Investigar la vulnerabilidad de seguridad informática para el kernel de Linux que afectó a todos los sistemas operativos basados en Linux, incluidos los dispositivos Android, que usaban versiones anteriores del kernel de Linux creadas antes de 2018. ● Realizar transferencia de archivos después de vulnerar con exploits. ● Crear túneles con proxychains. ● Exponer como se hace limpieza de huellas y rastros.
Reportes y Documentación	

Competencias	Actividades de aprendizaje
Específica(s): Crea la documentación para poder concluir las pruebas de penetración. Crea los reportes con las que concluyen las pruebas de penetración. Genéricas: ● Capacidad de abstracción, análisis y síntesis. ● Capacidad de comunicación oral y escrita. ● Habilidades para buscar, procesar y analizar información procedente de fuentes diversas. ● Compromiso con la calidad.	● Realizar la documentación necesaria para poder concluir las pruebas de penetración. ● Utilizar Metasploit para documentar. ● Construir el reporte ejecutivo con el que se concluyen las pruebas de penetración. ● Construir el reporte técnico con el que concluyen las pruebas de penetración.

8. Práctica(s)

- Realizar ataques de Cross-Site Scripting (XSS).
- Realizar inyección SQL.
- Realizar inclusión local y remota de archivos, y navegación de directorios.
- Crear scripts para sustraer cookies de autenticación.
- Utilizar exploit públicos.
- Utilizar herramientas como MSFVenom
- Realizar prácticas de desbordamiento de memoria (buffer overflow)
- Realizar exploit sobre el software SLMail 5
- Realizar evasión de antivirus.
- Realizar ataques de contraseña.
- Escalar privilegios en Windows.
- Escalar privilegios en Linux.
- Crear exploits disruptivos (DirtyCow)
- Crear túneles con Proxychains.
- Utilizar métodos de transferencia de archivos.
- Hacer limpieza de huellas y rastros.
- Realizar documentación y reportes: Metasploit, Reporte ejecutivo y Reporte técnico

9. Proyecto de asignatura

Implementar técnicas de hacking avanzadas que garanticen un alto valor de éxito en la seguridad de un sistema informático.

10. Evaluación por competencias

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

- Evaluación diagnóstica.
- Investigación en diversas fuentes de información.
- Desarrollo de actividad(es) y reporte de prácticas.
- Exposición de temas específicos.
- Exámenes teóricos - prácticos que demuestre parte del conocimiento adquirido durante la asignatura.

11. Fuentes de información

Exploit DB. (05 de 2021). *Google Hacking Database*. Obtenido de exploit-db.com: https://www.exploit-db.com/google-hacking-database

Grant, J. (2019). *Ethical Hacking, A comprehensive Beginner's Guide to Learn and Understand the Concept of Ethical Hacking.* ASIN : B07SKRSSP3.

Hadnagy, C. (2011). *Social Engineering, The Art of Human Hacking.* Indianapolis: Wiley Publishing.

Hadnagy, C. (2018). *Social Engineering, The Science of Human Hacking.* Indianapolis, IN: John Wiley & Sons, Inc.

Maurushat, A. (2019). *ETHICAL HACKING.* Ottawa, CA: Gauvin, University of Ottawa Press.

osintux. (05 de 2021). *Google Hacking Database*. Obtenido de osintux.org: http://www.osintux.org/documentacion/google-hacking-database

Pablo González Pérez, G. S. (2013). *Pentesting con Kali.* Madrid, España: 0xWord Computing.

Papazov, Y. (2016). Social Engineering. *North Atlantic Treaty Organization*, 18.

Raphaël Hertzog, J. O. (2021). *Kali Linux Revealed.* New York NY, USA: OffSec Press.

Yadav, S. (2018). *Ethical Hacking, From Beginner to Advanceed.* Delhi, India: ASIN : B0892TYGDK.