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 redes

| Clave de la materia: | Horas de teoría: | Horas de práctica: | Carga horaria global: | Valor en créditos: |
|---|---|---|---|---|
| IG197 | 40 | 40 | 80 | 8 |

| Tipo de curso: | | Nivel en que se ubica: | Prerrequisitos: |
|---|---|---|---|
| C = curso | | Técnico Medio<br>Técnico Superior<br>Universitario<br>**Licenciatura**<br>Especialidad<br>Maestría<br>Doctorado | IG192 Escalabilidad de redes |
| CL = curso laboratorio | | | |
| L = laboratorio | | | |
| P = práctica | | | |
| T = taller | | | |
| **CT = curso - taller** | | | |
| N = clínica | | | |
| M = módulo | | | |
| S = seminario | | | |

Área de formación:

Básica Particular Obligatoria

Perfil docente:

- Licenciatura en Informática, sistemas computacionales o afines.
- Maestría o Doctorado en áreas de computación, redes o afines.
- Experiencia en manejo de sistemas GNU/Linux.
- Experiencia en herramientas de seguridad informática.

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

| Fecha de elaboración: | Fecha de última actualización: | Fecha de última evaluación: | Fecha de aprobación por Colegio Departamental: |
|---|---|---|---|
| 10/ 08 /2020 | 12/12/2022 | 12/12/2022 | |

## 1. PRESENTACIÓN DE LA UNIDAD DE APRENDIZAJE

El propósito de esta unidad de aprendizaje es evaluar redes de computadoras, basándose en lineamientos y estándares establecidos para determinar su nivel de seguridad, confianza e integridad tanto en su infraestructura como en el uso de protocolos de comunicación y configuración de dispositivos. Este propósito se relaciona con el perfil de egreso del Ingeniero en Telemática el cual menciona que “Implementa y administra redes para garantizar las telecomunicaciones con seguridad”.

## 2. OBJETIVO GENERAL/COMPETENCIA

Desarrollar habilidades y conocimientos basados en métodos calificados y aprobados por instancias y organismos certificadores para llevar a cabo pruebas de estrés, accesos, control y fortaleza en un sistema de redes para evaluar el nivel de seguridad y dar propuestas de mejora. Todo esto bajo una política de buenas practicas y ética profesional.

- Entender las bases tecnológicas y protocolos de comunicación que determinan la manera en la que la información es transferida, almacenada y accedida al mismo.
- Realizar pruebas de seguridad y control bajo herramientas especializadas en un entorno controlado y seguro
- Establecer medidas de seguridad o mejoras en configuraciones para así evitar o minimizar el impacto negativo que pueda tener una red bajo alguna amenaza informática.
- Auditar una red de datos o servicio de red buscando identificar las características de aquellos protocolos en uso para evaluar la seguridad del mismo.
- Diseñar y proponer soluciones que fortalezcan la integridad de los datos, confiabilidad en la transmisión y autenticación con sus pares.

## 3. CAMPO DE APLICACIÓN PROFESIONAL DE LOS CONOCIMIENTOS

Aplicar los conocimientos y habilidades en las redes de datos tanto locales como remotas para determinar el nivel de seguridad establecido en los equipos y la integridad de la información que se almacena y fluye a través de la red loca.

## 4. SABERES:

| | |
|---|---|
| **Prácticos** | • Analiza las características de las redes de computadoras y evalua las vulnerabilidades presentadas y potenciales, así como sus posibles consecuencias.<br>• Realiza una propuesta de mejora que erradique o minimice las vulnerabilidades detectadas en la red. |
| **Teóricos** | • Relaciona el uso de los estándares y protocolos seguros con los servicios de red y el acceso a la conexión del cliente.<br>• Identifica los malos hábitos con el uso de las tecnologías que pueden comprometer la integridad de los datos de los usuarios.<br>• Aprende a formalizar reportes por escritos para dar detalles de lo analizado, puesto a prueba y consecuencias propensas a suceder. |
| **Formativos** | • Fortalecerá la redacción de documentos técnicos<br>• Fortalecerá las habilidades para expresar y defender sus ideas mediante la presentación y defensa de un proyecto de diseño<br>• Fortalecerá las habilidades de comunicación y trabajo en equipo |

## 5. CONTENIDO TEMÁTICO (TEÓRICO-PRÁCTICO)

- Introducción a la seguridad informática.
  - Panorama general.
  - Estructura de la seguridad de redes.
  - Conceptos básicos y aspectos legales.

