LEA Level 2

Organizers:

Collaborators:

PROFESSOR

César Lorenzana

Workshop 10

Cybersecurity Intelligence

Workshop duration: 35 hours

Description

The course initially focuses on intelligence, understanding intelligence as the materialization of the classic intelligence cycle (management, gathering, development and dissemination).

For this purpose, the information gathering phase will include research techniques on different computer elements that differ from the forensic context.

Syllabus

1. **Introduction**
   - Intelligence and research basis
   - Information gathering techniques by means of open sources
     - Tools required and OSINT technique
     - Browsers
     - Monitoring of events
     - Domains and websites
2. **Social Networks**
   - Introduction
   - Information gathering on Twitter
   - Information gathering on LinkedIn
   - Information gathering on Facebook (I)
3. **Social Networks (II)**
   - Information gathering on Facebook – final
4. **Forensic (I)**
   - Introduction to Forensic Analysis
   - Important points for research
     - Windows Analysis: user data and technical data.
5. **Forense (II)**
   - Other operating systems: Apple and Linux
6. **Forense (III)**
   - Mobile telephone technology
   - “Ad hoc” scenarios
     - Traffic analysis
     - Malware analysis
     - Others
7. **CTF**
   - Practical exercise relating to information gathering to solve and clarify an event of interest.
   - All the elements explained in the course will be applied in this scenario.

PONENTE

Carlos Álvarez

Master Class ICANN

Hours: 5 hours

Description

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.

Pendiente traducción