

# LABS II: ENCODING INFORMATION AND SHARING IT (E.303)

INVESTIGATE A COMPROMISED LINUX HOST

CIRCL COMPUTER INCIDENT RESPONSE CENTER LUXEMBOURG

MISP PROJECT

<https://www.misp-project.org/>

MARCH 21, 2022



2022-03-21

Labs II: Encoding information and sharing it (e.303)

LABS II: ENCODING INFORMATION AND SHARING IT (E.303)

INVESTIGATE A COMPROMISED LINUX HOST

CIRCL COMPUTER INCIDENT RESPONSE CENTER LUXEMBOURG

MISP PROJECT  
<https://www.misp-project.org/>

MARCH 21, 2022



- A compromised Linux host needs to be analysed and the only evidence is a single **network packet capture file**<sup>1</sup>.
- No more information or context were given.
- Investigation and **interpreting results must be shared** with colleagues and other CSIRTs.

<sup>1</sup><https://github.com/MISP/misp-training-lea/raw/main/e.303-lab2-encoding-information-and-sharing-it/for-student/capture-e.303.cap>

## └ Lab e.303

1. The trainer might explain the challenges concerning lack of evidences and context, the partial information often received by LEA or a CSIRT from victims. The goal is to share information as early as possible to discover if other participants are already working on the case.

- A compromised Linux host needs to be analysed and the only evidence is a single **network packet capture file**.
- No more information or context were given.
- Investigation and **interpreting results must be shared** with colleagues and other CSIRTs.

<sup>1</sup><https://github.com/MISP/misp-training-lea/raw/main/e.303-lab2-encoding-information-and-sharing-it/for-student/capture-e.303.cap>

- What could **be deduced from these evidences** by using mainly the **MISP instance** and misp module expansion?
- How can you describe your investigation in a structured way and as a textual report in MISP?
- Can you attach **level of confidence** in your analytical judgment and probability of likelihood?
- Can we would describe **preventive measure(s)** for such case?

2022-03-21

## Labs II: Encoding information and sharing it (e.303)

### └ Open general questions and leads

1. The goal is to focus on the maximum of evidences which can be extracted from a single network packet capture. Some assumption can be extracted and will need to be explained and classify with a specific level of confidence. The taxonomy in MISP might be used such as admiralty-scale, or estimative-language. LEA or CSIRTs can share preventive measures from known case. What would be the preventive measures from this evidence?

- What could **be deduced from these evidences** by using mainly the **MISP instance** and misp module expansion?
- How can you describe your investigation in a structured way and as a textual report in MISP?
- Can you attach **level of confidence** in your analytical judgment and probability of likelihood?
- Can we would describe **preventive measure(s)** for such case?