Linux/C++ Reverse Engineering

Course Summary

Description

This course enables the skilled malware analyst to branch into the less mainstream (but equally important) areas of reversing C++ binaries and Linux binaries. After a review of assembly, including a deeper dive into the differences between x86 and x64 architectures, students will learn about C++ calling conventions, classes, objects, and exception handling and how these affect reverse engineering. The course then turns to the Linux operating system, covering topics such as kernel structure and the Linux Application Binary Interface (ABI) in preparation for statically analyzing and debugging Linux executables and malware.

Topics

- Understand the implications of features from high- level languages at the assembly level.
- Recognize and analyze the structure of C++ binaries.
- Describe the Linux System V ABI, including how processes and threads are executed in Linux.
- Understand the structure of the Linux Executable and Linkable Format (ELF).
- Statically analyze Linux binaries using IDA and other tools.
- Debug Linux binaries using GDB and the IDA Remote Debugger.

Audience

This course is designed for malware analysts.

Prerequisites

Successful completion of Malware Reverse Engineering course and reverse engineering experience in a Windows environment, and strong understanding of operating system internals.

Duration

Five days
30 CPE/CEU credits

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically