AIEH

Course code: AIEH

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 advancementWhat 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 outlineDay 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

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.

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk

- 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

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk