FCSE Nivel 1

Organizado por:

GOBIERNO DE ESPAÑA MINISTERIO DE ECONOMÍA Y EMPRESA

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

OEA OAS

Con la colaboración de:

GOBIERNO DE ESPAÑA MINISTERIO DE ASUNTOS EXTERIORES, UNIÓN EUROPEA Y COOPERACIÓN

universidad de león

AYUNTAMIENTO DE LEÓN

León

LEÓN

Santander

IDB Inter-American Development Bank

Canada

aws

EUROPOL EC3 European Cybercrime Centre

INTERPOL

PROFESOR

José Luis Narbona

Taller 7

Análisis Forense

Duración taller: 20 horas

Descripción

Finalizado este módulo, el asistente dispondrá de conocimientos y capacidades para poder llevar a efecto un análisis forense digital enfocado a arquitecturas Windows. Para ello se le hará conocedor de las arquitecturas internas de los sistemas operativos y versiones, así como su operativa. Finalizado el módulo, igualmente será conocedor de las posibilidades y diversas metodologías para la localización de evidencias y su posterior análisis.

En el desarrollo del módulo se capacitará al asistente para ser resolutivo en la planificación, desarrollo y la ejecución de análisis forenses desde una perspectiva de análisis en vivo, así como de análisis de tipo offline: Metodología forense, procesos y ficheros, extracción de memoria RAM o cómo hacer un Triage serán los principales temas a tratar. En el siguiente párrafo podrá encontrar el contenido del módulo de un modo detallado.

Temario

1. Metodología de análisis forense y peritaje
2. Adquisición y clonado de evidencias
3. Triage básico
4. Triage con WMI y Powershell
5. La captura de la memoria
6. El Registro de Windows
7. Herramientas de búsqueda ciega selectiva
8. Los eventos en Windows
9. Artifacts: Papelera, Prefetching, USBs, LNKs, Jumplists, Recents, Shellbags, Tareas programadas, Shadow Copies, ADS, Navegadores, Correo, aplicaciones Metro,
10. Malware: características, ocultación, servicios y procesos de Windows, persistencia, descubrimiento de ataques laterales
11. Análisis de Memoria Ram, Técnicas de análisis remota o local, Volatility/Rekall, Volcado de archivos, Credenciales en memoria
12. Ficheros: Sistema de ficheros NTFS (MFT, Logfile y UsnJrnl:$J) y ficheros eliminados
13. Monitorización: Sysmon

PROFESOR

Simón Roses

Taller 8

OSINT: herramientas, técnicas de búsqueda y análisis de información

Duración taller: 10 horas

Descripción

La sociedad de la información es un concepto del siglo XX nacido de la integración de las nuevas tecnologías (TIC) en las relaciones humanas y sociales. Internet y toda la información que contiene es un claro ejemplo de cómo las personas deseamos compartir pensamientos, ideas, sucesos, etc. Desde 2005, la UNESCO ha decidido elevar el concepto hacia la sociedad del conocimiento, pues el reto ya no es conseguir que fluya la información, sino que ésta aporte valor a las civilizaciones. Es así como saber buscar la información adecuada y analizarla puede ayudarnos a construir verdadero conocimiento que facilite la toma de decisiones en una organización y en nuestra propia vida.

En esta sesión se utilizarán algunas técnicas utilizadas para encontrar información en fuentes abiertas en Internet. También se hablará de algunas herramientas imprescindibles para localizar aquello que resulte de interés. Además, se tratará la importancia de utilizar métodos y técnicas propios del análisis de inteligencia para procesar la información proveniente de Fuentes Abiertas y metodologías específicas para la detección de tendencias y la interpretación de la realidad como el Time Line y los Mapas Mentales.

Temario

1. **Descripción y casos prácticos de uso**
2. **Fases del proceso**
   - Requisitos
   - Fuentes de información
   - Adquisición
   - Procesamiento
   - Análisis
   - Inteligencia
3. **Herramientas comunes**
   - Búsquedas parametrizadas en buscadores
   - Buscadores de personas
   - Herramientas específicas
   - Datos y Metadatos
   - Explorando APIs
   - Visualización de datos
3. **Profiling de usuarios**

PROFESOR

Alexandre Rodríguez

Taller 9

Forense en la nube

Duración taller: 5 horas

Descripción

En un entorno tecnológico cada vez más deslocalizado, el almacenamiento de información remota y sincronización entre nuestros dispositivos se ha convertido en una práctica común. Compartimos ficheros con terceros, tomamos notas que consultamos desde cualquier equipo y en definitiva, trabajamos en movimiento.

El propósito del taller es tomar conciencia de la información residual que las tecnologías de almacenamiento en la nube dejan en los diferentes equipos de trabajo desde los que operamos, analizando los mecanismos de conexión que empleamos, la información que transmiten y las trazas de información en disco y volátil que su empleo dejan. El análisis será enfocado de manera procedimental y realizado sobre las soluciones más comúnmente usadas y a su última versión disponible, con la intención de que los asistentes puedan adquirir una serie de técnicas y aproximaciones que les permitan enfocar el análisis de las mismas o de otras similares que pudieran tener que afrontar.

Temario

1. **Introducción y conceptos básicos**
    - Historia y evolución
    - Arquitectura general de las soluciones
2. **Análisis forense**
    - Mecanismos de conexión
    - Información transmitida
    - Información almacenada localmente
        - Análisis de artefactos en disco
        - Análisis volátil
3. **Prácticas**

PONENTE

Carlos Álvarez

Seminario ICANN

Duración seminario: 5 horas

Descripción

El entrenamiento ofrece estrategias, técnicas y herramientas a los investigadores, fiscales y otros agentes de la ley, que los profesionales en seguridad operacional y threat research utilizan para identificar diferentes formas de actividad maliciosa o delictiva que haga uso de recursos del Sistema de Nombres de Dominio (DNS). El objetivo es familiarizar a los asistentes con el DNS, permitirles conocer los tipos de información que están disponibles en el DNS y cómo acceder a ella para identificar infraestructura delictiva o identificar a los responsables de determinada actividad, cuando esto es posible.