

SkillNexa Cybersecurity Academy

Cybersecurity Practitioner

Ethical Hacking & Cyber Defense

Program Level: Practitioner

Total Duration: 96 Hours

Delivery: Cohort-Based + Instructor-Led + Hands-On Labs

Pathway: Foundation → Practitioner

Program Goal

These programs emphasize:

- Cyber defense
- Network security
- Vulnerability assessment
- Security operations
- Ethical hacking principles

Students transition from cybersecurity awareness to practical defensive security skills.

Students learn how attackers identify weaknesses and how cybersecurity professionals protect systems using security controls, monitoring, and ethical testing techniques.

Program Structure Overview

Module	Topic	Hours
Module 1	Security Fundamentals	16 Hours
Module 2	Ethical Hacking Fundamentals	24 Hours
Module 3	Network Security	24 Hours
Module 4	Web Security	20 Hours
Module 5	Cyber Defense Challenge	12 Hours

Total

96 Hours

Course Curriculum

MODULE 1 — SECURITY FUNDAMENTALS

1.1 Cybersecurity Principles & Information Security

LAB 1.1 — CIA Security Analysis

1.2 Security Threats & Risk

LAB 1.2 — Risk Assessment

1.3 Authentication & Identity Management

LAB 1.3 — Authentication Design

1.4 Authorization & Access Control

LAB 1.4

1.5 Encryption Fundamentals

LAB 1.5 — Protecting Digital Information

1.6 Module 1 Mini Project

MODULE 1 ASSESMENT

MODULE 2 — ETHICAL HACKING FUNDAMENTALS

2.1 Introduction to Ethical Hacking

LAB 2.1

2.2 Reconnaissance Fundamentals

LAB 2.2

2.3 Vulnerability Discovery

LAB 2.3

2.4 Security Testing Concepts

LAB 2.4

2.5 Security Testing Tools

LAB 2.5

2.6 Ethical Hacking Mini Project

MODULE 2 ASSESSMENT

MODULE 3 — NETWORK SECURITY

3.1 Network Security Fundamentals

LAB 3.1

3.2 Firewalls & Network Protection

LAB 3.2

3.3 VPN & Secure Communication

LAB 3.3

3.4 IDS/IPS & Threat Detection

LAB 3.4

3.5 Secure Network Protocols

LAB 3.5

3.6 Network Security Project

MODULE 3 ASSESSMENT

MODULE 4 — WEB SECURITY

4.1 Introduction to Web Applications

LAB 4.1

4.2 Web Application Vulnerabilities

LAB 4.2

4.3 OWASP Top 10 Concepts

LAB 4.3

4.4 Secure Coding Practices

LAB 4.4

4.5 Web Security Project

MODULE 4 ASSESSMENT

MODULE 5 — CYBER DEFENSE CHALLENGE

5.1 Capture-the-Flag Fundamentals

LAB 5.1

5.2 Cyber Defense Simulation

LAB 5.2

5.3 Final Cyber Defense Challenge

5.4 Final Practitioner Project

MODULE 5 ASSESSMENT

FINAL COURSE ASSESSMENT