Grant Agreement Number: *833673*

Project acronym: **FORESIGHT**

Project full title: Advanced cyber-security simulation platform for preparedness training in Aviation, Power-grid and Naval environments

Syllabus

Online Training "Hacking Firmware"

Advanced LEVEL

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 833673. The content of this document reflects only the authors' view and the European Commission is not responsible for any use that may be made of the information it contains.

COURSE: Hacking Firmware

DELIVERY DATE: 1 session, FEBRUARY 3rd 2022, 13:30 – 17:30 (CET)

COURSE DESCRIPTION: Attacks against the hardware and firmware of a device stand as some of the highest impact threats facing modern organizations. Firmware retains the highest privileges, allowing attackers to bypass traditional controls, and grants a higher level of persistence. The firmware layer has also quickly become one of the most active areas of cybersecurity with attackers increasingly setting their sights on the area of the enterprise where vulnerabilities are plentiful, and defenses are often weakest. This not only affect high end network devices but everyday IoT devices that we use in our lives.

Firmware and hardware attacks are also significantly different from traditional malware and network threats. Security teams must be prepared to defend against a new set of attacker strategies, vectors, and understand how the wide variety of firmware components can be used as part of a persistent attack.

The objective is to develop theoretical knowledge about firmware structure, components, and attack vectors, complemented by hands-on exercises to investigate and experiment with firmware images.

INTENDED AUDIENCE

This training’s intended audience is IT, cyber security, and OT personnel with good knowledge of IT and networks fundamentals.

DELIVERY MODALITY: E-LEARNING CLASS: Webinar + Hands-on

DURATION: 4 hours

SESSIONS: 1

PREREQUISITE: Proficiency with IT systems and Linux administration.

The maximum number of trainees per session is 12

CONTENTS

1. What is a firmware and firmware use in embedded devices?
2. Firmware structures and file systems
3. Deconstruction and reconstruction of a firmware for embedded devices
4. Tools of trade
5. Backdooring firmware with and without using FMK (hands on)
6. Firmware exploits and vulnerabilities
7. Firmware integrity checks and backdoor detection

TRAINING STRUCTURE

The training will be delivered online through Zoom Webinar and CybExer Range Platform. The attendees will receive individual credentials and links to join the training.

LEARNING OUTCOMES

Participants will have a basic knowledge about firmware internals and tools and methods for working with firmware images.