CCNA Security Syllabus

Course Details:

- Duration: 30 Days (3 Hours Daily).
- Certificates: CCNA Security.
- Exams: 640-553.

Semester 1: Network Security and building Security insurance policies

- Understanding network security principles
- Security threats classifications
- The three primary goals of network security (Security Triangle)
- Data categorizing
- Classification roles
- Controls in security solutions
- Responding to security incident
- Understanding methods of network attacks
- Hacker types
- Attack types
    - IP-spoofing attack and counter-measurements
    - Understanding confidentiality attacks
    - Understanding Integrity attacks
    - Understanding availability attacks
- Best practice recommendations
- System Development Life cycle (SDLC)
- Operation Security Recommendations
- Evaluating network security
- Disaster recovery considerations
- Constructing a comprehensive network security policy
- Creating a Cisco self-defending network

Semester 2: Security Main Network Device

Securing Routers

- IOS Security features
- Cisco Integrated Services Routers (ISR)
- ISR-Enhanced Features
- Creating local users Database
- Overview about AAA
- AAA authentication configuration
- AAA authorization configuration
- AAA Accounting configuration
- Troubleshooting AAA using CLI
- Configuring AAA using SDM
- Configuring AAA using Cisco Secure ACS
- Overview of TACACS+ and its Attributes
    - Configuring Cisco routers to use TACACS + using CLI and SDM
- Overview of RADIUS and its attributes
- Comparing TACACS+ and RADIUS
- Managing Router passwords
- Limiting number of failed login attempts
- Telnet connection login enhancements
- Configuring privilege levels
- CLI views
- Protecting router files and Cisco IOS Resilient configurations
- Security Device Manager (SDM)
- Preparing to launch SDM and exploring SDM
- Locking down the router using CLI and SDM
- Using Secure management and reporting

Securing Switches

- Defending against layer 2 attacks
- Basic approaches to protecting layer2 switches
- VLAN hopping
- Switch spoofing
- Double tagging
- STP attacks
- DHCP server spoofing
- CAM table overflow attack
- Spoofing MAC addresses
- Additional Cisco catalyst switches security features
- Port Security Configurations
- Cisco Identity Based Networking Services (IBNS)
- IEEE 802.1x
- Combing 802.1x and port security features

Securing Endpoints

- Defining End point security
- Examining OS and application vulnerabilities
- Buffer overflow attack, Anatomy, and types
- Additional Attacks types
- Worm attack anatomy
- Securing Endpoints with Cisco technologies
    - IronPort
    - Cisco NAC appliance
    - Cisco Security agents
- Best practice for securing Endpoints

Semester 3: Securing Network with Security – Specialist Network Devices

Firewall

- Introduction to firewall
- How firewall works
- Firewall Types
- Overview of Cisco Adaptive Security Appliances (ASA)
- Configuring ACL
- Implementing Cisco IOS Zone-Based Firewall
    - Cisco IOS firewall
    - Traffic Filtering and traffic inspection
    - Alerts and audit trails
    - SPI and CBAC
    - Zone-Based firewall Principles
    - Understanding Security zones
    - Zone membership rules, restrictions, and pairs
    - Zone firewall policies

Intrusion Prevention System (IPS) and Intrusion detection Systems (IDS)

- Overview about IPS and IDS
- Detection methods
- Network-based Vs Host-based IPS
- IDS and IPS appliances
- Signature types
- Alarms
- Configuring IPS using SDM

Semester 4: Securing Network connections

- Overview of IPSec
- Introduction to cryptography
- Cryptography types
- Cryptanalysis
- Encryption algorithm categorizations
    - Symmetric encryption protocols: DES, 3DES, AES, SEAL, Rivest
    - Asymmetric encryption protocols: RSA
    - Block cipher and stream cipher
- Understanding Security algorithms
- Understanding cryptographic hash
    - Hash algorithms: MD5, SHA-1
    - HMAC
    - Applications of cryptographic hash
- Understanding digital signature
- Digital signature scheme
- Digital Signature Algorithm (DSA)
- Key management
- Understanding Diffie-Hellman key exchange
- Understanding Pubic Key Infrastructure (PKI)
- PKI components
- PKI Standards
- Using Certificates
- SSL VPN
- How IPSec Works
    - Internet Key Exchange (IKE) modes and phases
    - AH and ESP
    - IPSec modes
- Cisco VPN solutions and products
- VPN design consideration and recommendations
- Configuring IPSec Site-to-Site VPN using CLI
    - Configuring IPSec Site-to-Site VPN using SDM

Semester 5: Securing some Application – Specific Networks

Securing Storage Area Networks

- Overview of SAN, Fundamentals, and benefits
- SAN security fundamentals
- SAN Attacks
- SAN Security Technologies

Securing VOIP-enabled Networks

- Defining VOIP, VOIP benefits, VOIP Network, VOIP network Components, and VOIP protocols
- Common voice vulnerabilities
- Securing VOIP Network