

Overview:

The Certified Ethical Hacker (CEH) credential is the most trusted ethical hacking certification and accomplishment recommended by employers globally. It is the most desired information security certification and represents one of the fastest-growing cyber credentials required by critical infrastructure and essential service providers. Since the introduction of CEH in 2003, it is recognized as a standard within the information security community. CEH v11 continues to introduce the latest hacking techniques and the most advanced hacking tools and exploits used by hackers and information security professionals today. The Five Phases of Ethical Hacking and the original core mission of CEH remain valid and relevant today: "To beat a hacker, you need to think like a hacker."

Certified Ethical Hacker (CEH) Version 11 provides an in-depth understanding of ethical hacking phases, various attack vectors, and preventative countermeasures. It will teach you how hackers think and act maliciously so that you will be better positioned to set up your security infrastructure and defend future attacks. Understanding system weaknesses and vulnerabilities help organizations strengthen their system security controls to minimize the risk of an incident.

CEH was built to incorporate a hands-on environment and systematic process across every ethical hacking domain and methodology, giving you the opportunity to work towards proving the required knowledge and skills needed to perform the job of an ethical hacker. You will be exposed to an entirely different posture towards the responsibilities and measures required to be secure.

Certified ethical hacker (CEH) version 11

In its 11th version, CEH continues to evolve with the latest operating systems, tools, tactics, exploits, and technologies. Here are some critical updates of CEH v11:

- **Incorporating Parrot Security OS** - When compared to Kali Linux, Parrot Security OS offers better performance on lower-powered laptops and machines while offering an intuitive look and feel with a larger repository of general tools.
- **Re-Mapped to NIST/NICE Framework** - CEH v11 is mapped rigorously to important Specialty Areas under the NIST/NICE framework's Protect and Defend (PR) job role category overlapping with other job roles, including Analyze (AN) and Securely Provision (SP).
- **Enhanced Cloud Security, IoT, and OT Modules** - CEH v11 covers updated Cloud and IoT modules to incorporate CSP's Container Technologies (e.g., Docker, Kubernetes), Cloud Computing threats, and a number of IoT hacking tools (e.g. Shikra, Bus Pirate, Facedancer21, and more). This is critical as the world moves towards broader and deeper cloud adoptions.
- **Modern Malware Analysis** - CEH v11 now includes the latest malware analysis tactics for ransomware, banking
- **Covering the Latest Threats - Fileless Malware** - As the security community observed a rise in fileless attacks, it began to raise concerns about fileless malware attacks. As fileless malware is a relatively new form of malware attack, organizations find it difficult to detect with endpoint security solutions. With the CEH v11, you can now learn various fileless malware techniques with associated defensive strategies, as the course focuses on the taxonomy of fileless malware threats, fileless malware obfuscation techniques to bypass antivirus, launching fileless malware through script-based injection, launching fileless malware through phishing, and more.
- **New Lab Designs and Operating Systems** - This latest iteration of CEH v11 includes new operating systems, including Windows Server 2019, Windows Server 2016, and Windows 10 configured with Domain Controller, firewalls, and vulnerable web applications for practicing and improving hacking skills.
- **Increased Lab Time and Hands-on** - Focus More than 50% of the CEH v11 course is dedicated to practical skills in live ranges via EC-Council labs. EC-Council leads in this aspect of the industry.
- **Industry's Most Comprehensive Tools Library** - The CEH v11 course includes a library of the latest tools required by security practitioners and pen testers across the world.

Certification

- The Certified Ethical Hacker exam 312-50 may be taken on the last day of the training (optional). Students need to pass the online exam to receive CEH certification.

Audience:

- Information Security Analyst / Administrator
- Information Assurance (IA) Security Officer
- Information Security Manager / Specialist
- Information Systems Security Engineer / Manager
- Information Security Professionals / Officers
- Information Security / IT Auditors
- Risk / Threat/Vulnerability Analyst
- System Administrators
- Network Administrators and Engineers

Course objectives:

- Key issues include plaguing the information security world, ethical hacking, information security controls, laws, and standards.
- Perform footprinting and reconnaissance using the latest footprinting techniques and tools as a critical pre-attack phase required in ethical hacking.
- Network scanning techniques and scanning countermeasures.
- Enumeration techniques and enumeration countermeasures.
- Vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems.
- System hacking methodology, steganography, steganalysis attacks, and covering tracks to discover system and network vulnerabilities.
- Different types of malware (Trojan, Virus, worms, etc.), system auditing for malware attacks, malware analysis, and countermeasures.
- Packet sniffing techniques to discover network vulnerabilities and countermeasures to defend sniffing.
- Social engineering techniques and how to identify theft attacks to audit human-level vulnerabilities and suggest social engineering countermeasures.
- DoS/DDoS attack techniques and tools to audit a target and DoS/DDoS countermeasures.
- Session hijacking techniques to discover network-level session management, authentication/authorization, cryptographic weaknesses, and countermeasures.
- Web server attacks and a comprehensive attack methodology to audit vulnerabilities in web server infrastructure, and countermeasures.
- Web application attacks and comprehensive web application hacking methodology to audit vulnerabilities in web applications, and countermeasures.
- SQL injection attack techniques, injection detection tools to detect SQL injection attempts, and countermeasures.
- Wireless encryption, wireless hacking methodology, wireless hacking tools, and Wi-Fi security tools.
- Mobile platform attack vector, android vulnerability exploitations, and mobile security guidelines and tools.
- Firewall, IDS and honeypot evasion techniques, evasion tools and techniques to audit a network perimeter for weaknesses, and countermeasures.
- Cloud computing concepts (Container technology, serverless computing), various threats/attacks, and security techniques and tools.
- Penetration testing, security audit, vulnerability assessment, and penetration testing roadmap.
- Threats to IoT and OT platforms and learn how to defend IoT and OT devices securely.
- Cryptography ciphers, Public Key Infrastructure (PKI), cryptography attacks, and cryptanalysis tools.

