kaspersky.academy

Incident Response and Digital Forensics

Curriculum

Konstantin Sapronov, Ayman Shaaban
Kaspersky Lab

17.06.2019

kaspersky.academy

Incident Response and Digital Forensics

Course Duration

44 instructor-led hours (+ 70 hours of individual study)

Abstract

In a world where cyber-attacks are discovered every day, skills such as responding to security incidents, conducting an initial live analysis of compromised computer to detect threats, collecting digital evidence in a forensically sound environment and analyzing collected evidence to uncover the attack scenario, are no longer optional.

All of these skills are highly required for security professionals to face the well-organized cyber-attacks which target institutions regardless of their business type; financial, governmental or industrial.

In this course, we will provide the knowledge needed to assemble different types of evidence properly, and walk through the various stages of the analysis process.

Objectives & Learning Goals

This course will fully introduce attendees to incident response and digital forensics. The hands-on, practice-oriented format of this course will allow students to obtain the required skills to conduct the cycle of detection, response, and analysis of compromised systems, in both live and postmortem situations, with best practices to discover different cyber attacks.

We will start by discussing the principles of incident response and digital forensics processes and move on to learning about the approaches that are used to conduct evidence collection and analysis. We will study various tools to perform evidence collection and live analysis and go through different techniques to analyze volatile and nonvolatile data. We also will talk about data recovery and learn how to use multiple tools to perform registry and system logs analysis.

Next, we will be taught how to build a timeline of all operating system activities and how to analyze browsers artifacts and e-mails clients, then go on to extract data from a computer’s memory and investigate network traffic.

Methodology

Almost all the course’s topics will be covered with theoretical and practical parts. The practical exercises are presented as labs, and they will require access to desktops or laptops with network connectivities. Also, students will have homework to apply their newly gained skills to a better understanding of the study topics and for course assessment as well.

Evaluation and grading

Evaluation will be based on homework (45%), class tests (35%) and the final test (20%).

kaspersky.academy

Course Outline

1. **Introduction**
   - 1.1. General security definitions
   - 1.2. Security in nutshell
     - 1.2.1. Security cycle
     - 1.2.2. Confidentiality
     - 1.2.3. Integrity
     - 1.2.4. Availability
     - 1.2.5. Non repudiation
   - 1.3. Impact of recent major hacking incident
   - 1.4. How targeted attacks work
     - 1.4.1. APT attacks vs normal infections
     - 1.4.2. Kill chain process
   - 1.5. Security services.
     - 1.5.1. Types of security services
     - 1.5.2. Reactive vs proactive security services

2. **Incident response**
   - 2.1. Incident response terms and definitions
   - 2.2. Incident response process and phases
     - 2.2.1. How to prepare enterprise environment for IR?
     - 2.2.2. Determining scope of attack
     - 2.2.3. Isolating infected system/s
     - 2.2.4. Analysis
     - 2.2.5. Scanning the environment
     - 2.2.6. Lessons learned
   - 2.3. Incident detection
     - 2.3.1. Host vs network based detection
     - 2.3.2. Live analysis
       - 2.3.2.1. Sysinternals suite
       - 2.3.2.2. IRCDs
       - 2.3.2.3. Powershell (Local and remote executions)
     - 2.3.3. Evidence acquisition
       - 2.3.3.1. Order of volatility
       - 2.3.3.2. live vs post-mortem acquisitions
       - 2.3.3.3. Host based evidence acquisition
       - 2.3.3.4. Network based evidence acquisition
     - 2.3.4. Log file analysis using regular expression
   - 2.4. Indicator of compromise
     - 2.4.1. STIX
     - 2.4.2. TAXII
     - 2.4.3. OpenIOC
   - 2.5. Scanning using IOC
     - 2.5.1. YARA
     - 2.5.2. SNORT
     - 2.5.3. BRO Network Security Monitor
   - 2.6. Network analysis using Wireshark
   - 2.7. Testing executables using Noriben sandbox

3. **Digital Forensics**
   - 3.1. Digital forensics introduction
   - 3.2. Building digital forensics lab
     - 3.2.1. Hardware and software

- 3.2.2. Lab size
- 3.2.3. Lab security
- 3.2.4. Workspace

3.3. Virtualization in digital forensics
3.4. Numeric systems and Hex-editor
- 3.4.1. Binary
- 3.4.2. Hexadecimal
- 3.4.3. Big endian and little endian

