CYBER SECURITY
CAREER LAUNCHPAD

Start Your Cybersecurity Journey with Real-World Practical Skills

BEGINNER TO PRACTICAL CYBERSECURITY TRAINING

ABOUT THE PROGRAM

Build Strong Cybersecurity Foundations

Cyber Security Career Launchpad is a beginner-friendly, practical training program designed to help students understand how cybersecurity works in real-world environments. This program focuses on building a strong foundation in networking, web security, and ethical hacking concepts while providing hands-on exposure to tools and attack methodologies used by professionals.

Unlike traditional courses, this program follows a practical-first approach where students learn by doing, not just theory. By the end of the training, participants will clearly understand how vulnerabilities are identified, exploited, and reported in real-world scenarios.

Program Structure	
Duration: 3 Months	Hands-on Practical Sessions
Classes: Weekend (Sat & Sun)	Real-World Examples
Mode: 100% Online	Industry-Oriented Learning
Level: Beginner Friendly	Certificate on Completion

WHY CHOOSE THIS PROGRAM

- ✓ **Learn cybersecurity from scratch with a structured approach**
- ✓ **Focus on practical learning instead of theory**
- ✓ **Understand real-world attack scenarios**
- ✓ **Work with tools used by professional pentesters**
- ✓ **Build confidence to move into advanced cybersecurity domains**

COURSE CONTENT

Structured Learning from Basics to Practical Cybersecurity Skills

---

[01] Cybersecurity Industry & Career Roadmap

Understand the cybersecurity landscape, different career paths, and how professionals work in real-world environments. This module helps you plan your journey from beginner to security professional.

- Introduction to Cybersecurity Domains
- Career Paths (VAPT, SOC, Red Team)
- Real-World Attack Scenarios
- Industry Expectations & Growth

[02] Hacker Mindset & Attack Methodology

Develop an attacker's mindset and learn structured approaches used in penetration testing. This module builds the foundation for thinking like a hacker.

- Reconnaissance Techniques
- Attack Surface Identification
- Exploitation Workflow
- Attack Chaining Concepts

[03] Networking Fundamentals for Hackers

Learn how systems communicate and how attackers exploit network-level weaknesses. This module is essential for understanding real-world attack flows.

- TCP/IP & OSI Model
- Ports, Protocols & Services
- HTTP & DNS Deep Dive
- Packet Flow Analysis

[04] Linux & Command Line Mastery

Gain hands-on experience with Linux, the core operating system for cybersecurity professionals. Learn essential commands and system handling.

- Linux Navigation & Commands
- File Permissions & Ownership
- Process & Service Management
- Networking Commands

COURSE CONTENT

Structured Learning from Basics to Practical Cybersecurity Skills

---

[05] Lab Setup & Security Tools

Set up your own cybersecurity lab and learn essential tools used in penetration testing. This module prepares you for practical execution.

- Kali Linux Setup
- Burp Suite Configuration
- Proxy Setup & Browser Tools
- Introduction to Docker

[06] Web Application Architecture & Recon

Understand how web applications work and how attackers gather information before launching attacks. This is the base for web security testing.

- Client-Server Architecture
- APIs & JSON Handling
- Authentication vs Authorization
- Subdomain & Directory Enumeration

[07] Core Web Vulnerabilities

Learn and exploit the most common vulnerabilities found in web applications. This is where real hacking starts.

- SQL Injection (Practical)
- Cross-Site Scripting (XSS)
- IDOR Vulnerabilities
- Authentication & Session Issues

[08] Burp Suite & Traffic Manipulation

Master Burp Suite to intercept and manipulate web traffic. Learn how professionals test applications manually.

- Intercepting Requests
- Modifying Parameters
- Repeater & Intruder
- Request Analysis

COURSE CONTENT

Structured Learning from Basics to Practical Cybersecurity Skills

---

[09] Network Scanning & Service Enumeration

Identify entry points and services running on systems using scanning techniques. This module teaches reconnaissance at the network level.

- Nmap Basics & Advanced Scans
- Port Scanning Techniques
- Service & Version Detection
- Banner Grabbing

[10] Exploitation & Privilege Escalation Basics

Learn how vulnerabilities are exploited and how attackers gain higher privileges in systems.

- Weak Credential Attacks
- File Upload Exploitation
- Misconfiguration Abuse
- Basic Privilege Escalation

[11] CTF Approach & Real-World Attack Strategy

Apply your knowledge in real-world style challenges and develop problem-solving skills required for cybersecurity roles.

- Introduction to CTF
- Machine Solving Approach
- Attack Strategy Development
- Writeup Methodology

[12] Docker for Cyber Range & Lab Building

Learn how to create isolated environments for testing and building vulnerable systems using Docker.

- Docker Basics
- Running Containers
- Lab Environment Setup
- Multi-Service Labs

[13] Vulnerability Engineering

Understand how vulnerabilities are created and how systems become insecure. This module builds a deeper understanding of security flaws.

- Designing Vulnerable Apps
- Input Validation Weaknesses
- Authentication Flaws
- Misconfiguration Setup

COURSE CONTENT

Structured Learning from Basics to Practical Cybersecurity Skills

---

[14] Cyber Range & CTF Design

Design your own hacking challenges and environments. This module helps you think like both attacker and defender.

- Flag-Based Systems
- Scenario Design
- Difficulty Levels
- Attack Chain Design

[15] Exploiting Self-Created Labs

Test and exploit your own created environments. This builds confidence and real-world understanding.

- Lab Testing & Debugging
- Exploitation Validation
- Peer-to-Peer Attacks
- Scenario Testing

[16] VAPT Reporting & Documentation

Learn how to write professional security reports used in real organizations. Communication is a key skill in cybersecurity.

- Writing Observations
- Root Cause Analysis
- Business Impact Writing
- Mitigation Recommendations

[17] Portfolio, GitHub & Career Launch

Prepare for real-world opportunities by building your portfolio, improving your profile, and getting ready for job roles.

- GitHub Project Upload
- CTF Writeups
- Resume Building
- LinkedIn Optimization

Who Should Join This Program?

- ✓ College Students (any stream)
- ✓ Beginners in Cybersecurity
- ✓ Career Switchers
- ✓ IT / Non-IT Learners
- ✓ Anyone interested in Ethical Hacking

What You Will Achieve

- ✓ Strong cybersecurity foundation
- ✓ Understanding of real-world attack techniques
- ✓ Hands-on experience with tools
- ✓ Ability to identify basic vulnerabilities
- ✓ Confidence to move to advanced cybersecurity

Certification

- ✓ Internship Certificate from PentestHint
- ✓ Proof of practical learning
- ✓ Useful for internships & career growth

Start Your Cybersecurity Journey Today

Enroll Now

+91 7062317451 | info@pentesthint.com | www.pentesthint.com