Cyber Security

A 45-hour journey from beginner to intermediate level in cybersecurity, designed for St. Bede's College, Shimla.

Module 1: Foundations of Cyber Security

Introduction & Importance

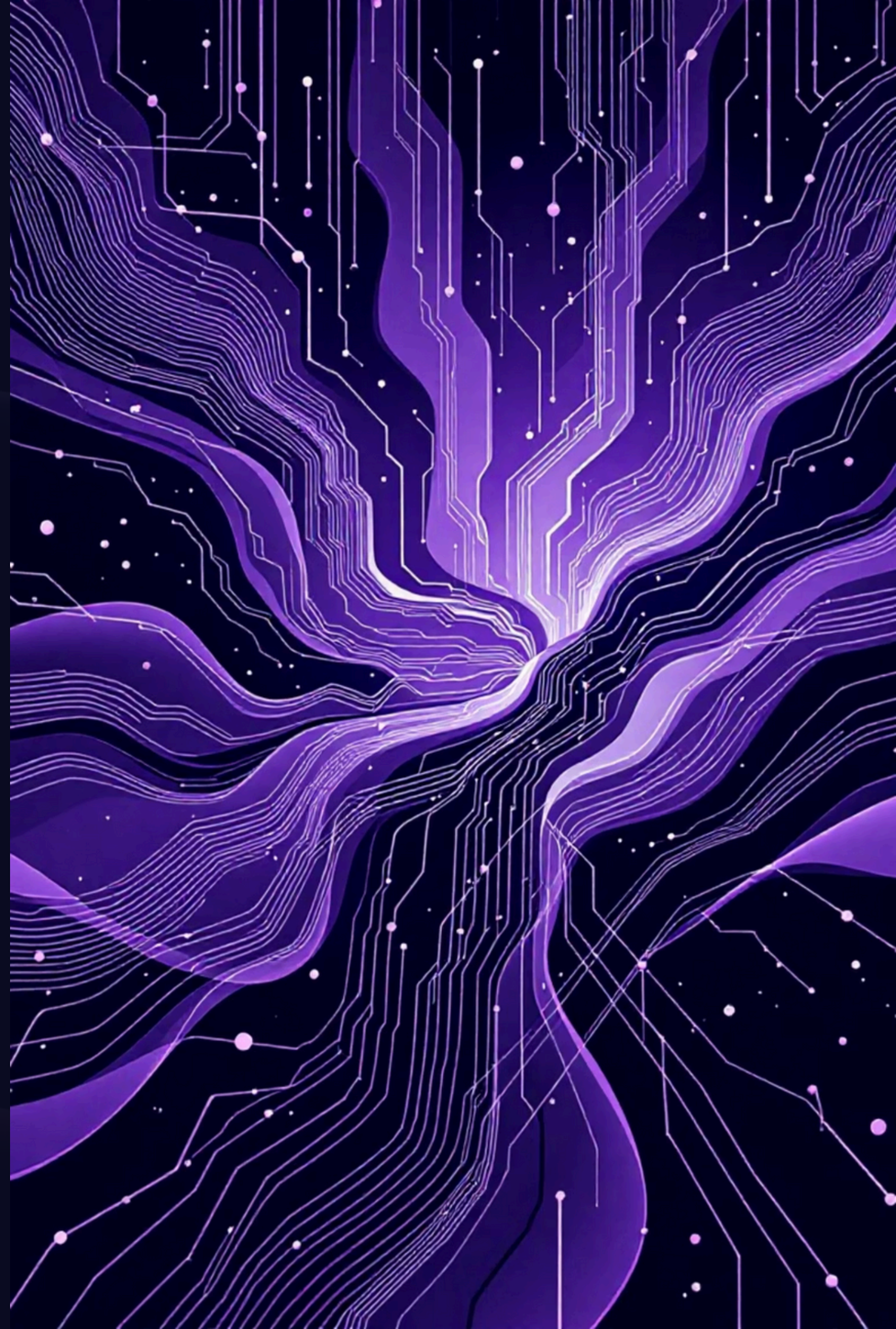
Understand basic concepts and why cybersecurity is crucial in the modern world.

Cybersecurity Landscape

Learn about common threats, attack vectors, and different types of cyber threats (phishing, ransomware, DDoS).

Cryptography Basics

Understand the fundamentals of cryptography and network security principles.



Module 2: Secure Communication Protocols

Focus on SSL/TLS and secure web browsing.

SSL and TLS Evolution

Understand the basics of SSL, its evolution into TLS, and why TLS is the preferred standard.

HTTPS and SSL Configuration

Learn how SSL enables HTTPS for secure web browsing. Includes setting up and configuring SSL on web servers.

VPN and Free Certificates

Explore how SSL is used in VPN technologies (SSL VPN) and how to use Let's Encrypt for free SSL setup.

Module 3: Ethical Hacking & Lab Setup

Introduction to Ethical Hacking

Understand the role and principles of ethical hacking in defense.

Setting Up a Lab Environment

Practical exercise: Set up a cybersecurity lab for hands-on exercises.

Kali Linux for Penetration Testing

Learn to use Kali Linux for ethical hacking, including installation on a virtual machine.

This module provides the essential practical environment for the course.

Module 4: Penetration Testing Techniques

A deep dive into the core methods used by security professionals.

1

Reconnaissance

Learn techniques for gathering information about targets.

2

Vulnerability Analysis

Analyze and identify weaknesses and vulnerabilities in systems.

