Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

GIAC Certified Intrusion Analyst

Course Description & Overview

SecureNinja's GIAC* Certified Intrusion Analyst (GCIA) certification training equips cybersecurity professionals with the skills necessary to monitor, detect, and analyze network traffic for signs of unauthorized activity. This hands-on course focuses on deep packet analysis, network security monitoring, and intrusion detection using open-source and commercial tools.

The GCIA certification, developed by GIAC (Global Information Assurance Certification), is highly regarded by blue team professionals and SOC analysts worldwide. Participants will learn how to interpret traffic patterns, analyze packet headers and payloads, and respond to suspicious behaviors. The training emphasizes practical detection strategies using tools such as Wireshark, tcpdump, and Snort.

Why Choose GCIA

- Advanced Traffic Analysis: Master techniques for interpreting packet-level network activity.
- Blue Team Focus: Ideal for SOC analysts, incident responders, and defenders responsible for intrusion detection and response.
- Real-World Tools: Training includes extensive use of tcpdump, Wireshark, Snort, and intrusion detection systems.
- Global Recognition: GIAC is trusted across government, military, and private sector cybersecurity operations.

Topics Covered

- Network Fundamentals: Understanding IP, TCP, UDP, ICMP, and other core protocols.
- Packet Capture and Analysis: Using tcpdump and Wireshark to dissect network traffic.
- Intrusion Detection Techniques: Writing and tuning Snort rules for high-fidelity alerting.
- Traffic Pattern Recognition: Identifying anomalies, scans, and attacks through flow analysis.
- Protocol and Application Layer Analysis: Examining DNS, HTTP, SMTP, and custom protocols.
- IDS Management: Deploying and optimizing network-based IDS platforms.

Who is it for

- Security Operations Center (SOC) Analysts: Professionals responsible for monitoring and responding to network threats.
- Intrusion Analysts: Specialists focused on detecting and analyzing unauthorized network activity.
- Network Security Engineers: IT pros managing and securing enterprise network infrastructure.

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

- Incident Responders: Teams investigating and containing active cyber threats.

Who Would Benefit

- Blue Team Members: Anyone tasked with detecting, defending, and responding to cyberattacks.
- Penetration Testers: Red teamers seeking to understand how their actions are detected by defenders.
- IT Professionals: Network administrators aiming to transition into security-focused roles.

Prerequisites

Familiarity with TCP/IP networking, Linux command-line tools, and basic security concepts is recommended. Prior experience with Wireshark or packet analysis is helpful but not required.

Course Outline

1. Module 1: Network Protocol Analysis

    - Interpreting headers and traffic flow in real-time network captures.
    - Using tcpdump and Wireshark for protocol dissection.

2. Module 2: Intrusion Detection Techniques

    - Identifying common attack patterns and network scans.
    - Tuning IDS systems to reduce false positives and improve accuracy.

3. Module 3: Snort and Rule Writing

    - Writing custom Snort signatures.
    - Deploying and managing Snort-based IDS deployments.

4. Module 4: Detection Strategy and Reporting

    - Designing detection strategies for layered defense.
    - Documenting findings and reporting incidents effectively.

Course Length

- 5 Days
- 40 Hours

Exam Details

- OPEN BOOK EXAM
- Number of Questions: Approximately 106
- Question Types: Multiple-choice
- Duration: 4 Hours

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

- Passing Score: 67%

The GIAC Certified Intrusion Analyst (GCIA) certification is ideal for defenders responsible for identifying and analyzing malicious activity in enterprise environments. With its focus on traffic analysis, protocol understanding, and IDS management, GCIA provides the practical skills needed to protect networks from increasingly advanced threats.