Escola Aberta
de Formación Permanente
Universidade Vigo

FICHA MATERIA MÁSTER PROPIO

O nome da materia debe indicarse en galego, castelán e inglés mentres que o resto dos apartados deberanse cubrir no idioma en que se impartirá o título propio

NOME MATERIA (Galego): Malware, ciberamenazas e Intelixencia Artificial		
NOME MATERIA (Castelán): Malware, ciberamenazas e Inteligencia Artificial		
NOME MATERIA (Inglés): Malware, Cyberthreat and Artificial Intelligence		
Módulo/Especialidade:		
Tipo: ☒Obrigatoria ☐Optativa		
ECTS TOTALES: 7,5	ECTS TEORICOS: 7,5	ECTS PRÁCTICOS:
Semestre/Cuadrimestre:Primeiro		
Modalidade: Síncrona virtual		
COMPETENCIAS ASOCIADAS: CG2, CE2, CE4, CE6, CE7, CE9 Indicar códigos da táboa 2.3 da proposta		

Descrición general:

Esta materia ofrece una visión integral de las ciberamenazas desde un enfoque técnico-operativo, estratégico y doctrinal, proporcionando al estudiante las competencias necesarias para identificar, analizar y contrarrestar amenazas dirigidas contra entornos militares y sectores estratégicos de la seguridad nacional, con especial énfasis en la aplicación de la inteligencia artificial

El programa abarca el estudio de modelos de ciberamenazas ampliamente adoptados, como la Cyber Kill Chain y MITRE ATT&CK, junto con el análisis de indicadores de compromiso (IoCs) y de ataque (IoAs), fundamentales para la detección y respuesta en operaciones de ciberdefensa.

En el ámbito específico del malware, la asignatura estudia su taxonomía, técnicas de desarrollo (ingeniería de malware) y metodologías de análisis avanzado mediante ingeniería inversa, permitiendo al estudiante conocer el ciclo de vida completo de una amenaza, desde su desarrollo hasta su despliegue y detección.

Además, se trabajan técnicas de explotación de sistemas, incluyendo actividades de hacking ético y pentesting, con el objetivo de simular ataques reales, identificar superficies de ataque y detectar vulnerabilidades en sistemas estratégicos. El uso de frameworks como Metasploit y Empire, y de herramientas de simulación de ataques APT como Caldera y Atomic Red Team, permitirá al alumno familiarizarse con herramientas empleadas tanto en entornos ofensivos como defensivos.

Una parte importante de la materia se centra en la aplicación de la inteligencia artificial a la detección de ciberamenazas, explorando su aplicación en el análisis automatizado de malware, el análisis de tráfico de red, la detección de comportamientos anómalos de usuarios y entidades (UEBA), el reconocimiento automatizado de campañas de phishing, y la gestión y detección de vulnerabilidades.

Esta formación proporciona a los futuros especialistas un conjunto completo de técnicas, herramientas y metodologías que les permitirán participar activamente en el ciclo de inteligencia y en las ciberoperaciones de las Fuerzas Armadas y otros organismos de sectores estratégicos para la seguridad nacional.

Coordinador/a: Raúl Fernando Rodríguez Rubio
Equipo docente:
1) Raúl Fernando Rodríguez Rubio
2) Alberto Gil Solla
3) José Carlos López Ardao
4) Gabriel González Fernández

Resultados de aprendizaje:
Al finalizar la materia, el estudiante será capaz de:

1. **Comprender y aplicar modelos de ciberamenazas** como la **Cyber Kill Chain** y **MITRE ATT&CK**, utilizando estas referencias para mapear tácticas y técnicas observadas en incidentes reales.
2. **Distinguir y aplicar los conceptos de indicadores de compromiso (IoCs) e indicadores de ataque (IoAs)**, integrándolos en procesos de detección, análisis forense y generación de inteligencia operativa.
3. **Clasificar y caracterizar el malware** mediante el estudio de su taxonomía y técnicas de desarrollo, comprendiendo sus objetivos, mecanismos de propagación, persistencia y evasión.
4. **Realizar análisis estático y dinámico de malware**, utilizando herramientas y técnicas de **ingeniería inversa**, respetando las medidas de seguridad necesarias en el análisis de muestras maliciosas.
5. **Identificar y explotar vulnerabilidades en sistemas estratégicos** mediante la aplicación de técnicas de **hacking ético** y **pentesting**, con especial atención a la obtención de información sobre la superficie de ataque y la simulación de ataques reales.
6. **Emplear frameworks de explotación como Metasploit y Empire**, **y herramientas de simulación de ataques APT basados en MITRE como Caldera y Atomic Red Team**, entendiendo su funcionamiento y aplicación tanto en ejercicios de Red Team como en análisis de amenazas.
7. **Aplicar técnicas de inteligencia artificial para la detección temprana de amenazas**, utilizando modelos de IA para el análisis automatizado de malware, el estudio de patrones en tráfico de red, la detección de comportamientos anómalos (UEBA), la identificación de campañas de phishing y la gestión y detección de vulnerabilidades
8. **Correlacionar la información técnica obtenida del análisis de malware y ciberamenazas** con productos de ciberinteligencia estratégica, contribuyendo a la toma de decisiones informadas en el ámbito de la defensa nacional.
9. **Elaborar informes técnicos y de inteligencia** sobre malware y amenazas analizadas, adaptados a distintos niveles de mando, facilitando su integración en el ciclo de inteligencia militar y de sectores estratégicos

