C)PTC Certified Penetration Testing Consultant

Course Summary

Description

The Certified Penetration Testing Consultant, C)PTC , course is designed for IT Security Professionals and IT Network Administrators who are interested in taking an in-depth look into specific penetration testing techniques used against operating systems. This course will teach you the necessary skills to work with a penetration testing team, the exploitation process, and how to create a buffer overflow against programs running on Windows and Linux while subverting features such as DEP and ASLR.

Topics

- Penetration Testing Team Formation
- NMAP Automation
- Exploitation Process
- Fuzzing with Spike
- Simple Buffer Overflow
- Stack Based Windows Buffer Overflow
- Web Application Security and Exploitation
- Linux Stack Smashing & Scanning
- Linux Address Space Layout Randomization
- Windows Exploit Protection
- Getting Around SEH ASLR
- Penetration Testing Report Writing

- Lab 1 – Skills Assessment
- Lab 2 – Automation Breakdown
- Lab 3 – Fuzzing with Spike
- Lab 4 – Let's Crash and Callback
- Lab 5 – Minishare for the Win
- Lab 6 – WebGoat Exploitation
- Lab 7 – Stack Overflow, Did we get Root
- Lab 8 – Defeat Me and Lookout ASLR
- Lab 9 – Time to Overwrite SEH and ASLR
- Lab 10 – Windows Exploit Protection
- Lab 11 – Getting AroundSEH ASLR
- Lab 12 – Penetration Testing Report Writing

Audience

- IS Security Officers
- Cybersecurity Managers/Administrators
- Penetration Testers
- Ethical Hackers
- Auditors

Prerequisites

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

Duration

Five days
CPEs 40