Certified Ethical Hacker v12 (CEH)

Duration 5 Days

COURSE DESCRIPTION

The Certified Ethical Hacker has been battle-hardened over the last 20 years, creating hundreds of thousands of Certified Ethical Hackers employed by top companies, militaries, and governments worldwide.

In its 12th version, the Certified Ethical Hacker provides comprehensive training, handson learning labs, practice cyber ranges for engagement, certification assessments, cyber competitions, and opportunities for continuous learning into one comprehensive program curated through our **new learning framework: 1. Learn 2. Certify 3. Engage 4. Compete.**

The C|EH v12 also equips aspiring cybersecurity professionals with the tactics, techniques, and procedures (TTPs) to build ethical hackers who can uncover weaknesses in nearly any type of target system before cybercriminals do.

COURSE OUTLINE

The C|EH® v12 training program includes 20 modules covering various technologies, tactics, and procedures, providing prospective ethical hackers with the core knowledge needed to thrive in cybersecurity. Delivered through a carefully curated training plan that typically spans five days, the 12th version of the C|EH® continues to evolve to keep up with the latest OS, exploits, tools, and techniques. The concepts covered in the training program are split 50/50 between knowledge-based training and hands-on application through our cyber range.Every tactic discussed in training is backed by step-by-step labs conducted in a virtualized environment with live targets, live tools, and vulnerable systems. Through our lab technology, every participant will have comprehensive hands-on practice to learn and apply their knowledge.

- **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:** Foot Printing and Reconnaissance

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 03:** Scanning Networks

Learn different network scanning techniques and countermeasures.

- **Module 04:** Enumeration

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

- **Module 05:** Vulnerability Analysis

Learn how to identify security loopholes in a target organization's network, communication infrastructure, and end systems. Different types of vulnerability assessment and vulnerability assessment tools.

- **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

Learn different types of malware (Trojan, virus, worms, etc.), APT and fileless malware, malware analysis procedure, and malware 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 (IDS), 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 hacking methodology used to audit vulnerabilities in web applications and countermeasures.

- **Module 15:** SQL Injection

Learn about SQL injection attacks, evasion techniques, and SQL injection countermeasures.

- **Module 16:** Hacking Wireless Networks

Understand different types of wireless technologies, including encryption, threats, hacking methodologies, hacking tools, Wi-Fi sedcurity tools, and countermeasures.

- **Module 17:** Hacking Mobile Platforms

Learn Mobile platform attack vector, android and iOS hacking, mobile device management, mobile security guidelines, and security tools.

- **Module 18:** IoT Hacking

Learn different types of IoT and OT attacks, hacking methodology, hacking tools, and countermeasures.

- **Module 19:** Cloud Computing

Learn different cloud computing concepts, such as container technologies and server less computing, various cloud computing threats, attacks, hacking methodology, and cloud security techniques and tools.

- **Module 20:** Cryptography

Learn about encryption algorithms, cryptography tools, Public Key Infrastructure (PKI), email encryption, disk encryption, cryptography attacks, and cryptanalysis tools.

TARGET AUDIENCE

- Mid-Level Information Security Auditor
- Cybersecurity Auditor
- Security Administrator
- IT Security Administrator
- Cyber Defense Analyst
- Vulnerability Assessment Analyst
- Warning Analyst
- Information Security Analyst 1
- Security Analyst L1
- Infosec Security Administrator
- Cybersecurity Analyst level 1, level 2, & level 3
- Network Security Engineer
- SOC Security Analyst
- Security Analyst
- Network Engineer
- Senior Security Consultant
- Information Security Manager
- Senior SOC Analyst
- Solution Architect
- Cybersecurity Consultant

CERTIFICATION

The C|EH® exam is a 4-hour exam with 125 multiple-choice questions. This knowledge-based exam will test your skills in information security threats and attack vectors, attack detection, attack prevention, procedures, methodologies, and more!

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th

Call us today 0-2634-7993-4

177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th