CCIE Security Overview

The Cisco Certified Internetwork Expert Security (CCIE Security) program acknowledge security experts who have the knowledge and skills to implement, architect, engineer, troubleshoot, and support the full suite of Cisco security solutions and technologies using the recent and upgraded industry best practices to safeguard systems and surroundings against modern requirements, vulnerabilities, security risks, and threats.

About the training

- **Study Material:-** Live lectures, Streaming Recorded Videos, Online Lab Workbook, and Remote Virtual Lab access.
- **Duration:-** 4 Months

Requirements

Aspirants are recommended to have atleast 5 to 7 years of experience with operating, designing, optimizing and deploying, security technologies and solutions prior to taking the exam.

What you will learn

- Brief knowledge about Cloud security and network security
- Understanding endpoint detection and protection
- Explore more about visibility and enforcement
- Implementing secure network access and content security

About Instructor

The trainer of this course has 9+ years of industrial experience and is expert in technology. The trainer is also verified by UniNets itself. He has delivered vast and complex project on the same around the globe.

Course content

Qualifying Exam (SCOR 350 – 701)

- Describing Information Security Concepts*
  - Information Security Overview
  - Assets, Vulnerabilities, and Countermeasures
  - Managing Risk
  - Vulnerability Assessment
  - Exploring Common Vulnerability Scoring System (CVSS)
- Describing Common TCP/IP Attacks*
  - Legacy TCP/IP Vulnerabilities
  - IP Vulnerabilities
  - Internet Control Message Protocol (ICMP) Vulnerabilities
  - TCP Vulnerabilities
  - User Datagram Protocol (UDP) Vulnerabilities
  - Attack Surface and Attack Vectors
  - Reconnaissance Attacks
  - Access Attacks
  - Man-in-the-Middle Attacks
  - Denial of Service and Distributed Denial of Service Attacks
  - Reflection and Amplification Attacks
  - Spoofing Attacks
  - Dynamic Host Configuration Protocol (DHCP) Attacks
- Describing Common Network Application Attacks*
  - Password Attacks
  - Domain Name System (DNS)-Based Attacks
  - DNS Tunneling
  - Web-Based Attacks
  - HTTP 302 Cushioning
  - Command Injections
  - SQL Injections
  - Cross-Site Scripting and Request Forgery
  - Email-Based Attacks
- Describing Common Endpoint Attacks*
  - Buffer Overflow
  - Malware
  - Reconnaissance Attack
  - Gaining Access and Control
  - Gaining Access via Social Engineering

- Gaining Access via Web-Based Attacks
- Exploit Kits and Rootkits
- Privilege Escalation
- Post-Exploitation Phase
- Angler Exploit Kit

- Describing Network Security Technologies
  - Defense-in-Depth Strategy
  - Defending Across the Attack Continuum
  - Network Segmentation and Virtualization Overview
  - Stateful Firewall Overview
  - Security Intelligence Overview
  - Threat Information Standardization
  - Network-Based Malware Protection Overview
  - Intrusion Prevention System (IPS) Overview
  - Next Generation Firewall Overview
  - Email Content Security Overview
  - Web Content Security Overview
  - Threat Analytic Systems Overview
  - DNS Security Overview
  - Authentication, Authorization, and Accounting Overview
  - Identity and Access Management Overview
  - Virtual Private Network Technology Overview
  - Network Security Device Form Factors Overview
- Deploying Cisco ASA Firewall
  - Cisco ASA Deployment Types
  - Cisco ASA Interface Security Levels
  - Cisco ASA Objects and Object Groups
  - Network Address Translation
  - Cisco ASA Interface Access Control Lists (ACLs)
  - Cisco ASA Global ACLs
  - Cisco ASA Advanced Access Policies
  - Cisco ASA High Availability Overview
- Deploying Cisco Firepower Next-Generation Firewall
  - Cisco Firepower NGFW Deployments
  - Cisco Firepower NGFW Packet Processing and Policies
  - Cisco Firepower NGFW Objects
  - Cisco Firepower NGFW Network Address Translation (NAT)
  - Cisco Firepower NGFW Prefilter Policies
  - Cisco Firepower NGFW Access Control Policies
  - Cisco Firepower NGFW Security Intelligence

- Cisco Firepower NGFW Discovery Policies
- Cisco Firepower NGFW IPS Policies
- Cisco Firepower NGFW Malware and File Policies

