Network Forensics and Real-Time Intrusion Detection Training Course



26 - 30 Oct 2026

Kuala Lumpur

5200 € (Per Person)

Ref: #NO5422_119245

Course Introduction / Overview:

In today's hyper-connected digital landscape, the ability to dissect network traffic and detect intrusions is no longer a specialized skill but a fundamental requirement for robust cybersecurity. This course provides a comprehensive exploration of network forensics and intrusion detection, transforming participants from passive observers to proactive defenders. We delve into the methodologies required to capture, analyze, and interpret network evidence, enabling the reconstruction of security incidents and the identification of malicious actors. Drawing upon the foundational principles articulated by experts like Richard Bejtlich in his seminal work, "The Tao of Network Security Monitoring: Beyond Intrusion Detection," this program emphasizes a proactive, evidence-based approach. Participants will learn to think like an attacker to better anticipate and counter threats. At BIG BEN Training Center, we have designed this training to be intensely practical, moving beyond theoretical concepts to provide hands-on experience with the tools and techniques used by elite security professionals. This course equips you with the critical skills to safeguard digital assets, ensure regulatory compliance, and effectively respond to the ever-evolving threats targeting modern networks.

Target Audience / This training course is suitable for:

- Cybersecurity Analysts.
- Incident Responders.
- Network Administrators and Engineers.
- IT Security Managers.
- Digital Forensic Investigators.
- Security Operations Center (SOC) Personnel.
- Law Enforcement and Government Agency Investigators.
- Information Security Consultants.
- System Administrators with security responsibilities.
- IT Auditors.

Target Sectors and Industries:

- Financial Services and Banking.
- Healthcare and Medical Institutions.
- Government and Public Sector Agencies.
- Telecommunications and Internet Service Providers.
- Technology and Software Development.
- Energy and Utilities.
- Retail and E-commerce.
- Defense and Aerospace.
- Consulting and Professional Services.
- Education and Research Institutions.

Target Organizations Departments:

- Information Technology (IT).
- Cybersecurity and Information Security.
- Security Operations Center (SOC).
- Network Operations Center (NOC).
- Incident Response Teams.
- Digital Forensics Units.
- Internal Audit and Compliance.
- Risk Management.
- Legal and Corporate Security.
- Research and Development.

Course Offerings:

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

- Analyze network protocols to identify anomalies and malicious traffic.
- Utilize packet capture tools like Wireshark for in-depth traffic analysis.
- Deploy and configure Intrusion Detection Systems (IDS) like Snort.
- Investigate security alerts and differentiate between true and false positives.
- Conduct comprehensive network forensic investigations from evidence acquisition to reporting.
- Reconstruct digital incidents and create a timeline of events.
- Identify indicators of compromise (IOCs) within network data.
- Understand techniques used by attackers to evade detection.
- Preserve network evidence while maintaining the chain of custody.
- Develop strategies for proactive network security monitoring and threat hunting.

Course Methodology:

The training methodology at BIG BEN Training Center is designed for maximum knowledge retention and practical application. This course adopts a blended learning approach that combines expert-led instruction with intensive, hands-on lab exercises. We believe that complex skills like network forensics are best learned by doing. Therefore, a significant portion of the course is dedicated to immersive simulations where participants work with real-world datasets and network traffic captures. These practical sessions allow for the application of learned concepts in a controlled, realistic environment. The curriculum is enriched with case studies of prominent security breaches, enabling participants to analyze the attack lifecycle and forensic response. Interactive group discussions and collaborative problem-solving activities are integral to the learning process, fostering a dynamic environment where participants can share insights and experiences. Our instructors provide continuous feedback and personalized guidance, ensuring that every participant masters the core competencies and can confidently apply these skills in their professional roles immediately upon completion of the course.

Course Agenda (Course Units):

Unit One: Foundations of Network Forensics and Security Monitoring

- Introduction to Network Forensics and Incident Response.
- The TCP/IP Protocol Suite Revisited for Forensics.
- Network Architecture and Evidence Sources.
- Legal and Ethical Considerations in Network Investigations.
- Setting Up a Secure Forensic Analysis Environment.
- Fundamentals of Intrusion Detection and Prevention Systems (IDS/IPS).
- The Network Security Monitoring (NSM) Paradigm.

Unit Two: Network Traffic Capture and Analysis

- Mastering Wireshark for Packet Analysis.
- Advanced Filtering and Display Techniques.
- Network Data Acquisition Methods (Taps, SPAN Ports).
- Command-Line Packet Analysis with tcpdump.
- Introduction to Network Flow Analysis and Tools.
- Reconstructing Data Streams and Extracting Files.
- Identifying and Analyzing Common Network Protocols (HTTP, DNS, SMTP).

Unit Three: Intrusion Detection Systems in Practice

- Principles of Signature-Based and Anomaly-Based Detection.
- Deploying and Configuring Snort as a Network IDS.
- Writing and Managing Custom Snort Rules.
- Analyzing IDS Alerts and Managing False Positives.
- Understanding Attacker Evasion Techniques.
- Bypassing Firewalls and IDS.
- Integrating IDS with Security Information and Event Management (SIEM) Systems.

Unit Four: Advanced Forensic Techniques

- Investigating Malware and Ransomware Network Activity.
- Analyzing Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks.
- Wireless Network Forensics (802.11).
- Forensic Analysis of Encrypted Traffic (TLS/SSL).
- Log Correlation and Analysis from Firewalls, Proxies, and Servers.
- Identifying Data Exfiltration and Lateral Movement.
- Advanced Persistent Threat (APT) Detection Strategies.

Unit Five: Incident Response, Reporting, and Case Studies

- Integrating Network Forensics into the Incident Response Lifecycle.
- Evidence Handling and Maintaining the Chain of Custody.
- Creating a Detailed Timeline of a Security Breach.
- Developing a Comprehensive Forensic Report.
- Presenting Technical Findings to Non-Technical Stakeholders.
- Capstone Exercise: A Complete Network Forensic Investigation.
- Review of Real-World Case Studies and Lessons Learned.

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 network encryption becomes ubiquitous, how must the principles of network forensics evolve to maintain visibility into malicious activities?

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

This course distinguishes itself by focusing on the cognitive processes and analytical mindset essential for effective network investigation, rather than merely providing a superficial tour of software tools. While participants will gain proficiency in industry-standard applications, our primary emphasis is on developing the critical thinking skills needed to interpret complex network data and understand the narrative of an attack. We move beyond basic packet analysis to explore the strategic integration of network evidence within the broader incident response framework. The curriculum is built upon real-world scenarios and case studies, challenging participants to solve problems that mirror the complexities they will face in their professional roles. Unlike other programs that may isolate forensics from security operations, this course bridges that gap, teaching how to use forensic findings to proactively hunt for threats and strengthen network defenses. The hands-on labs are designed not just to teach a function, but to build analytical muscle, ensuring that graduates can adapt to new tools and evolving threat landscapes with confidence and expertise.