



Universidad Nacional de Ingeniería (UNI)

Escuela Profesional de

Ciberseguridad

Sílabo 2024-II

1. CURSO

CY241. Seguridad de Conexiones (Obligatorio)

2. INFORMACIÓN GENERAL

2.1 Curso	:	CY241. Seguridad de Conexiones
2.2 Semestre	:	8 ^{vo} Semestre.
2.3 Créditos	:	3
2.4 horas	:	2 HT; 2 HP;
2.5 Duración del periodo	:	16 semanas
2.6 Condición	:	Obligatorio
2.7 Modalidad de aprendizaje	:	Presencial
2.8 Prerrequisitos	:	CS3I1. Seguridad en Computación. (7 ^{mo} Sem)

3. PROFESORES

Atención previa coordinación con el profesor

4. INTRODUCCIÓN AL CURSO

Este curso se centra en la seguridad de las conexiones en sistemas informáticos, abordando tanto las conexiones físicas como las lógicas. Se examinan protocolos, arquitecturas, vulnerabilidades y mejores prácticas para asegurar la comunicación entre componentes y sistemas, capacitando a los estudiantes para diseñar e implementar soluciones de seguridad de conexiones robustas.

5. OBJETIVOS

- Comprender los principios de seguridad de las conexiones físicas y lógicas.
- Analizar protocolos y arquitecturas de red desde una perspectiva de seguridad.
- Implementar medidas para proteger las conexiones de ataques y garantizar la integridad y confidencialidad de la información transmitida.

6. RESULTADOS DEL ESTUDIANTE

3) ()

5) ()

6) Aplicar principios y prácticas de seguridad para mantener las operaciones en presencia de riesgos y amenazas.()

7. TEMAS

Unidad 1: Medios físicos (8 horas)	
Resultados esperados: 3,6	
Temas	Objetivos de Aprendizaje
<ul style="list-style-type: none"> • Transmisión en un medio. <ul style="list-style-type: none"> – Señales en coaxial, par trenzado, fibra óptica y aire. • Medios compartidos y punto a punto <ul style="list-style-type: none"> – Analiza las características comunicativas de los medios. • Compartiendo modelos <ul style="list-style-type: none"> – Describe los diversos esquemas para compartir medios entre múltiples clientes. Por ejemplo: direccionamiento MAC 802.1 y PPP. • Tecnologías comunes <ul style="list-style-type: none"> – examina varias implementaciones de los modelos cubiertos anteriormente. IEEE 802.3 (Ethernet), IEEE 802.11 (Wi-Fi), IEEE 802.16 (banda ancha inalámbrica fija). 	<ul style="list-style-type: none"> • Discuta la necesidad de modelos y arquitecturas comunes para describir sistemas [Usar] • Describir un modelo de sistemas que consta de componentes e interfaces para conexiones [Usar] • Explique por qué un componente requiere al menos una interfaz [Usar] • Enumere varios estándares que definen modelos que constan de sistemas de componentes e interfaces [Usar] • Describir los componentes e interfaces de un estándar de red proporcionado [Usar]
Lecturas : [Kurose2016]	

Unidad 2: Interfaces físicas y conectores (7 horas)	
Resultados esperados: 6	
Temas	Objetivos de Aprendizaje
<ul style="list-style-type: none"> • Características y materiales del hardware. <ul style="list-style-type: none"> – presenta las características de conexión de varios medios y los requisitos para las conexiones físicas. • Estándares <ul style="list-style-type: none"> – examina varios estándares para conectores • Conectores comunes <ul style="list-style-type: none"> – RJ 11, Rj 45, ST, SC, MTRJ, SFF ISA Bus, etc. 	<ul style="list-style-type: none"> • Discuta la necesidad de modelos y arquitecturas comunes para describir sistemas [Usar] • Describir un modelo de sistemas que consta de componentes e interfaces para conexiones [Usar] • Explique por qué un componente requiere al menos una interfaz [Usar] • Enumere varios estándares que definen modelos que constan de sistemas de componentes e interfaces [Usar] • Describir los componentes e interfaces de un estándar de red proporcionado [Usar]
Lecturas : [Tanenbaum2010]	

