

CERTIFIED CYBERSECURITY TECHNICIAN

Course Duration: 40 Hrs.

Course code: 212-82

Course Overview

The Certified Cybersecurity Technician (C|CT) course, offered by EC-Council, is an entry-level program designed to equip individuals with foundational cybersecurity skills, covering areas like network defense, ethical hacking, digital forensics, and security operations, culminating in a certification validating practical skills.

What you'll learn?

❖ **Network Defense:**

Learn to implement and manage network security solutions, including firewalls, intrusion detection systems, and network segmentation.

❖ **Ethical Hacking:**

Understand penetration testing techniques to identify vulnerabilities and improve security posture.

❖ **Digital Forensics:**

Develop skills in collecting, analyzing, and preserving digital evidence for incident investigation.

Target Audience

The target audience for a Certified Cybersecurity Technician (C|CT) course includes entry-level cybersecurity technicians, network administrators seeking cybersecurity skills, IT professionals wanting to transition into cybersecurity roles, and helpdesk technicians aiming to specialize in security.

Pre-Requisites

❖ **No Mandatory Requirements:**

Unlike some certifications, the C|CT program doesn't require specific degrees, certifications, or years of experience to enroll.

❖ **Beneficial Background:**

While not mandatory, having a foundation in IT and networking, especially with cybersecurity concepts, can significantly aid in understanding the course material.

❖ **Curriculum Focus:**

The C|CT curriculum covers essential technologies, but having some prior experience with computers and computer networks is recommended.

Course content

- Module 1 Information Security Threats and Vulnerabilities
- Module 2 Information Security Attacks
- Module 3 Network Security Fundamentals
- Module 4 Identification, Authentication, and Authorization
- Module 5 Network Security Controls: Administrative Controls
- Module 6 Network Security Controls: Physical Controls
- Module 7 Network Security Controls: Technical Controls
- Module 8 Network Security Assessment Techniques and Tools
- Module 9 Application Security
- Module 10 Virtualization and Cloud Computing
- Module 11 Wireless Network Security
- Module 12 Mobile Device Security
- Module 13 Internet of Things (IoT) and Operational Technology (OT) Security
- Module 14 Cryptography
- Module 15 Data Security
- Module 16 Network Troubleshooting
- Module 17 Network Traffic Monitoring
- Module 18 Network Log Monitoring and Analysis
- Module 19 Incident Response

Module 20 Computer Forensics

Module 21 Business Continuity and Disaster Recovery

Module 22 Risk Management

Exam Preference

Exam Code	212-82
Number Of Questions	60 Questions
Type Of Questions	50 MCQ, 10 hands-on practical exercises
Passing Score	70%