Programa académico:

1. Modelos de ciberamenazas:
    - Ciberamenazas y actores de amenazas. APT (*Advanced Persistent Threat*)
    - Cyber Kill Chain y MITRE ATT&CK.
    - IoCs vs IoAS
2. Malware:
    - Taxonomía.
    - Ingeniería del malware.
    - Ingeniería inversa
3. Explotación de sistemas:
    - Hacking ético y Pentesting.
    - Obtención de información sobre la superficie de ataque. Vulnerabilidades.
    - Frameworks de Explotación de Sistemas: Metasploit y Empire
    - Simulación de ataques APT basados en MITRE: Caldera y Atomic Red Team
4. Uso de IA para detección de malware y ciberamenazas:
    - Análisis de malware basado en IA.
    - Análisis de Tráfico de Red mediante IA.
    - *User & Entity Behaviour Analyis* (UEBA).
    - Detección de phishing basado en IA.
    - Aplicación de la IA a la gestión y detección de vulnerabilidades: SAST (Static Application Security Testing) y DAST (Dynamic Application Security Testing)

Metodoloxía docente:

Durante el bimestre se imparten 50 horas de clase síncrona a través de videoconferencia. En estas clases se alternan explicaciones teóricas con la realización de actividades, ejercicios y demostraciones de tipo práctico por parte del profesorado. Cada dos semanas, se dedica una hora de clase semanal a realizar una tutoría grupal para resolver dudas, aclarar conceptos, etc.

Tras cada sesión de clase se proponen tareas en el aula virtual, esencialmente de tipo práctico, que debe realizar de forma asíncrona y autónoma cada alumno y deben ser entregadas dentro de los plazos establecidos.

Competencias asociadas	Actividades formativas SÍNCRONAS	Horas síncronas presenciais	Horas síncronas virtuais	Horas de traballo autónomo do estudante
	Clase magistral		50	100
	Tutoría grupal		5	0
	Pruebas de evaluación		5	27,5
	ECTS TOTALES = 7,50	0,00	60,00	127,50

Las horas síncronas estarán comprendidas entre 8 y 12 por ECTS en modalidade síncrona

Competencias asociadas	Actividades formativas ASÍNCRONAS	Horas titorización	Horas de traballo autónomo do estudante
	ECTS TOTALES = 0,00	0,00	0,00

Las horas de titorización estarán comprendidas entre 4 e 8 por ECTS en modalidade asíncrona

Metodoloxía de avaliación:

Se usará un **mecanismo de evaluación continua** que consiste, por un lado, en la realización a lo largo del período de docencia de **tareas** asociadas a los distintos temas, que deben ser entregadas en los plazos establecidos y, por otro lado, la realización de varias **pruebas intermedias de evaluación** para verificar la adecuada adquisición de conocimientos.

Cada **tarea** permite obtener una cantidad de puntos variable que depende de la dificultad y tiempo estimado de dedicación. Las tareas suman 1000 puntos en total.

Las **pruebas intermedias** consisten en cuestionarios con preguntas en las que hay que elegir la opción correcta entre varias opciones de respuesta. Se trata de 5 pruebas de 1 hora que se realizarán de forma síncrona a través de la plataforma MooVi mediante *Safe Exam Browser* y el uso obligatorio de una cámara durante la realización de la prueba. Todas las pruebas intermedias se puntúan entre 0 y 10 y poseen el mismo peso sobre la nota final (10%).

Para superar la materia es necesario realizar el 80% de las tareas, obteniendo una puntuación mínima de 500 puntos, y obtener una media de 5.0 en las 5 pruebas de evaluación. En ese caso, la calificación final de la materia se obtiene como:

CF = 0,5*(TOTAL_TAREAS)/100 + 0,1*(P1+P2+P3+P4+P5)

La **Segunda oportunidad de evaluación** consistirá en la entrega de un conjunto de tareas propuestas dentro del plazo señalado en el mes de Junio, y en la realización de un único examen oral de en torno a 1 hora de duración sobre el contenido teórico de toda la materia, así como sobre las tareas entregadas

Competencias avaliadas	Probas de avaliación	% Ponderación
	Tareas en aula virtual	50
	Pruebas intermedias de evaluación	50
		100%

Plataformas de Teledocencia e titorización:

Las clases síncronas se imparten a través de Campus Remoto. Toda la documentación y comunicación relacionada con el curso se realiza a través de una materia en MooVi. En dicha materia de MooVi se publicarán también las distintas tareas, en las que deben realizarse las entregas dentro del plazo establecido y donde el profesorado realizará su evaluación. Las calificaciones de todas las tareas y pruebas de evaluación serán visibles en MooVi. Se habilitará adicionalmente un foro en la materia de MooVi para la resolución colaborativa de dudas.