- Deploying Email Content Security
  - Cisco Email Content Security Overview
  - Simple Mail Transfer Protocol (SMTP) Overview
  - Email Pipeline Overview
  - Public and Private Listeners
  - Host Access Table Overview
  - Recipient Access Table Overview
  - Mail Policies Overview
  - Protection Against Spam and Graymail
  - Anti-virus and Anti-malware Protection
  - Outbreak Filters
  - Content Filters
  - Data Loss Prevention
  - Email Encryption
- Deploying Web Content Security
  - Cisco Web Security Appliance (WSA) Overview
  - Deployment Options
  - Network Users Authentication
  - Secure HTTP (HTTPS) Traffic Decryption
  - Access Policies and Identification Profiles
  - Acceptable Use Controls Settings
  - Anti-Malware Protection
- Deploying Cisco Umbrella*
  - Cisco Umbrella Architecture
  - Deploying Cisco Umbrella
  - Cisco Umbrella Roaming Client
  - Managing Cisco Umbrella
  - Cisco Umbrella Investigate Overview and Concepts
- Introducing VPN Technologies and Cryptography
  - VPN Definition
  - VPN Types
  - Secure Communication and Cryptographic Services
  - Keys in Cryptography
  - Public Key Infrastructure
- Explaining Cisco Secure Site-to-Site VPN Solutions
  - Site-to-Site VPN Topologies
  - IPsec VPN Overview

- IPsec Static Crypto Maps
- IPsec Static Virtual Tunnel Interface
- Dynamic Multipoint VPN
- Cisco IOS FlexVPN

- Implementing Cisco IOS VTI-Based Point-to-Point IPsec VPNs
  - Cisco IOS VTIs
  - Static VTI Point-to-Point IPsec Internet Key Exchange (IKE) v2 VPN Configuration
- Implementing Point-to-Point IPsec VPNs on the Cisco ASA and Cisco Firepower NGFW
  - Point-to-Point VPNs on the Cisco ASA and Cisco Firepower NGFW
  - Cisco ASA Point-to-Point VPN Configuration
  - Cisco Firepower NGFW Point-to-Point VPN Configuration
- Explaining Cisco Secure Remote Access VPN Solutions
  - Remote Access VPN Components
  - Remote Access VPN Technologies
  - Secure Sockets Layer (SSL) Overview
- Implementing Remote Access SSL VPNs on the Cisco ASA and Cisco Firepower NGFW
  - Remote Access Configuration Concepts
  - Connection Profiles
  - Group Policies
  - Cisco ASA Remote Access VPN Configuration
  - Cisco Firepower NGFW Remote Access VPN Configuration
- Implementing Cisco Secure Network Access Solutions
  - Cisco Secure Network Access
  - Cisco Secure Network Access Components
  - AAA Role in Cisco Secure Network Access Solution
  - Cisco Identity Services Engine
  - Cisco TrustSec
- Describing 802.1X Authentication
  - 802.1X and Extensible Authentication Protocol (EAP)
  - EAP Methods
  - Role of Remote Authentication Dial-in User Service (RADIUS) in 802.1X Communications
  - RADIUS Change of Authorization
- Configuring 802.1X Authentication
  - Cisco Catalyst® Switch 802.1X Configuration
  - Cisco Wireless LAN Controller (WLC) 802.1X Configuration
  - Cisco Identity Services Engine (ISE) 802.1X Configuration
  - Supplicant 802.1x Configuration

- Cisco Central Web Authentication

- Explaining Endpoint Security Technologies*
  - Host-Based Personal Firewall
  - Host-Based Anti-Virus
  - Host-Based Intrusion Prevention System
  - Application Whitelists and Blacklists
  - Host-Based Malware Protection
  - Sandboxing Overview
  - File Integrity Checking
- Implementing Cisco Advanced Malware Protection (AMP) for Endpoints*
  - Cisco AMP for Endpoints Architecture
  - Cisco AMP for Endpoints Engines
  - Retrospective Security with Cisco AMP
  - Cisco AMP Device and File Trajectory
  - Managing Cisco AMP for Endpoints
- Explaining Network Infrastructure Protection*
  - Identifying Network Device Planes
  - Control Plane Security Controls
  - Management Plane Security Controls
  - Network Telemetry
  - Layer 2 Data Plane Security Controls
  - Layer 3 Data Plane Security Controls
- Deploying Control Plane Security Controls*
  - Infrastructure ACLs
  - Control Plane Policing
  - Control Plane Protection
  - Routing Protocol Security
- Implementing Layer 2 Data Plane Security Controls*
  - Overview of Layer 2 Data Plane Security Controls
  - Virtual LAN (VLAN)-Based Attacks Mitigation
  - Spanning Tree Protocol (STP) Attacks Mitigation
  - Port Security
  - Private VLANs
  - Dynamic Host Configuration Protocol (DHCP) Snooping
  - Address Resolution Protocol (ARP) Inspection
  - Storm Control
  - MACsec Encryption
- Implementing Layer 3 Data Plane Security Controls*
  - Infrastructure Antispoofing ACLs
  - Unicast Reverse Path Forwarding

