CompTIA A+, Network+, and Security+ Day

Length: 35 days
Format: Classroom
Time: Day

About This Course

If you are getting ready for a career as an entry-level information technology (IT) professional or computer service technician, the CompTIA A+ course is the first step in your preparation. The course will build on your existing user-level knowledge and experience with personal computer (PC) software and hardware to present fundamental skills and concepts that you will use on the job. In this course, you will acquire the essential skills and information you will need to install, configure, optimize, troubleshoot, repair, upgrade, and perform preventive maintenance on PCs, digital devices, and operating systems.

The CompTIA Network+ 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. If you are pursuing a CompTIA technical certification path, the CompTIA A+ certification is an excellent first step to take before preparing for the CompTIA Network+ certification.

CompTIA Security+ is the primary course you will need to take if your job responsibilities include securing network services, devices, and traffic in your organization. You can also take this course to prepare for the CompTIA Security+ certification examination. In this course, you will build on your knowledge of and professional experience with security fundamentals, networks, and organizational security as you acquire the specific skills required to implement basic security services on any type of computer network.

Click here to find your place on the CompTIA pathway.

Required Exams

220-901: A+ IT Essentials/220-902: A+ Practical Application/N10-006: Network+/SY0-501: Security+

Audience Profile

This course is intended for students seeking to earn the CompTIA A+, Network+, and Security+ certifications and who need an expert instructor to guide them throughout the training and exam preparation process.

Course Objectives

After completing this course, students will be able to:

* Identify the hardware components of personal computers and mobile digital devices.
* Identify the basic components and functions of operating systems.
* Identify networking and security fundamentals.
* Identify the operational procedures that should be followed by professional PC technicians.
* Install, configure, and troubleshoot display devices.
* Install and configure peripheral components.
* Manage system components.
* Manage data storage.
* Optimize and maintain Microsoft Windows.
* Work with other operating systems.
* Identify the hardware and software requirements for client environment configurations.
* Identify network technologies.
* Install and configure networking capabilities.
* Support mobile digital devices.
* Support printers and multifunction devices.
* Identify security threats, vulnerabilities, and controls.
* Implement security controls.
* Troubleshoot system-wide issues.
* Identify basic network theory concepts and major network communications methods.
* Describe bounded network media.
* Identify unbounded network media.
* Identify the major types of network implementations.
* Identify TCP/IP addressing and data delivery methods.
* Implement routing technologies.
* Identify the major services deployed on TCP/IP networks.
* Identify the infrastructure of a WAN implementation.
* Identify the components used in cloud computing and virtualization.
* Describe basic concepts related to network security.
* Prevent security breaches.
* Respond to security incidents.
* Identify the components of a remote network implementation.
* Identify the tools, methods, and techniques used in managing a network.
* Describe troubleshooting of issues on a network
* Identify the fundamental concepts of computer security.
* Identify security threats and vulnerabilities.
* Manage data, application, and host security.
* Implement network security.
* Identify and implement access control and account management security measures.
* Manage certificates.
* Identify and implement compliance and operational security measures.
* Manage risk.
* Troubleshoot and manage security incidents.
* Plan for business continuity and disaster recovery.

Outline

Section 1: Hardware Fundamentals * Personal Computer Components
* Storage Devices
* Mobile Digital Devices
* Connection Interfaces

Section 2: Operating System Fundamentals * PC and Mobile Operating Systems
* PC Operating System Tools and Utilities

Section 3: Networking and Security Fundamentals * Network Types
* Network Compenents
* Common Network Services
* Cloud Concepts
* Security Fundamentals

Section 4: Safety and Operational Procedures * Basic Maintenance Tools and Techniques
* Personal and Electrical Safety
* Environmental Safety and Materials Handling
* Professionalism and Communication
* Organizational Policies and Procedures
* Troubleshooting Theories

Section 5: Supporting Display Devices * Install Display Devices
* Configure Display Devices
* Troubleshoot Video and Display Devices

Section 6: Installing and Configuring Peripheral Components * Install and Configure Input Devices
* Install and Configure Output Devices
* Install and Configure Input/Output Devices
* Install and Configure Expansion Cards

Section 7: Managing System Components * Identify Motherboard Components and Features
* Install and Configure CPU&rsquos and Coolings Systems
* Install Power Supplies
* Troubleshoot System Components

Section 8: Managing Data Storage * Identify RAM Types and Features
* Troubleshoot RAM Issues
* Install and Configure Storage Devices

* Configure the System Firmware
* Troubleshoot Hard Drives and RAID Arrays

Section 9: Installing and Configuring Microsoft Windows * Implement Client-Side Virtualization
* Install Microsoft Windows
* Use Microsoft Windows
* Configure Microsoft Windows
* Upgrade Microsoft Windows

Section 10: Optimizing and Maintaining Microsoft Windows * Optimize Microsoft Windows
* Back Up and Restore System Data
* Perform Disk Maintenance
* Update Section 11: Working With Other Operating Systems
* The OS X Operating System
* The Linux Operating System

Section 12: Customized Client Environments * Types of Common Business Clients
* Custom Client Environments

Section 13: Networking Technologies * TCP/IP Problems and Characteristics
* TCP/IP
* Internet Connections
* Ports and Protocols
* Networking Tools

