4LINUX
FREE SOFTWARE SOLUTIONS

The EDB Project

H2HC 2010

Brazil

$ whoami

4LINUX
FREE SOFTWARE SOLUTIONS

Free Software Consultant at 4Linux, LPI and A+ certified, Bachelor in Computer Science, security envolved since 2001, when I had my Windows 98 hacked by NetBus. :)

Working with RE since 2002, when I've tried to run Elifoot 98 trial for unlimited time. =P

$ whatis edb-debugger

4LINUX
FREE SOFTWARE SOLUTIONS

Evan's Debugger is a multi-arch and extensible disassembler and debugger for ELF binaries, based on famous PE32 debugger OllyDbg.

The goal is make a powerful debugger for ELF, like OllyDbg is for PE32.

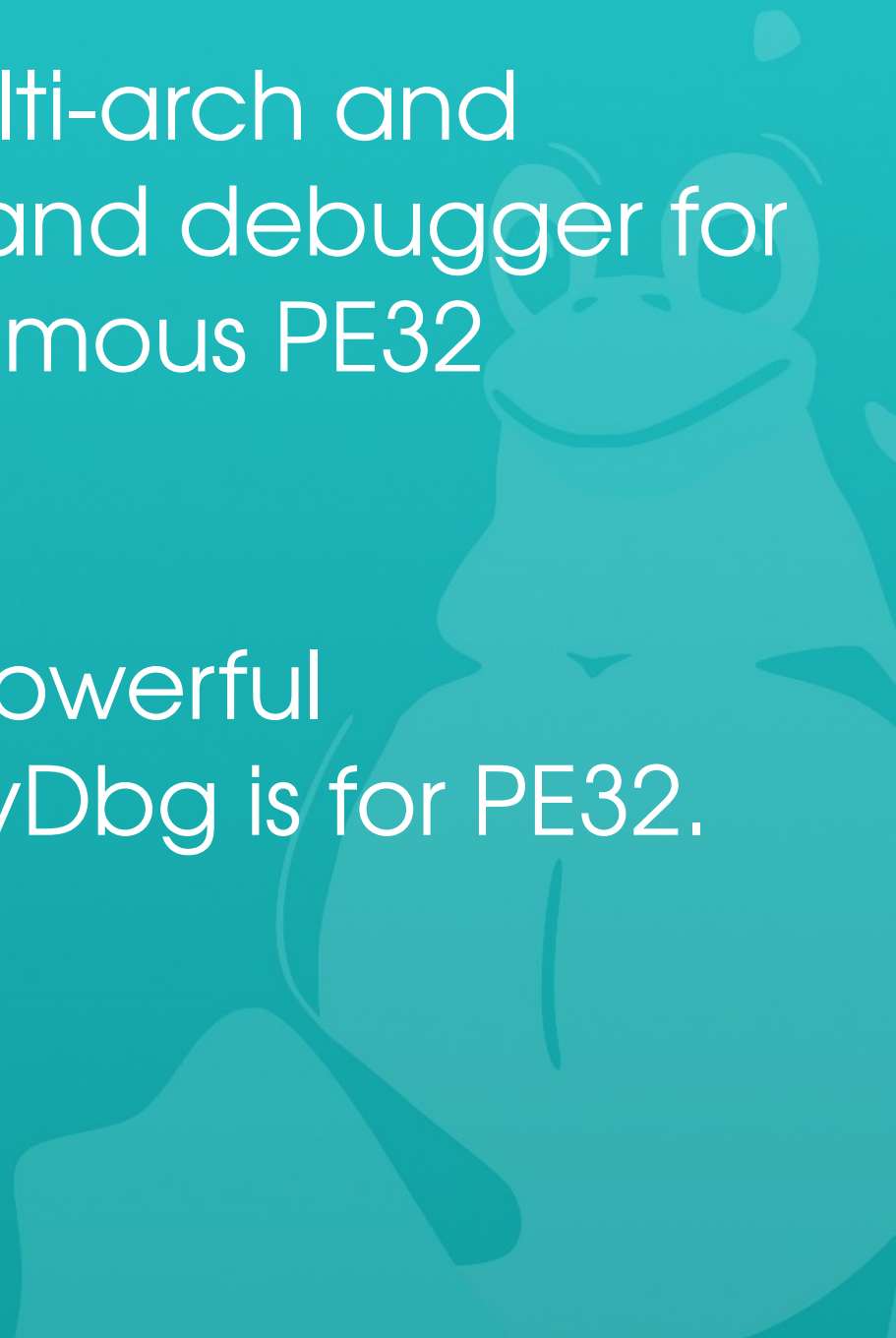
EDB is a FOSS (Free and Open Source Software) licensed by GPL.

$ whatis edb-debugger

4LINUX
FREE SOFTWARE SOLUTIONS

Evan's Debugger is a multi-arch and extensible disassembler and debugger for ELF binaries, based on famous PE32 debugger OllyDbg.

The intent is to make a powerful debugger for ELF like OllyDbg is for PE32.



$ Why not gdb?

4LINUX
FREE SOFTWARE SOLUTIONS

- gdb expects a source code to debug.

- It's hard to debugging a binary compiled without debug symbols.

- gdb does not have a fully-featured and easy-to-use GUI interface.

- Otherwise, gdb is a great tool and can be found in many systems.

EDB architecture

4LINUX
FREE SOFTWARE SOLUTIONS

EDB runs on normal user mode. No root account needed. You can open a binary with EDB or attach to a running process.

Main features

4LINUX
FREE SOFTWARE SOLUTIONS

- Hardware and conditional breakpoints.
- Function finder.
- String searcher.
- *New* ROPTool (for Return-Oriented Programming).
- Symbols generating with *edb --symbol* option.

Example

4LINUX
FREE SOFTWARE SOLUTIONS

"Talk is cheap, show me the code!"

Linus Torvalds

Get the tool of trade

4LINUX
FREE SOFTWARE SOLUTIONS

Latest version is **0.9.16**.

Yet unreleased DEB package:
http://linuxreversing.org/down

Source code (project page):
http://codef00.com

We need hackers!

4LINUX
FREE SOFTWARE SOLUTIONS

Please, consider join this project. We need a lot of work until 1.0 release of EDB. Talk with us!

Evan Teran - eteran@alum.rit.edu
Fernando Mercês – fernandomerces@mentebinaria.com.br

Questions

4LINUX
FREE SOFTWARE SOLUTIONS

?

Thank you!

4LINUX
FREE SOFTWARE SOLUTIONS