Certified Ethical Hacking–Penetration Testing In Ahmedabad

Master cybersecurity with comprehensive training in ethical hacking, penetration testing, and vulnerability assessment,

WHAT YOU'LL LEARN

- Understand ethical hacking principles, methodologies, and tools.
- Develop expertise in penetration testing, vulnerability assessment, and exploitation techniques.
- Gain hands-on experience with advanced hacking tools and real-world scenarios.
- Prepare for industry-recognized certifications: CPEH and CPTE.

REQUIREMENTS

Basic knowledge of networking and operating systems is recommended.

A keen interest in cybersecurity and ethical hacking.

WHO'S THIS COURSE IS FOR

Aspiring cybersecurity professionals and ethical hackers.

IT professionals seeking to enhance their security expertise.

Organizations looking to train employees in advanced cybersecurity practices.

DESCRIPTION

Certified Ethical Hacking and Penetration Testing Program

- **Duration:** 6 Months
- **Start Date:** Option to start today also, instructor will adjust you to recently started batch. **Enroll now**
- **Days:** Mon-Tue-Wed-Thu-Fri, 5 days a week and 2 Hours/Session
- **Timings**: 3:00 PM-5:00 PM or 5:00 PM to 7:00 PM or 7:00 PM to 5:00 PM (Choose any 2 hours)
- **Mode:** Offline(Swastik Cross Road, above Kundanlal Jwellers, Vasant Vihar, Navrangpura, Ahmedabad, Gujarat 380009)
- **Languages**: English, Hindi & Gujarati
- **Fees:** INR 59,000/-

_____
_____

Part 1: CPEH — Certified Professional Ethical Hacker

₹59000 ~~₹70000~~   15.7% off

★★★★★

Date
01 May to 01 Nov 2025

Time
03:00 PM - 09:00 PM

Total Sessions (Hours)
100 (150h 0min)

Location

C.G Road

Level

All

Language

Hindi

Vipinchandra Sandhansive
Instructor

Cybersecurity Expert | Certified Ethical Hacker | Passionate Educator | Empowering the Next Generation of Cyber Defenders

Instructor Rating

5

Students

88

Courses

1

Module 1: Introduction to Ethical Hacking

- Overview of ethical hacking and its importance in cybersecurity.
- Ethical guidelines and legal frameworks for hacking.

Module 2: Linux Fundamentals

- Key Linux commands, file structures, and their relevance to cybersecurity.

Module 3: Networking Protocols and Cryptography

- Understanding networking protocols and their vulnerabilities.
- Encryption techniques and algorithms for securing data.

Module 4: Core Hacking Techniques

- Password cracking methods and tools for testing password security.
- Malware types, behavior analysis, and mitigation strategies.
- Configuration and deployment of firewalls, IDS/IPS, and other security devices.

Module 5: Reconnaissance

- Passive reconnaissance: Gathering information discreetly.
- Active reconnaissance: Probing networks and systems.
- Social engineering techniques for psychological manipulation.

Module 6: Exploitation Techniques

- Vulnerability assessment: Identifying and mitigating risks.
- Network attacks: Exploiting and securing network vulnerabilities.
- Hacking servers and web technologies to uncover and address weaknesses.

_____

_____

Part 2: CPTE — Certified Penetration Testing Engineer

Module 1: Penetration Testing Fundamentals

- Business and technical logistics of penetration testing projects.
- Planning, scope, and execution of pen testing.

Module 2: Information Gathering and Reconnaissance

- Passive and active techniques for data collection.
- Detecting live systems and identifying network assets.

Module 3: Advanced Hacking Techniques

- Banner grabbing and enumeration for service discovery.
- Automated vulnerability assessments with industry-leading tools.
- Operating system exploitation and securing measures.

Module 4: Specialized Pen Testing

- Advanced assessment and exploitation strategies.
- PowerShell hacking for automation and penetration testing.
- Network sniffing to monitor traffic and identify potential issues.

Module 5: Web, Mobile, and IoT Security

- Techniques for hacking web technologies and securing platforms.
- Identifying vulnerabilities in mobile and IoT devices.

Module 6: Reporting and Documentation

- Basics of report writing to document findings, risks, and mitigation plans.

_____

_____

Certifications by Mile2 USA

- **CPEH — Certified Professional Ethical Hacker**
- **CPTE — Certified Penetration Testing Engineer**

These certifications validate your ability to safeguard systems, mitigate cyber threats, and perform penetration testing effectively.