Section 14: Installing and Configuring Networking Capabilities * Configure Basic Windows Networking
* Configure Network Parameters
* Using Windows Networking Features
* Install and Configure SOHO Networks

Section 15: Supporting Mobile Digital Devices * Install and Configure Exterior Laptop Components
* Install and Configure Interior Laptop Components
* Other Mobile Devices
* Mobile Device Accessories and Ports
* Mobile Device Connectivity
* Mobile Device Synchronization
* Troubleshoot Mobile Device Hardware

Section 16: Supporting Printers and Multifunction Devices * Printers and Multifunction Devices
* Install and Configure Printers

* Maintain Printers
* Troubleshoot Printers

Section 17: Security Threats, Vulnerabilities, and Controls * Common Security Threats and Vulnerabilities
* General Security Controls
* Mobile Security Controls
* Data Destruction and Disposal Methods

Section 18: Implementing Security Controls * Secure Operating Systems
* Secure Workstations
* Secure SOHO Networks
* Secure Mobile Devices

Section 19: Troubleshooting System-Wide Issues * Troubleshoot PC Operating Systems
* Troubleshoot Mobile Device Operating Systems and Applications
* Troubleshoot Wired and Wireless Networks
* Troubleshoot Common Security Issue

Section 20:Network Theory * Networking Overview
* Network Standards and the OSI Model
* Network Types
* Identify Network Configurations
* Data Transmission Methods

Section 21:Bounded Network Media * Copper Media
* Fiber Optic Media
* Bounded Network Media Installation
* Noise Control

Section 22:Unbounded Network Media * Wireless Networking
* Wireless Network Devices and Components
* Install a Wireless Network

Section 23:Network Implementations * Physical Network Topologies
* Logical Network Topologies
* Ethernet Networks

* Network Devices
* VLANs

Section 24:TCP/IP Addressing and Data Delivery * The TCP/IP Protocol Suite
* IPv4 Addressing
* Default IP Addressing Schemes
* Create Custom IP Addressing Schemes
* IPv6 Address Implementation
* Delivery Techniques

Section 25:Routing * Enable Static Routing
* Implement Dynamic IP Routing

Section 26:TCP/IP Services * Assign IP Addresses
* Domain Naming Services
* TCP/IP Commands
* Common TCP/IP Protocols

Section 27:WAN Infrastructure * WAN Basics
* WAN Connectivity Methods
* WAN Transmission Technologies
* Unified Communication Technologies

Section 28:Cloud and Virtualization Technologies * Virtualization
* SAN Implementations
* Cloud Computing

Section 29:Network Security Basics * Introduction to Network Security
* Vulnerabilities
* Threats and Attacks
* Authentication Methods
* Encryption Methods

Section 30:Preventing Security Breaches * Physical Security Controls
* Network Access Controls
* Install and Configure Firewalls
* Harden Networks
* Intrusion Detection and Prevention
* Educate Users

Section 31:Responding to Security Incidents * Incident Management and Response
* Basic Forensic Concepts

Section 32:Remote Networking * Remote Network Architectures
* Remote Access Networking Implementations
* Virtual Private Networking
* VPN Protocols

Section 33:Network Management * Network Monitoring
* Configuration Management Documentation
* Network Performance Optimization

Section 34:Troubleshooting Network Issues * Network Troubleshooting Models
* Network Troubleshooting Utilities
* Hardware Troubleshooting Tools Common Connectivity Issues
* Troubleshoot Security Configuration Issues
* Troubleshoot Security Issues

Section 35:Security Fundamentals * The Information Security Cycle
* Information Security Controls
* Authentication Methods
* Cryptography Fundamentals
* Security Policy Fundamentals

Section 36:Identifying Security Threats and Vulnerabilities * Social Engineering
* Malware
* Software-Based Threats
* Network-Based Threats
* Wireless Threats and Vulnerabilities
* Physical Threats and Vulnerabilities

Section 37:Managing Data, Application, and Host Security * Manage Data Security

* Manage Application Security
* Manage Device and Host Security
* Manage Mobile Security

Section 38:Implementing Network Security * Configure Security Parameters on Network Devices and Technologies
* Network Design Elements and Components
* Implement Networking Protocols and Services
* Apply Secure Network Administration Principles
* Secure Wireless Traffic

Section 39:Implementing Access Control, Authentication, and Account Management * Access Control and Authentication Services
* Implement Account Management Security Controls

Section 40:Managing Certificates * Install a CA Hierarchy
* Enroll Certificates
* Secure Network Traffic by Using Certificates
* Renew Certificates
* Back Up and Restore Certificates and Private Keys
* Revoke Certificates

Section 41:Implementing Compliance and Operational Security * Physical Security
* Legal Compliance
* Security Awareness and Training
* Integrate Systems and Data with Third Parties

Section 42:Risk Management * Risk Analysis
* Implement Vulnerability Assessment Tools and Techniques
* Scan for Vulnerabilities
* Mitigation and Deterrent Techniques

Section 43:Troubleshooting and Managing Security Incidents * Respond to Security Incidents
* Recover from a Security Incident

Section 44:Business Continuity and Disaster Recovery Planning * Business Continuity
* Plan for Disaster Recovery
* Execute DRPs and Procedures