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

GCIH - GIAC Certified Incident Handler

Course Description & Overview

SecureNinja's GIAC* Certified Incident Handler (GCIH) certification training equips cybersecurity professionals with the skills required to detect, respond to, and resolve computer security incidents. This hands-on course explores the attacker's tactics, techniques, and procedures (TTPs) while teaching defenders how to effectively manage and respond to intrusions using real-world tools and techniques.

The GCIH certification, developed by the Global Information Assurance Certification (GIAC), is recognized across industries for its rigorous focus on incident handling and active defense. Training topics span reconnaissance, scanning, exploitation, backdoors, rootkits, and denial of service attacks. This course prepares professionals to not only identify signs of compromise but to act quickly and decisively to limit impact and begin remediation.

Why Choose GCIH

- Incident Response Focus: Emphasizes detection, containment, eradication, and recovery from cyber incidents.
- Real-World Tools and Tactics: Includes hands-on labs using Metasploit, Netcat, and other attacker and defender utilities.
- Global Recognition: Highly regarded by employers in government, military, and commercial cybersecurity roles.
- Offensive and Defensive Viewpoints: Covers both attacker techniques and defensive countermeasures.

Topics Covered

- Network Attacks: IP scanning, sniffing, spoofing, and man-in-the-middle tactics.
- Exploit Techniques: Buffer overflows, privilege escalation, and remote code execution.
- Malware and Persistence: Rootkits, backdoors, and command-and-control mechanisms.
- Incident Handling Process: Preparation, detection, containment, eradication, and recovery phases.
- Intrusion Detection Systems: Deploying and analyzing alerts with tools like Snort and Zeek.
- Password Cracking and Bypassing Controls: Tools like John the Ripper and Mimikatz.

Who is it for

- Security Analysts: Professionals monitoring and responding to security alerts.
- Incident Response Team Members: Those responsible for investigating and resolving breaches.
- System and Network Administrators: IT personnel seeking deeper security expertise.
- Penetration Testers: Ethical hackers interested in attacker methodologies and

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

defensive countermeasures.

Who Would Benefit

- Cybersecurity Professionals: Anyone working in a blue team or security operations center (SOC) environment.
- Red Teamers: Offensive security experts looking to improve their understanding of detection and response mechanisms.
- IT Managers: Decision-makers overseeing incident response and enterprise defense operations.

Prerequisites

Basic knowledge of networking, operating systems, and security fundamentals is recommended. Prior exposure to incident response or security analysis is helpful but not required.

Course Outline

Module 1: Introduction to Incident Handling

- Incident handling process overview and frameworks (NIST, SANS).
- Legal considerations and evidence handling.

Module 2: Network Reconnaissance and Scanning

- Footprinting, scanning, enumeration, and vulnerability discovery.
- Tool usage: Nmap, Netcat, Hping.

Module 3: Exploitation and Malware

- Buffer overflows, shellcode, and post-exploitation tools.
- Backdoors, Trojans, and persistence mechanisms.

Module 4: Defending the Enterprise

- Log analysis, intrusion detection systems (IDS), and endpoint protection strategies.
- Incident containment and eradication tactics.

Course Length

- 5 Days
- 40 Hours

Exam Details

Note: Exam vouchers are not included for any of SecureNinja's GIAC training courses.

- OPEN BOOK EXAM
- Number of Questions: 106

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

- Question Types: Multiple-choice
- Duration: 4 Hours
- Passing Score: 70%

The GIAC Certified Incident Handler (GCIH) is an essential certification for professionals working in or entering the field of incident response and security operations. With its deep dive into attacker behaviors and hands-on labs for defensive tactics, GCIH ensures participants are well-prepared to handle real-world cyber threats with confidence and precision.