Heritage Status

A Comprehensive 45-Hour Cyber Security Course

St.Bede's College, Shimla | Beginner to Advanced | 45Hours

Cyber Security Fundamentals · Ethical Hacking · Network Security · Web Security · DigitalForensics · CyberLaws

COE

Course Objectives

This 45-hour programme equips you with the knowledge and hands-on skills to understand, identify, and respond to cyber threats 4 preparing you for real-world security roles and industry certifications.

Cyber Security Fundamentals

Core concepts, threat landscape, and security domains

Network & Web Security

Protocols, vulnerabilities, and defensive strategies

Ethical Hacking

Reconnaissance, scanning, and vulnerability assessment

Security Tools & Technologies

Kali Linux, Wireshark, Nmap, and more

Cyber Laws & Ethics

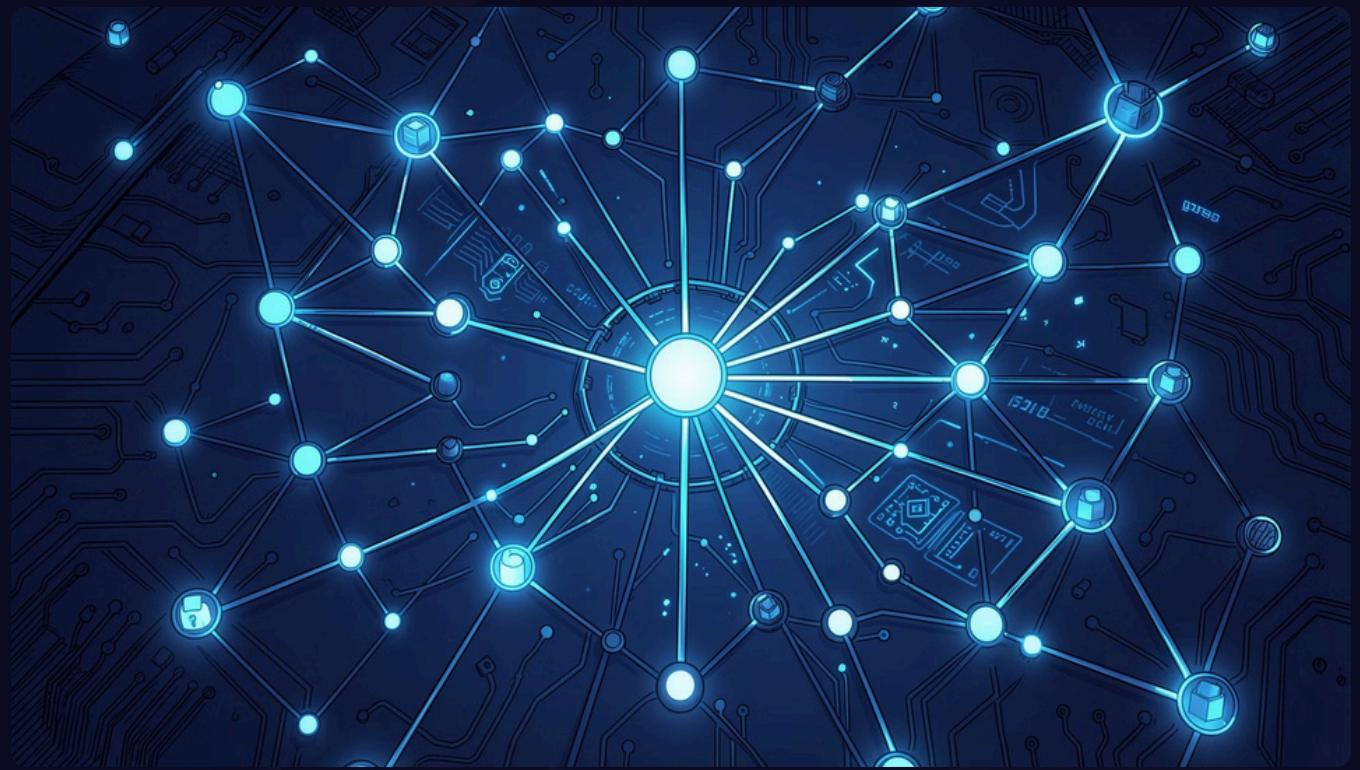
Indian IT Act, data privacy, and digital rights

