

## System and Network Security: A Comprehensive Introduction - 4 Days

### *Course 468 Overview*

- You Will Learn How To**
- Analyse your exposure to security threats and protect your organisation's systems and data
  - Reduce your susceptibility to an attack by deploying firewalls and data encryption
  - Assess alternative user and host authentication mechanisms
  - Manage risks emanating from inside the organisation and from the Internet
  - Protect network users from hostile applications and viruses
  - Identify the security risks that need to be addressed within your organisation

**Course Benefits** In today's Internet-dependent business environment, organisations must link their systems across enterprise-wide and virtual private networks as well as connect mobile users. Each connection increases exposure to customers, competitors and hackers, magnifying vulnerability to attack. In this course, you learn how to analyse risks to your networks and the steps needed to select and deploy the appropriate countermeasures to reduce your exposure to network threats.

**Who Should Attend** Those who require the fundamental skills to develop and implement security schemes designed to protect their organisation's information from threats.

**Workshop Course** Workshops providing you with experience analysing system and network security, include:

- Cracking passwords using rainbow tables
- Scanning systems with Microsoft Baseline Security Analyzer (MBSA)
- Ensuring trusted server access via digital certificates
- Preventing unwanted network access with a personal firewall
- Encrypting and signing important data
- Exposing and rectifying communication vulnerabilities with remote hosts

# System and Network Security: A Comprehensive Introduction - 4 Days

## Course 468 Outline

### Building a Secure Organisation

#### Real threats that impact cybersecurity

- Hackers inside and out
- Eavesdropping
- Spoofing
- Sniffing
- Trojan horses
- Viruses
- Wiretaps

#### A cybersecurity policy: the foundation of your protection

- Defining your information assurance objectives
- Assessing your exposure

### A Cryptography Primer

#### Securing data with symmetric encryption

- Choosing your algorithm: DES, AES, RC4 and others
- Assessing key length and key distribution

#### Solving key distribution issues with asymmetric encryption

- Generating keys
- Encrypting with RSA
- PGP and GnuPG
- Evaluating Web of Trust and PKI

#### Ensuring integrity with hashes

- Hashing with MD5 and SHA
- Protecting data in transit
- Building the digital signature

### Verifying User and Host Identity

#### Assessing traditional static password schemes

- Creating a good quality password policy to prevent password guessing and cracking
- Protecting against social engineering attacks
- Encrypting passwords to mitigate the impact of password sniffing

#### Evaluating strong authentication methods

- Challenge-response to prevent man-in-the-middle attacks
- Preventing password replay using one-time and tokenised passwords
- Employing biometrics as part of two-factor authentication

#### Authenticating hosts

- Shortcomings of IP addresses
- Address-spoofing issues and countermeasures
- Solutions for wireless networks

### Preventing System Intrusions

#### Discovering system vulnerabilities

- Searching for operating system holes
- Discovering file permission issues
- Limiting access via physical security

#### Encrypting files for confidentiality

- Encryption with application-specific tools
- Recovering encrypted data

#### Hardening the operating system

- Locking down user accounts
- Securing administrator's permissions
- Protecting against viruses

### Guarding against Network Intrusions

#### Scanning for vulnerabilities

- Restricting access to critical services
- Preventing buffer overflows

#### Reducing denial-of-service (DoS) attacks

- Securing DNS
- Limiting the impact of common attacks

#### Deploying firewalls to control network traffic

- Contrasting firewall architectures
- Preventing intrusions with filters
- Implementing cybersecurity policy

#### Building network firewalls

- Evaluating firewall features
- Selecting an architecture and a personal firewall

### Ensuring Network Confidentiality

#### Threats from the LAN

- Sniffing the network
- Mitigating threats from connected hosts
- Partitioning the network to prevent data leakage
- Identifying wireless LAN vulnerabilities

#### Confidentiality on external connections

- Ensuring confidentiality with encryption
- Securing data-link layer with PPTP and L2TP
- Middleware information assurance with SSL and TLS
- Deploying SSH (the Secure Shell)

#### Protecting data with IPsec

- Authenticating remote locations
- Tunnelling traffic between sites
- Exchanging keys

### Managing Your Organisation's Security

- Developing a security plan
- Responding to incidents
- Enumerating the six critical steps