1. Datos Generales de la asignatura

Nombre de la asignatura:	Análisis de vulnerabilidades I
Clave de la asignatura:	CSD-2402
SATCA[1]:	2 – 3 – 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 estudia las técnicas para realizar, detectar y defenderse de ataques de ingeniería social, así como los métodos más utilizadas en la actualidad para identificar vulnerabilidades en sistemas informáticos.

Intención didáctica

La asignatura se encuentra organizada en cuatro temas.

En el primer tema se estudian los principales conceptos de la “Ingeniería Social”, sentará las bases para conocer los mecanismos para defender un sistema informático, así como detectar las vulnerabilidades en las organizaciones.

El tema dos presenta el proceso de reconocimiento pasivo donde se consigue la información sin interacción directa con el objetivo mediante el uso de técnicas tales como la ingeniería social, sniffing de red, búsquedas por internet o vigilancia de instalaciones para recabar información sobre empleados, accesos, infraestructura, etc.

El tercer tema, explora diferentes metodologías del reconocimiento activo, el cual comprende el estudio de la red para descubrir los equipos individuales, las direcciones IP y los servicios que se prestan. Este proceso implica más riesgo de detección que el reconocimiento pasivo.

[1] Sistema de Asignación y Transferencia de Créditos Académicos

El tema cuatro concluye proporcionando el conocimiento y aplicación de herramientas de escaneo de vulnerabilidades, en esta fase se usa la información proporcionada por los dos temas anteriores para examinar la red, siendo los recursos que puede emplear el hacker auditor.

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
• Conoce cómo realizar ataques de ingeniería social. • Detecta los ataques de Ingeniería Social. • Defiende los ataques de Ingeniería Social. • Emplea el ciclo de vida de una prueba de penetración.

5. Competencias previas

- Se recomiendan las competencias desarrolladas y adquiridas en la asignatura de 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	Ingeniaría Social	1.1 Conceptos básicos y su importancia 1.2 Herramientas de investigación. 1.3 Las doce bases para aplicar IS. 1.4 Phishing - Detección de phishing (Reflexión e importancia). 1.5 Aplicación de IS con OSINT (Open Source Intelligence). 1.6 Ingeniería social Directa. 1.7 Ingeniería social indirecta. 1.8 Ingeniería social sin TI.
2	Hacking Ético – Reconocimiento pasivo	2.1 Teoría del reconocimiento 2.2 Reconocimiento pasivo con motores de búsqueda. 2.3 Google dorks – Google Hacking Data Base (GHDB) 2.4 Herramientas de reconocimiento pasivo
3	Hacking Ético – Reconocimiento activo	3.1 Lookups 3.2 DMZ (transferencia de zona) 3.3 NMAP (Escaneo de Puertos) 3.4 NSE (Nmap, scripting Engine, motor de secuencias de comandos) 3.5 Enumeración SMB (Server Message Block) 3.6 Enumeración SMTP (Simple Mail Transfer Protocol) 3.7 Enumeración SNMP (Simple Network Management Protocol)
4	Herramientas de Escaneo de vulnerabilidades.	4.1 Teoría del escaneo 4.2 Herramientas 4.3 Escaneo y enumeración de aplicaciones web.

7. Actividades de aprendizaje de los temas

Ingeniaría Social	
Competencias	Actividades de aprendizaje
Específica(s): Detecta y defiende los ataques de Ingeniería Social.	• Esquematizar los diferentes métodos de la IS. • Realizar un plan de ataque de IS. • Realizar prácticas de IS con OSINT.

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 prácticas con herramientas para no ser víctima de IS. • Realizar prácticas de detección y defensa de IS.
Hacking Ético – Reconocimiento pasivo	
Competencias	Actividades de aprendizaje
Específica(s): Emplea el ciclo de vida de una prueba de penetración. Utilizar las funcionalidades avanzadas de los motores de búsqueda para recolectar información. 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 prácticas con motores de búsqueda. • Utilizar la herramienta MXToolBox • Utilizar la herramienta Shodan engine. • Emplear la base de datos Google hacking para aplicar las cadenas de búsqueda necesarias y así encontrar problemas de seguridad existentes en Internet. • Realizar búsquedas de Footholds, de archivos con contenido de nombres de usuario, directorios con información sensible, de servidores web con una tecnología concreta, de archivos vulnerables, servidores vulnerables, mensajes de error, archivos con información importante, archivos con contraseñas, información sensible de sitios de compras online, información concreta de red o vulnerabilidades, páginas que contienen portales de login concretos, dispositivos concretos en línea. • Utilizar herramientas de reconocimiento pasivo.
Hacking Ético – Reconocimiento activo	
Competencias	Actividades de aprendizaje
Específica(s): Utiliza herramientas de reconocimiento activo. Emplea el ciclo de vida de una prueba de penetración.	• Realizar búsquedas (lookups) automatizadas. • Realizar búsquedas en fuerza bruta • Realizar recolección de información a través de servidores DNS por medio de DMZ. • Realizar escaneo de puertos con la herramienta nmap.

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.	• Crear scripts propios para automatizar aún más los escaneos de puertos y servicios. • Realizar enumeración de información a través del Protocolo SMB a un equipo en Windows desde un equipo en Linux. • Realizar enumeración de información a través del Protocolo SMTP para la recolección de información como cuentas válidas. • Realizar enumeración SNMP para ver las tecnologías, aplicaciones y servicios que existen en un target.
Herramientas de Escaneo de vulnerabilidades	
Competencias	Actividades de aprendizaje
Específica(s): Emplea reconocimiento activo y pasivo a través de herramientas de escaneo. Implementar técnicas de hacking avanzadas. Emplea el ciclo de vida de una prueba 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.	• Definir el alcance y los objetivos que tiene el assessment en general. • Utilizar el motor de scripting de Nmap para explorar las posibles vulnerabilidades en los diferentes sistemas dentro del alcance. • Investigar cómo operan normalmente los motores de escaneo de vulnerabilidades • Examinar específicamente cómo Nessus Essentials puede configurarse para el escaneo de diferentes targets y cómo interpretar la información presentada. • Investigar cómo OpenVas se contrasta con el motor privativo Nessus Essentials, • Investigar cómo la perspectiva de OpenVas y Nessus Essentials varía según los objetivos de implementación dentro de la organización.

8. Práctica(s)

- Realizar ataques de ingeniería social indirecta
- Realizar ataques de ingeniería social directa
- Realizar ingeniería social con OSINT
- Influir a las personas para alcanzar ciertos objetivos
- Defender y detectar los ataques de Ingeniería Social
- Efectuar reconocimiento pasivo a través de motores de búsqueda
- Efectuar reconocimiento pasivo utilizando Google Dorks (GHDB)
- Efectuar reconocimiento activo utilizando lookups automatizados y con fuerza bruta
- Realizar escaneo de puertos

- Ejecutar transferencia de zonas (DMZ)
- Realizar diferentes tipos de enumeraciones (SMB, SMTP, SNMP)
- Realizar escaneo de vulnerabilidades por medio de herramientas especializadas (Nessus, OpenVas)

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 prácticos que demuestre el 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.