SecureIOT Academy Sdn. Bhd.

A subsidiary of SysArmy

Certified Penetration Testing Engineer

The module was developed around principles and behaviours used to combat malicious hackers and focuses on professional penetration testing. In this course, you will go through a complete penetration test from A-Z!

Venue : Suite 12-12, Level 12th, Wisma Zelan No1, Jalan Tasik Permaisuri 2, Bandar Tun Razak, 56000, Kuala Lumpur.

Key Information

Duration: 5 days

Class Format Options:

- Instructor-led classroom

Prerequisites:

- A minimum of 12 months experience in networking technologies
- Sound knowledge of TCP/IP
- Knowledge of Microsoft packages
- Network+, Microsoft, Security+
- Basic Knowledge of Linux is essential

Student Material:

- Student Workbook
- Student Lab Guide
- Prep Guide

CPEs: 40

Who Should Attend:

- Pen Testers
- Ethical Hackers
- Network Auditors
- Cyber Security Professionals
- Vulnerability Assessors
- Cyber Security Managers
- IS Managers

Please contact
commercial@sysarmy.net
for more information

What You Will Learn?

Course Content

Module 0: Course Overview
Module 1: Business &Technical Logistics of Pen Testing
Module 2: Linux Fundamentals
Module 3: Information Gathering
Module 4: Detecting Live Systems
Module 5: Enumeration
Module 6: Vulnerability Assessments
Module 7: Malware Goes Undercover
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: Project Documentation
Module 16: Securing Windows w/ Powershell
Module 17: Pen Testing with Powershell

Lab Content

Lab 1: Introduction to PenTesting Setup
Lab 2: Linux Fundamentals
Lab 3: Using Tools for Reporting
Lab 4: Information Gathering
Lab 5: Detecting Live System - Scanning Techniques
Lab 6: Enumeration
Lab 7: Vulnerability Assessments
Lab 8: Software Goes Undercover
Lab 9: System Hacking - Windows Hacking
Lab 10: System Hacking - Linux/Unix Hacking
Lab 11: Advance Vulnerability and Exploitation Techniques
Lab 12: Network Sniffing/IDS
Lab 13: Attacking Databases
Lab 14: Attacking Web Applications

ACCREDITATIONS

CNSS

NICCS™ NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES

mile2

is **ACCREDITED** by the **NSA CNSS 4011-4016**
Is **MAPPED** to NIST/Homeland Security NICCS's Cyber Security Workforce Framework
is **APPROVED** on the **FBI Cyber Security Certification Requirement list (Tier 1-3)**