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

Mis à jour le 26/08/2026

S'inscrire

Formation Certification CREST CRT

5 jours (35 heures)

Présentation

La formation Certification CREST CRT prépare à la certification officielle CREST Registered Penetration Tester et vous permet de consolider les compétences pratiques attendues pour conduire des tests d'intrusion sur des infrastructures, systèmes et applications web. Cette formation de niveau intermédiaire vous accompagne dans la préparation de l'examen CREST Registered Penetration Tester. Vous apprendrez à appliquer une méthodologie de test structurée, à utiliser les outils de reconnaissance, d'énumération et d'analyse de vulnérabilités, puis à interpréter leurs résultats avec rigueur. Vous travaillerez les domaines évalués par la certification, notamment les réseaux IP, les services courants, les environnements Windows et Linux, la manipulation de routage, le contournement de restrictions sur poste de travail et la sécurité des applications web. Les ateliers guidés vous placent dans des situations proches de l'évaluation pratique. Vous serez entraîné à identifier des services, exploiter des vulnérabilités simples, récupérer des preuves techniques et formuler des réponses précises dans un environnement contraint basé sur Kali Linux. À l'issue de la formation, vous disposerez d'une stratégie de préparation efficace pour l'examen, d'une meilleure maîtrise du temps et des réflexes nécessaires pour valider les compétences attendues d'un pentester opérationnel.

Comme toutes nos formations, celle-ci vous présentera **la dernière version stable** de la technologie et ses nouveautés.

Objectifs

- Comprendre le périmètre et les modalités de l'examen CREST Registered Penetration Tester
- Appliquer une méthodologie de test d'intrusion sur des cibles réseau, systèmes et web
- Réaliser la reconnaissance, l'énumération et l'analyse de vulnérabilités avec les outils adaptés
- Exploiter des vulnérabilités simples et collecter des preuves techniques exploitables
- Gérer le temps, les réponses et les priorités dans les conditions de l'évaluation pratique

Public visé

- Pentester
- Consultant en cybersécurité
- Analyste sécurité
- Auditeur de sécurité
- Administrateur systèmes et réseaux

Pré-requis

- Détenir une certification CREST CPSA valide, obligatoire pour se présenter à l'examen
- Maîtriser les fondamentaux des réseaux TCP/IP, du routage et des services courants
- Disposer de connaissances opérationnelles des systèmes Windows et Linux
- Connaître les bases des vulnérabilités applicatives, notamment SQL, XSS et l'authentification web

Pré-requis techniques

- PC équipé de Windows 10 ou 11, macOS ou Linux, avec processeur 64 bits et 16 Go de RAM recommandés
- Solution de virtualisation installée, telle que VMware Workstation Player, VMware Fusion ou VirtualBox
- Machine virtuelle Kali Linux fonctionnelle, avec au moins 60 Go d'espace disque disponible
- Connexion Internet stable, sans filtrage bloquant les téléchargements, dépôts logiciels et accès aux plateformes de laboratoire

Programme de notre formation CREST CRT

[Jour 1 - Matin]

Certification et méthodologie de test

- Positionnement de la certification CREST Registered Penetration Tester et compétences validées
- Structure de l'évaluation pratique, périmètre, notation et critères de réussite
- Cadre légal, autorisation de test, règles d'engagement et collecte de preuves
- Cycle de vie d'un test d'intrusion : reconnaissance, énumération, exploitation et restitution
- Atelier pratique : prise en main d'un laboratoire autorisé et qualification initiale d'une cible

[Jour 1 - Après-midi]

Reconnaissance et cartographie réseau

- Fondamentaux TCP/IP, segmentation, VLAN, routage et filtrage
- Découverte d'hôtes, identification de services et fingerprinting des systèmes
- Analyse des protocoles TCP, UDP, ICMP, ARP et DNS
- Utilisation raisonnée de Nmap et interprétation des résultats de scan
- Atelier pratique : cartographier un réseau de laboratoire, identifier les hôtes et prioriser les services exposés

[Jour 2 - Matin]

