// LEARNING PATH

# Cybersecurity Roadmap

Foundation to Core Offensive Security to Specializations, converging on the CISE expert program.

**12 COURSES · 191 MODULES · 4 TIERS · 18 MONTHS (CISE)**

// FULL MODULE BREAKDOWN

# Every course, every module

## 01 Foundation

5 courses

### 1. Enterprise Windows Infrastructure Security

BEGINNER TO ADVANCED · 14 MODULES

1. Networking Fundamentals
2. Lab Setup and Virtualization
3. Windows Server Management
4. Dynamic Host Configuration Protocol (DHCP)
5. Domain Name System (DNS)
6. Windows Operating System Administration
7. Active Directory Domain Services (AD DS)
8. Group Policy Objects (GPO)
9. File Services & Distributed File System (DFS)
10. Web Server (IIS)
11. FTP Server Administration
12. Proxy Server Administration
13. Remote Access and VPN Configuration
14. Windows Server Backup, Restore & Recovery

### 2. Linux Administration & Server Hardening

BEGINNER TO ADVANCED · 18 MODULES

1. Introduction to Linux
2. Linux Basic Commands
3. Text Editors
4. String Processing & Finding Files
5. Users, Groups & Permissions
6. Package Management
7. File System & Disk Management
8. Network Configuration & Controlling Services
9. Security, Process Management & Monitoring
10. Dynamic Host Configuration Protocol (DHCP)
11. Domain Name System (DNS)
12. Apache Web Server
13. FTP Server (VSFTPD)
14. Samba/SMB/CIFS Server
15. NFS Server
16. Telnet & Remote Desktop Server
17. Proxy Server
18. TFTP & PXE Boot Server

### 3. Secure PHP Development

BEGINNER TO INTERMEDIATE · 19 MODULES

1. Introduction to PHP
2. First Steps in PHP
3. Variables & Data Types
4. Arrays & Associative Arrays
5. Control Structures
6. Loops & Iterations
7. User-Defined Functions
8. Scope & Global Variables
9. Debugging & Error Handling
10. Building Dynamic Web Pages
11. Working with Forms & Validation
12. Cookies & Sessions
13. MySQL Fundamentals
14. CRUD Operations
15. PHP & MySQL Integration
16. SQL Injection Prevention
17. Prepared Statements
18. File & Directory Handling
19. Secure PHP Development Practices

## 4. Secure WordPress Administration

**BEGINNER · 17 MODULES**

1. Introduction to WordPress
2. WordPress Installation
3. WordPress Dashboard Management
4. User Roles & Permissions
5. WordPress Settings Configuration
6. Media Management
7. Posts & Pages Management
8. Categories & Tags
9. Plugin Installation & Management
10. Theme Customization
11. CSS Customization
12. Website Homepage Setup
13. Content Management
14. Comments Management
15. User Management
16. WordPress Security Best Practices
17. Website Maintenance & Administration

## 5. Python for Security Professionals

**BEGINNER TO ADVANCED · 14 MODULES**

1. Python Environment Setup
2. Python Objects & Data Structure Basics
3. Python Comparison Operators
4. Python Statements & Control Flow
5. Methods & Functions
6. Object-Oriented Programming (OOP)
7. Input/Output File Handling
8. Error & Exception Handling
9. Modules & Packages
10. Built-in Functions
11. Advanced Python Modules
12. Advanced Python Data Structures
13. Python Automation for Security
14. Security Tool Development

## 02 Core Offensive Security

1 course

### Certified Ethical Hacking & Penetration Testing

**BEGINNER TO ADVANCED · 16 MODULES**

1. Kali Linux Fundamentals
2. Introduction to Penetration Testing & Ethical Hacking
3. Footprinting & Reconnaissance
4. Scanning Networks
5. Proxies, VPNs & Tor
6. Tunneling Techniques
7. Enumeration
8. System Hacking & Malware Threats
9. Privilege Escalation
10. Buffer Overflow
11. Advanced Exploitation & Metasploit Framework
12. Evading IDS, Firewalls & Honeypots
13. Sniffing & MITM Attacks
14. Social Engineering
15. Denial of Service (DoS/DDoS)
16. Cryptography

