SÍLABO

FACULTAD DE INGENIERÍA

SEPTIEMBRE 2023-FEBRERO 2024

NOMBRE DE LA ASIGNATURA	CÓDIGO:	20113

SEGURIDAD EN REDES - GRUPO: 1			
CARRERA	TELECOMUNICACIONES		
CICLO O SEMESTRE	SEPTIMO NIVEL	**EJE DE FORMACIÓN**	PROFESIONALES, PRAXIS PROFESIONAL
CRÉDITOS DE LA ASIGNATURA	2	**MODALIDAD:**	PRESENCIAL

CARGA HORARIA

COMPONENTES DEL APRENDIZAJE	Horas / Semana	Horas / Periodo Académico
APRENDIZAJE EN CONTACTO CON EL DOCENTE (ACD)	2.0	32.0
APRENDIZAJE PRÁCTICO EXPERIMENTAL - ASIGNATURA (APE/A)	2.0	32.0
APRENDIZAJE AUTÓNOMO (AA)	2.0	32.0
Total Horas:	6.0	96.0

PROFESOR(ES) RESPONSABLE(S):

ASTUDILLO SALINAS DARWIN FABIAN - (D.A.)	(fabian.astudillos@ucuenca.edu.ec)	PRINCIPAL

DESCRIPCIÓN DE LA ASIGNATURA:

Resumen descriptivo en torno al propósito, la estrategia metodológica y el contenido fundamental de la asignatura.

En esta asignatura, el estudiante aprenderá los principios fundamentales de la seguridad de redes al estudiar los ataques a la red. Los estudiantes aprenderán cómo funcionan esos ataques y cómo prevenirlos y detectarlos. El curso enfatiza "aprender haciendo" y requiere que los estudiantes realicen una serie de ejercicios de laboratorio. A través de estos laboratorios, los estudiantes
pueden mejorar su comprensión de los principios y pueden aplicar esos principios para resolver problemas reales.

La asignatura aporta al perfil de egreso formando profesionales cualificados en sistemas y redes de Telecomunicaciones con habilidad para trabajar en equipos multi e inter disciplinarios en los distintos sectores productivos. Formando profesionales que ayuden a mejorar la seguridad de las redes de las instituciones.

REQUISITOS DE LA ASIGNATURA

Esta asignatura no tiene co-requisitos

PRE-REQUISITOS	
Asignatura	**Código**
REDES DE COMPUTADORES	19323

OBJETIVO(S) DE LA ASIGNATURA:

Objetivos general y específicos de la asignatura en relación al Perfil de salida de la carrera.

Objetivo general: APRENDER Y APLICAR LOS PRINCIPIOS FUNDAMENTALES DE LA SEGURIDAD DE REDES

Objetivos específicos:

1. Conocer los principios de la seguridad de redes

2. Conocer cómo funcionan varios tipos de ataques

3. Describir y generalizar varias vulnerabilidades de red

4. Aplicar los principios de seguridad para resolver problemas

LOGRO DE LOS RESULTADOS DE APRENDIZAJE, INDICADOR(ES) Y ESTRATEGIA(S) DE EVALUACIÓN

Resultados o Logros de Aprendizaje (RdA's) de la Unidad de Organización Curricular (UOC) correspondiente, Indicadores y Estrategias de Evaluación de la Asignatura, tomando como referencia el Perfil de salida (PdS) y la Organización Curricular (OC) del Proyecto de Carrera (PdC).

RESULTADOS O LOGROS DE APRENDIZAJE	INDICADORES	ESTRATEGIAS DE EVALUACIÓN
RdA1. Ser capaz de explicar los principios de seguridad de redes	• Explica los principios de seguridad	• Exposición de prácticas • Reporte de prácticas
RdA2. Ser capaz de explicar cómo funcionan varios ataques	• Explica cómo funcionan varios ataques	• Exposición de prácticas • Reporte de prácticas
RdA3. Ser capaz de describir y generalizar varias vulnerabilidades de red	• Describe y generaliza varias vulnerabilidades de red	• Exposición de prácticas • Reporte de prácticas
RdA4. Ser capaz de detectar vulnerabilidades en la red	• Maneja las herramientas para implementar detección de vulnerabilidades en la red • Interpreta los resultados de salida de las herramientas de detección de vulnerabilidades	• Exposición de prácticas • Reporte de prácticas
RdA5. Ser capaz de aplicar principios de seguridad de redes para resolver problemas	• Aplica principios de seguridad para proponer y resolver problemas en cualquier institución	• Exposición de prácticas • Reporte de prácticas

CONTENIDOS, SESIONES Y ACTIVIDADES DE APRENDIZAJE

Título de la Unidad, sub -unidades, nro. de sesión y actividades para los componentes de aprendizaje.

