Analyze ELF Executable File using Detect It Easy (DIE)

ILABS
CEH PRACTICAL

The Executable and Linkable Format (ELF) is a generic executable file format in Linux environment. It contains three main components including ELF header, sections, and segments. Each component plays an independent role in the loading and execution of ELF executables. The static analysis of an ELF file involves investigating an ELF executable file without running or installing it. It also involves accessing the binary code and extracting valuable artifacts from the program

Aim

Detect It Easy (DIE) is an application used for determining the types of files. Apart from the Windows, DIE is also available for Linux and Mac OS. It has a completely open architecture of signatures and can easily add its own algorithms for detecting or modifying the existing signatures. It detects a file's compiler, linker, packer, etc. using a signature-based detection method.

In this task, we will be using Detect It Easy (DIE) tool to analyze ELF file.

Other tools to identify packing/obfuscation methods

- ✓ Macro_Pack (https://github.com)
- ✓ UPX (https://upx.github.io)
- ✓ ASPack (http://www.aspack.com)

DEMO

THANKS