Linux Forensics

Course 71588 – 40 Hours

Overview

OS Forensics is the ART of extracting evidence and important artifacts from a digital crime scene that can help the investigator reconstruct the chain of events. During this course, students will learn the basics of computer hardware and the Linux-OS filesystem. The students will learn to collect and analyze forensic evidence and write official reports.

The course helps prepare for the certification exam CLFP (7Safe).

On completion, Delegates will be able to

- Access concealed files on the system and extracting relevant information
- Master the steps of incident response
- Analyze relevant case studies

Who should attend

- Law enforcement officers & intelligence corps
- Incident responders
- Computer investigators
- IT/network administrators

Prerequisites

Advanced knowledge of:

- Linux
- Network Forensics (Course 71586) or Windows Forensics (Course 71585)

Course Contents:

Module Title	Description
Module 1: Computer Hardware The first module will cover different components of computer hardware. Students will learn the main components of Storage-Disks, and the structure of the Linux OS.	▪ **Drives and Disks** ○ The Anatomy of a Drive ○ Data Sizes ○ Volumes & Partitions ○ Disk Partitioning and the Disk Management Tool ○ Solid State Drive (SSD) Features ▪ **Understanding Linux-OS Structure** ○ Linux Directory Structure ○ Services and systemd ○ Users and Groups ○ Understanding Shells
Module 2: Forensic Fundamentals This module will expose students to the internal components of the Linux OS. Students will learn about tools that will help them with the Forensics investigation process.	▪ **Understanding Hashes and Encodings** ○ Hash as a Digital Signature ○ The Use of Hash for Forensics ○ Base Encodings ▪ **Linux-OS Artifacts** ○ User Activity Files ○ Physically Accessing Running Process ○ Service Logging Using Journalctl ○ Logfile Analysis ▪ **Cracking the Shadow and Passwd Files** ▪ **Files in /dev** ▪ **SUID/SGID files** ▪ **Data and Files structure** ○ Hexadecimal Editing Tools ○ File Structure ○ Embedded Metadata ○ Working with Clusters
Module 3: Collecting Evidence Students will master techniques for collecting evidence during this module, accessing, and retrieving volatile and non-volatile information. Students will master techniques for collecting evidence, accessing, and retrieving volatile and non-volatile information.	▪ **Forensic Data Carving** ○ Using Bvi for Forensics Carving ○ Automatic File Carving Tools ○ Files with Basic System-Info and Suspicious User-Info ▪ **Collecting Information** ○ Indenting Evidence of Program Execution

	○ Detecting Hidden Files and Directories ○ Collecting Network Information ○ Investigating Server Logs ○ Mounted Filesystems ○ Loaded Kernel Modules ▪ **Drive Data Acquisition** ○ Introduction to FTK-Imager CLI ○ Capturing Volatile-Memory using LiME vs. using fmem
Module 4: Analyzing Forensic Findings In this module, students will understand how to uncover hidden information, detect tampered files, work with memory, and analyze the RAM.	▪ **Analyzing captured images** ○ Features of FTK CLI ○ Analyzing Inode Numbering ○ Building Timelines as a CSV ○ Extracting and Examining System Logs ▪ **Advanced Linux-OS Analysis** ○ Strace and Ltrace ○ Understanding Obfuscation ○ Working with Binaries ○ Introduction to GDB ▪ **Working with Volatile-Memory** ○ Extracting Data from RAM ○ Identifying Network Connections ○ Dumping Processes from Memory
Module 5: Data Labelling and Report Writing Participants will study different forensics reports prepared by investigators following past incidents and learn how to write a professional summary, including which points to consider when addressing the documentation of findings of an event.	▪ **Introduction to Report Writing** ○ Device Identification ○ Preservation of Data ○ Collecting Evidence ○ Examination and Analysis ○ Documentation ○ Evidence Presentation ○ Final Guidelines ▪ **Tools for Correct Reporting** ○ Autopsy ○ Dradis