Services réseau et énumération

- Énumération des services DNS, SMB, LDAP, SNMP, SSH et FTP
- Recherche d'informations dans les bannières, partages, annuaires et configurations exposées
- Analyse des mécanismes de résolution de noms, dont NetBIOS, LLMNR et mDNS
- Identification des défauts de configuration et des chemins d'attaque à faible complexité
- Atelier pratique : conduire l'énumération de services d'une infrastructure et constituer un inventaire de preuves

[Jour 2 - Après-midi]

Analyse de vulnérabilités et exploitation simple

- Principes d'une analyse de vulnérabilités : détection, validation et qualification
- Utilisation de scanners et lecture critique des résultats, faux positifs et limites des outils
- Recherche de vulnérabilités connues et corrélation avec les versions de services
- Exploitation simple et récupération contrôlée de données de preuve
- Atelier pratique : analyser les résultats d'un scan, valider une vulnérabilité et récupérer une valeur de preuve

[Jour 3 - Matin]

Évaluation de la sécurité Windows

- Reconnaissance d'un hôte Windows, comptes, groupes, processus, services et correctifs
- Énumération locale et distante, partages, permissions et mécanismes d'administration
- Notions d'Active Directory, domaines, authentification et relations de confiance
- Identification des faiblesses liées aux mots de passe, aux droits et aux configurations de services
- Atelier pratique : énumérer un environnement Windows de laboratoire et identifier un chemin de compromission simple

[Jour 3 - Après-midi]

Évaluation de la sécurité Linux et Unix

- Reconnaissance des systèmes Linux et Unix, utilisateurs, processus et services
- Analyse des permissions de fichiers, répertoires sensibles et tâches planifiées
- Énumération des services distants, notamment NFS, RPC, SMTP et SSH
- Recherche de mauvaises configurations et de vulnérabilités exploitables à faible impact
- Atelier pratique : auditer un serveur Linux, identifier une faiblesse de permission et collecter une preuve

[Jour 4 - Matin]

Routage et environnements contraints

- Comprendre les chemins réseau, passerelles, tables de routage et réseaux inaccessibles directement
- Manipuler les routes dans un environnement contrôlé pour atteindre des services internes
- Approche de l'épreuve Desktop Lockdown et analyse des restrictions de poste
- Techniques de diagnostic, de vérification d'accès et de collecte de données dans un environnement limité
- Atelier pratique : atteindre un service isolé par manipulation de routage et extraire une information attendue

[Jour 4 - Après-midi]

Sécurité des applications web

- Reconnaissance d'applications web, cartographie des fonctionnalités, paramètres et technologies
- Contrôle de l'authentification, de l'autorisation, des sessions, des cookies et des jetons
- Identification des vulnérabilités SQL Injection, XSS, traversée de répertoires et téléversement de fichiers
- Utilisation de Burp Suite pour intercepter, rejouer et analyser les requêtes HTTP
- Atelier pratique : analyser une application web de laboratoire et exploiter une vulnérabilité pour obtenir une preuve

[Jour 5 - Matin]

Stratégie et gestion de l'examen

- Révision ciblée des domaines infrastructure et application évalués au CRT
- Gestion du temps sur une évaluation de 2 heures 30, lecture, priorisation et traitement parallèle des questions

- Prise en main de l'environnement Kali Linux fourni lors de l'examen
- Formulation des réponses courtes, saisie des valeurs de preuve et vérification avant soumission
- Atelier pratique : réaliser une série chronométrée de questions de type CRT avec analyse collective des réponses

[Jour 5 - Après-midi]

Simulation de certification et consolidation

- Simulation d'un parcours pratique combinant réseau, systèmes, routage et application web
- Application d'une démarche autonome de reconnaissance, d'analyse et d'exploitation
- Arbitrage entre les tâches, estimation de l'effort et optimisation du score potentiel
- Correction détaillée, retour sur les erreurs fréquentes et plan de révision avant l'examen
- Atelier pratique : simulation finale chronométrée d'un parcours CREST CRT et débriefing personnalisé

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.