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

Updated on 08/26/2026

Sign Up

CREST CPSA Certification Training

5 days (35 hours)

Overview

The CREST Practitioner Security Analyst certification validates the fundamental skills required to conduct security assessments on infrastructure, systems, and web applications. It prepares you for the practical challenges of penetration testing, vulnerability analysis, and interpreting technical results.

Our CREST CPSA Certification Training course provides structured preparation for the official CREST Practitioner Security Analyst exam. You will build the knowledge needed to understand the scope of an assignment, identify attack surfaces, and apply a responsible testing methodology.

You will learn to analyze network protocols, conduct reconnaissance phases, interpret scan results, and assess the security of Windows, Unix, and web environments. Concepts such as authentication, session management, injection, XSS, and database security are also covered.

Upon completion of the training, you will be able to effectively prepare for the exam format—which consists of multiple-choice questions—and apply the skills validated by the certification in a supervised penetration testing environment.

This course combines targeted review, scenario-based exercises, and exam-style practice to strengthen your mastery of the syllabus topics, your analytical skills, and your time management on exam day.

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

Objectives

- Understand the subject areas and format of the CREST Practitioner Security Analyst exam
- Apply a methodology for vulnerability reconnaissance and analysis
- Interpret the results of network and application scanning tools
- Assess common risks in Windows, Unix, and web environments
- Identify the main web vulnerabilities and their associated remediation measures
- Prepare for multiple-choice questions and manage your exam time

Target Audience

- Junior penetration tester
- Cybersecurity analyst
- IT security consultant
- Systems and network administrator
- SOC Analyst

Prerequisites

- Knowledge of TCP/IP networks, routing, and common services
- Proficiency with essential Linux and Windows commands
- Basic understanding of system, network, and web application security
- Basic experience with Nmap and network diagnostic tools

Technical Prerequisites

- Computer running Windows 10 or 11, macOS, or Linux, with at least 16 GB of RAM
- Installation and administrative privileges on the workstation
- VirtualBox 7 or VMware Workstation installed to run the lab machines
- Stable Internet connection, without filtering that blocks downloads, software repositories, and network communications for the lab environments
- A recent web browser and a text editor or terminal available

CREST CPSA Training Program

[Day 1 - Morning]

Certification framework and testing methodology

- Overview of the CREST Practitioner Security Analyst certification, its competency areas, and its market positioning
- Exam format, multiple-choice questions, exam rules, and time management strategy
  Time management strategies
- Life cycle of a penetration testing engagement, authorization, scope, rules of engagement, and traceability

- Principles of ethics, confidentiality, evidence management, and communication with the client
- Fundamentals of risk analysis, attack surface, and prioritization of findings

[Day 1 – Afternoon]

Networks and Target Mapping

- Review of TCP/IP protocols, addressing, routing, ARP, DNS, and ports
- Network architecture, segmentation, filtering, firewalls, and access control mechanisms
- Host discovery, service identification, and principles of system fingerprinting
- Reading and interpreting scan results with Nmap and network diagnostic tools
- Filtering bypass techniques to be familiar with for the exam, within an authorized environment
- Hands-on workshop: mapping a lab network, identifying exposed hosts, services, and ports, and interpreting the results

[Day 2 - Morning]

Reconnaissance and Information Gathering

- Objectives of passive and active reconnaissance in a penetration testing approach
- Searching for public information, domain names, DNS records, and analyzing web presence
- Enumeration of subdomains, services, users, and accessible resources
- Analysis of metadata, exposed technologies, and information leaks
- Qualifying results, reducing false positives, and documenting useful findings

[Day 2 - Afternoon]

Assessment of network services and equipment

- Analysis of common services: FTP, SMTP, SSH, SNMP, SMB, and RPC services
- Basics of traffic capture and analysis, plaintext protocols, and detection of weak configurations
- Network device security, administration interfaces, monitoring services, and configurations
- Security principles for wireless networks, IP telephony, and IPSec tunnels
- Reading banners, correlating versions, and identifying likely vulnerabilities
- Hands-on workshop: analyzing multiple exposed services in a lab environment and producing a summary of the observed risks

[Day 3 - Morning]

Windows Environment Security

- Windows Security Architecture, Local Accounts, Groups, Permissions, Services, and Patch Mechanisms
- Active Directory Fundamentals: Domains, Users, Groups, Policies, and Trust Relationships trust
- Enumerating users, shares, services, and system information on a Windows target
- Password management, lockout policies, hashing, and principles of resistance to attacks
- Identifying configuration flaws, missing patches, and common escalation vectors

[Day 3 - Afternoon]

Security of Unix and Linux Environments

- Unix and Linux permission architecture, users, groups, processes, and services
- Enumeration of accounts, shares, scheduled tasks, binaries, and sensitive configurations
- Analysis of NFS, FTP, SMTP, SSH, RPC, and X11 services
- Searching for vulnerabilities related to version vulnerabilities, weak permissions, and exposed secrets
- Best practices for hardening, logging, and reducing the attack surface
- Hands-on Workshop: Conduct a guided assessment of a vulnerable Linux machine and classify findings by severity

[Day 4 - Morning]

Web Technologies and Testing Methodology

- Web application architecture, servers, proxies, APIs, client components, and data services
- How HTTP and HTTPS work: methods, headers, cookies, response codes, and redirects
- Application recognition, content mapping, parameters, directories, and features
- Threat modeling, attack vectors, and user input validation
- Authentication, authorization, session management, and information disclosure via error messages

[Day 4 - Afternoon]

Application and Database Vulnerabilities

- Principles and detection of XSS vulnerabilities, SQL injections, and parameter manipulation
- Analysis of validation controls, encoding, filtering, and error handling
- Risks related to sessions, cookies, tokens, and access control mechanisms
- Security concepts for MySQL, Microsoft SQL Server, and Oracle databases
- Interpreting application responses and formulating remediation recommendations
- Hands-on workshop: identifying web vulnerabilities in a lab application and matching each finding to a remediation

[Day 5 - Morning]

Consolidation and targeted practice

- Comprehensive review of syllabus topics: networks, systems, the web, databases, and mission management
- Analysis of multiple-choice question scenarios and identification of key terms
- Methods for eliminating incorrect answers and making decisions when multiple answers seem plausible
- Review of concepts in cryptography, encryption, hashing, integrity, and security applications
- Logistical preparation for the exam, Pearson VUE account, closed-book exam, and rules to follow
- Hands-on workshop: taking a timed practice exam, reviewing answers, and creating a personalized study plan

[Day 5 - Afternoon]

Final simulation and exam preparation

- Comprehensive case study, from defining the scope to analyzing identified vulnerabilities
- Correlating the results of reconnaissance, network scanning, system enumeration, and web testing
- Classifying findings, assessing impact, and prioritizing remediation actions
- Summary of common exam pitfalls and areas requiring special attention
- Time-management tips, reviewing questions, and personal preparation before taking the exam
- Hands-on workshop: Solving a final simulation of multiple-choice questions and debriefing collectively reviewing answer choices

Target Companies

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

Assessment upon enrollment

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 with 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.