

FICHA DE ASIGNATURA

Título: Análisis de Malware

Descripción: El malware es una clase de software cuyo propósito es llevar a cabo diversas acciones en un sistema informático, no deseadas por el usuario legítimo del mismo, generalmente de forma oculta o discreta y que resultan perjudiciales para dicho usuario legítimo o para terceros. El malware hoy en día es usado por organizaciones criminales, gobiernos, agencias de seguridad y otros tantos actores, para muy diversos fines, entre los que destacan la obtención de un rédito económico mediante el robo de datos, operaciones financieras fraudulentas, extorsión, secuestros de datos o espionaje.

Carácter: *Obligatoria*

Créditos ECTS: 3

Contextualización (*Máximo 60 palabras*): Comprender qué es el malware, cómo se comporta, cómo se distribuye y cómo evade las medidas de seguridad. Efectuar análisis de muestras de malware (tanto malware para entornos Windows como entornos Android), que permitan al analista obtener información orientada a determinar de qué tipo de amenaza se trata, qué acciones realiza y cuál es su propósito. Para ello se llevarán a cabo análisis de forma estática (sin ejecutarlo) y de forma dinámica (ejecutándolo).

Modalidad: Online

Temario:

Tema 1: Introducción Análisis Malware

- 1.1 – Qué es el malware
- 1.2 – Tipos de malware
- 1.3 – Evolución del malware
- 1.4 – Estado actual
- 1.5 – Teoría de las amenazas
- 1.6 – Casos de estudio

Tema 2: Análisis estático (x86)

- 2.1 – Introducción
- 2.2 – Antivirus
- 2.3 – Packers y crypters (evasión de antivirus)
- 2.4 – Hashing / fingerprinting
- 2.5 – Strings
- 2.6 – PE: formato Portable Executable
- 2.7 – Herramientas de análisis estático

Tema 3: Análisis dinámico (x86)

- 3.1 – Introducción
- 3.2 – Entorno
- 3.3 – Herramientas de análisis dinámico

3.4 – Análisis basado en memoria

- 3.5 – Análisis basado en debug
- 3.6 – Análisis basado en sandbox

Tema 4: Análisis en entornos móviles

- 4.1 – Introducción a las amenazas para dispositivos móviles
- 4.2 – ThreatIntelligence (Amenazas Móviles)
- 4.3 – Búsqueda de Malware para Android.
- 4.4 – Clasificación de Malware para Android.
- 4.5 – IntelligenceResearch
- 4.6 – Análisis estático en Android
- 4.5 – Análisis dinámico en Android

Competencias Específicas:

CE4 – Identificar las vulnerabilidades, amenazas, y software malicioso a los que estén expuestos los diferentes activos de una organización

CE7 - Conocer las tendencias actuales en ciberataques, técnicas de ocultación y principales vectores utilizados.

CE8 - Crear informes de carácter ejecutivo y de carácter científico-técnico que respondan a las necesidades de comunicación en términos de ciberseguridad dentro de una organización.

Actividades Formativas

Actividad Formativa	Horas	Presencialidad
Clases Magistrales (Video-Sesiones)	20	50%
Ejercicios	6	

Metodologías docentes:

- Clase magistral / método expositivo
- Plataforma virtual de aprendizaje
- Aprendizaje Cooperativo (realización de trabajos)
- Aprendizaje Basado en Problemas (ABP)
- Entornos de simulación (recreación de problemas reales)

Sistema de Evaluación:

Sistemas de evaluación	Ponderación mínima	Ponderación máxima
Presentación de trabajos y/o proyectos	50.0	50.0
Examen escrito/oral (prueba objetiva, prueba de respuesta corta y/o prueba de desarrollo).	50.0	50.0

Normativa específica:

Bibliografía:

1.- Practical Malware Analysis. The Hands-On Guide to Dissecting Malicious Software

Michael Sikorsky, Andrew Honi

Editor: No Starch Press, 1 de febrero de 2012

ISBN-10: 1593272901

Google vista previa:

<https://books.google.es/books?id=DhuTduZ-pc4C&printsec=frontcover&hl=es#v=onepage&q&f=false>

2.- Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code

Michael Hale Ligh, Matthew Richard, Steven Adair, Blake Hartstein

Editor: John Wiley & Sons Inc; Edición: Pap/Dvdr (15 de octubre de 2010)

ISBN-10: 0470613033

Google vista previa:

https://books.google.es/books?id=PFGeEx4LT4C&printsec=frontcover&hl=es&source=gbs_atb#v=onepage&q&f=false

3.- Android Malware and Analysis

Ken Dunham, Shane Hartman, Manu Quintans, Jose Andre Morales, Tim

Strazzere

Editor: Auerbach Publications, October 24, 2014

ISBN 9781482252194 - CAT# K23862

Ref: <https://www.crcpress.com/Android-Malware-and-Analysis/Dunham-Hartman-Quintans-Morales-Strazzere/p/book/9781482252194>