

Hands ON Malware Analysis

Duration :5 Days

Introduction to Malware Analysis

Types Of Malware Analysis

Setting Up The Lab Environment 1

Malware Sources

Static Analysis

Determining the File Type

Fingerprinting the Malware

Multiple Anti-Virus Scanning

Extracting Strings

Determining File Obfuscation

Inspecting PE Header Information

Comparing And Classifying The Malware

Dynamic Analysis

Lab Environment Overview

Dynamic Analysis (Monitoring) Tools

Dynamic Analysis Steps

Putting it All Together: Analyzing a Malware Executable

Dynamic-Link Library (DLL) Analysis