PEN

Professional Penetration Testing Techniques and Vulnerability Assessment

Course Introduction

Today Hackers are everywhere, if your corporate system connects to internet that means your system might be facing with hacker. This five days course "Professional Penetration Testing Techniques and Vulnerability Assessment" brings you a hands-on course focusing on hacking techniques and how to counterattack them.

The course revolves around series of exercises based on "hacking" into a network (penetration testing the network) and then defending against the hacks. This hands-on course focusing on hacking techniques, exploit techniques, vulnerability assessment and penetrating testing techniques.

Participants will gain hacking techniques to perform penetration testing for the organization and with the same basis participants can use for countermeasures.

Course Objectives

- To understand how to examine vulnerabilities of your network and systems
- To understand how to develop participants' skills and knowledge in performing vulnerability assessment (VA) and penetration testing (Pen-Testing)
- To provide a structured methodology for detailing the practices and techniques an advanced penetration testing professional uses in assessing the security of networks.
- To understand how to develop advanced participants' skills all aspects of a network security assessment.

Course Highlights

- Windows and Linux Penetration testing tools provided
- Real World experience penetration testing from Instructor
- Free membership for ACIS Alumni
    - Access to the latest information related to the course subjects
    - A life-time class re-sit

Learning Level

- Advanced

Course Duration

- 5 Days (30 Hours)

Prerequisites

- Basic knowledge Network architecture
- Basic knowledge Operating System

Target Group

- IT Auditors
- IT Security Officer
- Anyone interested in learning vulnerability assessment and penetration testing

Course Outline

Module 1: Information Security Testing Overview

- Information Security Testing Policy
- Information Security Testing Methodologies
  - The Open Source Security Testing Methodology (OSSTMM)
  - The Information Systems Security Assessment Framework (ISSAF)
  - The NIST Guideline on Network Security Testing (SP 800-115)
- Information Security Testing Techniques
  - Passive and Active
  - DEMO: Passive and Active Gathering/Scanning
  - White-Box and Black-Box Approach
  - Blue Team and Red Team
- Phases in Information Security Testing
- Legal Perspective

Module 2: Foot printing and Information Gathering

- How information about a target may be gathered discreetly
- Acquiring target information (Passive Reconnaissance)
  - NICs
  - DNS Anonymous Zone Transfer
  - Web Archives/Statistics
  - Social Networking Web Sites
- Scanning and enumerating resources (Active Reconnaissance)
  - Network Mapping
  - LAB: Network Scanners
  - Operating System and Services banner grabbing
  - Operating System and Services Fingerprinting
  - LAB: Service and OS Scanners
- NetBIOS Name Service Enumeration
  - LAB: NetBIOS Enumeration

- LAB: RPC Enumeration
- Microsoft SMB
- Enumerating Users, Group, SID (Security Principals)
- Automated SMB Enumeration Tools
  - LAB: SMB Enumeration (via Null Session)
- SNMP Protocol
  - LAB: SNMP Enumeration
  - LAB: Automated Windows Enumeration Tools

Module 3: Vulnerability Assessments (VA) Concept

- Definition of Risk, Vulnerability and Threat
- Risk Assessment
- Vulnerability Assessment Methodology
- Common Vulnerabilities and Exposure (CVE) list
- NIST SCAP Project
- Vulnerability Assessment tools
  - LAB: Vulnerability Scanner

Module 4: System Hacking

- Introduction to Malware
- What is Trojan
  - LAB: Setup and Deploy Trojan
- Introduction to APT
- What is Password Cracking
- Type of Password Cracking
- Windows Password
  - LM ,NTLM Hashing
  - SAM File
  - How to steal windows password
- Password Cracking Tools
  - LAB: Password Cracking in Linux
  - LAB: Password Cracking in Windows
  - LAB: Password Cracking for other hashing algorithm
- Linux – Basics
- Linux File Structure
- Linux Vulnerabilities

- Linux Services Level Hacking
- Linux Exploitation
    - LAB: Exploit Linux Operating System
    - LAB: Password Cracking in Linux
- Memory Organization
- Buffer and Heap Overflows
- Attacking with Metasploit Framework
- Pilfering target information
- Metasploit Framework
    - LAB: Metasploit Framework

Module 5: Sniffing

- Definition of Sniffing
- Protocols Vulnerable to Sniffing
- Types of Sniffing
    - LAB: Packet Sniffing using Wireshark
- ARP - What is Address Resolution Protocol?
- ARP Spoofing Attack
- ARP Poisoning
    - LAB: ARP Poisoning
- Mac Duplicating Attack
- DNS Poisoning Techniques
    - LAB: DNS Poisoning

Module 6: Firewall & IDS Evasion

- How attacks may traverse a firewall
- IDS Evasion Techniques
- The role of intrusion detection & how it may be evaded using advanced techniques
    - LAB: Evasion Tools

Module 7: Wireless LAN Hacking

- WEP, WPA, and WPA2
- Steps for Hacking Wireless Networks
- LAB: Cracking WEP
    - LAB: Cracking WPA
- Temporal Key Integrity Protocol (TKIP)

- LEAP: The Lightweight Extensible Authentication Protocol
    - LAB: MAC Spoofing
- Scanning Tools
    - LAB: Active and Passive Scanners

Module 8: Denial of Services

- What is Denial of Services
- Type of Denial of Services
- Denial of Services Techniques (DoS)
- Distributed Denial of Services Techniques (DDoS)
- What is Botnet
    - Denial of Services Tools
    - LAB: Denial of Services Techniques

Module 9: Web Application Hacking

- How are Web Servers Compromised?
- Web Application Hacking
- Web Application Threats
- OWASP Top 10
    - LAB: Cross-Site Scripting/XSS Flaws
    - LAB: SQL injection
    - LAB: Command Injection Flaws
    - LAB: Parameter/Form Tampering
    - LAB: Directory Traversal/Forceful Browsing
    - LAB: Cryptographic Interception
    - LAB: Session Hijacking
- Google Hack Database (GHDB)
    - LAB: Improper Error Handing
    - LAB: Broken Access Control

Recommended Course tracks

- PEN-X : Expert Penetration Testing with Hardcore Offensive Techniques
- MPEN : Mobile Penetration Testing Techniques

สำรองที่นั่งและขอรับรายละเอียดเพิ่มเติมกรุณาติดต่อ (FOR MORE INFORMATION & REGISTRATION PLEASE CONTACT)

คุณธนภัทร ไชยพิมล
Mr. Tanapat Chaipimol
Tel:(66) 2-650-5771 Ext.105 Fax: (66) 2-650 5776
Mobile: (66) 86-330-8532
Email: tanapat.ch@acisonline.net

คุณกิตมณี นิยมญาติ
Ms. Kitmanee Niyomyat
Tel:(66) 2-650-5771 ext. 108 Fax: (66) 2-650 5776
Mobile: (66) 86-325-7129
Email: kitmanee.ni@acisonline.net

ACIS Professional Center Co.Ltd.

2101, 21 Fl., 62 The Millennia Building, Lungsuan Rd., Lumpini, Pathumwan, Bangkok 10330
Tel: +(66)2-650-5771 Fax: +(66)2-650-5776 Hotline: +(66)86-352-7129 Email: registration@acisonline.net
Website: www.acisonline.net