National University of Engineering (UNI)
School of Cybersecurity
Syllabus 2024-II

1. COURSE

CY351. Advanced System Security (Mandatory)

2. GENERAL INFORMATION

2.1 Course	:	CY351. Advanced System Security
2.2 Semester	:	10^{th} Semester.
2.3 Credits	:	3
2.4 Horas	:	2 HT; 2 HP;
2.5 Duration of the period	:	16 weeks
2.6 Type of course	:	Mandatory
2.7 Learning modality	:	Face to face
2.8 Prerrequisites	:	• CY231. Component Security. (9^{th} Sem) • CY251. System Security. (7^{th} Sem)

3. PROFESSORS

Meetings after coordination with the professor

4. INTRODUCTION TO THE COURSE

This advanced course expands on system security knowledge, delving deeper into risk analysis, vulnerability mitigation, and the design of robust security solutions for complex systems. Topics covered include cloud security, industrial control systems, advanced forensic analysis, and formal verification methods.

5. GOALS

- Analyze and mitigate security risks in complex systems, including cloud environments and critical infrastructure.
- Apply advanced forensic analysis techniques to investigate security incidents.
- Design and implement robust security solutions using formal verification methods.

6. COMPETENCES

1) ()

5) ()

6) Apply security principles and practices to maintain operations in the presence of risks and threats.()

7. TOPICS

Unit 1: Pruebas del sistema (10 hours)	
Competences Expected: 1,6	
Topics	**Learning Outcomes**
• Requisitos de validación – Describe metodologías para mostrar que los requisitos cumplen con los objetivos. • Validación de la composición de los componentes. – Este tema cubre cómo probar un sistema en su conjunto. • Pruebas unitarias versus de sistema T – Este tema cubre en qué se diferencian las pruebas del sistema de las pruebas de componentes y conexiones. • Verificación formal de sistemas. – Este tema cubre lenguajes, demostradores de teoremas y descomposición jerárquica.	• Describe qué es una prueba de penetración y por qué es valiosa [Usar] • Analice cómo documentar una prueba que revele una vulnerabilidad [Usar] • Discuta la importancia de validar los requisitos [Usar]
Readings : [**Pezze2008**]	

Unit 2: Arquitecturas de sistemas comunes (14 hours)	
Competences Expected: 1,6	
Topics	**Learning Outcomes**
• Máquinas virtuales – Cubre hipervisores, virtualización de discos y memoria y el uso de máquinas virtuales en seguridad. • Sistemas de control industriales – Este tema incluye SCADA • Internet de las cosas (IoT) – Este tema incluye ejemplos como refrigeradores y sensores. • Sistemas integrados – Este tema incluye ejemplos como sistemas en • Sistemas móviles – Este tema incluye ejemplos como computadoras portátiles y teléfonos inteligentes. • Sistemas autónomos – Este tema incluye ejemplos como robots y vehículos aéreos no tripulados que no requieren control humano. • Sistema de propósito general – Este tema incluye ejemplos como computadoras de escritorio, portátiles y mainframes.	• Analice la importancia de documentar la instalación y configuración adecuadas de un sistema [Usar] • Ser capaz de escribir documentación sobre intrusiones de red y host [Usar] • Ser capaz de explicar las implicaciones de seguridad de una documentación poco clara o incompleta del funcionamiento del sistema [Usar]
Readings : [**Stallings2018**]	

Unit 3: Control de sistema (12 hours)

Competences Expected: 1,6

Topics	Learning Outcomes
• control de acceso – Este tema se centra en controlar el acceso a los recursos y la integridad de los controles, en lugar de controlar el acceso a los datos, lo que se trata en el área de conocimiento de Seguridad de datos. • Modelos de autorización – Cubre la gestión de la autorización en muchos sistemas y la distinción entre autenticación y autorización. • Detección de intrusiones – Cubre anomalías, uso indebido (basado en reglas, basado en firmas) y técnicas basadas en especificaciones. • Ataques – Este tema cubre modelos de ataque (como árboles y gráficos de ataque) y ataques específicos. • Defensas – Este tema incluye ejemplos como ASLR, salto de IP y tolerancia a intrusiones. • Auditoría – cubre el registro, el análisis de registros y la relación con la detección de intrusiones • malware – Ejemplos como virus informáticos, gusanos, ransomware y otras formas de malware. • Modelos de vulnerabilidades – Ejemplos como RISOS y PA; y enumeraciones como CVE y CWE. • Pruebas de penetración – Cubre la Metodología de Hipótesis de Fallas y otras formas (ISSAF, OSSTMM, GISTA, PTES, etc.). • forense – Este tema se centra en los requisitos del sistema para análisis forense. • Recuperación, resiliencia – Este tema incluye mecanismos de disponibilidad.	• Describir una lista de control de acceso [Usar] • Describir el control de acceso físico y lógico, compararlos y contrastarlos [Usar] • Distinga entre autorización y autenticación [Usar]

Readings : [**Bishop2002**]

Unit 4: Continuidad del negocio, recuperación ante desastres y gestión de incidentes (12 hours)	
Competences Expected: 1,6	
Topics	**Learning Outcomes**
• Respuesta a incidentes – incluye la creación y el uso de los planes IR, la organización de los planes, las ocasiones para revisar/reescribir los planes y el examen de los planes saneados. • Recuperación ante desastres – incluye la creación y el uso de los planes de recuperación ante desastres, la organización de los planes, las ocasiones para revisar/reescribir los planes y el examen de los planes saneados. – Se deben brindar oportunidades a los estudiantes para que escriban planes reales o basados en casos para adquirir algo de experiencia. • Continuidad del negocio – la creación y uso de los planos BC – organizacion de los planes – Ocasiones para revisar/reescribir planes. – y examen de planos sanitizados – Se deben brindar oportunidades a los estudiantes para que escriban planes reales o basados en casos para adquirir algo de experiencia.	• Explicar la planificación organizacional estratégica para la ciberseguridad y su relación con la planificación estratégica de TI y para toda la organización [Usar] • Identificar las partes interesadas clave de la organización y sus roles [Usar] • Describir los componentes principales de la planificación de la implementación del sistema de ciberseguridad [Usar]
Readings : [**NIST-SP800-61r2**]	

8. WORKPLAN

8.1 Methodology

Individual and team participation is encouraged to present their ideas, motivating them with additional points in the different stages of the course evaluation.

8.2 Theory Sessions

The theory sessions are held in master classes with activities including active learning and roleplay to allow students to internalize the concepts.

8.3 Practical Sessions

The practical sessions are held in class where a series of exercises and/or practical concepts are developed through problem solving, problem solving, specific exercises and/or in application contexts.

9. EVALUATION SYSTEM

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

10. BASIC BIBLIOGRAPHY