summer bootcamp

LEÓN - 2016

Organised by:

GOBIERNO DE ESPAÑA MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

10 incibe_ TRABAJANDO POR LA CONFIANZA DIGITAL

GOBIERNO DE ESPAÑA MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

CNPIC CENTRO NACIONAL PARA LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS

Organización de los Estados Americanos | Más derechos para más gente

With the support of:

universidad de león

AYUNTAMIENTO DE LEÓN

León Cuna del Parlamentarismo

FIRST Improving Security Together

CONTENTS

1. BACKGROUND

As reports show, the shortage of qualified professionals in cybersecurity is a reality. According to the CISCO 2014 report, there is worldwide shortage of more than one million cybersecurity[1] professionals and, according to the ISACA 2015 report, the number of openings is expected to rise to 2 million by 2019[2]. It is for this reason that cybersecurity powerhouses such as the United States and the United Kingdom are launching highly-skilled, practical training programmes (BootCamp format) in order to train professionals in several cybersecurity-related areas.

Some of the initiatives that we can highlight[3] include those carried out by leading universities such as San José State University and SVBCC (Silicon Valley Big Data and Cybersecurity Center), Stanford University, the University of Delaware through the USCC (U.S. Cyber Challenge), James Madison University, the University of Maryland, the University of Texas at Dallas, Lowcountry Tech Academy in Charleston, Penn State University through its campus at Penn State Berks, Norfolk State University and De Montfort Leicester University (DMU) in the UK.

Other noteworthy initiatives include those carried out by other types of public and private entities such as SANS Cyber Academy, Wright-Patterson Air Force Base and the National Security Agency (NSA) through 43 campuses located all over the United States.

Figure 1 - References to cybersecurity training programmes that employ the "BootCamp" format

In light of this, INCIBE will organise the first edition of the Summer BootCamp (powered by Cybercamp) to take place in the summer of 2016, in order to provide, as currently they were doing in the winter edition of CyberCamp, training activities and specific Cybersecurity training to:

- State Law Enforcement Authorities (FCSE).

[1] http://noticias.lainformacion.com/espana/espana-se-prepara-para-el-boom-de-los-empleos-de-ciberseguridad_3AyB6L7qqPXOPSI0Wx2q25/

[2] http://blog.firebrandtraining.co.uk/2016/02/2016-cyber-security-skills-gap.html

[3] Some noteworthy references:
http://www.hrreview.co.uk/hr-news/recruitment/cyber-security-boot-camp-turns-graduates-cyber-experts-defend-businesses/56444
http://www.computerworlduk.com/news/careers/sans-launches-boot-camp-teach-cyber-security-in-8-weeks-3607928/
http://www.wpafb.af.mil/news/story.asp?id=123262849
http://www.sjsu.edu/cybersecurity/
http://www.uscyberchallenge.org/2015/07/20/u-s-cyber-challenge-and-delaware-universities-to-host-cybersecurity-boot-camp-competition/
http://news.stanford.edu/news/2015/august/cyber-boot-camp-082415.html
http://www.dmu.ac.uk/about-dmu/news/2015/august/cyber-security-bootcamp-will-train-experts-of-the-future.aspx
http://www.jmu.edu/events/cs/2015/07/27-31-cyber-defense-boot-camp-va.shtml
https://www.nsa.gov/public_info/press_room/2015/gencyber_summer_camps.shtml
http://www.computerworlduk.com/news/careers/sans-launches-boot-camp-teach-cyber-security-in-8-weeks-3607928/
http://www.bbc.co.uk/newsbeat/article/19515213/first-boot-camp-gets-young-people-into-cybersecurity
http://cyber.umd.edu/education/cyber-defense
http://www.utdallas.edu/k12/cyber/
https://niccs.us-cert.gov/education/cyber-camps-clubs
http://www.bk.psu.edu/CE/computer-and-cyber-security-camp.htm
https://www.nsu.edu/cset/csetgraduate/cybersecurity/index

- Professionals involved in the management and operation of Computer Emergency Response Teams (CERTs)

Organising this Summer Bootcamp will contribute towards making the city of León and Spain a Worldwide Centre of Reference in Cybersecurity training, making full use of the opportunity to carry out the first Spanish-speaking cybersecurity BootCamp. Furthermore, it will comprise groups with worldwide international presence.

In order to carry out this initiative, INCIBE provides its national and international positioning, its knowledge in cybersecurity and its experience in the field by designing the programme and providing top professors both from its staff and from leading Spanish companies dedicated to the field of cybersecurity.