Career Opportunities

SOC Analyst, Ethical Hacker, Security Consultant

MODULES 1-3

Cyber Security Fundamentals



Introduction to Cyber Security

- Cyber Crime vs. Cyber Security
- Security Domains & Career Paths

Cyber Threat Landscape

- Malware, Ransomware& Spyware
- Phishing, Botnets&Social Attacks

Networking Fundamentals

- OSI Model&TCP/IP
- DNS, HTTP/HTTPS, Ports & Protocols

MODULES 4-6

Security Principles & Data Protection

Information Security

The**CIATriad** formsthefoundation of all security decisions 4 Confidentiality, Integrity, and Availability. Risk management and authentication frameworks build on these principles.

Cryptography

Encryption,hashing, digital signatures, and SSL/TLS

protocolsprotectdataintransit and at rest.

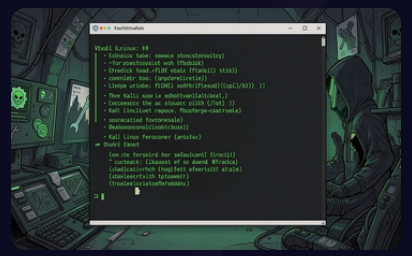
Password Security

Understanding password attacks, Multi-Factor Authentication (MFA), and Identity & Access Management (IAM) strengthens your first line of defence.

MODULES 7-9

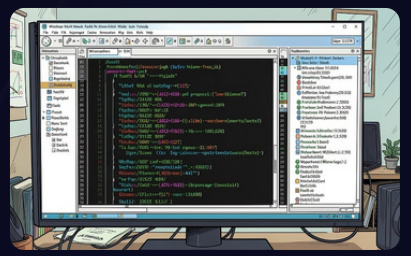
Hands-On Security Tools

Practicallabsareintegratedthroughout4youwilluseindustry-standard tools in real scenarios.



Kali Linux

Linux basics, security environment setup, and essential penetration testing commands



Wireshark

Packet analysis, network monitoring, and live traffic inspection for threat detection

Nmap

Network discovery, port scanning, and service detection to map vulnerable systems

