kod szkolenia: CEHv12 Pro / ENG AA 5d

Certified Ethical Hacker

As per the latest ongoing trends in IT Industries and to meet the growing demand for new skills and knowledge about cybersecurity, EC-Council has developed the Certified Ethical Hacker training. An unconventional approach to thinking about the companies infrastructure from an intruders perspective is an extremely effective learning mechanism that opens the eyes to many often neglected areas of our work. Although it is an "entry-level" course, CEH contains a lot of material and practical exercises which also touches upon very technically advanced aspects of IT.

Purpose of the training

The training is aimed at network administrators, people responsible for IT infrastructure, website administrators and anyone who plans to increase the IT security level of their organization. Non-IT security specialists will increase awareness of threats and learn about various attack technologies commonly used by hackers. IT security specialists, auditors and so-called security officers will be able to consolidate, systematize or supplement their knowledge.

Benefits of completing the training

The ethical hacker's goal is to identify the weaknesses of their organization and help find an effective method of defence against such attacks on corporate systems. Course participants make controlled intrusions into the "target" system and gain practical skills on how to effectively protect the network. While conventional security measures are essential, it is important to gain the perspective of the cybercriminals who could potentially compromise the systems. During exercises, everyone will get

acquainted with many tools used by security specialists.
Students will learn how to :

- define and characterize the most important techniques of attacks used by hackers
- carry out a reconnaissance about your own company or competition
- scan, test and break system security
- identify and analyse vulnerabilities in the organization
- recognize and prevent authority escalation methods in systems
- create better intrusion detection policies on IDS / IPS devices
- recognize social engineering used by criminals
- create viruses, hack mobile devices, smartphones
- analyse malware
- identify the potential of threats from the "Internet of Things" (IoT) and how to protect against them
- identify challenges for industrial networks and the impact of cybersecurity on OT (Operational Technology) concepts
- characterize the most important elements of container systems (Docker, Kubernetes)
- verify the security of cloud solutions such as AWS
- recognize subtle differences between backdoors, Trojans, and other threats
- ultimately, they will be able to make company employees more aware of information security issues

Examination method

You can take the exam at authorized EC-Council examination centers.
Information about the CEH Examination (ANSI)
Title – Certified Ethical Hacker
Test format: Multiple-choice questions
Number of questions – 125
Duration – 4 hours
Note: by passing the CEH exam in the online formula with the so-called with remote protection, there is an additional fee of USD 100 net. The cost includes hiring an exam supervisor (the so-called proctor), the purchase is made individually on the vendor's website:
https://store.eccouncil.org/product/voucher-upgrade-rps-to-vue/

Expected Listener Preparation

Basic knowledge of Windows and Linux is required. Basic understanding of network essentials, core concepts including server and network components (basic knowledge of TCP/IP communication, services such as DNS/DHCP, the understanding concept of IP addressing). We recommend at least 2 years of

experience in the IT industry.

Training Language

- Training: English
- Materials: English

Training Includes

Czas trwania

5 dni / 40 godzin

Training agenda

1. Introduction to Ethical Hacking
2. Foot Printing and Reconnaissance
3. Scanning Networks
4. Enumeration
5. Vulnerability Analysis
6. System Hacking
7. Malware Threats
8. Sniffing
9. Social Engineering
10. Denial-of-Service
11. Session Hijacking
12. Evading IDS, Firewalls, and Honeypots
13. Hacking Web Servers
14. Hacking Web Applications
15. SQL Injection

16. Hacking Wireless Networks
17. Hacking Mobile Platforms
18. IoT Hacking
19. Cloud Computing
20. Session Hijacking