CYBER SECURITY TRAINING PROGRAM

CYBER SKILLSHALA

Job-Oriented Cybersecurity Training Program

www.cyberskillshala.com

CYBER SKILLSHALA

Job-Oriented Cybersecurity Training Program

Program Overview

Cyber Skillshala offers comprehensive, hands-on **Cybersecurity & Ethical Hacking training programs** that take learners from beginner level to industry-ready professionals. Designed with real-world scenarios in mind, these programs combine theory, interactive labs, live projects, and career guidance to prepare students for the fast-evolving cybersecurity landscape.

Course Duration

Program Format:

- Duration: **3 Months | 6 Months | 1 Year ***
- Schedule: **5 Days/Week, 1 Hour/Day**

Why Cyber Skillshala?

- **Expert Faculty:** Training delivered by experienced cybersecurity professionals with real-world expertise.
- **Practical Exposure:** Hands-on labs, live international projects, and real-time attack simulations.
- **Career-Oriented:** Personalized mentorship, resume building, interview prep, and placement assistance.
- **Backed by Industry:** Supported by a reputed Australia-based SAAS solutions company.
- **AI-Infused Curriculum:** Stay ahead with AI-powered cybersecurity tools and techniques integrated into learning.

We bridge the gap between traditional academic knowledge and real industry requirements, ensuring you're prepared not just to learn, but to lead.

- Terms & Conditions Apply

3-Months Job-Oriented Certification

Module 1: Introduction to Cybersecurity
- Cyber Threats & Attack Vectors
- Role of AI in Cybersecurity

Module 2: Security Concepts
- Traditional vs. AI Security Techniques
- Intrusion Detection & Prevention Systems

Module 3: Networking Basics
- OSI & TCP/IP Models
- Firewalls, IDS/IPS & AI-based Network Security

Module 4: Ethical Hacking Foundations
- Hacking Concepts & Cyber Kill Chain

Module 5: Lab Setup
- Penetration Testing Lab Creation
- Hands-on Kali Linux Setup

Module 6: Reconnaissance & Enumeration
- OSINT, Social Media, IoT Search
- Advanced Google Dorks, Wayback Machine

AI-Powered Recon Techniques

Module 7: Scanning Techniques
- Host Discovery
- Automated Scanning Tools

Module 8: Vulnerability Assessment
- Manual & Automated Vulnerability Testing
- AI in Vulnerability Detection

Module 9: Social Engineering
- Psychology of Hacking
- Phishing Techniques

Module 10: System Hacking
- OS Hacking (Windows & Linux)
- Privilege Escalation & AI-Assisted Password Cracking

Module 11: Sniffing (MITM Attacks)
- Concepts & Packet Analysis

Module 12: Malware Analysis
- Malware Deployment & Detection
- OS/Mobile Malware Tactics

Module 13: Cryptography
- Encryption, Decryption
- Cryptography in AI Security

Module 14: Penetration Testing Basics
- PenTesting Lifecycle & Methodologies

Module 15: Web Application Penetration Testing
- OWASP Top 10
- API Testing & AI-Powered Exploits

Module 16: Mobile Application Security
- OWASP Mobile Top 10
- Mobile App Testing Automation

Module 17: Network Penetration Testing
- Tools & Techniques
- AI in Network Traffic Analysis & Evasion

Module 18: Wireless Network Security
- Wireless Attacks & Defense Mechanisms

Module 19: Cloud Security & Pentesting
- Cloud Concepts, Attacks, Monitoring

Module 20: Capture The Flag (CTF)
- Live CTF Challenges & Real-Time Practice

Module 21: Specializations
- Security Research & Bug Bounty Skills

Module 22: Resume & Portfolio Development
- Showcasing Projects & AI-Cyber Synergy

Module 23: Interview Preparation
- Technical Q&A, Soft Skills
- AI Trends in Cyber Security

Module 24: Certification Practice
- Simulated Exams for Industry Certifications

6-Months Advanced Certification

FOUNDATION & CORE CONCEPTS

Module 1: Introduction to Cyber Security
- Cyber threats, attack landscape
- Cyber security domains & career paths

Module 2: Cyber Threats & Attack Vectors
- Malware, phishing, ransomware
- Modern threat actors & tactics

Module 3: Role of AI in Cyber Security
- AI-driven attacks & defenses
- Machine learning use cases in security

Module 4: Security Fundamentals & Principles
- CIA Triad, risk, threat & vulnerability
- Security policies & best practices

Module 5: Traditional vs AI-Based Security
- Signature-based vs behavior-based detection
- AI in SOC & threat detection

NETWORKING & INFRASTRUCTURE SECURITY

Module 6: Networking Basics for Security
- OSI & TCP/IP models
- Network communication & protocols

