+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 03/16/2026

Sign up

CCT™ Certification Training

5 days (35 hours)

Overview

The EC-Council CCT™ training course introduces you to the fundamentals of penetration testing with a structured and immediately applicable approach. It enables you to replicate realistic attack scenarios to detect, exploit, and document vulnerabilities in a controlled environment.

You will learn to follow a comprehensive process: reconnaissance, enumeration, exploitation, post-exploitation, and reporting. The goal is to gain the autonomy to analyze an attack surface and prioritize risks, whether in internal audits, security engagements, or SOC skill development.

The training is practice-oriented: guided workshops, tool demonstrations, and exercises in lab environments. Deliverables include operational checklists, sample commands, a report template, and remediation recommendations.

Objectives

- Identify an attack surface and gather useful information.
- Perform service enumeration and interpret the results.
- Exploit common vulnerabilities in a controlled manner.
- Assess the impact and propose corrective measures.
- Write a clear and actionable audit report.

Target Audience

- System and network administrators
- SOC analysts / Blue Team members seeking to understand attack techniques
- Cybersecurity beginners with a focus on penetration testing
- Security project managers

Prerequisites

- Basic network knowledge (TCP/IP, ports, DNS)
- Linux basics (shell, permissions, services)
- Understanding of common protocols (HTTP, SSH, SMB)
- Security awareness: vulnerabilities, patches, hardening

Technical prerequisites

- PC with at least 8 GB of RAM (16 GB recommended)
- Windows (with WSL2), Linux, or macOS
- Virtualization: VirtualBox or VMware + installation rights
- Tools: Kali Linux, modern web browser, code editor, terminal

EC-Council CCT Training: Certified Cybersecurity Technician

[Day 1 - Morning]

Fundamentals and Modern Threats

- CCT Role: Technician’s Role, Scope, and Ethical Boundaries
- Threat Landscape: Evolution of Phishing, Ransomware, and Social Engineering
- Basic Concepts: The CIA Triad (Confidentiality, Integrity, Availability)
- Attack surface, vulnerabilities, and risk management
- Hands-on Workshop: Mapping an Attack Surface via Passive Reconnaissance (OSINT).

[Day 1 - Afternoon]

Endpoint Security

- OS Architecture: Processes, Services, and Privileges (Windows and Linux)
- Digital Hygiene: MFA, password management, and disk encryption
- Endpoint Threats: Malware, Privilege Escalation, and Persistence
- Introduction to System Hardening
- Hands-on Workshop: Configuration Audit and Securing a Workstation.

[Day 2 - Morning]

Network Architecture and Secure Protocols

- TCP/IP Model and Critical Protocols: DNS, DHCP, HTTP(S), SMB, SSH
- Segmentation and Isolation: VLANs, DMZ, and Microsegmentation
- Security Equipment: Firewalling (Stateful), IDS/IPS, and VPN
- Wi-Fi Network Security and Encryption Protocols
- Hands-on workshop: Configuring filtering rules and routing analysis.

[Day 2 - Afternoon]

Traffic Analysis and Detection

- Data capture: Using Wireshark and Tcpdump
- Network log analysis: NetFlow, firewall logs, and timestamping
- Identifying anomalies: Port scans, data exfiltration, and C2 communications
- Network Event Correlation
- Hands-on Workshop: Analyzing a PCAP file to identify a network intrusion.

[Day 3 - Morning]

Web Application Security

- How the Web Works: HTTP Requests, Security Headers, and Cookies
- Introduction to the OWASP Top 10: SQL Injections, XSS, and Access Control Flaws
- Authentication and Session Management
- Risks Associated with Third-Party Components and APIs
- Hands-on Workshop: Identifying Vulnerabilities in a Test Web Application.

[Day 3 - Afternoon] Application

and Cloud Security

- Web Protection: Using a WAF (Web Application Firewall)
- Introduction to Cloud Computing: Shared Responsibility Model
- Securing Virtualized Environments and Containers
- Secure Development Best Practices (Introduction)
- Hands-on Workshop: Implementing Security Controls on a Web Infrastructure.

[Day 4 - Morning]

Introduction to Computer Forensics

- Principles of Forensics: Evidence Preservation and Chain of Custody
- Data collection: RAM acquisition and disk imaging
- Analysis of artifacts: History, recent files, system logs
- Standard Forensic Tools (FTK Imager, Autopsy)

- Hands-on Workshop: Digital Investigation to Trace a Suspicious Execution.

[Day 4 - Afternoon] Incident Response (IR)

- The Incident Handling Workflow: Detection, Containment, Eradication
- Communication and escalation: Documentation and traceability of actions
- Containment strategies: Network isolation and immediate remediation
- Service restoration and lessons learned
- Hands-on Workshop: Full Incident Simulation and Writing an Incident Report.

[Day 5 - Morning]

Vulnerability and Risk Management

- Vulnerability Lifecycle: Scanning (Nessus), CVSS Scoring
- Patch Prioritization and Patch Management
- Introduction to compliance frameworks (ISO 27001, NIST)
- User Awareness and Cybersecurity Culture
- Hands-on Workshop: Vulnerability scanning of an IT environment and drafting a remediation plan.

[Day 5 - Afternoon]

Review and Certification Preparation

- Summary of Key CCT Domains
- Mock Exam: Simulation with EC-Council-style questions
- Review of technical concepts and exam methodology
- Final checklist before taking the certification exam
- Hands-on Workshop: Group review of the practice exam and closing session.

FAQ – QUESTIONS & ANSWERS

In what language is the CCT™ training conducted?

The training is in French.

Is the exam included in the training price?

Yes, the certification fee is included in the course cost ($499 as a rough estimate). You will be able to take the exam at the end of the session.

How does the CCT™ certification exam work?

The exam consists of a performance-based multiple-choice test comprising 85 questions. It is

administered online at an approved Pearson VUE testing center.

Target Audience

This training is intended for both individuals and companies, large or small, wishing to train their teams in new advanced IT technology or to acquire specific professional knowledge or modern methods.

Entry-level assessment

The pre-training assessment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency in various types of technologies, as well as their expectations and personal goals regarding the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for monitoring and ensuring the smooth running of the training session.

Teaching Methods

Practical Course: 60% Practical, 40% Theory. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical instruction from the instructor—supported by examples and discussion sessions—and group work.

Assessment

At the end of the session, a multiple-choice questionnaire is used to verify that the skills have been properly acquired.

Certification

A certificate will be issued to each trainee who has completed the entire training program.