

Course Introduction

Windows is a famous platform in the world. It is a multi-role, rich of functions and user friendly platform.

Windows was natively designed for functional and ease of use but not security purpose that may cause Windows platforms to be the first line of attacking.

Windows has a lot of configurations to improve security but user need to familiar with it to configure it properly. In the course will have knowledge to let attendees know what the hackers think about Windows and then learn how to improve security with its built-in tools and its configurations to prevent Windows from attacking.

Course Objectives

- To know the Windows's inherent vulnerabilities
- To know the basic hacking, especially in Windows platform
- To improve Windows security with its built-in tools and its configurations

Learning Level

- Intermediate

Course Duration

- 3 Days

Target Group

- Enterprise Architect
- Security Administrator
- Systems Engineer
- Security Architect
- Security Consultant
- Security Engineer
- Security Manager
- Systems Architect

Course Outline

Day 1

For More Information & Registration, Please Contact Training Division

Tel:(66) 2253-4736, Fax:(66) 2253-4737, Hotline:(66) 86-325-7129, E-mail: registration@acisonline.net

- Overview of Windows Server Hacking and Hardening
- Using of VMware
- Hacking and Hardening Active Directory Domain Controller

Day 2

- Hacking and Hardening DNS service
- Hacking and Hardening DHCP service

Day 3

- Hacking and Hardening IIS
- Final Workshop

Official Training Partner



For More Information & Registration, Please Contact Training Division

Tel:(66) 2253-4736, Fax:(66) 2253-4737, Hotline:(66) 86-325-7129, E-mail: registration@acisonline.net