CompTIA PenTest+ Certification Prep Course

Duration: 5 Days Course Code: G015 Version: PT0-003

Overview:

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.

Company Events

These events can be delivered exclusively for your company at our locations or yours, specifically for your delegates and your needs. The Company Events can be tailored or standard course deliveries.

Target Audience:

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

Objectives:

- 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.

Prerequisites:

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 - CompTIA Network+
- G013 - CompTIA Security+

Follow-on-Courses:

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

Content:

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

Further Information:

For More information, or to book your course, please call us on Head Office Tel.: +974 40316639

training@globalknowledge.qa

www.globalknowledge.com/en-qa/

Global Knowledge, Qatar Financial Center, Burj Doha,Level 21, P.O.Box 27110, West Bay, Doha, Qatar