- IP Source Guard

- Implementing Management Plane Security Controls*
  - Cisco Secure Management Access
  - Simple Network Management Protocol Version 3
  - Secure Access to Cisco Devices
  - AAA for Management Access
- Deploying Traffic Telemetry Methods*
  - Network Time Protocol
  - Device and Network Events Logging and Export
  - Network Traffic Monitoring Using NetFlow
- Implementing Cisco Stealthwatch Enterprise*
  - Cisco Stealthwatch Offerings Overview
  - Cisco Stealthwatch Enterprise Required Components
  - Flow Stitching and Deduplication
  - Stealthwatch Enterprise Optional Components
  - Stealthwatch Enterprise and ISE Integration
  - Cisco Stealthwatch with Cognitive Analytics
  - Cisco Encrypted Traffic Analytics
  - Host Groups
  - Security Events and Alarms
  - Host, Role, and Default Policies
- Compare Cloud and Common Cloud Attacks*
  - Evolution of Cloud Computing
  - Cloud Service Models
  - Security Responsibilities in Cloud
  - Cloud Deployment Models
  - Common Security Threats in Cloud
  - Patch Management in the Cloud
  - Security Assessment in the Cloud
- Securing the Cloud*
  - Cisco Threat-Centric Approach to Network Security
  - Cloud Physical Environment Security
  - Application and Workload Security
  - Cloud Management and API Security
  - Network Function Virtualization (NFV) and Virtual Network Functions (VNF)
  - Cisco NFV Examples
  - Reporting and Threat Visibility in Cloud
  - Cloud Access Security Broker
  - Cisco CloudLock®
  - OAuth and OAuth Attacks

- Implementing Cisco Stealthwatch Cloud*
  - Cisco Stealthwatch Cloud for Public Cloud Monitoring
  - Cisco Stealthwatch Cloud for Private Network Monitoring
  - Cisco Stealthwatch Cloud Operations
- Comparing Software-Defined Networking (SDN*)
  - Software-Defined Networking Concepts
  - Network Programmability and Automation
  - Cisco Platforms and APIs
  - Basic Python Scripts for Automation

Lab outline

- Configure and Implement Network Settings and NAT on Cisco ASA
- Configure and Implement Cisco ASA Access Control Policies
- Configure and Implement Cisco Firepower NGFW NAT
- Configure and Implement Cisco Firepower NGFW Access Control Policy
- Configure and Implement Cisco Firepower NGFW Discovery and IPS Policy
- Configure and Implement Cisco NGFW Malware and File Policy
- Implement Listener, Host Access Table (HAT), and Recipient Access Table (RAT) on Cisco Email Security Appliance (ESA)
- Configure Mail Policies
- Implement Proxy Services, Authentication, and HTTPS Decryption
- Enforce Acceptable Use Control and Malware Protection
- Examine the Umbrella Dashboard
- Examine Cisco Umbrella Investigate
- Explore DNS Ransomware Protection by Cisco Umbrella
- Configure Static VTI Point-to-Point IPsec IKEv2 Tunnel
- Configure Point-to-Point VPN between the Cisco ASA and Cisco Firepower NGFW
- Configure Remote Access VPN on the Cisco Firepower NGFW
- Explore Cisco AMP for Endpoints
- Do Endpoint Analysis Using AMP for Endpoints Console
- Do File Ransomware Protection by Cisco AMP for Endpoints Console
- Do Cisco Stealthwatch Enterprise v6.9.3
- Do Cognitive Threat Analytics (CTA) in Stealthwatch Enterprise v7.0
- Do the Cisco Cloudlock Dashboard and User Security
- Do Cisco Cloudlock Application and Data Security
- Do Cisco Stealthwatch Cloud
- Do Stealthwatch Cloud Alert Settings, Watchlists, and Sensors

