

A preliminary task for the technically oriented attendees of Flagship 1

Template version: 2020-12-01, authored by:



|  |  |  |  |
| --- | --- | --- | --- |
| Author | Name | | |
| E-mail | E-mail | | |
| Organisation | Organisation name | Date | dd.mm.yyyy |

Table of Contents

[1 Course presentation 3](#_Toc57705748)

[2 Background 3](#_Toc57705749)

[3 Cyber Attack 4](#_Toc57705750)

[4 Digital Forensics 4](#_Toc57705751)

[5 Auditing 5](#_Toc57705752)

[6 Cybersecurity Exercise 5](#_Toc57705753)

[7 References 5](#_Toc57705754)

[8 Feedback 5](#_Toc57705755)

# Course presentation

Welcome to the preliminary course of Flagship 1, an online-only cybersecurity exercise organised by CyberSec4Europe. The exercise is available to CyberSec4Europe partners. Even if your organisation is not a partner in the project (<https://cybersec4europe.eu/partners/>), you can do this course for your own development.

The target audience for this course are the technically-oriented attendees of Flagship 1. The objective of this course is that you learn basic knowledge and skills on digital incident forensics. By taking the course, you will acquire deeper information about the technical environment of Flagship 1. The acquired information will support you in performing the exercise. We hope that it also advances your personal development.

The course materials are available at <https://cs4e.pages.labranet.jamk.fi/ooc/>**.**

**Main guidelines**

This template contains a set of questions, which are voluntary to answer. If you are participating in Flagship 1, it’s an advantage for you to answer them. Write your answer to all locations that have a yellow background, as shown below:

<Write your answer here>

You may be as verbose or sententious as you see appropriate. Because this is a voluntary course, we do not want to make this a burden for you. Instead, we welcome the effort you make.

There are also some optional questions, which you may answer if you find it suitable.

Please use this template and its current styles. Return your final document by email to cs4e-flagship@jamk.fi. If you have any questions, please send your email to the mentioned email address. The conductor team is available for you.

Before returning your results, please:

* update your contact information on the cover page
* update the table of contents

You may return your results in .pdf or .docx format.

The exercise and this course are conducted and prepared by JAMK University of Applied Sciences, Finland.

# Background

**What are your goals for this course?**

* <Write your answer here>

**What thoughts did the video “Setting the scene for Flagship 1” create in your mind?**

* <Write your answer here>

# Cyber Attack

**How many threats have you seen at your work (ENISAThreat Landscape, Top 15 Threats)?**

* <Write your answer here>

**Can you give some real-life examples of unintentional or intentional threats?**

* <Write your answer here>

**What were the main challenges on building a test environment?**

* <Write your answer here>

# Digital Forensics

**How can you identify:**

**A message as a phishing email?**

* <Write your answer here>

**Where the phishing site mentioned in the email is located?**

* <Write your answer here>

**Where the user credentials from the phishing site end up?**

* <Write your answer here>

**How many users have visited the phishing site?**

* <Write your answer here>

**How the attacker has carried out his criminal actions?**

* <Write your answer here>

**What has enabled the attacker's criminal actions?**

* <Write your answer here>

**OPTIONAL:** Describe your investigation working path (how did you do it)?

* <Write your answer here>

**OPTIONAL:** Describe the attacker’s modus operandi (Attack path)

* <Write your answer here>

# Auditing

At this point we assume that you have familiarised yourself with a specific part of Kybereo’s environment, that are available from the course materials.

**What are the main threats in this environment?**

* <Write your answer here>

**How many critical vulnerabilities did you find by using CPE (Apache, WordPress, SQL)?**

* <Write your answer here>

# Cybersecurity Exercise

In the registation form we enquired your experience on cybersecurity exercises. Since then, has your knowledge or experience changed some how?

* <Write your answer here>

# References

If you have some references, that you would to share with us, please do so :)

* <Write your answer here>

# Feedback

In the context of this course, please answer the following four questions.

**What is working well?**

* <Write your answer here>

**What could be better?**

* <Write your answer here>

**How should this be developed?**

* <Write your answer here>

**In your own words please let us have your feedback**

* <Write your answer here>