

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 23, 2022



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

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

OPEN GENERAL QUESTIONS AND LEADS

- 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?

- Extract evidences from the small network capture using techniques seen previously for network capture (hints: tcpflow, tshark, misp-wireshark)
- Add the first evidences extracted such as files, network indicators into MISP

SECOND STEP OF THE LAB

- Gather meta-data from files using hashlookup² and associated MISP module
- **Evaluate the information and describe the potential use** following the evidences collected
- Assign an **analytical judgment** to your analysis
- Define the **sharing and distribution level** of the analysis with partners including CSIRTs and other LEAs via MISP

²<https://www.circl.lu/services/hashlookup/>