3

Exploitation

Explore common exploitation techniques used to gain unauthorized access.

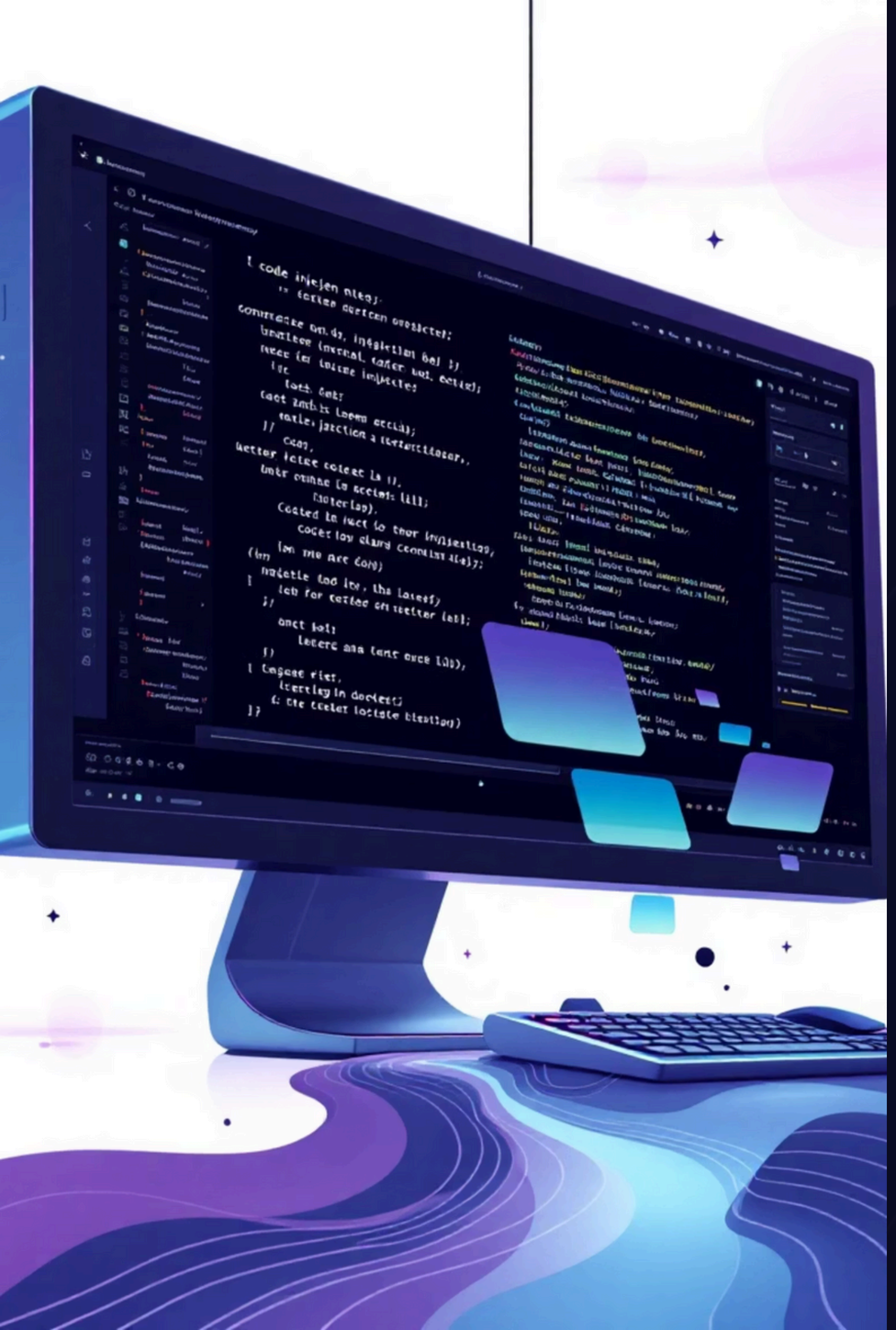
Module 5: Social Engineering and Malware

Social Engineering

- Understand and identify social engineering techniques.
- Learn how attackers manipulate human psychology through phishing and spear phishing.

Malware Analysis

- Understand different types of malware.
- Explore how specific malware types like Ransomware and Spyware function.



Module 6: Application and Network Security

1

Web Application Security

Learn about common web application vulnerabilities, including SQL Injection and Cross-Site Scripting (XSS).

2

Wireless Network Security

Understand how to secure wireless networks and best practices for securing Wi-Fi and Bluetooth networks.

Module 7: Advanced Security Domains

Cloud Security

Basics of securing cloud environments and Identity and Access Management (IAM).

Mobile & Physical Security

Understand security challenges in mobile environments and the importance of physical security.

Data Protection & Compliance

Importance of data protection, privacy, security audits, and compliance requirements.

Secure Software Development

Introduction to secure coding practices to prevent vulnerabilities.

Module 8: Incident Response and Threat Intelligence

- Incident Response: Learn how to respond effectively to security incidents.
- Threat Hunting: Proactively hunt for threats and understand Advanced Persistent Threats (APTs).
- SIEM: Understand the role of Security Information and Event Management systems.

Career Path and Final Project

1

Penetration Testing Fundamentals

Learn the basics and apply ethical hacking techniques in a controlled practice session.

2

Future Trends

Explore the latest cybersecurity trends and emerging threats.

3

Career Development

Understand career opportunities and developing a path in cybersecurity.

Final Project

Preparation and presentation of a final project to review and apply learned skills.