CYBERIUM ARENA

Description

Windows Forensics plays a crucial role in cybersecurity. Trainees will understand the data storage mechanisms of the Windows OS and acquire the skills to conduct investigations during and post cyber incidents.

WINDOWS FORENSICS

Module 1: Digital Data

This module explores file and disk handling, encoding, and number systems, delving into digital sizes and SSD features. It includes hands-on training with a Hex Editor and teaches disk and file viewing techniques. The section proceeds to cover automatic carving, and methods to examine system files and metadata in Windows.

Files and Disks
Encoding
Number Systems
Digital Sizes
Solid State Drive (SSD) Features
Hex Editor
Working with Offsets
Viewing Files
Viewing Disks
Automatic Carving
Carving Methods
Automatic Carvers
Windows System Files
Metadata
Viewing Metadata
Modified Accessed Created
Editing Exif Data

Module 2: File Forensics

This module delves into steganography, teaching how to identify, extract, and create hidden files. It transitions into hard disk analysis, focusing on system files and Master File Table (MFT) analysis. It also imparts hands-on experience with Forensic Toolkit (FTK), a crucial tool for digital forensics. This module equips learners with vital skills in data hiding and disk analysis.

Steganography
Identify Hidden Files
Extracting Hidden Files
Creating Hidden Files
Hard Disk Analysis
System Files
MFT Analysis
Working with FTK

Module 3: Collecting Evidence

This module delves into the analysis of digital artifacts. It focuses on registry analysis, including data extraction and examination of NTUSER.DAT files. The module concludes with techniques for conducting a general search and the use of registry viewers, thereby enhancing learners' understanding of digital artifact investigation.

Artifacts
Artifact Directories
Browsers
Shadow Copies
Registry Analysis
Extracting Data
NTUSER.DAT Analysis
General Search
Registry Viewers

Module 4: Analysis

This module delves into the complex realms of memory, event, network, and malware analysis. It imparts key skills for inspecting computer memory, investigating system events, analyzing network interactions, and examining malicious software, thereby equipping learners with critical abilities for cyber forensics investigations.

Memory Analysis
Creating an Image
Working with Volatility
Carving Data from RAM
Events Analysis
Event Viewers
Setting Audit Policy
Custom Search
Network Analysis
Service Protocol Analysis
Identifying Darknet Connections
Malware Analysis
Basic Static Analysis
Basic Dynamic Analysis

NX Defense | LEVEL: 3 | DURATION: 10-12 weeks (self-paced) / 40h (trainer-led)