Network and System Security

Course Title:

Network and System Security

Duration:

5 days, 40 Hours

Class Format Options:

Instructor-led classroom

Who Should Attend:

- *System Administrators and Security Administrators interested in enhancing their security skills and becoming more familiar with security tools necessary to secure the enterprise network*
- *Graduate Students of CS, Engineering and MIS fields who are interested in getting hands-on experience in the field of computer and network security*
- *Anyone who is preparing for key industry security certifications*

Prerequisites:

Introduction to Information Security course or equivalent knowledge

Course Overview

This five-day course provides more in depth analysis of the selected topics, which can be utilized to perform day-to-day security functions. It will provide extensive computer-based exercises and workshops to provide the attendee with practical experience analyzing system and network security. This course is designed for the system or network administrator who may be responsible for the security administration of systems or networks in an enterprise as an additional duty along-side their regular responsibilities. It will also provide the attendee with industry best practices that can be used to enhance enterprise security.

Upon Completion

Students will gain the following knowledge:

- Network Essentials
- Security Threats Network Security
- Host Security
- Physical Security
- Cryptography

Hands-On Workshops

Attendees will practice using the following tools to enhance the knowledge gained throughout the course:

- TCPDump
- EatherPeak
- Microsoft Baseline Security Analyzer
- Password Cracking Software (Crack, LC4)
- Port Scanners (Nmap, Nessus)
- Network IDS (Snort) and Host IDS (Tripwire)
- PGP

Contact: info@cyberm.co.za / +27 83 262 2025

Network and System Security: Course Content

Network Essentials:

- Network Topologies
- OSI vs. TCP/IP Model
- LAN and WAN Devices
- LAN Technologies
- WAN Technologies
  Wireless Networks
- Internet Protocol (IP)
- Transmission Control Protocol (TCP)
- Security Protocols (IPSec, SSL, SET, PEM)
- Hands-On exercises analyzing network traffic with TCPDump and EatherPeak

Network Security:

- Firewalls Types
- Packet filtering
- Proxies
- DMZ
- Virtual Private Networks (VPN)
- Intrusion Detection Systems (IDS)
- Policy
- Firewall
- Avoidance methods
- Honeypots
- Defense In Depth

Physical Security

- Computing Facilities Considerations
- Access Control
- Media security
- UPS
- Fire Safety Programs

Security Threats and Protection

- Types of Attacks (Brute Force, Denial of Service, Spoofing)
- Trojans
- Worms
- Virus
- Logic Bomb
- Trap Door
- Inference
- Traffic Analysis
- Flooding
- Attack Scenarios

System Security

- System Patches
- Access control
- Authentication methods
- File Access Restriction
- System auditing
- Backup methods
- System hardening
- System and account policies

Cryptography

- Cryptography Concepts
- Symmetric and Asymmetric Algorithms
- Digital Signatures
- PKI
- Key Escrow
- Steganography