Advanced Malware Analysis and Reverse Engineering Training Course



19 - 23 Oct 2026

Boston

7500 € (Per Person)

Ref: #CYB4203_87844

Course Introduction / Overview:

This intensive training course provides a comprehensive exploration of modern malware analysis and reverse engineering techniques. In an era of escalating cyber threats, understanding the inner workings of malicious software is no longer optional but a critical necessity for cybersecurity professionals. This program is designed to move beyond theoretical concepts, immersing participants in hands-on labs and real-world scenarios to build practical, job-ready skills. Drawing upon foundational principles outlined by experts like Michael Sikorski in his seminal work, "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software," the curriculum covers the full spectrum of analysis. Participants will learn to safely dissect malware, from basic static and dynamic analysis to advanced code deobfuscation and memory forensics. BIG BEN Training Center has developed this course to empower security teams to effectively respond to incidents, develop robust detection signatures, and gain deep insights into attacker methodologies. By mastering these advanced skills, attendees will be equipped to dismantle sophisticated threats, including ransomware, spyware, and advanced persistent threats (APTs), thereby significantly enhancing their organization's defensive posture and threat intelligence capabilities.

Target Audience / This training course is suitable for:

- Cybersecurity Analysts.
- Incident Responders.
- Threat Intelligence Analysts.
- Security Researchers.
- Digital Forensics Investigators.
- Security Operations Center (SOC) Engineers.
- Penetration Testers.
- IT Professionals with a focus on security.
- Software Developers interested in security.
- Malware Analysts.

Target Sectors and Industries:

- Financial Services and Banking.
- Information Technology and Software Development.
- Telecommunications.
- Healthcare and Pharmaceuticals.
- Government, Defense, and Intelligence Agencies.
- Energy and Critical Infrastructure.
- Consulting and Professional Services.
- E-commerce and Retail.

Target Organizations Departments:

- Cybersecurity and Information Security.
- Security Operations Center (SOC).
- Incident Response and Management.
- Threat Intelligence and Research.
- Digital Forensics and Investigations.
- Information Technology Operations.
- Research and Development (R&D).
- Risk and Compliance.

Course Offerings:

By the end of this course, the participants will have able to:

- Establish a secure and isolated laboratory environment for malware analysis.
- Perform comprehensive static analysis on malicious binaries without execution.
- Conduct in-depth dynamic analysis to observe malware behavior in a controlled setting.
- Utilize disassemblers and debuggers to reverse engineer complex code.
- Analyze obfuscated and packed malware to uncover its true functionality.
- Perform memory forensics to identify malicious artifacts in system RAM.
- Identify and bypass common anti-analysis and anti-debugging techniques.
- Analyze network traffic to understand malware command and control (C2) communications.
- Develop custom signatures and indicators of compromise (IOCs) for threat detection.
- Create detailed technical reports on malware functionality and attribution.

Course Methodology:

The training methodology at BIG BEN Training Center is centered on immersive, hands-on learning to ensure participants can immediately apply their new skills. This course eschews a purely lecture-based format in favor of a highly interactive and practical approach. Over 60% of the course is dedicated to hands-on labs where participants will work with real, albeit neutralized, malware samples in a secure virtual environment. The learning process is reinforced through a combination of expert-led instruction, live demonstrations, and collaborative group exercises that simulate real-world incident response scenarios. We emphasize a problem-solving mindset, encouraging participants to think critically and creatively as they dissect complex threats. Case studies of recent, high-profile cyberattacks are integrated throughout the curriculum to provide context and highlight the real-world relevance of the techniques being taught. Continuous feedback and personalized guidance from our experienced instructors ensure that every participant, regardless of their initial skill level, can grasp the advanced concepts and master the practical tools. This experiential learning environment is designed to build not just knowledge, but true competence and confidence in malware analysis and reverse engineering.

Course Agenda (Course Units):

Unit One: Foundations of Malware Analysis

- Introduction to Malware and Threat Landscape.
- Types of Malicious Software (Viruses, Worms, Trojans, Ransomware).
- Legal and Ethical Considerations in Malware Analysis.
- Setting Up a Secure and Isolated Analysis Laboratory.
- Introduction to Static Analysis Techniques.
- File Hashing, String Extraction, and Header Analysis.
- Using Basic Static Analysis Tools and Utilities.

Unit Two: Advanced Static Analysis and Code Reversing

- Fundamentals of x86 and x64 Assembly Language.
- Introduction to Disassemblers like IDA Pro and Ghidra.
- Navigating and Understanding Disassembled Code.
- Identifying Key Functions, Loops, and Control Structures.
- Analyzing Windows API Calls and System Interactions.
- Recognizing Common C/C++ Code Constructs in Assembly.
- Decompilation Techniques and Limitations.

Unit Three: Dynamic Analysis and Behavioral Monitoring

- Principles of Dynamic Analysis and Sandboxing.
- Using Debuggers like x64dbg and WinDbg.
- Setting Breakpoints and Stepping Through Code Execution.
- Monitoring System Changes (Registry, Filesystem, Processes).
- Analyzing Malware Network Communications with Wireshark.
- Intercepting and Decrypting C2 Traffic.
- Automated vs. Manual Dynamic Analysis.

Unit Four: Deobfuscation and Anti-Analysis Techniques

- Understanding Code Obfuscation and Packing.
- Manual and Automated Unpacking Techniques.
- Identifying and Defeating Anti-Debugging Tricks.
- Bypassing Anti-VM and Anti-Sandbox Detection.
- Analyzing Encrypted Data and Custom Encoding Schemes.
- Deobfuscating Malicious Scripts (PowerShell, VBScript).
- Introduction to Memory Forensics for Malware Analysis.

Unit Five: Advanced Topics and Capstone Project

- Analyzing Ransomware and Encryption Routines.
- Dissecting Document-Based Malware and Shellcode.
- Introduction to Mobile Malware Analysis (Android).
- Developing Custom YARA Rules and Detection Signatures.
- Threat Intelligence and Attributing Malware to Threat Actors.
- Comprehensive Malware Analysis Reporting.
- Capstone Project: Full Analysis of a Modern Malware Sample.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

As malware increasingly leverages AI for evasion and adaptation, how must reverse engineering techniques evolve to stay ahead of these autonomous threats?

What unique qualities does this course offer compared to other courses?

This course distinguishes itself by focusing on developing the analytical mindset of a reverse engineer, rather than merely teaching tool proficiency. While participants will gain mastery over essential tools like IDA Pro, Ghidra, and x64dbg, the core emphasis is on the strategic process of inquiry and logical deduction. We move beyond the "what" to the "why," training participants to think like an adversary to understand the intent behind every line of code. The curriculum is built around a series of hands-on labs using contemporary, real-world malware samples, ensuring the skills learned are immediately applicable to current threats. Unlike courses that rely on outdated examples, our content is continuously updated to reflect the evolving tactics, techniques, and procedures (TTPs) of modern threat actors. Furthermore, the course integrates threat intelligence concepts, teaching participants not just how to analyze a binary, but how to extract actionable intelligence, generate high-fidelity indicators of compromise (IOCs), and produce comprehensive reports that inform an organization's broader security strategy. This holistic, intelligence-driven approach transforms participants from tool operators into genuine threat analysts.