Implementing Cisco Network Security v3.0 - IINS (Associate)

Course Details

Course Outline

1. **Security Concepts**
   a. **Threatscape**
      - Threatscape Overview
      - DoS and DDoS
      - Spoofing
      - Reflection and Amplification Attacks
      - Social Engineering
      - Evolution of Phishing
      - Password Attacks
      - Reconnaissance Attacks
      - Buffer Overflow Attacks
      - Man-in-the-Middle Attacks
      - Malware
      - Vectors of Data Loss and Exfiltration
      - Hacking Tools
      - Other Considerations

   b. **Threat Defense Technologies**
      - Firewalls
      - Intrusion Prevention Systems
      - Content Security
      - VPNs
      - Endpoint Security
      - Logging

   c. **Security Policy and Basic Security Architectures**
      - Information Security Overview
      - Classifying Assets, Vulnerabilities, and Countermeasures

- Managing Risk
- Regulatory Compliance
- Principles of Secure Network Design
- Security Policy
- Security Zones
- The Functional Planes of the Network

d. Cryptographic Technologies

- Cryptography Overview
- Hash Algorithms
- Encryption Overview
- Cryptanalysis
- Symmetric Encryption Algorithms
- Asymmetric Encryption Algorithms
- Use Case: SSH
- Digital Signatures
- PKI Overview
- PKI Operations
- Use Case: SSL/TLS
- Key Management
- Discovery 1: Exploring Cryptographic Technologies

2. Secure Network Devices

a. Implementing AAA

- Introduction to AAA
- AAA Databases
- AAA Protocols
- AAA Servers
- SSH Configuration and Operation on IOS
- IOS Authorization with Privilege Levels
- Implementing Local AAA Authentication and Authorization
- Authorization with Role-Based CLI
- TACACS+ on IOS

        - Discovery 2: Configure and Verify AAA

    b. **Management Protocols and Systems**

        - IOS File System
        - Copying Files to and from Network Devices
        - Validating IOS Images Using MD5
        - Digitally Signed Images
        - IOS Resilient Configuration
        - NTP
        - Syslog
        - Memory and CPU Threshold Notifications
        - Netflow
        - Configuration Management Protocol Options
        - HTTPS Configuration and Operation
        - SNMPv3 Configuration and Operation
        - Locking Down Management Access with ACLs
        - Other Password Considerations
        - Discovery 3: Configuration Management Protocols

    c. **Securing the Control Plane**

        - The Control Plane
        - Control Plane Policing
        - Control Plane Protection
        - Authenticating Routing Protocols
        - OSPF Route Authentication
        - EIGRP Route Authentication
        - Discovery 4: Securing Routing Protocols

3. **Layer 2 Security**

    a. **Securing Layer 2 Infrastructure**

        - Introduction to Layer 2 Security
        - Ethernet Switching Overview
        - VLAN Overview
        - VLAN Configuration

- 802.1Q Trunking
- Trunk Attacks
- Trunk Configuration and Attack Mitigation
- CDP
- ACL Primer
- ACLs on Switches
- MAC Address Abuse
- Port Security
- Private VLANs
- Private VLAN Edge
- Private VLAN Proxy Attack and Mitigation
- Discovery 5: VLAN Security and ACLs on Switches
- Discovery 6: Port Security and Private VLAN Edge

b. **Securing Layer 2 Protocols**

- STP Overview
- STP Attacks
- STP Attack Mitigation
- DHCP Overview
- DHCP Attacks
- DHCP Snooping
- ARP Overview
- ARP Cache Poisoning Attack
- Dynamic ARP Inspection
- Discovery 7: Securing DHCP, ARP, and STP

4. **Firewall**

a. **Firewall Technologies**

- Firewall Overview
- Packet Filters
- Stateful Firewalls
- Proxy Servers
- Next Generation Firewalls

- Logging
- Discovery 8: Explore Firewall Technologies

b. Introducing the Cisco ASA v9.2

- Introducing the Cisco ASA Family of Security Appliances
- Cisco ASA Firewall Features
- Modes of Deployment
- Security Contexts
- High-Availability and Failover
- Configuring Management Access on the Cisco ASA
- Configuring Cisco ASA Interfaces
- NAT Fundamentals
- Configure NAT on Cisco ASA
- Configure Static NAT on Cisco ASA
- Configure Dynamic NAT on Cisco ASA
- Configure PAT on Cisco ASA
- Configure Policy NAT on Cisco ASA
- Verify NAT Operations
- Discovery 9: Cisco ASA Interfaces and NAT

c. Cisco ASA Access Control and Service Policies

- Overview of Interface Access Rules
- Configure Interface Access Rules
- Configure Object Groups
- Introducing Cisco ASA Modular Policy Framework
- Configuring Cisco MPF Service Policy Rules
- Discovery 10: Access Control Using the Cisco ASA

d. Cisco IOS Zone Based Firewall

- Zone-Based Policy Firewall Overview
- Zones and Zone Pairs
- Introduction to Cisco Common Classification Policy Language
- Default Policies, Traffic Flows, and Zone Interaction
- Cisco Common Classification Policy Language (C3PL) Configuration Overview

