MASTER

Ciberseguridad

FORMACIÓN A TU MEDIDA

Aula Informática Profesional

CERTIFICADA POR

CompTIA Authorized Partner

ACADEMIC PARTNER

CompTIA CASP+

CompTIA PenTest+

MASTER

Ciberseguridad

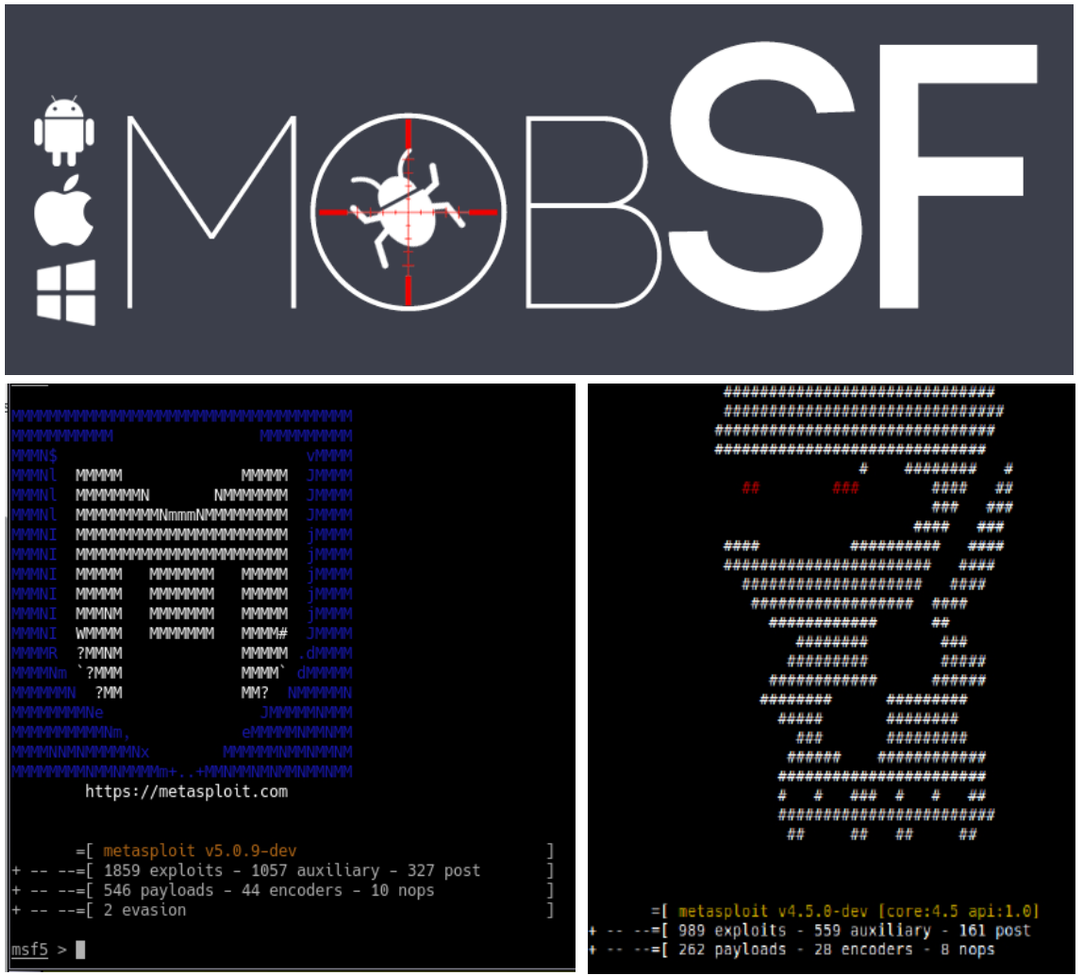
Introducción

En los últimos años el número de empresas que decidieron invertir en protegerse ante **ciberataques ha aumentado un 33%**. Un reciente informe de la Unión Europea prevé la creación de casi 1 millón de puestos de trabajo relacionados con la seguridad informática para el año 2020. La ciberseguridad ha sido identificada en el World Economic Forum como uno de los **principales riesgos de la economía en el mundo**.

Dada la creciente demanda de profesionales cualificados, AIP y CNE, empresa especializada en ciberseguridad, han desarrollado este **Master en Ciberseguridad**, que logra amoldarse a las necesidades de los interesados, optando por una formación de alto nivel

> “Existen dos tipos de empresas: las que han sido hackeadas y las que aún no saben que fueron hackeadas“.
> *– John Chambers*

