Syllabus

FCSE basic level

Cybersecurity
Summer
BootCamp

2017

Cybersecurity Summer BootCamp 2017
18-29 july - León (Spain)
www.incibe.es/en/summer-bootcamp

Organised by:

GOBIERNO DE ESPAÑA — MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

OEA | OAS

With the cooperation of:

universidad de león

AYUNTAMIENTO DE LEÓN

León Cuna del Parlamentarismo

GOBIERNO DE ESPAÑA — MINISTERIO DE ASUNTOS EXTERIORES Y DE COOPERACIÓN

Santander

IDB Inter-American Development Bank

EUROPOL EC3 European Cybercrime Centre

INTERPOL

PROFESSORS

Jesús Díaz Vico

Francisco J. Rodríguez

Workshop 10

Introduction to Deep Web

Hours workshop: 20 hours

Description

Internet is the global network composed by hundreds of thousands of computers to which we usually access through a web browser (Firefox, Chrome, Safari...) and with the help of search engines (Google, Bing, DuckDuckGo...). Nevertheless, the information that we can obtain through this 'common' mechanisms is just a small portion of the total. Terms such as Deep Web and Dark Web are each time more frequent in the technological world, especially after scandals like Silk Road and other illegal markets or the support received from privacy activist like Edward Snowden and Julian Assange.

Syllabus

1. **Introduction to anonymous networks**
   - Surface web / Deep Web / Dark web
   - Proxys Tor2Web
   - The two sides of the coin: privacy and anonymity vs criminal activities
2. **Types of anonymous systems and networks**
   - Most popular anonymous networks and its chronology
   - Other networks and tools
   - DC-nets, mix-nets and onion networks
   - OutProxy / Inproxy networks
   - Linux distributions
   - Tor in IOS and Android
3. **Onion networks and Tor**
   - Internals of onion networks
   - Directory authorities
   - Consensus document. Voting process
   - Flags assigned to nodes
   - Types of nodes (guard, middle, exit)
   - Node mapping, statistics...
   - Bridges / cache directories / circuit establishment
   - Hidden services and rendezvous points negotiation
   - Descriptors
   - Information encryption. Onion encryption
   - Practice
   - Attacks to the TOR network
4. **Other Onion networks**
5. **Other tools: Stem, ARM**

PROFESSOR

Pedro Sánchez

Workshop 11

Introduction to mobile forensics

Hours workshop: 10 hours

Description

According to reports by different consultancy firms, it is estimated that mobile devices are more frequently used in comparison with traditional computers in terms of navigation and use. Communications, social networks, financial transactions and videogames make these devices an ideal target for hackers.

On the other hand, there is an increasing number of cases in which the spies protected by many governments use mobile devices as a weapon and a mechanism for intrusion into companies and public figures.

The course is aimed at offering a basic view on security of the different mobile devices and how to make a forensic analysis of these devices if an attack or intrusion occurs.

Syllabus

1. **Introduction to mobile devices**
   - Background and evolution: mobile devices / operating systems / new threats in mobile environments
   - WiFi Networks: GSM / 3G / 4G / Bluetooth / NFC
2. **Basic architecture of mobile devices**
   - IOS / Android / Windows Phone
3. **Forensic analysis**
   - SIM/USIM cards
     - Description and internal architecture
     - Data in SIM / USIM cards
     - Physical cloning of SIM cards
     - Evidence acquisition
   - Windows phone devices
     - Windows phone architecture / memory structure / file structure / internal architecture / file system
     - Recovery
     - SD cards
     - Evidence acquisition / cloning vs files / extraction tools / business utilities
   - Android devices
     - Android internals / YAFFS2 files system / system configuration and information
     - Evidence acquisition / memory analysis / device locking/unlocking / logs in Android
     - Forensics analysis of applications
   - IOS devices
     - Acquisition: from iTunes Backup, from iCloud; of logical copy
     - Analysis of acquired evidence
     - Forensics analysis of applications
     - Analysis with free and business tools

PROFESSOR

Josep Albors

Workshop 12

Introduction to malware

Hours workshop: 10 hours

Description

The objective of this course is for the students to get familiar with malware analysis and have enough knowledge to analyze malware fast enough, mainly focusing in dynamic analysis. We will be explaining and using tools in a way that the students can continue their practices once the course is over and they can apply the knowledge achieved in a daily basis.

Syllabus

1. **Basic concepts**
   - Basic concepts of IT Security
   - Brief history of malware
   - Malware spreading techniques
   - Operating systems and their vulnerabilities
   - Malware on mobile devices
   - How do the cybercriminals earn money with malware
2. **Malware**
   - What is a malware analysis lab?
   - Choosing between virtualization and physical machines
3. **Malware Analysis**
   - Malware analysis (1) Objectives (2) Types: dynamic and static
   - Tools used in malware analysis
   - Obtaining malware samples
   - Obfuscation and antidebugging techniques used by malware
   - Malicious codes and web sites
4. **Network traffic analysis**
   - Capturing and analysing network traffic / Wireshark and T-shark tools
   - IP addresses and DNS domains analysis
   - Anonymity techniques
5. **Malware analysis results**
   - Practical approach for malware analysis and report generation
6. **Incident response**
   - Handling and incident response
   - Business continuity
7. **Practices**