Course Outline:

- Module 01: Introduction to Ethical Hacking
- Module 02: Footprinting and Reconnaissance
- Module 03: Scanning Networks
- Module 04: Enumeration
- Module 05: Vulnerability Analysis
- Module 06: System Hacking
- Module 07: Malware Threats
- Module 08: Sniffing
- Module 09: Social Engineering
- Module 10: Denial-of-Service
- Module 11: Session Hijacking
- Module 12: Evading IDS, Firewalls, and Honeypots
- Module 13: Hacking Web Servers
- Module 14: Hacking Web Applications
- Module 15: SQL Injection
- Module 16: Hacking Wireless Networks
- Module 17: Hacking Mobile Platforms
- Module 18: IoT Hacking
- Module 19: Cloud Computing
- Module 20: Cryptography

วิทยากร: อ.เอกฤทธิ์ ธรรมสกลิต



- MASTER OF BUSINESS ADMINISTRATION (EXECUTIVE) DEGREE
SASIN GRADUATE INSTITUTE OF BUSINESS ADMINISTRATION OF
CHULALONGKORN UNIVERSITY
- MASTER OF SCIENCE, MAJOR IN INFORMATION
Technology Faculty of Information Technology
KING'S MONGKUT INSTITUTE OF TECHNOLOGY LADKRABANG
- BACHELOR OF SCIENCE
KING'S MONGKUT INSTITUTE OF TECHNOLOGY NORTH BANGKOK
- DIPLOMA PROGRAM FOR MANAGEMENT
KELLOGG – NORTHWESTERN UNIVERSITY, UNITED STATE OF AMERICA

Certificate:

- Microsoft Certified professional (MCP)
- Microsoft Certified Systems Administrator (MSCA)
- Microsoft Certified Systems Engineer (MSCE)
- Cisco Certified Network Associate (CCNA)
- Certificate of CompTIA Security+
- Certified Technical training CTT+
- Certified Ethical Hacker
- Certified Hacking Forensic Investigator
- Certified Wireless Network Administrator
- Certified Wireless Security Professional

จำนวนชั่วโมงในการฝึกอบรม: 5 วัน (30 ชั่วโมง)

ช่วงเวลาฝึกอบรม: 9.00 - 16.00 น.

กำหนดการอบรม: ตามตารางปฏิทินอบรมประจำปี <https://www.career4future.com/trainingprogram>

ค่าลงทะเบียนอบรม: ท่านละ 35,000 บาท

<p>หมายเหตุ</p> <ul style="list-style-type: none">• ราคาค่าลงทะเบียนอบรม ไม่รวมภาษีมูลค่าเพิ่ม• เฉพาะหน่วยงานภาครัฐ และองค์กรของรัฐ ที่ไม่ใช่ธุรกิจ และไม่แสวงหากำไร จะได้รับการยกเว้นภาษีมูลค่าเพิ่ม• สถาบันฯ เป็นหน่วยงานราชการ ได้รับการยกเว้นไม่ต้องหักภาษี ณ ที่จ่าย 3%• ค่าใช้จ่ายในการส่งบุคลากรเข้าอบรมทางวิชาชีพของ บริษัทหรือห้างหุ้นส่วนนิติบุคคล สามารถนำไปลดหย่อนภาษีได้ 200%• ข้าราชการมีสิทธิ์เบิกค่าลงทะเบียนได้ตามระเบียบกระทรวงการคลังและเข้าร่วมอบรมสัมมนาโดยไม่ถือเป็นวันลา	<ul style="list-style-type: none">• สถาบันฯ ขอสงวนสิทธิ์ในการเปลี่ยนแปลงเนื้อหาหลักสูตร วิทยากร รูปแบบการอบรม ตามความเหมาะสมและความจำเป็น เพื่อประโยชน์สูงสุดของผู้เข้ารับการอบรม• สถาบันฯ ขอสงวนสิทธิ์ ไม่บันทึกภาพ วิดีโอ หรือบันทึกเสียง ตลอดระยะเวลาการอบรม เนื่องจากเป็นลิขสิทธิ์ร่วมระหว่างวิทยากรกับสถาบันฯ และเพื่อป้องกันการละเมิดข้อมูลส่วนบุคคล ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล• ผู้เข้าอบรมต้องมีเวลาเรียนไม่ต่ำกว่า 80% และทำกิจกรรมทุกหัวข้อของหลักสูตร จึงจะได้รับวุฒิบัตรจากสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.)
<p>หลักสูตรจัดอบรมรูปแบบ Onsite เท่านั้น</p> <ul style="list-style-type: none">• สถาบันฯ มีการจัดเตรียมเครื่องคอมพิวเตอร์ เอกสารการอบรม พร้อมอาหารว่าง และอาหารกลางวันให้กับผู้เข้าอบรม• มอบวุฒิบัตรภายหลังจบการอบรม• สถานที่อบรม ห้องอบรม ณ สถาบันพัฒนาบุคลากรแห่งอนาคต อาคาร สวทช. ชั้น 6 ถนนพระรามที่ 6 แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพฯ 10400	

ติดต่อสอบถามรายละเอียด

สถาบันพัฒนาบุคลากรแห่งอนาคต (Career for the Future Academy)
73/1 อาคารสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) ชั้น 6
ถนนพระรามที่ 6 แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพฯ 10400
โทรศัพท์ 0 2644 8150 ต่อ 81886-7
โทรสาร 0 2644 8150
E-mail: trianing@nstda.or.th
www.career4future.com