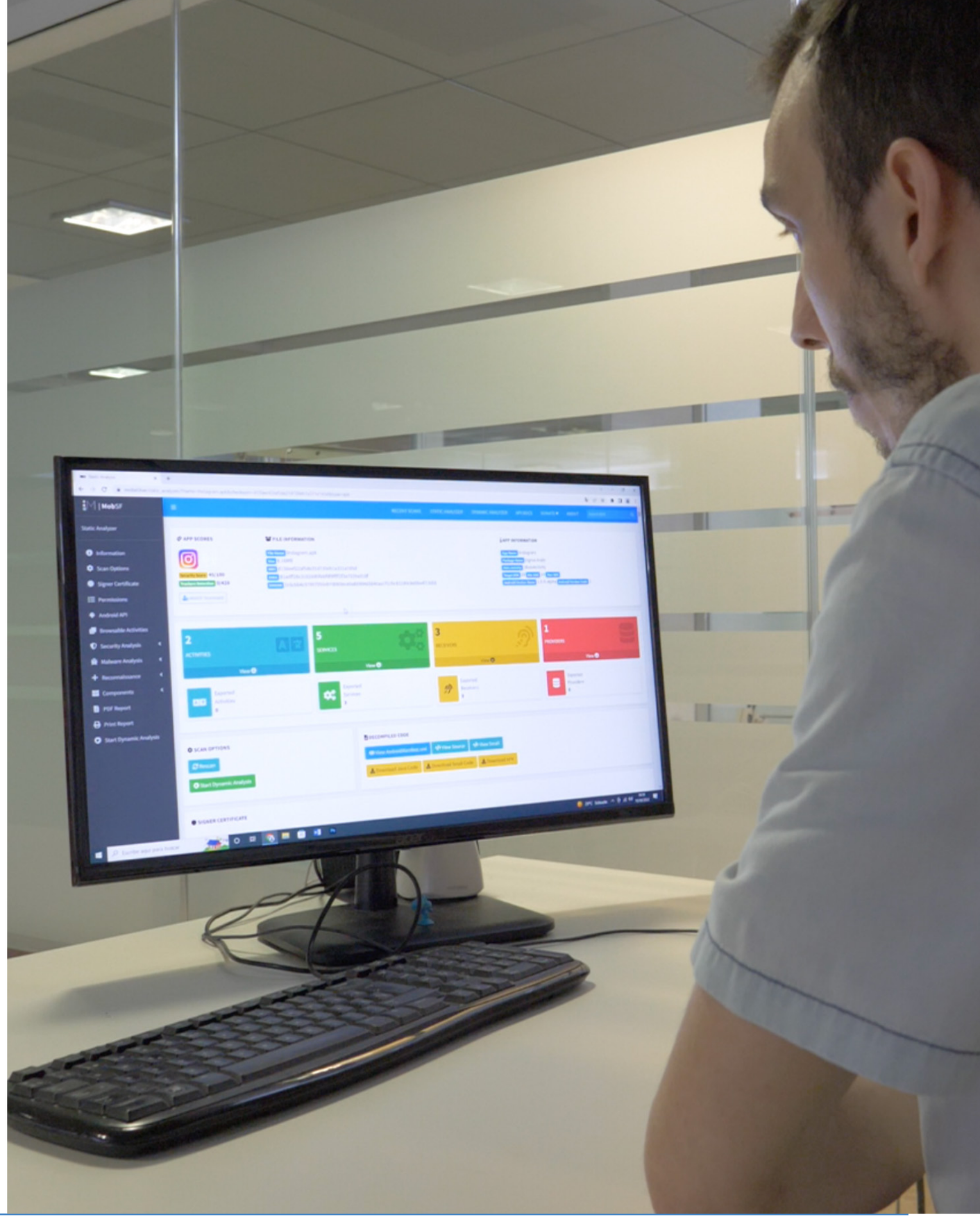
https://github.com/



metasploit

¿Por qué hacer el máster en ciberseguridad de AIP Barcelona?

- Hecho por profesionales y diseñado para una rápida inserción en el mercado laboral.
- Profesor/tutor como mentor para un seguimiento personalizado.
- Oportunidades de networking a través de docentes con experiencia en empresas líderes en ciberseguridad.
- Flexibilidad de pago en tres cuotas.
- Beca del 15% para matrículas realizadas antes del 10 de enero del 2024.
- Obtención de la titulación AIP y 2 certificaciones internacionales.
- Enfoque práctico del contenido.
- Posibilidad de unirse al curso en cualquier momento.



FAQs

¿Qué es un Máster en Ciberseguridad y para qué me va a servir?

Un Máster en Ciberseguridad es un programa de posgrado diseñado para proporcionar conocimientos avanzados y habilidades especializadas en el campo de la seguridad informática. Deberías considerarlo si estás interesado en una carrera en Ciberseguridad, ya que es fundamental para enfrentar las amenazas crecientes en línea y proteger los sistemas de información.

¿A quién va dirigido el Máster en Ciberseguridad?

- Administradores de redes
- Administradores de sistemas
- Programadores

En general, todas las personas que tienen formación y/o trabajan en puestos TI están cualificadas para realizar este Máster.

¿Cuáles son los requisitos de admisión?

El Máster en Ciberseguridad de AIP no requiere título de licenciatura en una disciplina relacionada (como informática o tecnología de la información).

Sin embargo, sí es necesario tener una base de conocimientos en redes, sistemas informáticos (Windows, Linux, Osx), programación, etc.

También es aconsejable tener experiencia en el campo TI: administradores de redes, administradores de sistemas, programadores, personas provenientes de telecomunicaciones, etc.

Unos conocimientos medios de inglés también son necesarios, aunque las clases serán en castellano, la mayor parte de la información de este sector es en inglés y es indispensable poder entender el inglés escrito para aspirar a ser un profesional en el sector de la ciberseguridad.

Si no tengo los requisitos previos, ¿hay alguna forma de poder realizar el Máster en Ciberseguridad?

Una opción para probar unos conocimientos mínimos es realizar el curso: Introducción al Hacking Ético, y superarlo mostrando unos conocimientos suficientes como para poder realizar el Máster (la aprobación del curso no implica una aceptación en el Máster, la decisión siempre recaerá en el profesor, que considere que tiene los conocimiento sobre ciberseguridad suficientes).

¿Cuánto tiempo dura el Máster en Ciberseguridad?

La duración del Máster en Ciberseguridad de AIP es de un año, con clases presenciales u online lunes, martes y jueves

¿Cuáles son las áreas de estudio comunes en un programa de Máster en Ciberseguridad?

Los programas de Máster en Ciberseguridad profundizan en:

- Seguridad de redes
- Seguridad de aplicaciones
- Forense digital
- Gestión de riesgos
- Criptografía
- Ética en la Ciberseguridad
- Cumplimiento normativo

¿Cuál es la demanda laboral para los graduados en Ciberseguridad?

