Perform Malware Disassembly using IDA

ILABS
CEH PRACTICAL

Static analysis also includes the dismantling of a given executable into binary format to study its functionalities and features. This process helps identify the language used for programming the malware, look for APIs that reveal its function, and retrieve other information. Based on the reconstructed assembly code, you can inspect the program logic and recognize its threat potential. This process uses debugging tools

Aim

IDA As a disassembler, IDA explores binary programs, for which the source code might not be available, to create maps of their execution. The primary purpose of a disassembler is to display the instructions executed by the processor in a symbolic representation called “assembly language.”

Here, we will use IDA to analyse a malicious file

DEMO

THANKS