FULL CURRICULUM · 2026

Cybersecurity

Defend systems, data and people — and build a career doing it.

Every module, every lesson — the complete syllabus, end to end.

12	60	3	₹18,000
MODULES	LESSONS	MONTHS	FULL PROGRAMME

What this course covers

1 Level 1 · Beginner

Introduction · Linux & Python Fundamentals · Foundations of Information Security

1 month · **4** modules · **26** lessons · **₹5,500**

2 Level 2 · Intermediate

Network Defense & Penetration Testing · Data Protection and Cryptography · Governance, Risk & Compliance (ISO, SMS)

1 month · **3** modules · **19** lessons · **₹6,500**

3 Level 3 · Advanced

Securing Emerging Technologies · Security Operations Center: Overview & Roles · SIEM Architecture & Hands-On Splunk

1 month · **5** modules · **15** lessons · **₹6,000**

The whole journey

This is the complete syllabus for Cybersecurity — 12 modules and 60 lessons, in the order you will learn them. The level markers show how far each stage carries you, but the curriculum runs as one continuous path from the first lesson to the last.

1

LEVEL 1

Beginner

Introduction · Linux & Python Fundamentals · Foundations of Information Security

1 month · **4** modules · **26** lessons · **₹5,500**

1. Introduction

5 lessons

- Introduction to Me & the Course
- CyberSecurity Jobs
- WannaCry Ransomware Introduction
- WannaCry Attack (SETTING UP A TEST ENVIRONMENT)
- System Hacking & WannaCry Execution

2. Linux & Python Fundamentals

7 lessons

- Introduction to Linux
- File Permissions and Ownership
- Text Editors in Linux
- Essential Linux File Management Commands
- Introduction to servers
- Bash Scripting - (Variables)
- Bash Scripting - (Arrays & Conditional Statements)

3. Foundations of Information Security

3 lessons

- Information Gathering (Active and Passive)
- Common Threat Vectors : Malicious Code and Phishing
- Modern Attacks Methodologies: From Social to Technical

4. Application Security and Penetration Testing

11 lessons

- How Websites Works?
- WebApp Security Concepts (Cookies, Sessions, Authentication Mechanisms)
- Hacking Your First Website
- Ubuntu Setup & Linux File Sharing
- Introduction to Apache: Hosting Your First Website
- Website Defacement Practical
- Setting Up Burpsuite
- OWASP TOP 10 (2025 Edition) Part 1
- OWASP TOP 10 (2025 Edition) Part 2
- Bug Bounty Workflow Part 1(Reconnaisance & SQL Injection)
- Bug Bounty Workflow Part 2 (CSRF & RCE)

2

LEVEL 2

Intermediate

Network Defense & Penetration Testing · Data Protection and Cryptography · Governance, Risk & Compliance (ISO, SMS)

1 month · **3** modules · **19** lessons · **₹6,500**

5. Network Defense & Penetration Testing

11 lessons

- Network Types and Topologies
- Network Devices & Fundamentals
- Network Security Concepts
- Attacker Profiles & Cyber KillChain
- Black Box vs Grey Box VAPT
- Nessus Installation & Setup
- Setting Up Metasploitable in VirtualBox
- Scanning : Nmap Service Discovery
- Hands On : End-to-End Black Box VAPT
- Hands On :End to End Grey Box VAPT
- Analysis : Detailed Wireshark Investigation

6. Data Protection and Cryptography

3 lessons

- Cryptography Fundamentals
- Data Protection and Security Principles (Part 1)
- Data Protection & Security Principles [Part 2]

7. Governance, Risk & Compliance (ISO, SMS)

5 lessons

- GRC Fundamentals: An Overview
- Governance: Principles and Frameworks
- Risk Management: Identification and Mitigation
- Compliance: Standards and Regulatory Requirements
- The DPDP Act 2023: Privacy and Data Protection

3

LEVEL 3

Advanced

Securing Emerging Technologies · Security Operations Center: Overview & Roles · SIEM Architecture & Hands-On Splunk

1 month · **5** modules · **15** lessons · **₹6,000**

8. Securing Emerging Technologies

4 lessons

- The Dual-Edge of AI: Offensive Evolution and Defensive Pillars
- Securing LLMs: Understanding Privileged Intermediaries and Prompt Injection
- Hands-on Lab: Breaking Chatbots with Prompt Injection Attacks
- IoT Security Fundamentals: MQTT Packet Manipulation

9. Security Operations Center: Overview & Roles

2 lessons

- SOC Operations: People, Processes, and Defensive Technology
- Advanced Detection Frameworks and Splunk SIEM Implementation

10. RCA (Root Cause Analysis) & Cyber Breach Investigation

3 lessons

- Incident Respone Management
- Digital Forensics Process
- Data Aquisition (Volatile & Non-Volatile)

11. SIEM Architecture & Hands-On Splunk

3 lessons

- Setting Up Splunk (Installation & Configuration)
- Investigating Phishing Attack on Splunk
- Wazuh Installation and Bruteforce Incident Analysis

12. Bonus - Job Prep Module

3 lessons

- Cybersecurity Projects (VAPT,SOC,Forensics)
- The Professional Toolkit Resume, Linkedin, Conferences & CTFs
- Building your Portfolio Website!

Certificates & what comes next

You receive a certificate at the end of every level you finish. Join for a single level or the full programme — the choice is yours. Learners who stand out may be invited to work on live client projects as interns; these places are merit-based, limited, and depend on projects being available.