1. Datos Generales de la asignatura

Nombre de la asignatura:	Seguridad en Redes
Clave de la asignatura:	SDI-1804
SATCA[1]:	(2 - 3 - 5)
Carrera:	Ingeniería en Sistemas Computacionales Ingeniería en Tecnologías de la Información y Comunicaciones Ingeniería Informática

2. Presentación

Caracterización de la asignatura
La administración de la seguridad de la red no sólo implica el mantener al día las políticas y procedimientos de seguridad establecidos, sino la realización de auditorías, mediante pruebas de penetración y desempeño de la red.
Intención didáctica
El alumno conocerá elementos para llevar a cabo un análisis de riesgos y su implementación en los servicios de red, establecidos en la organización.

[1] Sistema de Asignación y Transferencia de Créditos Académicos

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Instituto Tecnológico de Morelia, 13 de Agosto de 2018.	Dr. Juan Manuel García García Dr. Anastacio Antolino Hernandez Dr. Heberto Ferreira Medina Ing. Juan Jesús Ruiz Lagunas M.C. Juan Carlos Olivares Rojas M.C. Abel Alberto Pintor Estrada M.C. Christhian Torres Millares	Diseño Curricular basado en Competencias del Módulo.

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
El alumno conocerá metodologías de análisis de riesgos, elaboración de procedimientos y políticas de seguridad, para su uso e implementación de la red dentro de la organización, así como llevar a cabo pruebas de penetración y vulnerabilidades de los servicios en red.

5. Competencias previas

- Seleccionar, clasificar y analizar información.
- Observar el escenario problema e identificar oportunidades de desarrollo de proyectos generando ideas innovadoras de la aplicación de la investigación en su área profesional.

6. Temario

No.	Temas	Subtemas
1	Introducción	1.1 Objetivos de la Seguridad Informática. 1.2 Amenazas, vulnerabilidades, riesgos y controles en redes. 1.3 Definición de SGSI 1.4 Normas y estándares de redes

2	Análisis de riesgos en servicios de red	2.1 Objetivos del análisis de riesgos 2.2 Servicios de red seguros 2.3 Monitoreo y reconocimiento 2.4 Herramientas
3	Pruebas de penetración (Pentesting)	3.1 Antecedentes, conceptos y ética 3.2 Herramientas 3.3 Escaneo 3.4 Metodologías
4	Hackeo ético	4.1 Obtener acceso 4.2 Mantener acceso 4.3 Técnicas de eliminación de rastros 4.4 Reporte técnico

7. Actividades de aprendizaje de los temas

Tema 1: Introducción	
Competencias	Actividades de aprendizaje
Específica(s): - Conocerá los conceptos de seguridad informática Genéricas: - Conocerá los conceptos de seguridad informática y los estándares enfocados al mismo	1. Documentarse en todos los conceptos de seguridad informática, aclarando las diferencias entre algunos conceptos.
Tema 2: Análisis de riesgos en servicios de red	
Competencias	Actividades de aprendizaje
Específica(s): - Conocer la metodología FRAP, para llevarla a cabo en un análisis de riesgos sobre los dispositivos y servicios de red. Genéricas: - Llevar a cabo la metodología para llevar a cabo el proceso del análisis de riesgos y su implementación.	1. Llevar a cabo la documentación de dicho análisis y la elaboración de los manuales de políticas y procedimientos derivados de dichas reuniones.

Tema 3: Pruebas de penetración (Pentesting)	
Competencias	Actividades de aprendizaje
Específica(s): - Implementar los procesos de auditoria informática en la red. Genéricas: - Desarrollar e implementar un planes de auditoria de la seguridad en la red.	1.- Implementará los procesos iniciales de hackeo ético para las auditorias de seguridad en la red.
Tema 4: Hackeo ético	
Competencias	Actividades de aprendizaje
Específica(s): - Podrá llevar hackeo ético en servicios de red. Genéricas: - Sera capaz de llevar a cabo un análisis forense en equipo de cómputo, para recuperar datos o conocer la forma de ataque recibida.	1- Llevar a cabo hacking ético para vulnerar servidores. 2- Realizar análisis forense de dichos ataques.

