C)PTE™ CERTIFIED PENETRATION TESTING ENGINEER

mile2 AUTHORIZED PARTNER RESOURCES

C)PTEngineer™

Saturday –Wednesday
5 days
31 March – 4 April
8:30 — 16:30

30% Earlybird registration discount before 15/3/2012 to become the cost 1000$

Certified Penetration Testing Engineer (CPTE)

will obtain real world security knowledge enabling them to recognize vulnerabilities, exploit system weaknesses, and safeguard organizations against threats. Graduates will learn the art of Ethical Hacking with a professional edge (Penetration Testing).

The CPTEngineer presents information based on the 5 Key Elements of Pen Testing:

- Information Gathering,
- Scanning,
- Enumeration,
- Exploitation
- Reporting.

System vulnerabilities will be discovered using these tried and true steps alongside the use of the latest hacking techniques.

Objective of Labs :

This is an intensive hands-on class. Students may spend 20 hours or more performing labs that walk them through a real world Pen Testing model. Labs begin with simple activities and move on to more complex procedures. During labs, students move through a detailed Lab Guide containing screen shots, commands to be typed, and steps students should take. will make use of scores of traditional and cutting edge Pen Testing tools (GUI and command line, Windows and Linux) as they make their way through mile2's time-tested methodology. (See Outline below for tool titles) Customers can be confident that as new methods arise in the security world, our labs are updated to reflect them

Upon Completion:

Upon proper completion of the course, CPTEngineer students will be able to confidently sit for the CPTEngineer certification exam (recommended). Students will enjoy an in-depth course that is continuously updated to maintain and incorporate changes in the security environment. This course offers up-to-date proprietary labs that have been researched and developed by leading security professionals from around the world

Certified Penetration Testing Engineer

Module Topics:

Module 0: Course Overview
Module 1: Business and Technical Logistics of Pen Testing
Module 2: Financial Sector Regulations
Module 3: Information Gathering
Module 4: Detecting Live Systems
Module 5: Enumeration
Module 6: Vulnerability Assessments
Module 7: Malware, Trojans and BackDoors
Module 8: Windows Hacking
Module 9: Hacking UNIX/Linux
Module 10: Advanced Exploitation Techniques
Module 11: Pen Testing Wireless Networks
Module 12: Networks, Sniffing and IDS
Module 13: Injecting the Database
Module 14: Attacking Web Technologies
Module 15: Report Writing

Student Materials:

- Student Workbook
- Student CD
- Key Security Concepts & Definitions Book
- Quick Tips section, Summary section
- Questions and answers for each module

Information and Communication Technology Center ICTC

Tel: 02 2 2964571,2,3 EXT: 168;128 Mobile: 00972 59 7777277 Fax: 00972 2 2964995 Email: training @qou.edu

www.qou.edu