Malware Forensics for Forensic Investigator and Incident Response Team

Duration: 5 Days

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)
- Analysis of Executable Files, Malicious Document Files, ZIP and Rar files, Network Traffic Capture Packets, and many more sample malicious files.
- In-Depth Analysis of Malicious Browser Scripts and Web-Based Malware.
- 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

WHO SHOULD ATTEND

- Network Administrator who are working in the areas of computer and network security
- Incident Response Team Members who regularly respond to complex security incidents/intrusions from APT groups/advanced adversaries
- Digital Forensic Analysts who want to investigate cyber incidences and advanced intrusion attacks.
- Information Security Staffs who are dealing with cyber-attacks and data breach incidents and intrusions
- IT staffs who are interested in the area of cyber security and digital forensics, and need to know how to detect, investigate, remediate, and recover from compromised systems

PREREQUISITES

- General knowledge of computer and network system.
- Some experience in computer programming languages.
- Background in assembly, hex editor, disassembler tools, etc.
- Some basic of Linux command

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