Las empresas, organizaciones gubernamentales y el sector financiero están constantemente en busca de expertos en ciberseguridad para proteger sus activos digitales. Actualmente la oferta no cubre la demanda actual en puestos de ciberseguridad y esta demanda sube cada año, por eso es tan importante aprender esta profesión de la mano de un profesor y mentor experimentado en la materia.

¿Cuánto puedo esperar ganar después de obtener un Máster en Ciberseguridad?

El sueldo medio de un profesional de ciberseguridad puede variar significativamente según factores como la ubicación geográfica, la experiencia, la educación, las certificaciones y el tipo de empleador.

En los Estados Unidos, por ejemplo, el sueldo medio de un profesional de ciberseguridad varía según la ubicación. En áreas metropolitanas de alto costo, como Silicon Valley o Nueva York, los salarios tienden a ser más altos. En promedio, un profesional de ciberseguridad con experiencia puede ganar entre $80,000 y $150,000 al año. Los expertos en ciberseguridad con experiencia y habilidades especializadas, como los investigadores de amenazas o los analistas de seguridad de alto nivel, pueden ganar salarios considerablemente más altos, a menudo superando los $150,000 o más.

En España, un profesional de ciberseguridad con poca experiencia o recién graduado podría esperar un salario inicial en el rango de 20,000 a 35,000 euros al año. Con varios años de experiencia y habilidades especializadas, o certificaciones relevantes, es posible ganar salarios significativamente más altos. Los profesionales de ciberseguridad con experiencia y habilidades demandadas pueden ganar entre 40,000 y 70,000 euros al año o incluso más, dependiendo de su nivel de experiencia y responsabilidades.

¿Necesito certificaciones adicionales además de un Máster en Ciberseguridad?

Además de la titulación del Máster, tener una certificación internacional es lo que te abrirá más puertas. Las certificaciones más reconocidas son las de Offsec (certificación OSCP), el Certified Ethical Hacker (CEH) y las certificaciones Comptia.

Por ello, en el Máster de Ciberseguridad de AIP incluimos la preparación intensiva en las dos certificaciones Comptia más importantes:

- La de profesional en ciberseguridad ofensiva (Comptia Pentest+, el PT0-002)
- La de profesional en ciberseguridad defensiva (Comptia Casp+, el CAS-004)

Con ellas, podrás optar a puestos de trabajo en ciberseguridad en cualquier parte del mundo y tu profesionalidad será reconocida al momento.

¿Hay becas disponibles en el Máster en Ciberseguridad de AIP?

- Actualmente, para los alumnos que cumplan los requisitos y formalicen su matrícula antes del 10 de enero de 2024, se les está concediendo una beca por valor del 15% de la matrícula. A partir del 10 de enero de 2024 el Máster volverá a su precio original.
- El pago al contado también incluye un descuento.

¿Existen posibilidades de financiación?

El Máster en Ciberseguridad AIP puede financiarse en 3 plazos; él 1º al formalizarse la matrícula, el 2º a pagar en marzo y el último en junio.

¿Hay becas/financiación para desempleados?

El 10% de los alumnos podrá optar además a Becas de financiación flexible. Nos haremos cargo del costo del master hasta que el estudiante encuentre empleo (solamente tendrá que abonar el importe de la reserva). A cambio, una vez éste haya encontradoun empleo, abonará un porcentaje fijo de su salario durante un número predeterminado de meses.

¿Es un Máster presencial u online?

El Máster en Ciberseguridad AIP es presencial y también se puede cursar online asistiendo a las clases en directo desde cualquier parte.

Este es un Máster profesional, con exigencia alta y totalmente orientado a la práctica, donde vas a aprender a un ritmo rápido y de la mano de un docente y mentor experto. Nuestro objetivo es que el 100% de nuestros alumnos se conviertan en profesionales de la ciberseguridad.

¿Hay limitación de plazas?

Si, la naturaleza de este Máster hace que el número máximo de alumnos por grupo sea de 20 para poder ofrecer la máxima calidad en la formación.

¿Cuándo comienza el Máster en Ciberseguridad de AIP?

La fecha de comienzo del Master en Ciberseguridad es el 22 de enero de 2024.

¿Quién será el docente encargado de impartir el Máster en Ciberseguridad de AIP?

Conecta con Luis Miguel Chica en Linkedin

MÓDULOS

01. Hacking Ético (Curso Intensivo Práctico) + Certificación Pentesting con CompTIA

Este módulo de Hacking Ético y Certificación está diseñado para proporcionar a los participantes una experiencia altamente práctica y orientada a la obtención de la certificación internacional en ciberseguridad ofensiva Pentesting+ de CompTIA. El temario abarca una amplia gama de temas relacionados con la identificación y explotación de vulnerabilidades en sistemas y redes, con un enfoque práctico y realista.

OBJETIVO

- Definición y Alcance del Proyecto: Aprender a establecer claramente el alcance de un proyecto de pruebas de penetración, enfocándose en aplicaciones prácticas y casos reales.
- Identificación de Vulnerabilidades: Adquirir habilidades prácticas para identificar y evaluar vulnerabilidades en sistemas y redes, a través de ejercicios de laboratorio y escenarios reales.
- Explotación y Penetración: Practicar técnicas seguras y éticas para explotar sistemas y redes en entornos controlados, desarrollando la capacidad de llevar a cabo pruebas de penetración de manera efectiva.
- Comunicación Efectiva: Mejorar las habilidades de comunicación y documentación a través de la práctica en la preparación de informes técnicos y presentaciones claras y efectivas.
- Certificación Internacional: Prepararte para obtener la certificación internacional en ciberseguridad ofensiva de CompTIA, validando tus habilidades y conocimientos adquiridos durante el curso.