Additionally, this project requires the collaboration of partners and reference entities in order to become a reality, such as:

- Organisation of American States (OAS).
- European Police Office (EUROPOL).
- Forum of Incident Response and Security Teams **(FIRST).**
- Spanish Ministry of Foreign Affairs and Cooperation (MAEC).
- Spanish Ministry of Internal Affairs (MINIT).
- Spanish Government Department for Telecommunications and the Information Society (SETSI).
- Castile-León Regional Government, through the Economic Development Agency (ADE)
- León City Council.
- University of León (ULe).
- Private partners.

2. EVENT DESCRIPTION

The Summer BootCamp 2016 is an international event with a highly practical format, which aims to train and instruct 100 State Law Enforcement Authorities specialists and 100 public CERTs technicians or public organisation staff who work in issues directly related to cybersecurity.

The event will take place in León (Spain) in 4 headquarters, depending on the activities being carried out.

- INCIBE (Spanish National Institute of Cybersecurity): Workshops (Groups 1 and 2).
- CRAI-TIC (Learning and Research Resource Centre-ICT) (University of León): Technical Workshops (Groups 3 - 10).
- León Auditorium: Lectures
- León West Community Auditorium: International CyberEx Review.

Illustration 2 - Location1

Summer BootCamp 2016 will take place during the last two weeks of July (17-30 July) according to the following calendar:

	July '16						
	Mon	Tues	Wed	Thur	Fri	Sat	Sun
	11	12	13	14	15	16	17
Morning							
Afternoon							Inauguration
	18	19	20	21	22	23	24
Morning	Technical Workshops (FCSE / CERTs)			Technical Workshops (FCSE)	International CyberEx Review (CERTs) Master Seminars (FCSE / CERTs) International CyberEx review (CERTs) Lectures (FCSE / CERTs)		
Afternoon			HELIOS Presentation (Spanish FCSE) International CyberEx Presentation (CERTs Presentation: HELIOS (Spanish FCSE) Presentation: International CyberEx (CERTs)	International CyberEx (CERTs)			
	25	26	27	28	29	30	31
Morning	Technical Workshops (FCSE / CERTs)				Master Seminars (FCSE / CERTs) Lectures (FCSE / CERTs)	Closing Events	
Afternoon							

Figure 1 – Summer BootCamp 2016 calendar

The event is targeted at the:

- FCSE Training:
  - FCSE staff in active employment who work in operational units related to the cybersecurity of countries belonging to the OAS.[4]
  - FCSE staff in active employment who work in operational units related to the cybersecurity of countries belonging to EUROPOL.[5]
  - Spanish territory FCSE staff in active employment who work in operational units related to cybersecurity.[6]
- CERT Training:
  - Public CERT staff in active employment in Latin American countries belonging to the OAS. [4]
  - Public institution staff in active employment who work in issues directly related to cybersecurity (university professors and researchers, public institution cybersecurity technicians, etc.) in Latin American countries belonging to the OAS. [4]

[4] In this case, admission to the course is subject to prior validation by OAS.

[5] In this case, to be admitted t the course the application must come from the competent body of the country belonging to EUROPOL.

[6] In this case, admission to the course is subject to prior validation by the Spanish Cybernetic Coordination Office (OCC), part of the National Centre for the Protection of Critical Infrastructures (CNPIC).

5 groups will be created, each group consisting of 20 people. They will receive advanced training. As regards the FCSEs, they will receive practical training on issues specific to this organisation. All training will be supported by tools focused on technological research of cybercrime and cyberterrorism.

Additionally, another 5 groups will be created, also with 20 people in each group. They will receive advanced training in the management of level 2 and 3 incidents. It will mainly focus on practical cases related to the day-to-day activities of a CERT operator, resolving incidents related to advanced malware (APTs, Botnets, Ransomwares, etc.) and reversing, forensic analysis, exploits analysis, etc. Furthermore, an introduction of challenges or cyber excercises or CTfs will be given, based on INCIBE´s experience gained from CYBEREX and the Cybercamp 2014 and 2015.

Classes will be in English and Spanish, depending on the reference language of each group. Joint activities will be in Spanish, with a simultaneous translation service included for English-speaking participants.

3. PROGRAMMES

Given the practical nature of the training, a programme has been developed aimed at specialisation in the form of 5-hour technical and practical workshops, in which drills, challenges and a variety of practical exercises will be conducted. Each participant will have a team at their disposal to facilitate these tasks.

The course will also incorporate 2-hour lectures of more theoretical content; these will be delivered to all 200 participants.

Given their specialised nature, both courses will be worth 6 ECT credits from the University of León. Sessions will be delivered by first-class speakers and trainers who are leaders in their subjects at the national and international levels.

