KITECH

Knowledge & Innovation In Technology and Education

CYBER SECURITY & ETHICAL HACKING

NURTURE | UPGRADE | IGNITE

FEATURES OF PROGRAM

STUDY ONLINE

According to your availability

CERTIFICATIONS

Training completion certificate

BEGINNER FRIENDLY

No basic knowledge required

DOUBT CLEARING SESSIONS

Get Your Doubts Solved Fast

PROJECTS

Mini& Major projects

PLACEMENT GUIDANCE

Empowering Your Career

OUR MOTIVE

NURTURE

Guiding growth,inspiring futures

UPGRADE

Transfor Today upgrade for tomorrow

IGNITE

Ignite Ideas,Transform possibilites

ABOUT US

KI-TECH is an online education platform dedicated to providing students with exceptional learning opportunities and growth. Our mission is to address student’s needs and prepare them for success in their fields. With a wide range of programs and courses, we focus on delivering excellence through top-quality study materials and expert instructors, helping students achieve remarkable growth.

WHY CYBER SECURITY & ETHICAL HACKING

- Protects Data: Safeguards sensitive information from unauthorized access and breaches.
- Prevents Attacks: Identifies and mitigates vulnerabilities to prevent cyberattacks
- Ensures Privacy: Maintains user privacy and secures personal data.
- Compliance: Meets regulatory and legal requirements for data protection.
- Promotes Trust: Builds confidence among users and clients by ensuring secure systems.

TRAINING OUTCOMES

- Identify Threats: Recognize common cybersecurity threats and vulnerabilities.
- Basic Security Measures: Implement fundamental security practices and controls.
- Ethical Hacking Skills: Understand ethical hacking principles and methodologies.
- Vulnerability Assessment: Perform basic vulnerability assessments and penetration testing.
- Network Security: Secure and monitor network infrastructure.
- Incident Response: Respond to and manage security incidents effectively.
- Compliance Knowledge: Understand key regulations and compliance requirements.

TRAINING PATH WAY

- Introduction to Cybersecurity
- Basic Security Concepts
- Network Security Fundamentals
- Cryptography Basics
- Operating System Security
- Ethical Hacking Fundamentals
- Reconnaissance Techniques
- Vulnerability Assessment
- Penetration Testing Basics
- Web Application Security
- Incident Response and Management
- Compliance and Best Practices

Module-I

- Overview of Cybersecurity
- Types of Threats and Attacks
- Importance of Cybersecurity

Module-II

- Confidentiality, Integrity, and Availability (CIA) Triad
- Authentication and Authorization
- Security Policies and Procedures

Module-III

- Networking Basics (TCP/IP, OSI Model)
- Firewalls and Intrusion Detection Systems (IDS)
- Network Segmentation and VPNs

Module-IV

- Encryption and Decryption
- Symmetric vs. Asymmetric Encryption
- Hashing and Digital Signatures

Module-V

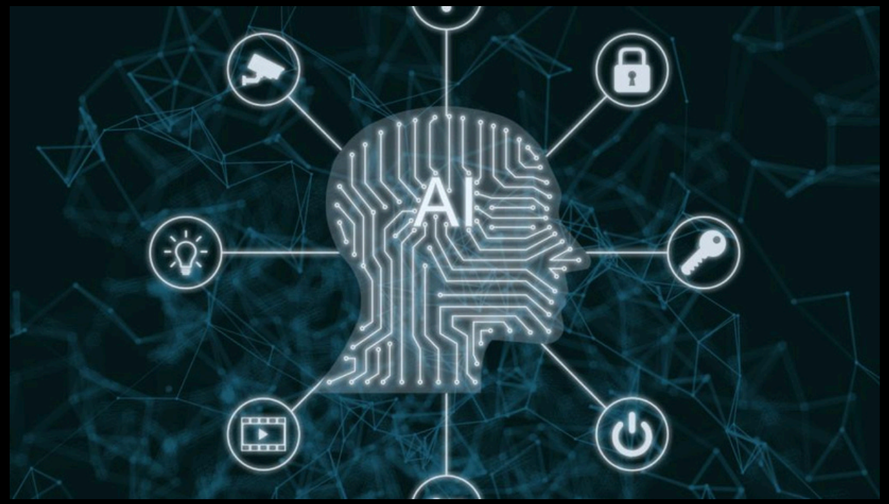
- Securing Windows and Linux Systems
- Patch Management
- File System Permissions

Module-VI

- Ethical Hacking vs. Black Hat Hacking
- Phases of Ethical Hacking (Reconnaissance, Scanning, Exploitation)
- Legal and Ethical Considerations

Module-VII

- Information Gathering
- Footprinting and Scanning
- Social Engineering



Module-VIII

- Identifying Vulnerabilities
- Using Vulnerability Scanners
- Interpreting Scan Results

Module-IX

- Penetration Testing Methodologies
- Exploit Development and Execution
- Post-Exploitation and Reporting

Module-X

- Common Web Vulnerabilities (XSS, SQL Injection)
- Web Application Firewalls (WAF)
- Secure Coding Practices

Module-XI

- Ethical considerations in AI development
- Bias and fairness in machine learning models
- Regulatory and compliance aspects

Module-XII

- Case studies and industry applications
- Building a complete AI project from data collection to deployment
- Presenting findings and solutions

Tools,Languages& softwares used

Sample Projects

- Network Vulnerability Scan
- Basic Firewall Configuration
- Password Strength Analyzer

CERTIFICATIONS