Grant Agreement Number: ***833389***

Project acronym: Cyber-MAR

Project full title: Cyber preparedness actions for a holistic approach and awareness raising in the MARitime logistics supply chain

Syllabus

Online Training A003 "Unlock the capacities of a Cyber Range for Network and Computer Forensics"

ADVANCED LEVEL

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 833389. 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: A003 - Introduction to computer and network forensics

DELIVERY DATE: 2 sessions, FEBRUARY 3rd AM + FEBRUARY 4th 2022 AM

COURSE DESCRIPTION: The training course is designed to provide learners with an understanding of the interest of using a cyber range for forensics use, use the dedicated CR features, create a topology for computer and forensics use, use the topology to conduct a forensics operation on a Cyber-MAR Scenario.

This training's intended audience is IT or cyber security interested people, with a good first knowledge or experience of the IT and networks fundamentals.

The objective is to increase knowledge of the cyber forensics discipline

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

DURATION: 3 hours

SESSIONS: 1 on Thursday morning, 1 on Friday morning

PREREQUISITE: Good knowledge of TCP/IP networking protocol, routing, switching fundamentals, proficiency with IT systems and networks administration.

Only trainees that have successfully passed an online pre-enrollment quiz will be admitted to the training. Further details on this quiz will be given to prospective students.

The maximum number of trainees per session is 10

CONTENTS

1. Cyber-MAR H2020 project overview
2. Cyber range capacities for forensics use
    a. accessing the CR

   b. network traffic capture

3. Forensics operations on a Cyber-MAR scenario
   a. tools for forensics in the cyber range
   b. conducting the forensics operation

✓ Initial and Final quiz for training efficacy evaluation

TRAINING STRUCTURE

The training will be delivered online through Zoom Webinar, Cyber-MAR Learning Management System and the Cyber-MAR Cyber Range via Cyber-MAR Labs.

The attendees will receive individual credentials and links to join the training.

LEARNING OUTCOMES

The participants will develop knowledge and skills necessary to apply the principles of:

- Application of techniques for detecting host and network-based intrusions using intrusion detection technologies
- Knowledge of incident response and handling methodologies
- Knowledge of packet-level analysis
- Collect intrusion artifacts (e.g., source code, malware, Trojans) and use discovered data to enable mitigation of potential cyber defense incidents within the enterprise
- Preserve evidence integrity according to standard operating procedures or national standards
- Recognize and categorize types of vulnerabilities and associated attacks
- What constitutes a network attack and a network attack's relationship to both threats and vulnerabilities
- An organization's threat environment