CERT Games

Who Should Attend?

The workshop is intended for IT systems administrators and IT security incident responders.

Course Content

The aim of the exercise is to develop proper habits and practice in handling incidents defending against attacks targeting IT infrastructure. Participants will be given an existing infrastructure containing a web server, mail server, file server, DNS server, etc., which they must defend using various defense techniques. They will be required to properly protect infrastructure, detect attacks, and make rapid decisions related to the current threat. The participants' group-work and problem-solving abilities will also be evaluated. The teams will be evaluated throughout the exercise in order to assess the effectiveness of each action. The exercise ends with presentation of team results and additional discussion.

This exercise consists of group of challenges. In each challenge participants have to solve a problem, analyse code/data or find information. After completing each challenge, participants answer control questions or find hidden flags. Various tasks require different sets of skills to complete – network analysis skills, information gathering, data/log analysis, and/or reverse engineering. Not all challenges will be available from the start. The challenges focus on attacks on a telecom operator, a bank or financial institution (the company) and its clients. The exercise aims to test cybersecurity teams: how they are capable of dealing with real-life attacks and scenarios. To complete some of the challenges, malware analysis labs are necessary (one challenge involves analysis of a real malware sample). There will be six challenges, but information about them should NOT be disclosed to the participants -- it is available on request for organisers.

Course Objectives

Detecting, understanding, and reacting to live vulnerability exploitation on a dedicated infrastructure.

Prerequisites and Requirements

- Basic knowledge of Linux systems administration.
- Knowledge of network protocols.
- Ability to analyse network traffic
- Basic knowledge of IT security
- Ability to analyse logs of popular services
- Basic understanding of Unix file system structure
- Each participant must bring a laptop with an ethernet card or WiFi to have Open VPN, ssh client, and a web browser installed.

All participants must have access to the Internet. For a group of up to 50 participants, a bandwidth of 20 Mbps is recommended. Participants in the exercises are requested to prepare a computer environment in which they will be able to analyse malware designed for Windows OS (preferably in an isolated, secure environment, e.g. virtual machines). There must be at least one environment for each exercise group. We also recommend participants have Linux OS for other types of analysis. We recommend using the following ENISA exercise to prepare the environment: https://www.enisa.europa.eu/activities/cert/training/training-resources/technical-operational#building

Training structure

4-day session: 2-day CERT Games training and 2-day CERT exercises.

Methodology

Instructor-led workshop. In a learning set-up designed by experts in the field, you will work in teams and practice different security skills.