SETC Training Corporate Logo

IT Security Training: Windows Forensics from A to Z (WIFORE, 4 jours)

Description

The course Windows Forensic Forensics Analysis (IT Security Training) explores the complexities of gathering digital evidence on everything Windows. The training starts with a general discussion of evidence types and related evidence gathering techniques. This is followed by a detailed exploration of love response and the collection of both volatile and non-volatile data on the Windows platform. The training course covers the analysis of Windows memory, the FAT and NTFS file systems and various Windows artefacts including web browsers, event logs, page files and more.

Tarifs

- Tarification: $3,750/person
- Rabais de 10% lorsque vous inscrivez 3 personnes.

Plan de cours

First Steps

The Forensics Process: Concepts and Requirements

Understanding the Lab Environment

General Principles: Integrity, Chain of Custody and More

Phases of Investigation

High-level Process

Similarities and Differences: Windows 7, Windows 10 and Windows Server

Getting File System Images

Techniques for Getting File System Images

Building a Toolkit

Building a Lab

Building a Report Template

Live Response: Collecting Volatile Data

Exploring Forensic Requirements

Conducting Immediate Response and Triage

Exploring Live Response

Understanding the Difference between Volatile and Non-Volatile Data

Understanding Local, Remote and Hybrid Response Strategies

Reactive vs Proactive Methods

What Data to Collect?

Writing the Report

Data Collection – Volatile Information

Overview of Volatile Information

Exploring Available Tools

Collecting Logged-On Users

Collecting Open Files

Collecting Network Information and Status

Collecting Process Information

Collecting Process to Port Mappings

Collecting Process memory

Exploring Clipboard Concepts

Collecting Service Driver Information

- Collecting Command History
- Collecting Mapped Drives
- Collecting Shares

Data Collection – Non-Volatile Information

- Overview of Non-Volatile Information
- Exploring Available Tools
- Exploring the Registry
- Clearing the Page File
- Disabling Last Access
- Managing Autoruns
- Exploring Event Logs
- Collecting Device and Other Information

Live Analysis

- Analyzing Results form the Initial Scan
- Getting File Metadata
- Building a Timeline
- Examining User Command History
- Collecting File Hashes
- Dumping RAM
- Moving On

Windows Memory Analysis

- About Memory Architecture – Essential Concepts
- Exploring Memory Collection and Dumps
- Exploring Methods for Dumping Memory
- Dumping Physical Memory: The Tools of the Trade
- Analysis of a Physical Memory Dump
- Understanding Processes
- Parsing Memory Dump Contents
- Parsing Process Memory
- Extracting the Process Image
- The Page File
- Understanding Pool Allocation
- Memory Forensics

The FAT Filesystem

- FAT Basics
- Exploring Volume Boot Records
- Exploring File Allocation Tables
- Exploring Directories and Deleted Files
- Putting it All Together
- About File Forensics
- Exploring Hidden Information
- Exploring File Signatures
- Analyzing Mounted Images
- Putting it All Together

The NTFS File System

- NTFS Essential Concepts
- NTFS Volume Boot Record
- The Master File Table
- Exploring Large and Small Files
- Exploring Directories

Exploring Deleted Files
Using Python for NTFS
Exploring Timelines

Registry Analysis

Understanding the Structure and Role of the Registry
Working with the Registry
Registry Analysis with RegRipper
Getting System Information
Exploring Autostart Locations
Exploring Removable Devices
Exploring Mounted Devices
Finding and tracking Users
Exploring Virtualization

Windows Artifacts

Exploring the Recycle Bin
Exploring Event Logs
Exploring Prefetch Files
Exploring User Directories
Exploring Web Browser History
Exploring EMail
Exploring Various Artefacts

About Malware

A Brief History of Malware
Doing your Research
Investigating Unknown Files
Packers
Setting up a Sandbox Environment