SDA-ACADEMY
Cybersecurity training

THINKCYBER

NX-212

Syllabus

Windows Forensics

CYBERIUM **ARENA**

- SIMULATOR -

Description

Windows Forensics is an essential skill in the cybersecurity world. Participants will learn how different computer components work and how to investigate during and after a cyber incident. The training will focus on developing hands-on capabilities of forensics teams or individual practitioners.

The course helps prepare for the certification exams CHFI (ECICouncil) and GCIH (SANS).

Target Audience

This course targets participants with basic knowledge who wish to understand cyber investigations.

Objectives

- Understanding the Windows files structure
- Accessing concealed files on the system
- Extracting sensitive information
- Mastering the steps of incident response

Module 1: Computer Hardware

The module will cover different components of computer hardware. Students will learn main components of storage-disks, and the Windows OS structure.

Drives and Disks
Data Representation
Volumes & Partitions
Disk Partitioning and Management Tool
Solid State Drive (SSD) Features

Data and Files structure
Hex Editors File
Structure

Understanding Windows OS structure
NTFS Structure Master
File Table Windows
System Files

Module 2: Forensic Fundamentals

In this module, students will learn the Windows OS's internal components and the forensic investigation process.

Understanding Hashes and Encodings
The Use of Hash for Forensics
Base Encodings
Windows Artifacts

Startup Files
Jump List
Thumbnail Cache
Shadow Copy
Prefetch and Temp Directories
Registry Hives
Embedded Meta Data

Module 3: Collecting Evidence

Students will master techniques for collecting evidence, accessing, and retrieving volatile and non-volatile information during this module. Students will learn techniques for collecting evidence, accessing, and retrieving volatile and non-volatile information.

Forensic Data Carving
Manual Carving
Automatic Tools

Collecting Information
Event Viewer
Detecting Hidden Files
Collecting Network Information
Sysinternals
Extracting Credentials

Module 4: Analyzing Forensic Findings

In this module, students will understand how to uncover hidden information, detect tampered files, work with memory, and analyze the Ram.

Drive Data Acquisition
Creating an Image
Analyzing Prefetch Files

Working with Volatile-Memory
Extracting Data from RAM
Identifying Network
Connections Dumping Processes from Memory

Registry analysis
Viewing Registry Dumps Using Oat Files
Forensics Findings in the Registry

Anti-Forensics Techniques
Wiping Drives
Artifact Removing