



**EXCELLENCE** : We will passionately strive to achieve excellence in all our undertakings

**RESPONSIBILITY** : We will take complete ownership to create a better world for our future generations

**PURPOSE** : We will put purpose before profit for our stakeholders

**INTEGRITY** : We will be honest and ethical in all our actions & behaviour



## CERTIFIED PENETRATION TESTER AND ETHICAL HACKER (CPTEH)



## Who we are

### Confederation of Educational

IZOMER Education is national education space with a mission to support communities, industries and governments through the promotion of global knowledge, learning, research, education and training initiatives. To this effect, through various of its endeavors and programmes, the Confederation of Educational Institutions of India remains passionate about ensuring that information and knowledge are disseminated without restrictions of any kind, throughout civil society, industry and the government

## Our mission

Education has the power to revolutionise and transform lives of human beings and the world. And this is precisely why the Confederation of Educational Institutions of India is passionately committed to fostering learned and capable humanistic responsible young global leaders through developing and providing life-transforming, empowering, value-creating educational programmes and experiences to the individuals, educators, institutions, businesses, governments, societies. We partner with world's leading colleges and universities to provide students with knowledge, skills and critical-real world experiences relevant to them

## Our vision

We see ourselves as the most trusted, reliable and contributive leader in the education arena to help individuals, businesses, organisations and communities achieve their excellence.

## Our values

Our values drive us. They are fundamental beliefs of our organisation, which define our purpose of existence and the role each one of us play in bringing a transformation in the world and lives of every individual through our actions, behaviours and and deliverables.

## About the Program:

This program is designed to acquaint students with the fundamentals of cyber security and the diverse career opportunities within the field, enabling them to grasp the real-world hurdles organizations encounter today. Through practical application and skill development, participants will learn how to effectively tackle these challenges. Emphasizing hands-on engagement, this course actively involves students in various public and industry cyber security challenges, fostering a proactive learning environment.



- **Physical sessions tailored for graduates and professionals**
- **Comprehensive employability skills training Offered**
- **100% placement assistance guarantee for the eligible candidates**



The IZOMER Academy offers hands-on training sessions aimed at bridging the skill gap in the information and communication technology (ICT) domain. These online or offline sessions provide job-oriented courses in information technology (IT), furnishing participants with the essential skills and certifications required for various IT job roles. This proactive approach has proven instrumental in assisting numerous individuals in securing employment within the ICT sector.

## Job Roles

Candidates participating in this program can anticipate a wide range of potential career paths upon completion.

### Cyber Security Analyst

~ 4 L

### Penetration Tester

~ 5 L

### Network Security Engineer

~ 4 L

### Information Security Analyst

~ 5 L

## Learning Outcome Upon completion of the program, participant's will be equipped with:

- Comprehensive Cyber Security knowledge:** A thorough understanding of fundamental and advanced cyber security concepts, including network security, cryptography, cyber attack life cycles, and cyber security standards and frameworks.
- Practical Skills:** Proficiency in using cyber security tools and techniques for network and web application penetration testing, WiFi security assessments, and malware analysis, along with hands-on experience in social engineering and OSINT.
- Critical Thinking and Problem-Solving:** Enhanced ability to identify, analyze, and mitigate various cyber security threats, employing critical thinking and problem-solving skills to address complex security challenges.
- Career Readiness:** Preparedness to enter the cyber security field with a competitive edge, equipped to handle real-world security issues and contribute effectively to organizational security measures and projects.
- Agenda**
  - Cyber Security Fundamentals
  - Cyber Security Standards
  - Types of Cyber Security Framework
  - Introduction to Careers in Cyber Security
  - Cyber Attack Life cycle
  - Building a secure Hacking Lab
  - Types of Attacks
  - Network Security Attacks
  - Web Application Attacks
  - Zero-Day Exploit

## About IZOMER



IZOMER Educational institutions are responsible for a wide range of functions, from transmitting knowledge and skills for economic and professional success to inculcating values, fostering social mobility, and driving innovation. They prepare individuals for careers, promote critical thinking, and shape well-rounded citizens who can contribute positively to society, both through formal curricula and the hidden curriculum of school life.

## Certified Penetration Tester and Ethical Hacker (CPTEH)

### ELIGIBILITY

- Minimum Qualification: Class 10th or 12th pass
- Technical Skill: Basic Knowledge of Computers and Networks
- Preferred Background: Students from any Stream

### Skill Required for Cyber Security Courses

- Basic knowledge of computers systems and networks
- Interest in problem solving and critical thinking



## Appendix: Detailed Program Curriculum

### CERTIFIED PENETRATION TESTER AND ETHICAL HACKER (CPTEH)

The Certified Penetration Tester and Ethical Hacker (CPTEH) course is designed to equip learners with the practical skills and mindset needed to identify, exploit, and defend against modern cyber threats. The program focuses on real-world scenarios, combining offensive and defensive techniques to build a complete understanding of cyber security. Through guided labs, hands-on exercises, and structured modules, learners explore topics such as network

exploitation, vulnerability assessment, privilege escalation, web and cloud security, and blue team defense. The course emphasizes ethical practices, legal boundaries, and responsible testing, preparing participants to become skilled, professional, and ethical cybersecurity practitioners.



### Hacker ACTIVITY

By the end of this course, learners will be able to:

- Understand core cybersecurity and ethical hacking concepts.
- Perform information gathering and vulnerability analysis.
- Exploit systems using port-based and service-based methods.
- Conduct web and cloud pentesting safely.
- Apply Linux and Windows privilege escalation techniques.
- Detect, respond, and defend in SOC-style environments.
- Produce professional pentesting and compliance reports.
- Follow ethical, legal, and responsible testing practices.

### COURSE OBJECTIVES

### COURSE PHILOSOPHY

**Hands-On First : every topic links to a practical lab.**

- **Ethics Always:** no unauthorized testing; every step follows written consent.
- **Continuous Learning:** blend red team and blue team understanding.
- **Realistic Practice:** use real-world tools (Nmap, Metasploit, Burp, OpenVAS, Wireshark, etc.).
- **Self-Development:** build critical thinking and report-writing skills.
- **Security Mindset:** think like an attacker, act like a defender.

### CONCLUSION

The CPTEH course concludes by reinforcing a strong foundation in both ethical hacking and penetration testing methodologies.

Participants emerge with practical experience, technical confidence, and a professional understanding of how to secure systems through responsible testing and remediation. This certification encourages continuous learning, disciplined research, and ethical responsibility within the cybersecurity field. By completing the course, learners are prepared to contribute to real-world security operations, strengthen organizational defenses, and uphold the highest standards of integrity in the practice of ethical hacking.

**MODULE 1: FOUNDATIONS OF NETWORKING AND CYBERSECURITY**

**MODULE 2: LINUX FUNDAMENTALS FOR CYBERSECURITY PROFESSIONALS**

**MODULE 3: ANONYMITY, PROXIES, VPNS & PRIVACY-FOCUSED OPERATING SYSTEMS**

**MODULE 4: ETHICAL HACKING, RECONNAISSANCE**

**MODULE 5: NETWORK & PORT-BASED EXPLOITATION**

**MODULE 6: WEB APPLICATION PENETRATION TESTING**

**MODULE 7: WIRELESS & IOT PENTESTING**

**MODULE 8: REPORTING & COMPLIANCE**

