NEXT
CAREER DEVELOPMENT ACADEMY

SOC Engineer Career

Table of Content

CompTIA Network+

Days:	4 Days
Duration:	16 Hours
Language:	English

Job Description

The CompTIA® Network+® (Exam N10-007) 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.

The CompTIA® Network+® (Exam N10-007) course can benefit you in two ways. It can assist you if you are preparing to take the CompTIA Network+ examination (Exam N10-007). Also, if your job duties include network troubleshooting, installation, or maintenance, or if you are preparing for any type of network-related career, it provides the background knowledge and skills you will require to be successful.

Job Profile Outcome

- 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.

Job Outline

Module 1 / Local Area Networks

- Topologies and the OSI Model
- Key Features of Networks
- Network Topologies
- The OSI Model
- Physical Layer
- Data Link Layer
- Network Layer
- Transport Layer
- Upper Layers
- OSI Model Summary
- VM Orientation Ethernet
- Transmission Media
- Media Access Control
- Broadcast Domains
- Ethernet Frames
- Ethernet Deployment Standards
- MAC Addressing

- Address Resolution Protocol (ARP)
- Packet Sniffers
- Configuring Ethernet Networking Hubs, Bridges, and Switches
- Hubs and Bridges
- Switches
- Switch Interface Configuration
- Spanning Tree Protocol (STP)
- Power over Ethernet (PoE) Infrastructure and Design
- Network Infrastructure Implementations
- Planning an Enterprise Campus Network
- Network Hierarchy and Distributed Switching
- Software Defined Networking
- Planning a SOHO Network
- TCP/IP Protocol Suite Policies and Best Practices
- Procedures and Standards
- Safety Procedures
- Incident Response Policies
- Security and Data Policies
- Password Policy
- Employee Policies

Module 2 / IP Addressing

- Internet Protocol
- IPv4
- IPv4 Address Structure
- Subnet Masks
- IP Routing Basics
- ipconfig / ifconfig
- ICMP and ping
- Configuring IPv4 Networking IPv4 Addressing
- IPv4 Addressing Schemes
- Classful Addressing
- Public versus Private Addressing
- Subnetting and Classless Addressing
- Planning an IPv4 Addressing Scheme
- Public Internet Addressing
- Variable Length Subnet Masks (VLSM)
- Configuring IPv4 Subnets IPv6 Addressing
- IPv6 Address Format
- IPv6 Addressing Schemes
- IPv6 Address Autoconfiguration
- Migrating to IPv6
- Configuring IPv6 Networking DHCP and APIPA
- IPv4 Address Autoconfiguration
- Configuring DHCP
- DHCPv6
- Configuring Address Autoconfiguration

Module 3 / Internetworking

- Routing
- Routing Basics
- Routing Algorithms and Metrics
- Dynamic Routing Protocols
- Administrative Distance and Route Redistribution
- IPv4 and IPv6 Internet Routing
- High Availability Routing
- Installing and Configuring Routers
- Routing Troubleshooting Tools
- Configuring Routing TCP and UDP
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- TCP and UDP Ports
- Port Scanners
- Protocol Analyzers
- TCP and Port Scanning Name Resolution and IPAM
- Host Names and FQDNs
- Domain Name System
- Configuring DNS Servers
- Resource Records
- Name Resolution Tools
- IP Address Management (IPAM)
- Configuring Name Resolution and IPAM Monitoring and Scanning
- Performance Monitoring
- Network Monitoring Utilities
- Logs and Event Management
- Simple Network Management Protocol
- Analyzing Performance Metrics
- Patch Management
- Vulnerability Scanning
- Performance Testing and Monitoring
- Network Troubleshooting

- Troubleshooting Procedures
- Identifying the Problem
- Establishing a Probable Cause
- Establishing a Plan of Action
- Troubleshooting Hardware Failure Issues
- Troubleshooting Addressing Issues
- Troubleshooting DHCP Issues
- Troubleshooting Name Resolution
- Troubleshooting Services

