multisoft
Systems

CompTIA Pentest+ (PT0-002) Training

COURSE CONTENT

GET IN TOUCH

Multisoft Systems
B - 125, Sector - 2, Noida

(+91) 9810-306-956

info@multisoftsystems.com

www.multisoftsystems.com

About Multisoft

Train yourself with the best and develop valuable in-demand skills with Multisoft Systems. A leading certification training provider, Multisoft collaborates with top technologies to bring world-class one-on-one and certification trainings. With the goal to empower professionals and business across the globe, we offer more than 1500 training courses, which are delivered by Multisoft's global subject matter experts. We offer tailored corporate training; project Based Training, comprehensive learning solution with lifetime e-learning access, after training support and globally recognized training certificates.

About Course

The CompTIA PenTest+ (PT0-002) training offered by Multisoft Systems is designed for cybersecurity professionals looking to advance their skills in penetration testing and vulnerability management. This comprehensive course covers the latest practices for assessing, identifying, and managing network vulnerabilities effectively.

Module 1: Planning and Scoping

- ✓ Compare and contrast governance, risk, and compliance concepts
- ✓ Explain the importance of scoping and organizational/customer requirements
- ✓ Demonstrate an ethical hacking mindset by maintaining professionalism and integrity

Module 2: Information Gathering and Vulnerability Scanning

- ✓ Perform passive reconnaissance
- ✓ perform active reconnaissance
- ✓ Analyze the results of a reconnaissance exercise
- ✓ Perform vulnerability scanning

Module 3: Attacks and Exploits

- ✓ Research attack vectors and perform network attacks
- ✓ Research attack vectors and perform wireless attacks
- ✓ Research attack vectors and perform application-based attacks
- ✓ Research attack vectors and perform attacks on cloud technologies
- ✓ Explain common attacks and vulnerabilities against specialized systems
- ✓ Perform a social engineering or physical attack
- ✓ Perform post-exploitation techniques

Module 4: Reporting and Communication

- ✓ Compare and contrast important components of written reports
- ✓ Analyze the findings and recommend the appropriate remediation within a report
- ✓ Explain the importance of communication during the penetration testing process
- ✓ Explain post-report delivery activities

Module 5: Tools and Code Analysis

- ✓ Explain the basic concepts of scripting and software development

- ✓ Analyze a script or code sample for use in a penetration test
- ✓ Explain use cases of the following tools during the phases of a penetration test