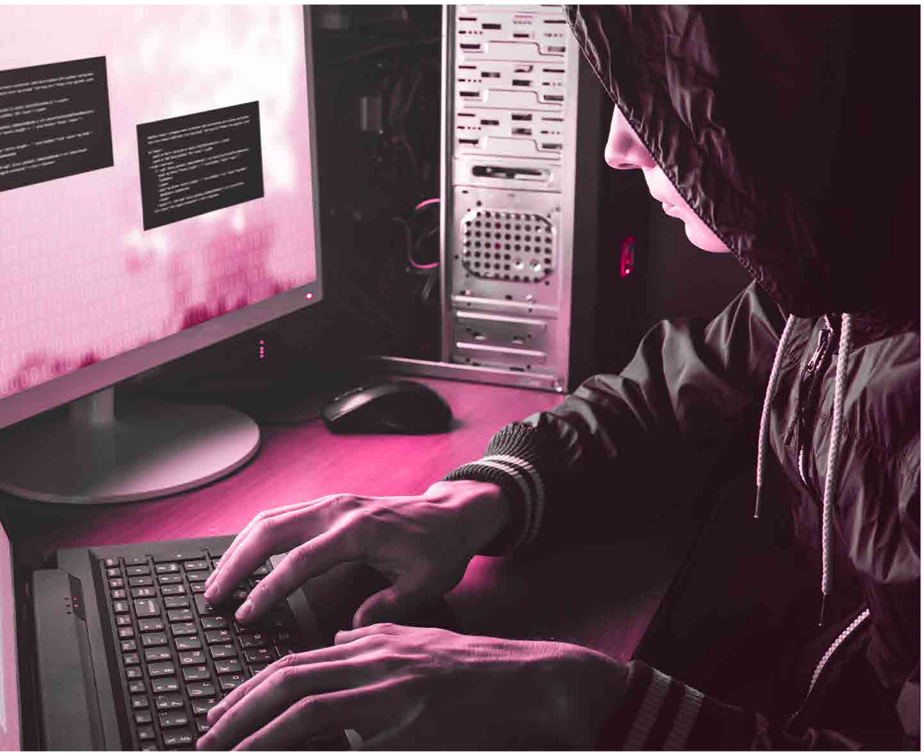
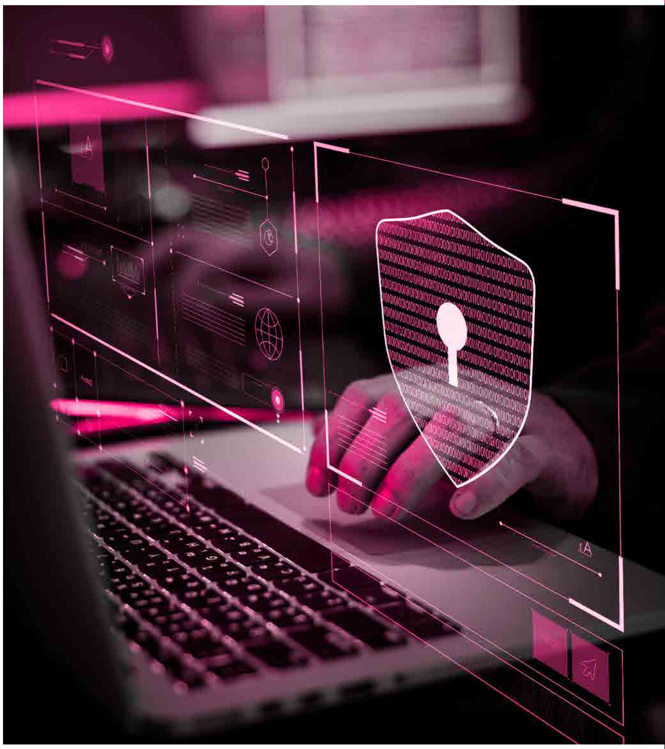
INFOSECTRAIN



CEH v11

Certified Ethical Hacker

CERTIFICATION & TRAINING



KEY FEATURES

- 40 hrs of instructor-led training
- EC-Council Authorized Partner
- Access to the recorded sessions
- Certified & Experienced Trainers

www.infosectrain.com
sales@infosectrain.com

Overview

The Certified Ethical Hacker (CEH v11 Training) program by EC-Council upgrades your understanding of core security fundamentals. Certified Ethical Hacker (CEH V11 Certification Course) is one of the most sought-after security certifications globally that is considered in high regard. This internationally valued security training validates your abilities to identify the vulnerabilities in the organization's network infrastructure and helps to combat cyber-attacks effectively.

CEH v11 Training is the second course in the new Vulnerability Assessment and Penetration Testing (VAPT) Track developed by EC-Council. In the latest version, EC-Council has added topics and concepts considering the recent advancements in the field of cybersecurity. The course equips you with the understanding of the latest commercial hacking tools, practices, and methodologies used by real-world hackers.

Target Audience

- Ethical hackers
- System Administrators
- Network Administrators
- Engineers
- Web managers
- Auditors
- Security Professionals

Pre-Requisite

CEH v11 certification Course Needs:

Basic understanding of network essentials, core concepts including server and network components

Why Infosec Train?

