



DATOS IDENTIFICATIVOS

Análise de malware

Materia	Análise de malware			
Código	V05M175V01204			
Titulación	Máster Universitario en Ciberseguridade			
Descritores	Creditos ECTS	Carácter	Curso	Cuadrimestre
	5	OB	1	2c
Lingua impartición	Inglés			
Departamento	Dpto. Externo Enxeñaría telemática			
Coordinador/a	Burguillo Rial, Juan Carlos			
Profesorado	Burguillo Rial, Juan Carlos Rivas López, Jose Luis			
Correo-e	jrial@uvigo.es			
Web	http://http://faitic.uvigo.es			
Descrición xeral	O malware utiliza os sistemas e as redes de comunicacións para propagar virus, secuestrar dispositivos ou robar datos confidenciais. O obxectivo desta asignatura é dotar o estudante da capacidade para analizar, detectar e eliminar malware. Para elo se explorarán e exemplificarán, de forma práctica e con casos reais, as técnicas actuais de ocultación e persistencia de malware, así como as tendencias máis novedosas para a súa detección e eliminación.			

Esta asignatura impartirase en inglés.

Competencias

Código	
CB1	Posuír e comprender coñecementos que aporten unha base ou oportunidade de ser orixinais no desenvolvemento e aplicación de ideas, a miúdo nun contexto de investigación.
CG1	Ter capacidade de análise e síntesis. Ter capacidade para proxectar, modelar, calcular e deseñar solucións de seguridade da información, as redes e/ou os sistemas de comunicacións en todos os ámbitos de aplicación
CE8	Ter capacidade para concibir, deseñar, poñer en práctica e manter sistemas de ciberseguridade
CE11	Reunir e interpretar datos relevantes dentro do área da seguridade informática e das comunicacións.
CE13	Ter capacidade de análise, detección e eliminación de vulnerabilidades, e do malware susceptible de utilizalas, en sistemas e redes
CT4	Valorar a importancia da seguridade da información no avance socioeconómico da sociedade
CT5	Ter capacidade para comunicarse oralmente e por escrito en inglés.

Resultados de aprendizaxe

Resultados de aprendizaxe	Competencias
Analizar, detectar e eliminar malware en sistemas e redes.	CG1 CE11 CE13 CT5
Conocer, detectar e loitar contra as técnicas de ocultación e persistencia de malware en sistemas e redes.	CB1 CG1 CE8 CE11 CE13 CT5

Estudiar sistemas e redes para detectar e eliminar as vulnerabilidades susceptibles de ser utilizadas polo malware.	CG1 CE8 CE11 CE13 CT5
Conocer as tendencias actuais en malware e as experiencias aprendidas de casos reais.	CB1 CG1 CT4 CT5

Contidos

Tema	
Introducción a enxeñaría do malware.	a) Qué é o malware? b) Cómo detectalo e eliminalo? c) En qué consiste a enxeñaría de malware?
Tipos de malware.	a) Estructura. b) Compoñentes. c) Vectores de infección.
Enxeñaría de malware.	a) Técnicas de propagación. b) Procesos de infección. c) Persistencia do malware. d) Técnicas de ocultación.
Enxeñaría inversa de malware.	a) ¿Cómo analizar e inferir o funcionamento do malware? b) Comprensión do funcionamento de novos tipos de malware.
Ferramentas de análise de malware.	a) Ferramentas para a detección de malware. b) Ferramentas para a eliminación de malware.

Planificación

	Horas na aula	Horas fóra da aula	Horas totais
Actividades introdutorias	2	2	4
Lección maxistral	10	30	40
Prácticas de laboratorio	15	40	55
Foros de discusión	0	2	2
Estudo de casos	5	4	9
Exame de preguntas obxectivas	2	4	6
Resolución de problemas e/ou exercicios	3	6	9

*Os datos que aparecen na táboa de planificación son de carácter orientador, considerando a heteroxeneidade do alumnado.

