

Perform Malware Disassembly using OllyDbg

ILABS
CEH PRACTICAL



OllyDbg is a debugger that emphasizes binary code analysis, which is useful when source code is unavailable. It traces registers, recognizes procedures, API calls switches, tables, constants, and strings, and locates routines from object files and libraries.



Aim

Here, we will use OllyDbg to analyse a malicious file

DEMO

4

<https://t.me/learningnets>



THANKS