- Seguridad en la red a nivel local.
  - Análisis y auditoría de trafico.
  - Identificación y clasificación de dispositivos.
  - Listado de usuarios activos.
  - Sondeo de servicios de red.
  - Patrones de trafico en una red local.

- Programas maliciosos.
  - Introducción al Malware.
  - Tipos de Malware.
  - Métodos de infección.
  - Estudio de Phishing.
  - Estudio de Ransomware.
  - Análisis de trafico malicioso.

- Estudio de técnicas de ataque/defensa en una red local.
  - Ataque tipo MITM.
  - Inanición de un servicio DHCP.
  - Inundación de paquetes tipo CDP.
  - Suplantación mediante protocolo STP.
  - Envenenamiento de tablas ARP.
  - Suplantación de gateway mediante protocolo HSRP.
  - Envenenamiento de tablas en el servicio DNS.
  - Ataque a contraseñas por diccionario y fuerza bruta.
  - Ejecución de ataques tipo DOSy DDOS.

- Redes encriptadas.
  - Darknet/Deepweb en la cultura popular.
  - Estructura y funcionamiento de una red “Onion Routing”.
  - Análisis de trafico en redes encriptadas.

## 6. ESTRATEGIAS DE ENSEÑANZA-APRENDIZAJE

- Clases Teóricas.
- Mesa de discusión y debate.
- Clases practicas en laboratorio.
- Trabajo Autónomo.

## 7. EVALUACIÓN DEL APRENDIZAJE

| 8.1. Evidencias de aprendizaje | 8.2. Criterios de desempeño |
|---|---|
| Ejercicio práctico de conceptos básicos. | Valoración de los factores de seguridad en la red de computadoras en casos académicos. |
| Muestras de tráfico aleatorio de red. | Se requiere el análisis exhaustivo y la interpretación del mismo. |
| Muestra de patrones de trafico. | Se requiere el análisis exhaustivo, la interpretación e identificación de posibles amenazas latentes. |
| Propuesta de configuración. | Se genere una propuesta con base al desarrollo de políticas y configuraciones que erradiquen o minimicen los fallos o amenazas detectadas. |

## 8. CALIFICACIÓN

| |
|---|
| Reportes de lecturas..... 20%<br>Actividades de laboratorio .....40%<br>Actividades Practicas .....30%<br>Actividad extracurricular .....5% |

## 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:<br>I. Estar inscrito en el plan de estudios y curso correspondiente, y<br>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:<br>I. Estar inscrito en el plan de estudios y curso correspondiente.<br>II. Haber pagado el arancel y presentar el comprobante correspondiente.<br>III. Tener un mínimo de asistencia del 65% a clases y actividades registradas durante el curso.<br>Se exceptúan de este caso las materias de orden práctico que requerirán la repetición del curso (Art. 23 RGEYPA). |

## 10. BIBLIOGRAFÍA

### BIBLIOGRAFÍA BÁSICA


- Justin Hutchens. (2014). Kali Linux Network Scanning Cookbook. Packt Publishing.
- Monika Agarwal. (2013). Metasploit Penetration testing Cookbook. Packt Publishing.
- Michael Hixon. (2018 )Kali Linux Network Scanning Cookbook. Packt Publishing.
- William Stallings (2014). Cryptography and Network Security. Pearson Publishing


### BIBLIOGRAFÍA COMPLEMENTARIA


- Jefrey Carr. (2012) Cyber Warfare. O'Reilly.


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

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

**Firma:** **Vo.Bo.**

**Presidente de Academia** **Jefe de Departamento**