ARCADIA
Cyber Defense

THE HIGHEST QUALITY
CYBER SECURITY TRAINING

We believe your cyber security team deserves a better learning experience

INTRODUCTION TO REVERSE ENGINEERING

5 days

Course Overview

In this course we present the fundamental skills for understanding the malware actions and behaviour of Windows programs.

We start with an introduction to Intel assembly language - both 32 and 64 bit, and carry on with a detailed exposition of Windows executables and dynamic libraries. Reverse engineering of actual malware examples are then presented in a tutorial fashion using professional disassembly and debugging software.

Through hands-on labs, the students learn how to defeat code obfuscation and techniques used by malware authors to hamper dynamic reverse engineering.

Materials to bring

Laptop computer able to run 64-bits virtual machines.

VMware Workstation 11+, or VMware Fusion 6+, or VMware Player 11+

Course prerequisites

Medium-level computer programming skills

Course Breakdown

Day 1 Static reverse engineering

- Introduction
- Binary analysis
- PE file format
- Introduction to x86 assembly
- Introduction to IDA

Day 2 Dynamic reverse engineering

- VM configuration
- Sysinternals tools for reverse engineering
- Introduction to the IDA debugger

Day 3 Common malware behaviours

- Types and families
- Persistence
- Data encoding

Day 4 Advanced dynamic reverse engineering

- Introduction to AMD64
- Code obfuscation
- Real malware reverse engineering

Day 5 Anti-reverse engineering techniques

- Basic techniques
- Bypass approaches