WhatsApp/ Tel: +1-929-672-1814
Email: info@genai-training.com
www.genai-training.com

Course Title
Digital Forensics & Cyber Security Bootcamp (CEH, CHFI, CompTIA Security+)
Course ID
CYB-SEC-601
Course Level
Intermediate to Advanced
Duration
200 Hours (Bootcamp)
Includes instructor-led training, labs, practical simulations, assignments, certification preparation, and final project assessment.
Delivery Mode
Hybrid / Onsite + Online LMS Support

Course Description
This bootcamp provides practical training in Cyber Security and Digital Forensics aligned with CEH, CHFI, and CompTIA Security+ certifications. Learners will develop skills in ethical hacking, threat detection, vulnerability assessment, incident response, and digital forensic investigation. The program focuses on real-world attack simulations, system security implementation, and forensic analysis using industry tools.

Course Objectives
By the end of the course, learners will understand cybersecurity principles, identify vulnerabilities, perform ethical hacking techniques, analyze digital evidence, and implement security controls. Participants will gain hands-on experience in penetration testing, malware analysis basics, network security, and forensic investigation procedures aligned with global certification standards.

Intended Audience
This course is suitable for IT students, network administrators, system engineers, security enthusiasts, and professionals seeking careers in cyber security, ethical hacking, and digital forensics.

Prerequisites
Basic knowledge of computer systems, networking fundamentals, and operating systems is recommended. A laptop with minimum i5 processor, 8GB RAM (16GB recommended), and virtualization support is required.

Tools & Platforms

Kali Linux, Metasploit, Nmap, Wireshark, Burp Suite, Autopsy, FTK (overview), Linux & Windows environments, VirtualBox/VMware, and LMS portal for resources and assessments.

Course Outline (Modules & Topics)

Module 1: Cyber Security Foundations & Network Security

Introduction to cybersecurity concepts, threat landscape, security models, networking fundamentals, TCP/IP, firewalls, IDS/IPS, and security protocols. Lab includes basic network scanning and security configuration.

Module 2: Ethical Hacking & Penetration Testing (CEH Aligned)

Footprinting, reconnaissance, scanning techniques, vulnerability assessment, system hacking concepts, password attacks, social engineering basics, and web application attacks. Lab includes controlled penetration testing using Kali Linux tools.

Module 3: Network & Web Application Security

Common vulnerabilities (OWASP basics), SQL injection, XSS, session hijacking, secure coding awareness, and mitigation strategies. Lab includes testing and securing web applications.

Module 4: Malware, Cryptography & Security Controls

Malware types, basic analysis concepts, encryption fundamentals, hashing, PKI, authentication mechanisms, and access control models. Lab includes encryption implementation and malware behavior analysis basics.

Module 5: Digital Forensics Investigation (CHFI Aligned)

Digital evidence handling, forensic process, disk imaging, log analysis, chain of custody, forensic reporting, and legal considerations. Lab includes evidence of acquisition and analysis using Autopsy.

Module 6: Incident Response & Security Operations

Incident handling procedures, threat detection, SIEM basics, vulnerability management, risk assessment, and security policies. The lab includes a simulated incident response scenario.

Module 7: CompTIA Security+ Certification Domains

Security architecture, risk management, identity management, cloud security basics, operational security, and exam-focused revision aligned with Security+ domains.

Module 8: Capstone Project & Certification Preparation

Final security assessment project including vulnerability scanning, risk reporting, and forensic analysis case studies. Includes mock certification exams, interview preparation, and final evaluation.

Assessment & Evaluation

Assessment includes quizzes, lab exercises, simulated attack scenarios, forensic case analysis, and final project evaluation to ensure practical competency and certification of readiness.