Module 4 / Applications and Security

- Applications and Services
- TCP/IP Services
- HTTP and Web Servers
- SSL / TLS and HTTPS
- Email (SMTP / POP / IMAP)
- Voice Services (VoIP and VTC)
- Real-time Services Protocols
- Quality of Service
- Traffic Shaping
- Bottlenecks and Load Balancing
- Multilayer Switches
- Configuring Application Protocols
- Virtualization, SAN, and Cloud Services
- Virtualization Technologies
- Network Storage Types
- Fibre Channel and InfiniBand
- iSCSI
- Cloud Computing
- Configuring Cloud Connectivity
- Network Security Design
- Security Basics
- Common Networking Attacks
- Network Segmentation and DMZ
- Virtual LANs (VLAN)
- VLAN Trunks
- Network Address Translation (NAT)
- Device and Service Hardening
- Honeypots and Penetration Tests
- Network Security Appliances
- Basic Firewalls
- Stateful Firewalls
- Deploying a Firewall
- Configuring a Firewall
- Deploying a Proxy
- Intrusion Detection Systems (IDS)
- Denial of Service
- Configuring a NAT Firewall
- Authentication and Endpoint Security
- Authentication and Access Controls
- Social Engineering
- Authentication Technologies
- PKI and Digital Certificates
- Local Authentication
- RADIUS and TACACS+
- Directory Services
- Endpoint Security
- Network Access Control
- Secure Appliance Administration

Module 5 / Operations and Infrastructure

- Network Site Management
- Network Cabling Solutions
- Distribution Frames
- Change and Configuration Management
- Network Documentation and Diagrams
- Physical Security Devices
- Business Continuity and Disaster Recovery
- Network Link Management
- Power Management
- Backup Management
- Network Inventory Management
- Installing Cabled Networks
- Twisted Pair Cable (UTP / STP / ScTP)
- Twisted Pair Connectors
- Wiring Tools and Techniques
- Cable Testing Tools
- Troubleshooting Wired Connectivity
- Other Copper Cable Types
- Fiber Optic Cable and Connectors
- Transceivers and Media Converters
- Installing Wireless Networks
- Wireless Standards (IEEE 802.11)
- Wireless Network Topologies
- Wireless Site Design
- Troubleshooting Wireless Connectivity

- Wireless Security
- Wi-Fi Authentication
- Extensible Authentication Protocol
- Troubleshooting Wireless Security
- Wireless Controllers
- Installing WAN Links
- Wide Area Networks (WAN)
- Telecommunications Networks
- Modern Telecommunications Networks
- Local Loop Services
- Installing WAN Links
- Wireless WAN Services
- Internet of Things
- Configuring Remote Access
- Remote Access Services (RAS)
- MPLS and PPP
- SIP Trunks
- Virtual Private Networks (VPN)
- SSL / TLS / DTLS VPNs
- IPsec
- Internet Key Exchange / ISAKMP
- Remote Access Servers
- Remote Administration Tools
- Managing Network Appliances
- Remote File Access
- Configuring Secure Access Channels
- Configuring a Virtual Private Network

MCSA: Windows Server

Days:	4 Days
Duration:	16 Hours
Language:	English

Job Description

Are you interested in learning about the Information Technology or computer career field? If so, then this course if for you. This course is designed to give you a solid foundation with Windows Server 2016 which is the latest Windows Server operating system available (released Oct 2016). The Microsoft Certified Solutions Associate (MCSA): Windows Server 2016 is an intermediate level certification that covers skills required to manage Windows Server 2016 Operating System, Client- Server Model, Network Infrastructure, Virtualization, Domain Management, Security Implementation, etc.

