Masterclass:

Compromise Aftermath:

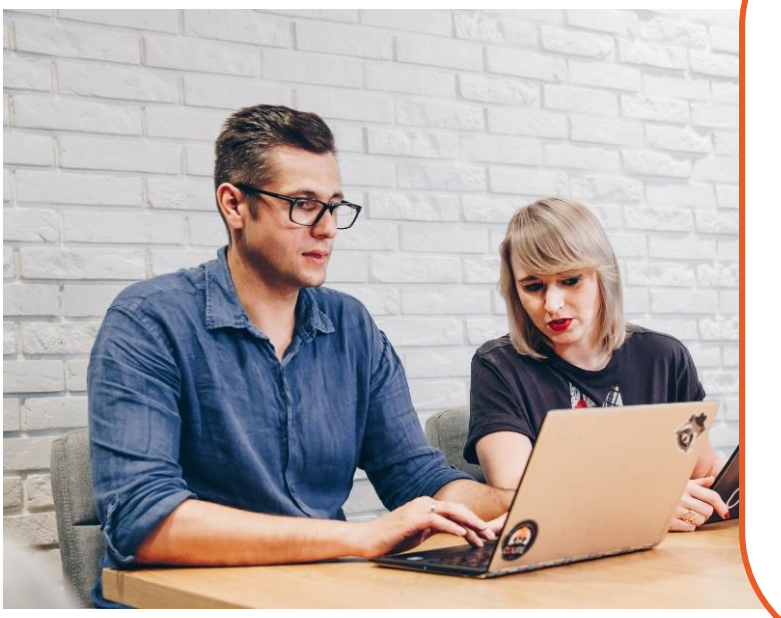
Forensic Skills Training

CQURE

Warsaw New York Dubai Zug

info@cqure.pl

www.cqure.pl
www.cqureacademy.com



Paula Januszkiewicz is a world-renowned cybersecurity Expert, a founder of CQURE and CQURE Academy, and Microsoft Regional Director and MVP.

CQURE Academy focuses on cybersecurity training program consisting of over 20 high-quality technical workshops and seminars and providing certification to specialists. Additionally, in October 2016 CQURE has successfully launched online and subscription-based training.

CQURE Experts speak at international events and engage in multiple cybersecurity projects – they bring their knowledge and experience to trainings. CQURE Academy also involves R&D – that is why CQURE Team is recognizable in the cybersecurity field.

About the course

System Forensics is a contantly evolving and crucial topics in the area of cybersecurity. In order to stay on top of the attackers, the knowledge of Individuals and Teams responsible for collecting digital evidences has to be constantly enhanced and updated. This advanced training provides skills necessary to find, collect and preserve data in a correct manner, analyze it and get to know as much about the incident as possible. This is an intense hands-on course where you will deep-dive into post-breach analysis and incident handling. We'll learn what indicators of compromise to look out for and how to perform memory and disk dumping and analysis.

Target audience

IT professionals, Forensics and Incident Handling Specialists, Security Consultants, Enterprise Administrators, Infrastructure Architects, Security Professionals, Systems Engineers, Network Administrators and other people responsible for implementing network and perimeter security.

Materials

Author's unique tools, virtual lab environment, hands-on exercises, presentation slides with notes.

Agenda

Module 1: Windows Internals

1. Introduction to Windows Internals
2. Fooling Windows Task Manager
3. Processes and threads
4. PID and TID
5. Information gathering from the running operating system
6. Obtaining Volatile Data
7. A deep dive to Autoruns
8. Effective permissions auditing
9. PowerShell get NTFS permissions
10. Obtaining permissions information with AccessChck
11. Unnecessary and malicious services
12. Detecting unnecessary services with PowerShell

Module 2: Handling Malicious Code Incidents

1. Count of Malware Samples
2. Virus, Worms, Trojans and Spywares
3. Incident Handling Preparation
4. Incident Prevention
5. Detection of Malicious Code
6. Containment Strategy
7. Evidence Gathering and Handling
8. Eradication and Recovery

Module 3: Network Forensics and Monitoring

1. Types and approaches to network monitoring
2. Network evidence acquisition
3. Network protocols and Logs
4. LAB: Detecting Data Thievery
5. LAB: Detecting WebShells
6. Gathering data from network security appliances
7. Detecting intrusion patterns and attack indicators
8. Data correlation
9. Hunting malware in network traffic
10. Encoding and Encryption
11. Denial-of-Service Incidents
12. Distributed Denial-of-Service Attack
13. Detecting DoS Attack
14. Incident Handling Preparation for DoS
15. DoS Response and Preventing Strategies

Module 4: Memory: Dumping and Analysis

1. Introduction to memory dumping and analysis
2. Creating memory dump - Belkasoft RAM Capturer and DumpIt
3. Utilizing Volatility to analyze Windows memory image
4. Analyzing Stuxnet memory dump with Volatility
5. Automatic memory analysis with Volatile

Module 5: Memory: Indicators of compromise

1. Yara rules language
2. Malware detonation
3. Introduction to reverse engineering

Module 6: Disk: Storage Acquisition and Analysis

1. Introduction to storage acquisition and analysis
2. Drive Acquisition
3. Mounting Forensic Disk Images
4. Virtual disk images
5. Signature vs. file carving
6. Introduction to NTFS File System
7. Windows File System Analysis
8. Autopsy with other filesystems

9. External device usage data extraction (USB usage etc.)
10. Reviving the account usage
11. Extracting data relate with the recent use of application, file etc.
12. Recovering data after deleting partitions
13. Extracting delete file and file related information
14. Extracting data from file artifacts like $STANDARD_INFORMATION etc.
15. Password recovery
16. Extracting Windows Indexing Service data
17. Deep-dive into Automatic Destinations
18. Detailed analysis of Windows Prefetch
19. Extracting information about program execution (UserAssist, RecentApps, Shimcache, appcompatcache etc.)
20. Extracting information about browser usage (web browsing history, cache, cookies etc.)
21. Communicator apps data extraction
22. Extracting information about network activity
23. Building timelines

Module 7: Reporting – Digital Evidence

This module covers the restrictions and important details about digital evidence gathering. Moreover, a proper structure of digital evidence report will be introduced.