Plan de Estudios
Master Universitario en Ciberseguridad

Bloque I: Auditoría de sistemas de información

Hacking Ético

- Definiciones y planificación: etapas y metodologías del proceso de auditoría de seguridad
- Information Gathering (herramientas y organización de la información).
- Vulnerabilidades comunes: CVSS (Common Vulnerability Scoring System), reportes, vulnerabilidades "0-day".
- Herramientas para análisis manual y automatizado.
- Exploiting: romper la seguridad como parte del proceso de auditoría de seguridad, consideraciones éticas y sistemas críticos.
- Técnicas para elevación de privilegios.
- Límites legales: marco regulatorio y normativa en auditorías de seguridad.
- Elaboración de informes técnicos y ejecutivos

Análisis de Malware

- Introducción al malware
- Análisis estático: herramientas (desensambladores) y metodología (cadenas, grafo de control de flujo, códigos de operación, N-gramas).
- Análisis dinámico: herramientas (máquinas virtuales y emuladores) y metodología (monitorización de llamadas a funciones y salidas, análisis del espacio de parámetros, trazado de instrucciones) .
- Análisis en memoria y en móviles (análisis de malware en Android).

Respuesta a incidentes y Análisis forense

- Respuesta a Incidentes:
    - Metodología de gestión, normativa aplicable y notificaciones a organismosde referencia
    - Centros de respuesta a incidentes, centros de emergencias en seguridad ycentros de operaciones
    - Plan de respuesta a incidentes (ISO 23301) y continuidad de negocio
- Análisis forense
    - Herramientas de ataque y evidencias en registros del sistema (redes,sistemas de ficheros y actividad maliciosa)
    - Evidencia electrónica: custodia, preservación de pruebas, peritaje y jurisprudencia.
    - Artefactos de forense

Bloque II: Gobierno y gestión de las tecnologías de la información

Gobierno de la seguridad

- Certificación de seguridad: Marcos de referencia (COBIT), estándares (ISO) y optimización de recursos.
- Gestión estratégica de la seguridad en una organización.
- Beneficios derivados del gobierno de la seguridad y certificaciones
- Alineación de la normativa con las necesidades de negocio

Amenazas y análisis de riesgo

- Seguridad en redes. Identificación de amenazas y vectores de ataque.
- El proceso de gestión de riesgos: introducción y definiciones
- Etapas del proceso de gestión de riesgos: metodologías (MAGERIT, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), NIST SP 800-30
- Aplicaciones del proceso de análisis y gestión de riesgos.

Monitorización y data mining

- Registros propios del sistema: peculiaridades de Windows y Linux
- Monitorización del tráfico en redes: tipos de protocolos, puertos y backdoors.
- Sistemas de detección y monitorización, automatización del proceso
- Fuentes heterogéneas de datos y correlación de logs
- Data Science: Principios de Cloud Computing & Big Data.
- Minería de Datos y R como herramientas de ciberseguridad

Bloque III: Desarrollo, implantación, operación y mantenimiento de Sistemas

Diseño, desarrollo e implantación de soluciones de ciberseguridad

- Diseño de arquitecturas de seguridad en sistemas complejos y en redes, webservices y microservicios: protección pasiva, activa y aplicativa
- Entornos y metodologías de desarrollo (NIST Cibersecurity Framework, SDLC): servicios, software y aplicaciones
- Entornos de producción e implantación de soluciones

Entornos ubicuos (SCADA, móviles) e Infraestructuras Críticas

- Entornos ubicuos, definiciones, características y vulnerabilidades
- Comunicaciones y almacenamiento en computación ubicua: protocolos y encriptación, aplicaciones a IoT (Internet de las cosas) y Smart Cities
- Seguridad en dispositivos móviles: consideraciones de seguridad en redes 4G/5G, SMS y bluetooth
- Entornos industriales: protección de entornos empotrados (SCADA), seguridad en Industria 4.0
- Infraestructuras críticas en la Estrategia Nacional de Ciberseguridad: securización, gestión de riesgos y normativa nacional aplicable (PIC)

Bloque IV: Protección de los activos de información

Criptografía y autenticación

- Nociones de cirptografía, TLS y PKI
- Servicios de confianza, autorizaciones y tokens.
- Servicios de identidad, autenticación segura y biometria.
- Servicios cloud y gestión de autenticación y autorización

Cumplimiento normativo y RGPD

- Legislación aplicable en España a la Ciberseguridad. Código de Derecho de la Cibserseguridad.
- Privacidad, protección de datos (RGPD) y valoración y notificación de brechas.
- Derechos digitales
- Seguridad en la administración, estrategia nacional y esquema nacional de seguridad (ENS). Legislación específica para infraestructuras críticas y su protección (PIC)
- Marcos de referencia y mejores prácticas: ISO, SANS, COBIT, ISACA
- Ciberdelincuencia Nacional e Internacional (Convenio de Budapest)

Bloque V: Optativa

Formación CISA

- Entidades certificadoras: funciones y relevancia
- Tipos de certificación y certificados
- Bloque técnico CISA: Auditorias, protección de activos y datos
- Bloque de gestión CISA: Gobierno de la seguridad, mantenimiento y gestión

Código Seguro y QA

- Thread modelling: definiciones y metodología
- DevSecOps como metodología de desarrollo y control de calidad
- Contenedores como herrramienta de desarrollo y buenas prácticas
- Fortificación de contenedores en kubernetes

Bloque VI: TFM