NAT Network Management, Monitoring and Troubleshooting Workshop

Course Introduction

Currently network professionals are dealing with many issues going on their corporate network. Advanced skills on network management, network monitoring and network troubleshooting are required for network professionals in order to operate, maintain and improve corporate network to certain satisfaction of users and managements.

A hands-on course provides knowledge and experience of network management, monitoring and troubleshooting, using a powerful tool like packet snifter, Network Management Console and centralized Logging.

This course is focusing on design, installation, configuring and operating tools to support monitoring, troubleshooting and management of corporate network.

Course Objectives

- To understand concept and principle of network management, monitoring and troubleshooting
- To understand network management protocols that are practical for corporate network
- To be able to use packet sniffer to troubleshoot network problems
- To use Log File as a tools to monitor and troubleshoot network

Course Highlights

- Software and Network monitoring tools provided
- 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

- TCP/IP and basic networking knowledge
- Internetworking concept

Target Group

- System and Network Administrators
- Network Administrator

- Network Troubleshooter
- IT Security Professional
- IT Support

Course Outline

Module 1: Network Architecture and Terminology

- Devices, Network Elements, Agents, and Proxies
- ISO Network Management Model
- Network Management Protocols and Communications
- Network Management Systems, Element Managers
- Operating Systems

Module 2: Monitoring and Troubleshooting Tools

- Ping, Trace Route, Route, etc.
- Protocol Analyzers
- Telnet and Command Line Interfaces
- Nslookup

Module 3: RMON and netFlow Background, Components, and Commands

- RMON Agents and Probes
- RMON and RMON1 Background
- RMON Groups
- netFlow Background

Module 4: SNMP Background, Components, and Commands

- Management Information Base (MIB)
- SNMP Security
- SNMPv1 ,SNMPv2 and SNMPv3 Interoperability
- Structure of Management Information
- LAB : Install SNMP Agents
- DEMO : SNMP Management tool Solarwinds

Module 5: Using SNMP and RMON Tools

- Accounting Management
- Configuration Management
- Fault Management
- Performance Management
- Security Management

Module 6: Network Management Console (NMC)

- Performance Base Monitoring
  - Cacti
  - Orion (Solarwinds) Network Performance Monitoring
  - MRTG ,PRTG
- Availability Base Monitoring
  - Nagios
  - Zenoss
- Network flow Monitoring
  - netFLOW
  - ntop
- Hybrid
  - groundwork monitor open souse
    - LAB : Implement Cacti
    - LAB : Management Cacti

Module 7: Sniffing and Anti-Sniffing

- Introduction to Wireshark
- Capturing Packets
- Configuring Global Preferences
- Navigation and Colorization Techniques
- Using Time Values and Summaries
- Examining Basic Trace File Statistics
- Examining Advanced Trace File Statistics
- Creating Display Filters
- Save, Export and Print
- Expert System and Miscellaneous Tasks
- Using Command-Line Tools

Module 8: Network Troubleshooting

- Troubleshoot IP and Routing
- ICMP Troubleshooting
- NAT Troubleshooting
- TCP ,UDP Troubleshooting
- DHCP Troubleshooting
- ARP Troubleshooting

- DNS Troubleshooting Tools
- HTTP Troubleshooting
- FTP Troubleshooting
- Telnet Troubleshooting
- SMTP ,POP Troubleshooting
- LAB : Traffic Analysis workshop
- LAB: Troubleshooting network problem using Network analysis tools

Module 9: Optimize Network Performance

- Analyzer Placement
- Normal Network Communications
- Causes of Performance Problem
- Wireshark Functions for Troubleshooting
- Latency Issues
- Packet Loss and Retransmissions
- Misconfigurations and Redirections
- Dealing with Congestion
- Baseline Network Communications

Module 10: Network Forensic and Security

- Analyzer Placement
- Unususal Network Communications
- Reconnaissance Processes
- Analyzing ICMP Traffic
- TCP Security
- Address Spoofing
- Building Firewall ACL Rules
- Signatures of Attack
- LAB: Analysis Network Attack
- LAB: Forensic Network by using Open Source tools

Recommended Course tracks

- HDN : Hardening Network Infrastructure
- SSCP : The Official SSCP CBK Review Seminar (Accredited Training by ISC^2)

NAT Network Management, Monitoring and Troubleshooting Workshop

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