Current Technologies
Computer Learning Centers

EC-Council

6210 Central Ave, Portage, IN. 46368 Phone: 219.764.3800 Fax: 219.764.3805 Web: http://www.ctclc.com

Certified Penetration Testing Professional (CPENT)

This course teaches you how to perform an effective penetration test in an enterprise network environment that must be attacked, exploited, evaded, and defended. If you have only been working in flat networks, CPENT's live practice range will teach you to take your skills to the next level by teaching you how to pen test IoT systems, OT systems, how to write your own exploits, build your own tools, conduct advanced binaries exploitation, double pivot to access hidden networks, and also customize scripts/exploits to get into the innermost segments of the network.

How you'll benefit

This class will help you:

- Focus on the latest technologies including Cloud, IoT, Virtualization and Remote Worker Threats, Attack Surface Analysis, Threat Intelligence, Software Defined Networks (SDN), and Network Function Virtualization (NFV), as well as docker, Kubernetes, and container security.

Why Attend with Current Technologies CLC

- Our Instructors are in the top 10%
- Our Lab has a dedicated 1 Gig Fiber Connection for our Labs
- Our Labs Run up to Date Code for all our courses

Objectives

Upon completing this course, the student will be able to meet these objectives:

- Work Advanced Windows Attacks
- Attacking IoT Systems
- Writing Exploits: Advanced Binary Exploitation
- Bypassing a Filtered Network
- Pentesting Operational Technology (OT)
- Access Hidden Networks with Pivoting
- Double Pivoting
- Privilege Escalation
- Evading Defense Mechanisms
- Attack Automation with Scripts
- Weaponize Your Exploits
- Write Professional Reports

Course Duration

5 days

Course Price

$3,495.00

Methods of Delivery

- Instructor Led
- Virtual ILT
- On-Site

Certification Exam

CPENT exam 112-12

Who Should Attend

The job roles best suited to the material in this course are:

Certified Penetration Testing Professional (CPENT)

- Penetration Testers
- Ethical Hackers
- Information Security Consultant
- Security Testers
- Security Analysts
- Security Engineers
- Network Server Administrators
- Firewall Administrators
- Systems Administrators
- Risk Assessment Professionals

AGE REQUIREMENTS AND POLICIES CONCERNING MINORS

- The age requirement for attending the training or attempting the CSCU exam is restricted to any candidate that is at least 13 years old.
- If the candidate is under the age of 13, they are not eligible to attend the official training or eligible to attempt the certification exam unless they provide the accredited training center (ATC) or EC-Council a written consent of their parent or their legal guardian and a supporting letter from their institution of higher learning. Only applicants from nationally accredited institutions of higher learning shall be considered.

Disclaimer

- EC-Council reserves the right to impose additional restriction to comply with the policy. Failure to act in accordance with this clause shall render the authorized training center (ATC) in violation of their agreement with EC-Council. EC-Council reserves the right to revoke the certification of any person in breach of this requirement.

Perquisites

To fully benefit from this course, you should have the following knowledge:

- Knowledge attained from Certified Network Defender Course
- Knowledge attained from Certified Ethical Hacker Course

6210 Central Ave, Portage, IN. 46368 Phone: 219.764.3800 Fax: 219.764.3805 Web: http://www.ctclc.com

Certified Penetration Testing Professional (CPENT)

Outline

Module 01: Introduction to Penetration Testing

Module 02: Penetration Testing Scoping and Engagement

Module 03: Open Source Intelligence (OSINT)

Module 04: Social Engineering Penetration Testing

Module 05: Network Penetration Testing – External

Module 06: Network Penetration Testing– Internal

Module 07: Network Penetration Testing – Perimeter Devices

Module 08: Web Application Penetration Testing

Module 09: Wireless Penetration Testing

Module 10: IoT Penetration Testing

Module 11: OT/SCADA Penetration Testing

Module 12: Cloud Penetration Testing

Module 13: Binary Analysis and Exploitation

Module 14: Report Writing and Post Testing Actions