CompTIA PenTest+

Duration 5 Days

COURSE DESCRIPTION

CompTIA PenTest+ is a certification for intermediate skills level cybersecurity professionals who are tasked with hands-on penetration testing to identify, exploit, report, and manage vulnerabilities on a network. PenTest+ is unique because the certification requires a candidate to demonstrate the hands-on ability and knowledge to test devices in new environments such as the cloud and mobile, in addition to traditional desktops and servers.

COURSE OBJECTIVES

After completing this course, you will accomplish following:

- 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.
- Conduct information gathering using appropriate techniques.
- Perform a vulnerability scan.
- Analyze vulnerability scan results.
- Explain the process of leveraging information to prepare for exploitation.
- Explain weaknesses related to specialized systems.
- Compare and contrast social engineering attacks.
- Exploit network-based vulnerabilities.
- Exploit wireless and RF-based vulnerabilities.
- Exploit application-based vulnerabilities.
- Exploit local host vulnerabilities.
- Summarize physical security attacks related to facilities.
- Perform post-exploitation techniques.
- Use Nmap to conduct information gathering exercises.
- Compare and contrast various use cases of tools.
- Analyze tool output or data related to a penetration test.
- Analyze a basic script (limited to Bash, Python, Ruby, and PowerShell) Reporting and Communication.
- Use report writing and handling best practices.
- Explain post-report delivery activities.
- Recommend mitigation strategies for discovered vulnerabilities.
- Explain the importance of communication during the penetration testing process.

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th
Call us today 0-2634-7993-4
177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th

COURSE OUTLINE

Lesson 1: Planning and Scoping Penetration Tests

- Introduction to Penetration Testing Concepts
- Plan a Pen Test Engagement
- Scope and Negotiate a Pen Test Engagement
- Prepare for a Pen Test Engagement

Lesson 2: Conducting Passive Reconnaissance

- Gather Background Information
- Prepare Background Findings for Next Steps

Lesson 3: Performing Non-Technical Tests

- Perform Social Engineering Tests
- Perform Physical Security Tests on Facilities

Lesson 4: Conducting Active Reconnaissance

- Scan Networks
- Enumerate Targets
- Scan for Vulnerabilities
- Analyze Basic Scripts

Lesson 5: Analyzing Vulnerabilities

- Analyze Vulnerability Scan Results
- Leverage Information to Prepare for Exploitation

Lesson 6: Penetrating Networks

- Exploit Network-Based Vulnerabilities
- Exploit Wireless and RF-Based Vulnerabilities
- Exploit Specialized Systems

Lesson 7: Exploiting Host-Based Vulnerabilities

- Exploit Windows-Based Vulnerabilities
- Exploit *Nix-Based Vulnerabilities

Lesson 8: Testing Applications

- Exploit Web Application Vulnerabilities
- Test Source Code and Compiled Apps

Lesson 9: Completing Post-Exploit Tasks

- Use Lateral Movement Techniques
- Use Persistence Techniques
- Use Anti-Forensics Techniques

Lesson 10: Analyzing and Reporting Pen Test Results

- Analyze Pen Test Data
- Develop Recommendations for Mitigation Strategies
- Write and Handle Reports
- Conduct Post-Report-Delivery Activities

PREREQUISITES

- 3-4 years of hands-on information security or related experience
- Network+, Security+, or equivalent knowledge

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th
Call us today 0-2634-7993-4
177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th