Certified Ethical Hacker v12 PRO

Course code: CEHv12

Certified Ethical Hacker v12 is the latest version of the world's most popular and most prestigious EC-Council training. The CEHv12 training is the best training for advanced administrators and future penetration testers. Students have the unique opportunity to become familiar with the strategies, techniques and tools that are used in the current hacking and penetration testing of business environment. The price of the training includes the globally recognized 312-50-ANSI CEH certification exam, during which students demonstrate mastery of the ethical hacking techniques taught in the course.

Course materials

The price of the training includes official study materials, access to the labs (for 6 months) and voucher for the 312-50-ANSI certification exam (the voucher is valid for one year from its purchase).

Course outline

Module 01: Introduction to Ethical Hacking. Cover the fundamentals of key issues in the information security world, including the basics of ethical hacking, information security controls, relevant laws, and standard procedures.

Module 02: Footprinting and Reconnaissance. Learn how to use the latest techniques and tools to perform foot printing and reconnaissance, a critical pre-attack phase of the ethical hacking process.

Module 03: Scanning Networks. Cover the fundamentals of key issues in the information security world, including the basics of ethical hacking, information security controls, relevant laws, and standard procedures.

Module 04: Enumeration. Learn various enumeration techniques, such as Border Gateway Protocol (BGP) and Network File Sharing (NFS) exploits, plus associated countermeasures.

Module 05: Vulnerability Analysis. Learn how to identify security loopholes in a target organization´s network, communication infrastructure, and end systems.

Module 06: System Hacking. Learn about the various system hacking methodologies—including steganography, steganalysis attacks, and covering tracks—used to discover system and network vulnerabilities.

Module 07: Malware Threats. Get an introduction to the different types of malware, such as Trojans, viruses, and worms, as well as system auditing for malware attacks, malware analysis, and countermeasures.

Module 08: Sniffing. Learn about packet-sniffing techniques and how to use them to discover network vulnerabilities, as well as countermeasures to defend against sniffing attacks.

Module 09: Social Engineering. Learn social engineering concepts and techniques, including how to identify theft attempts, audit human-level vulnerabilities, and suggest social engineering countermeasures.

Module 10: Denial-of-Service. Learn about different Denial-of-Service (DoS) and Distributed DoS (DDoS) attack techniques, as well as the tools used to audit a target and devise DoS and DDoS countermeasures and protections.

Module 11: Session Hijacking. Understand the various session hijacking techniques used to discover network-level session management, authentication, authorization, and cryptographic weaknesses and associated countermeasures.

Module 12: Evading IDS, Firewalls, and Honeypots. Get introduced to firewall, intrusion detection system, and honeypot evasion techniques; the tools used to audit a network perimeter for weaknesses; and countermeasures.

Module 13: Hacking Web Servers. Learn about web server attacks, including a comprehensive attack methodology used to audit vulnerabilities in web server infrastructures and countermeasures.

Module 14: Hacking Web Applications. Learn about web application attacks, including a comprehensive web application

Copyright © 2020 GOPAS, a.s.,
All rights reserved

hacking methodology used to audit vulnerabilities in web applications and countermeasures.

Module 15: SQL Injection. Learn about SQL injection attack techniques, injection detection tools, and countermeasures to detect and defend against SQL injection attempts.

Module 16: Hacking Wireless Networks. Learn about wireless encryption, wireless hacking methodologies and tools, and Wi-Fi security tools.

Module 17: Hacking Mobile Platforms. Learn about mobile platform attack vectors, Android vulnerability exploits, and mobile security guidelines and tools.

Module 18: IoT Hacking. Learn about packet-sniffing techniques and how to use them to discover network vulnerabilities, as well as countermeasures to defend against sniffing attacks.

Module 19: Cloud Computing. Learn different cloud computing concepts, such as container technologies and server less computing, various cloud-based threats and attacks, and cloud security techniques and tools.

Module 20: Cryptography. In the final module, learn about cryptography and ciphers, public-key infrastructure, cryptography attacks, and cryptanalysis tools.

Please note that due to the difficulty of the content and the large number of practical exercises it is not possible to contain the complete syllabus on the course, a part is only intended for self-study.

C|EH Certification

- proctored exam, can be passed in our testing centres in Praha and Brno
- 125 multiple-choices questions
- 4 hours
- EC-Council doesn´t publish pass rates for the exam, typical pass rates globally range from 60%-80%

Copyright © 2020 GOPAS, a.s.,
All rights reserved