Incident Handling and Response for Cyber Attack

Duration 4 Days

COURSE DESCRIPTION

Cyber-attacks, nowadays, requires effective detection and quick response. To achieve this requirement, Computer Incident Response Teams (CIRTs) play a very important role to deal with these issues. Therefore, many organizations are demanding that incident handling and response teams must be able to handle, collect, and analyze digital evidences from the system after the attacks. Based on these reasons, this course mainly focuses on the technique to collect digital evidences, as well as the process of examination and analyzing after cyber-attacks.

COURSE OUTLINE

- The Cyber Attack and Investigation Techniques – Introduction to the techniques of cyber attack investigation, and methods of attack analysis. This topic includes the following topics: Network Log Collection, Log Investigation and Analysis, and Techniques and Tools for Attack Investigation
- The Incident Response Process – Introduction to the cyber attack, the steps of an effective incident response process, and the recovery and remediation process. This topic includes the following topics: Preparation, Detection and Analysis, and Remediation.
- The Digital Evidence Acquisition – Overview of the acquisition techniques for digital forensic evidence collection which is mainly used for finding the source of attack. This topic includes the following topics: Forensic Imaging, and Live Response Acquisition.
- Introduction to Windows Evidence – Basic concept of the key sources of evidence that can be used to investigate a compromised Windows system. This module focuses on the following artifacts: Network Connections and Browser History, File System Analysis, Windows Registry, Event Logs, and Live Memory Forensics etc.
- Introduction to Cyber attack using malware – Overview of the primary types of malware, how to create a safe malware analysis environment, the malware analysis and reporting process, static and dynamic analysis, tools used to detect, identify, and analyze malware.
- Demonstration and Hand-on Exercises for Attack and Malware Detection and Analysis – This section demonstrate how malware works, how to detect the malicious processes and connections. The attendances receive hand-on exercises in order to practice and improve some technical skill for analyzing and responding to incidents.
- Detecting and Analyzing Malware in Memory – Introduction to the architecture of Windows operating system, the architecture of Random Access Memory (RAM), pagefile, and virtual memory. The techniques to identify and trace malware artifact running in memory such as processes, handles, and memory sections. This topic introduces standard techniques and favorite tools used for detecting and analyzing malware running in memory.
- Advanced Persistent Threat (APT) – Introduction to the nature of cyber attack named Advanced Persistent Threat (APT). In-depth review of malware analysis used by APT in order to monitor, create a covert channel, and communicate back to command & control center (C&C). The process of forensic investigation to examine network log, Windows registry, shellbags, LNK files, and MRU keys
- Cases Study and Hand-on Exercises for APT – Instructor provides an in-depth review of an actual intrusion case that involved the use of multiple pieces of malware. This section also demonstrates how APT and malware works, as well as how to identify the malicious processes and connections. The

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

attendances receive hand-on exercises in order to practice and improve some technical skill for analyzing and responding to incidents.

PREREQUISITES

- 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.

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

Advanced.

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