Metodoloxía docente

	Descrición
Actividades introdutorias	Faremos unha introdución xenérica aos obxectivos, contidos globais xenerais da materia e resultados esperados. Esta actividade realizarase individualmente.
Lección maxistral	Introduciremos os distintos temas da materia proporcionando o material docente necesario para o seu seguimento. Con esta metodoloxía se traballan as competencias CB1, CG1, CE8, CE11, CE13, CT4 y CT5. Esta actividade realizarase individualmente.
Prácticas de laboratorio	Realizaranse prácticas no laboratorio para comprender mellor os contidos explicados nas leccións maxistras. Con esta metodoloxía trabállanse as competencias CG1, CE8, CE11, CE13 y CT5. Algunhas prácticas realizaranse de forma individual e outras en grupos (dependendo do número de estudantes).
Foros de discusión	Os estudantes deben participar no foro dentro da plataforma TEMA en FAITIC. Con esta metodoloxía se traballan as competencias CE8, CE11, CE13 y CT5. Esta actividade realizarase individualmente.
Estudo de casos	Durante as clases maxistras presentaranse casos de estudo típicos de ameazas, problemas de seguridade coñecidos ou tecnoloxías actuais. Con esta metodoloxía se traballan as competencias CG1, CE11, CE13 y CT5. Esta actividade realizarase en grupo.

Atención personalizada

Metodoloxías	Descrición
Actividades introductorias	Nas actividades formativas prácticas e tutorías, os profesores da asignatura ofrecerán guías de atención personalizada a cada alumno sobre as tarefas a realizar, co fin de orientar o plantexamento e a metodoloxía de elaboración. Tamén se ofrecerá información de coordinación con outros contenidos e asignaturas do programa de estudos. Se recomenda consultar as dúbidas o profesorado o longo de todo o desenvolvemento da materia, tanto para a comprensión dos fundamentos como para a realización dos proxectos e actividades de avaliación.
Lección maxistral	Nas actividades formativas prácticas e tutorías, os profesores da asignatura ofrecerán guías de atención personalizada a cada alumno sobre as tarefas a realizar, co fin de orientar o plantexamento e a metodoloxía de elaboración. Tamén se ofrecerá información de coordinación con outros contenidos e asignaturas do programa de estudos. Se recomenda consultar as dúbidas o profesorado o longo de todo o desenvolvemento da materia, tanto para a comprensión dos fundamentos como para a realización dos proxectos e actividades de avaliación.
Estudo de casos	Nas actividades formativas prácticas e tutorías, os profesores da asignatura ofrecerán guías de atención personalizada a cada alumno sobre as tarefas a realizar, co fin de orientar o plantexamento e a metodoloxía de elaboración. Tamén se ofrecerá información de coordinación con outros contenidos e asignaturas do programa de estudos. Se recomenda consultar as dúbidas o profesorado o longo de todo o desenvolvemento da materia, tanto para a comprensión dos fundamentos como para a realización dos proxectos e actividades de avaliación.
Prácticas de laboratorio	Nas actividades formativas prácticas e tutorías, os profesores da asignatura ofrecerán guías de atención personalizada a cada alumno sobre as tarefas a realizar, co fin de orientar o plantexamento e a metodoloxía de elaboración. Tamén se ofrecerá información de coordinación con outros contenidos e asignaturas do programa de estudos. Se recomenda consultar as dúbidas o profesorado o longo de todo o desenvolvemento da materia, tanto para a comprensión dos fundamentos como para a realización dos proxectos e actividades de avaliación.
Foros de discusión	Nas actividades formativas prácticas e tutorías, os profesores da asignatura ofrecerán guías de atención personalizada a cada alumno sobre as tarefas a realizar, co fin de orientar o plantexamento e a metodoloxía de elaboración. Tamén se ofrecerá información de coordinación con outros contenidos e asignaturas do programa de estudos. Se recomenda consultar as dúbidas o profesorado o longo de todo o desenvolvemento da materia, tanto para a comprensión dos fundamentos como para a realización dos proxectos e actividades de avaliación.

Avaliación						
	Descrición	Cualificación	Competencias Avaliadas			
Prácticas de laboratorio	Os alumnos realizarán prácticas de laboratorio, onde se traballará cos conceptos estudados nas clases teóricas.	45	CB1	CG1	CE8	CT5
					CE11	
					CE13	
Foros de discusión	Os estudantes deben participar no foro da plataforma TEMA.	5	CB1	CG1	CE11	CT4
					CE13	CT5
Estudo de casos	El alumnado realizará presentación de casos de estudio, seleccionados por eles, para analizar amenazas actuais.	15		CG1	CE11	CT5
					CE13	
Exame de preguntas obxectivas	Dous test de avaliación sucesivos para o contido parcial da materia impartida ata ese momento. Os tests serán individuais e de tempo limitado.	30	CB1	CG1	CE11	CT5
					CE13	
Resolución de problemas e/ou exercicios	Durante as clases maxistras realizaranse preguntas aos estudantes para coñecer a súa comprensión do tema baixo estudo.	5	CB1		CE11	CT5
					CE13	

