

Cybersecurity Summer Bootcamp

Del 17-28 Julio del 2018
León, España

www.incibe.es/summer-bootcamp
Más información: contacto_summerBC@incibe.es

LEÓN - 2018

#CyberSBC18

FCSE Nivel 2

Organizado por:



OEA OAS

Con la colaboración de:





Javier Rodríguez



Francisco Javier García
Fernández

Taller 10

Inteligencia en ciberseguridad

Duración: 35 horas

Descripción

La temática del curso versa inicialmente en la parte de inteligencia, entendiendo por inteligencia la materialización del ciclo de inteligencia clásico (dirección, obtención, elaboración y difusión).

Por ello, para la fase de obtención se mostrarán técnicas de investigación sobre distintos elementos informáticos y que dimanen del ámbito forense.

Temario

1. Introducción

- Fundamentos inteligencia e investigación
- Técnicas de obtención de información a través de fuentes abiertas
 - Herramientas necesarias y doctrina OSINT
 - Buscadores
 - Seguimiento de eventos y acontecimientos
 - Dominios y páginas web

2. Redes Sociales

- Introducción
- Obtención en Twitter
- Obtención en LinkedIn
- Obtención Facebook (I)

3. Redes Sociales (II)

- Obtención Facebook - final

4. Forense (I)

- Introducción al análisis forense
- Qué es lo importante para la investigación
 - Análisis Windows: datos de usuario y datos técnicos.

5. Forense (II)

- Otros sistemas operativos: Apple y Linux

6. Forense (III)

- Telefonía móvil
- Escenarios "ad hoc"
 - Análisis de tráfico
 - Análisis de malware
 - Otros

7. CTF

- Ejercicio práctico donde se desarrollará un ejercicio que consistirá en la obtención de información para la resolución y esclarecimiento de un hecho de interés.
- En este escenario se aplicará todo lo mostrado en durante el curso.





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.

