AMBIENT-IT

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

Updated on 08/24/2026

Sign Up

CREST CCP INF Certification Training

4 days (28 hours)

Overview

The CREST CCP INF Certification Training prepares you for the official CREST Certified Tester - Infrastructure (CCT INF) certification, an advanced standard for validating your skills in infrastructure penetration testing, risk analysis, and professional reporting.

This training course enables you to methodically prepare for the CREST Certified Tester - Infrastructure (CCT INF) exam, designed for professionals capable of assessing the security of systems, networks, exposed services, and enterprise environments. You will solidify the skills required for Windows and Linux infrastructures, networks, the cloud, virtualization, and web technologies.

You will learn how to organize a penetration testing engagement, from the scoping phase to report writing, by applying a rigorous methodology of reconnaissance, enumeration, exploitation, and validation. The preparation also covers protocol analysis, vulnerability identification, pivoting, directory services, and network security mechanisms.

Upon completion of the training, you will be able to apply the techniques assessed during the written and practical exams, prioritize findings based on risk, and produce deliverables that can be acted upon by technical teams and decision-makers. You will have a preparation strategy tailored to the Pearson VUE format and the certification requirements.

The training also covers certification scenarios, time management, hands-on exercises in a controlled environment, and best practices for reporting findings. It helps you develop the autonomy needed to conduct complex infrastructure assessments within a legal, ethical, and professional framework.

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 technical areas assessed by the CREST Certified Tester - Infrastructure (CCT INF) certification.
- Structure an infrastructure penetration testing engagement, from scoping to reporting.
- Identify, exploit, and classify vulnerabilities in Windows, Linux, network, and cloud environments.
- Analyze the results from security tools and conduct controlled pivoting operations.
- Prepare for the certification’s written, scenario-based, and practical exams.
- Write precise, prioritized, and risk-based security reports.

Target Audience

- Penetration Tester
- Cybersecurity consultant
- Security auditor
- Red Team member
- Network security engineer

Requirements

- Proven experience in penetration testing and infrastructure security assessments.
- Operational proficiency with Windows and Linux systems.
- Advanced knowledge of TCP/IP networks, DNS, SMB, LDAP, and Active Directory services.
- Proficiency with Nmap, Wireshark, Burp Suite, and Metasploit.
- Ability to write technical security reports in English.

Technical Requirements

- Computer running Windows 11, macOS, or Linux, with a 64-bit processor, at least 16 GB of RAM, and 80 GB of available disk space.
- Virtualization software: VMware Workstation 17, VMware Fusion 13, or VirtualBox 7.
- A recent Kali Linux virtual machine and an isolated lab environment compatible with penetration testing exercises.
- Stable internet connection, without filtering that blocks downloads, software repositories, and access to authorized labs.
- Up-to-date Google Chrome, Mozilla Firefox, or Microsoft Edge browser.

CREST CCP INF Training Program

[Day 1 - Morning]

Certification framework and assessment methodology

- Overview of the official CREST Certified Tester - Infrastructure (CCT INF) certification and expected competencies.
- Exam structure, passing criteria, breakdown of competencies, and preparation.
- Life cycle of a penetration testing engagement: authorization, scope definition, rules of engagement, evidence collection, and risk management.
- Development of a reproducible methodology for reconnaissance, enumeration, validation, and reporting.
- Hands-on workshop: analyzing a mission statement, defining the scope, assumptions, rules of engagement, and test plan.

[Day 1 – Afternoon]

Networks, Protocols, and Attack Mapping

- Advanced review of the TCP/IP layers, routing, VLANs, IPv4, IPv6, and filtering mechanisms.
- Analysis of DNS, ARP, DHCP, SMB, SNMP, SSH, and email services.
- Host discovery, system fingerprinting, service enumeration, and interpretation of network responses.
- Traffic analysis, packet manipulation, detection of NAC controls, and identification of surfaces of exposure.
- Hands-on workshop: mapping an authorized target network using Nmap and Wireshark, then generating a matrix of exploitable services.

[Day 2 - Morning]

Assessment of Windows and Active Directory Environments

- Windows security architecture: accounts, tokens, privileges, services, registry, local policies, and hardening mechanisms.
- Active Directory reconnaissance: domains, forests, trusts, objects, groups, GPOs, delegations, and attack paths.
- Authenticated and unauthenticated enumeration of LDAP, Kerberos, SMB, and RPC services.
- Analysis of configuration errors: excessive permissions, exposed secrets, shares, password policies, and lateral movement.
- Hands-on workshop: conducting an Active Directory enumeration phase and documenting .

[Day 2 - Afternoon]

Linux Systems, Unix Services, and Privilege Escalation

- Linux and Unix security model: accounts, permissions, sudo, capabilities, services, processes, and logs.
- Scan for FTP, NFS, SMTP, RPC, SSH, X11, and database services.

- Scanning for local vulnerabilities: SUID binaries, scheduled tasks, write permissions, secrets, weak configurations, and vulnerable kernels.
- Principles of controlled exploitation, access stabilization, evidence collection, and traceability traceability.
- Hands-on workshop: audit a vulnerable Linux server, demonstrate a controlled privilege escalation, and document the evidence.

[Day 3 - Morning]

Web, database, and cloud technologies

- Reconnaissance of web servers, APIs, frameworks, authentication mechanisms, sessions, and authorization controls.
- Analysis of SQL, NoSQL, LDAP, and XML vulnerabilities; command injection, XSS, file upload, and directory traversal.
- Security assessment of databases, application secrets, and connection strings.
- Fundamentals of cloud assessment: identities, roles, storage, metadata, , and containerization.
- Hands-on workshop: identifying and classifying vulnerabilities in an administrative application exposing an API and a database.

[Day 3 - Afternoon]

Exploitation, pivoting, and attack chains

- Reasoned selection of exploitation vectors based on context, business impact, and engagement constraints.
- Techniques for pivoting, proxying, tunneling, relaying, and accessing authorized internal segments.
- Credential management, session reuse, lateral movement, and limitations imposed by security controls.
- Assessment of virtualized environments, snapshots, isolation mechanisms, and risks of virtual machine escape.
- Hands-on workshop: Build a lab attack chain from an exposed service to an internal asset, justifying each step.

[Day 4 - Morning]

Written scenario, risk analysis, and reporting

- Preparation for the written exam: multiple-choice questions, mission scenario, time management, and reading the instructions.
- Vulnerability assessment: likelihood, impact, severity, prioritization, and formulation of a understandable risk description.
- Drafting findings: evidence, technical description, exploitation scenario, consequences, recommendations, and compensating controls.

- Communication with the client: presentation of findings, limitations of the assessment, writing quality, compliance, and legal obligations.
- Hands-on workshop: working through a certification scenario, drafting prioritized findings, and presenting a
  risk summary.

[Day 4 – Afternoon]

Final simulation and operational preparation

- Review of syllabus topics: networking, systems, services, virtualization, web, cloud, macOS, and cross-functional skills.
- Strategy for the practical exam: rapid assessment, prioritization, validation of answers, and handling dead ends.
- Getting familiar with the Kali Linux-style environment, authorized tools, and preloaded resources.
- Analysis of common errors: insufficient evidence collection, confusion between vulnerability and risk, poor prioritization, and incomplete reporting.
- Hands-on workshop: Conduct a timed certification simulation combining reconnaissance, controlled exploitation, risk analysis, and reporting.

Target Audience

This training is intended for both individuals and companies—large or small—seeking to train their teams in new, advanced IT technologies or to acquire specific industry knowledge or modern methodologies.

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

of the skills.

Certification

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