eHACK ACADEMY™
INSTITUTE OF EMERGING TECHNOLOGIES

MASTER'S CERTIFICATION PROGRAM in CYBER SECURITY

Course Objective

The Masters Program in Ethical Hacking & Cyber Security by eHack Academy is an intensive, job-oriented program designed to take learners from fundamentals to advanced cybersecurity skills. It focuses on ethical hacking, penetration testing, network and application security, cyber defense, and digital forensics through hands-on labs and real-world tools. The program is suitable for beginners as well as professionals and prepares students for globally recognized certifications, enabling them to identify vulnerabilities, secure systems, and build a strong career in the cybersecurity domain.

Earn 6 Global Certifications

CSCU CND CEH CHFI CPENT LPT

9-12 MONTHS
Duration

300+
Training Hours

2 YEARS
Membership

info@ehackacademy.com +91-9886035330 www.ehackacademy.com

Course Syllabus

Module 00

ICE Breaker, Program Kick-off & Orientation -

Your journey into a high-growth cyber security career begins from Day One. The ICE Breaker & Orientation session is a power-packed 4-hour onboarding experience designed to align learners with industry expectations, global certifications, and a clear career roadmap—before core technical training begins.

What you'll learn:

- Interactive introductions to build confidence and collaboration
- Clear understanding of the Master's Program structure
- Alignment on learning discipline, ethics, and performance standards
- Setting expectations for real-world cyber security careers
- Introduction to eHack Academy – Institute of Emerging Technologies
- Overview of EC-Council, the world's leading cyber security certification body
- Academic, university, and industry partnerships
- Industry-aligned curriculum with real-world relevance
- Guided walkthrough of the EC-Council LMS
- Access to official courseware, labs, and licensed tools
- Importance of classroom training and hands-on practice
- Transparent evaluation, exam pattern, and certification process
- Cyber Security–specific resume building
- Understanding job roles, domains, and growth paths
- Smart job application strategies and LinkedIn optimization
- Long-term career success roadmap in cyber security

Module 01

P|CSF - Professional | Cyber Security Fundamentals -

Build a strong foundation in Cyber Security essentials covering hardware, operating systems, networking, servers, and cloud technologies.

What you'll learn:

- Computer Hardware & Architecture
- Operating Systems (Windows/Linux/Mac)
- Networking FundamentalsTCP/IP & Network Protocols
- Server Administration Basics
- Cloud Computing Concepts
- Virtualization Technologies
- Basic Troubleshooting

Module 02

P|SCSP[AI] - Professional | Secure Computer Systems Program[AI] -

Establish a strong foundation in cybersecurity principles. Learn essential security awareness and secure computing practices for personal and professional environments.

What you'll learn:

- Introduction to Digital Security
- Operating System Protection Techniques
- Malicious Software and System Defense
- Internet Usage Security Practices
- Security AwarSecuring Emaeness for Social Media Platforms
- Email Communication Protection Methods
- Mobile Device Security Fundamentals
- Cloud Usage and Data Protection
- Network Connectivity and Access Security
- Data Backup and Business Continuity Planning
- Protection of Smart and Connected Devices
- Safe Digital Workspaces and Remote Access Security

Module 03

P|NDP[AI] - Professional | Network Defense Program[AI] -

Master the protect, detect, respond, and predict approach to network security with enterprise-level defense strategies.

What you'll learn:

- Network Attacks and Defense Approaches
- Administrative Network Security
- Technical Network Security
- Network Boundary and Perimeter Security
- Endpoint Protection for Windows Systems
- Endpoint Protection for Linux Systems
- Endpoint Protection for Mobile Devices
- Endpoint Protection for IoT and Smart Devices
- Administrative Application Security
- Data Security and Protection Controls
- Network Threat Analysis and Response
- Network Policy and Governance Management
- Secure Network Architecture Design
- Perimeter Monitoring and Defense Systems
- Windows Endpoint Hardening Techniques
- Linux Endpoint Hardening Techniques

- IoT Security Administration
- Application Security Administration
- Enterprise Data Protection Strategies

Module 04

P|EHCOP^{AI} - Professional | Ethical Hacking and Cyber Offense Program^{AI} -

Think like an attacker to defend like a professional. Master reconnaissance, exploitation, and over 550 attack techniques.

