

## Certified Pen Testing Specialist – Web Analysis

### KEY DATA



#### Course Name:

Certified Pen Testing Specialist  
– Web Analysis

**Duration:** 5 days

**Language:** English

#### Format:

Instructor-led (Lecture and Lab)

#### Prerequisite:

- Mandatory – basic knowledge of a high level language such as C, Java, Perl, PHP and C#
- Knowledge of information security principles
- Basic understanding of networking protocols
- Completion of CPTS or equivalent Knowledge

#### Student Materials:

- Student Workbook with labs
- Mile2 CD Case
- Student CD
- Mile2 Notebook
- Mile2 Pen



### BENEFITS OF THIS COURSE

This 5-day course delivers a strong and in-depth knowledge of Web Penetration Testing principles and practices. An instructor-led lecture mixed with hands-on practical application will deliver an overview of the principles and practices of Web Penetration Testing. Emphasis is on World Wide Web penetration testing based on the understanding of the web architecture and the languages used to develop web applications

### COURSE OVERVIEW

This course seeks to establish the fundamental architecture and languages of the web as it applies to penetration testing together with the fundamental practices of Web Penetration Testing. The various types of vulnerabilities found in software today will be explained while providing hands-on training in the art of Web Penetration Testing.

### UPON COMPLETION

Whereas this course is not an in-depth programming class or a low-level assembly language class, nevertheless, participants will gain a sound understanding of common vulnerabilities inherent in prevailing web software. They will gain knowledge of the principles of Web Penetration Testing and practise these principles with lessons designed to be as real-world as possible.

### COURSE DETAILS

#### Modules

1. Introduction
2. Business and Technical Logistics of Web Penetration Testing
3. Web Architecture
4. Information Gathering
5. Fingerprinting
6. Code Vulnerability Basics
7. Scanning and Assessment
8. Enumeration of Possible Weak Points
9. Penetration
10. Other Issues

## DETAILED MODULE DESCRIPTION

### 1. Introduction

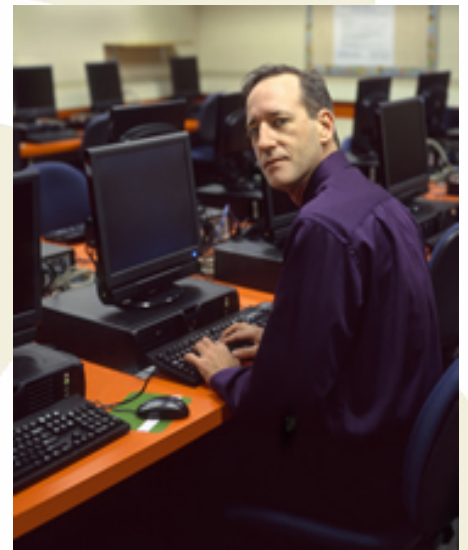
- Course Objectives
  - Principles (Theoretical)
  - Practices (Practical)
- Resources
  - Helpful websites
  - Tools

### 2. Business and Technical Logistics of Web Penetration Testing

- Soft side of Web based Penetration Testing
  - Business reasons to test
  - Legal issues when testing
  - Ethics

### 3. Web Architecture

- Client Architecture
  - HTML/XML
  - Cookies
  - Caching
  - Scripting
  - Applets
  - Plugins
  - Server Side Architecture
    - SSL
    - Proxies
      - Caching
      - Reverse
    - Applications
      - Server side includes
      - SSH Tunnel
      - Databases
      - Java (Tomcat/Jakarta)
      - Scripting Languages
        - PHP
        - ModPerl
        - TCL
        - Ruby
      - Languages
        - C
        - C++
        - Fortran
        - VB
    - XSS (Cross Site Scripting)
    - SUEXEC
    - Encryption
      - SSL
      - Other methods
  - Design Lab



#### 4. Information Gathering

- Public Website Information
  - Whois
  - Searching for information about a website
    - IP and Ports
    - Basic understanding of what the website does
      - Search Engine
      - Database Frontend
      - Application
  - Other sources of information
- Information Gathering Lab

#### 5. Fingerprinting

- Port Scanners (nmap)
- Port and Application Scanners (nessus)
- Fingerprinting Lab

#### 6. Code Vulnerability Basics

- Vulnerabilities in code
  - Architectural Flaws
  - Design Flaws
  - Code Flaws
- Code Lab

#### 7. Scanning and Assessment

- Is there dynamic content?
  - Which backend tool is in use
    - Header output inspection
    - Webpage inspection
- Assessment Labs

#### 8. Enumeration of Possible Weak Points

- Designing an attack
  - Use enumeration and understanding of how the code works
  - Think outside the box
- Design Labs

#### 9. Penetration

- Crafting Attacks
  - Techniques w/Nessus
- Penetration Labs

#### 10. Other Issues

- Mandatory Access Controls
- Enhanced Encryption