Universidad Guadalajara

Centro Universitario del Sur

Programa de Estudio

1. IDENTIFICACIÓN DE LA UNIDAD DE APRENDIZAJE

División

División de Ciencias Exactas, Naturales y Tecnológicas.

Departamento

Ciencias Computacionales e Innovación Tecnológica.

Academia

Academia de Redes y Comunicaciones.

Programa(s) educativo(s)

Ingeniería en Telemática

Denominación de la unidad de aprendizaje:

Seguridad de Acceso a Redes Publicas

Clave de la materia:	Horas de teoría:	Horas de práctica:	Carga horaria global:	Valor en créditos:
IG206	30	50	80	8

Tipo de curso:		Nivel en que se ubica:	Prerrequisitos:
C = curso		Técnico Medio Técnico Superior Universitario **Licenciatura** Especialidad Maestría Doctorado	IG215
CL = curso laboratorio			
L = laboratorio			
P = práctica			
T = taller			
CT = curso - taller			
N = clínica			
M = módulo			
S = seminario			

Área de formación:

Especializante Selectiva.

Perfil docente:

- Licenciatura en Informática, sistemas computacionales o afines.
- Maestría o Doctorado en áreas de computación, redes o afines.
- Experiencia en manejo de sistemas “Cisco IOS”.
  Experiencia en manejo de sistemas “GNU/Linux”.
- Acreditación por parte de Cisco Networking Academy. Preferentemente en area de seguridad
- Experiencia en el área de docencia o capacitación mínima un año.

Elaborado por:	Actualizado por:
Mtro. Jesús Enrique Ponce Corona	

Fecha de elaboración:	Fecha de última actualización:	Fecha de última evaluación:	Fecha de aprobación por Colegio Departamental:
12/ 07 /2023			

1. PRESENTACIÓN DE LA UNIDAD DE APRENDIZAJE

El propósito de esta unidad de aprendizaje es evaluar y dar propuesta a las distintas tecnologías, técnicas y protocolos de autenticación, cifrado y privacidad que ofrecen las redes de acceso de carácter publico. Dando un enfoque ético se realizan ejecuciones y pruebas sobre el sistema que ofrece el servicio, buscando vulnerabilidades que comprometan al usuario común para así ofrecer soluciones que eviten minimicen el impacto sobre los diversos ataques informaticos.

2. OBJETIVO GENERAL/COMPETENCIA

Desarrollar habilidades y conocimiento para ofrecer soluciones profesionales en el campo de la seguridad informática con respecto a la preservación de la privacidad del usuario e integridad de la información en las redes informáticas de acceso publico. Por medio de protocolos, aplicaciones y técnicas aprobadas en el marco ético legal.

- Entender las bases tecnológicas en lo que a tecnologías de acceso se refiere.
- Ejecutar auditorias y pruebas de penetración a sistemas de acceso público con un enfoque ético, para encontrar fallos ya sea en el diseño o configuración del mismo.
- Implementar soluciones que prevengan o reduzcan el riesgo a una amenaza que comprometa la integridad del usuario y su información.
- Generar reportes profesionales donde especifique vulnerabilidades y ofrezca propuesta para evitar o minimizar amenazas de la red.

3. CAMPO DE APLICACIÓN PROFESIONAL DE LOS CONOCIMIENTOS

Aplicar los conocimientos y habilidades en seguridad de acceso a la red para dar solución a proyectos de infraestructura de conexión, gestión de datos y usuarios, políticas de seguridad que una empresa, institución, organismo requiera. Teniendo transparencia y compatibilidad entre protocolos abiertos y propietarios.

4. SABERES:

Prácticos	• Ejecuta eficientemente pruebas de estrés y desempeño en los accesos a las redes • Caracteriza el tráfico de las aplicaciones de usuario e interpreta los resultados para proponer una solución de seguridad. • Propone mejoras a la infraestructura tecnologíca en el acceso al servicio, con base en en analisis y pruebas realizadas.
Teóricos	• Identifica los parámetros básicos en el acceso a la red. • Observa la relación entre los factores de desempeño de dispositivos y sus efectos que puedan fortalecer o debilitar las medidas de seguridad. • Aprende a desarrollar entrevistas para obtener los requerimientos de usuario
Formativos	• Fortalecerá la redacción de documentos técnicos • Fortalecerá las habilidades para expresar y defender sus ideas mediante la presentación y defensa de un proyecto de diseño • Fortalecerá las habilidades de comunicación y trabajo en equipo

5. CONTENIDO TEMÁTICO (TEÓRICO-PRÁCTICO)

1.- Redes Locales Inalámbricas WLAN
- Arquitectura de redes WLAN
- Características y funcionamiento
- Protocolos de autenticación.
- Protocolos de cifrado.

2.- Encriptación y anonimato en redes publicas
- Redes Tor y Freenet.
- IPSec y VPNs en dispositivos móviles.
- Anonimato por navegación.
- Uso de servicios Proxys.

