

## CompTIA PenTest+

Durée: 5 Jours    Réf de cours: G015    Version: PT0-002

### Résumé:

CompTIA PenTest+ is the most comprehensive cybersecurity exam covering all red team activities and is designed for cybersecurity professionals tasked with penetration testing and vulnerability management.

PenTest+ assesses the most up-to-date penetration testing, and vulnerability assessment and management skills necessary to determine the resiliency of the network against attacks. The CompTIA PenTest+ certification exam will verify successful candidates have the knowledge and skills required to: Plan and scope a penetration testing engagement Understand legal and compliance requirements Perform vulnerability scanning and penetration testing using appropriate tools and techniques, and then analyze the results Produce a written report containing proposed remediation techniques, effectively communicate results to the management team, and provide practical recommendations

### Public visé:

Penetration Tester Security Consultant Cloud Penetration Tester Web App Penetration Tester Cloud Security Specialist Network & Security Specialist

### Objectifs pédagogiques:

- **After completing this course you should be able to:**
- Explain the importance of planning and key aspects of compliance-based assessments.
- Conduct information gathering exercises with various tools and analyse output and basic scripts (limited to: Bash, Python, Ruby, PowerShell).
- Gather information to prepare for exploitation then perform a vulnerability scan and analyse results.
- Utilise report writing and handling best practices explaining recommended mitigation strategies for discovered vulnerabilities.
- Exploit network, wireless, application, and RF-based vulnerabilities, summarize physical security attacks, and perform post-exploitation techniques.

### Pré-requis:

#### Attendees should meet the following prerequisites:

- 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.
- CompTIA Network + or CompTIA Security + or equivalent knowledge
- Hands-on information security experience
- G005 - Préparation à la certification Network+ - Compétences support
- G013 - Formation CompTIA Security+

### Test et certification

#### Recommended as preparation for the following exams:

- **PT0-002** - CompTIA Pentest+ Certification

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

The following courses are recommended for further study.

- **GK5867** - CompTIA CySA+ Cybersecurity Analyst
- GK2951 - CompTIA Advanced Security Practitioner (CASP) 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	

## Méthodes pédagogiques :

PenTest+ is compliant with ISO 17024 standards and approved by the US DoD to meet directive 8140/8570.01-M requirements. Regulators and government rely on ANSI accreditation, because it provides confidence and trust in the outputs of an accredited program. Over 2.3 million CompTIA ISO/ANSI-accredited exams have been delivered since January 1, 2011.

## 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](http://moncompteformation.gouv.fr).

Accueil des bénéficiaires :

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