Malware Forensics

Duration: 4 Days

COURSE DESCRIPTION

This course focuses on the technique and tool for analyzing various types of malwares which are generally used in cyber-attack. In-depth analysis of malwares using both static and dynamic analysis will be introduced and explained step-by-step throughout in this training. This course is suitable for a security analyst who works at Tier 3 of Security Operation Center.

COURSE OUTLINE

- Assembling a toolkit for effective malware analysis, Examining static properties of suspicious programs
- Recognizing common malware characteristics at the Windows API level (registry manipulation, keylogging, HTTP communications, droppers)
- In-Depth Analysis of Executable Files, Malicious Document Files, ZIP and Rar files, Network Traffic Captured Packets, and many more sample malicious files.
- Static and Dynamic Methods for Malware Analysis Using Memory Forensics and Malware Code and Behavioral Analysis Fundamentals.
- Reversing Malicious Code, analyzing techniques that malware use to protect malicious software from being examined.
- Demonstration and Hand-on Exercises.

PREREQUISITES

- Basic of SOC Tier 1: Processes and Tools
- General knowledge of computer and operating system.
- Some experience in computer programming languages.
- Background in Computer Network and Tools such as Wireshark.
- Some basic of Linux command.
- Be familiar with Virtual Machine (VMware or Virtual Box)

WHO SHOULD ATTEND

A system administrator, a security analyst, and a forensic investigator with some background in conducting forensic analysis, network traffic analysis, log analysis, and security assessments. It is also well suited for those managing CIRT / incident response teams, or those in roles that require oversight of forensic analysis and other investigative tasks.

SKILL LEVEL

- Intermediate – Advanced Users / SOC Tier 2 and 3

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th
Call us today 0-2634-7993-4
177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th