"Comprehensive Network Forensics and Investigation Certification Course"

GIAC Network Forensic Analyst (GNFA) Training Curriculum

Course Introduction:

The GIAC Network Forensic Analyst (GNFA) certification is designed to validate the skills necessary to conduct network forensic investigations. This course provides a detailed understanding of network forensic principles, techniques, and tools used to identify, collect, analyze, and report on network-based evidence. Participants will develop the expertise to track network intrusions, uncover malicious activity, and support legal proceedings with digital evidence.

Module 1: Introduction to Network Forensics

• Overview of Network Forensics: Explore the fundamental concepts and importance of network forensics in cybersecurity.

• Understanding Network Traffic and Protocols: Gain insights into how network protocols function and their relevance in forensic investigations.

• Legal and Ethical Considerations: Learn about the legal implications and ethical responsibilities involved in conducting network forensic analysis.

Module 2: Network Evidence Acquisition

• Tools and Techniques for Data Collection: Review the essential tools and methodologies for capturing network data effectively.

• Packet Capture and Analysis: Understand the process of capturing and analyzing network packets for forensic purposes.

• Forensic Data Integrity and Chain of Custody: Learn how to maintain data integrity and document the chain of custody for forensic evidence.

Module 3: Network Traffic Analysis

• Analyzing Network Traffic Patterns: Identify and interpret patterns in network traffic to detect anomalies and potential security threats.

• Intrusion Detection and Network Monitoring: Explore techniques for using intrusion detection systems and network monitoring tools to enhance forensic investigations.

• Advanced Protocol Analysis: Delve into complex protocol analysis to identify hidden threats and covert communications.

Module 4: Network Intrusion Investigation

• Identifying and Responding to Network Intrusions: Learn how to detect network intrusions and respond effectively to mitigate damage.

• Malware Traffic Analysis: Examine techniques for identifying and analyzing malicious network traffic associated with malware.

• Attribution and Actor Profiling: Understand methods for profiling threat actors and attributing network attacks to specific entities.

Module 5: Forensic Reporting and Documentation

• Documenting Findings and Writing Reports: Master the skills required to document forensic findings and prepare comprehensive reports.

• Presenting Evidence in Legal Proceedings: Explore best practices for presenting network forensic evidence in court or other legal settings.

• Case Studies and Practical Exercises: Engage in hands-on exercises and real-world case studies to reinforce learning and apply concepts.

Module 6: Advanced Network Forensic Techniques

• Network Artifact Recovery: Learn techniques for recovering artifacts from network devices and logs for forensic analysis.

• Encrypted Traffic Analysis: Develop skills to analyze encrypted network traffic and identify potential security issues.

• Emerging Trends in Network Forensics: Stay updated with the latest trends and emerging technologies in network forensic analysis.

Module 7: Specialized Network Forensics

• Cloud and Virtual Network Forensics: Explore the unique challenges and strategies for conducting forensic investigations in cloud and virtualized environments.

• Wireless Network Forensics: Gain expertise in analyzing wireless network traffic and identifying unauthorized access points.

• Internet of Things (IoT) Forensics: Understand the forensic implications of IoT devices and how to analyze their network activity.

Module 8: Capstone Project and Certification Preparation

• Capstone Project: Apply the knowledge and skills acquired throughout the course in a comprehensive capstone project simulating a real-world forensic investigation.

• Certification Exam Preparation: Review key concepts and practice exam questions to prepare for the GNFA certification exam.

• Continuing Education and Professional Development: Explore opportunities for further learning and professional growth in the field of network forensics.

This curriculum is designed to equip participants with the necessary skills and knowledge to excel as a GIAC Network Forensic Analyst, preparing them for real-world challenges and the GNFA certification exam.