What you'll learn:

- Fundamentals of Ethical Hacking
- Information Gathering and Reconnaissance
- Network Scanning Techniques
- System Enumeration Methods
- Vulnerability Identification and Analysis
- System Exploitation Techniques
- Malware Threat Analysis
- Network Traffic Monitoring and Sniffing
- Social Engineering Attack Methods
- Service Disruption Attacks
- Session Hijacking Session Control and Hijacking
- Security Control Evasion Techniques
- Web Server Security Testing
- Web Application Security Assessment
- Database and Injection Attacks
- Wireless Network Exploitation
- Mobile Platform Security Testing
- IoT Security Attacks
- Cloud Infrastructure Security Risks
- Cryptography and Data Protection Basics

Module 05

P|APTP^{AI} - Professional | Advanced Penetration Testing Program^{AI} -

Elevate your skills with advanced red team techniques including IoT exploitation, OT/SCADA security, and live cyber range exercises.

What you'll learn:

- Penetration Testing Foundations
- Testing Scope and Engagement Planning
- Open-Source Intelligence Techniques
- Social Engineering Assessment
- External Network Penetration Testing

- Internal Network Penetration Testing
- Perimeter Network Testing
- Web Application Penetration Testing
- Wireless Security Testing
- IoT Penetration Testing
- Operational Technology and SCADA Security Testing
- Cloud Penetration Testing
- Binary Analysis and Exploitation
- Reporting, Documentation, and Post-Test Actions

Module 06

P|DFIP[AI] - Professional | Digital Forensics and Investigation Program[AI] -

Master the science of cyber investigations with evidence collection, forensic analysis, and reporting techniques.

What you'll learn:

- Computer Forensics Overview
- Digital Investigation Methodology
- Storage Media and File System Analysis
- Evidence Acquisition and Duplication
- Anti-Forensics and Counter Techniques
- Windows System Forensics
- Linux and macOS Forensics
- Network Forensics Analysis
- Malware Forensic Investigation
- Web Attack Investigation
- Dark Web Investigation Techniques
- Cloud Forensics and Data Analysis
- Email and Social Media Forensics
- Mobile Device Forensics
- IoT Forensic Investigation

Module 07

Personality and Softskill Development -

Understand the importance of personality in career growth, industry expectations, and placement readiness.

What you'll learn:

- Self-Awareness & Confidence Building
- Attitude, Mindset & Professional Behavior
- Emotional Intelligence (EQ)
- Time Management & Productivity

- Verbal Communication Skills
- Non-Verbal Communication & Body Language
- Listening Skills & Question Handling
- Public Speaking & Presentation Skills
- Teamwork & Leadership Skills
- Corporate Communication Skills
- Problem-Solving & Critical Thinking
- Resume Building (ATS-Friendly)
- LinkedIn Profile & Personal Branding
- Group Discussion (GD) Techniques
- HR Interview Preparation
- Mock Interviews – HR & Technical
- Corporate Readiness & Workplace Ethics
- Placement Readiness & Career Roadmap

Module 08

OWASP Top 10 -

Master the OWASP Top 10 web application security risks and learn how to identify, exploit, and mitigate them.

What you'll learn:

- Injection Attacks (SQL, NoSQL, OS)
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access Control
- Security Misconfigurations
- Cross-Site Scripting (XSS)
- Insecure Deserialization
- Using Components with Known Vulnerabilities
- Insufficient Logging & Monitoring

Module 09

3 Months Internship -

Each Master Program student must select ANY TWO advanced projects.

What you'll learn:

- Advanced Penetration Testing & Red Team Operations
- Enterprise Security Operations & Incident Management
- Advanced Digital Forensics & Incident Response
- Cloud Security Architecture & Compliance
- Threat Intelligence & Security Strategy