# Practical Cybersecurity

Hands-on skills for real-world security challenges

## Table of contents



## Course Overview

A comprehensive introduction to cybersecurity concepts, tools, and practices, with a focus on hands-on exercises and real-world applications. This 12-week course provides practical skills to identify and mitigate security vulnerabilities, understand attack vectors, and implement effective security measures in various environments.

### Next Cohort

- Start Date: April 1, 2026
- Format: Available in instructor-led online, self-paced, and in-person formats
- Prerequisites: Basic understanding of computer networks, familiarity with operating systems

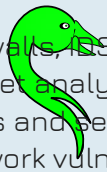
## Course Curriculum

### Module 1: Cybersecurity Fundamentals (Weeks 1-2)

- Introduction to cybersecurity concepts and terminology
- The cybersecurity landscape: threats, actors, and motivations
- Security principles: CIA triad, defense in depth, least privilege
- Regulatory frameworks and compliance
- Setting up a security lab environment

### Module 2: Network Security (Weeks 3-4)

- Network fundamentals and security architecture



- Firewalls, IDS/IPS, and network monitoring
- Packet analysis and traffic inspection
- VPNs and secure network communication
- Network vulnerability assessment

### Module 3: Web Application Security (Weeks 5-6)

- Web application architecture and vulnerabilities
- OWASP Top 10 risks and mitigations
- Web application security testing
- Client-side vs. server-side security
- Secure coding practices

### Module 4: Cryptography and Secure Communications (Week 7)

- Cryptographic concepts and algorithms
- Symmetric vs. asymmetric encryption
- Digital signatures and certificates
- PKI infrastructure
- Implementing encryption in applications

### Module 5: Vulnerability Assessment and Penetration Testing (Weeks 8-9)

- Vulnerability assessment methodology
- Penetration testing frameworks and tools
- Exploitation techniques and privilege escalation
- Reporting and remediation
- Legal and ethical considerations

### Module 6: Security Operations and Incident Response (Weeks 10-11)

- Security monitoring and log analysis
- Building a SOC capability
- Incident detection and triage
- Incident response planning and execution
- Digital forensics fundamentals

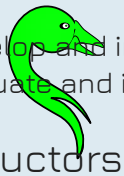
### Module 7: Advanced Topics and Capstone Project (Week 12)

- Cloud security considerations
- Mobile security fundamentals
- IoT security challenges
- Career pathways in cybersecurity
- Capstone project presentation

## Learning Outcomes

By the end of this course, you will be able to:

- Identify and analyze security threats and vulnerabilities in various environments
- Implement network security controls and monitoring solutions
- Conduct basic vulnerability assessments and security tests
- Apply cryptographic solutions to protect sensitive information
- Respond effectively to security incidents and perform basic forensic analysis



- Develop and implement security policies and procedures
- Evaluate and improve the security posture of systems and applications

## Instructors

Our instructors are experienced cybersecurity professionals with backgrounds in various sectors including finance, healthcare, government, and technology. They bring real-world experience and practical insights to the classroom.

## Assessment and Certification

- Weekly hands-on labs and technical challenges
- Practical security assessments and documentation
- Team-based security scenarios and exercises
- Final capstone project demonstrating comprehensive security skills
- Industry-recognized course completion certificate

## Resources

- Dedicated virtual lab environment for hands-on practice
- Comprehensive course materials and reference guides
- Security tools and software for practical exercises
- Community forum for discussion and collaboration
- Office hours with instructors for personalized support

## Download

## Contact

Interested in enrolling or have questions about this course?

- Email: office@chen.ist
- Phone: Schedule a call to discuss your goals
- Web: Book a free consultation