Details of the proposed programmes and the general content of each workshop is shown in the following agenda[7]

[7] This programme is provisional and may be subject to changes made by the organisation. Any changes will be duly notified using established channels.

Date		Activity Group 1	Activity Group 2	Activity Group 3	Activity Group 4	Activity Group 5
Week 1	Monday 18	**Workshop 1** OSINT: tools, search techniques and information analysis	**Workshop 3** Malware Analysis (I)	**Workshop 7** Encryption, Anonymous navigation and Deep Web	**Workshop 2** Forensic analysis in mobile devices	**Workshop 8** Advanced Hacking
	Tuesday 19	**Workshop 2** Forensic analysis in mobile devices	**Workshop 4** Malware analysis (II)	**Workshop 3** Malware Analysis (I)	**Workshop 1** OSINT: tools, search techniques and information analysis	**Workshop 7** Encryption, Anonymous navigation and Deep Web
	Wednesday 20	**Workshop 3** Malware Analysis (I)	**Workshop 8** Advanced Hacking	**Workshop 4** Malware analysis (II)	**Workshop 5** Forensic analysis of Windows systems (I)	**Workshop 1** OSINT: tools, search techniques and information analysis
		For Spanish FCSE´s, afternoon session, HELIOS presentation practical lecture				
	Thursday 21	**Workshop 4** Malware analysis (II)	**Workshop 1** OSINT: tools, search techniques and information analysis	**Workshop 2** Forensic analysis in mobile devices	**Workshop 6** Forensic analysis of Windows systems (II)	**Workshop 5** Forensic analysis of Windows systems (I)
	Friday 22	**Lecture 1** The business of cybercrime **Lecture 2** Offensive security				
Week 2	Monday 25	**Workshop 7** Encryption, Anonymous navigation and Deep Web	**Workshop 5** Forensic analysis of Windows systems (I)	**Workshop 1** OSINT: tools, search techniques and information analysis	**Workshop 8** Advanced Hacking	**Workshop 6** Forensic analysis of Windows systems (II)
	Tuesday 26	**Workshop 8** Advanced Hacking	**Workshop 6** Forensic analysis of Windows systems (II)	**Workshop 5** Forensic analysis of Windows systems (I)	**Workshop 7** Encryption, Anonymous navigation and Deep Web	**Workshop 3** Malware Analysis (I)

Date		Activity Group 1	Activity Group 2	Activity Group 3	Activity Group 4	Activity Group 5
	Wednesday 27	**Workshop 5** Forensic analysis of Windows systems (I)	**Workshop 2** Forensic analysis in mobile devices	**Workshop 6** Forensic analysis of Windows systems (II)	**Workshop 3** Malware Analysis (I)	**Workshop 4** Malware analysis (II)
	Thursday 28	**Workshop 6** Forensic analysis of Windows systems (II)	**Workshop 7** Encryption, Anonymous navigation and Deep Web	**Workshop 8** Advanced Hacking	**Workshop 4** Malware analysis (II)	**Workshop 2** Forensic analysis in mobile devices
	Friday 29	**Lecture 3** 5 **Lecture 4** Industrial Cybersecurity				

SPECIALISATION COURSE FOR CERTs

Date		Activity Group 1	Activity Group 2	Activity Group 3	Activity Group 4	Activity Group 5
Week 1	**Monday 18**	**Workshop 12** Windows and Linux forensic analysis (I)	**Workshop 2** Forensic analysis in mobile devices	**Workshops 3 and 4** Malware analysis	**Workshop 10** Security in networks (I)	**Workshop 9** Management of security incidents
	Tuesday 19	**Workshop 13** Windows and Linux forensic analysis (II)	**Workshop 12** Windows and Linux forensic analysis (I)	**Workshop 9** Management of security incidents	**Workshop 11** Security in networks (II)	**Workshop 10** Security in networks (I)
	Wednesday 20	**Workshop 9** Management of security incidents	**Workshop 13** Windows and Linux forensic analysis (II)	**Workshop 2** Forensic analysis in mobile devices	**Workshops 3 and 4** Malware analysis	**Workshop 11** Security in networks (II)
		CyberEx International Presentation				
	Thursday 21	International CyberEx (8:00pm) INCIBE				