Plan de estudios

1. Organización del alcance/Requisitos del cliente
2. Definición de las reglas de enfrentamiento
3. Huella y recopilación de inteligencia
4. Evaluación de las vulnerabilidades humanas y físicas
5. Preparación del análisis de vulnerabilidades
6.Escaneo de vulnerabilidades lógicas
7. Análisis de los resultados del escaneo
8. Evitar la detección y cubrir huellas
9. Explotación de la LAN y la Nube
10. Prueba de redes inalámbricas
11. Dirigirse a dispositivos móviles
12. Atacar sistemas especializados
13. Ataques basados en aplicaciones web
14. Realizar piratería del sistema
15. Scripting y Desarrollo de Software
16. Aprovechar el ataque: pivotar y penetrar
17. Comunicación durante el proceso de PenTesting
18. Resumir los componentes del informe
19. Recomendar remediación
20. Realizar actividades posteriores a la entrega del informe

02. Tecnologías SIEM + Certificación CASP+ con CompTIA

Este módulo en Tecnologías SIEM (Security Information and Event Management) está diseñado para proporcionar a los participantes una experiencia altamente práctica en la gestión de la seguridad de la información. El temario abarca una amplia gama de temas relacionados con la gestión de riesgos, la seguridad de la infraestructura, la nube y la respuesta a incidentes, todo ello con un enfoque práctico y orientado a la obtención de la certificación internacional CASP+ de CompTIA

OBJETIVO

- Gestión de Riesgos y Cumplimiento: Aprender a identificar y gestionar riesgos de seguridad, alineándolos con las normativas y estándares de cumplimiento.
- Continuidad del Negocio y Recuperación ante Desastres: Desarrollar habilidades para garantizar la disponibilidad de servicios críticos en situaciones de emergencia.
- Seguridad de Infraestructura y Software: Adquirir conocimientos sobre cómo proteger la infraestructura y realizar integraciones de software seguras.
- Seguridad en la Nube y Plataformas Especializadas: Comprender las consideraciones específicas de seguridad en la nube y en plataformas especializadas.
- Criptografía y Respuesta a Incidentes: Implementar técnicas de criptografía y desarrollar capacidades de respuesta a incidentes para proteger la información y actuar efectivamente en situaciones de seguridad.

Plan de estudios

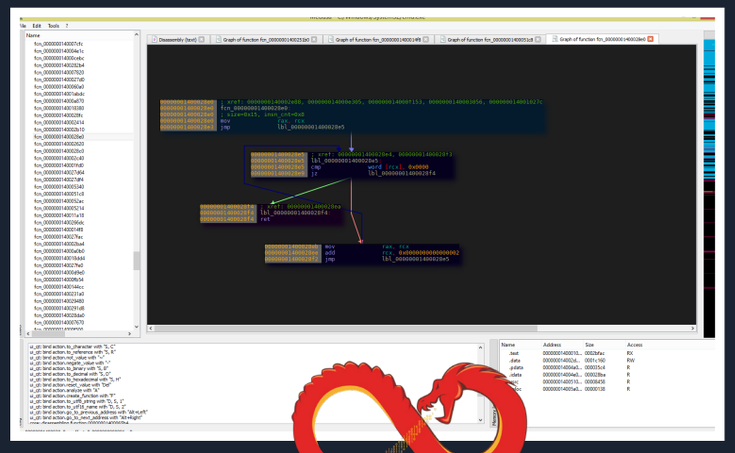
1. Realizar actividades de gestión de riesgos
2. Resumir las estrategias de gobernanza y cumplimiento
3. Implementación de la continuidad del negocio y la recuperación ante desastres
4. Identificación de servicios de infraestructura
5. Realizar la integración de software
6. Explicar la virtualización, la nube y la tecnología emergente
7. Exploración de configuraciones seguras y refuerzo del sistema
8. Comprender las consideraciones de seguridad de la nube y las plataformas especializadas
9. Implementación de criptografía
10. Implementación de infraestructura de clave pública (PKI)
11. Comprender la gestión de amenazas y vulnerabilidades
12. Desarrollo de capacidades de respuesta a incidentes

03. Ingeniería inversa

La ingeniería inversa, o “reversing”, es una parte del mundo de la ciberseguridad de gran importancia, puesto que permite realizar multitud de tareas sobre un software, tales como estudiar su código fuente o realizar análisis sobre partes o la totalidad del software. Para ello, los especialistas se apoyan en herramientas y técnicas como los compiladores o los análisis estáticos.

OBJETIVO

- El objetivo de este curso es que los estudiantes se adentren en el mundo de la ingeniería inversa y el análisis de malware. El curso enseña cómo desensamblar y descomprimir archivos binarios y cómo estudiar la intencionalidad, funcionalidades y daño potencial de una muestra de malware.



https://ghidra-sre.org/

Plan de estudios

INTRODUCCIÓN
1. Introducción
2. Objetivos
3. Definiciones
4. Motivaciones.
5. Limitaciones
6. Aspectos legales

COMPILADORES
1. Teoría de compiladores
   1.1 Programa fuente
   1.2 Programa objeto
   1.3 Programa binario ejecutable
2. Fases de un compilador
3 Análisis léxico
   3.1 Definición de términos
   3.2 Especificación de componentes léxicos
   3.3 Reconocimiento de componentes léxicos
4. Análisis sintáctico
   4.1 Gramáticas independientes del contexto
   4.2 Árboles de análisis sintáctico y derivaciones
   4.3 Analizadores sintácticos LR
   4.4 Analizadores sintácticos LALR
5. Análisis semántico
6. Generación de código intermedio
   6.1 Código de tres direcciones
   6.2 Tipos de proposiciones de 3 direcciones
7. Generación de código y optimizaciones
8. Herramientas para la compilación

