DICC INSTITUTE

Make Your Career In

ETHICAL HACKING

C|EH® v12
Certified Ethical Hacker

REGISTER FOR A FREE DEMO

91-9899127357

WWW.DICC.IN

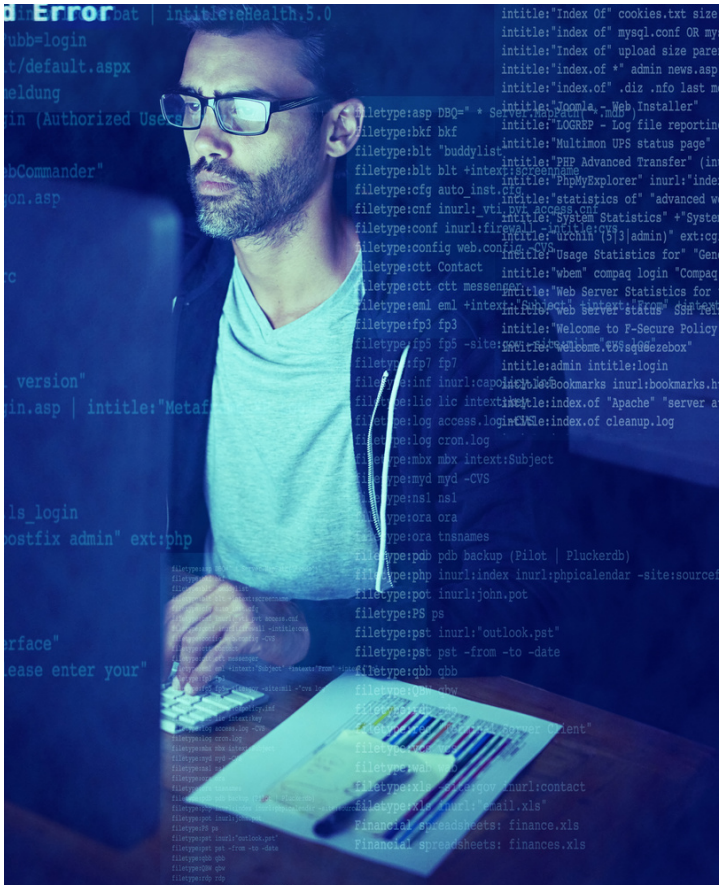
Make your Career in the Most Demand Certification in the world..

Delhi's No. 1 Institute For Cyber Security Course for 15 Years

- **40+ hours Training**
- **Advanced Techniques**
- **CEH V12 Certification**
- **Best & Award-Winning Institute**
- **Live Training - No boring Lectures**
- **Free Tools, Software, PDFs**
- **Learn From Expert Faculties**
- **Internships on Live Projects**

What is CEH?

A Certified Ethical Hacker is a specialist who works in a red team and focuses on breaking into computer systems to find weaknesses. They understand attack strategies, use creative methods to gain access, and imitate malicious hackers. But, unlike malicious hackers, they have permission and keep the results private. Bug bounty researchers are ethical hackers who find system flaws for rewards. Certified Ethical Hackers (CEHs) are trained professionals in cybersecurity who use their skills to identify and fix vulnerabilities in computer systems and networks. They are like digital detectives, but instead of solving crimes, they prevent them by understanding how attackers think and operate. CEHs often work in "red teams," which are groups that simulate cyberattacks to help organizations improve their defenses. In its 12th version, the Certified Ethical Hacker provides comprehensive training, hands- on 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



Module 01

Introduction to Ethical Hacking

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 02

Footprinting and Reconnaissance

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 03

Scanning Networks

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 04

Enumeration

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 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 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 07

Malware Threats

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 08

Sniffing

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 09

Social Engineering

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 10

Denial-of-Service

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 11

Session Hijacking

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 12

IDS, Firewalls & Honeypots

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 13

Hacking Web Servers

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 14

Hacking Web Applications

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 15

SQL Injection

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 16

Hacking Wireless Networks

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 17

Hacking Mobile Platforms

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 18

IoT Hacking

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 19

Cloud Computing

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 20

Cryptography

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.

C|EH

Certified Ethical Hacker

The C|EH Practical is a 6-hour, 100% hands-on exam delivered in our Cyber Range that requires you to demonstrate skills and abilities of ethical hacking techniques such as:

Pre Requisites :

- Minimum 10+2 Passed.
- Basic Knowledge of Networking.
- Basic Knowledge of Programming.
- Having Interest in Cyber Security.
- Have Extraordinary Learning skills.

EC-Council

CEH Exam Details	C|EH® (MCQ Exam)	C|EH® (Practical)
Number ofQuestions/Practical Challenges	125	20
Test Duration	4 Hours	6 Hours
Test Format	Multiple Choice Questions	iLabs Cyber
Test Delivery	ECC EXAM, VUE	Range
Availability	-	-
Exam Prefix	312-50 (ECC EXAM), 312-50	Aspen-iLabs
Passing Score	-	- 70%

REGISTER FOR A FREE TRIAL CLASS

CALL US AT
+91 9210640422

OR

DROP US A MAIL AT
Info@dicc.in

www.dicc.in

ADDRESS

K-39, II Floor, Central Market Lajpat Nagar - II Delhi, India (110024)