8. Práctica(s)

Implementar servicios de red en los servidores, para ser vulnerados y analizados de manera posterior. Reconocer y escanear servicios y vulnerabilidades en la red Vulnerar los servicios con baja seguridad para lograr acceso a los servidores. Elaborar reportes e informes de la auditoria de seguridad llevada a cabo con las herramientas de pentesting

9. Proyecto de asignatura

Que el alumno, sea capaz de llevar a cabo ethical hacking, para conocer el nivel de seguridad implementado en las redes actuales y futuras.

10. Evaluación por competencias

- En un laboratorio de especialidad, preferentemente con Linux Distribución Debian y/o Centos, configurar los servicios de DNS, DHCP, FTP, WEB y CORREO.
- Elaborar los planes de auditoria de seguridad para cada uno de los servicios.
- Resguardar cada uno de los servicios.
- Recuperar cada uno de los servicios después de haber experimentado una contingencia.

11. Fuentes de información

S.SHAH; W.SOYINKA. “Linux Administration”, Mac Graw Hill, 2005.

H.BRELSFORD. “Windows 2000 Server” Arrayan, 2007.

J.RAYA; E.RAYA. “Windows NT Server”,Ra-Ma.

E.NAVARRO; V.PIATTINI. ”Auditoria Informática: Un enfoque practico”, RaMa.

G.MARK “Commands, Editors, and shell Programming ”

TANENBAUM A. (2003). Redes de computadoras. Prentice Hall. Cuarta ed.

Mexico.

Cert coordination Center, “Análisis de un sistema comprometido”,

http://www.cert.org/security-improvement/practices/p046.html

Página dedicada a la seguridad desarrollada por Universidad Nacional Autónoma de México.

http://www.seguridad.unam.mx.

Cert Coordination Center, Trabajo sobre el análisis de información en Unix,

http://www.cert.org/tech_tips/win-UNIX-system_compromise.html.

Trabajo sobre cómo hacer una auditoria informática,

http://www.auditoria.com.mx/.

Benson C., (s.f.), Estrategia de seguridad, Microsoft TechNet. Desde

https://www.microsoft.com/latam/technet/articulos/200011/art04/default.asp

Carli F. (2003), Security Issues With DNS.

http://www.sans.org/reading room/whitepapers/dns/1069.php.

Scarfone K., Mell P., (2007) Guide to Intrusion Detection and Prevention

Systems (IDPS), NIST.

http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

Wack J., Cutler K., y Pole J. (2002), Guidelines on Firewalls and Firewall Policy,

NIST, Computer Security Division.

http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf

May C., Baker M., y Gabbard D., et. al., (2004), Advanced Information

Assurance Hand-book, CERT, Carnegie Mellon University, USA.

http://www.cert.org/archive/pdf/aia-handbook.pdf

Ferrer J., Fernández-Sanguino J., (s.f.), El sistema operativo GNU/Linux y sus

herramientas libres en el mundo de la seguridad: estudio del estado del arte.

http://mmc.igeofcu.unam.mx/LuCAS/Presentaciones/200103hispalinux/ferrer/pdf/seguridad-y-sw-libre v1.0.pdf

Herzog P. (2003), Manual de la Metodología Abierta de Testeo de Seguridad,

ISECOM, segunda ed., USA.

http://isecom.securenetltd.com/osstmm.en.2.2.pdf

Miles T., Wayne J., McLarnon M., (2002), Guidelines on Securing Public Web

Servers, NIST, USA.

http://csrc.nist.gov/publications/nistpubs/800-44 ver2/SP800-44v2.pdf

Stoneburner G., Goguen A., Feringa A., (2001), Underlying Technical Models for

Information Technology Security, NIST.

http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf