GLOBAL PLUS HORIZON TRAINING CENTER

Certified Ethical Hacker v12 Training Course

Online -

15-09-2024

Certified Ethical Hacker v12 Training Course

Course code: IT263 From: 15-09-2024 Venue: Online - Course Fees: 1450 £

Introduction

In today's interconnected world, cybersecurity threats are more prevalent and sophisticated than ever before. The Certified Ethical Hacker (CEH) v12 Training Course is designed to equip IT professionals with the knowledge and skills needed to identify, counter, and defend against malicious hackers. This comprehensive course dives deep into the methodologies and tools used by hackers, providing participants with a thorough understanding of how to protect their organizations from cyber threats. Through hands-on exercises, real-world scenarios, and expert instruction, participants will learn to think and act like a hacker to better secure their networks and systems.

Course Objectives of Certified Ethical Hacker

By the end of the CEH v12 Training Course, participants will be able to:

- Understand the core concepts of ethical hacking and cybersecurity.
- Conduct thorough reconnaissance and footprinting.
- Perform network scanning and enumeration to identify vulnerabilities.
- Execute system hacking techniques and implement countermeasures.
- Detect and mitigate the impact of trojans, backdoors, viruses, and worms.
- Utilize sniffing tools and techniques while implementing appropriate defenses.
- Employ social engineering tactics and recognize related security breaches.
- Identify and prevent denial of service (DoS) attacks.
- Secure web servers, web applications, and perform SQL injection testing.
- Protect wireless networks and mobile platforms from hacking attempts.
- Evade intrusion detection systems (IDS), firewalls, and honeypots.
- Understand and mitigate buffer overflow vulnerabilities.
- Apply cryptographic techniques to protect data.
- Conduct comprehensive penetration testing to assess security postures.

Course Methodology of Certified Ethical Hacker

- Lectures and Expert Insights: Leading industry experts will share their insights and best practices.

- Case Studies: Analyze real-world talent acquisition challenges and solutions.
- Group Discussions: Engage in meaningful discussions and share experiences with peers.
- Role-Playing and Simulations: Practice recruitment scenarios to enhance skills.
- Hands-on Workshops: Gain practical experience in using recruitment tools and techniques.

Organizational Impact of Certified Ethical Hacker

Implementing the CEH v12 Training Course within your organization will:

- Enhance the overall security posture by empowering employees with advanced cybersecurity skills.
- Reduce the risk of data breaches and cyber attacks through proactive defense measures.
- Foster a culture of security awareness and continuous improvement.
- Improve incident response times and reduce the impact of security incidents.
- Ensure compliance with industry standards and regulations related to cybersecurity.
- Strengthen customer and stakeholder confidence in the organization's commitment to cybersecurity.

Personal Impact of Certified Ethical Hacker

For individual participants, completing the CEH v12 Training Course will:

- Provide a competitive edge in the cybersecurity job market.
- Deepen understanding of ethical hacking principles and practices.
- Enhance problem-solving and analytical skills through practical exercises.
- Increase readiness to handle real-world cyber threats and incidents.
- Support career advancement through recognized certification and expertise.
- Build a strong foundation for further specialized cybersecurity training and certifications.

Who Should Attend

The CEH v12 Training Course is ideal for:

- IT and network security professionals seeking to expand their knowledge in ethical hacking.
- Security officers, auditors, security professionals, site administrators, and anyone concerned about the integrity of network infrastructure.

- IT managers and IT professionals wanting to enhance their security skills.
- Network and system administrators responsible for securing their organizational networks.
- Individuals pursuing a career in ethical hacking and cybersecurity.

Course Outlines

Day 1

Introduction to Ethical Hacking

- Overview of Ethical Hacking Concepts
- Legal and Ethical Aspects
- The Role of an Ethical Hacker
- Introduction to Cybersecurity Frameworks
- Ethical Hacking Methodologies

Day 2

Footprinting and Reconnaissance, Scanning Networks, Enumeration

- Footprinting Techniques and Tools
- Network Scanning Methods
- Types of Scans and Tools
- Enumerating Network Resources
- Countermeasures and Defense Techniques

Day 3

System Hacking, Trojans and Backdoors, Viruses and Worms

- Understanding System Hacking Phases
- Password Cracking and Privilege Escalation
- Introduction to Trojans and Backdoors
- Virus and Worm Types and Propagation

- Detection and Removal Techniques

Day 4

Sniffers, Social Engineering, Denial of Service, Session Hijacking

- Sniffing Techniques and Tools
- Mitigating Sniffing Attacks
- Social Engineering Tactics and Prevention
- Understanding Denial of Service (DoS) Attacks
- Techniques for Session Hijacking and Countermeasures

Day 5

Web Servers, Web Applications, SQL Injection, Wireless Networks, Mobile Platforms, IDS, Firewalls, Honeypots, Buffer Overflow, Cryptography, Penetration Testing

- Securing Web Servers and Applications
- Performing SQL Injection Attacks and Defenses
- Hacking Wireless Networks and Mobile Platforms
- Evading IDS, Firewalls, and Honeypots
- Understanding Buffer Overflows
- Basics of Cryptography and Data Protection
- Conducting Penetration Tests and Reporting