Sistemas de Ciberdefensa

Curso Académico: (2022 / 2023) **Fecha de revisión: 19-01-2023**

Departamento asignado a la asignatura: Departamento de Informática

Coordinador/a: PASTRANA PORTILLO, SERGIO

Tipo: Obligatoria Créditos ECTS : 6.0

Curso : 1 Cuatrimestre : 1

OBJETIVOS

Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación.

Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.

Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.

Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades.

Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando.

Concebir, diseñar, poner en práctica y mantener un sistema global de Ciberdefensa en un contexto definido.

Elaborar concisa, clara y razonadamente documentos, planes y proyectos de trabajo en el ámbito de la Ciberseguridad.

Conocer la normativa técnica y las disposiciones legales de aplicación en la materia de ciberseguridad, sus implicaciones en el diseño de sistemas y en la aplicación de herramientas de seguridad.

Analizar sistemas para encontrar evidencias de ataques en los mismos y adoptar las medidas precisas para mantener la cadena de custodia de dichas evidencias.

Aplicar los servicios, mecanismos y protocolos de seguridad oportunos en un caso concreto.

Diseñar y evaluar arquitecturas de seguridad de sistemas y redes.

Conocer y aplicar los mecanismos de cifrado y esteganografiado pertinentes para proteger los datos residentes en un sistema o en tránsito por una red.

Analizar los riesgos de la introducción de dispositivos personales en un entorno profesional. Conocer y aplicar las medidas para controlar dichos riesgos.

RESULTADOS DE APRENDIZAJE

Esta asignatura contribuye a los siguientes resultados de aprendizaje:

Diseñar estrategias de sensorización para distintos elementos de un sistema en red y analizar los eventos observados en un ataque concreto para distinguir cuáles son de interés.

Dado un sistema bajo distintos tipos de ataques, ser capaz de detectar las características de la mayoría de dichos ataques y señalar las fuentes más probables.

Identificado un ataque y su fuente, proponer las contramedidas para contrarrestarlo explicando la

medida de su eficacia. Evaluar estrategias de zonificación de redes y diseñar políticas de filtrado de tráfico.

Diseñar y evaluar medidas apropiadas para la identificación y autenticación de usuarios, así como la gestión de las identidades y las autorizaciones asociadas.

DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

Sistemas de Ciberdefensa:
1. Introducción a los Sistemas de Ciberdefensa

2. Sensores locales: Auditoría y análisis de eventos
   2.1. Gestión de usuarios y accesos
   2.2. Análisis de logs de seguridad

3. Cortafuegos y segmentación de redes
   3.1. Fundamentos de filtrado de tráfico
   3.2. Tipos de cortafuegos
   3.3. Segmentación de redes

4. Sistemas de Detección y Prevención de Ataques
   4.1. Detección de firmas de ataque
   4.2. Detección de anomalías
   4.3. Respuesta automática a intentos de intrusión

5. Sistemas de Gestión de Eventos e Información de Seguridad (SIEM)
   5.1. Conceptos y arquitecturas de SIEMs
   5.2. Reglas de agregación y correlación
   5.3. Arquitecturas distribuidas de sensores de detección
   5.4. Estrategias de sensorización de redes

ACTIVIDADES FORMATIVAS, METODOLOGÍA A UTILIZAR Y RÉGIMEN DE TUTORÍAS

Actividades Formativas:

-- Clase teórica
-- Clases prácticas
-- Prácticas de laboratorio
-- Tutorías
-- Trabajo en grupo

Metodologías Docentes:

-- Exposiciones en clase del profesor con soporte de medios informáticos y audiovisuales, en las que se desarrollan los conceptos principales de la materia y se proporciona la bibliografía para complementar el aprendizaje de los alumnos.

-- Lectura crítica de textos recomendados por el profesor de la asignatura: Artículos de prensa, informes, manuales y/o artículos académicos, bien para su posterior discusión en clase, bien para ampliar y consolidar los conocimientos de la asignatura.

-- Resolución de casos prácticos, problemas, etc. planteados por el profesor de manera individual o en grupo.

-- Exposición y discusión en clase, bajo la moderación del profesor de temas relacionados con el contenido de la materia, así como de casos prácticos.

-- Elaboración de trabajos e informes de manera individual o en grupo.

SISTEMA DE EVALUACIÓN

El sistema de evaluación se basa en la realización de prácticas en grupo, además de un examen final individual. Específicamente, la evaluación de la asignatura se desglosa en:
- Evaluación continua (60% de la nota final).
- Examen final (40% de la nota final). Se requiere una nota mínima de 3,5 puntos sobre 10.

La evaluación en la convocatoria extraordinaria se realizará con un único examen con peso del 100%. Este examen incluirá preguntas prácticas.

Peso porcentual del Examen Final:	40
Peso porcentual del resto de la evaluación:	60

BIBLIOGRAFÍA BÁSICA

- P.W. Singer Cybersecurity and Cyberwar: What Everyone Needs to Know, Oxford University Press , 2014

- Anton A. Chuvakin, Kevin J. Schmidt Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management, Syngress, 2012
- Brian Caswell, Jay Beale, Andrew Baker Snort Intrusion Detection and Prevention Toolkit, Syngress, 2007

- Chris Sanders, Jason Smith Applied Network Security Monitoring: Collection, Detection, and Analysis, Syngress, 2013
- David R. Miller , Shon Harris, Allen Harper, Stephen VanDyke, Chris Blask Security Information and Event Management (SIEM) Implementation , Network Pro Library, 2010
- Dobromir Todorov Mechanics of User Identification and Authentication: Fundamentals of Identity Management , Auerbach Publications , 2007
- J. Michael Stewart Network Security, Firewalls And Vpns, Jones & Bartlett Learning, 2013

- Richard Bejtlich The Practice of Network Security Monitoring: Understanding Incident Detection and Response, No Starch Press, 2013
- Timur Mehmet Firewall Hacking Secrets For Security Professionals, HackerStorm.com Publishing, 2013