+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 CRT Certification Training

5 days (35 hours)

Overview

The CREST CRT Certification Training prepares you for the official CREST Registered Penetration Tester certification and helps you build the practical skills needed to conduct penetration tests on infrastructure, systems, and web applications. This intermediate-level training course guides you through your preparation for the CREST Registered Penetration Tester exam. You will learn to apply a structured testing methodology, use tools for reconnaissance, enumeration, and vulnerability analysis, and then rigorously interpret the results. You will work on the areas assessed by the certification, including IP networks, common services, Windows and Linux environments, routing manipulation, bypassing workstation restrictions, and web application security. Guided workshops place you in scenarios similar to the practical exam. You will be trained to identify services, exploit simple vulnerabilities, collect technical evidence, and formulate precise responses in a controlled environment based on Kali Linux. By the end of the course, you will have an effective exam preparation strategy, better time management skills, and the reflexes needed to demonstrate the competencies expected of an operational penetration tester.

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 scope and format of the CREST Registered Penetration Tester exam
- Apply a penetration testing methodology to network, system, and web targets
- Perform reconnaissance, enumeration, and vulnerability analysis using appropriate tools
- Exploit simple vulnerabilities and collect actionable technical evidence
- Manage time, responses, and priorities under the conditions of the practical assessment

Target Audience

- Penetration Tester
- Cybersecurity consultant
- Security analyst
- Security auditor
- Systems and Network Administrator

Prerequisites

- Must hold a valid CREST CPSA certification, which is required to take the exam
- Proficiency in the fundamentals of TCP/IP networks, routing, and common services
- Have practical knowledge of Windows and Linux systems
- Understand the basics of application vulnerabilities, including SQL, XSS, and web authentication

Technical Prerequisites

- PC running Windows 10 or 11, macOS, or Linux; a 64-bit processor and 16 GB of RAM are recommended
- Installed virtualization solution, such as VMware Workstation Player, VMware Fusion, or VirtualBox
- A functional Kali Linux virtual machine with at least 60 GB of available disk space
- Stable internet connection, without filtering that blocks downloads, software repositories, and access to lab platforms

CREST CRT Training Course Outline

[Day 1 - Morning]

Certification and Testing Methodology

- Positioning of the CREST Registered Penetration Tester certification and validated skills
- Structure of the practical assessment, scope, grading, and passing criteria
- Legal framework, testing authorization, rules of engagement, and evidence collection
- Penetration testing lifecycle: reconnaissance, enumeration, exploitation, and reporting
- Hands-on Workshop: Getting Started with an Authorized Lab and Initial Target Assessment

[Day 1 – Afternoon]

Reconnaissance and Network Mapping

- TCP/IP fundamentals, segmentation, VLANs, routing, and filtering
- Host discovery, service identification, and system fingerprinting
- Analysis of TCP, UDP, ICMP, ARP, and DNS protocols
- Practical use of Nmap and interpretation of scan results
- Hands-on Workshop: Mapping a Lab Network, Identifying Hosts, and Prioritizing Exposed Services

[Day 2 - Morning]

Network services and enumeration

- Enumeration of DNS, SMB, LDAP, SNMP, SSH, and FTP services
- Gathering information from banners, shares, directories, and exposed configurations
- Analysis of name resolution mechanisms, including NetBIOS, LLMNR, and mDNS
- Identifying configuration flaws and low-complexity attack vectors
- Hands-on workshop: Conducting service enumeration of an infrastructure and compiling an evidence inventory

[Day 2 - Afternoon]

Vulnerability analysis and basic exploitation

- Principles of vulnerability analysis: detection, validation, and qualification
- Using scanners and critically evaluating results, false positives, and tool limitations
- Searching for known vulnerabilities and correlating them with service versions
- Simple exploitation and controlled collection of evidence
- Hands-on workshop: analyzing scan results, validating a vulnerability, and retrieving evidence

[Day 3 - Morning]

Windows Security Assessment

- Reconnaissance of a Windows host, accounts, groups, processes, services, and patches
- Local and remote enumeration, shares, permissions, and administration mechanisms
- Active Directory basics: domains, authentication, and trust relationships
- Identifying vulnerabilities related to passwords, permissions, and service configurations
- Hands-on Workshop: Enumerating a Windows Lab Environment and Identifying a Simple Path to Compromise

[Day 3 - Afternoon]

Linux and Unix Security Assessment

- Identifying Linux and Unix systems, users, processes, and services
- Analysis of file permissions, sensitive directories, and scheduled tasks
- Enumeration of remote services, including NFS, RPC, SMTP, and SSH
- Searching for misconfigurations and exploitable vulnerabilities with low impact
- Hands-on workshop: auditing a Linux server, identifying a permission weakness, and collecting evidence

[Day 4 - Morning]

Routing and Constrained Environments

- Understanding network paths, gateways, routing tables, and networks that cannot be accessed directly
- Manipulating routes in a controlled environment to reach internal services
- Introduction to the Desktop Lockdown challenge and analysis of workstation restrictions
- Techniques for diagnostics, access verification, and data collection in a restricted environment
- Hands-on workshop: Accessing an isolated service by manipulating routing and extracting expected

[Day 4 - Afternoon]

Web Application Security

- Web application reconnaissance, mapping of features, settings, and technologies
- Checking authentication, authorization, sessions, cookies, and tokens
- Identifying vulnerabilities such as SQL injection, XSS, directory traversal, and file uploads
- Using Burp Suite to intercept, replay, and analyze HTTP requests
- Hands-on Workshop: Analyzing a lab web application and exploiting a vulnerability to obtain proof-of-concept

[Day 5 - Morning]

Exam Strategy and Management

- Targeted review of the infrastructure and application domains assessed in the CRT
- Time management for a 2-hour-30-minute assessment: reading, prioritizing, and processing questions in parallel

- Getting familiar with the Kali Linux environment provided during the exam
- Formulating short answers, entering evidence values, and verifying them before submission
- Hands-on workshop: Complete a timed series of CRT-style questions with a group analysis of the answers

[Day 5 – Afternoon]

Certification simulation and review

- Simulation of a hands-on track combining networking, systems, routing, and web applications
- Applying an independent approach to identification, analysis, and utilization
- Prioritizing tasks, estimating effort, and optimizing potential scores
- Detailed review, feedback on common mistakes, and a study plan for the exam
- Hands-on workshop: final timed simulation of a CREST CRT course and personalized debriefing

Target Companies

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 the skills.

Certification

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