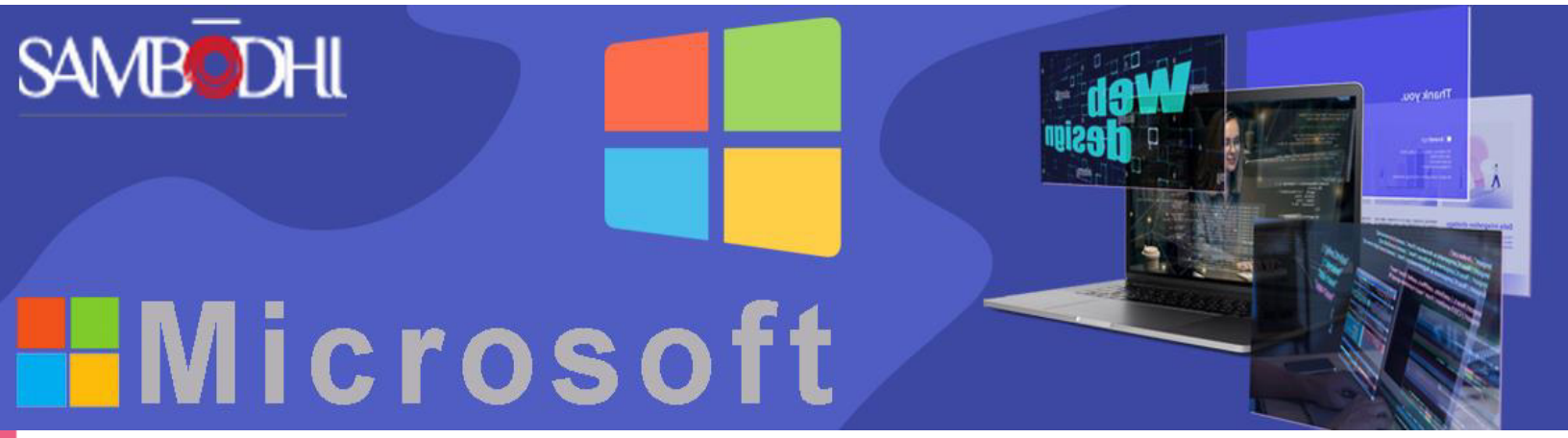

Certified Ethical Hacker (CEH) Training Course

Project Based Immersive Learning Course

Certified Ethical Hacker (CEH) Training Course Overview

Sambodhi and Education Nest offer a Certified Ethical Hacker (CEH) training course designed to equip you with the necessary skills to become a proficient hacker and fortify your network systems against cyber-attacks. Aligned with the latest CEH v12 by the EC-Council, this hands-on training program prepares you to enhance your blue team skills. The CEH certification course focuses on essential cybersecurity skills for security and network analysts. It validates your expertise in areas like network security, session hijacking, cryptography, system penetration testing, building firewalls, footprinting, and more, making you a Certified Ethical Hacker (CEH). The training enables you to handle cybersecurity challenges and provides a comprehensive understanding of security aspects. On successful completion of the course, you will receive a Course Completion Certificate from Sambodhi and Education Nest.

Benefits of Certified Ethical Hacker (CEH) Training Course:

Sambodhi and Education Nest's Certified Ethical Hacker (CEH) course is a valuable program for businesses seeking to enhance their cybersecurity practices. This ethical hacking certification verifies the skills necessary to succeed in the information security field and is mandatory for security-related positions in many IT departments. CEH certified professionals earn 44% more than non-certified counterparts, and being CEH certified is a badge of trust. NASSCOM reported that India alone would need 1 million cyber security professionals by 2020, while job portal Indeed reported a spike of 150 percent in cyber security roles between January 2017 and March 2018. By completing the CEH course, businesses can develop a strong understanding of security aspects and have the expertise to address cybersecurity issues.

Who should learn?

- IT security professionals
- Network security professionals
- Technical Support Engineers
- System Engineers
- Network Support Engineers
- Senior System Engineers
- It Operation Managers
- Individuals interested in a career in cybersecurity

Why do you need Certified Ethical Hacker (CEH) Training Course?

