

SEC013: CompTIA Security+

Overview:

This course builds on your existing user-level knowledge and experience with personal computer operating systems and networks to present the fundamental skills and concepts that you will need to use on the job in any type of networking career. It also addresses the content described in the exam objectives for the CompTIA Network+ certification. If you are pursuing a CompTIA technical certification path, obtaining the CompTIA® A+® certification is an excellent first step to take before preparing for the CompTIA Network+ N10-007 examination.

Audience:

This course is intended for entry-level computer support professionals with a basic knowledge of computer hardware, software, and operating systems who wish to increase their knowledge and understanding of networking concepts and acquire the required skills to prepare for a career in network support or administration, or who wish to prepare for the CompTIA Network+ certification (Exam N10-007). A typical student taking the CompTIA® Network+® (Exam N10-007) course should have a minimum of nine months of professional computer support experience as a PC or help desk technician. Networking experience is helpful but not mandatory; A+ certification or equivalent skills and knowledge is helpful but not mandatory.

Prerequisites:

- To ensure your success in this course, you will need basic Windows end-user computer skills.
- In order to obtain the Network+ certification students must pass the CompTIA® Network+® (Exam N10-007).

Course completion:

In this course, you will describe the major networking technologies and systems of modern networks, and configure, manage, and troubleshoot modern networks. You will:

- Identify basic network theory concepts and major network communications methods.
- Describe bounded network media.
- Describe unbounded network media.
- Identify the major types of network implementations.
- Identify TCP/IP addressing and data delivery methods.
- Analyze routing and switching technologies.
- Identify the components of a TCP/IP implementation.
- Analyze network security.
- Implement network security.
- Identify the components of a WAN implementation.
- Identify the components used in cloud computing and virtualization.
- Identify the components of a remote network implementation.
- Manage networks.
- Troubleshoot network issues.

Course Outline:

Lesson 1: Comparing and Contrasting Attacks

- Compare and Contrast Information Security Roles
- Explain Threat Actor Types
- Compare and Contrast Social Engineering Attack Types
- Determine Malware Types

Lesson 2 - Comparing and Contrasting Security Controls

- Compare and Contrast Security Control and Framework Types
- Follow Incident Response Procedures

Lesson 3 - Assessing Security Posture with Software Tools

- Explain Penetration Testing Concepts
- Assess Security Posture with Topology Discovery Software Tools
- Assess Security Posture with Fingerprinting and Sniffing Software Tools
- Assess Security Posture with Vulnerability Scanning Software Tools

Lesson 4 – Explaining Basic Cryptography Concepts

- Compare and Contrast Basic Concepts of Cryptography
- Explain Hashing and Symmetric Cryptographic Algorithms
- Explain Asymmetric Cryptographic Algorithms

Lesson 5 - Implementing a Public Key Infrastructure

- Implement Certificates and Certificate Authorities
- Implement PKI Management

Lesson 6 - Implementing Identity and Access Management Controls

- Compare and Contrast Identity and Authentication Concepts
- Install and Configure Authentication Protocols
- Implement Multifactor Authentication

Lesson 7 – Managing Access Services and Accounts

- Install and Configure Authorization and Directory Services
- Implement Access Management Controls
- Differentiate Account Management Practices
- Implement Account Auditing and Recertification

Lesson 8 - Implementing a Secure Network Architecture

- Implement Secure Network Architecture Concepts
- Install and Configure a Secure Switching Infrastructure
- Install and Configure Network Access Control
- Install and Configure a Secure Routing and NAT Infrastructure

Lesson 9 - Installing and Configuring Security Appliances

- Install and Configure Firewalls and Proxies
- Install and Configure Load Balancers
- Install and Configure Intrusion Detection/Prevention Systems
- Install and Configure Data Loss Prevention (DLP) Systems
- Install and Configure Logging and SIEM Systems

Lesson 10 - Installing and Configuring Wireless and Physical Access Security

- Install and Configure a Wireless Infrastructure
- Install and Configure Wireless Security Settings
- Explain the Importance of Physical Security Controls

Lesson 11 - Deploying Secure Host, Mobile, and Embedded Systems

- Implement Secure Hardware Systems Design
- Implement Secure Host Systems Design
- Implement Secure Mobile Device Systems Design
- Implement Secure Embedded Systems Design

Lesson 12 - Implementing Secure Network Access Protocols

- Implement Secure Network Operations Protocols
- Implement Secure Remote Access Protocols
- Implement Secure Remote Administration Protocols

Lesson 13 - Implementing Secure Network Applications

- Implement Secure Web Services
- Implement Secure Communications Services
- Summarize Secure Virtualization Infrastructure
- Summarize Secure Cloud Services

Lesson 14 - Explaining Risk Management and Disaster Recovery Concepts

- Explain Risk Management Processes and Concepts
- Explain Resiliency and Automation Strategies
- Explain Disaster Recovery and Continuity of Operation Concepts
- Summarize Basic Concepts of Forensics

Lesson 15 - Summarizing Secure Application Development Concepts

- Explain the Impact of Vulnerability Types
- Summarize Secure Application Development Concepts

Lesson 16 - Explaining Organizational Security Concepts

- Explain the Importance of Security Policies
- Implement Data Security and Privacy Practices
- Explain the Importance of Personnel Management

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: 5 วัน (30 ชั่วโมง)

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

ช่วงเวลาฝึกอบรม: 9.00 - 16.00 น.

ค่าลงทะเบียนอบรม: ท่านละ 35,000 บาท (ราคารวมภาษีมูลค่าเพิ่มแล้ว)

** สถาบันฯ เป็นหน่วยงานราชการ จึงไม่อยู่ในเกณฑ์ที่ต้องถูกหักภาษี ณ ที่จ่าย

Career for the Future Academy: CFA

สถานที่ฝึกอบรม:

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

วิธีการสำรองที่นั่ง:

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