Module 7: Network Devices & Defense
- Firewalls, IDS, IPS
- AI-based network monitoring

Module 8: Network Attacks & Defense Strategies
- ARP spoofing, DNS attacks
- Network hardening techniques

ETHICAL HACKING & LAB ENVIRONMENT

Module 9: Ethical Hacking Concepts
- Hacker types & ethics
- Legal boundaries & authorization

Module 10: Cyber Kill Chain & MITRE ATT&CK
- Attack lifecycle
- Mapping real-world attacks

Module 11: Penetration Testing Lab Setup
- Kali Linux installation
- Vulnerable machines & lab configuration

RECONNAISSANCE & SCANNING

Module 12: Information Gathering Techniques
- Passive vs active reconnaissance
- Footprinting methods

Module 13: OSINT & Digital Footprinting
- Social media intelligence
- IoT & exposed asset discovery

Module 14: Advanced Recon Techniques
- Google Dorks
- Wayback Machine
- AI-powered reconnaissance

Module 15: Scanning & Enumeration
- Host discovery
- Port & service enumeration

VULNERABILITY & EXPLOITATION

Module 16: Vulnerability Assessment Fundamentals
- Vulnerability lifecycle
- CVE, CVSS & risk scoring

Module 17: Automated & Manual Vulnerability Testing
- Scanners & manual validation
- False positive elimination

Module 18: AI in Vulnerability Detection
- Pattern analysis
- Intelligent vulnerability prioritization

SYSTEM, NETWORK & WIRELESS ATTACKS

Module 19: System Hacking
- Windows & Linux attacks
- Privilege escalation techniques

Module 20: Password Attacks & Credential Abuse
- Brute force & credential stuffing
- AI-assisted password analysis

Module 21: Sniffing & MITM Attacks
- Packet capture & traffic analysis
- Man-in-the-Middle attacks

Module 22: Wireless Network Security
- Wi-Fi attacks
- Wireless defense mechanisms

APPLICATION & CLOUD SECURITY

Module 23: Web Application Security
- OWASP Top 10
- Manual & automated testing

Module 24: API Security Testing
- API vulnerabilities
- Token & authorization flaws

Module 25: Mobile Application Security
- OWASP Mobile Top 10
- Android security testing basics

Module 26: Cloud Security Fundamentals
- Cloud service models
- Common misconfigurations

Module 27: Cloud Attacks & Monitoring
- Cloud attack vectors
- Logging & monitoring basics

MALWARE, CRYPTOGRAPHY & ADVANCED TOPICS

Module 28: Malware Concepts & Analysis
- Malware types & behavior
- OS & mobile malware techniques

Module 29: Cryptography & Secure Communication
- Encryption & hashing
- Cryptography in AI security systems

PRACTICE, CAREER & INDUSTRY READINESS

Module 30: Capture The Flag (CTF)
- Live attack simulations
- Practical security challenges

Module 31: Security Research & Bug Bounty Basics
- Vulnerability research
- Responsible disclosure

Module 32: Reporting, Resume & Interview Preparation
- Penetration testing reports
- Resume & portfolio building
- Technical & HR interview preparation

1-Year Master Certification

LEVEL 1 – Cyber Security Foundations

(Semester I – Months 1–3)

Objective: Build strong fundamentals in cyber security, systems, networking, and security concepts.

COURSE 1: FUNDAMENTALS OF CYBER SECURITY

Module 1: Introduction to Cyber Security

- Definition and scope of cyber security
- Evolution of cyber threats
- Cyber security domains and roles
- Career pathways in cyber security

Module 2: Cyber Threat Landscape

- Malware, ransomware, phishing, DDoS
- Insider threats and APTs
- Real-world cyber attack case studies

Module 3: Role of AI in Cyber Security

- AI-based threat detection
- Machine learning in security analytics
- Limitations and risks of AI in cyber security

COURSE 2: SECURITY PRINCIPLES & RISK MANAGEMENT

Module 4: Core Security Principles

- CIA Triad
- Authentication, authorization, accounting
- Defense-in-depth strategy

Module 5: Risk & Vulnerability Management

- Threat modeling
- Risk assessment methodologies
- Vulnerability lifecycle

Module 6: Security Policies & Governance

- Security policies and procedures
- Awareness and training
- Introduction to governance frameworks

COURSE 3: NETWORKING & OPERATING SYSTEM SECURITY

Module 7: Networking Fundamentals

- OSI and TCP/IP models
- Network protocols and ports
- Data flow and packet structure

Module 8: Network Security Architecture

- Firewalls, IDS, IPS
- Network segmentation
- AI-based network monitoring

Module 9: Operating System Security

- Linux fundamentals for security
- Windows security architecture
- User privileges and access control

COURSE 4: ETHICAL HACKING FOUNDATIONS & LAB SETUP

Module 10: Ethical Hacking Concepts

- Hacker classifications
- Ethical hacking methodology
- Legal boundaries and compliance

Module 11: Cyber Kill Chain & MITRE ATT&CK

- Attack lifecycle stages
- Mapping real-world attacks

Module 12: Penetration Testing Lab Setup

- Kali Linux installation
- Vulnerable machines
- Tool introduction and usage

1-Year Master Certification

LEVEL 2 – Offensive Security & Penetration Testing

(Semester I – Months 4–6)
Objective: Develop hands-on skills in reconnaissance, exploitation, and reporting.

