AI Tactical Skills: Hacking & Defense

Course code: AIEH

This course, structured and designed by Kevin Cardwell (author of EC Council's CPENT) and Wayne Burke (author of CPTS / CPTE Mile2), is built on industry-expected levels of AI / ML competency and practical real-world skills. Cyber2 Labs is the first company to bring this kind of AI skills-building to market, without old-fashioned multiple-choice exams. Our comprehensive 5-day Ethical Hacking class integrates AI and machine learning to enhance your existing tools, techniques, and attack tactics. In this new AI-driven landscape, security professionals are expected to proficiently leverage AI to improve their daily workload.This is an in-depth hands-on practical course, straight to the point, that teaches students how to build, break, fix and modify an array of dedicated hardware devices that hackers frequently use to assist hacking into systems.The course focuses on using mobile hardware / software to exploit targets and network hacking wired, Wi-Fi and RF communication. Each participant will get 6 months access to Premier Private Lab-Range.

Affiliate	Duration	Course price	ITB
Praha	5	59 000 Kč	75
Brno	5	59 000 Kč	75
Bratislava	5	2 380 €	75

The prices are without VAT.

Course terms

Date	Duration	Course price	Type	Course language	Location
07.04.2025	5	2 380 €	Presence	EN	Gopas Bratislava Prezenční
16.06.2025	5	59 000 Kč	Presence	CZ/SK	Gopas Praha Prezenční

The prices are without VAT.

Who is the course for

- Cyber Security engineers / analysts
- EC Council CEH Certified Students
- OSCP Certified Students
- SecOps Certified ProfessionalsCompTIA Certified Professionals
- Network and system administrators
- Drone, &Robotic Engineers &Developers
- Drone Operators
- Digital Forensics Investigators
- Penetration Testers
- Cloud computing personnel
- Cloud project managers
- Operations support looking for career advancement

What we teach you

- Understand the Fundamentals of Cybersecurity and Ethical Hacking
- Grasp the basic concepts, principles, and importance of the ethical considerations in hacking practices
- Identify and Assess Network Vulnerabilities
- Learn AI and Machine Learning to augment attack tools, techniques and tactics
- Learn techniques to discover, analyze, and exploit vulnerabilities in networks and systems.
- Master Various Hacking Tools and Technique
- Gain hands-on experience with popular hacking tools and methodologies
- Conduct Reconnaissance and Information Gathering

- Develop skills in gathering intelligence on targets both passive and active reconnaissance methods
- Perform Network Scanning and Enumeration
- Learn to use tools to scan and enumerate network devices, services, and open ports to map out potential attack vectors
- Exploit System and Network Vulnerabilities
- Practice exploiting identified vulnerabilities to gain unauthorized access and control over systems and networks
- Implement Web Application Hacking Techniques
- Understand common web application vulnerabilities such as SQL injection, XSS, and CSRF, and learn to exploit them effectively
- Develop Skills in Wireless Network Security Testing
- Learn how to test and secure wireless networks against common attacks such as Wi-Fi cracking and man-in-the-middle (MITM) attacks
- Analyze and Defend Against Malware and Exploits
- Study various types of malware, their attack vectors, and defensive strategies to mitigate their impact on systems
- Apply Ethical Hacking in Real-World Scenarios
- Engage in practical exercises and simulations that mimic real-world cyber-attacks, applying ethical hacking techniques to secure systems and improve defenses
- By the end of the course, participants will have a comprehensive understanding of ethical hacking principles, practical skills in various hacking techniques, and the ability to apply these skills to enhance cybersecurity measures in their organizations.

Course outline

Day 1: Introduction to AI in Cybersecurity

Day 2: AI Techniques for Offensive Security

Day 3: AI Techniques for Defensive Security

Day 4: Advanced AI Techniques and Application in Security

Day 5: AI Integration and Future Trends