MINDCORE

DFIR 101

Practical Forensics – An Essential Guide to Incident Response

About this course

This course provides the knowledge and resources required to triage, analyze and effectively respond to computer security incidents. The participants, through the understanding of theory and a strong focus on practical exercises, will be able to acquire best-of-breed tools and techniques aimed at quickly identifying and thwarting attacks, uncovering and preserving vital evidence, while allowing for complete and accurate recovery of the affected assets.

Overview

The **Practical Forensics course** is a comprehensive and strategic overview of digital forensics and incident response based on industry best practices and real world experience, including real cases related to breach of payment card data, hacktivism and insider threat.

The course is based on NIST's special publication 800-61 (Computer Incident Handling Guide) and other guidelines. The topics covered include:

- Organizing an Incident Response Capability
- Threat Intelligence: cyber kill-chain and the MITRE ATT&CK framework
- Preparing for an incident
- Handling an incident
    - Incident detection and analysis
    - Containment, eradication and recovery
    - Evidence collection and retention
        - Network forensics
        - Live response data
        - Memory forensics
        - File system forensics
        - Mobile devices and cloud environments

- Post-incident activities
- Coordination and information sharing

Format: The course combines theory and hands-on practical exercises. The participants start by learning about computer security incidents and the process of preparing and handling these incidents. They are then given access to a purpose-built environment where they can use the tools and techniques learned to spot, contain and uncover evidence of cyber incidents that can be used to prosecute or take the appropriate response.

Duration: 2 days (16 hours)

Attendee Profile

The course is designed for professionals who are involved in threat management and the handling of computer related incidents, such as:

- CSIRT and Blue Team Members
- Incident Responders
- Information Security professionals / CISOs
- IT Auditors
- Members of Legal Team

Materials

- Printed materials
- Virtual image containing all tools used
- Certificate of Participation (CPE Points)