RECONSTRUCCIÓN DE CÓDIGO 1
1. Conceptos básicos sobre reconstrucción de código
2. Variables (x86 32 y 64 bits / ARM)
3. Arrays (x86 32 y 64 bits / ARM)
4. Punteros (x86 32 y 64 bits / ARM)
5. Objetos (x86 32 y 64 bits / ARM)

RECONSTRUCCIÓN DE CÓDIGO 2
1. Estructuras de código
2. Operadores
3. Condicionales y bifurcaciones (x86 32 y 64 bits / ARM)
   3.1 If {} else if {} else
   3.2 Switches
   3.3 For
   3.4 While-do/while
   3.5 Break and continue
4 Funciones (x86 32 y 64 bits / ARM)

FORMATOS DE FICHEROS BINARIOS Y ENLAZADORES DINÁMICOS
1 Binarios ELF
   1.1 Formato de fichero
   1.2 Cabecera ELF
   1.3 Segmentos
   1.4 Secciones
   1.5 Table de símbolos
   1.6 Cargador dinámico
2 Binarios PE
   2.1 Formato de fichero
   2.2 Cabecera PE
   2.3 Table de secciones
   2.4 Table de importaciones
   2.5 Table de exportaciones
   2.6 Cargador dinámico

ANÁLISIS ESTÁTICO: DESENSAMBLADORES Y RECONSTRUCCIONES DE CÓDIGO
1. Conceptos iniciales
2. Desensambladores
   2.1 Conceptos básicos
3. Herramientas disponibles
   3.1 IDA Pro
4 Reconstructores de código
   4.1 Herramientas disponibles
   4.2 Hex-Rays Decompiler

ANÁLISIS DINÁMICO: DEPURADORES DE CÓDIGO
1. Aspectos generales
2. Caja negra: Análisis de comportamiento
   2.1 Interpretación de comunicaciones
   2.2 Monitorización de funciones del sistema
3. Caja blanca: Depuradores de código
   3.1 Depuradores en Linux
   3.2 Depuradores en Windows

APLICACIONES PRÁCTICAS
1. Punto de partida
2. Análisis de vulnerabilidades
3. Análisis de funcionalidades ocultas
4. Análisis de un formato de fichero desconocido

RESUMEN

EVALUACIÓN FINAL DE MÓDULO
1. Examen práctico
2. Examen teórico

04. Análisis forense

Investigar un incidente de seguridad o una caída del sistema, así como el robo o espionaje de información pueden ser tareas de suma dificultad. En este curso, los estudiantes aprenderán a llevar a cabo investigaciones forenses eficientes, así como a obtener resultados óptimos de estas investigaciones y evidencias digitales para los procedimientos legales que puedan producirse.

OBJETIVO

- El curso explica las técnicas y herramientas necesarias para llevar a cabo investigaciones forenses en objetivos y localizaciones comprometidas y la extracción acciones mediante evidencias digitales que se han llevado a cabo contra el objetivo.

"La conciencia del peligro es ya la mitad de la seguridad y de la salvación"

-Ramón J. Sénder

Plan de estudios

INTRODUCCIÓN
1. Introducción
2. Objetivos
3. Introducción al análisis forense
4. Como se desarrolla un ciberataque.

METODOLOGÍA FORENSE
1. Metodología
   1.1 Perito forense y analista forense
   1.2 El laboratorio forense
2. Fases de un análisis forense
   2.1 Preservación
   2.2 Análisis
   2.3 Presentación
   2.4 Cadena de custodia

EL PROCESO DE ADQUISICIÓN
1. Sistema encendido
1.1 Volatilidad de la memoria RAM
2 Comandos
3 Herramientas
   3.1 RAMCAPTURE
   3.2 RAWCOPY
   3.3 LASTACTIVITYVIEW
   3.4 WINAUDIT
   3.5 PSTOOLS
   3.6 WMI
4. Distribucions Forenses
   4.1 OSFORESINCS
   4.2 CAINE
   4.3 DEFT
   4.4 SIFT Workstation
   4.5 SCRIPTING

SISTEMA APAGADO
1 Sistema de apagado
   1.1 Clonado
   1.2 Tipos de clonado
2 Formatos
   2.1 RAW
   2.2 Contenedores virtuales
3. Clonado por software
4. Clonado por hardware
5. Integridad de los datos
   5.1 Valor HASH
6. Acceso a discos clonados

ARTEFACTOS DE SISTEMAS WINDOWS
1. Artefactos
2. Visor de eventos
3. Prefetch

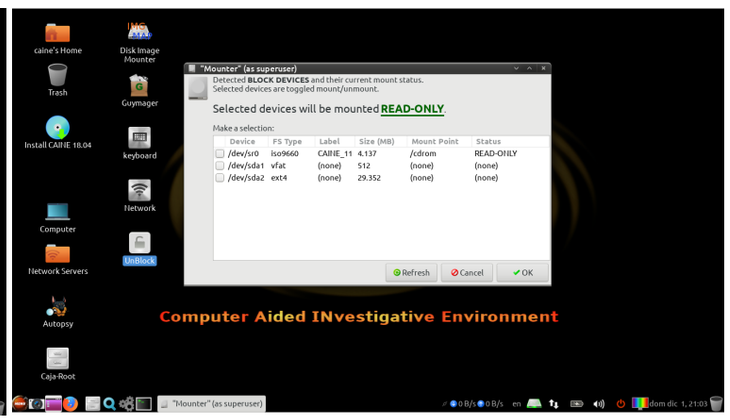
ANÁLISIS FORENSE DE REDES Y PREVENCIÓN DE INTRUSIÓN
1. Wireshark
2. Network Miner
3. Xplico
4. Snort