- Certified & Experienced Instructor
- Flexible Schedule
- Access to the recorded sessions
- Post Training Support
- Tailor Made Training
- 4 hrs/day in Weekend/ Weekday

Our Expert Instructors

"

Bharat served as a corporate trainer & Consultant with nearly 8+ years of experience across the diverse industry. Good hands-on experience in vulnerability assessment, Penetration Testing.

BHARAT MUTHA

CEH I ECIH I CHFI I ECSA I CTIA I CSCU I CySA+ I PenTest+ I securitY+

"

Information security Instructor and a security researcher . Performed Web App. Security assessment, identifying various application related vulnerabilities.performing Internal and external pen-test.

DEEPAK BHATT

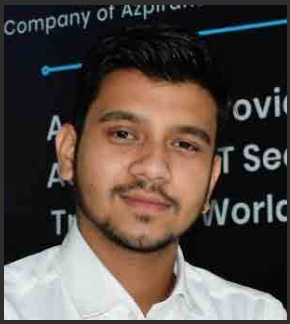
CEH v11 I CND I ECSA I ECSS I CHFI I Network + I security + I Pen test + I CYSA+ I CCISO I ISO

"

Sanyam served as a corporate trainer & Consultant with nearly 5+ years of experience across the diverse industry. Delivering more than 30+ training programs yearly, with 250+ professionals overall.

SANYAM NEGI

CEH | CHFI | CTIA | Sec+ | Pentest+ | AWS Sec | AWS Architect



"

Ashish Delivered training to government and non-government organizations around the globe on different cyber security verticals and Network Security.

ASHISH DHYANI

CEH | CCNA | Network+ | Sec+

HAPPY LEARNERS FROM THE WORLD

Siddharth Shankar Shetty

CEH | India

All expectations were fullfilled via infosec , i might enroll for futher courses in future highly recommended

Satish Appalla

CEH | India

The training was very good and engaging. I feel this online training was more convenient and effective in this new normal stage. InfosecTrain support and trainer were very good. I will definitely consider other courses with InfosecTrain.

