QUICKSTART

Over 35 Years Of Technology Training

Document Generated: 12/15/2025

Learning Style: On Demand

Technology:

Difficulty: Advanced

Course Duration: 7 Hours

Certified Penetration Testing Consultant

About this Exam:

We should have an understanding of what Penetration Testing is. Penetration testing (also known as pen testing) is the act of testing a PC framework, Web application or network to discover vulnerabilities that an assailant could abuse. Penetration testing ordinarily incorporates network application security testing and Penetration testing and also procedures and controls around the systems and applications and ought to happen from both outside the network attempting to come in (outer testing) and from inside the system. This propelled level credential course is intended for IT Network Administrators and IT Security Professionals who are keen on leading Penetration tests against enormous system foundations like Services Providers, huge corporate networks, and Telecommunication Companies. This credential course helps the understudies in the preparation for the Certification Exam of CPTC.

The normal compensation for a Certified Penetration Testing Consultant is $88,080 every year.

Course Objective:

- Set up an industry acceptable process for pen testing
- Packet Capturing
- Layer 2 Attacks
- Pivoting and Relays
- Layer 3 Attacks on Cisco Based Infrastructures
- IPv6 Attacks
- Defeating SSL
- VPN Attacks
- IDS/IPS Evasion

Audience:

This course is designed for:

- Cyber Security Admins and Managers
- IS Security Officers
- Penetration Testers
- Auditors
- Ethical Hackers

Prerequisites:

- At least 2 years of experience in Networking Technologies
- Computer hardware knowledge
- Sound knowledge of TCP/IP

Suggested prerequisites courses:

- Certified Security Leadership Officer

- Software-Defined Networking Fundamentals - LFS265
- Linux Networking and Administration - LFS211

Course Outline:

This Course Includes:

- Module 1 - Pentesting Team Formation
- Module 2 - NMAP Automation
- Module 3 - Exploitation Process
- Module 4 - Fuzzing with Spike
- Module 5 - Writing Simple Buffer Overflow Exploits
- Module 6 - Stack Based Windows Buffer Overflow
- Module 7 - Web Application Security and Exploitation
- Module 8 - Linux Stack Smashing
- Module 9 - Linux Address Space Layout Randomization
- Module 10 - Windows Exploit Protection
- Module 11 - Getting Around SEH and ASLR (Windows)
- Module 12 - Penetration Testing Report Writing