TEC013: Hardening Network Infrastructure

COURSE DESCRIPTION:

This course teaches you how to protect your infrastructure and protect your network by using network security technology such as Firewall, Proxy IDS/IPS and harden Operating system and services and Network device such as Routers/Switches and also how to manage your network with network monitoring tools to detect threats.

COURSE OBJECTIVES:

- To understand Information Security Hardening Concept
- To understand Network Infrastructure Security Design
- To understand and Implement Operating System Security
- To understand and Implement Network Devices Security
- To understand and Implement Security Monitoring Concept
- To understand and Implement Security Devices in Network Infrastructure

PREREQUISITE:

- Knowledge of network fundamentals including OSI model, TCP/IP Protocol, and basic Cisco hardware familiarity.
- Existing Internetworking knowledge.
- Knowledge about Basic Operating system (Windows, Linux)

WHO SHOULD ATTEND:
- Network and Systems Administrators
- Network and Systems Engineers
- Information Security Professional

COURSE OUTLINE:

Module 1: Network Threats

- Understand Network Attack
    - Denial-of-service (DoS) Attacks
    - Distributed denial-of-service (DDoS) Attacks
    - Back door Attacks
    - Spoofing Attacks
    - Man-in-the-Middle Attacks
    - Replay Attacks
    - Password Guessing Attacks
- TCP/IP Attacks
    - TCP SYN or TCP ACK Flood Attack
    - TCP Sequence Number Attack
    - TCP/IP Hijacking
    - ICMP Attacks
    - Smurf Attacks
    - ICMP Tunneling

Module 2: OS Hardening

- Role Supported by Server Core
- OU Design for Security Policies
- GPO Design for Security Policies
- Implementing a Security Baseline
- Local Security Policy

- o Account Policy Best Practice
- o Developing Good Auditing Policy
- o User Rights Assignment
- o Security Options
- Deploy Domain Level Security Policy using GPO

Module 3: Hardening your Network with Firewall
- Firewall Placement Design
- Firewall Categorized
- Firewall Architectures
- Configuring and Managing Firewalls

Module 4: Hardening your Network with Intrusion Detection and Prevention
- Intrusion Detection Systems
- Type of IDS and IPS
- IDS Detection Methods
- IDS Response Methods
- Deployment and Implementation of and IDS and IPS

Module 5: Implement VPN and Dial-in Remote Access
- VPN Concept
- Type of VPN
- VPN Implementation in Network Infrastructure
- Implementing 2 Factor Authentication

Module 6: Hardening Routers and Switches
- Introduction Switch and Router threats
- Hardening Management Access
- Hardening Service and Features
- Hardening Router and Switch

Module 7: Secure Network with Content Filters
- Content Filtering Architectures

Module 8: Hardening Wireless LAN Connection
- Introduction Wireless LAN Threats
- Introduction Wireless Security
- Hardening Wireless LAN Technology

Module 9: Implement AAA
- Explain the functions and importance of AAA
- Describe the features of TACACS+ and RADIUS AAA protocols
- Configure AAA authentication
- Configure AAA authorization
- Configure AAA accounting

Module 10: Hardening your Network with Network management
- Management Information Base (MIB)
- SNMP Security
- SNMPv1, SNMPv2 and SNMPv3 Interoperability
- Structure of Management Information
- Performance Base Monitoring
  - o Cacti
  - o Orion (Solarwinds) Network Performance Monitoring
  - o MRTG, PRTG

- Availability Base Monitoring
    - Nagios
    - Zenoss
- Network flow Monitoring
    - netFLOW
    - ntop

Module 11: Implementing a Secure Perimeter
- DMZ Implementation and Design
- Internet Access Module
- WAN Access Module
- Extranet Access Module
- Wireless Access Module
- E-commerce Access Module
    - Web Application Threats
    - Web Application Security

วิทยากร: อ.เอกฤทธิ์ ธรรมสถิต

- MASTER OF BUSINESS ADMINISTRATION (EXECUTIVE) DEGREE
  SASIN GRADUATE INSTITUTE OF BUSINESS ADMINISTRATION OF
  CHULALONGKORN UNIVERSITY
- MASTER OF SCIENCE, MAJOR IN INFORMATION
  Technology Faculty of Information Technology
  KING'S MONGKUT INSTITUTE OF TECHNOLOGY LADKRABANG
- BACHELOR OF SCIENCE
  KING'S MONGKUT INSTITUTE OF TECHNOLOGY NORTH BANGKOK
- DIPLOMA PROGRAM FOR MANAGEMENT
  KELLOGG – NORTHWESTERN UNIVERSITY, UNITED STATE OF AMERICA
  Certificate:

    - Microsoft Certified professional (MCP)
    - Microsoft Certified Systems Administrator (MSCA)
    - Microsoft Certified Systems Engineer (MSCE)
    - Cisco Certified Network Associate (CCNA)
    - Certificate of CompTIA Security+
    - Certified Technical training CTT+
    - Certified Ethical Hacker
    - Certified Hacking Forensic Investigator
    - Certified Wireless Network Administrator
    - Certified Wireless Security Professional

จำนวนชั่วโมงในการฝึกอบรม: 3 วัน (18 ชั่วโมง)

กำหนดการอบรม: ตามตารางปฏิทินอบรมประจำปี https://www.career4future.com/trainingprogram

ช่วงเวลาฝึกอบรม: 9.00 - 16.00 น.

ค่าลงทะเบียนอบรม: ท่านละ 16,500 บาท (ราคารวมภาษีมูลค่าเพิ่มแล้ว)
** สถาบันฯ เป็นหน่วยงานราชการ จึงไม่อยู่ในเกณฑ์ที่ต้องถูกหักภาษี ณ ที่จ่าย

สถานที่ฝึกอบรม:
สถาบันพัฒนาบุคลากรแห่งอนาคต
เลขที่ 73/1 อาคารสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) ชั้น 6
ถนนพระรามที่ 6 แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพฯ 10400

วิธีการการสำรองที่นั่ง:
ติดต่อสำรองที่นั่งล่วงหน้า ในวัน-เวลาราชการ
โทรศัพท์: 0 2644 8150 ต่อ 81886, 81887
โทรสาร: 0 2644 8110
Website: www.career4future.com
E-mail: training@nstda.or.th