COURSE 5: RECONNAISSANCE & OSINT

Module 13: Information Gathering
- Passive and active reconnaissance
- Footprinting techniques

Module 14: OSINT Techniques
- Social media intelligence
- IoT and exposed asset discovery

Module 15: Advanced Recon Techniques
- Google Dorks
- Wayback Machine
- AI-powered reconnaissance

COURSE 6: SCANNING, ENUMERATION & VULNERABILITY ASSESSMENT

Module 16: Scanning Techniques
- Host discovery
- Port and service scanning

Module 17: Enumeration
- OS and service enumeration
- Banner grabbing

Module 18: Vulnerability Assessment
- Manual vs automated testing
- CVE, CVSS scoring
- AI-based vulnerability prioritization

COURSE 7: SYSTEM, NETWORK & WIRELESS ATTACKS

Module 19: System Hacking
- Windows and Linux attacks
- Privilege escalation

Module 20: Network Attacks
- Sniffing and MITM
- DNS and ARP attacks

Module 21: Wireless Security
- Wi-Fi attack techniques
- Wireless defense mechanisms

COURSE 8: WEB, API & MOBILE APPLICATION SECURITY

Module 22: Web Application Security
- OWASP Top 10
- Manual and automated testing

Module 23: API Security
- Authentication and authorization flaws
- Token and session attacks

Module 24: Mobile Application Security
- OWASP Mobile Top 10
- Android security testing basics

LEVEL 3 – Defensive Security & Enterprise Protection

(Semester II – Months 7–9)
Objective: Train students in detection, monitoring, response, and enterprise security.

COURSE 9: SOC OPERATIONS & INCIDENT RESPONSE

Module 25: SOC Fundamentals
- SOC architecture
- Roles and responsibilities

Module 26: SIEM & Log Management
- Log sources and correlation
- Alert triaging

Module 27: Incident Response
- IR lifecycle
- Containment and recovery

COURSE 10: MALWARE, ENDPOINT & DATA SECURITY

Module 28: Malware Concepts
- Malware types and behavior
- Malware delivery methods

Module 29: Endpoint Security
- Antivirus, EDR, XDR
- Endpoint hardening

Module 30: Data Security & Cryptography
- Encryption and hashing
- Secure data handling

COURSE 11: CLOUD SECURITY & COMPLIANCE

Module 31: Cloud Security Fundamentals
- Cloud service models
- Shared responsibility model

Module 32: Cloud Threats & Monitoring
- Misconfigurations
- Logging and visibility

Module 33: Compliance & Governance
- ISO 27001
- SOC 2, GDPR basics

1-Year Master Certification

LEVEL 4 – Specialization, Internship & Capstone

(Semester II – Months 10–12)

Objective: Prepare students for real-world cyber security roles.

COURSE 12: ADVANCED SECURITY, RESEARCH & SPECIALIZATION

Module 34: Advanced Penetration Testing

- Red team concepts
- Advanced exploitation techniques

Module 35: Bug Bounty & Security Research

- Vulnerability discovery
- Responsible disclosure

COURSE 13: CAPSTONE PROJECT & INTERNSHIP

Module 36: Capstone Project

- Real-world security scenario
- Risk analysis and mitigation

Module 37: Internship / Industry Exposure

- Live security operations
- Mentored practical work

COURSE 14: PROFESSIONAL READINESS & CERTIFICATION PRACTICE

Module 38: Security Reporting & Documentation

- Client-style penetration testing reports

Module 39: Career Preparation

- Resume and portfolio development
- Interview preparation

Module 40: Certification Practice

- Simulated exams
- Industry certification orientation

PROGRAM OUTCOMES

Graduates of this certification will be able to:

- Identify and assess cyber security risks
- Perform penetration testing and vulnerability assessment
- Analyze security incidents and recommend controls
- Work in SOC, VAPT, and security analyst roles
- Demonstrate professional and ethical security practices

CYBER SKILLSHALA

CONTACT US

+91 9220580068

WEBSITE

www.cyberskillshala.com