SUB-UNIDADES	Nro. SESIÓN	COMPONENTE DE APRENDIZAJE	ACTIVIDADES DE APRENDIZAJE	
1. INTRODUCCIÓN A LA SEGURIDAD DE REDES INFORMÁTICAS				
1. Introducción 2. Asegurando una red de computadoras 3. Formas de protección (control de acceso, autenticación, confidencialidad, integridad, y no repudiación) 4. Estándares de seguridad	1	APRENDIZAJE EN CONTACTO CON EL DOCENTE (ACD)	Exposición dialogada	2 horas
		APRENDIZAJE PRÁCTICO EXPERIMENTAL - ASIGNATURA (APE/A)	Práctica dirigida	1 horas
		APRENDIZAJE AUTÓNOMO (AA)	Revisión de literatura y videos	1 horas
2. PROBLEMAS Y DESAFÍOS DE LA SEGURIDAD DE REDES INFORMÁTICAS				
1. Amenazas de seguridad y motivos de amenazas a las redes informáticas 2. Introducción a las vulnerabilidades de las redes informáticas 3. Delitos cibernéticos y piratas informáticos 4. Scripting y seguridad en redes informáticas y navegadores web 5. Evaluación, análisis y garantía de seguridad	2	APRENDIZAJE EN CONTACTO CON EL DOCENTE (ACD)	Exposición dialogada	4 horas
		APRENDIZAJE PRÁCTICO EXPERIMENTAL - ASIGNATURA (APE/A)	Práctica dirigida	1 horas
		APRENDIZAJE AUTÓNOMO (AA)	Revisión de literatura y videos	1 horas
3. DETECCIÓN Y PREVENCIÓN DE INTRUSIONES EN EL SISTEMA				

SUB-UNIDADES	Nro. SESIÓN	COMPONENTE DE APRENDIZAJE	ACTIVIDADES DE APRENDIZAJE	
1. Detección de intrusos 2. Sistemas de detección de intrusos (IDS) 3. Tipos de sistemas de detección de intrusos 4. Respuesta a una intrusión en el sistema 5. Desafíos en los sistemas de detección de intrusos	12	APRENDIZAJE EN CONTACTO CON EL DOCENTE (ACD)	Exposición dialogada	4 horas
		APRENDIZAJE PRÁCTICO EXPERIMENTAL - ASIGNATURA (APE/A)	Práctica	4 horas
		APRENDIZAJE AUTÓNOMO (AA)	Práctica	2 horas
4. INTRODUCCIÓN A PENTESTING				
1. Visión general 2. Instalando y usando un sistema para realizar pentesting 3. Analizando los reportes del sistema 4. Redactando un informe del pentesting	13	APRENDIZAJE EN CONTACTO CON EL DOCENTE (ACD)	Exposición dialogada	4 horas
		APRENDIZAJE PRÁCTICO EXPERIMENTAL - ASIGNATURA (APE/A)	Práctica	4 horas
		APRENDIZAJE AUTÓNOMO (AA)	Práctica	4 horas
5. ENCRIPTACIÓN DE CLAVE SECRETA				
1. Algoritmos de encriptación DES y AES 2. Modos de encriptación 3. Vector de inicialización y errores comunes	3	APRENDIZAJE EN CONTACTO CON EL DOCENTE (ACD)	Exposición dialogada	2 horas
		APRENDIZAJE AUTÓNOMO (AA)	Práctica: Laboratorio de encriptación de clave secreta	2 horas
4. Programación usando APIs criptográficas	4	APRENDIZAJE PRÁCTICO EXPERIMENTAL - ASIGNATURA (APE/A)	Práctica: Laboratorio de encriptación de clave secreta	2 horas
6. FUNCIONES HASH DE UNA VÍA				
1. Conceptos y propiedades 2. Algoritmos y programas 3. Aplicaciones de las funciones hash de una vía 4. Message Authentication Code (MAC) 5. Ataques de colisiones hash	4	APRENDIZAJE EN CONTACTO CON EL DOCENTE (ACD)	Exposición dialogada	2 horas
		APRENDIZAJE PRÁCTICO EXPERIMENTAL - ASIGNATURA (APE/A)	Práctica: Laboratorio de ataque de colisión MD5	2 horas
		APRENDIZAJE AUTÓNOMO (AA)	Práctica: Laboratorio de ataque de colisión MD5	2 horas
7. CRIPTOGRAFÍA DE CLAVE PÚBLICA				
1. Intercambio de claves Diffie-Hellman 2. Al algoritmo RSA 3. Usando OpenSSL para realizar operaciones RSA 4. Firma digital 5. Programación usando las APIs de criptografía de clave pública 6. Aplicaciones	5	APRENDIZAJE EN CONTACTO CON EL DOCENTE (ACD)	Exposición dialogada	2 horas
		APRENDIZAJE PRÁCTICO EXPERIMENTAL - ASIGNATURA (APE/A)	Práctica: Laboratorio de firma y cifrado de clave pública RSA	2 horas
		APRENDIZAJE AUTÓNOMO (AA)	Práctica: Laboratorio de firma y cifrado de clave pública RSA	2 horas
8. DETECCIÓN Y SUPLANTACIÓN DE PAQUETES				

