IT251:
Reverse-Engineering Malware: Tools & Techniques

Tel No:+97126654546 | Fax No:+97126654182 | Email: training@cmc-me.com | www.cmc-me.com

Training Description:

The comprehensive and advanced training course designed to equip cybersecurity professionals with the practical skills required to analyze, dissect and understand malicious software. As modern threat actors deploy increasingly sophisticated malware—including ransomware, fileless attacks, packed binaries and advanced persistent threats—security teams must develop strong reverse-engineering capabilities to detect, contain and mitigate threats effectively.

This intensive training course focuses on static and dynamic malware analysis, reverse-engineering methodologies and threat attribution techniques. Participants will work with industry-standard analysis tools in controlled environments to examine real-world malware samples, identify functionality, extract indicators of compromise (IOCs) and understand attacker behavior. Emphasis is placed on structured analysis processes, safe handling procedures and technical reporting for incident response and digital forensics.

By the end of the training course, participants will be able to safely analyze suspicious binaries, unpack and obfuscate malicious code, understand persistence and evasion mechanisms and produce actionable intelligence to strengthen organizational cybersecurity defenses.

Training Objectives:

By the end of the training, participants will be able to:

- ✓ Understand malware architecture, behavior and attack lifecycles
- ✓ Perform safe malware handling and lab environment configuration
- ✓ Conduct static analysis using disassemblers and reverse-engineering tools
- ✓ Perform dynamic analysis using sandboxing and debugging techniques
- ✓ Identify packing, obfuscation and anti-analysis techniques
- ✓ Extract indicators of compromise (IOCs) and threat intelligence artifacts
- ✓ Analyze persistence, privilege escalation and lateral movement techniques
- ✓ Reverse-engineer network communications and command-and-control (C2) behavior
- ✓ Document findings in structured forensic and incident response reports

Training Designed for:

This training course is designed for cybersecurity analysts, incident responders, digital forensic investigators and threat intelligence professionals seeking advanced malware analysis skills. It is also suitable for SOC analysts, penetration testers, vulnerability researchers and security engineers responsible for detecting and mitigating advanced threats. Participants should have foundational knowledge of operating systems, networking concepts and basic programming (preferably in C, C++ or Python) to fully benefit from this course.

Training Requirement:

"Hands on practical sessions, equipment and software will be applied during the course if required and as per the client's request."

Contents can be adapted to your specific wishes. It is therefore possible to focus on specific modules of the training course as per client's learning needs and objectives. Further, it should be forwarded to us a month prior to the course dates.

Training Program:

DAY ONE:

MALWARE FUNDAMENTALS AND SAFE ANALYSIS ENVIRONMENTS

- ❖ Foundations of Malware Reverse Engineering
  - Malware types and attack methodologies (trojans, ransomware, rootkits, worms)
  - Malware kill chain and attacker objectives
  - Setting up a secure malware analysis lab (VMs, isolation techniques)
  - Introduction to static vs. dynamic analysis
  - File format fundamentals (PE structure and headers)
  - Hashing, signatures and basic triage techniques
  - **Workshop:** Configuring a secure malware analysis environment

DAY TWO:

STATIC ANALYSIS AND CODE INSPECTION

- ❖ Understanding Malware Without Execution
  - Binary structure and executable analysis
  - Strings analysis and metadata extraction
  - Disassembly fundamentals and assembly language basics
  - Using disassemblers and reverse-engineering frameworks
  - Identifying malicious functions and API calls
  - Detecting obfuscation and packing techniques
  - **Case Study:** Static analysis of real malware samples

DAY THREE:

DYNAMIC ANALYSIS AND DEBUGGING TECHNIQUES

- ❖ Observing Malware in Action
  - Sandbox environments and behavioral monitoring
  - Process monitoring and registry tracking
  - Network traffic capture and analysis
  - Debugging basics and breakpoint analysis
  - Memory analysis fundamentals
  - Identifying persistence mechanisms
  - Workshop: Behavioral analysis and debugging exercises

DAY FOUR:

ADVANCED REVERSE ENGINEERING TECHNIQUES

- ❖ Deobfuscation, Unpacking and Anti-Analysis Bypass
  - Manual and automated unpacking techniques
  - Analyzing obfuscated and encrypted payloads
  - Anti-debugging and anti-VM detection methods
  - Bypassing evasion mechanisms
  - Reverse-engineering command-and-control (C2) communications
  - Extracting embedded payloads
  - **Case Study:** Advanced malware reverse-engineering challenge

DAY FIVE:

THREAT INTELLIGENCE, REPORTING AND INCIDENT RESPONSE INTEGRATION

- From Analysis to Actionable Intelligence
  - Extracting and validating indicators of compromise (IOCs)
  - Mapping findings to MITRE ATT&CK techniques
  - Attribution basics and threat actor profiling
  - Writing structured malware analysis reports
  - Integrating findings into incident response workflows
  - Improving detection signatures and defensive controls
  - **Workshop:** Comprehensive malware analysis case study
- Course Conclusion
- POST-ASSESSMENT and EVALUATION

Training Methodology:

This interactive training course includes the following training methodologies as a percentage of the total tuition hours:

- 30% Lectures, Concepts, Role Play
- 70% Workshops & Work Presentations, Techniques, Based on Case Studies & Practical Exercises, Gamification, Software & General Discussions
- Pre and Post Test

Training Certificate(s):

CMCT Internationally recognized certificate(s) will be issued to each participant who completed the course.

Training Fees:

TBA as per the course location - This rate includes participant's manual, hand-outs, buffet lunch, coffee/tea on arrival, morning & afternoon of each day.

Note: The 5% VAT (Value Added Tax), will be effective starting 01st of January 2018 as per the new regulation from the UAE Government. The VAT applies for all quotation both for local and abroad.

Training Timings:

Daily Timings:

07:45 - 08:00	Morning Coffee / Tea
08:00 - 10:00	First Session
10:00 - 10:20	Recess (Coffee/Tea/Snacks)
10:20 - 12:20	Second Session
12:20 - 13:00	Recess (Prayer Break & Lunch)
13:00 - 14:00	Last Session

For training registrations or in-house enquiries, please contact:
Aisha Relativo - Training & Career Development Manager
aisha@cmc-me.com / training@cmc-me.com
Tel.: +971 2 665 3945 or +971 2 643 6653 | Mob.: +971 52 2954615