MERCURY

CompTIA PenTest+

Istanbul - Turkey: +90 539 599 12 06
Amman - Jordan: +962 785 666 966
London - UK: +44 748 136 28 02

MERCURY

CompTIA PenTest+

Introduction:

The CompTIA PenTest+ course is designed to equip aspiring cybersecurity professionals with the knowledge and practical skills required to effectively identify, exploit, and remediate vulnerabilities in network infrastructures. This comprehensive training program combines theoretical foundations with hands-on lab exercises, allowing participants to develop expertise in penetration testing techniques and methodologies. By the end of the course, students will have a strong understanding of how to conduct security assessments and enhance the overall security posture of organizations.

Targeted Groups:

- Cybersecurity professionals
- Network administrators
- System administrators
- Security analysts
- IT professionals interested in pursuing a career in penetration testing

Targeted Competencies:

To fully benefit from this course, participants should have a solid understanding of network protocols, operating systems, and security concepts. Additionally, familiarity with basic networking tools and techniques would be advantageous.

Course Objectives:

- Gain a solid understanding of penetration testing methodologies, including planning, scoping, and reconnaissance.
- Develop expertise in performing vulnerability assessments and identifying network security weaknesses.
- Learn various techniques for exploiting vulnerabilities, such as network attacks, web application attacks, and wireless attacks.
- Understand the importance of post-exploitation activities and learn how to assess and document potential impacts.
- Master the art of writing comprehensive penetration testing reports and effectively communicate findings to stakeholders.
- Familiarize yourself with legal and ethical considerations associated with penetration testing.
- Explore the latest tools and technologies used in the field of penetration testing.

Course Outline:

Unit 1: Introduction to Penetration Testing

- Understanding the fundamentals of penetration testing
- Legal and ethical considerations
- Scoping and planning a penetration test
- Information gathering and reconnaissance techniques

Istanbul - Turkey: +90 539 599 12 06
Amman - Jordan: +962 785 666 966
London - UK: +44 748 136 28 02

Unit 2: Vulnerability Assessment and Exploitation

- Performing vulnerability assessments and scans
- Exploiting network vulnerabilities
- Exploiting web application vulnerabilities
- Exploiting wireless network vulnerabilities

Unit 3: Post-Exploitation and Reporting

- Assessing post-exploitation impacts
- Escalating privileges and maintaining access
- Writing effective penetration testing reports
- Communicating findings to stakeholders

Unit 4: Advanced Techniques and Tools

- Exploiting cloud-based environments
- Advanced network attacks and defenses
- Web application security testing methodologies
- Wireless network security testing methodologies

Unit 5: Real-World Penetration Testing

- Conducting a comprehensive penetration test
- Engaging in red teaming exercises
- Social engineering techniques and countermeasures
- Physical security assessments