SUB-UNIDADES	Nro. SESIÓN	COMPONENTE DE APRENDIZAJE	ACTIVIDADES DE APRENDIZAJE	
1. ¿Cómo son recibidos los paquetes? 2. Sniffing de paquetes 3. Spoofing de paquetes 4. Sniffing y spoofing usando python y scapy	6	APRENDIZAJE EN CONTACTO CON EL DOCENTE (ACD)	Exposición dialogada	2 horas
		APRENDIZAJE PRÁCTICO EXPERIMENTAL - ASIGNATURA (APE/A)	Práctica: Laboratorio de Sniffing y Spoofing de paquetes Práctica: Laboratorio de ataques de envenenamiento de caché ARP Práctica: Laboratorio de ataques de redireccionamiento ICMP	2 horas 2 horas 2 horas
		APRENDIZAJE AUTÓNOMO (AA)	Práctica: Laboratorio de Sniffing y Spoofing de paquetes Práctica: Laboratorio de ataques de envenenamiento de caché ARP Práctica: Laboratorio de ataques de redireccionamiento ICMP	2 horas 2 horas 2 horas
9. ATAQUES AL PROTOCOLO TCP				
1. ¿Cómo trabaja el protocolo TCP? 2. Ataque SYN flooding 3. Ataque TCP reset 4. Ataque de Hijacking de una sesión TCP	2	APRENDIZAJE EN CONTACTO CON EL DOCENTE (ACD)	Exposición dialogada	2 horas
		APRENDIZAJE PRÁCTICO EXPERIMENTAL - ASIGNATURA (APE/A)	Práctica: Laboratorio de ataque a TCP/IP	2 horas
		APRENDIZAJE AUTÓNOMO (AA)	Práctica: Laboratorio de ataque a TCP/IP	2 horas
10. FIREWALLS				
1. Tipos de Firewalls 2. Implementando un Firewall simple usando netfilter 3. Netfilter 4. El Firewall iptables en Linux 5. Evadiendo Firewalls	7	APRENDIZAJE EN CONTACTO CON EL DOCENTE (ACD)	Exposición dialogada	2 horas
		APRENDIZAJE PRÁCTICO EXPERIMENTAL - ASIGNATURA (APE/A)	Práctica: Laboratorio de exploración de Firewall	2 horas
		APRENDIZAJE AUTÓNOMO (AA)	Práctica: Laboratorio de exploración de Firewall	2 horas
11. SISTEMA DE NOMBRES DE DOMINIO (DNS) Y ATAQUES				
1. Configurando un servidor DNS y un ambiente de experimentación 2. Construyendo una solicitud y respuesta de DNS usando scapy 3. Ataques de DNS	9	APRENDIZAJE EN CONTACTO CON EL DOCENTE (ACD)	Exposición dialogada Práctica: Laboratorio de ataque de rebinding DNS	2 horas 2 horas
		APRENDIZAJE PRÁCTICO EXPERIMENTAL - ASIGNATURA (APE/A)	Práctica: Laboratorio de ataque de un DNS local	2 horas
		APRENDIZAJE AUTÓNOMO (AA)	Práctica: Laboratorio de ataque de un DNS local Práctica: Laboratorio de ataque de rebinding DNS	2 horas 2 horas
12. REDES PRIVADAS VIRTUALES				