ANÁLISIS FORENSE EN CORREO ELECTRÓNICO
1. Cabeceras
2. MIME, S/MIME Y SMTP
3. Comandos SMTP
4. Protocolo extendido SMTP

GESTIÓN DE ANÁLISIS DE LOGS EN WINDOWS
1. Logs de Windows
2. Shadow Copy

RESUMEN

EVALUACIÓN FINAL DE MÓDULO
1. Examen práctico
2. Examen teórico



https://www.caine-live.net/

05. Hacking e Inteligencia Artificial (OWASP Top 10 LLM Models)

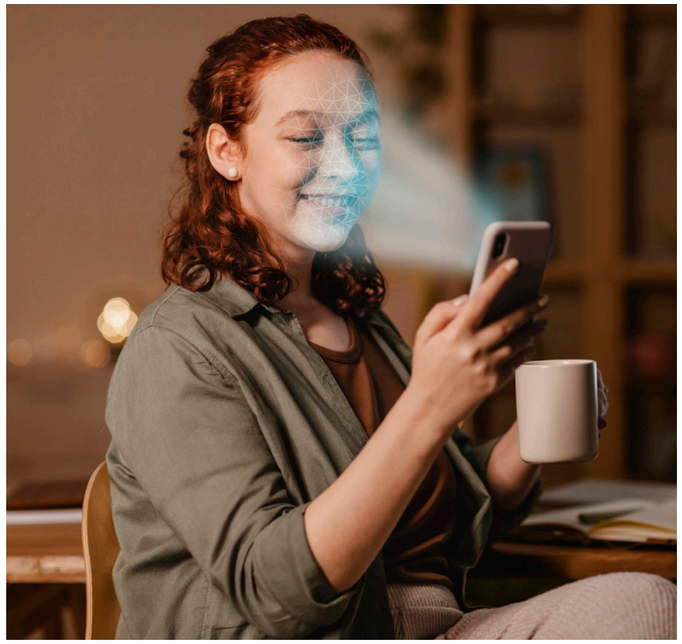
Este módulo se basa en la última actualización de OWASP Top 10 y se ha diseñado para adaptarse a la creciente revolución de las tecnologías de Inteligencia Artificial y su rápida adopción por parte de empresas y usuarios particulares.
En la actualidad, las tecnologías de IA están presentes en diversas aplicaciones y servicios, desde chatbots hasta sistemas de reconocimiento facial y análisis de datos. Sin embargo, su amplia utilización a menudo ocurre sin un entendimiento profundo de su funcionamiento y las implicaciones de seguridad asociadas.

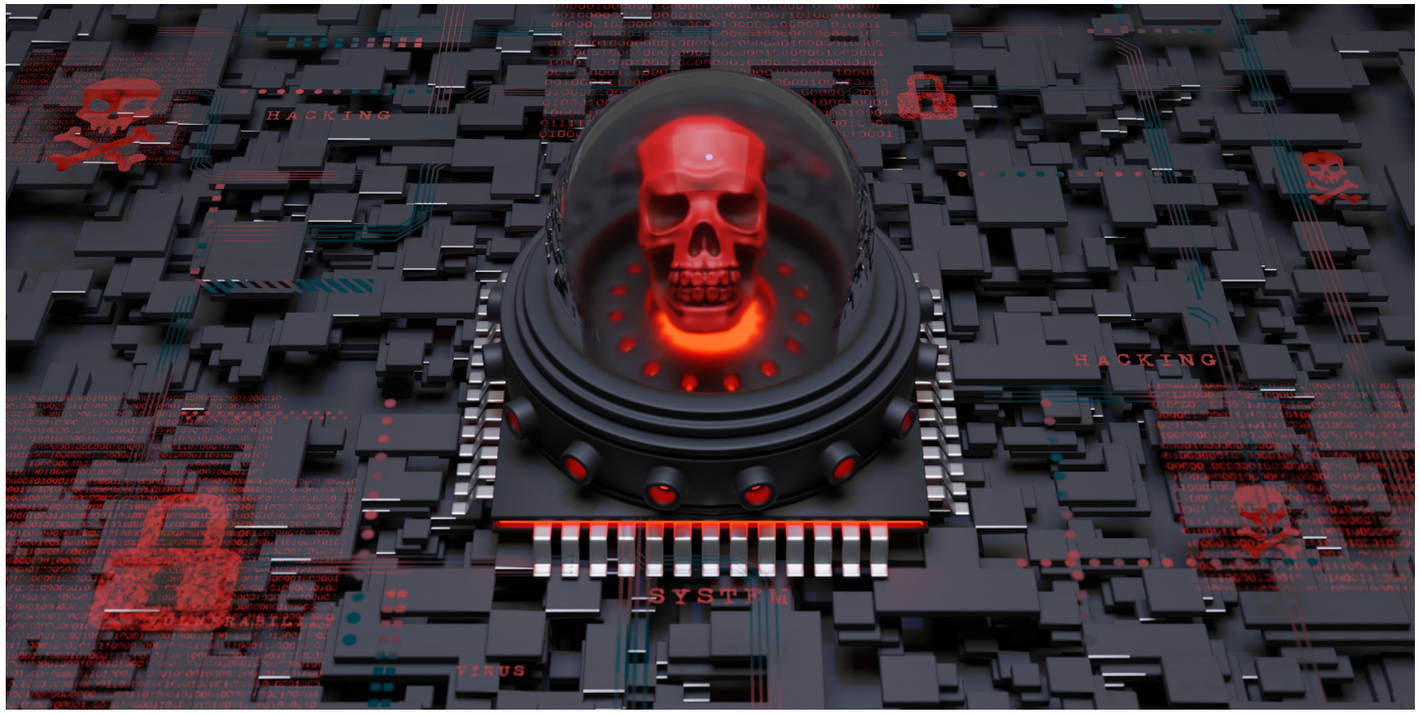
OBJETIVO

- El objetivo principal es capacitar a los alumnos del Máster en Ciberseguridad en la comprensión y abordaje de los desafíos de seguridad en el contexto de la IA. A través de la introducción a la programación de modelos de IA, los diferentes tipos de ataque, la realización de auditorías de sistemas de IA y la promoción de la ética y la responsabilidad, este módulo brindará las habilidades necesarias para comprender y mitigar las vulnerabilidades en estas tecnologías de vanguardia.ciones comprometidas y la extracción acciones mediante evidencias digitales que se han llevado a cabo contra el objetivo.

