CERTs Level 2

Organizers:

Collaborators:

PROFESSOR

Jorge Capmany

Workshop 6: Cybersecurity Intelligence

Introduction

Threats on the internet have evolved in such a way that now there are hardly any attacks from what today might be called a classic point of view; that is, directly attacking the infrastructure exposed to the internet.

Current threats use services, products and infrastructure layers able to avoid the traditional security checks, such as signature-based products or classic heuristics.

The current focus of information security must evolve towards a more aggressive and dynamic model based on profound knowledge of this type of threat in order to protect our infrastructure and information.

Objectives

The workshops delivered by Manu Quintans and Jorge Capmany are not meant to be an academic manual on threats and the fundamentals of security. They are not aimed at sticking to a rigid structure, but at evolving from a basic perspective towards a deeper knowledge of threats and presenting different techniques that allow participants to be one step ahead of threats on the internet.

These workshops offer the participants access to a new mindset when processing intelligence and facing emerging threats.

This analytical view provides the analysts and responders with the ability to detect and protect themselves from new threats on the internet, while they are still evolving.

The final purpose of these workshops is to offer proactive and practical methodologies which give visibility on the new evasive and sophisticated threats.

Contents

During the workshops the work will be focused on a single methodology but with different work environments.

The following points may vary based on the dynamics of the work group.

All participants will work at the same place and shall not advance through topics until the group has fully complied with the objectives of each of the points.

PROFESSOR

Jorge Capmany

Workshop 6.1 - Threat Intelligence

Workshop duration: 10 hours

Syllabus

- Know Your Enemy
- Threat Theory
- Types of Threats
- Threat Evolution
- Current State of Threats
- Threat Modelling
- Threat Life Cycle
- Malware Research
- Intelligence Research
- Fraud Prevention, IR, APTs

PROFESSOR

Jorge Capmany

Workshop 6.2 - Intelligence research

Workshop duration: 10 hours

Syllabus

- Introduction to the Underground World
- Open Source Intelligence
- Intelligence Crawling
- Malware Crawling
- Monitoring of Stakeholders
- Analysis with Graphs
- Campaign Monitoring
- Botnet Monitoring
- IOC Extraction
- From the Newspaper to VirusTotal

PROFESSOR

Jorge Capmany

Workshop 6.3 - Intel & DFIR

Workshop duration: 10 hours

Syllabus

- Intel Focused DFIR
- Kill Chain Model
- Diamond Model
- Malware Characterisation
- Consuming Intel for Detection and Response
  - Log washing
  - Event contextualisation
  - Hunting
- Generating Your Own Intel
- Structuring Adversaries' Knowledge

PROFESSOR

Jorge Capmany

Workshop 6.4 - CounterOPs

Workshop duration: 10 hours

Syllabus

- Basic Concepts
- Methodology
- Offensive Tracking
- Attacking Threat Infrastructures
- Workshops and Final Assessment