CompTIA Pentest+

Duration : 4 Days.

Exam :

- CompTIA PenTest+ Exam
  - Number of Questions: Maximum of 110
  - Type of Questions: Multiple choice and performance based
  - Duration: 165 minutes

This exam is currently in beta, which means that your exam scores will only be available in summer 2018. The beta exam scores are only numbered scores and will not include a breakdown of exam objectives. The beta status will end when 400 people have taken the beta exam or April 25, 2018.

TOC

Planning and Scoping

- Explain the importance of planning for an engagement
- Explain key legal concepts.
- Explain the importance of scoping an engagement properly.
- Explain the key aspects of compliance-based assessments.

Information Gathering and Vulnerability Identification

- Given a scenario, conduct information gathering using appropriate techniques
- Given a scenario, perform a vulnerability scan.
- Given a scenario, analyse vulnerability scan results
- Explain the process of leveraging information to prepare for exploitation.
- Explain weaknesses related to specialised systems

Attacks and Exploits

- Compare and contrast social engineering attacks
- Given a scenario, exploit network-based vulnerabilities
- Given a scenario, exploit wireless and RF-based vulnerabilities
- Given a scenario, exploit application-based vulnerabilities
- Given a scenario, exploit local host vulnerabilities
- Summarise physical security attacks related to facilities
- Given a scenario, perform post-exploitation techniques

Penetration Testing Tools

- Given a scenario, use Nmap to conduct information gathering exercises
- Compare and contrast various use cases of tools
- Given a scenario, analyse tool output or data related to a penetration test
- Given a scenario, analyse a basic script (limited to Bash, Python, Ruby, and PowerShell)

Reporting and Communication

- Given a scenario, use report writing and handling best practices
- Explain post-report delivery activities
- Given a scenario, recommend mitigation strategies for discovered vulnerabilities
- Explain the importance of communication during the penetration testing process