ProTech protechtraining.com *"Charting the Course ... ... to Your Success!"*

Assembly for Reverse Engineers

Course Summary

Description

Assembly for Reverse Engineers was designed for those entering the field of Malware Analysis. The course will teach you the common assembly statements and operands as well as how to write and reverse assembly.

Day five of the class is the Student Practical Demonstration. Using the tools, skills, and methodologies taught in Days one through four of the class, students will derive answers in a Stack Tracing Assignment. Upon completion, each student will reverse engineer a binary application to uncover its capabilities and document its procedures and code paths.

Objectives

After taking this course, students will be able to understand:

- Data Representation
- Stack Memory, Heap Memory, Stack Tracing
- Common Assembly Instructions
- x86 Addressing Modes
- Repetition, Branching, and Function Calls
- Writing ASSM Statements in C
- Encryption and Obfuscation of Assembly

Topics

- What is Assembly?
- Computer Architecture Review
- X86 Memory Layout
- Essential Assembly Instructions
- X86 Memory Addressing Modes
- Strings and Arrays
- Control Structures
- Functions
- How Compilers Work
- Modern Compilers
- PE File Structure
- Dynamic Memory Allocation
- Floating Point Arithmetic
- Identifying Developer Code
- Malware Specific Assembly Analysis
- Student Practical Demonstration

Audience

This course is designed for:
Forensic Investigators who need to identify and examine malicious code on systems
Exploitation Analysts needing reverse engineering skills
Penetration Testers who want to develop their own tools
Malware Analysts requiring a thorough understanding malicious code

Prerequisites

Before taking this course, previous knowledge of C programming as well as a solid understanding of operating systems is recommended. Introduction to C Programming and Operating Systems Fundamentals are good preparatory classes.

Duration

Five days