Técnicas de Ciberataque

Curso Académico: (2020 / 2021) **Fecha de revisión: 10/07/2020 01:07:35**

Departamento asignado a la asignatura: Departamento de Ingeniería Telemática

Coordinador/a: ALMENARES MENDOZA, FLORINA

Tipo: Obligatoria Créditos ECTS : 6.0

Curso : 1 Cuatrimestre : 1

REQUISITOS (ASIGNATURAS O MATERIAS CUYO CONOCIMIENTO SE PRESUPONE)

Esta asignatura necesita conocimientos y habilidades adquiridas en los Grados universitarios que dan acceso al máster o bien a través de la práctica profesional.
Los estudiantes deberán manejarse cómodamente en entornos Unix y tener conocimientos de programación en algún lenguaje interpretado tipo Python, Ruby, o shell script. También necesitarán conocimientos de redes de comunicaciones, y es básico conocer el funcionamiento de la pila de protocolos de TCP/IP y algunas herramientas administrativas de redes en linux y preferiblemente también en Windows.

OBJETIVOS

Esta asignatura obligatoria refuerza las competencias básicas y generales siguientes:
- CB6: 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.
- CB7: 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.
- CB8: 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.
- CB9: 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.
- CB10: Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando.
- CG1: Comprender y aplicar métodos y técnicas de investigación de ciberataques a una instalación específica.
- CG3: Elaborar concisa, clara y razonadamente documentos, planes y proyectos de trabajo en el ámbito de la Ciberseguridad.
- CG4: 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.

Esta asignatura obligatoria también contribuye a reforzar las siguientes competencias específicas:
- CE1: Analizar y detectar anomalías y firmas de ataques en los sistemas y redes.
- CE2: Analizar y detectar técnicas de ocultación de ataques a sistemas y redes.
- CE3: Conocer las tendencias actuales en técnicas de ciberataque y las experiencias aprendidas en casos reales.
- CE7: Conocer y aplicar los mecanismos de cifrado y esteganografiado pertinentes para proteger los datos residentes en un sistema o en tránsito por una red.

DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

1. Introducción a las técnicas de ciberataque
1.1. Conceptos y definiciones
1.2. Tipos de ciberataques
1.3. Fases típicas de una intrusión

2. Adquisición de información del objetivo y análisis de vulnerabilidades
2.1. Técnicas de reconocimiento. Fuentes abiertas
2.2. Enumeración de redes y escaneo de servicios
2.3. Identificación y análisis de vulnerabilidades

3. Explotación
3.1. Explotación de sistemas de autenticación y explotación de software
3.2. Consumo de recursos y DoS
3.3. Ingeniería social, malware y técnicas de evasión

4. Persistencia
4.1. Eliminación de evidencias
4.2. Escalado de privilegios
4.3. Establecimiento de canales de acceso alternativos
4.4. Ocultación de presencia

ACTIVIDADES FORMATIVAS, METODOLOGÍA A UTILIZAR Y RÉGIMEN DE TUTORÍAS

ACTIVIDADES FORMATIVAS
Clases teóricas
Clases 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 prácticas de laboratorio y problemas planteados por el profesor de manera individual o en grupo.

SISTEMA DE EVALUACIÓN

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

Solo se considera que un alumno sigue la evaluación continua si se entregan todos los trabajos y se hacen todos los examenes, en caso contrario se evaluará por el examen final exclusivamente: evaluación ordinaria 80% de la nota del final, evaluación extraordinaria 100% de la nota del final.

La evaluación continua tendrá en cuenta la participación en clase, la entrega de problemas y casos de estudio y las prácticas de laboratorio.
Habrá entre tres y cuatro prácticas evaluables por grupo que supondrán un 70% de la nota final
Habrá dos exámenes que supondrán un 30% de la nota final. será necesario tener una media de 4.0 en los exámenes para hacer media. En caso contrario será necesario sacar un 4.0 en el examen final para puntuar (70% prácticas de evaluación continua y 30% examen final).

BIBLIOGRAFÍA BÁSICA

- Broad, James, CISSP y Bindner, Andrew Hacking with Kali: practical penetration testing techniques, Syngress (Elsevier), 2014

- Pat Engebretson, David Kennedy The basics of hacking and penetration testing: ethical hacking and penetration testing made easy, Syngress (Elsevier), 2013, 2nd ed.

BIBLIOGRAFÍA COMPLEMENTARIA

- Johnny Long Google Hacking for Penetration Testers, Syngress, 2011

- Michael Hale Ligh; Steven Adair; Blake Hartstein; Matthew Richard Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code, John Wiley & Sons, 2010

RECURSOS ELECTRÓNICOS BÁSICOS

- Kali Linux . Penetration Testing Distribution: https://www.kali.org/

- OWASP . Web Security: https://owasp.org