MODULES 10-12

Web & Network Security

Web Security 4 OWASP Top 10

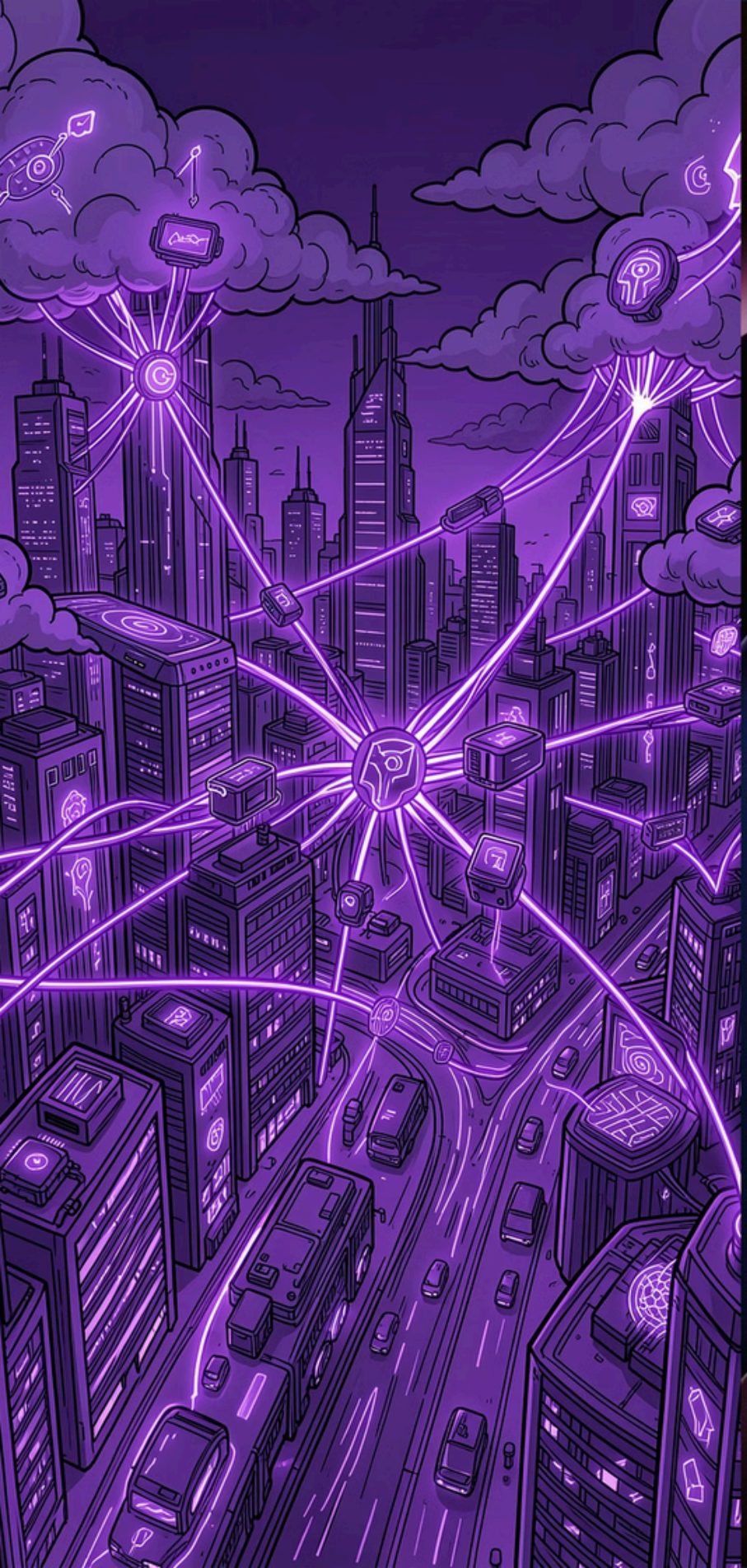
- SQL Injection& Cross-SiteScripting (XSS)
- CSRF & common web vulnerabilities

Ethical Hacking Concepts

- Reconnaissance & footprinting
- Scanning&vulnerability assessment

Network Security

- Firewalls, IDS/IPS &VPNs
- Wireless security best practices



MODULES 13-15

Human & Emerging Security

Social Engineering

Phishing,Vishing&Smishing 4 how attackers exploit human psychology

Cloud Security

Cloudrisks,sharedresponsibility model, and AWS & Azure security basics

Emerging Technologies

AIincybersecurity,IoTvulnerabilities, and blockchain for secure systems

Digital Forensics

Incidentresponseworkflows and evidence collection for cyber investigations

Cyber Laws & Career Opportunities

Indian Cyber Laws

- **ITAct 2000** 4legal framework for cybercrime in India
- Data privacy, digital rights & compliance obligations