3.5. Registry analysis
- 3.5.1. Raw structure
- 3.5.2. Looking under the rocks!
- 3.5.3. Registry analysis programs

3.6. Windows OS artifacts
- 3.6.1. Recycle bin
- 3.6.2. LNK file
- 3.6.3. Thumbs DB
- 3.6.4. Prefetching
- 3.6.5. Windows tasks
- 3.6.6. Windows events

3.7. OLE compound file and Exif metadata
3.8. Browser forensics
- 3.8.1. History, cache, cookies and favorites
- 3.8.2. Internet explorer
- 3.8.3. Chrome
- 3.8.4. Firefox

3.9. Email clients' PFF analysis
3.10. HDD structure
- 3.10.1. MBR analysis
- 3.10.2. Boot sector analysis
- 3.10.3. Boot process

3.11. File system analysis
- 3.11.1. FAT file system
- 3.11.2. NTFS and MFT analysis
- 3.11.3. File deletion vs wiping in HDD
- 3.11.4. Slack space
- 3.11.5. File header

3.12. SSD forensics
- 3.12.1. SSD vs HDD
- 3.12.2. Challenges and solutions

3.13. Widows File system forensics
- 3.13.1. The Sleuth Kit
- 3.13.2. Autopsy
- 3.13.3. Data recovery
- 3.13.4. Data carving
- 3.13.5. Restore points
- 3.13.6. Shadow copies

3.14. Network traffic forensic
- 3.14.1. Dumping network traffic
- 3.14.2. Network tapping
- 3.14.3. Analysis programs

3.15. Memory analysis
- 3.15.1. Kernel mode vs user mode
- 3.15.2. Memory acquisition
- 3.15.3. Hibernation file

kaspersky.academy

Practice Sessions

Practical labs will be delivered through all the days of the course. The exercises will be delivered through real-life incidents simulated in a virtual environment. Practical exam for course assessment will take place and the end of the course.

- Kill chain reconnaissance using Maltego as OSINT example
- Ticketing system for Incident Response management
- Conducting targeted attack using simulated virtual environment. Using Acrobat reader exploit, Mimikatz and Remote access tool.
- Students will use their newly gained knowledge and skills in order to analyze the infected machine while considering incident response phases. Their task will be to identify the infection, understand all the attack components and rebuild the attack scenario. Students will work on a live virtual machine.
- Acquiring network and host based evidences of the infected machine for further analysis
- Log file analysis exercise using regular expression
- Writing Yara rule for malicious files
- Malware analysis using Sysmon and Noriben sandbox
- Network analysis using Network miner and wireshark
- Writing Snort rules for malicious traffic detection.
- IRCDs in live analysis
    - Caine
    - DEFT
- Mounting forensics HDD image to Windows and Linux Oss
- HEX editors
- Parsing registry file
- Registry file analysis using different tools; Accessdata registry viewer, MiTec WRR, RegRipper.
    - SAM
    - SYSTEM
    - SOFTWARE
- OLE Compound file analysis
- Windows special files analysis
    - Prefetch files
    - Windows Events using libevt
- Browser forensics
    - Index.dat history file analysis
    - WebcacheV01.dat file analysis
    - Cache files analysis
- OST file analysis using OST viewer and libpff
- Parsing NTFS boot sector
- Parsing MFT file’s entries including headers and different attributes.
- Sleuth Kit and autopsy
- String search on forensic image
- File carving using Foremost
- Recovering files from shadow copies
- Network traffic analysis using Bro framework
- Memory forensics
    - Process listing
    - Network activities
    - Detecting malicious code injection
    - Reading registry hives from memory
    - Dumping process from memory
- Timeline analysis
    - The Sleuth Kit for timeline creation

    - Plaso framework for super timeline
- Network analysis using Bro Network Security Monitor.

kaspersky.academy

Bibliography

- Jason T. Luttgens, Matthew Pepe, Kevin Mandia - Incident Response & Computer Forensics, Third Edition 3rd Edition
- Harlan Carvey - Windows Forensic Analysis Toolkit, Fourth Edition: Advanced Analysis Techniques for Windows 8 4th Edition
- Brian Carrier - File System Forensic Analysis 1st Edition
- Harlan Carvey - Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry 2nd Edition
- Michael Hale Ligh, Andrew Case, Jamie Levy, AAron Walters - The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory 1st Edition

Prerequisites

Basic knowledge of operating system concepts, file systems and network fundamentals.

Any scriptable language (Python, Bash, PowerShell etc.) experience is highly recommended.

kaspersky

www.kaspersky.com/
www.securelist.com

© 2019 AO Kaspersky Lab.
All rights reserved. Registered trademarks and service marks are the property of their respective owners.