

Course Introduction

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

The course revolves around a 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 advanced hacking techniques, exploit techniques, vulnerability assessment and advanced penetrating testing techniques.

Participants will gain advanced 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 advance Penetration testing techniques
- 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 advance technique 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

- Expert

Course Duration

- 3 Days (18 Hours)

Prerequisites

- Knowledge about Internetworking
- Knowledge about Basic wireless
- Knowledge about Basic Database system (Mysql ,MSSQL ,Orcle)
- Knowledge about Basic web application development (PHP ,ASP ,JSP)
- Knowledge about Information Security

- Knowledge about Operating system (Windows ,Linux Command-line)
- Knowledge about Basic Penetration testing

Target Group

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

Course Outline

Module 1: Web Application Advanced Techniques

- SQL Injection Advanced Techniques
- SQL Injection Tools with sqlmap
 - SQL Injection + Vulnerability Exploitation with sqlmap
 - Configuring Tor for sqlmap
- How to Bypass Web Application Firewall
- Gain Access with Web Shell
- Advanced XSS
- XSS Exploitation Tools
- LFI / RFI Techniques
- HTML5 Hacking
- Lab: Web Application Hacking

Module 2: Reverse Engineering Techniques

- Basic of Intel CPU Architecture
- Basic Assembly Language
- Reverse Engineering Concept
- Understand Function calling/return steps
- Helpful Tools for Reverse Engineering
- Software Debugging Techniques
 - Ollydbg
 - Immunity Debugger
 - IDA Pro
- Patching! Software
- Lab: Cracking Real Software

Module 3: Advanced System Hacking

- Password Cracking Techniques
 - Advanced John the Ripper
 - GPU Cracking
- Advanced Metasploit Framework Attack
 - Windows Hash Attack Techniques
 - Pass-the-Hash Techniques
 - Cracking without Cracking
 - Post-Exploitation Techniques
 - Advanced Escalation Privileges Techniques
 - Advanced Tunneling & Pivoting Techniques
 - Lab: Advanced Metasploit Exploitation
- Anti-Viruses Evasion Techniques
 - What is Crypter!
 - Turn a Malware to be Undetectable
 - Lab: Making Undetectable Malware
- Exploitation Development
 - Basic Python Programming
 - Wrap-up Assembly Language
 - How to Fuzzing & Debugging Program
 - Understanding Shellcode
 - Stack overflow Exploitation
 - Heap overflow exploitation
 - Understanding DEP
 - Understanding ASLR
 - Advanced Exploitation Techniques
 - Lab: Software Exploitation

Module 4: Advanced System Hacking

- Browser Exploitation
- PDF Exploitation
- Web Browser Attack
- Java Applet Attack
- Deploy Malware for Document Files (PDF, MS-Office)
- Hardcore Social Engineering Techniques

- Bypassing any Detection Mechanism
- Lab: Perfect! Hacking Techniques

Module 5: Advanced Network Hacking

- Layer 2 Hacking
 - DHCP Hacking
 - ARP Hacking
 - VLAN Hacking
 - Spanning Tree Hacking
 - DTP Hacking
 - Tools for Layer 2 Hacking
 - Lab: Layer 2 Hacking
- Layer 3 Hacking
 - Routing Protocol Hacking
 - Tools for Layer 3 Hacking
- IPv6 Hacking
 - Tools for IPv6 Security Testing
 - Lab: IPv6 Hacking
- Man-in-the-Middle Advanced Techniques
 - SSLStrip
 - Traffic Redirect
 - Patching Exploitation
 - Lab: SSLStrip Techniques & Make your remote control
- Advanced Wireless Hacking
 - Advanced WPA2 Cracking
 - WPS Cracking
 - Advanced Wireless Man-in-the-Middle Techniques
 - WPA2 Enterprise Hacking
 - Lab: Advanced Wireless Hacking

Module 6: Mobile Penetration Testing

- Overview Mobile Threats
- Type of Mobile Penetration Testing
- How to Prepare for Mobile Penetration Tester
- Smartphone Software Hacking
- Introduction to OWASP Mobile Top 10

- HTML5 Hacking

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