Unidad 3: (8 horas)	
Resultados esperados: 6	
Temas	Objetivos de Aprendizaje
<ul style="list-style-type: none"> • Arquitecturas estándar <ul style="list-style-type: none"> – Introducir la idea de arquitecturas estándar y las ventajas de la estandarización. – La historia de las placas base de PC podría usarse como ejemplo que muestra la evolución desde ISA hasta PCI y más allá. – La capacidad de las tarjetas para agregar funcionalidad sin cambiar la arquitectura base es importante – Agregar puertos Ethernet multipuerto en una tarjeta permite que una PC se convierta en un enrutador • Estándares de interfaz de hardware <ul style="list-style-type: none"> – Este tema presenta varios estándares de interfaz de hardware comenzando con el diseño de paquetes IC, pasando por buses como ISA y PCI para plataformas de integración y hasta estándares de redes como IEEE 802.3. • Arquitecturas comunes <ul style="list-style-type: none"> – Este tema debe examinar las tecnologías actuales que enfrentarán los estudiantes (chips de CPU, placa base de PC, estándares Ethernet). 	<ul style="list-style-type: none"> • Explique por qué un dispositivo de hardware siempre se modela como un componente físico [Usar] • Enumere varios ejemplos de interfaces de componentes físicos con sus vulnerabilidades asociadas [Usar] • Describir un exploit para una vulnerabilidad de una interfaz física proporcionada [Usar]
Lecturas : [Stallings2018]	

Unidad 4: (8 horas)	
Resultados esperados: 3,6	
Temas	Objetivos de Aprendizaje
<ul style="list-style-type: none"> • Conceptos generales <ul style="list-style-type: none"> – Debe comenzar con la idea de un proceso en un sistema operativo y luego presentar las diversas arquitecturas para ejecutar procesos y permitir su comunicación. – Multiprocesamiento simétrico y memoria compartida, basado en red con un modelo de comunicación entre procesos. • World Wide Web <ul style="list-style-type: none"> – cubre el protocolo HTTP/HTTPS y demuestra cómo es un ejemplo de un estándar de procesamiento distribuido. • La Internet <ul style="list-style-type: none"> – Cubre la evolución de Internet como plataforma de procesamiento distribuido – Los alumnos deben tener claro por qué la red mundial e Internet no son equivalentes. • Protocolos y capas <ul style="list-style-type: none"> – cubre el modelo OSI de 7 capas junto con el modelo de Internet de 5 capas y los compara como un ejemplo de encapsulación y capas para permitir servicios que se basan entre sí. • Computación de alto rendimiento (supercomputadoras) <ul style="list-style-type: none"> – presenta HPC y casos de uso que distinguen HPC de Internet estándar. • Hipervisores e implementaciones de computación en la nube. <ul style="list-style-type: none"> – Introduce los conceptos de proporcionar infraestructura como servicio (IaaS), software como servicio (SaaS), plataforma como servicio (PaaS) y todos sus aspectos relevantes para los alumnos. • Vulnerabilidades y ejemplos de exploits <ul style="list-style-type: none"> – examina las superficies de ataque de los diversos modelos de computación distribuida enfatizando el hecho de que cada interfaz introduce vulnerabilidades potenciales. – Se deben cubrir el hipervisor, las redes virtuales, la red física y la comunicación entre procesos. 	<ul style="list-style-type: none"> • Explique por qué un dispositivo de hardware siempre se modela como un componente físico [Usar] • Enumere varios ejemplos de interfaces de componentes físicos con sus vulnerabilidades asociadas [Usar] • Describir un exploit para una vulnerabilidad de una interfaz física proporcionada [Usar]
Lecturas : [Coulouris2011]	

