C)PTC: Certified Penetration Testing Consultant

Course ID #: 7000-814-ZZ-Z

Hours: 35

Course Content

Course Description:

In this course, you will cover an in-depth look into specific penetration testing and 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.

Course Objectives:

Upon successful completion of this course students will:

- Have solid knowledge of testing and reporting proceedures which will prepare them for upper management roles within a cybersecurity system
- Be able to competently take the C)PTC exam

Prerequisites:

- C)PEH and C)PTE or equivalent knowledge
- 2 years of experience in Networking Technologies
- Sound Knowledge of TCP/IP
- Computer Hardware Knowledge

Target Audience:

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

Topics:

Lesson 1 – Pentesting Team Foundation

- Project Management
- Pentesting Metrics
- Team Roles, Responsibilities and Benefits

Lesson 2 – NMAP Automation

- NMAP Basics
- NMAP Automation
- NMAP Report Documentation

Lesson 3 – Exploitation Processes

- Purpose
- Countermeasures
- Evasion
- Precision Strike
- Customized Exploitation
- Tailored Exploits
- Zero Day Angle
- Example Avenues of Attack
- Overall Objective of Exploitation

C)PTC: Certified Penetration Testing Consultant

Course ID #: 7000-814-ZZ-Z

Hours: 35

Lesson 4 – Fuzzing with Spike
- Vulnserver
- Spike Fuzzing Setup
- Fuzzing a TCP Application
- Custom Fuzzing Script

Lesson 5 – Privilege Escalation
- Exploit-DB
- Immunity Debugger
- Python
- Shellcode

Lesson 6 – Stack Based Windows Buffer Overflow
- Debugger
- Vulnerability Research
- Control EIP, Control the Crash
- JMP ESP Instruction
- Finding the Offset
- Code Execution and Shellcode
- Does the Exploit Work?

Lesson 7 – Web Application Security and Exploitation
- Web Applications
- OWASP Top 10 - 2017
- Zap
- Scapy

Lesson 8 – Linux Stack Smashing
- Exploiting the Stack on Linux

Lesson 9 – Linux Address Space Layout Randomization
- Stack Smashing to the Extreme

Lesson 10 – Windows Exploit Protection
- Introduction to Windows Exploit Protection
- Structured Exception Handling
- Data Execution Prevention (DEP)
- SafeSEH/SEHOP

Lesson 11 – Getting Around SEH and ASLR (Windows)
- Vulnerable Server Setup
- Time to Test it Out
- "Vulnserver" meets Immunity
- VulnServer Demo

Labs:

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 – Stack Overflow: Did we get root?
Lab 7 – Defeat Me and Lookout ASLR
Lab 8 – Time to Overwrite SHE and ASLR

Accreditations:

Register for this class by visiting us at:
www.tcworkshop.com or calling us at 800-639-3535