Joseph Lamine

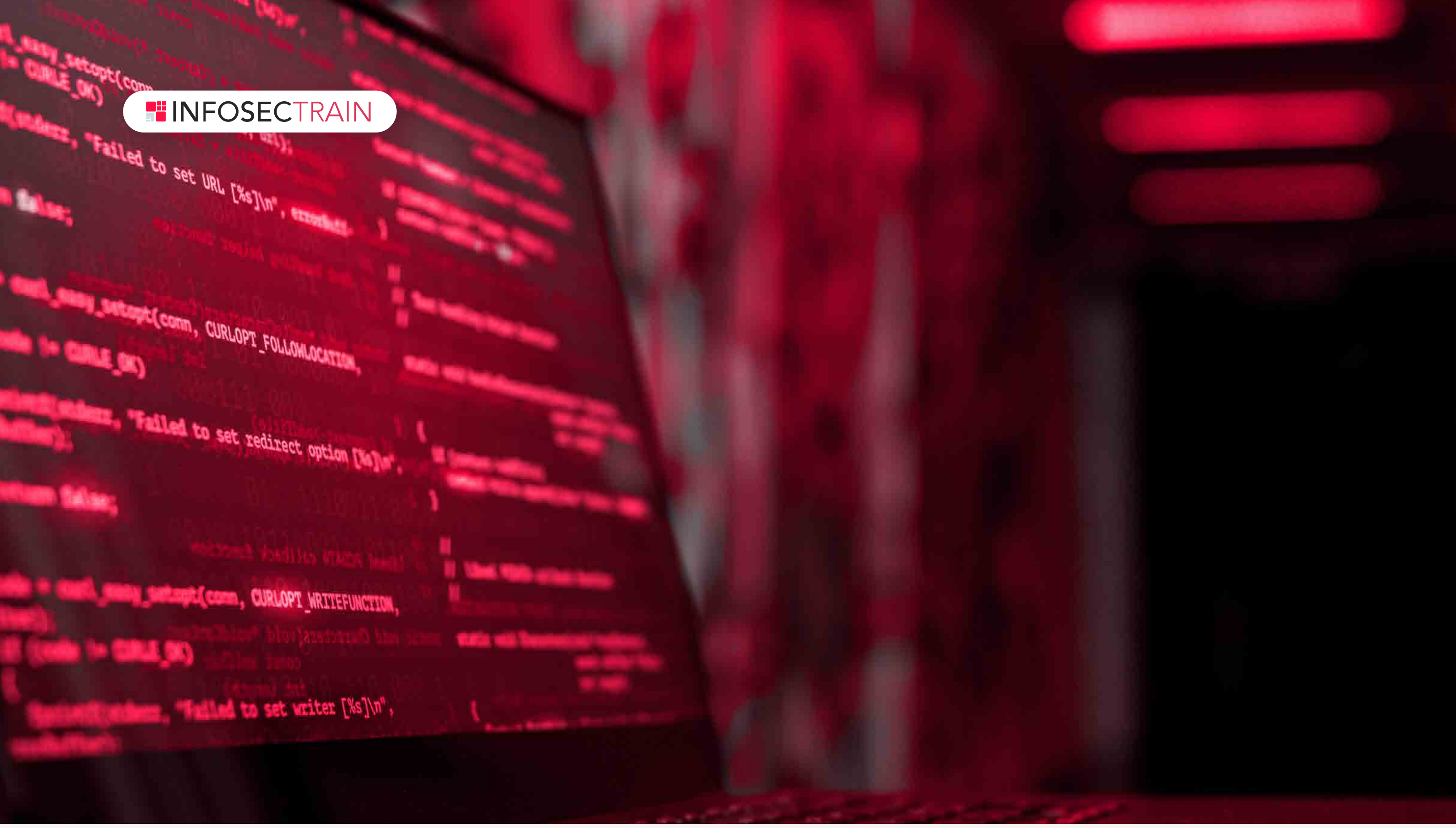
CEH | Senegal

I really appreciate the training, good control of training subject by the trainer and he provides excelllent references/advisor to dive deeper. This course will be helpful in my daily job as soc analyst.

Sahaya Emmanuel

CEH | Singapore

The Training was good. Course Content was good. Learnt lot of new things which will be helpfull in my career.



INFOSECTRAIN

Exam Information

For EC-Council Certified Ethical Hacker (CEH) certification

Certification Name	312-50 (ECC EXAM), 312-50 (VUE)
Test Format	Multiple Choice
Number of questions	125
Test Duration	4 Hours
Test Delivery	ECC EXAM, VUE

EC council provides exam in the form of different question banks with varying difficulty levels. Cut scores can range from 60% to 85%, depending on which Exam information of CEH v11 form is challenged.

COURSE OUTLINE

Module 01: Introduction to Ethical Hacking

This module introduces you to the basic concepts of hacking, what is hacking, who are hackers, their intent, and other related terminologies.

The next modules dive deeper into the various phases of hacking, which would help you in thinking with the mindset of a hacker.

Module 02: Footprinting and Reconnaissance

Gathering information from various sources using footprinting tools and how to defend against the same.

Module 03: Scanning Networks

Different techniques to identify and scan the network, host, and port discovery by utilizing various scanning tools.

Module 04: Enumeration

Finding detailed information about the hosts and ports discovered during scanning. This module now includes sub-domains like NFS enumeration and related tools, DNS cache snooping, and DNSSEC Zone walking, along with the countermeasures.

Module 05: Vulnerability Analysis

It introduces the concepts of vulnerability assessment, its types, along with a hands-on experience of tools that are currently used in the industry.

Module 06: System Hacking

It focuses on the “how” part. How to gain access of the system, how to escalate privileges, how to maintain access, and how to clear your tracks.

The next modules help to develop a deeper understanding of various defense and attack methodologies and concepts that aid the process of hacking.

Module 07: Malware Threats

Malware threat terminologies, viruses, worms, trojans, their analysis, and countermeasures to prevent data loss. The introduction and analysis of malware like, Emotet and fileless that are gaining popularity have been updated under this section. APT concepts have also been added.

Module 08: Sniffing

Packet sniffing techniques, associated tools, and related defensive techniques.

Module 09: Social Engineering

Since humans are the most significant vulnerability for any organization, it becomes essential to understand how attackers use them for their purpose for carrying out attacks like identity theft, impersonation, insider threat, and how to defend against such social engineering attacks.

Module 10: Denial-of-Service

As DoS and DDoS are some of the most common purposes of attackers, this module talks about these attacks, use cases, and the related attack and defense tools.

Module 11: Session Hijacking

To provide a deeper understanding of the technique, its purpose, tools used along with the countermeasures.

Module 12: Evading IDS, Firewalls, and Honeypots

Understand the terminologies and working of these inline defenses and techniques to learn how to evade these while performing an attack.

Module 13: Hacking Web Servers:

Web servers based attacks, methodologies, tools used, and defense

Module 14: Hacking Web Applications

Web application-based attacks, techniques, and mitigation.

Module 15: SQL Injection

An in-depth understanding of the top OWASP top 10 web app vulnerability, it’s working and the mitigation.

Module 16: Hacking Wireless Networks

Wireless encryption, wireless hacking, and Bluetooth hacking-related concepts

Module 17: Hacking Mobile Platforms

Management of mobile devices, mobile platform attack vectors, and vulnerabilities related to Android and iOS systems

Module 18: IoT Hacking

Recognizing the vulnerabilities in IoT and ensuring the safety of IoT devices. Operational Technology (OT) essentials, introduction to ICS, SCADA, and PLC, threats, attack methodologies, and attack prevention. The concept of OT is a new addition.

Module 19: Cloud Computing

Cloud computing, threats, and security. Additionally, the essentials of container technology and serverless computing have been added.

Module 20: Cryptography

Encryption algorithms, Public Key Infrastructure (PKI), cryptographic attacks, and cryptanalysis.

INFOSECTRAIN

www.infosectrain.com | sales@infosectrain.com