Course Name: CCNA Security
Course Time: 100 Hrs.
Course Prerequisites: CCNA Routing & Switching

Course Outline:

- **Common Security Threats**
  - Describe common security threats
    - Common threats to the physical installation
    - Mitigation methods for common network attacks
    - Email-based threats
    - Web-based attacks
    - Mitigation methods for Worm, Virus, and Trojan Horse attacks
    - Phases of a secure network lifecycle
    - Security needs of a typical enterprise with a comprehensive security policy
    - Mobile/remote security
    - DLP
- **Security and Cisco Routers**
  - Implement security on Cisco routers
    - CCP Security Audit feature
    - CCP One-Step Lockdown feature
    - Secure router access using strong encrypted passwords, and using IOS login enhancements, IPV6 security.
    - Multiple privilege levels
    - Role-based CLI
    - Cisco IOS image and configuration files
  - Describe securing the control, data and management plane
  - Describe CSM
  - Describe IPv4 to IPv6 transition
    - Reasons for IPv6
    - Understanding IPv6 addressing
    - Assigning IPv6 addresses
    - Routing considerations for IPv6
- **AAA on Cisco Devices**
  - Implement authentication, authorization, and accounting (AAA)
    - AAA using CCP on routers
    - AAA using CLI on routers and switches
    - AAA on ASA
  - Describe TACACS+
  - Describe RADIUS
  - Describe AAA
    - Authentication
    - Authorization
    - Accounting
  - Verify AAA functionality.
- **IOS ACLs**
  - Describe standard, extended, and named IP IOS ACLs to filter packets
    - IPv4
    - IPv6
    - Object groups
    - ACL operations
    - Types of ACLs (dynamic, reflexive, time-based ACLs)
    - ACL wild card masking

        - Standard ACLs
        - Extended ACLs
        - Named ACLs
        - VLSM
    - Describe considerations when building ACLs
        - Sequencing of ACEs
        - Modification of ACEs
    - Implement IP ACLs to mitigate threats in a network
        - Filter IP traffic
        - SNMP
        - DDoS attacks
        - CLI
        - CCP
        - IP ACLs to prevent IP spoofing
        - VACLs
- **Secure Network Management and Reporting**
    - Describe secure network management
        - In-band
        - Out of band
        - Management protocols
        - Management enclave
        - Management plane
    - Implement secure network management
        - SSH
        - syslog
        - SNMP
        - NTP
        - SCP
        - CLI
        - CCP
        - SSL
- **Common Layer 2 Attacks**
    - Describe Layer 2 security using Cisco switches
        - STP attacks
        - ARP spoofing
        - MAC spoofing
        - CAM overflows
        - CDP/LLDP
    - Describe VLAN Security
        - Voice VLAN
        - PVLAN
        - VLAN hopping
        - Native VLAN
    - Implement VLANs and trunking
        - VLAN definition
        - Grouping functions into VLANs
        - Considering traffic source to destination paths
        - Trunking
        - Native VLAN

        - VLAN trunking protocols
        - Inter-VLAN routing
    - Implement Spanning Tree
        - Potential issues with redundant switch topologies
        - STP operations
        - Resolving issues with STP
- **Cisco Firewall Technologies**
    - Describe operational strengths and weaknesses of the different firewall technologies
        - Proxy firewalls
        - Packet and stateful packet
        - Application firewall
        - Personal firewall
    - Describe stateful firewalls
        - Operations
        - Function of the state table
    - Describe the types of NAT used in firewall technologies
        - Static
        - Dynamic
        - PAT
    - Implement Zone Based Firewall using CCP
        - Zone to zone
        - Self zone
    - Implement the Cisco Adaptive Security Appliance (ASA)
        - NAT
        - ACL
        - Default MPF
        - Cisco ASA sec level
    - Implement NAT and PAT
        - Functions of NAT, PAT, and NAT Overload
        - Translating inside source addresses
        - Overloading Inside global addresses
- **Cisco IPS**
    - Describe IPS deployment considerations
        - SPAN
        - IPS product portfolio
        - Placement
        - Caveats
    - Describe IPS technologies
        - Attack responses
        - Monitoring options
        - syslog
        - SDEE
        - Signature engines
        - Signatures
        - Global correlation and SIO
        - Network-based
        - Host-based
    - Configure Cisco IOS IPS using CCP
        - Logging
        - Signatures

- **VPN Technologies**
  - Describe the different methods used in cryptography
    - Symmetric
    - Asymetric
    - HMAC
    - Message digest
    - PKI
  - Describe VPN technologies
    - IPsec
    - SSL
  - Describe the building blocks of IPSec
    - IKE
    - ESP
    - AH
    - Tunnel mode
    - Transport mode
  - Implement an IOS IPSec site-to-site VPN with pre-shared key authentication
    - CCP
    - CLI
  - Verify VPN operations.
  - Implement SSL VPN using ASA device manager
    - Clientless
    - AnyConnect