Carrera INGENIERIA EN INFORMATICA		
Asignatura ELECTIVA II - 3678 - Tecnologías en Seguridad		
Trayecto Calidad y Seguridad de la Información		
Año académico 2023		
Responsable / Jefe de cátedra Lic Martin Hernán Zeballos		
Carga horaria semanal: 4 hs	**Carga horaria total:** 64 hs	**Créditos ----**
Modalidad: Presencial		
Correlativas anteriores: MATEMATICA APLICADA - SEGURIDAD APLICADA Y FORENSIA	**Correlativas posteriores**: ----------	
Conocimientos necesarios ----------		

Descripción de la asignatura

La asignatura electiva Tecnologías en Seguridad, está planteada como una materia teórico - práctica donde los alumnos conocerán los fundamentos de la seguridad en las redes de datos. Dada la dinámica de los contenidos de la materia los temas a tratar en la misma van desde tecnología de base a temas actuales de mercado.

Metodología de enseñanza

Las clases se desarrollarán empleando el modelo deductivo de exposición con participación de los alumnos. Las clases serán teóricas y prácticas.

Se utilizarán las siguientes estrategias en diferentes momentos del proceso enseñanza-aprendizaje: presentación de los conceptos, desarrollo del tema, tormenta de ideas, estadísticas, ilustraciones funcionales, mapas conceptuales, organizadores previos, resúmenes.

Durante la cursada los alumnos desarrollarán Trabajos Prácticos individuales que servirán como puente entre el marco teórico de la asignatura y su aplicación práctica permitiendo a los alumnos desarrollar las capacidades de trabajo en equipo; se utilizará la estrategia de Resolución de Casos.

También se desarrollarán actividades adicionales propuestas por los docentes y/o sugerencias de los alumnos.

Objetivos de aprendizaje

- Desarrollar en el alumno una actitud crítica y reflexiva con referencia a la seguridad de las redes.
- Dar al alumno las herramientas necesarias para desarrollar las políticas, planificar los procedimientos de seguridad e implementar los planes de mitigación y contingencia en las redes de datos.
- Facilitar al alumno los elementos necesarios para diseñar y configurar redes seguras.
- Proporcionar al alumno las metodologías y estándares de seguridad para la selección, implementación y uso de aplicaciones criptográficas.

Contenidos mínimos

Introducción a la seguridad en redes. Seguridad en aplicaciones Web. Conceptos de seguridad en la nube. Autenticación mediante servidor RADIUS. Protocolos EAP. Configuración de políticas de seguridad en Firewalls. Protocolo WEP, WPA, WPA2. Ataques. Tipos de amenazas: acceso no autorizado, suplantación de la identidad, denegación de servicio. Tecnologías VPDN, VPN. Vulnerabilidades ServerSide – Client Side. Temas actuales de seguridad en redes.

Competencias a desarrollar

Genéricas

- Identificación, formulación y resolución de problemas de ingeniería en sistemas de información/informática.
- Utilización de técnicas y herramientas de aplicación en la ingeniería en sistemas de información / informática.
- Actuación profesional ética y responsable.
- Aprendizaje continuo.
- Desempeño en equipos de trabajo.
- Comunicación efectiva.

Específicas

- Proyecto y dirección en lo referido a seguridad informática.
- Dirección y control de la implementación, operación y mantenimiento de sistemas de información, sistemas de comunicación de datos, software, seguridad informática y calidad de software.
- Procedimientos y certificaciones del funcionamiento, condición de uso o estado de sistemas de información, sistemas de comunicación de datos, software, seguridad informática y calidad de software.