Outros comentarios sobre a Avaliación

Os elementos que forman parte da avaliación da materia son os seguintes:

- **Cuestionarios:** ao longo do curso realizaranse dous cuestionarios que achegarán un 15% da nota final (cada un).
- **Presentación de casos de estudio:** cada alumno deberá realizar unha presentación orixinal que aportará un 15% da nota final.
- **Prácticas de laboratorio:** cada alumno deberá realizar un conxunto de prácticas propostas no laboratorio que achegarán un 45% da nota final.
- **Participación en clase:** os estudantes participarán e discutirán sobre as exposicións realizadas por o profesor e isto contribuirá ata un 5% a nota final.
- **Participación no foro:** os estudantes deben participar no foro da asignatura, de forma individual, e isto contribuirá ata un 5% a nota final. Para obter dito porcentaxe débense proporcionar, como mínimo, dúas contribucións relevantes.

Así temos:

Nota Final = Cuestionarios (2x15 = 30%) + Presentación de casos de estudio (15%) + Práctica de lab. (45%) + Participación en clase (5%) + Foro (5%) = 100%.

Os estudantes deben obter o menos 4 puntos sobre 10 na nota dos cuestionarios e a práctica para poder calcular a nota media final. Si calqueira das notas é inferior a 4, entón a nota final non poderá superar 4 puntos sobre 10.

A planificación das diferentes probas de avaliación intermedia aprobarase nunha Comisión Académica de Grado (CAG) e estará dispoñible ao principio do cuatrimestre.

En caso de detección de copia en calquera das probas (probas curtas, exames parciais ou exame final), a cualificación final será de SUSPENSO (0) e o feito será comunicado á dirección do Centro para os efectos oportunos.

Seguindo as directrices propias da titulación ofrecerase aos alumnos que cursen esta materia dous sistemas de avaliación: avaliación continua e avaliación final (fin do cuatrimestre).

Avaliación continua: o estudante segue a avaliación continua dende o momento en que se presenta os dous cuestionarios da materia. Un alumno que opta pola avaliación continua considérase que se presentou á materia, independentemente de que se presente ou non ao exame final.

Primeira oportunidade: o alumno deberá realizar un exame teórico que substitúe aos cuestionarios realizados ao longo do curso, ademais de entregar as prácticas e os traballos equivalentes aos que se realizaron como parte da avaliación continua.

Segunda oportunidade: o alumno deberá realizar a parte que non superase. No caso de non superar os cuestionarios deberá realizar un exame equivalente.

Os traballos e tarefas prácticas propostas e realizadas neste curso non son recuperables e só son válidas para o curso actual.

Bibliografía. Fontes de información

Bibliografía Básica

Michael Hale Ligh, Andrew Case, Jamie Levy, Aaron Walters, **The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory**, 1, John Wiley & Sons Inc, 2014

Michael Sikorski / Andrew Honig, **Practical Malware Analysis**, 1, William Pollock, 2012

Bibliografía Complementaria

Recomendacións

Materias que se recomenda cursar simultaneamente

Análise forense de equipos/V05M175V01207

Fortificación de sistemas operativos/V05M175V01202

Seguridade en dispositivos móbiles/V05M175V01206

Materias que se recomenda ter cursado previamente

Seguridade de aplicacións/V05M175V01104

Plan de Continxencias

Descrición

No caso de que a docencia sexa exclusivamente non presencial, as clases da materia desenvolveranse dun xeito similar, pero empregando as plataformas que proporciona a Universidade.

As clases virtuais impartiranse semanalmente a través do Campus Remoto, tanto nas sesións teóricas (grupos A) como nas sesións prácticas (grupos B). Neste segundo caso, os estudantes realizarán as prácticas empregando os seus ordenadores persoais ou a infraestrutura virtual do laboratorio.

Os medios habilitados para a resolución das dúbidas suscitadas polos estudantes incluírán foros de consulta en liña e titorías na oficina virtual do profesor.

A avaliación non presencial da materia rexerese polas condicións descritas na guía docente para a modalidade de docencia presencial, incluído o mesmo número de probas, idéntica ponderación e notas mínimas. Os exames teóricos e prácticos realizaranse practicamente, empregando as plataformas que proporciona a Universidade.