CCNA Certification (200-120)

Course Description:

Cisco Certified Network Associate Security (CCNA Security) validates associate-level knowledge and skills required to secure Cisco networks. With a CCNA Security program, a network professional demonstrates the skills required to develop a security infrastructure, recognize threats and vulnerabilities to networks, and mitigate security threats. The CCNA Security curriculum emphasizes core security technologies, the installation, troubleshooting and monitoring of network devices to maintain integrity, confidentiality and availability of data and devices, and competency in the technologies that Cisco uses in its security structure.

Course Prerequisites:

Prior experience or knowledge of CCNA (Routing & Switching).

Target Audience:

This course is specially designed for the B.Tech/B.E (CSE/IT/EEE/ECE/Mtech) and all other IT related Graduates and Post Graduate students. Mission Professionalism has conquered the job scenario and companies seek for well qualified, professional and skilled manpower. Quality Education and Performance Oriented Training is our motto.

What Student/Professionals Will Learn?

- Network Security Principles
- Developing a Secure Network
- Cryptographic Solution
- Digital Signatures
- Endpoint Security
- Site-to-Site IPsec VPN Solution

COURSE-CONTENT:

- Security Concepts
  - Common security principles
    - Describe confidentiality, integrity, availability (CIA)
    - Describe SIEM technology
    - Identify common security terms
    - Identify common network security zones
  - Common security threats
    - Identify common network attacks
    - Describe social engineering
    - Identify malware
    - Classify the vectors of data loss/exfiltration
  - Cryptography concepts
    - Describe key exchange
    - Describe hash algorithm
    - Compare and contrast symmetric and asymmetric encryption
    - Describe digital signatures, certificates, and PKI
  - 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
- Secure Access
  - Secure management
    - Compare in-band and out-of band
    - Configure secure network management
    - Configure and verify secure access through SNMP v3 using an ACL
    - Configure and verify security for NTP

        - Use SCP for file transfer
    - AAA concepts
        - Describe RADIUS and TACACS+ technologies
        - Configure administrative access on a Cisco router using TACACS+
        - Verify connectivity on a Cisco router to a TACACS+ server
        - Explain the integration of Active Directory with AAA
        - Describe authentication and authorization using ACS and ISE
    - 802.1X authentication
        - Identify the functions 802.1X components
    - BYOD
        - Describe the BYOD architecture framework
        - Describe the function of mobile device management (MDM)
- VPN
    - VPN concepts
        - Describe IPsec protocols and delivery modes (IKE, ESP, AH, tunnel mode, transport mode)
        - Describe hairpinning, split tunneling, always-on, NAT traversal
    - Remote access VPN
        - Implement basic clientless SSL VPN using ASDM
        - Verify clientless connection
        - Implement basic AnyConnect SSL VPN using ASDM
        - Verify AnyConnect connection
        - Identify endpoint posture assessment
    - Site-to-site VPN
        - Implement an IPsec site-to-site VPN with pre-shared key authentication on Cisco routers and ASA firewalls
        - Verify an IPsec site-to-site VPN
- Secure Routing and Switching
    - Security on Cisco routers
        - Configure multiple privilege levels
        - Configure Cisco IOS role-based CLI access
        - Implement Cisco IOS resilient configuration
    - Securing routing protocols
        - Implement routing update authentication on OSPF
    - Securing the control plane
        - Explain the function of control plane policing
    - Common Layer 2 attacks
        - Describe STP attacks
        - Describe ARP spoofing
        - Describe MAC spoofing

- Describe CAM table (MAC address table) overflows
- Describe CDP/LLDP reconnaissance
- Describe VLAN hopping
- Describe DHCP spoofing

➢ Mitigation procedures
- Implement DHCP snooping
- Implement Dynamic ARP Inspection
- Implement port security
- Describe BPDU guard, root guard, loop guard
- Verify mitigation procedures

➢ VLAN security
- Describe the security implications of a PVLAN
- Describe the security implications of a native VLAN

• Cisco Firewall Technologies

➢ Describe operational strengths and weaknesses of the different firewall technologies
- Proxy firewalls
- Application firewall
- Personal firewall

➢ Compare stateful vs. stateless firewalls
- Operations
- Function of the state table

➢ Implement NAT on Cisco ASA 9.x
- Static
- Dynamic
- PAT
- Policy NAT
- Verify NAT operations

➢ Implement zone-based firewall
- Zone to zone
- Self zone

➢ Firewall features on the Cisco Adaptive Security Appliance (ASA) 9.x
- Configure ASA access management
- Configure security access policies
- Configure Cisco ASA interface security levels
- Configure default Cisco Modular Policy Framework (MPF)
- Describe modes of deployment (routed firewall, transparent firewall)
- Describe methods of implementing high availability
- Describe security contexts
- Describe firewall services

- IPS
  - Describe IPS deployment considerations
    - Network-based IPS vs. host-based IPS
    - Modes of deployment (inline, promiscuous - SPAN, tap)
    - Placement (positioning of the IPS within the network)
    - False positives, false negatives, true positives, true negatives
  - Describe IPS technologies
    - Rules/signatures
    - Detection/signature engines
    - Trigger actions/responses (drop, reset, block, alert, monitor/log, shun)
    - Blacklist (static and dynamic)
- Content and Endpoint Security
  - Describe mitigation technology for email-based threats
    - SPAM filtering, anti-malware filtering, DLP, blacklisting, email encryption
  - Describe mitigation technology for web-based threats
    - Local and cloud-based web proxies
    - Blacklisting, URL filtering, malware scanning, URL categorization, web application filtering, TLS/SSL decryption
  - Describe mitigation technology for endpoint threats
    - Anti-virus/anti-malware
    - Personal firewall/HIPS
    - Hardware/software encryption of local data

INTEGER Innovation will provide:

- Training Slides taught during training by trainers
- Programmatic Examples
- Assignments of each topic in a module
- Demos executed during training session.
- Software's and installation guide (for future help)
- E-books for further reading in depth
- Reference links
- 24X7 online support for any queries or doubts.