Fundamentals of Incident Response and Digital Forensics

A 30-Hour Training Course

Description

This 30-hour training course (FOR111) is designed for those entering the field of incident response and digital forensics. The course covers Incident Response according to the NIST standard with the four phases of (1) Preparation, (2) Detection & Analysis, (3) Containment, Eradication, & Recovery, and (4) Post-Incident Activity. Likewise, the course covers Digital Forensics as per the NIST standard with the four phases of (1) Collection, (2) Examination, (3) Analysis, and (4) Reporting. The two processes are not independent of each other; the student will learn how integrate Digital Forensics within the context of Incident Response. The student will be equipped with forensics tools and techniques to handle data from various sources: Data Files, Operating Systems (including volatile and non-volatile data), Network Traffic, and Applications.

The course contains numerous hands-on labs and real-life exercises. The student will acquire practical skills in utilizing the Security Onion Linux distribution and the SIFT Workstation. Some of the main tools covered are Volatility Framework (for RAM analysis), Autopsy (for disk data analysis), FTK-Imager, WinPMem, and others. Additionally, the labs and techniques will be performed on Windows as well as Linux systems. After completing this course, the student will be able to start a career as Incident Responder and Digital Forensics Analyst.

Outline

Part 1 Incident Response

Module 01 Introduction to Incident Response (IR)

- The Cyber Kill-Chain and Attack Lifecycle
- Understanding Cyber Security Incident
- The Purpose of Incident Response
- Cyber Security Incident Response Team (CSIRT)
- The Incident Response Process
    - Preparation
    - Detection & Analysis
    - Containment
    - Eradication
    - Recovery
    - Post-Incident Activity
- Incident Response Playbook

Module 02 IR: Initial Preparation and Building Readiness

- Preparing the Incident Response Team
- Preparing your Infrastructure and Technology
    - Data Loss Prevention
    - Endpoint Detection and Response
    - Security Information and Event Management (SIEM)
- Building your Incident Response Process

Module 03 IR: Detection of Incidents

- Gathering and Recording Initial Facts
- Maintaining Clear Incident Notes
- Prioritizing the Elements of Investigation
- Indicator Generation
- Examining the Indicators
- Making Informed Decision

Module 04 IR: Containment and Eradication

- Network Disconnection
- Shutting-Down a Machine
- Sandboxing and Monitoring
- Containment Considerations
- Eliminating Incident Components
- Mitigating Exploited Vulnerabilities
- System Restoration

Module 05 IR: Recovery and Post-Incident Activity

- System Restoration

Part 2 Digital Forensics

Module 06 Introduction to Digital Forensics (DF)

- Staffing and Capabilities
- Tools and Techniques
- Digital Forensics Process
    - Collection
    - Examination
    - Analysis
    - Reporting
- Integrating Digital Forensics into Incident Response
- Incident Response Considerations

Module 07 DF: Using Data from Data Files

- Data File Basics
  - File Storage Media
  - Filesystems
  - Other Data on Media
- Collection of Data Files
  - Copying Files from Media
  - Data File Integrity
  - Modification, Access, & Creation Times
- Examination of Data Files
  - Locating the Files
  - Extracting the Data
  - Using Forensic Toolkit
- Analysis of Data Files

Module 08 DF: Using Data from Operating Systems

- OS Basics
  - Volatile Data
  - Non-Volatile Data
- Collection of Volatile OS Data
  - Types of Volatile Data
  - Prioritizing Data Collection
  - Local Acquisition of RAM
  - Remote Acquisition of RAM
  - Live Acquisition on Windows Systems
  - Live Acquisition on Linux systems
- Collecting of Non-Volatile OS Data
  - Forensic Imaging Techniques and Tools
  - The Use of Write-Blockers
  - Types of Disk Imaging
  - Duplication of Virtual Machines
- Examination and Analysis of OS Data

Module 09 DF: Using Data from Network Traffic

- TCP/IP Basics
  - Application Layer
  - Transport Layer
  - IP Layer
  - Physical Layer
  - Layer's Significance in Network Forensics
- Network Traffic Data Sources
  - Firewalls and Routers
  - Packet Sniffers and Protocol Analyzers

    - Remote Access
    - Security Event Management Software
    - Network Forensics Analysis Tools
    - Other Sources
- Collection of Network Traffic Data
    - Legal Consideration
    - Technical Issues
- Examination and Analysis of Network Traffic Data
    - Identifying an Event of Interest
    - Determining Data Source Value
    - Tools
    - Drawing Conclusions
    - Attacker Identification

Module 10 DF: Using Data from Applications

- Application Components
    - Configuration Settings
    - Authentication
    - Logs
    - Data
    - Supporting Files
    - Application Architecture
- Types of Applications
    - E-Mail
    - Web Usage
    - Interactive Communications
    - File Sharing
    - Document Usage
    - Security Applications
    - Data Concealment Tools
- Collection of Application Data
- Examination and Analysis of Application Data

Module 11 Malware Analysis

- Malware Classification
- Sandboxes and Scanners
- Static Analysis
- Dynamic Analysis