Hardening Network Infrastructure (HDN)

Duration 5 Days

COURSE DESCRIPTION

This Course is 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

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
  - Demo :Network Threats

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th
Call us today 0-2634-7993-4
177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th

- **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
  - Account Policy Best Practice
  - Developing Good Auditing Policy
  - User Rights Assignment
  - Security Options
  - Deploy Domain Level Security Policy using GPO
  - LAB: Audit Microsoft with Penetration Testing tools
  - LAB: Deploy Security Policy using GPO and Microsoft Security toolkit
  - LAB: Hardening Windows server 2003 & XP & 2008 & 7
  - LAB: Audit Active Directory

- **Module 3: Hardening your Network with Firewall**
  - Firewall Placement Design
  - Firewall Categorized
  - Firewall Architectures
  - Configuring and Managing Firewalls
  - LAB: IPTables Linux Firewall
  - LAB: Audit Firewall with Penetration Testing tools

- **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
  - LAB: Snort Installation

- **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
  - LAB: Hardening Cisco Router and Switch

- LAB: Audit Switch and Router with Penetration Testing tools

- **Module 7: Secure Network with Content Filters**
  - Content Filtering Architectures
  - LAB :Implement Content Filtering Firewall

- **Module 8: Hardening Wireless LAN Connection**
  - Introduction Wireless LAN Threats
  - Introduction Wireless Security
  - Hardening Wireless LAN Technology
  - LAB: Audit Wireless LAN Technology with Aircrack-ng Suite

- **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
  - LAB : Install SNMP Agents
  - Performance Base Monitoring
  - Cacti
  - Orion (Solarwinds) Network Performance Monitoring
  - MRTG ,PRTG

  Availability Base Monitoring
  - Nagios
  - Zenoss

  Network flow Monitoring
  - netFLOW
  - ntop
  - LAB : Implement Cacti
  - LAB : Management Cacti
  - DEMO : SNMP Management tool Solarwinds

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th
Call us today 0-2634-7993-4
177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th

- **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

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

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th
Call us today 0-2634-7993-4
177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th