Of course, MCSA Server 2016 have huge changes, number of exams still remains 3. The following exams are required to get Certified on MCSA Server 2016

- 70-740: Installation, Storage, and Compute with Windows Server 2016
- 70-741: Networking with Windows Server 2016
- 70-742: Identity with Windows Server 2016

Job Outline

Installation, Storage, and Compute with Windows Server 2016, Exam: 70-740

Install Windows Servers in Host and Compute Environments

- Introduction to Microsoft Server Operating Systems.
- Comparing Server 2012 to Server 2016
- Understanding Licensing of Server 2016
- Install, Upgrade, and Migrate Servers and workload
- Install and configure Nano Server

Implement Storage Solutions

- Configure disks and volumes
- Implement server storage

Implement Hyper-V

- Install and configure Hyper-V
- Configure virtual machine (VM) settings
- Configure Hyper-V storage
- Configure Hyper-V networking

Implement Windows Containers

- Deploy Windows containers
- Manage Windows containers

Implement High Availability

- Implement high availability and disaster recovery options in Hyper-V
- Implement failover clustering
- Implement Storage Spaces Direct
- Manage failover clustering
- Manage VM movement in clustered nodes
- Implement Network Load Balancing (NLB)

Maintain and Monitor Server Environments

- Maintain server installations
- Monitor server installations

Networking with Windows Server 2016 Exam: 70-741

Implement Domain Name System (DNS)

- Install and configure DNS servers
- Forward Lookup Zone and Reverse Lookup Zone
- Primary, Secondary and Stub Zone
- Forwarders and Conditional Forwarders
- Zone Transfer and DNSSEC
- DNS Resource Records (RR), including A, AAAA, PTR, SOA, NS, SRV, CNAME, and MX records

- Root Hints and Dynamic DNS

Implement Networking with DHCP and IPAM

- Introduction to IPv4 and IPv6 Address Space
- Install and configure DHCP
- Manage and maintain DHCP
- IPv4 and IPv6 Scope
- Lease, Reservation and Scope options
- Implement and Maintain IP Address Management (IPAM)

Implement Network Connectivity and Remote Access Solutions

- Implement network connectivity solutions with NAT
- Implement virtual private network (VPN) and DirectAccess solutions
- Implement Network Policy Server (NPS)

Implement Core and Distributed Network Solutions

- Implement IPv4 and IPv6 addressing
- Tunneling and Routing
- Implement Distributed File System (DFS)
- DFS Name Space and Replication
- Implement Branch Cache

Implement an Advanced Network Infrastructure

- Implement high performance network solutions
- NIC Teaming
- Determine scenarios and requirements for implementing Software Defined Networking (SDN)

Identity with Windows Server 2016 Exam: 70-742

Installing and Configuring Domain Controllers

- Introduction to Active Directory Domain Services
- Overview of Identity Management Concepts
- Active Directory Domain Services Components
- Overview of ADDS Domain Services
- Deploying Domain Controllers

Managing AD DS Objects

- Overview of Object Management
- Managing User Accounts
- Managing Groups
- Managing Computer Accounts
- Managing Organizational Units

Securing Active Directory Domain Services

- Managing Organizational Units
- Implementing Account Security
- Auditing AD DS
- Configuring Managed Service Accounts

Working with Complex AD Infrastructures

- Overview of Advanced AD DS Deployments
- Deploying a Distributed AD DS Environment
- Overview of AD DS Replication
- Configuring AD DS Services

Implementing Group Policy

- Overview of Group Policy
- Creating and Configuring GPOs
- Monitoring and Troubleshooting Group Policy
- Managing Security Options for Computers using Group Policy
- Managing User Environments

Understanding Microsoft Azure AD and Directory Synchronization

- Planning Directory Synchronization
- Implementing Azure AD Connect
- Managing Identities with Directory Synchronization

Monitoring and Recovering AD DS

- Monitoring AD DS
- Database Management
- Backup and Recovery in AD DS

Implementing Active Directory Certificate Services

- Overview of Public Key Infrastructure and AD CS
- Deploying Certificate Authority Hierarchy
- Administering Certificate Authorities
- Deploying and Managing Certificates
- Managing Revocation and Distribution

- Configuring Certificate Recovery

Implementing Active Directory Federation Services

- Overview of AD FS
- Planning and Deploying AD FS
- Overview of Web Application Proxy

Implementing Active Directory Rights Management Services

- Overview of AD RMS
- Deploying AD RMS
- Protecting with AD RMS
- Conclusion

Linux +

Days:	6 Days
Duration:	24 Hours
Language:	English

Job Description

This Course explores the various tools and techniques commonly used by Linux programmers, system administrators and end users to achieve their day -to-day work in Linux environments. It is designed for computer users who have limited or no previous exposure to Linux, whether they are working in an individual or Enterprise environment.

