Cybersecurity
Summer
BootCamp

2017

Syllabus
FCSE advanced level

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

PROFESSOR

Daniel Echeverri

Workshop 13

Deep Web

Workshop duration: 20 hours

Description

The main objective is to show the more important techniques and tools to configure and take advantage of the advanced features of main anonymous networks available currently. The students will learn the functional and technical details of Tor, I2P and Freenet and will understand their differences and particular features. Finally, the students will get the needed knowledge to perform analysis and information gathering processes over hidden services in the darknets mentioned before and in some cases, get information about the users that uses that kind of sites.

Syllabus

1. **TOR**
   - Installation and configuration of a Tor instance
   - Basic elements and Tor advanced configuration
   - Configuration of relays and hidden services in Tor
   - Configuration and use of TOR Bridges and Pluggable Transports
   - Configuration and use of OnionCAT
   - Protocol control of TOR
   - Avoiding information leaks: Torifying with TorSocks
   - Customizing onion addresses with Shallot
2. **I2P**
   - Installation and initial configuration of I2P
   - Elements of a router in I2P
   - Services and applications preconfigured
   - Domain resolution system in I2P
   - NetDB operation
   - Deep web and hidden services in I2P
   - Programatic access to I2P instances
3. **Freenet**
   - Freenet arquitecture and Fproxy operation
   - Functioning of keys in Freenet
   - Plugins and services in Freenet
   - Programatic access to Freenet instances
4. **Darknets**
   - Creating scripts for automating tasks against anonymous networks
   - Darknets content search
   - Top search engines in the darknets
   - Development of scripts for the automation of analysis tasks
   - Crawling and stemming processes against darknets
   - Information gathering processes against darknets
   - Creation of hooks to perform tracking processes against users

PROFESSOR

Lorenzo Martínez

Workshop 14

Mobile forensics

Workshop duration: 10 hours

Description

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 large amount of information that can be particularly important in investigation and/or forensics analysis.

The widespread use of mobile devices, on many occasions without a great deal of security measures for access by anyone, 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 forensics 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 situation.

Syllabus

1. **Incident response related to mobile devices**
   - What to do? How? When?
   - Steal? Malware?
   - Laboratory deployment required for activity analysis of mobile devices
2. **IOS**
   - IOS backup
   - Juicy Files
   - Timeline
   - Activity analysis with commercial tools: Oxigen
3. **Android**
   - Android applications
   - Static analysis
   - Dynamic analysis
   - Activity analysis with commercial tools: Oxigen

PROFESSOR

Ricardo Rodriguez

Workshop 15

Malware analysis

Workshop duration: 10 hours

Description

Software with malicious code, or malware, is software which daily disrupts computer operations. As reported by many industries within the cybersecurity sector, the number of threats and their complexity has increased over the last few years. This increase is not surprising given the amount of money that malware can "easily" and quickly generate.

The purpose of this workshop is to bring the State Security Forces closer to the concept of malware so that they know the different types of malware they will have to deal with, as well as the basic and advanced knowledge in malware analysis, together with good practices recommended for managing incidents of cybersecurity related to malicious code.

For this purpose, tools for the analysis of malicious evidence will be taught, both statically and dynamically, together with the guidelines for the creation of analysis environments, result reports and mitigation strategies.

Syllabus

1. **Introduction to malware**
   - Characteristics, types and evolution
   - Attack vectors and distribution channels
2. **Creation of analysis laboratory**
   - Minimum tools and needs
   - Malware analysis methodology
3. **Previous knowledge**
   - Assembly language and x86 architecture (minimum necessary knowledge)
   - Windows Internals: PE structure, binary loading, binaries in memory, APIs
4. **Basic analysis**
   - Static analysis
   - Dynamic analysis
5. **Phases of malware attack**
6. **Advanced analysis**
   - Static analysis
   - Dynamic analysis
7. **Reports on threats: scope and mitigation**
   - Disinfection
   - Rules for detection (YARA, SNORT, IOC)