Lab Exam (CCIE Security (v6.0)

- Perimeter Security and Intrusion Prevention
  - Deployment modes on Cisco ASA and Cisco FTD
    a. Routed
    b. Transparent
    c. Single
    d. Multi-Context
    e. Multi-Instance
  - Firewall features on Cisco ASA and Cisco FTD
    a. NAT
    b. Application inspection
    c. Traffic zones
    d. Policy-based routing
    e. Traffic redirection to service modules
    f. Identity firewall
  - Security features on Cisco IOS/IOS-XE
    a. Application awareness
    b. Zone-Based Firewall (ZBFW)
    c. NAT
  - Cisco Firepower Management Center (FMC) features
    a. Alerting
    b. Logging
    c. Reporting
  - NGIPS deployment modes

    a. In-Line
    b. Passive
    c. TAP

  - Next Generation Firewall (NGFW) features

    a. SSL inspection
    b. user identity
    c. Geolocation
    d. AVC

  - Detect, and mitigate common types of attacks
    a. DoS/DDoS
    b. Evasion Techniques
    c. Spoofing
    d. Man-In-The-Middle

e. Botnet

- Clustering/HA features on Cisco ASA and Cisco FTD
- Policies and rules for traffic control on Cisco ASA and Cisco FTD
- Routing protocols security on Cisco IOS, Cisco ASA and Cisco FTD
- Network connectivity through Cisco ASA and Cisco FTD
- Correlation and remediation rules on Cisco FMC

- Secure Connectivity and Segmentation
  - Any Connect client-based remote access VPN technologies on Cisco ASA, Cisco FTD, and Cisco Routers.
  - Cisco IOS CA for VPN authentication
  - FlexVPN, DMVPN, and IPsec L2L Tunnels
  - Uplink and downlink MACsec (802.1AE)
  - VPN high availability using
  - Infrastructure segmentation methods
  - Micro-segmentation with Cisco TrustSec using SGT and SXP

- Infrastructure Security
  - Device hardening techniques and control plane protection methods
  - Management plane protection techniques
  - Data plane protection techniques
  - Layer 2 security techniques
  - Wireless security technologies
  - Monitoring protocols
  - Security features to comply with organizational security policies, procedures, and standards BCP 38
  - Cisco SAFE model to validate network security design and to identify threats to different Places in the Network (PINs)
  - Interaction with network devices through APIs using basic Python scripts
  - Cisco DNAC Northbound APIs use cases

- Identity Management, Information Exchange, and Access Control
  - ISE scalability using multiple nodes and personas.
  - Cisco switches and Cisco Wireless LAN Controllers for network access AAA with ISE.
  - Cisco devices for administrative access with ISE
  - AAA for network access with 802.1X and MAB using ISE.
  - Guest lifecycle management using ISE and Cisco Wireless LAN controllers
  - BYOD on-boarding and network access flows
  - ISE integration with external identity sources
  - Provisioning of AnyConnect with ISE and ASA
  - Posture assessment with ISE

- Endpoint profiling using ISE and Cisco network infrastructure including device sensor
- Integration of MDM with ISE
- Certificate-based authentication using ISE
- Authentication methods
- Identity mapping on ASA, ISE, WSA, and FTD
- pxGrid integration between security devices WSA, ISE, and Cisco FMC
- Integration of ISE with multi-factor authentication
- Access control and single sign-on using Cisco DUO security technology

- Advanced Threat Protection and Content Security
  - AMP for networks, AMP for endpoints, and AMP for content security (ESA, and WSA)
  - Detect, analyze, and mitigate malware incidents
  - Perform packet capture and analysis using Wireshark, tcpdump, SPAN, ERSPAN, and RSPAN
  - DNS layer security, intelligent proxy, and user identification using Cisco Umbrella
  - Web filtering, user identification, and Application Visibility and Control (AVC) on Cisco FTD and WSA.
  - WCCP redirection on Cisco devices
  - Email security features
  - HTTPS decryption and inspection on Cisco FTD, WSA and Umbrella
  - SMA for centralized content security management
  - Cisco advanced threat solutions and their integration: Stealthwatch, FMC, AMP, Cognitive Threat Analytics (CTA), Threat Grid, Encrypted Traffic Analytics (ETA), WSA, SMA, CTR, and Umbrella

Note: ***Most of the course topics are covered with hands-on lab exercises and others are theoretical

Thank You
Visit us
https://www.uninets.com/