Plan de estudios

1. Introduction to the development of LLM models
2. Prompt Injection
3. Insecure Output Handling
4. Training Data Poisoning
5. Model Denial of Service
6. Supply Chain Vulnerabilities
7. Sensitive Information Disclosure
8. Insecure Plugin Design
9. Excessive Agency
10. Overreliance
11. Model Theft





MASTER

Ciberseguridad

Módulos

01. Hacking Ético (Curso Intensivo Práctico) + Certificación Pentesting con CompTIA

02. Tecnologías SIEM + Certificación CASP + con CompTIA

03. Ingeniería Inversa

04. Análisis forense

05. Hacking e Inteligencia Artificial (OWASP Top 10 LLM Models)

Modalidades de pago

Precio original: al contado: ~~5.350€~~ / fraccionado 3 pagos: ~~5880€~~

(descuento -15% si te apuntas antes del 10 de enero de 2024)

4.550€

PAGO AL CONTADO

4550€

PAGO FRACCIONADO

Tres pagos de 1.670€

1º. al momento de la inscripción

2º. 7 de marzo de 2024

3º. 7 de junio 2024

Horarios y modalidad

DURACIÓN Y HORARIO

1 curso lectivo Lunes, martes y jueves de 16h a 19h

MODALIDAD

Presencial u online (clases emitidas en directo)

ESTE CURSO ES APTO PARA VISADO DE ESTUDIANTES

Requerimientos técnicos

MÍNIMO
- Procesador: i5 10ª generación o equivalente
- Ram: 8Gb o superior
- Gráfica: 2Gb Gddr5 o equivalente
- Disco duro: SSD 256 GB

MEDIO
- Procesador: i5 11ª generación o i7 10ª generación
- Ram: 12Gb o superior
- Gráfica: 6Gb Gddr6 equivalente
- Disco duro: SSD 256 GB M2

OPTIMO
- Procesador i7 11ª o 12ª generación
- Ram: 16Gb o superior
- Gráfica: 10Gb Gddr6 / equivalente o superior
- Disco duro: SSD 512 Gb M2

Por ser alumno de AIP Barcelona tienes descuentos especiales en RED COMPUTER, Sepúlveda, 178

Profesor

Luis Miguel Chica
Ethical Hacker / Web & Software Developer

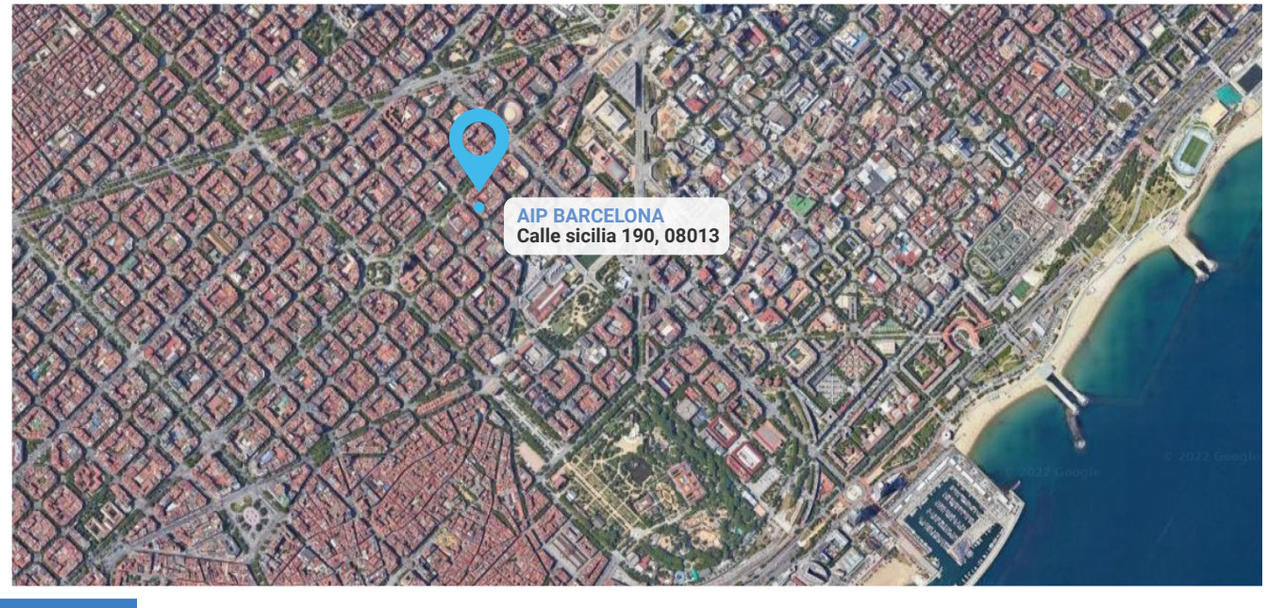
Consultor experto en Ciberseguridad IT: Ethical Hacking, con amplia experiencia en el Desarrollo de hazañas propias de Uso de Machine Learning y Deep Learning para crear herramientas de prevención y ataques e investigación de nuevas vulnerabilidades.
Cibercooperante en Incibe.