Upon completion of this training you should have a good working knowledge of Linux, from both a graphical and command line perspective, allowing you to easily navigate through any of the major Linux distributions. You will be able to continue your progress as either a user, system administrator or developer using the acquired skills set.

Job Outline

Introduction

- Linux Foundation
- Linux Foundation Training
- Course Linux Requirements

Linux Philosophy and Components

- Linux History
- Linux Philosophy
- Linux Community
- Linux Terminology
- Linux Distributions

Linux Structure and Installation

- Linux filesystem basics
- The boot process
- Linux Distribution Installation

Graphical Interface

- Session Management
- Basic Operations
- Graphical Desktop

System Configuration from the Graphical Interface

- System, Display, Time and Date Settings
- Network Manager
- Installing and Updating Software

Command-line Operations

- Command Line Mode Options
- Basic Operations
- Searching for Files
- Working with Files
- Installing Software

Finding Linux Documentation

- Documentation Sources
- The man pages• GNU info
- Help Command
- Other Documentation Sources

File Operations

- Filesystems
- Filesystem Architecture
- Comparing Files and File Types
- Backing Up and Compressing Data

User Environment

- Accounts
- Environmental Variables
- Recalling Commands
- Command Aliases
- File Permissions

Text Editors

- Basic Editors: nano and gedit
- Labs
- More Advanced Editors: vi and emacs

Local Security Principles

- Understanding Linux Security
- Understand the Uses of root

- Using the sudo Command
- Working with Passwords
- Bypassing User Authentication

Network Operations

- Introduction to Networking
- Browsers
- Transferring Files

Manipulating Text

- Modifying Files
- sed and awk Commands
- File Manipulation Utilities
- grep Command
- Misc Text Utilities
- Dealing with Large Files and Text-related Commands

Printing

- Configuration
- Printing Operations
- Manipulating Postscript and PDF Files

Bash Shell Scripting

- Features and Capabilities
- Syntax
- Constructs

Advanced Bash Shell Scripting

- String Manipulation
- Boolean Expressions
- File Tests
- Case Structure• Debugging
- Tips and Tricks

Processes

- Introduction to Processes and Process Attributes
- Listing Processes
- Process Metrics and Process Control
- Starting Processes in the Future

Common Applications

- Internet Applications
- Multimedia Applications
- Graphics Editors
- Using Secure Shell

CompTIA Advanced Security Practitioner (CASP+)

Days:	10 Days
Duration:	40 Hours
Language:	English

Job Description

CompTIA Advanced Security Practitioner (CASP+) is an advanced-level cybersecurity certification for security architects and senior security engineers charged with leading and improving an enterprise's cybersecurity readiness.

Job Outcome

- Architect, engineer, integrate, and implement secure solutions across complex environments to support a resilient enterprise
- Use monitoring, detection, incident response, and automation to proactively support ongoing security operations in an enterprise environment
- Apply security practices to cloud, on-premises, endpoint, and mobile infrastructure, while considering cryptographic technologies and techniques
- Consider the impact of governance, risk, and compliance requirements throughout the enterprise

Job Outline

Security Architecture

- Given a scenario, analyze the security requirements and objectives to ensure an appropriate, secure network architecture for a new or existing network
- Given a scenario, analyze the organizational requirements to determine the proper infrastructure security design.
- Given a scenario, integrate software applications securely into an enterprise architecture.
- Given a scenario, implement data security techniques for securing enterprise architecture.
- Given a scenario, analyze the security requirements and objectives to provide the appropriate authentication and authorization controls
- Given a set of requirements, implement secure cloud and virtualization solutions.
- Explain how cryptography and public key infrastructure (PKI) support security objectives and requirements
- Explain the impact of emerging technologies on enterprise security and privacy

Security Operations

- Given a scenario, perform threat management activities
- Given a scenario, analyze indicators of compromise and formulate an appropriate response.
- Given a scenario, perform vulnerability management activities
- Given a scenario, use the appropriate vulnerability assessment and penetration testing methods and tools
- Given a scenario, analyze vulnerabilities and recommend risk mitigations.
- Given a scenario, use processes to reduce risk
- Given an incident, implement the appropriate response.
- Explain the importance of forensic concepts
- Given a scenario, use forensic analysis tools.

