



Training Catalogue

Knowledge is power



IR 3.01 | Incident Response & Forensic Analysis (Level 1)

Overview

This intensive hands-on one-day course is designed to introduce you to the investigation methods and tools you can rely on in the event of a security incident. It will take you into the world of incident response and forensic analysis, covering the different scenarios for acquiring RAM and hard disks, then focusing on triage through live analysis, as well as in-depth investigation through offline analysis.

Who should attend

- Ethical hackers, incident responders
- IT system, networks admins

Skills you'll learn

- N/A
- Level 2
- 1 day
- French or English

Course Modules

- **Introduction to DFIR**
 - The pillars of incident response
 - A few words on digital forensics
 - Tactics, techniques and procedures
 - Incident response phases and common mistakes
 - Incident response lifecycle and success factors
- **Some words on incident response procedures**
 - The importance of documentation
 - Chain of custody
- **Acquisition**
 - Objectives, common pitfalls and data volatility
 - RAM acquisition on Windows
 - RAM acquisition on Linux
 - RAM acquisition on virtual machines
 - Disk acquisition
 - Various scenarios depending on conditions like physical access to the host, availability considerations, and disk extraction
 - Image file formats
 - Slack space
 - A few words on SSDs (interfaces and carving issues)
- **Analysis**
 - Bad VS good starts
 - Live analysis
 - Objective and drawbacks
 - What to look for?
 - Offline analysis
 - Advantages and prerequisites
 - Memory analysis
 - Filesystem analysis
- **Lab - Investigate an Active Directory compromise**
 - Triage
 - Memory analysis
 - Disk analysis
- **Small game to remember the most important points of the day with fun**