AIP Barcelona

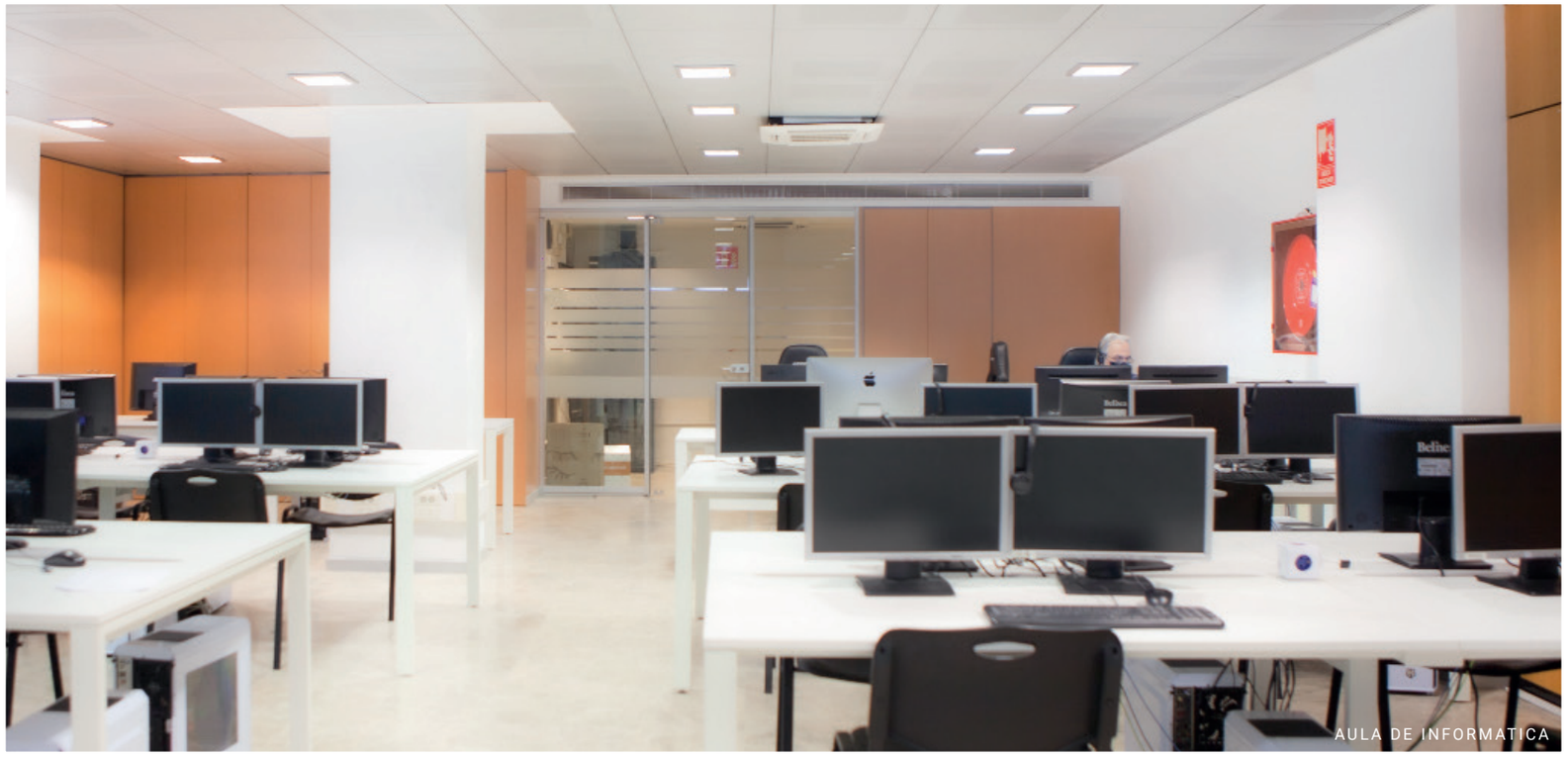
Aula Informática Profesional (AIP) nace en el año 1990, como escuela de informática.

Con los años la informática ha evolucionado muchísimo y con ella AIP. Desde la escuela, no solo ofrecemos cursos comunes como mecanografía u ofimática, sino que hemos crecido hasta abarcar todo un perfil ámpliamente capacitado, y avalados por un gran equipo de profesionales, hemos llegado a campos muy complejos y variados como son el diseño, la programación pura, diseño y programación de páginas web, creación de aplicaciones, redes sociales, posicionamiento en Internet, programas CAD, gestión empresarial o SAP, reparación y mantenimiento de PC, portátiles y teléfonos móviles... Dicho de otro modo, llegamos tan lejos como tú necesites.

Bajo demanda, también actuamos como consultoría de formación estudiando los defectos y las debilidades que presentan los trabajadores de una empresa a nivel formativo, para así poder focalizar la mejor formación en cada caso.



Instalaciones



AULA DE INFORMATICA

AULA TALLER

AULA POLIVALENTE

En AIP Barcelona, diponemos de instalaciones especialmente adecuadas para el desarrollo de clases magistrales y de talleres prácticos que te permitirán cumplir con todos los objetivos propuestos en tu plan de estudios.

Aula Informática Profesional

CERTIFICADA POR CompTIA Authorized Partner ACADEMIC PARTNER

CompTIA CASP+ | CompTIA PenTest+

AIP BARCELONA
TEL: 93265 05 20
WHATSAPP: 666 967 220
Calle Sicilia 190, 0013 , Barcelona
info@aipbarcelona.com