Average Salary Growth:

According to Payscale, the average salary for a Certified Ethical Hacker (CEH) professional in India ranges from INR 259k to INR 1.5m per year, depending on experience and job role. The salary growth for a CEH professional varies based on several factors, such as experience, skills, and the industry they work in. However, on average, CEH certified

professionals can expect a salary increase of around 10-15% compared to non-certified professionals in the same field.

Industries:

Certified Ethical Hacker (CEH) is a globally recognized and in-demand cybersecurity certification. CEH certified professionals are sought after in industries such as finance, healthcare, insurance, retail, telecommunications, and manufacturing, as well as multinational companies (MNCs). The skills and knowledge gained from CEH training are crucial in today's data-driven business environment, and professionals with expertise in CEH are in high demand. As companies continue to rely on data-driven insights to make strategic decisions, the demand for CEH certified professionals is projected to grow further.

Position in Market:

Research and Markets project that the global Certified Ethical Hacker (CEH) market will experience a compound annual growth rate (CAGR) of 11.2% from 2021 to 2026. According to Fortune Business Insights, the global cybersecurity market is also projected to grow at a CAGR of 13.4% from $155.83 billion in 2022 to $376.32 billion by 2029. This rapid growth is expected to increase the demand for professionals with CEH certification.

Designations:

- Information Security Officer
- Computer Forensics Engineer
- Ethical Hacker
- Vulnerability Analyst
- Network Security Engineer
- Security Analyst

Why Certified Ethical Hacker (CEH) Training Course from Education

- **Free Demo on Request**
- **Live Interactive Learning**
- **Lifetime Access**
- **Flexible Schedules**
- **24x7 Support**
- **One on One Doubt Clearing**
- **Real Time Project-Based Learning**
- **Certificate Oriented Curriculum**

Key Skills Covered:

- Hacker Types
- Tools, Skills
- Process, Reconnaissance
- Footprinting, Fingerprinting
- Malware Threats
- Sniffing & Tools
- Wireless Network Security
- ARP, DNS Poisoning
- Evading IDS
- Firewalls and Honeypots
- Social Engineering
- DDOS Attacks
- SQL Injection, Pen Testing

Certified Ethical Hacker (CEH) Training Course

Module 1: Information Security Overview

- Information Security Overview
- Hacking Methodologies and Frameworks
- Ethical Hacking Concepts
- Ethical Hacking Concepts
- Controls Information Security
- Information Security Attack and Threats vendors
- Information Security Laws and Standards
- Physical Security
- Risk
- Threat Modeling
- Incident Management

Module 2: FootPrinting and Reconnaissance

- Footprinting Concepts
- Footprinting through Search Engines
- Footprinting through Web Services
- Footprinting through Social Networking Sites
- Website Footprinting
- Email Footprinting
- Whois Footprinting
- DNS Footprinting
- Network Footprinting
- Footprinting through Social Engineering
- Footprinting Tools

- Footprinting Countermeasures

Module 3: Network Scanning Basics

- Network Scanning Concepts Overview
- Network Scanning Techniques
- Network Diagrams
- Host Discovery
- Port and Service Discovery
- OS Discovery (Banner Grabbing/OS Fingerprinting)
- Scanning Beyond IDS and Firewall
- Network Scanning Countermeasures

Module 4: Enumeration Basics

- Enumeration Concepts
- NetBIOS Enumeration
- SNMP Enumeration
- LDAP Enumeration
- NTP and NFS Enumeration
- SMTP and DNS Enumeration
- Other Enumeration Techniques (IPsec, VoIP, RPC, Unix/Linux, Telnet, FTP, TFTP, SMB, IPv6, and BGP enumeration)
- Enumeration Countermeasures

Module 5: Vulnerability Analysis

- Vulnerability Assessment Concepts
- Vulnerability Assessment Solutions Working
- Vulnerability Classification and Assessment Types
- Kinds of Vulnerability Assessment Tools
- Characteristics of a Vulnerability Assessment Tools
- Vulnerability Scoring Systems
- Vulnerability Assessment Tools

