Amenazas persistentes y fugas de Información

Curso Académico: (2024 / 2025) **Fecha de revisión: 23-04-2024**

Departamento asignado a la asignatura: Departamento de Informática

Coordinador/a: FUENTES GARCIA ROMERO DE TEJADA, JOSE MARIA DE

Tipo: Optativa Créditos ECTS : 3.0

Curso : 1 Cuatrimestre : 2

REQUISITOS (ASIGNATURAS O MATERIAS CUYO CONOCIMIENTO SE PRESUPONE)

No procede.

OBJETIVOS

COMPETENCIAS
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.

Comprender y aplicar métodos y técnicas de investigación de ciberataques a una instalación específica.

Analizar y detectar anomalías y firmas de ataques en los sistemas y redes.

Analizar y detectar técnicas de ocultación de ataques a sistemas y redes.

Conocer las tendencias actuales en técnicas de ciberataque y las experiencias aprendidas en casos reales.

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

RESULTADOS DE APRENDIZAJE:
Con respecto a los resultados del aprendizaje, la asignatura contribuye a los siguientes:

Conocido el tipo de información y los mecanismos de defensa desplegados en un sistema, explicar el impacto de distintas amenazas e intrusiones y en especial de las fugas de información.

Explicar los mecanismos que pueden utilizarse para ocultar la intrusión en un sistema.

DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

Amenazas Persistentes y Fugas de Información:
1. Amenazas Persistentes
1.1. Técnicas de persistencia en sistemas comprometidos
1.2. APT. Definiciones, caracterización y análisis. Tendencias actuales.
1.3 Técnicas de comando y control avanzado
1.4 Mecanismos de sigilo y evasión. Rootkits

2. Canales encubiertos. Esteganografía y estegoanálisis
2.1. Definición de la ciencia de la esteganografía. Historia
2.2. Clasificación de sistemas esteganográficos. Evaluación de su seguridad
2.3. Esteganografía moderna
2.4. Estegoanálisis moderno

ACTIVIDADES FORMATIVAS, METODOLOGÍA A UTILIZAR Y RÉGIMEN DE TUTORÍAS

ACTIVIDADES FORMATIVAS
Clase teórica
Clases prácticas
Clases teórico prácticas
Prácticas de laboratorio
Tutorías
Trabajo en grupo
Trabajo individual del estudiante

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
Elaboración de trabajos e informes de manera individual o en grupo

SISTEMA DE EVALUACIÓN

Peso porcentual del Examen Final:	30
Peso porcentual del resto de la evaluación:	70

Se establece el siguiente sistema de evaluación:
1. Convocatoria ordinaria

Examen final (30% de la nota final)
- La nota mínima será de 4.0 para superar la asignatura

Trabajos periódicos (70% de la nota final)
- De carácter individual o por grupos, según se anuncie al comienzo de la asignatura. Deberán entregarse todos los trabajos.

2. Convocatoria extraordinaria
La calificación de los estudiantes en la convocatoria extraordinaria se ajustará a las siguientes reglas:

a. Si el estudiante siguió el proceso de evaluación continua, el examen tendrá el mismo valor porcentual que en la convocatoria ordinaria, y la calificación final de la asignatura tendrá en cuenta la nota de la evaluación continua y la nota obtenida en el examen final.
b. Si el estudiante no siguió el proceso de evaluación continua, tendrá derecho a realizar un examen en la convocatoria extraordinaria con un valor del 100 % de la calificación total de la asignatura. Este examen podrá contener preguntas pertinentes a las actividades realizadas durante el curso. En esta asignatura no se permite la reentrega de los trabajos en esta convocatoria.

Peso porcentual del Examen Final:	30
Peso porcentual del resto de la evaluación:	70

Se establece el siguiente sistema de evaluación:
1. Convocatoria ordinaria

Examen final (30% de la nota final)
- La nota mínima será de 4.0 para superar la asignatura
Trabajos periódicos (70% de la nota final)
- De carácter individual o por grupos, según se anuncie al comienzo de la asignatura. Deberán entregarse todos los trabajos.

2. Convocatoria extraordinaria
La calificación de los estudiantes en la convocatoria extraordinaria se ajustará a las siguientes reglas:

a. Si el estudiante siguió el proceso de evaluación continua, el examen tendrá el mismo valor porcentual que en la convocatoria ordinaria, y la calificación final de la asignatura tendrá en cuenta la nota de la evaluación continua y la nota obtenida en el examen final.
b. Si el estudiante no siguió el proceso de evaluación continua, tendrá derecho a realizar un examen en la convocatoria extraordinaria con un valor del 100 % de la calificación total de la asignatura. Este examen podrá contener preguntas pertinentes a las actividades realizadas durante el curso. En esta asignatura no se permite la reentrega de los trabajos en esta convocatoria.

BIBLIOGRAFÍA BÁSICA

- Eric Cole Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization, Syngress, 2012

- Shabtai, Asaf, Elovici, Yuval, Rokach, Lior A Survey of Data Leakage Detection and Prevention Solutions, Springer, 2012

- Thales and Verint The cyberthreat handbook, Thales, 2019

BIBLIOGRAFÍA COMPLEMENTARIA

- ISACA Advanced Persistent Threats: How To Manage The Risk To Your Business , ISACA, 2015

RECURSOS ELECTRÓNICOS BÁSICOS

- George Silowash, Christopher King . Insider Threat Control: Understanding Data Loss Prevention (DLP) and Detection by Correlating Events from Multiple Sources: http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=34008

- ThaiCert . Threat Group Cards: A Threat Actor Encyclopedia 2.0: https://apt.thaicert.or.th/cgi-bin/aptgroups.cgi

- Thales group and Verint . The Cyberthreat handbook: https://thalesgroup-myfeed.com/THECYBERTHREATHANDBOOK