Curso

Ciberseguridad

Seguridad en aplicaciones web e inteligencia en fuentes abiertas

Modalidad presencial (bajo el modelo de Presencialidad Asistida por Tecnología PAT)

COMPETENCIA GLOBAL

Adquirir conocimientos y destrezas de la mano de profesionales y expertos del Centro Criptológico Nacional (CCN CERT de España), reconocido a nivel mundial por el desarrollo de capacidades en ciberseguridad, formación y expedición de las guías CCN-STIC de referencia para organismos públicos y privados.

COMPETENCIAS ESPECÍFICAS

a) Tener una visión general en el ámbito de la ciberseguridad en torno a dos (2) áreas fundamentales: el análisis de seguridad de aplicaciones web y la búsqueda de evidencias digitales como mecanismo de respuesta frente a incidentes cibernéticos.

b) Comprender y definir necesidades de información en cada paso del espectro de obtención de información en Fuentes Abiertas (OSINT).

c) Desarrollar la capacidad de definir utilidades tácticas para acortar procesos de búsqueda, rastreo de elementos informativos de interés, y monitorización de escenarios digitales específicos.

d) Desarrollo de ejemplos prácticos a modo de casos de estudio para poner en práctica los conceptos y aplicar las herramientas tratadas durante las sesiones.

MODALIDAD PRESENCIAL

Bajo el modelo de Presencialidad Asistida por Tecnología PAT

RESUMEN DE CONTENIDOS

Conocimientos previos: Para el desarrollo de las sesiones, los asistentes deben tener conocimientos básicos en:

1. Conceptos básicos de seguridad en TI.
2. Sistemas Linux y Windows.
3. Protocolos y equipamiento de red.
4. Programación web (PHP, ASP.NET, JAVA, etc.)

Sesiones	Actividades de aprendizaje
1 **Esquema Nacional de Seguridad**	Ciberseguridad: Educar y buenas prácticas.
2 **Módulo 1 (sesión am)** *Seguridad en aplicaciones web* **Módulo 1 (sesión pm)** *Autenticación y gestión de sesiones*	1. Arquitecturas, amenazas y seguridad en aplicaciones web. 2. Amenazas de seguridad en aplicaciones web (OWASP). 3. OWASP Top 10. 4. Protocolo HTTP. 5. Herramientas de auditoría. 6. Tipos de autenticación. 7. Cookies de sesión: flag secure y HttpOnly.
3 **Módulo 1** *Ataques comunes al usuario y robo de sesiones*	1. SQL Injection 2. XSS 3. CSRF 4. Clickjacking
4 **Módulo 1 (sesión am)** *Vulnerabilidades en el sistema de ficheros* **Módulo 1 (sesión pm)** *Evidencias digitales y recolección*	1. Directory trasversal. 2. Local y Remote File Inclusion. 3. Subida de archivos. 4. Otras vulnerabilidades. 5. Conceptos, tipos de evidencias y preservación. 6. Procedimientos de adquisición. 7. Adquisición de imágenes y adquisición de memoria
5 **Módulo 1** *Búsqueda de evidencias*	1. Evidencias eliminadas: File carving. 2. Análisis de memoria RAM con Volatility.
6 **Módulo 2 (sesión am)** *Inteligencia en fuentes abiertas* **Módulo 2 - (sesión pm)**	1. Cibervigilancia: Conceptos Esenciales. 2. Ciberprotección y Anonimización en Cibervigilancia.
7 **Módulo 2** *- Arquitectura de redes sociales* *- Herramientas y casos de uso de monitoreo e investigación.* *- Módulo 2 (sesión am)* *- Módulo 2 (sesión pm)*	1. Herramientas y casos de uso de monitoreo e investigación. 2. Organización de Unidades de Cibervigilancia.

RECURSOS TECNOLÓGICOS

Para el desarrollo de las sesiones, los asistentes deben contar con un equipo que tenga una **configuración mínima de:**

· **Hardware:** 8 GB de memoria RAM o superior.
· **Software:** Windows 7 o superior.
· **Entorno de virtualización** para ejecutar las máquinas virtuales a utilizar durante el curso (VMware Player o Virtualbox).
· **Oracle Virtual Box** (última versión disponible en el momento de la instalación).
· Virtualización habilitada en **BIOS.**
· **MS Hyper-V** en estado inactivo o deshabilitado.
· Equipo con procesadores **Dual Core con 8 GB de RAM.** La operativa con **4 GB** sería factible, pero podría presentar dificultades en el desarrollo de la formación.
· Acceso a Internet de **banda ancha** para el desarrollo de las prácticas previstas.