Security Engineering and Cryptography

- Given a scenario, apply secure configurations to enterprise mobility

- Given a scenario, configure and implement endpoint security controls.
- Explain security considerations impacting specific sectors and operational technologies.
- Explain how cloud technology adoption impacts organizational security.
- Given a business requirement, implement the appropriate PKI solution
- Given a business requirement, implement the appropriate cryptographic protocols and algorithms.
- Given a scenario, troubleshoot issues with cryptographic implementations

Governance, Risk, and Compliance

- Given a set of requirements, apply the appropriate risk strategies.
- Explain the importance of managing and mitigating vendor risk
- Explain compliance frameworks and legal considerations, and their organizational impact.
- Explain the importance of business continuity and disaster recovery concepts.

CCNA CyberOps

Days:	20 Days
Duration:	80 Hours
Language:	English

Job Description

Today's organizations are challenged with rapidly detecting cybersecurity breaches and effectively responding to security incidents. Teams of people in Security Operations Centers (SOCs) keep a vigilant eye on security systems, protecting their organizations by detecting and responding to cybersecurity threats. CCNA Cybersecurity Operations prepares candidates to begin a career working with associate-level cybersecurity analysts within security operations centers.

Job Outcomes

- Install virtual machines to create a safe environment for implementing and analyzing cybersecurity threat
- events.
- Explain the role of the Cybersecurity Operations Analyst in the enterprise.
- Explain the Windows Operating System features and characteristics needed to support cybersecurity
- analyses.
- Explain the features and characteristics of the Linux Operating System.
- Analyze the operation of network protocols and services.
- Explain the operation of the network infrastructure.
- Classify the various types of network attacks.
- Use network monitoring tools to identify attacks against network protocols and services.
- Use various methods to prevent malicious access to computer networks, hosts, and data.
- Explain the impacts of cryptography on network security monitoring.
- Explain how to investigate endpoint vulnerabilities and attacks.
- Evaluate network security alerts.
- Analyze network intrusion data to identify compromised hosts and vulnerabilities.
- Apply incident response models to manage network security incidents.

Job Outline

Cybersecurity and the Security Operations Center

- The Danger
- Fighters in the War Against Cybercrime

Windows Operating System

- Windows Overview
- Windows Administration

Linux Operating System

- Using Linux
- Linux Administration
- Linux Clients

Network Protocols and Services

- Network Protocols
- Ethernet and Internet Protocol (IP)
- Connectivity Verification
- Address Resolution Protocol
- The Transport Layer and Network Services
- Network Services

Network Infrastructure

- Network Communication Devices
- Network Security Infrastructure
- Network Representations

Principles of Network Security

- Attackers and Their Tools
- Common Threats and Attacks

Network Attacks: A Deeper Look

- Observing Network Operation
- Attacking the Foundation
- Attacking What We Do

Protecting the Network

- Understanding Defense
- Access Control
- Network Firewalls and Intrusion Prevention
- Content Filtering
- Threat Intelligence

Cryptography and the Public Key Infrastructure

- Cryptography
- Public Key Cryptography

Endpoint Security and Analysis

- Endpoint Protection
- Endpoint Vulnerability Assessment

Security Monitoring

- Technologies and Protocols
- Log Files

Intrusion Data Analysis

- Data Collection
- Data Preparation
- Data Analysis

Incident Response and Handling

- Incident Response Models
- CSIRTs and NIST 800-61r2
- Case-Based Practice