Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Du kan nå oss her

Postboks 6562 ETTERSTAD, 0606 Oslo, Norge

Email: kurs.ecs.no@arrow.com
Phone: +47 22 02 81 00

Introduction to Malware Analysis and Assembly Language

CODE:	LENGTH:	PRICE:
8H300G	20 Hours	kr6,580.00

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

Audience

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

Prerequisites

- Basic understanding of operating systems
- General programming knowledge is helpful, but not necessary

Programme

- 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

Session Dates

Date	Location	Time Zone	Language	Type	Guaranteed	PRICE
22 Nov 2024			English	Web based Training		kr6,580.00

Tilleggsinformasjon

Denne treningen er også tilgjengelig som trening på stedet. Kontakt oss for å finne ut mer.