SUB-UNIDADES	Nro. SESIÓN	COMPONENTE DE APRENDIZAJE	ACTIVIDADES DE APRENDIZAJE	
1. ¿Cómo trabaja una VPN? 2. Construyendo una VPN 3. Configurando una VPN 4. Probando una VPN 5. Usando VPNs para bypasear los Firewalls de salida	10	APRENDIZAJE EN CONTACTO CON EL DOCENTE (ACD)	Exposición dialogada	2 horas
		APRENDIZAJE PRÁCTICO EXPERIMENTAL - ASIGNATURA (APE/A)	Práctica: Laboratorio de tunneling VPN Práctica: Laboratorio de VPN	2 horas 2 horas
		APRENDIZAJE AUTÓNOMO (AA)	Práctica: Laboratorio de tunneling VPN Práctica: Laboratorio de VPN	2 horas 2 horas

APRENDIZAJE EN CONTACTO CON EL DOCENTE (ACD)	32 horas
APRENDIZAJE PRÁCTICO EXPERIMENTAL - ASIGNATURA (APE/A)	32 horas
APRENDIZAJE AUTÓNOMO (AA)	32 horas
Total Planificación:	96 horas

RECURSOS O MEDIOS PARA EL APRENDIZAJE

Equipos, materiales, instrumentos tecnológicos, reactivos, entre otros, que serán utilizados durante el desarrollo de la asignatura.

- Máquina virtual (Virtual Box)
- PC/Laptop
- Contenedor (docker)
- Sistema Operativo Linux (Ubuntu 20.04)
- Herramientas de videoconferencia (zoom)

CRITERIOS PARA LA ACREDITACIÓN DE LA ASIGNATURA

Parámetros de acreditación, tomando como referencia los Resultados de Aprendizaje (RdA's), indicadores y criterios de evaluación planteados y en base a la normativa de evaluación y calificaciones vigente en la Universidad de Cuenca y Consejo de Educación Superior (CES).

CRITERIO GENERAL DE ACREDITACIÓN	PUNTAJE
EXAMENES	50
PRACTICAS	50
TOTAL:	100

	DETALLE DE CRITERIOS DE ACREDITACIÓN	PUNTAJE / CRITERIO GENERAL	
C94	APROVECHAMIENTO I		
	Prácticas	25	PRACTICAS
C95	INTERCICLO		
	Proyecto 1	20	EXAMENES
C96	APROVECHAMIENTO II		
	Prácticas	25	PRACTICAS
C97	FINAL		
	Proyecto 2	30	EXAMENES
C98	SUSPENSIÓN		
	Total:	100	

TEXTOS U OTRAS REFERENCIAS REQUERIDAS PARA EL APRENDIZAJE DE LA ASIGNATURA

Libros, revistas, bases digitales, periódicos, direcciones de Internet y demás fuentes de información, pertinentes y actuales.

BÁSICA

1. Du, W. (2019). Computer & internet security: a hands-on approach. Independently published.

2. Kizza, J. M., Kizza, & Wheeler. (2013). Guide to computer network security (Vol. 8). Heidelberg, Germany: Springer.

COMPLEMENTARIA

Esta asignatura no tiene bibliografía complementaria

Docente: ASTUDILLO SALINAS DARWIN FABIAN

Director: ARAUJO PACHECO ALCIDES FABIAN

Finalizado: 15/9/2023

Publicado: 17/9/2023