Reverse Engineering with Ghidra Training

Duration: **5 Day**

BILGINÇ 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. Ghidra was developed at the US National Security Agency to meet or exceed the capabilities provided by modern commercial disassemblers. Ghidra is free to download, install, and use and is capable of disassembling and decompiling machine languages for a large number of microprocessors and microcontrollers. This course will cover essential background material for effective reverse engineering before diving into the features you will find most useful when using Ghidra for your reverse engineering tasks.

Course Structure: The course consists of 40 hours of instruction over five days, combining lectures with targeted hands-on exercises designed to familiarize the student with the capabilities of Ghidra and its uses in analysing various types of binary files. Students are provided with digital copies of all materials used throughout the course.

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, and software 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 Ghidra Training

Duration: **5 Day**

BILGINÇ 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 Ghidra's features and learn how it can assist you in determining the behaviour of various binary files. The course will cover the basics of the Ghidra 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. Coverage of Ghidra's decompiler will be woven throughout the course. Next, the use of Ghidra in a collaborative reverse engineering environment will be discussed.

The course then moves on to cover Ghidra function identification databases and how to use them effectively, creation of custom data type archives, and using Ghidra to patch binaries. Ghidra's programming API's including the Java and Python scripting API's are then covered along with using Ghidra in headless mode. After discussing how to integrate Ghidra module development into the Eclipse platform, we will discuss the creation and use of plugins, loader modules, and processor modules. Finally, the course will wrap up with a dive into using Ghidra's debugger for simple debugging tasks as well as more advanced uses such as de-obfuscating malware.