ProTech *"Charting the Course ...*

protechtraining.com

... to Your Success!"

Advanced Malware Analysis

Course Summary

Description

This final course takes students into advanced and specialist topics surrounding rootkit analysis. Students will learn about the Windows kernel, automated and manual unpacking, live kernel debugging with IDA and WinDbg, and reverse engineering drivers. This is a heavily lab-intensive course that requires students to have a solid background in reverse engineering and malware analysis prior to attending. In addition, one of two optional modules can be included in this course: Document-Embedded Malware or IDA Scripting with IDAPython. Either one can be added to the week-long course while still dedicating sufficient time to cover rootkit analysis, though in less detail.

Topics

- Bypassing Anti-Debugging Techniques
- Extracting embedded Shell Scripts
- Manually Unpacking Obfuscated Malware
- IDAPro Plugins
- Analyzing and Defeating Armored Malware
- Advanced Rootkits

Audience

This course is designed for Malware Analysts, Software Engineers, and Forensic Investigators.

Prerequisites

This is an advanced level, fast-paced course. In addition to previous reverse engineering practice, students should also have strong assembly language knowledge as well as Python scripting skill.

We recommend *Assembly For Reverse Engineers*, *Python for Network Defenders* and *Malware Reverse Engineering* classes in preparation for this course.

Duration

Five days