CERTs Level 1

Organizers:

GOBIERNO DE ESPAÑA · MINISTERIO DE ECONOMÍA Y EMPRESA · incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · OEA OAS

Collaborators:

GOBIERNO DE ESPAÑA · MINISTERIO DE ASUNTOS EXTERIORES, UNIÓN EUROPEA Y COOPERACIÓN · universidad de león · AYUNTAMIENTO DE LEÓN · León · LEÓN · Santander · IDB Inter-American Development Bank · Canada · aws · EUROPOL EC3 European Cybercrime Centre · INTERPOL

PROFESSOR

Paco Montserrat

Workshop 1

Creation of a CERT

Workshop duration: 5 hours

Description

The main mission of a CERT is to provide a support service in security incident handling. The compromises and violation of the TIC security of an organization is a reality. When the incidents occur, the CERTs should be prepared to deal with them appropriately on a technical and organizational level.

Syllabus

1. What is a CERT?
- CERTS types
- Services that can be offered by a CERT
- Event vs incident
- The importance of reactive services in the CERT

2. CERT original planning
- Objectives
- Expectations
- Service hours / 24*7

3. Incidents handling
- Processes and procedures
- Preparing / Training
- Coordination / communication plan
- Crisis management
    - Mitigation
    - Custody chain
    - Lessons learned
- Tools

4. Metrics

5. Community
- Communication to/ relation with other CERTs
- FIRST / Terena Geant
- Incibe
- Standars
- PGP/GPG key Signing Ceremony

PROFESSOR

Luis Jurado

Workshop 2

Legal and cooperation aspects

Workshop duration: 5 hours

Description

This course is aimed at providing a comprehensive training on international judicial cooperation in criminal matters.

The syllabus is designed to have a practical approach for attendants. Given the wide variety of legal situations and channels at an international level regarding the application of cooperation measures in criminal matters, we will try to adapt them -to the extent practicable- to the countries of origin of attendants.

Syllabus

1. Extradition
2. European Arrest Warrant
3. Mutual recognition of criminal resolutions in the European Union
4. Persons and institutions of judicial cooperation
5. Judicial assistance within the framework of the criminal investigation
6. Specific cooperation resources
7. Information exchange of criminal records and taking into account of a previous conviction handed down in another State by virtue of the principle of mutual recognition
8. Transfer of proceedings and assignment of jurisdiction
9. Precautionary measures
10. Enforcement of court decisions. Seizure
11. Enforcement of court decisions. Custodial sentences
12. International judicial cooperation outside the EU
13. International judicial cooperation in Ibero-America
14. Universal jurisdiction and cooperation with the International Criminal Court
15. Police cooperation
16. Probative value of foreign proceedings

PROFESSOR

David Gallardo

Workshop 3

Operations

Workshop duration: 10 hours

Description

Information security incidents are inevitable. Sooner or later any organization will suffer one. This is why, if we want to minimise its consequences in a business, we must be prepared and count on suitable instruments that allows to identify, evaluate and manage the answer in an efficient and planned way.

An appropiate management of the incidents must be always present because it will allow to reduce its impact in the business both in the short and in the long term. In the long term the advantages, among others, include improved resilience and assurance of business continuity, increased reputation and customer/stakeholder confidence as well as a better protection against economical loss and a risk reduction.

This workshop combines theory and practical exercises in order to analyse the main components of the incident management and how they interact between them and between others.

Syllabus

1. **Incidents handling**
   - Concepts
   - Objectives
   - Incident handling vs incident response
   - Methodologies
   - Tools
   - Life of an incident
2. **Critical incidents**
   - Severity
   - Levels
3. **Alerts, warnings and announcements**
   - Reactive services: Alerts and warnings
   - Proactive services: Announcements
   - Others
   - Related processes
4. **Information sources**
   - Security warnings
   - Other tools: logs, events, records...
5. **Role-play**
   - Usefulness
   - Decision making

PROFESSOR

José Miguel Esparza

Workshop 4

Threat analysis

Workshop duration: 10 hours

Description

Nowadays, the number of threats and cyberattacks reported by the different CERTs worldwide is overwhelming. However, there is no expectation that these amounts will go forward, but rather the opposite, since they are expected to continue to increase over the years. With this cyber 'war' scenario in mind it is crucial that incident response teams are minimally familiar with the different kinds of threats and how to analyse them.

In this training we will delve into the types of threats that we can find, how to identify them and how to prepare a suitable environment for their analysis. The major focus will be given to dynamic malware analysis, leaving aside static analysis for advanced courses.

Syllabus

1. **Introduction to types of threats and infection vectors**
2. **Differences between static and dynamic analysis**
3. **Preparation of the working environment**
    - Needed tools
    - Anti-analysis and virtual machine hiding
    - Isolation
4. **Introduction to malware analysis**
    - Identification of an infected machine
    - Indicators Of Compromise gathering (IOCs)
    - Malware classification
    - Malware identification in memory
    - Network traffic analysis

PROFESSOR

Víctor Manuel Calzado Mayo

Workshop 5

Forensics analysis introduction

Workshop duration: 10 hours

Description

Once the training is completed, the student will be able to perform a forensic analysis in live mode, know if a computer has been compromised and perform a subsequent analysis in offline mode.

Likewise, the student will learn notions about reverse engineering, analysis of executables and suspicious files.

Overall, the training addresses the entire line of response to an incident from a forensic point of view, recovering and analyzing information from various sources, such as RAM, file systems, process integrity and log analysis.

Syllabus

1. **Intro. Guidelines for forensic analysis**
2. **Linux**
   - Boot Analysis
   - Log Analysis
   - File System Analysis
   - RAM Analysis
3. **Windows**
   - Boot Analysis
   - Log Analysis
   - File System and Registry Analysis
   - RAM Analysis
4. **Timeline Analysis**
   - Linux
   - Windows
5. **Malware Forensics**
   - Office Files
   - Executable File Analysis: ELF Files
   - Executable File Analysis: PE Files
6. **Network forensics**