5 Days

Cisco CCNA Security

The Cisco CCNA Security is the first step for individuals wishing to obtain CCNP Security Certification. This course sets the foundation base for Security Administrators and Network Consultants to understand the discipline of a good network security. This training imparts real-time security implementation and troubleshooting skills to network security engineers.

The CCNA Security course qualifies an individual to test, configure, deploy and monitor the latest Cisco security hardware and software solutions. Not only this, but a qualified Network Associate will be able to identify system threats and also create effective strategies to mitigate the security threats.

Course Details

Course Outline

1.0 Security Concepts

1.1 Common security principles

- Describing confidentiality, integrity, availability (CIA)
- Describing SIEM technology
- Identifying common security terms
- Identifying common network security zones

1.2 Common security threats

- Identifying common network attacks
- Describing social engineering
- Identifying malware
- Classifying the vectors of data loss/exfiltration

1.3 Cryptography concepts and contrast symmetric and asymmetric encryption

- Describing key exchange
- Describing hash algorithm
- Comparing and contrasting symmetric and asymmetric encryption
- Describing digital signatures, certificates, and PKI

1.4 Describe network topologies

- Campus area network (CAN)
- Cloud, wide area network (WAN)
- Data center
- Small office/home office (SOHO)
- Network security for a virtual environment

2.0 Secure Access

2.1 Secure management

- Comparing in-band and out-of-band
- Configuring secure network management
- Configuring and verify secure access through SNMP v3 using an ACL
- Configuring and verify security for NTP
- Using SCP for file transfer

2.2 AAA concepts

- Describing RADIUS and TACACS+ technologies
- Configuring administrative access on a Cisco router using TACACS+
- Verifying connectivity on a Cisco router to a TACACS+ server
- Explaining the integration of Active Directory with AAA
- Describing authentication and authorization using ACS and ISE

2.3 802.1X authentication

- Identifying the functions 802.1X components

2.4 BYOD (Bring Your Own Device)

- Describing the BYOD architecture framework
- Describing the function of mobile device management (MDM)

3.0 VPN (Virtual Private Networks)

3.1 VPN concepts

- Describing IPsec protocols and delivery modes (IKE, ESP, AH, tunnel mode, transport mode)
- Describing hair pinning, split tunneling, always-on, NAT traversal

3.2 Remote access VPN

- Implementing basic clientless SSL VPN using ASDM
- Verifying clientless connection
- Implementing basic AnyConnect SSL VPN using ASDM
- Verifying AnyConnect connection

- Identifying endpoint posture assessment

3.3 Site-to-site VPN

- Implementing an IPsec site-to-site VPN with pre-shared key authentication on Cisco routers and ASA firewalls
- Verifying an IPsec site-to-site VPN

4.0 Secure Routing and Switching

4.1 Security on Cisco routers

- Configuring multiple privilege levels
- Configuring Cisco IOS role-based CLI access
- Implementing Cisco IOS resilient configuration

4.2 Secure routing protocols

- Implementing routing update authentication on OSPF

4.3 Secure the control plane

- Explaining the function of control plane policing

4.4 Common Layer 2 attacks

- Describing STP attacks
- Describing ARP spoofing
- Describing MAC spoofing
- Describing CAM table (MAC address table) overflows
- Describing CDP/LLDP reconnaissance
- Describing VLAN hopping
- Describing DHCP spoofing

4.5 Mitigation procedures

- Implementing DHCP snooping
- Implementing Dynamic ARP Inspection
- Implementing port security
- Describing BPDU guard, root guard, loop guard
- Verifying mitigation procedures

4.6 VLAN security

- Describing the security implications of a PVLAN
- Describing the security implications of a native VLAN

5.0 Cisco Firewall Technologies

5.1 Describing operational strengths and weaknesses of the different firewall technologies

- Proxy firewalls

- Application firewall
- Personal firewall

5.2 Comparing stateful vs. stateless firewalls

- Operations
- Function of the state table

5.3 Implementing NAT on Cisco ASA 9.x

- Static
- Dynamic
- PAT
- Policy NAT
- Verify NAT operations

5.4 Implementing zone-based firewall

- Zone to zone
- Self zone

5.5 Firewall features on the Cisco Adaptive Security Appliance (ASA) 9.x

- Configuring ASA access management
- Configuring security access policies
- Configuring Cisco ASA interface security levels
- Configuring default Cisco Modular Policy Framework (MPF)
- Describing modes of deployment (routed firewall, transparent firewall)
- Describing methods of implementing high availability
- Describing security contexts
- Describing firewall services

6.0 IPS

6.1 Describe IPS deployment considerations

- Modes of deployment (inline, promiscuous - SPAN, tap)
- Network-based IPS vs. host-based IPS
- False positives, false negatives, true positives, true negatives
- Placement (positioning of the IPS within the network)

6.2 Describe IPS technologies

- Rules/signatures
- Detection/signature engines
- Trigger actions/responses
- Blacklist (static and dynamic)

7.0 Content and Endpoint Security

7.1 Describing mitigation technology for email-based threats

- SPAM filtering, anti-malware filtering
- DLP, blacklisting, email encryption

7.2 Describing mitigation technology for web-based threats

- Local and cloud-based web proxies
- Blacklisting, URL filtering, malware scanning, URL categorization, web application filtering

7.3 Describing mitigation technology for endpoint threats

- Anti-virus/anti-malware
- Hardware/software encryption of local data
- Personal firewall/HIPS

Who Should Attend

This course is intended for those who are motivated to work as:

- System Analyst
- Network engineers
- Network developers
- Network administrators
- Network planners

Pre Requisite

A valid CCENT or a valid CCNA Routing and Switching or any CCIE certification can act as a prerequisite.

Exams

210-260 IINS Implementing Cisco Network Security (IINS) []

NCR)-122016,India

Date - Apr 25, 2024