Course Introduction

This class has been designed for any security personnel whose job duties involve assessing target networks and systems to find security vulnerabilities. And it also covers issues that matters in performing professional penetration test including legal issues, how to properly conduct a penetration test as well as best practice in both technical and non-technical techniques specific to a penetration test.

Learning Level

- Advance

Course Duration

- 5 Days

Course Prerequisite

- Deep understanding of networking, Familiar with Linux environment, Programming, Ready to be out-of-the-box

Target Group

- All Information Security related jobs.

Course Outline

Day 1 – Planning, Scope, Initiation, Information Gathering

– The mindset of a penetration tester.
– Types of penetration tests.
– Limitations of penetration testing.
– How to create a testing infrastructure.
– Defining rules of engagement and scoping a project.
– Reporting
– A pen tester's tool chest of information gathering resources.

Day 2 – Scanning and Enumeration

– Types of scans - Network sweeps, network tracing, port scans, OS fingerprinting, version scans, and vulnerability scans.

– Network mapping.

– Port scanning

– OS Fingerprinting.

– Vulnerability Scanning.

Day 3 – Gaining Access and Post-Exploitation Activities

– Exploit categories - server-side, client-side, and local privilege escalation

– Metasploit Framework

– The Metepreter

– Exploit without Metasploit

– Backdooring

– Transferring file techniques

– Windows commandline for penetration tester

Day 4 – Password attack and Wireless attack

– Passwords

– Password attack

– Password Guessing with Hydra

– Knowing password format in Windows and Linux

– Dumping Windows Hash

– Offline password attack with John the Ripper

– Cain

– Rainbow table attacks using Ophcrack

– Pass-the-hash attacks

Day 5 – Web application attack

– Web application scanning and exploitation tools

– Web application manipulation tools

– Injection attacks

– Building a wireless pentest platform

– Identifying unsecured access points and peer-to-peer systems

– Identifying wireless misconfigurations

– Exploiting various wireless protocols

Official Training Partner