## 03 Specializations

6 courses

### 1. Wireless Security & WiFi Pentesting

ADVANCED · 14 MODULES

1. Introduction to Wireless Networks
2. Wireless Encryption & Authentication
3. Wireless Network Cards in Linux
4. Wireless Security Measures & Bypass
5. Wireless Reconnaissance & Traffic Analysis
6. Wireless Denial-of-Service Attacks
7. Wireless MITM & Rogue Access Points
8. WEP Cracking Techniques
9. Chop-Chop & Packet Replay Attacks
10. Caffe Latte Attack
11. WPA/WPA2 Cracking
12. Cowpatty & Hash Table Attacks
13. Advanced WPA/TKIP Attacks
14. Enterprise Wireless Security & Reporting

### 2. Active Directory Security & Enterprise Attacks

ADVANCED · 13 MODULES

1. LDAP Enumeration
2. Kerberos Authentication
3. Kerberoasting Attacks
4. Pass-the-Ticket (PtT)
5. AS-REP Roasting
6. Manual Enumeration
7. Password Attacks & Credential Dumping
8. Pass-the-Hash (PtH)
9. LLMNR Poisoning & SMB Relay Attacks
10. Active Directory Offensive Security Tools
11. Active Directory Privilege Escalation
12. Enterprise Lateral Movement & Persistence
13. Active Directory Hardening & Reporting

### 3. Advanced Web Application Security

ADVANCED · 17 MODULES

1. Web Server Concepts
2. Web Server Hardening & Security
3. Web Server Enumeration & Misconfigurations
4. Web Application Security Tools
5. Web Application Concepts & Architecture
6. Web Application Security Fundamentals
7. Web Application Testing Methodology
8. Injection Attacks
9. Authentication & Session Attacks
10. Cross-Site Scripting (XSS)
11. Security Misconfiguration
12. Sensitive Data Exposure
13. File Inclusion & Path Traversal
14. SSRF & XXE Attacks
15. Access Control & IDOR
16. Advanced Web Exploitation Techniques
17. Additional Web Attack Vectors

## 4. API Security & Advanced Exploitation

**INTERMEDIATE TO ADVANCED · 22 MODULES**

1. Introduction to API Penetration Testing
2. Lab Setup & Testing Environment
3. SOAP API Security
4. REST API Security
5. GraphQL API Security
6. API Reconnaissance
7. Endpoint Analysis & Discovery
8. JWT Vulnerabilities & Exploits
9. API Injection Attacks
10. Broken Object Level Authorization (BOLA)
11. Broken Authentication
12. Exploiting API Authorization
13. Broken Object Property Level Authorization (BOPLA)
14. Broken Function Level Authorization (BFLA)
15. Rate Limiting & Resource Consumption
16. Business Logic & Sensitive Flows
17. Server-Side Request Forgery (SSRF)
18. Security Misconfiguration
19. Improper Inventory & Asset Management
20. Unsafe Consumption of APIs
21. GraphQL-Specific Attacks
22. Reporting & Remediation

## 5. Mobile Application Penetration Testing

**ADVANCED · 14 MODULES**

1. Mobile Security Landscape & Threat Modeling
2. Android Platform Internals
3. iOS Platform Internals
4. Lab Setup: Devices, Emulators & Tooling
5. Android Static Analysis
6. iOS Static Analysis
7. Dynamic Analysis & Runtime Instrumentation
8. Root & Jailbreak Detection Bypass
9. Certificate Pinning Bypass
10. Insecure Data Storage
11. IPC & Component Vulnerabilities
12. Runtime Manipulation & Tampering
13. Mobile Backend API Testing
14. Reporting & OWASP MASVS Verification

## 6. AI/ML Penetration Testing

**ADVANCED · 13 MODULES**

1. AI/ML Security Landscape & Threat Modeling
2. MITRE ATLAS & NIST AI RMF
3. LLM Prompt Injection
4. Jailbreaks & Guardrail Bypass
5. RAG Pipeline Attacks
6. MCP & Agentic System Abuse
7. Adversarial Examples for ML Classifiers
8. Training-Data Poisoning & Backdoors
9. Model Extraction & Model Inversion
10. ML Supply Chain Attacks
11. LLM Application Security Testing
12. Tooling Deep Dive
13. Reporting, Governance & AI Red Team Operations

// CAPSTONE · CISE

## Certified Information Security Expert

The complete program that unifies every track into one career-defining qualification — all 12 courses · 191 modules.