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

Updated on 08/20/2026

Sign Up

CREST CCT APP Certification Training

4 days (28 hours)

Overview

The CREST CCT APP Certification Training prepares you for the official CREST Certified Tester Application exam, an advanced certification that validates your ability to conduct application, system, and cloud penetration tests in demanding environments.

This preparatory course allows you to solidify the skills required to pass the CREST Certified Tester Application certification. You will gain in-depth knowledge of penetration testing methodologies, attack surface analysis, vulnerability exploitation, and reporting results in a professional context.

You will learn to master the technical areas covered by the exam, including web application security, APIs, injections, authentication, Windows and Linux environments, databases, the cloud, and containerization.

The course prepares you for both parts of the official exam: the written exam, consisting of multiple-choice questions and an essay-style scenario, as well as the practical exam conducted in a controlled environment. You will develop a structured approach to assessing risks, writing actionable findings, and optimizing your time management.

Upon completion of the training, you will be able to approach the certification with a solid methodology, demonstrate your skills as a senior penetration tester, and conduct application security assessments that meet the expectations of a real-world assignment.

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

Objectives

- Master the scope and expectations of the CREST Certified Tester Application exam
- Identify and exploit advanced vulnerabilities in web applications, APIs, and associated infrastructure
- Implement a penetration testing methodology tailored to certification scenarios
- Analyze impacts, assess risks, and produce structured security reports
- Effectively prepare for the written and practical exam components within the exam’s time constraints

Target Audience

- Penetration Tester
- Cybersecurity consultant
- Application security auditor
- Red Teamers

Prerequisites

- Proven experience in application and system penetration testing
- Proficiency in HTTP, TCP/IP, DNS, and TLS protocols
- Advanced knowledge of Linux and Windows environments
- Experience with web vulnerabilities, APIs, SQL databases, and authentication mechanisms

Technical Requirements

- Computer running Windows 10 or 11, macOS, or a recent Linux distribution
- 64-bit processor; 16 GB of RAM recommended and 50 GB of available disk space
- VMware Workstation, VMware Fusion, or VirtualBox virtualization solution installed and operational
- Stable internet connection allowing for virtual machine downloads and access to lab platforms

CREST CCT APP Training Program

[Day 1 - Morning]

Certification framework and assessment methodology

- Positioning of the CREST Certified Tester Application certification and expected competency level
- Breakdown of the exam: multiple-choice questions, written scenario, and Practical
- Syllabus analysis: web applications, infrastructure, systems, cloud, containers, and macOS
- Pentest project lifecycle: authorization, scope, rules of engagement, evidence collection, and debriefing

- Time management, reading instructions, response strategy, and passing criteria

[Day 1 - Afternoon]

Reconnaissance and mapping of the attack surface

- Structured approach to passive and active reconnaissance within an authorized scope
- Service enumeration, technology fingerprints, DNS, HTTP, TLS, and metadata analysis
- Mapping of applications, APIs, administrative environments, and sources of information leaks
- Prioritizing attack vectors based on exposure, criticality, and compromise
- Hands-on workshop: mapping a lab target, identifying exposed technologies, and creating a prioritized test plan

[Day 2 - Morning]

Application security and input-based attacks

- Modeling application threats and analyzing modern web attack vectors
- Searching for and validating SQL injection, NoSQL injection, XPath injection, and command injection vulnerabilities
- Analysis of validation weaknesses: XSS, XXE, SSRF, CRLF injection, and directory traversal
- Reasoned fuzzing, filter bypass, encodings, query strings, and exploitability testing
- Building reliable evidence and distinguishing between theoretical vulnerabilities, demonstrated impact, and false
  false positives

[Day 2 - Afternoon]

Authentication, authorization, and business logic

- Evaluation of authentication, password management, MFA, and account recovery mechanisms
- Authorization testing: horizontal and vertical escalation, IDOR, mass assignment, and access control
  for APIs
- Analysis of sessions, cookies, tokens, session fixation, replay attacks, and JWT weaknesses
- Identification of vulnerabilities in business logic, concurrency, and workflow bypass
- Hands-on workshop: Compromising a lab application workflow through authorization abuse, then documenting the impact and remediation

[Day 3 - Morning]

Pivoting, systems, and infrastructure environments

- Pivoting techniques, port forwarding, proxification, and maintaining a chain of evidence
- Enumeration and exploitation of Windows environments, Active Directory, remote services, and local permissions
- Reconnaissance of Linux and Unix systems, processes, services, secrets, and

- Local privilege escalation, post-exploitation, data access, and analysis of persistence mechanisms
- Testing network services, administration protocols, shares, directories, and
  [Day 3 - Afternoon]

[Day 3 - Afternoon]

Cloud, containers, and chains of compromise

- Reconnaissance and risks of cloud environments: IAM, logging, storage, metadata, and virtual networks
- Assessing configuration errors in Docker containers, Kubernetes clusters, and virtualized platforms
- Analysis of secrets, service identities, registries, volumes, roles, and movements between host and cloud
- Identification of compromise scenarios combining applications, infrastructure, and cloud services
- Hands-on workshop: Exploiting a chain of compromise in a lab environment, starting from a web application and moving to a containerized environment

[Day 4 - Morning]

Written exam and submission of deliverables

- Targeted review of high-density technical areas for multiple-choice questions
- Reading and breaking down a scenario: scope, constraints, risks, requirements, and expected deliverables
- Vulnerability assessment: plausibility, business impact, criticality, exploitation conditions, and prioritization
- Drafting of findings: evidence, technical description, consequences, recommendations, and communication to the client
- Simulation of the scenario-based exam: time management, structured long-form answers, and final quality control

[Day 4 – Afternoon]

Integrated certification simulation

- Preparing the practical environment: available tools, workstation constraints, permitted files, and scoring strategy

- Methodical analysis of a target environment combining applications, systems, databases, and network services
- Balancing technical depth, scope coverage, response collection, and stopwatch
- Debriefing on common mistakes: red herrings, insufficient evidence, imprecise answers, and wasted time
- Hands-on workshop: conducting a timed simulation of the practical exam, answering questions, and present a personalized correction strategy

Target Companies

This training is intended for both individuals and companies—large or small—that wish 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 level across various types of technologies, as well as their expectations and personal goals for 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

Hands-On Training: 60% Practical, 40% Theoretical. Training materials distributed in digital format to all participants.

Organization

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

Assessment

At the end of the session, a multiple-choice quiz is administered to verify that participants have successfully acquired the skills.

Certification

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