Unidad 5: Red de arquitectura (9 horas)	
Resultados esperados: 3,6	
Temas	Objetivos de Aprendizaje
<ul style="list-style-type: none"> • Conceptos generales <ul style="list-style-type: none"> – debe cubrir las ideas de nodos y bordes con los nombres de las distintas topologías y las características de transmisión de las topologías • Arquitecturas comunes <ul style="list-style-type: none"> – Cubre la arquitectura de red IEEE 802 y cómo se nombran las distintas redes en función de las características físicas (LAN, MAN, etc.). • Reenvío <ul style="list-style-type: none"> – cubre el reenvío de paquetes en general. Dado que ahora se utiliza silicón de conmutación similar en enrutadores y conmutadores, y SDN trata el reenvío por separado de la construcción de la tabla de reenvío, este es su propio tema. • Enrutamiento <ul style="list-style-type: none"> – cubre algoritmos de enrutamiento y explica cómo se crean tablas de reenvío utilizando algoritmos de análisis de gráficos, como estado de enlace y vector de distancia. • Conmutación/puente <ul style="list-style-type: none"> – Este tema cubre algoritmos de aprendizaje y puentes IEEE 802.1 junto con el protocolo Spanning Tree y su relación con el enrutamiento. Actualmente no está claro cómo evolucionará este tema con el reemplazo de STP por la aparición de Trill y STP. • Tendencias emergentes <ul style="list-style-type: none"> – Cubre las tecnologías emergentes y su impacto a medida que surgen. Actualmente, el contenido sería el impacto de SDN y la adición de enrutamiento a la capa 2 con puentes de aprendizaje mejorados. Esto está evolucionando rápidamente • Virtualización y arquitectura de hipervisor virtual. <ul style="list-style-type: none"> – Arquitectura de red Virtualización y arquitectura de hipervisor virtual. 	<ul style="list-style-type: none"> • Explique por qué cada interfaz física tiene un componente de software correspondiente para proporcionar una interfaz de software correspondiente [Usar] • Explique cómo se organizan los componentes de software para representar capas lógicas en un modelo estándar [Usar] • Analice cómo se puede ver el modelo de cinco capas de Internet como componentes de software e interfaces que representan niveles de servicios encapsulados por servicios de nivel inferior [Usar] • Analice cómo TCP/IP como servicio se representa mediante diferentes interfaces en diferentes sistemas de software [Usar]
Lecturas : [Peterson2011]	

Unidad 6: Implementaciones de red (8 horas)	
Resultados esperados: 3,6	
Temas	Objetivos de Aprendizaje
<ul style="list-style-type: none"> • Redes IEEE 802/ISO <ul style="list-style-type: none"> – Este tema es una inmersión profunda en los estándares ISO. Se espera que este tema se introduzca en otros lugares. • Redes IETF y TCP/IP <ul style="list-style-type: none"> – Esta es una inmersión profunda en la infraestructura básica de Internet y TCP. • Protocolos prácticos de integración y pegado. <ul style="list-style-type: none"> – Analiza el problema de la integración de tecnologías mediante la implementación de lo que podría llamarse cuñas de interfaz o código adhesivo – ARP es el ejemplo obvio – Se requería un mecanismo para asignar las direcciones IP del modelo de interconexión de redes del IETF a las direcciones MAC de las redes subyacentes. – ARP es el pegamento. De manera similar, Infiniband necesita una cuña para transportar el tráfico IP. • Vulnerabilidades y ejemplos de exploits <ul style="list-style-type: none"> – debe proporcionar ejemplos de las tecnologías importantes para el programa. – Si se elige ARP como ejemplo, el envenenamiento de ARP como adjunto MitM funciona bien. – USB y otras conexiones en serie también podrían proporcionar ejemplos. 	<ul style="list-style-type: none"> • Explique cómo se pueden entender los ataques de conexión en términos de ataques a las interfaces de componentes de software [Usar] • Describir cómo una interfaz estándar específica podría exponer vulnerabilidades en un componente de software que implementa la interfaz [Usar] • Describa cómo una implementación podría protegerse de una vulnerabilidad específica en una interfaz estándar específica [Usar]
Lecturas : [Stevens2011]	

8. PLAN DE TRABAJO

8.1 Metodología

Se fomenta la participación individual y en equipo para exponer sus ideas, motivándolos con puntos adicionales en las diferentes etapas de la evaluación del curso.

8.2 Sesiones Teóricas

Las sesiones de teoría se llevan a cabo en clases magistrales donde se realizarán actividades que propicien un aprendizaje activo, con dinámicas que permitan a los estudiantes interiorizar los conceptos.

8.3 Sesiones Prácticas

Las sesiones prácticas se llevan en clase donde se desarrollan una serie de ejercicios y/o conceptos prácticos mediante planteamiento de problemas, la resolución de problemas, ejercicios puntuales y/o en contextos aplicativos.

9. SISTEMA DE EVALUACIÓN

***** EVALUATION MISSING *****

10. BIBLIOGRAFÍA BÁSICA