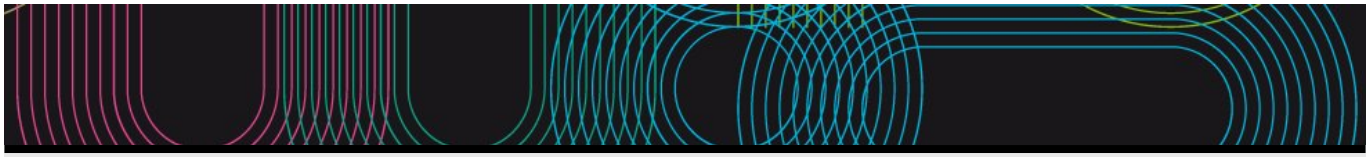

DATOS IDENTIFICATIVOS				
Análise de malware				
Materia	Análise de malware			
Código	V05M175V11109			
Titulación	Máster Universitario en Ciberseguridade			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	5	OB	1	1c
Lingua de impartición	Inglés			
Departamento				
Coordinador/a	Burguillo Rial, Juan Carlos			
Profesorado	Burguillo Rial, Juan Carlos Hernández Pereira, Elena María Rivas López, Jose Luis			
Correo-e	jrial@uvigo.es			
Web	http://https://moovi.uvigo.gal			
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 estudiante da capacidade para analizar, detectar e eliminar malware. Para elo se explorarán y 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 sua detección e eliminación. Esta materia impartirase en inglés.			

Resultados de Formación e Aprendizaxe
Código

Resultados previstos na materia	
Resultados previstos na materia	Resultados de Formación e Aprendizaxe

Contidos	
Tema	
Introducción a enxeñaría do malware.	a) Que 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 funcionamiento do malware? b) Comprensión do funcionamiento 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 traballa o coñecemento B2, a destreza C2 e a competencia D6. Esta actividade realizarase individualmente.
Prácticas de laboratorio	Realizaranse prácticas no laboratorio para comprender mellor os contenidos explicados nas lecciones maxistrais. Con esta metodoloxía trabállase o coñecemento B2, a destreza C2 e as competencias D3 e D6. Algunhas prácticas realizaranse de forma individual e outras en grupos (dependendo do número de estudiantes).
Foros de discusión	Os alunos/as deben participar no foro dentro da plataforma MOOVI. Con esta metodoloxía se traballa o coñecemento B2 e a competencia D6. Esta actividade realizarase individualmente.
Estudo de casos	Durante as clases maxistrais presentaranse casos de estudio típicos de ameazas, problemas de seguridade coñecidos ou tecnoloxías actuáis. Con esta metodoloxía se traballa o coñecemento B2 e as competencias D3 e D6. Esta actividade realizarase en grupo.

Atención personalizada	
Metodoloxías	**Descrición**
Actividades introdutorias	Nas actividades formativas prácticas e titorías, os profesores da materia 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 otros contidos e materias 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. O alumnado podrá consultar e solicitar titorías a través da plataforma Moovi (https://moovi.uvigo.gal).
Lección maxistral	Nas actividades formativas prácticas e titorías, os profesores da materia 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 otros contidos e materias 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. O alumnado podrá consultar e solicitar titorías a través da plataforma Moovi (https://moovi.uvigo.gal).
Prácticas de laboratorio	Nas actividades formativas prácticas e titorías, os profesores da materia 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 otros contidos e materias 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. O alumnado podrá consultar e solicitar titorías a través da plataforma Moovi (https://moovi.uvigo.gal).
Foros de discusión	Nas actividades formativas prácticas e titorías, os profesores da materia 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 otros contidos e materias 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. O alumnado podrá consultar e solicitar titorías a través da plataforma Moovi (https://moovi.uvigo.gal).

Estudo de casos	Nas actividades formativas prácticas e titorías, os profesores da materia 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 otros contidos e materias 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. O alumnado podrá consultar e solicitar titorías a través da plataforma Moovi (https://moovi.uvigo.gal).

Avaliación

	Descrición	Cualificación	Resultados de Formación e Aprendizaxe
Prácticas de laboratorio	Os estudantes realizarán prácticas de laboratorio (3 x 15% = 45%), onde se traballará cos conceptos introducidos nas clases teóricas.	45	
Foros de discusión	Os estudantes deben participar no foro da plataforma MOOVI.	5	
Estudo de casos	Os estudantes realizarán presentacións de casos de estudo, seleccionados por eles, para analizar amenazas actuáis.	15	
Exame de preguntas obxectivas	Dous test de avaliación sucesivos para o contido parcial da materia impartida ata ese momento. Os tests serán individuáis e de tempo limitado.	30	
Resolución de problemas e/ou exercicios	Durante as clases maxistrais realizaranse preguntas aos estudantes para coñecer a súa comprensión do tema baixo estudo.	5	

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 estudo**: cada alumno (de forma individual o en grupo) deberá realizar unha presentación orixinal que aportará un 15% da nota final.

- **Prácticas de laboratorio**: cada alumno deberá realizar un conxunto de prácticas (por defecto 3, cunha ponderación de 15% cada unha) propostas no laboratorio e que achegarán un 45% da nota final.

- **Participación en clase**: os estudiantes participarán e discutirán sobre as exposiciones realizadas polo profesor e esto contribuirá ata un 5% a nota final.

- **Participación no foro**: os estudiantes deben participar no foro da asignatura, de forma individual, e isto contribuirá ata un 5% a nota final; proporcionando, como mınimo, dúas contribucions relevantes.

Así temos:

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

Os estudantes deben obter o menos 4 puntos sobre 10 na nota dos cuestionarios, os casos de estudio e todas as prácticas para poder calcular a nota media final. Si algunha das notas é inferior a 4, entón a notal final non poderá superar 4.9 puntos sobre 10.

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

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

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.

Avaliación global: 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.

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

Convocatoria de fin de carrera: el alumno deberá realizar la parte que no haya superado. En el caso de no haber superado los cuestionarios deberá realizar un examen equivalente.

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.

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/V05M175V11216