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 22, 2022

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 22, 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?

First step of the lab

- 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

First step of the lab
- 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

1. The goal is not to deep dive in all strategies for reassembling TCP, flows even if it's an interesting topic for digital network forensic. The objective is to grasp the different data models in MISP and how such evidence can be represented.

Second step of the lab

- Gather meta-data from files using hashlookup[2] 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/

Second step of the lab
Gather meta-data from files using hashlookup[2] 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/

1. Using known libraries of file such as hashlookup, saves a lot of times during analysis. How this information can help to support logical analysis and inference.