

Cybersecurity Summer Bootcamp

July 17-28, 2018
León, Spain

www.incibe.es/summer-bootcamp
More information: contacto_summerBC@incibe.es

LEÓN - 2018

#CyberSBC18

LEA Level 1

Organizers:



Collaborators:





Lorenzo Martínez

Workshop 7

Forensic Analysis

Hours workshop: 20 hours

Description

When this training is completed, the participant will have the knowledge and ability to be able to carry out a digital forensic analysis under Windows architecture. For this purpose, the participant will be instructed in the operating system internal architectures, as well as in their performance. When the module has been completed, they earn a knowledge in the possibilities and methodologies for the location of evidences and their subsequently analysis.

Syllabus

1. Methodology of forensic and expert analysis
2. Evidence acquisition and cloning
3. Basic triage
4. Triage with WMI and Powershell
5. Memory capture
6. Windows Registry
7. Selective blind search tools
8. Windows events
9. Artifacts: Recycle bin, Prefetching, USBs, LNKs, Jumplists, Recents, Shellbags, Programmed tasks, Shadow Copies, ADS, Browsers, Email, Metro applications.
10. Malware: characteristics, concealment, Windows services and processes, persistence, discovery of lateral attacks
11. RAM memory analysis, remote or local analysis techniques, volatility/rekall, file dumping, memory credentials
12. Files: NTFS files system (MFT, Logfile and Usnjrnl:\$J) and deleted files
13. Monitoring: Sysmon





Simón Roses

Workshop 8

OSINT: tools, search techniques, and information analysis

Hours workshop: 10 hours

Description

The information society is a 20th century concept born from integration of new technologies (TIC) in human and social relationships. The internet and all its information is a clear example of how people want to share thoughts, ideas, events, etc. Since 2005, UNESCO has elevated the concept to that of the knowledge society as the challenge is no longer to achieve a flow of information but to ensure that flow contributes value to civilization. Knowing how to search for the right information and analyse it can help us build true knowledge that facilitates decision making in an organization and in our own lives.

In this session, some of the techniques used to find information from open sources on the Internet will be used. It will also look at some essential tools for locating what most interests us. There is also the importance of using own analysis methods and techniques for intelligence analysis to process information from Open Sources and specific methodologies for the detection of trends and the interpretation of reality such as Time Line and Mental Maps.

Syllabus

1. **Description and practical use cases**
2. **Process phases**
 - Requirements
 - Information sources
 - Acquisition
 - Processing
 - Analysis
 - Intelligence
3. **Common tools**
 - Parametrized searches in search engines
 - People search engines
 - Specific tools
 - Data and metadata
 - Exploring APIs
 - Visualizing data
4. **User profiling**





Alexandre Rodríguez

Workshop 9

Forensics in the cloud

Hours workshop: 10 hours

Description

In an increasingly delocalized technological environment, remote storage of information and synchronization between our devices has become common practice. We share files with third parties, we take notes that we consult from any computer and ultimately, we work on the move.

What this workshop proposes is to be aware of the residual data that cloud storage technologies leave on the different work devices from which we operate, analysing the connection mechanisms we use, the information they transmit and the traces of information on discs and volatile data left by after use. The analysis will be focussed on a procedural approach and will use the most common solutions and their latest available versions, so that those present can acquire a series of techniques and approaches that allow them to focus their own analysis in the same or other, similar areas.

Syllabus

1. Introduction and basic concepts

- History and evolution
- General architecture and solution

2. Forensic analysis

- Connection mechanisms
- Transferred data
- Locally stored data
 - Analysis of disk artefacts
 - Volatile analysis

3. Practical cases





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