	Date	Activity Group 1	Activity Group 2	Activity Group 3	Activity Group 4	Activity Group 5
	Friday 22	International CyberEx Review **Lecture 2** Offensive security				
Week 2	**Monday 25**	**Workshop 10** Security in networks (I)	**Workshop 9** Management of security incidents	**Workshop 12** Windows and Linux forensic analysis (I)	**Workshop 2** Forensic analysis in mobile devices	**Workshops 3 and 4** Malware analysis
	Tuesday 26	**Workshop 11** Security in networks (II)	**Workshop 10** Security in networks (I)	**Workshop 13** Windows and Linux forensic analysis (II)	**Workshop 12** Windows and Linux forensic analysis (I)	**Workshop 2** Forensic analysis in mobile devices
	Wednesday 27	**Workshops 3 and 4** Malware analysis	**Workshop 11** Security in networks (II)	**Workshop 10** Security in networks (I)	**Workshop 13** Windows and Linux forensic analysis (II)	**Workshop 12** Windows and Linux forensic analysis (I)
	Thursday 28	**Workshop 2** Forensic analysis in mobile devices	**Workshops 3 and 4** Malware analysis	**Workshop 11** Security in networks (II)	**Workshop 9** Management of security incidents	**Workshop 13** Windows and Linux forensic analysis (II)
	Friday 29	**Lecture 3** APT: Use cases **Lecture 4** Industrial Cybersecurity				

3.1. Workshop 1 – OSINT: tools, search techniques and information analysis

The information society is a 20th-Century concept, born out of the integration of new technologies (ICT) into human and social relations. The Internet and all the information it contains is a clear example of the way that people wish to share thoughts, ideas, events, etc. Since 2005, UNESCO has decided to elevate the concept to the knowledge society; now, the challenge is not in achieving information flow, but rather in making this bring value to civilisations In this way, knowing how to find and analyse the relevant information can help us to construct true knowledge to facilitate decision-making in organisations and in our own lives.

In this session, we will use different techniques to find information in open sources on the Internet. We will also speak about some essential tools for locating the information we're interested in. The session will also deal with the importance of using intelligence analysis methods and techniques to process Open Source information, in addition to specific techniques for detecting trends and interpreting the facts, such as Time Lines and Mental Maps.

The contents are as follows:

- Description and practical examples
- Process stages
    - Requirements
    - Sources of information
    - Acquisition
    - Processing
    - Analysis
    - Intelligence
- Common tools
    - Search parameters in search engines
    - People searches
    - Specific tools
        - TheHarvester
        - Tinfoleak
        - Cree.py
        - Social media API
        - Maltego
        - Palantir
- Profiling users

3.2. Workshop 2 - Forensic analysis in mobile devices

Smartphones and tablets have become an indispensable tool in users' day-to-day lives. These devices are not only able to store information about users' address books, photographs, messages, music or videos; they can also store a great quantity of information that can be particularly important in investigation and/or forensic analysis.

The widespread use of mobile devices, on many occasions without a great deal of security measures for access on the part of people in general, including cybercriminals,

opens a gateway to obtaining information that can decide the outcome of a police investigation.

For that reason, this session aims to examine in depth the knowledge required to run forensic analysis on mobile devices, and to show how to correctly use tools that facilitate that analysis in order to extract information that may be used in a real case.

- Introduction
    - Key concepts in forensic analysis Types of mobile devices.
    - Features of mobile platforms.
        - Android
        - iOS
        - Others: BlackBerry and Windows Phone
- Forensic analysis procedures applied in the context of mobile devices
    - Stages of forensic analysis
    - Chain of custody
    - Evidence management
- Data cloning
    - Android, iOS, Windows Phone, Blackberry
    - Tools
- Analysis of recovered information
    - Analysis of volatile memory
    - Analysis of non-volatile memory
        - Files
        - Free space
    - Recovery and analysis of deleted files
    - Tools

3.3. Workshop 3 - Malware analysis (I): Introduction, tools, preparation of environments and static analysis

Currently, cybersecurity issues related to malicious code or malware continue to grow. In fact, many organisations still consider malicious code to be the main source of attacks.

The aim of this session is to offer an introduction to malware in order that law enforcement agents have the basic knowledge for malware analysis and the recommended procedures and good practices in the event that they have to manage cybersecurity incidents related to malicious code.

We will also present tools and applications that allow relevant information to be obtained from the malware.

The session will be structured around the following points:

- Introduction to malware
- The characteristics, types and evolution of malware
- Mass attacks vs targeted attacks.
- Vectors of infection
- Responding to an infected machine
- Strengthening equipment. Techniques to avoid infection
- Static malware analysis

- Preparation of the work environment, isolation
- Analysis procedure
- Finding information on malware
- System tools and utilities
- Third party utilities

3.4. Workshop 4 - Malware analysis (II): Introduction, tools, preparation of environments and dynamic analysis

Complementing Workshop 3 - Malware analysis (I): Introduction, tools, preparation of environments and static analysis, the session will be structured around the following points:Workshop 3 - Malware analysis (I): Introduction, tools, preparation of environments and static analysis

- Dynamic malware analysis
  - Preparation of the work environment, isolation
  - Analysis procedure
  - Finding information on malware
  - System tools and utilities
  - Third party utilities
  - Analysis of network traffic generated by malware

3.5. Workshop 5 - Forensic analysis of Windows systems (I): Introduction and taking of evidence

The objective of this procedure is to provide answers to the following questions: what?, where?, when?, why?, who? and how?