Programa analítico	
Unidad 1	**Introducción a la Tecnologías en Seguridad** Conceptos básicos de la seguridad en redes. Historia de la seguridad en redes y su evolución en el tiempo. Componentes básicos de una seguridad en redes
Unidad 2	**Tecnologías actuales** Dada la dinámica de la seguridad en redes, en la materia se tratarán temas actuales de tecnología de última generación. Se presentarán herramientas utilizadas en las mejores compañías con casos reales de uso.
Unidad 3	**Análisis de vulnerabilidades en seguridad** Test de Detección de Vulnerabilidades. Test de penetración. Hacking ético. Metodología. Distintos tipos de Software Comerciales y de Libre Distribución. Aspectos contractuales y legales.
Unidad 4	**Configuración de políticas de seguridad en Firewalls** Dispositivos de seguridad en la arquitectura de las redes. Firewalls. Configuración de políticas de seguridad en Firewalls. Intrusion Detection Systems (IDS). Intrusion Prevention Systems (IPS). Next Generation Firewalls. Dispositivos Unified Threat Management (UTM).
Unidad 5	**Protocolo WEP, WPA, WPA2. Protocolos EAP.** Introducción a las Wireless LAN. Ataques y vulnerabilidades. Seguridad en las redes Wireless: 802.11x. Protocolo WEP. Protocolos WPA y WPA2. Protocolo EAP. Diseño de una arquitectura segura para instalar una red Wireless en una LAN corporativa.
Unidad 6	**Ataques.** Hackers, crackers y distintos tipos de Malware. Técnicas de ataque. Accesos no autorizados. Ataques a través de redes peer-to-peer. Vulnerabilidades de Sistemas Operativos, Aplicativos y Software de Seguridad.
Unidad 7	**Tipos de amenazas: acceso no autorizado, suplantación de identidad, denegación de servicio** Análisis y detección de distintos tipos de amenazas: acceso no autorizado, suplantación de identidad, denegación de servicio
Unidad 8	**Tecnologías VPDN, VPN** VPDN: Virtual Private Dial-up Network. Características de seguridad. Configuración. Protocolos. VPN: Virtual Private Network. Características básicas de seguridad. Ventajas. Tipos de VPN. Implementaciones. Tipos de conexión.
Unidad 9	**Vulnerabilidades Server Side – Client Side** Revisión de vulnerabilidades del lado del cliente y del lado del servidor. SQLi, Directory Traversal, SSRF, Cross Site Scripting, Cross Site Request Forgery,

Planificación de actividades					
Semana	Clase	Actividad Detalle de la actividad a desarrollar	Tipo (indicar el tipo de actividad a desarrollar: teoría, práctica, práctica de laboratorio, trabajo de campo, otra)	Duración estimada	Unidad
1	1	Presentación de la materia. Introducción a la seguridad informática. Instalación Kali Linux Firewalls, IDS, IPS	Teórico-Práctica	4	
2	2	Ingeniería Social. Footprinting Metodología basada en Certified Ethical Hacker (CEH)	Teórico	4	
3	3	Práctica 1 y 2 Footprinting and Reconnaissance Scanning Networks Enumeration Social Engineering	Práctica	4	
4	4	Escaneo de puertos. Escaneo de vulnerabilidades. Cloud Vulnerabilidades en redes Wireless Funcionamiento de VPN ventajas	Teórico	4	
5	5	Práctica 3 y 4 Sniffing Denial-of-Service Session Hijacking Hacking Webservers SQL Injection	Práctica	4	
6	6	PRIMER PARCIAL		4	-
7	7	Charla sobre temas de actualidad en seguridad	Teórico	4	
8	8	Práctica 5 y 6 System Hacking Hacking Wireless Networks Hacking Mobile Platforms Evading IDS, Firewalls, and Hacking Web Applications	Práctica	4	
9	9	OWASP Top Ten. Parte 1	Teórico-Práctica	4	
10	10	Práctica Server Side	Práctica	4	

		SQL injection vulnerability in WHERE clause allowing retrieval of hidden data SQL injection vulnerability allowing login bypass SQL injection UNION attack Directory Traversal SSRF			
11	11	OWASP Top Ten. Parte 2	Teórico	4	
12	12	Práctica Client Side Cross-site scripting (XSS) Reflected XSS into HTML DOM XSS Stored XSS into HTML Cross-site request forgery (CSRF)	Práctica	4	
13	13	Clase de consulta	Teórico-Práctica	4	
14	14	SEGUNDO PARCIAL		4	-
15	15	RECUPERATORIO 1ro ó 2do Parcial		4	-
16	16	Cierre de la materia		4	

Evaluación

La evaluación del alumno consta de dos parciales y ocho prácticas.