Career Roles

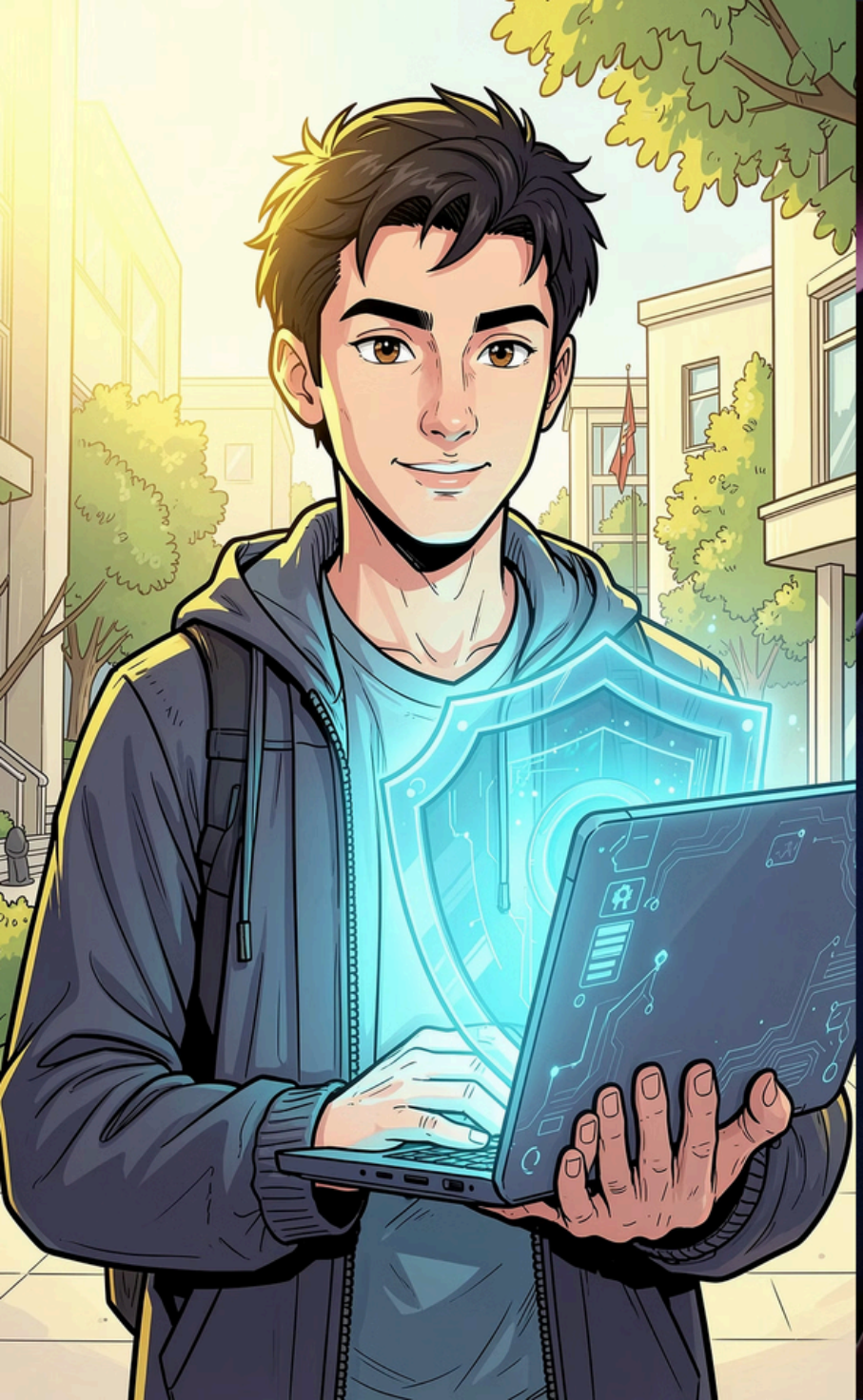
- SOCAnalyst · Security Analyst
- Ethical Hacker · Digital Forensics Analyst
- Security Consultant

Industry Certifications

Security+ · CEH · CiscoCyberOps · ISC^2 CC

Tools Covered & Assessment

- Kali Linux
- Wireshark
- Nmap
- Burp Suite
- OWASP Juice Shop
- Cisco Packet Tracer
- Nessus Essentials



By the End of This Course

- Understand core cyber security fundamentals and identify threats &vulnerabilities
- Use Kali Linux, Wireshark, and Nmap to analyse network traffic and detect anomalies
- Apply web security best practices and understand OWASP vulnerabilities
- Navigate Indian cyber laws, ethics, and prepare for entry-level security careers