Reverse Engineering with IDA PRO Training

Duration: **5 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

The need for reverse engineering binary software components arises in more and more contexts every day. Common cases include analysis of malicious software such as viruses, worms, trojans and rootkits, analysing binary drivers in order to develop open-source drivers for alternate platforms, analysing closed source software for security flaws, and source code recovery in legacy systems.

The first step in such an analysis is generally the acquisition of a high-quality disassembly of the binary component. Ida Pro is touted as the premier disassembler available today. Ida Pro is capable of disassembling machine languages for a large number of microprocessors and microcontrollers and is particularly strong when used on Windows and Linux x86 binaries. This course will cover essential background material for effective reverse engineering before diving into the features of Ida Pro that set it apart from other disassemblers.

Course Structure:

The course consists of 40 hours of instruction over five days combining lectures with increasingly difficult hands-on exercises designed to familiarize the student with the capabilities of Ida Pro and its uses in analysing various types of binary files. Students are provided with printed course notes as well as digital versions of the course notes and additional course related files.

Prerequisites

Remember that this course is practical and of an extremely technical nature, so a basic understanding of assembly language (preferably x86), C/C++ programming, networking, and security is a course prerequisite.

Who Should Attend? Information security officers, anti-virus vendors, vulnerability researchers, security consultants, software developers and other nice people will all benefit from the techniques presented in this class.

What to bring: Students will be provided access to a desktop computer running Windows 10 with all necessary software to complete the training already installed.

Reverse Engineering with IDA PRO Training

Duration: **5 Day**

BİLGİNÇ
IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

The course will provide an overview of disassembler theory followed by a review of the structure of compiler generated code. Armed with that background information, you will be introduced to the features of Ida Pro that set it apart from other disassemblers and learn how it can assist you in determining the behaviour of various binary files. The course will cover the basics of the Ida Pro interface including the many informational displays it contains before moving on to function calling conventions, stack frame analysis, and how to recognize and understand complex data structures including C++ classes.

The course then moves on to cover IDA's FLAIR signature generation utilities and how to use them effectively, creation of custom type libraries, using IDA to patch binaries, and batch mode usage. IDA's programming API's including the IDC and Python scripting API's as well as the native C++ API are then covered. Next, we will discuss the creation and use of plugins, custom loader modules, and custom processor modules using real world plugins to perform a variety of advance reverse engineering tasks. Finally, the course will wrap up with a dive into using IDA's debugger both locally and remotely for simple debugging tasks as well as more advanced uses such as de-obfuscating malware.