Malware Analysis 101 Workshop

Course 90908 – 8 Hours

Overview

The term malware describes a very broad domain of offensive tools used for a huge verity of tasks, from active information gathering to exploitation,hostile takeovers (ransomware), maintaining evasive footholds in systems and more.
One of the most effective ways the defence domain has to gain new insight into how new malware behaves is through the tools and techniques of the malware analysis field. This hands-on seminar will take you through some of the most interesting ways someone could take in order to analyse the behavior of a new and unknown system.
Relevant audience for this seminar are people with at least three years of experience in either the cyber security domain or low level software development.
A firm understanding of networking in win/linux system internals is a great plus.

Who Should Attend

- IT Manager
- SOC Analysts
- Research Groups

Prerequisites

- Windows operating system

Course Contents

- Malware Analysis Primer
  - Goals of Malware Analysis
  - Incident Response Role
  - Anti-Virus Signatures
  - Types of Malware and Definitions
- Malware Extraction
  - Receive it as a PCAP file
  - Receive it as a Memory
- Basic Static Techniques
  - Digital Signatures
  - Anti-virus Scanning
  - PE file
  - Strings, Functions and Headers
  - DLL Linking Methods
  - Packed Malware
- Basic Dynamic Analysis
  - Configuring Sandbox for Examine
  - Process Monitor
  - Process Explorer
  - Creating Fake Networking
  - Registry Analysis