CompTIA PenTest+

Course Outline

Module 1: Introduction to Ethical Hacking and Penetration Testing
- Understanding Ethical Hacking and Penetration Testing
- What is the Difference Between Ethical Hacking and Nonethical Hacking?
- Understanding the Current Threat Landscape
- Exploring Penetration Testing Methodologies
- Penetration Testing Methods

Module 2: Planning and Scoping a Penetration Testing Assessment
- Explaining the Importance of the Planning and Preparation Phase
- Understanding the Legal Concepts of Penetration Testing
- Learning How to Scope a Penetration Testing Engagement Properly
- Learning the Key Aspects of Compliance-Based Assessments

Module 3: Information Gathering and Vulnerability Identification
- Understanding Information Gathering and Reconnaissance
- Understanding the Art of Performing Vulnerability Scans
- Understanding How to Analyze Vulnerability Scan Results

Module 4: Social Engineering Attacks
- Understanding Social Engineering Attacks
- Phishing
- Pharming
- Malvertising
- Spear Phishing
- SMS Phishing
- Voice Phishing
- Whaling
- Elicitation, Interrogation, and Impersonation (Pretexting)
- Social Engineering Motivation Techniques
- Shoulder Surfing
- USB Key Drop and Social Engineering

Module 5: Exploiting Wired and Wireless Networks
- Exploiting Network-Based Vulnerabilities
- Exploiting Wireless and RF-Based Attacks and Vulnerabilities

Module 6: Exploiting Application-Based Vulnerabilities
- Overview of Web Applications for Security Professionals
- How to Build Your Own Web Application Lab
- Exploiting Authentication-Based Vulnerabilities
- Exploiting Authorisation-Based Vulnerabilities
- Understanding Cross-Site Scripting (XSS) Vulnerabilities
- Understanding Cross-Site Request Forgery Attacks

- Understanding Clickjacking
- Exploiting Security Misconfigurations
- Exploiting File Inclusion Vulnerabilities
- Exploiting Insecure Code Practices

Module 7: Exploiting Local Host and Physical Security Vulnerabilities
- Exploiting Local Host Vulnerabilities
- Understanding Physical Security Attacks

Module 8: Performing Post-Exploitation Techniques
- Maintaining Persistence After Compromising a System
- Understanding How to Perform Lateral Movement
- Understanding How to Cover Your Tracks and Clean Up Systems After a Penetration Testing Engagement

Module 9: Penetration Testing Tools
- Understanding the Different Use Cases of Penetration Testing Tools and How to Analyze Their Output
- Penetration Testing–Focused Linux Distributions
- Common Tools for Reconnaissance and Enumeration
- Encapsulation and Tunneling Using DNS and Other Protocols Like NTP
- Common Decompilation, Disassembling, and Debugging Tools
- Leveraging Bash, Python, Ruby, and PowerShell in Penetration Testing Engagements

Module 10: Understanding How to Finalize a Penetration Test
- Explaining Post-Engagement Activities
- Surveying Report Writing Best Practices
- Understanding the Importance of a Quality Report
- Discussing Best Practices of Writing a Penetration Testing Report
- Understanding Report Handling and Communications Best Practices