- Configuring Zone-Based Policy Firewall Class-Maps
- Configuring Zone-Based Policy Firewall Policy-Maps
- Discovery 11: Exploring Cisco IOS Zone-Based Firewall

5. **VPN**

   a. **IPsec Technologies**

   - IPsec VPNs
   - IPsec Security Services
   - IPsec Framework
   - Internet Key Exchange
   - IKE Phase 1
   - ISAKMP Configuration
   - IPsec Protocols
   - IKE Phase 2
   - IPsec Configuration
   - Suite B Cryptographic Standard
   - IKE Version 2
   - IPsec with IPv6
   - Discovery 12: Explore IPsec Technologies

   b. **Site-to-Site VPN**

   - Site-to-Site Tunnel Negotiation Process
   - Configuring Site-to-Site IPsec VPN
   - Step 1: Ensure That ACLs Are Compatible with IPsec
   - Step 2: Create ISAKMP IKE Phase 1 Policies
   - Step 3: Configure Transform Sets
   - Step 4: Create Crypto ACLs Using Extended ACLs
   - Step 5: Configure IPsec Crypto Maps
   - Verifying the IPsec Configuration
   - Configuring Site-to-Site VPN on Cisco ASA
   - Monitoring Site-to-Site VPN Configuration in ASDM
   - Discovery 13: IOS-Based Site-to-Site VPN
   - Discovery 14: ASA-Based Site-to-Site VPN

c. Client Based Remote Access VPN

- Secure Sockets Layer and Transport Layer Security
- Basic Cisco AnyConnect SSL VPN
- Cisco AnyConnect SSL VPN Solution Components
- SSL VPN Server Authentication
- SSL VPN Client Authentication
- SSL VPN Client IP Address Assignment
- Basic AnyConnect SSL VPN Configuration Tasks
- Discovery 15: Remote Access VPN: ASA and AnyConnect

d. Clientless Remote Access VPN

- Cisco Clientless SSL VPN
- Cisco Clientless SSL VPN Use Cases
- Cisco Clientless SSL VPN Resource Access Methods
- Basic Clientless SSL VPN Solution
- Server Authentication in Basic Clientless SSL VPN
- Client-Side Authentication in Basic Clientless SSL VPN
- Clientless SSL VPN URL Entry and Bookmarks
- Basic Access Control for Clientless SSL VPN
- Basic Clientless SSL VPN Configuration Tasks
- Discovery 16: Clientless Remote Access VPN

6. Advanced Topics

a. Intrusion Detection and Protection

- Introduction to IPS
- IPS Terminology
- Evasion Techniques and Countermeasures
- Protecting the Network with FireSIGHT
- FireSIGHT Protection Before an Attack
- FireSIGHT Protection During an Attack
- FireSIGHT Protection After an Attack
- FireSIGHT Deployment Options
- Inline and Passive Mode Deployment Options

b. Endpoint Protection

- Endpoint Security Overview
- Personal Firewalls
- Antivirus and Antispyware
- Centralized Endpoint Policy Enforcement
- Cisco AMP for Endpoints

c. Content Security

- Cisco ESA Deployment
- Cisco ESA Overview
- Cisco ESA Features and Benefits
- Cisco ESA GUI Management
- Cisco ESA Mail Processing
- Cisco WSA Deployment
- Cisco WSA Overview
- Cisco WSA Features and Benefits
- Cisco WSA GUI Management
- Cisco CWS Deployment
- Cisco CWS Overview
- Cisco CWS Features and Benefits

d. Advanced Network Security Architectures

- Modular Network Architectures
- Security Issues in Modern Networks
- Identity Management
- BYOD Challenge
- Cisco TrustSec

7. Lab

a. Challenge: Configure AAA and Secure Remote Administration

- Configure AAA and Secure Remote Administration

b. Challenge: Configure Secure Network Management Protocols

- Configure Secure Network Management Protocols

c. Challenge: Configure Secure EIGRP Routing

  - Configure EIGRP route authentication

d. **Challenge: Configure Secure Layer 2 Infrastructure**
  - Configure Secure Layer 2 Infrastructure

e. **Challenge: Configure DHCP Snooping and STP Protection**
  - Configure DHCP Snooping and STP Protection

f. **Challenge: Configure Interfaces and NAT on the Cisco ASA**
  - Configure Interfaces and NAT on Cisco ASA

g. **Challenge: Configure Network Access Control with the Cisco ASA**
  - Configure Network Access Control with the Cisco ASA

h. **Challenge: Configure Site-to-Site VPN on IOS**
  - Configure Site-to-Site VPN on IOS

i. **Challenge: Configure AnyConnect Remote Access VPN on ASA**
  - Configure AnyConnect Remote Access VPN on ASA

j. **Challenge: Configure Clientless SSL VPN on the ASA**
  - Configure Clientless SSL VPN on the ASA