- Vulnerability Assessment Reports

Module 6: System Hacking

- Gaining Access
- Escalating Privileges
- Maintaining Access
- Clearing Logs

Module 7: Malware Threats

- Malware Concepts
- APT Concepts
- Trojan Concepts
- Virus and Worm Concepts
- File-less Malware Concepts
- Malware Analysis
- Malware Countermeasures
- Anti-Malware Software

Module 8: Sniffing

- Sniffing Concepts
- Sniffing Technique: MAC Attacks
- Sniffing Technique: DHCP Attacks
- Sniffing Technique: ARP Poisoning
- Sniffing Technique: Spoofing Attacks
- Sniffing Technique: DNS Poisoning
- Sniffing Tools
- Sniffing Countermeasures

Module 9: Social Engineering

- Social Engineering Concepts
- Social Engineering Techniques

- Insider Threats
- Impersonation on Social Networking Sites
- Identity Theft
- Social Engineering Countermeasures

Module 10: Denial-of-Service(DoS)

- DoS/DDoS Concepts
- Botnets
- DoS/DDoS Attack Techniques
- DDoS Case Study
- DoS/DDoS Countermeasures

Module 11: Session Hijacking

- Session Hijacking Concepts
- Application Level Session Hijacking
- Network Level Session Hijacking
- Session Hijacking Tools
- Session Hijacking Countermeasures

Module 12: IDS, Honeypots, and Firewalls

- IDS, IPS, Firewall, and Honeypot Concepts
- IDS, IPS, Firewall, and Honeypot Solutions
- Evading IDS
- Evading Firewalls
- Evading NAC and Endpoint Security
- IDS/Firewall Evading Tools
- Detecting Honeypots
- IDS/Firewall Evasion Countermeasures

Module 13: Hacking Web Servers

- Web Server Concepts
- Web Server Attacks
- Web Server Attack Methodology
- Web Server Attack Countermeasures
- Patch Management

Module 14: Hacking Web Applications

- Web App Concepts
- Web App Threats
- Web App Hacking Methodology
- Web API, Webhooks and Web Shell
- Web Application Security

Module 15: SQL Injection

- SQL Injection Concepts
- Types of SQL Injection
- SQL Injection Methodology
- SQL Injection Tools
- Evasion Techniques
- SQL Injection Countermeasures

Module 16: Hacking Wireless Networks

- Wireless Concepts
- Wireless Encryption
- Wireless Threats
- Wireless Hacking Methodology
- Wireless Hacking Tools
- Bluetooth Hacking
- Wireless Attack Countermeasures
- Wireless Security Tools

Module 17: Hacking Mobile Platforms

- Mobile Platform Attack Vectors
- Hacking Android OS
- Hacking iOS
- Mobile Device Management
- Mobile Security Guidelines and Tools

Module 18: IoT Hacking

- IoT Fundamentals
- IoT Attacks
- IoT Hacking Methodology and IoT Hacking Tools
- IoT Attack Countermeasures
- OT Concepts
- OT Attacks
- OT Hacking Methodology
- OT Attack Countermeasures

Module 19: Cloud Computing

- Cloud Computing Concepts Basics
- Container Technology
- Serverless Computing
- Cloud Computing Threats and Attacks
- Cloud Hacking
- Cloud Security and Cloud Security Tools
- Cloud Penetration Testing

Module 20: Cryptography

- Cryptography Concepts and Encryption Algorithms
- Cryptography Tools

- Public Key Infrastructure (PKI) and Email Encryption
- Disk Encryption and Cryptanalysis
- Defending Cryptography Attack

Career Support

Profile Building:

Experienced professionals are available to offer tailored assistance in crafting your CV and online profiles, taking into account your unique educational and experiential background.

Interview Preparation:

The upcoming interview preparation service will include personalized one-on-one sessions and the option for mock interviews if needed.

Job Referrals:

At Education Nest, we receive a variety of job requirements from diverse sources such as organizations, our clients, HR consultants, and a vast network of Education Nest currently employed in different companies. We strive to meet these varied requirements to the best of our abilities.

Continuous Support:

We offer continuous support for as much time as you need it, and a considerable number of our learners receive multiple interviews offers and promising employment opportunities as a result of the abilities they gain during the program.