“Placement assurance for all, Minimum 50 learners get 100% Placement or Full fee refund.”

“ IITians-Founded Coder Pathshala ”

Expert **Ethical hacking** career support with **IIT alumni** and top professionals from **Google, Reliance-Jio**, **IISc-Bangalore** & leading research institutes.

Programming in C (Semester 1)

Module 1: Introduction to Programming & C Basics

- Problem-solving techniques
- Algorithms and flowcharts
- Structure of a C program
- Compilation and execution process

Module 2: Data Types & Operators

- Variables and constants
- Data types and type conversion
- Arithmetic, relational, logical operators
- Expressions and precedence

Module 3: Control Structures

- Conditional statements
- Looping constructs
- Nested loops
- Break and continue

Module 4: Arrays & Strings

- One-dimensional and two-dimensional arrays
- Character arrays and string functions
- Array applications

Module 5: Functions & Pointers

- Function declaration and definition
- Call by value and call by reference
- Pointer basics and pointer arithmetic
- Dynamic memory allocation

Module 6: Structures & File Handling

- Structures and unions
- File operations
- Command-line arguments
- Simple applications

Python Programming (Semester 1)

Module 1: Python Fundamentals

- Introduction to Python
- Syntax and indentation
- Variables and input/output

Module 2: Control Flow & Functions

- Conditional statements
- Loops
- Functions and parameters

Module 3: Python Data Structures

- Lists and tuples
- Sets and dictionaries
- Data manipulation techniques

Module 4: Strings, Files & Exceptions

- String operations and formatting
- File read/write
- Exception handling

Module 5: Modules & Libraries

- Importing modules
- Standard libraries
- Introduction to NumPy

Module 6: Problem Solving with Python

- Algorithmic thinking
- Logical problem solving
- Mini-project using Python

Object Oriented Programming using C++ (Semester 2)

Module 1: C++ Fundamentals

- C vs C++
- Program structure
- Input/output streams

Module 2: Classes & Objects

- Class definition
- Objects and access specifiers
- Constructors and destructors

Module 3: Inheritance

- Types of inheritance
- Method overriding
- Virtual base classes

Module 4: Polymorphism

- Function overloading
- Operator overloading
- Virtual functions

Module 5: Templates & STL

- Function and class templates
- STL containers
- Iterators and algorithms

Module 6: Exception & File Handling

- Exception handling mechanism
- File input/output
- Applications

Programming in Java (Semester 2)

Module 1: Java Basics & JVM

- Java features
- JVM, JDK, JRE
- Java program structure

Module 2: OOP Concepts in Java

- Classes and objects
- Constructors
- Inheritance

Module 3: Polymorphism & Abstraction

- Method overriding
- Abstract classes
- Interfaces

Module 4: Packages & Exception Handling

- Built-in packages
- User-defined packages
- Exception hierarchy

Module 5: Multithreading

- Thread lifecycle
- Synchronization
- Inter-thread communication

Module 6: File Handling & Collections

- File I/O streams
- Serialization
- Java Collection Framework

Semester 3 – Cybersecurity Core & Lab Fundamentals

Foundational knowledge and practical skills for building a robust cybersecurity defense.

Module 1: Introduction to Cybersecurity

- Cybersecurity overview
- CIA Triad & domains
- Threat landscape
- Cyber kill chain
- Real-world breach examples

Module 2: Cybersecurity Ethics & Laws

- White, Grey & Black hat
- IT Act, GDPR, HIPAA
- Responsible disclosure
- Legal case examples
- Ethical boundaries

Module 3: Cyber Threats & Vulnerabilities

- Malware & phishing
- Social engineering
- Common attack vectors
- CVE & CVSS basics
- Threat modeling

Module 4: Networking Fundamentals

- OSI & TCP/IP models
- Network devices
- IP addressing & subnetting
- Network attacks
- Packet flow basics

Module 5: Linux & System Security

- Linux file system
- Users & permissions
- Process monitoring
- System hardening
- SSH security

Module 6: Reconnaissance & Traffic Analysis

- Passive & active recon
- OSINT fundamentals
- Nmap basics
- Wireshark analysis
- Traffic anomaly detection

Semester 4 – Offensive Security & Exploitation

Dive deeper into advanced techniques to identify, exploit, and mitigate vulnerabilities in various systems.

Module 7: Ethical Hacking Methodology

- Penetration testing phases
- Scope & rules of engagement
- Threat modeling
- Reporting standards
- Legal considerations

Module 8: Footprinting & Scanning

- OSINT techniques
- Host discovery
- Port scanning
- Service enumeration
- Scan analysis

Module 9: Vulnerability Assessment

- Vulnerability lifecycle
- CVE & CVSS scoring
- Nessus & OpenVAS
- Risk prioritization
- False positives

Module 10: Exploitation Tools

- Exploit-DB
- Metasploit framework
- Payload concepts
- Privilege escalation basics
- Post-exploitation overview

Module 11: Web Application Security

- OWASP Top 10
- SQL Injection
- XSS & CSRF
- Authentication flaws
- Secure coding basics

Module 12: Cloud & Container Security

- Cloud service models
- Shared responsibility
- Misconfiguration risks
- Docker security basics
- Virtualization threats

Semester 5 – Advanced Attacks & Digital Forensics

Deep dive into sophisticated cyber threats, exploitation techniques, and forensic investigation methods.

Module 13: Advanced Web Exploitation

- SSRF vulnerabilities
- Remote Code Execution (RCE)
- Insecure deserialization
- JWT attacks
- Logic flaws

Module 14: API, Mobile & Wireless Security

- OWASP API Top 10
- Mobile app threats & analysis
- WiFi attacks
- Rogue access points
- BLE vulnerabilities

Module 15: Digital Forensics

- Evidence collection & chain of custody
- Disk & memory forensics
- Timeline analysis
- Artifact investigation
- Reporting & analysis tools

Module 16: Malware Analysis & Reverse Engineering

- Static vs. dynamic analysis
- Malware behavior patterns
- Sandboxing concepts
- Reverse engineering basics
- Binary analysis tools

Module 17: Ransomware & Incident Analysis

- Ransomware lifecycle & attack vectors
- Detection strategies
- Containment methods
- Post-incident recovery
- Real-world case studies

Module 18: Capture The Flag (CTF)

- Web exploitation challenges
- Privilege escalation scenarios
- Forensics puzzles
- Reverse engineering tasks
- Team-based problem solving

Semester 6 – Enterprise Security & Capstone

Master enterprise-level security operations, advanced attack simulations, and comprehensive incident response, culminating in a real-world capstone project.

Module 19: Cloud & Kubernetes Security

- Cloud IAM
- Storage security
- Key management
- Kubernetes RBAC
- Container hardening

Module 20: SOC & Threat Hunting

- SOC workflows
- SIEM fundamentals
- Log correlation
- MITRE ATT&CK
- Threat hunting methods

Module 21: Blue Team Operations

- Defensive strategies
- Endpoint monitoring
- Incident containment
- Detection engineering
- Response playbooks

Module 22: Red Teaming & Adversary Simulation

- Attack simulation
- Social engineering
- Phishing campaigns
- Purple teaming
- Post-attack reporting

Module 23: Incident Response & Crisis Management

- IR lifecycle
- Ransomware response
- Communication flow
- Legal considerations
- Recovery planning

Module 24: Capstone Module

- Full attack simulation
- Defensive response
- Risk assessment
- Final reporting
- Industry presentation