GTC International Consulting Limited
Riverbank House
1 Putney Bridge Approach
Fulham, London, SW6 3BQ
T: +44(0)2037055710
E:enquiries@thegtcgroup.com
W: www.thegtcgroup.com

EC-Council Certified Ethical Hacker (CCEH)

COURSE OVERVIEW

The Certified Ethical Hacker (CEH) course by EC-Council is a comprehensive program designed to equip cybersecurity professionals with the skills needed to identify, assess, and mitigate vulnerabilities in systems and networks. The course follows a structured, hands-on approach to ethical hacking, covering the latest tools, techniques, and methodologies used by hackers and information security professionals alike. It emphasizes real-world scenarios and practical labs, preparing learners to think like attackers and defend against threats proactively. CEH is globally recognized and is ideal for security officers, auditors, network administrators, and anyone concerned about the integrity of their network infrastructure.

WHO SHOULD ATTEND?

The Certified Ethical Hacking training course will significantly benefit security officers, Cybersecurity auditors, security professionals, Site administrators, Security Analyst and anyone who is concerned about the integrity of the network infrastructure.

COURSE OUTCOMES

Delegates will gain the skills and knowledge to:

- Key issues include plaguing the information security world, ethical hacking, information security controls, laws, and standards.
- Perform footprinting and reconnaissance using the latest footprinting techniques including Footprinting thru Web Services & Social Networking Sites and tools as a critical pre-attack phase required in ethical hacking.
- Network scanning techniques and scanning countermeasures.
- Enumeration techniques and enumeration countermeasures.
- Vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems.
- System hacking methodology, steganography, steganalysis attacks, and covering tracks to discover system and network vulnerabilities.
- Different types of malware threats (Trojan, Virus, worms, etc.), system auditing for malware attacks, malware analysis, and countermeasures.
- Packet sniffing techniques to discover network vulnerabilities and countermeasures to defend sniffing.
- Social engineering techniques and how to identify theft attacks to audit human level vulnerabilities and suggest social engineering countermeasures.
- DoS/DDoS attack techniques and tools to audit a target and DoS/DDoS countermeasures.
- Session hijacking techniques to discover network-level session management, authentication/authorization, cryptographic weaknesses, and countermeasures.
- Firewall, IDS , IPS and honeypot evasion techniques, evasion tools and techniques to audit a network perimeter for weaknesses, and countermeasures.
- Web server attacks and a comprehensive attack methodology to audit vulnerabilities in web server infrastructure, and countermeasures.
- Web application attacks and comprehensive web application hacking methodology to audit vulnerabilities in web applications, and countermeasures.
- SQL injection attack techniques, injection detection tools to detect SQL injection attempts, and countermeasures.
- Wireless encryption, wireless hacking methodology, wireless hacking tools, and Wi-Fi security tools.

- Mobile platform attack vector, android vulnerability exploitations, and mobile security guidelines and tools.
- Threats to IoT and OT platforms and learn how to defend IoT and OT devices securely.
- Cloud computing concepts (Container technology, serverless computing), various threats/attacks, and security techniques and tools.
- Cryptography ciphers, Public Key Infrastructure (PKI), Email encryption, cryptography attacks, and Cryptography Attack Countermeasures.

KEY COURSE HIGHLIGHTS

At the end of the course, you will understand;

- Footprinting and Reconnaissance.
- Scanning Networks.
- Enumeration Techniques.
- Vulnerability Analysis.
- System Hacking.
- Malware Threats.
- Sniffing and Social Engineering.
- Denial-of-Service (DoS) Attacks.
- Session Hijacking.
- Evading IDS, Firewalls, and Honeypots.
- Hacking Web Servers and Applications.
- SQL Injection.
- Hacking Wireless Networks.
- Hacking Mobile Platforms.
- IoT and OT Hacking.
- Cloud Computing Security.
- Cryptography Techniques.
- Hands-on Labs and Real-World Scenarios.
- Preparation for the CEH Certification Exam.

All our courses are dual-certificate courses. At the end of the training, the delegates will receive two certificates.

1. A GTC end-of-course certificate
2. Continuing Professional Development (CPD) Certificate of completion with earned credits awarded