Digital Intelligence®

Digitalintelligence.com

Known Network Intrusion Forensic Examinations (KNIFE)

INTERMEDIATE LEVEL

Course Objectives

This 3 day intermediate class is designed to provide the student with the skills and techniques to respond to a cyber intrusion incident. Students learn the anatomy of an intrusion, collection of memory and volatile artifacts, and techniques to unravel the mystery of the compromised network.

Prerequisites

This hands-on course is geared towards investigators with a minimum of 6 months experience in forensic casework and a basic understanding of Microsoft data structures.

To gain the maximum benefit from this course you should meet or exceed the following requirements:

- Read and understand the English language
- Have attended basic digital forensic training
- Have at least 6 months experience conducting digital forensic examinations
- Be familiar with the Microsoft Windows environment and data recovery concepts

The course will be structured as follows:

Course Outline

The course will follow adult learning principle through training aids such as presentations, diagrams, and practical instructor lead examples. Each artifact will be presented in either one or two 50 minute sessions followed by review questions. Students will be given the opportunity throughout the course to ask questions and discuss objectives covered in more detail. Throughout each day students will have practical exercises to work on in order to reinforce the topics with a final practical at the culmination of the training.

Introduction and Tools Used During the Course

- Introduction by the course instructor and students
- An overview of the tools that will be used in the course for demonstrations and student practical exercises. References may be made to commercial products in addition to tools that are free and in the public domain.

Understanding Attacks

- Anatomy of an Attack
  - Network Topology
  - Common Progression: Compromise, Stabilization, Expansion, Collection, & Exfiltration
  - Common Attacks
- Introduction to Wireshark
  - PCAP, TCP/IP, & Beaconing Activity

Planning Incident Response

- Incident Response Plan
  - Roles, Indicators (IOC), and Notification
- Phases of Response
  - Identification, Monitoring & Containment, Recovery, and Hardening
- Anatomy of an Attack
  - Common Progression: Compromise, Stabilization, Expansion, Collection, and Exfiltration
- Response Methods
  - Memory Collection, Persistence Examination, Execution Indicators, and Log Analysis

Live Response

- Response Toolkit and Commands
  - Toolkit creation, Sysinternal Tools, and Command Line Tools
- Basic Memory Structure
  - Pages, Kernal Debugger Data Block (KDBG), EPROCESS Block, Process Environment Block (PEB), and Virtual Address Descriptor Tree (VAD)
- Memory Acquisition
  - Live Collection, Pagefile, Hiberfil, Crash Dumps, and Virtual Machine Memory
- Introduction to Volatility
  - Profiles and Plugins
- Volatility - Malicious Processes
  - Pslist, Processbl, Psscan, Pstree, Psxview, Malfind, and Procdump
- Volatility - Memory Objects
  - Dllist, Handles, and Netscan

Execution Identification / Log Analysis

- Windows Artifacts
  - Prefetch, UserAsisst, Shimcache, Amcache, Link Files, Jump Lists, and Volume Shadow Copies
- Log File Analysis
  - Lateral Movement, Login Events, RDP Logs, and Account Creation

Contact info
sales@digitalintelligence.com
1.866.344.4683
Outside the US: +1 262.782.3332