

CompTIA PenTest+ Certification Prep Course

Durée: 5 Jours **Réf de cours: G015** **Version: PT0-003** **Méthodes d'apprentissage: Classe à distance**

Résumé:

Master the tools, techniques, and mindset of a professional penetration tester with hands-on training aligned to the CompTIA PenTest+ (PT0-003) exam

Pentest+ Certification Prep is designed to help learners confidently prepare for the CompTIA PenTest+ (PT0-003) exam, which validates the skills required to perform penetration testing and vulnerability management in a variety of IT environments. This course emphasizes hands-on, performance-based learning, guiding students through the full penetration testing process—from planning and scoping to exploitation and reporting. It's ideal for cybersecurity professionals who want to deepen their offensive security expertise and earn a globally recognized credential.

Students will explore the five domains covered in the PT0-003 exam: Planning and Scoping, Information Gathering and Vulnerability Identification, Attacks and Exploits, Reporting and Communication, and Tools and Code Analysis. Through practical labs, real-world scenarios, and exam-focused instruction, learners will gain experience using industry-standard tools and techniques to identify and exploit vulnerabilities, analyze systems, and communicate findings effectively. The course also reinforces ethical and legal considerations, ensuring students are prepared to operate responsibly in professional environments.

Whether you're pursuing a career as a penetration tester, vulnerability analyst, or security consultant, this course provides the structure and support needed to succeed on the PT0-003 exam and beyond. With updated content reflecting the latest threats and technologies, learners will be equipped to meet the demands of today's cybersecurity landscape.

Classe à Distance - site Client

Cette formation peut être suivie à distance en synchrone depuis n'importe quel site pourvu d'une connexion internet (2 Mb/s en symétrique recommandés). Le programme (théorie et pratique) suit le même déroulé pédagogique qu'en présentiel. La solution technologique adoptée permet aux apprenants à distance de suivre les présentations faites au tableau, de voir et d'entendre l'instructeur et les participants en temps réel, mais également d'échanger avec eux.

Public visé:

This course is best suited for IT and cybersecurity professionals who have foundational knowledge of network and system security and are looking to advance into offensive security roles. Learners are typically hands-on, analytical, and eager to develop practical skills in penetration testing, vulnerability assessment, and ethical hacking to enhance their career prospects or prepare for more advanced certifications.

Relevant Job Roles:

- Penetration Tester
- Vulnerability Analyst
- Security Consultant
- Red Team Member
- SOC Analyst (with offensive security focus)
- Cybersecurity Specialist
- Network Security Engineer
- Ethical Hacker

Objectifs pédagogiques:

- Plan and scope penetration tests while ensuring compliance with legal and ethical requirements, and develop detailed reports with remediation recommendations to support engagement management.
- Perform active and passive reconnaissance, gather information, and enumerate systems to uncover vulnerabilities effectively.
- Conduct vulnerability scans, analyze results, and validate findings to identify and address security weaknesses.
- Execute network, host-based, web application, and cloud-based attacks using appropriate tools and techniques to test system defenses.
- Maintain persistence, perform lateral movement, and document findings to support remediation efforts during post-exploitation activities.

Pré-requis:

To ensure your success in this course, you should have:

- Intermediate knowledge of information security concepts, including but not limited to identity and access management (IAM), cryptographic concepts and implementations, computer networking concepts and implementations, and common security technologies.
- Practical experience in securing various computing environments, including small to medium businesses, as well as enterprise environments.
- G005 - Préparation à la certification CompTIA Network+
- G013 - Formation CompTIA Security+

Après cette formation, nous vous conseillons le(s) module(s) suivant(s):

- GK2951 - CompTIA SecurityX Certification Prep Course
- GK5867 - CompTIA CySA+ Cybersecurity Analyst

Contenu:

- | | | |
|---|--|--|
| ■ Lesson 1: Scoping Organizational/Customer Requirements | ■ Lesson 8: Avoiding Detection and Covering Tracks | ■ Lesson 15: Scripting and Software Development |
| ■ Lesson 2: Defining the Rules of Engagement | ■ Lesson 9: Exploiting the LAN and Cloud | ■ Lesson 16: Leveraging the Attack: Pivot and Penetrate |
| ■ Lesson 3: Footprinting and Gathering Intelligence | ■ Lesson 10: Testing Wireless Networks | ■ Lesson 17: Communicating During the PenTesting Process |
| ■ Lesson 4: Evaluating Human and Physical Vulnerabilities | ■ Lesson 11: Targeting Mobile Devices | ■ Lesson 18: Summarizing Report Components |
| ■ Lesson 5: Preparing the Vulnerability Scan | ■ Lesson 12: Attacking Specialized Systems | ■ Lesson 19: Recommending Remediation |
| ■ Lesson 6: Scanning Logical Vulnerabilities | ■ Lesson 13: Web Application-Based Attacks | ■ Lesson 20: Performing Post-Report Delivery Activities |
| ■ Lesson 7: Analyzing Scanning Results | ■ Lesson 14: Performing System Hacking | |

Autres moyens pédagogiques et de suivi:

- Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
- Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
- En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

- Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
- Votre place sera confirmée à la réception d'un devis ou "booking form" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
- Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

- En cas de handicap : plus d'info sur globalknowledge.fr/handicap
- Le Règlement intérieur est disponible sur globalknowledge.fr/reglement