3.- Auditoria y "Pentesting" a servicios de redes de acceso público.
- Auditoria de trafico en autenticaciones.
- Análisis de cifrado durante una transferencia de datos.
- Pruebas de interceptación tipo "MiTM"
- Pruebas de suplantación tipo "Spoofing"
- Pruebas de secuestro tipo "Hijacking"
- Pruebas de estrés tipo "DoS"
- Pruebas de vulnerabilidad tipo "Exploit"

4.- Gestión de acceso y defensa de amenazas en redes publicas
- Control en el análisis pasivos y "Scanning"
- Detección y control de Phising.
- Detección y control de intermediarios o Proxys.
- Contención de secuestros y Ramsomware.
- Generación de reportes de incidencia y respuestas.

6. ESTRATEGIAS DE ENSEÑANZA-APRENDIZAJE

- Exposiciones por parte del docente
- Ejercicios teórico-práctico en equipo/individual (solución de ejercicios), por parte de los alumnos
- Realización de trabajo en equipo, individual por parte del alumno.

7. EVALUACIÓN DEL APRENDIZAJE

8.1. Evidencias de aprendizaje	8.2. Criterios de desempeño
Ejercicio práctico de diseño de redes con acceso seguro encriptado y privado	Se requiere el diseño de una red local básica con protocolos criptográficos efectivos.
Ejercicio práctico de configuración de redes con acceso publico, bajo esquemas seguros y no seguros	Se requiere la configuración de una red local básica con politicas aplicadas a dispositivos de seguridad y establecer listas de acceso hacia los usuarios.
Ejercicio práctico de configuración de redes para aplicar medidas de control en zonas internas y externas	Se requiere la configuracion y prueba de protocolos criptográficos, listado de politicas de acceso en zonas segurias e inseguras de la red local.
Propuesta de gestion de conexiones para identificar anomalías en el trafico y comportamiento de la red	Planear y diseñar una arquitectura de datos y topolog´ia de red que permita la separación de zonas y jerarquia de seguridad de acuerdo a las políticas necesarias por el usuario.

8. CALIFICACIÓN

Reportes de lecturas .....
Actividades de laboratorio.....
Actividades Practicas.....
Actividad extracurricular.....

9. ACREDITACIÓN

Periodo ordinario. De conformidad con el artículo 20 del Reglamento General de Evaluación y Promoción de Alumnos de la Universidad de Guadalajara, para que el alumno tenga derecho al registro del resultado final de la evaluación en el periodo ordinario, establecido en el calendario escolar aprobado por el Consejo General Universitario, se requiere: I. Estar inscrito en el plan de estudios y curso correspondiente, y II. Tener un mínimo de asistencia del 80% a clases y actividades registradas durante el curso.	**Periodo extraordinario.** De conformidad con el artículo 27 del Reglamento General de Evaluación y Promoción de Alumnos de la Universidad de Guadalajara, para que el alumno tenga derecho al registro de la calificación en el periodo extraordinario, se requiere: I. Estar inscrito en el plan de estudios y curso correspondiente. II. Haber pagado el arancel y presentar el comprobante correspondiente. III. Tener un mínimo de asistencia del 65% a clases y actividades registradas durante el curso. Se exceptúan de este caso las materias de orden práctico que requerirán la repetición del curso (Art. 23 RGEYPA).

10. BIBLIOGRAFÍA

BIBLIOGRAFÍA BÁSICA

1. Hacking y Seguridad en Internet. Fernando Picouto Ramos (2008). Ed Alfa Omega
2. Seguridad Digial y Hackers. Juan Diego Gutierrez (2005). Ed Anaya
3. Hacking Tecnicas Fundamentales. Jon Erickson (2009). Ed Anaya
4. Seguridad de Redes. Chris McNab (2008). Brandon A. Nordin (2002). Ed McGraw Hill
5. Hackers. Tecnicas y herramientas para defendernos. Juan Andreś Maillo (2021). Ed RaMa

BIBLIOGRAFÍA COMPLEMENTARIA

1. Enciclopedia de la Seguridad Informatica. Alvaro Gomez Vieites (2007). Ed RaMa
2. Seguridad Informatica y Cibercrimen. Moreno Perez Arnoldo (2012). Ed Linea Roja

11. RECURSOS COMPLEMENTARIOS (páginas web, mooc's, plataformas, objetos de aprendizaje)

Plataforma eductativa Networking Academy (requiere registro). Curso "Introduction to Cibersecurity": https://www.netacad.com/

Plataforma educativa Fortinet Training Institute (requiere registro). Curso :"Information Security Awareness" https://training.fortinet.com/auth/saml2/selectidp.php

Plataforma educativa Fortinet Training Institute (requiere registro). Curso :"Evolution to Cibersecurity" https://training.fortinet.com/auth/saml2/selectidp.php

Plataforma educativa Fortinet Training Institute (requiere registro). Curso : "Fortinet Product Awareness" https://training.fortinet.com/auth/saml2/selectidp.php

Firma:	**Vo.Bo.**
Presidente de Academia	**Jefe de Departamento**