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

Investigate a compromised Linux host

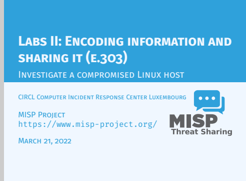
CIRCL Computer Incident Response Center Luxembourg

MISP Project
https://www.misp-project.org/

March 21, 2022

2022-03-21

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

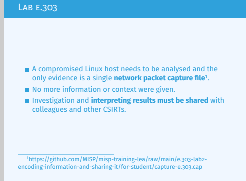


Labs II: Encoding information and sharing it (e.303)
Investigate a compromised Linux host
CIRCL Computer Incident Response Center Luxembourg
MISP Project
https://www.misp-project.org/
March 21, 2022

Lab e.303

- 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



Lab e.303

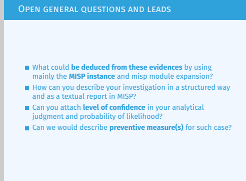
- A compromised Linux host needs to be analysed and the only evidence is a single **network packet capture file**[1].
- No more information or context were given.
- Investigation and **interpreting results must be shared** with colleagues and other CSIRTs.

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

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 othr participants are already working on the case.

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?



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?

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?