OT Lab 4 (Malware Analysis)

In this lab, you will learn malware analysis approaches such as static and dynamic.

Task 1: Set up your environment.

1. Use any virtualization environment, better to use the latest version.
2. Prepare and secure malware analysis environment, e.g. FlareVM or Remnux, etc. Make sure that VM uses a **HOST ONLY** network adapter.
3. Or you can create a Virtual Machine and set it up as a malware analysis environment.

Task 2 - Let's get some malware

1. Download some malware/ransomware from the Internet (for example, TheZoo repo).
2. Please be careful when you run them, THESE ARE REAL MALWARE.
3. Select at least two malware that you want to analyze in your malware analysis environment.

Task 3 - Static Analysis

1. Use any tool for static analysis of your selected malware (for example, Ghidra, IDA, Binary Ninja, Hopper, Radare2, ...).
2. Now try to use other online tools (for example, any.run, hybrid analysis, ...), upload the malware and see what artifact it gathers.
3. Compare the findings of both methods, and see if there are some artifacts that online solution did not manage to find, or vice versa. For example, a piece of code or information that helps you in your analysis.
4. Try to describe which method is better (Sandboxing vs Static analysis) is better, and which one is more useful in which case.

Task 4 - Mapping to ATT&CK mitre framework (Optional)

Map the malware that you have selected to the ATT&CK MATRIX, use this link.

Task 5 - Dynamic Analysis (Bonus)

1. You will be creating your own Dynamic Malware analysis Environment (i.e Cuckoo).
2. Try to use some debugger to analyze the malware WHILE IT IS RUNNING, be careful where you will run this malware.
3. Try some debugger that will allow you to debug the whole operating system (for example, PyReBox).
4. What kind of benefit does this method have?