El primer parcial se toma en la 6ta semana y se evaluarán las unidades 1,2,3,4 y 5 de teoría más las practicas 1,2,3 y 4.
El examen consta de preguntas del tipo opción múltiple, se realizarán de 30 a 40 preguntas las cuales solo tienen una opción válida correcta.
En el parcial se realizan preguntas para evaluar la teoría y también las prácticas.
La devolución al alumno es a través de Miel enviándole la nota y comentarios de ser necesario.
Los alumnos tienen la opción de la clase siguiente revisar su examen y realizar consultas.
Deberán tener los prácticos 1,2,3 y 4 entregados.

Este examen alcanza las competencias:
Actuación profesional ética y responsable.
Aprendizaje continuo.
Dirección y control de la implementación, operación y mantenimiento de sistemas de información, sistemas de comunicación de datos, software, seguridad informática y calidad de software.
Identificación, formulación y resolución de problemas de ingeniería en sistemas de información/informática.
Utilización de técnicas y herramientas de aplicación en la ingeniería en sistemas de información / informática.

El segundo parcial es un trabajo practico integrador grupal en donde los alumnos aplican los conocimientos adquiridos en la materia.

Deberán tener las prácticas 5,6, Server Side, Client Side entregados.
La entrega del TP integrador es a través de Miel y se hace una devolución presencial en donde se hacen preguntas sobre el TP de forma oral.

Este examen alcanza las competencias:
Desempeño en equipos de trabajo.
Comunicación efectiva.
Procedimientos y certificaciones del funcionamiento, condición de uso o estado de sistemas de información, sistemas de comunicación de datos, software, seguridad informática y calidad de software.
Utilización de técnicas y herramientas de aplicación en la ingeniería en sistemas de información / informática.

Las prácticas constan de ejercicios que se realizan en máquinas virtuales donde van reforzando los temas vistos en la teoría. Cada alumno entrega su práctica vía miel y se le realiza una devolución por la misma herramienta.

Primera evaluación	Semana 6	Presencial	2 horas (19 a 21 hs.)
Segunda evaluación	Semana 14	Presencial	4 horas (19 a 23 hs.)
Recuperatorio	Semana 15	Presencial	2 horas (19 a 21 hs.)

Bibliografía obligatoria (disponible en la Biblioteca Leopoldo Marechal, o con acceso digital)

Título	Autor	Editorial	Edición	Año
Diseño de seguridad en redes	Kaeo, Merike	Pearson Educación	1ra	2003
Hackers 2 : secretos y soluciones para la seguridad de redes	Scambray, Joel; McClure, Stuart; Kurtz, George.	Osborne/McGraw-Hill	1ra	2001
Computer Segurity : Principles and Practice	Stallings, William; Brown, Lawrie; Bauer, Mick; Howard, Michael	Pearson Education	2da	2012
Hackers de sitios web	Scambray, Joel; Shema, Mike	Osborne/McGraw-Hill	1ra	2003
Practical UNIX e Internet security	. Garfinkel, Simson; Spafford, Gene	Beijing: O'Reilly	2da	1996
Firewalls and Internet security : repelling the wily hacker	Cheswick, William R.; Bellovin, Steven M.	Reading, Mass.: Addison-Wesley	1ra	1994
Wireshark Network Analysis : the Official Wireshark Certified	Chappell, Laura	Chappell University; Protocol Analysis Institute	2da	2012

Network Analyst Study Guide				

Otros recursos obligatorios (videos, enlaces, otros) Incluir una fila por cada recurso	
Nombre	Material de la cátedra disponible en MIeL
Introducción Seguridad en redes	Introducción Seguridad en redes
Footprinting Ingenieria Social	Footprinting Ingenieria Social
Introducccion scaneo de vulnerabilidades	Introducccion scaneo de vulnerabilidades
Scanning Enumeration	Scanning Enumeration
Seguridad Cloud	Seguridad Cloud
OWASP Top 10	OWASP Top 10
Introducción a la Seguridad Aplicativa	Introducción a la Seguridad Aplicativa
Herramientas SAST	Herramientas SAST

Otros recursos complementarios (videos, enlaces, otros) Incluir una fila por cada recurso	
Nombre	