It is being used very diverse areas, included amongst which are:

- Prosecution of offences like financial fraud, tax evasion, harassment or child pornography
- Discrimination or harassment cases
- Insurance investigations
- Recovery of deleted files
- Intellectual property theft cases
- Cyberterrorism
- Ensuring companies´ resilience, that is to say, their ability to recover in the face of attacks

The session will be structured around the following points:

- Stages of forensic analysis
  - Preservation
  - Acquisition
    - Acquisition of RAM memory
    - Acquisition of windows registry
    - Acquisition of network traffic.
  - Documentation
  - Chain of custody

3.6. Workshop 6 - Forensic analysis of Windows systems (II): Analysis and recording of evidence

Complementing Workshop 5 - Forensic analysis of Windows systems (I): Introduction and taking evidence, t the session will be structured around the following points: Workshop 5 - Forensic analysis of Windows systems (I): Introduction and taking of evidence

- Stages of forensic analysis
    - Analysis
        - Analysis of RAM memory
        - Analysis of windows registry
        - Analysis of network traffic.
    - Documentation
    - Presentation
    - Chain of custody

3.7. Workshop 7 - Encryption, anonymous navigation and Deep Web.

The Deep Web is a part of the internet which is difficult to trace; it is thought to be much larger in size than the so called known internet, which is automatically indexed by search engines such as Google or Bing. Inside the Deep Web, where are networks or systems using the Tor Project, which was created to guarantee anonymity through encryption techniques, providing its users with privacy. Because of these features, it is used by criminals to hide their identities and commit many crimes.

This session aims to give a definition of the Deep Web, in addition to the main anonymous browsing methods or protocols and the different ways, both legitimate and illegitimate. in which they are put to use. Finally, there will be a detailed description of the structure and functioning of TOR, the best known anonymous network.

- Deep Web
- Encryption and its importance for anonymity
- Anonymous browsing: TOR, I2P, Freenet
    - Uses of the Deep Web
- TOR
    - Functioning
    - Structure
    - Illegitimate uses of TOR
        - TOR–Bticoin synergy: Black market
            - SilkRoad
            - SilkRoad Reloaded
        - Botnets
    - De-anonymisation attacks

3.8. Workshop 8 - Advanced Hacking

Yet to be developed.

3.9. Workshop 9: Gestión de incidentes de seguridad.

A CERT's main purpose is to provide a support service for security incident management, responsible for assisting with both technical and organisational measures for the different phases of the incident. We will therefore review the best practices and tools to be used in incident management.

- Formal aspects of CERTs
- Incident management stages:
    - Preparation
    - Identification
    - Containment
    - Erradication
    - Recovery
    - Lessons learned

3.10. Workshop 10 and 11: Security in networks.

One of the most common activities in the investigation and mitigation of incidents is the analysis of network devices with the objective of gathering as much information as possible about the type of attack, the assets involved and possible remediation. We will therefore study in great detail the devices involved in the security of a network and the analysis of the traces they leave.

- Intrusion Detection
- Secure connection services
- Perimeter security and secure segmentation
- Security events
- Wireless networks and VoIP

3.11. Workshops 12 and 13: Forensic analysis of Windows and Linux devices.

Windows uses mechanisms that leave traces of users' activity: the programs they use, access, connections and applications, whether they have used browsers or downloaded or run any programs. All this information is of vital importance for forensic analysis. In addition, given the large number of attacks on Linux servers, we will analyse the actions to be taken with this type of architecture.

The contents are as follows:

- Stages of forensic analysis
    - Preservation
    - Acquisition
        - Acquisition of RAM memory
        - Acquisition of windows registry
        - Acquisition of network traffic.
    - Analysis
        - Analysis of RAM memory
        - Analysis of windows registry
        - Analysis of network traffic.

- Documentation
- Presentation
- Chain of custody


GOBIERNO
DE ESPAÑA
MINISTERIO
DE INDUSTRIA, ENERGÍA
Y TURISMO


incibe_
2006-2016
TRABAJANDO POR
LA CONFIANZA DIGITAL