Course Code: 8H300GW

Course Title: Introduction to Malware Analysis and Assembly Language

Description:

In this course, through video demos, hands-on reverse engineering, and capture-the-flag activities, you will be introduced to the processes and methods for conducting malware analysis of different file types. You will analyze native executable files, and analyze popular files like PowerShell, JavaScripts, and Microsoft Office documents.Then you will learn the fundamentals of Assembly language, basic Win32 Assembly programming concepts, and how Reverse Engineers use Assembly to analyze malware.

Objectives:

- Discuss common malware analysis use cases
- Explain the types of malware analysis
- Set up a decompiler and a debugger
- Analyze various common file formats for malware
- Practice what you learn through capture the flag exercises

Prerequisites:

- Basic understanding of Operating Systems
- General programming knowledge helpful, but not necessary

Duration:

20 Hrs

Topics:

- Malware analysis overview and process
- Lab Setup
- Static and Dynamic analysis
- Manual code reversing
- Analyze PowerShell, JavaScript, and Word documents
- Analyze ELF file format
- Analyze ASPX Webshell and JAR files
- Introduction to Assembly Language

Audience:

This course would be ideal for students who have an interest in a Malware Analyst role.