NETLOGIC TRAINING CENTER

Course Training

Cisco Certificated Network Associated Security – CCNA Security (210-260 IINS) version 3.0

Course Content

Implementing Cisco Network Security (IINS) v3.0 is a 5-day instructor-led course presented by Cisco Learning Partners to end users and channel partner customers. The course focuses on security principles and technologies, using Cisco security products to provide hands-on examples. Using instructor-led discussions, extensive hands-on lab exercises, and supplemental materials, this course allows learners to understand common security concepts, and deploy basic security techniques utilizing a variety of popular security appliances within a "real-life" network infrastructure.

Course Objective

Upon completion of the course, students will have the knowledge and skills to:

- Describe common network security concepts
- Secure routing and switching infrastructure
- Deploy basic authentication, authorization and accounting services
- Deploy basic firewalling services
- Deploy basic site-to-site and remote access VPN services
- Describe the use of more advanced security services such as intrusion protection, content security and identity management

Course Prerequisite

It is strongly recommended, that students have the following knowledge and skills:

- Skills and knowledge equivalent to those learned in Interconnecting Cisco Networking Devices Part 1 (ICND1) and Cisco Networking Devices Part 2 (ICND2)
- Working knowledge of the Windows operating system
- Working knowledge of Cisco IOS networking and concepts

Course Pre-Test

Not Required

Course Details

Day 1

Item	Subject	Details	Personal Lab and devices	Workgroup Lab and devices
1	Security Concepts	• Common security principles a Describe confidentiality, integrity, availability (CIA) b Describe SIEM technology c Identify common security terms d Identify common network security zones • Common security threats a Identify common network attacks b Describe social engineering c Identify malware d Classify the vectors of data loss/exfiltration	Theory and Lecture	
		Break		
		• Cryptography concepts a Describe key exchange b Describe hash algorithm c Compare and contrast symmetric and asymmetric encryption d Describe digital signatures, certificates, and PKI • Describe network topologies a Campus area network (CAN) b Cloud, wide area network (WAN) c Data center d Small office/home office (SOHO) e Network security for a virtual environment	Theory and Lecture	
	Summary challenge advance lab for factory default and basic configure	(Lab 1) Factory Default ASA (Lab 2) ASA basic configuration and ASDM	(Lab 1 and Lab 2) **Real Devices** Switch 2960 1 Unit Switch 3650 1unit ISR router 4300 1 unit ASA 5506 1 Unit ASDM software	

Day 2

Item	Subject	Details	Trainee Lab and devices	Workgroup Lab and devices
2	Secure Access	• Secure management a Compare in-band and out-of-band b Configure secure network management c Configure and verify secure access through SNMP v3 using an ACL d Configure and verify security for NTP e Use SCP for file transfer • AAA concepts a Describe RADIUS and TACACS+ technologies b Configure administrative access on a Cisco router using TACACS+ c Verify connectivity on a Cisco router to a TACACS+ server d Explain the integration of Active Directory with AAA e Describe authentication and authorization using ACS and ISE • 802.1X authentication a Identify the functions 802.1X components • BYOD a Describe the BYOD architecture framework b Describe the function of mobile device management (MDM)	Theory and Lecture	
		Break		
3	VPN	• VPN concepts a Describe IPsec protocols and delivery modes (IKE, ESP, AH, tunnel mode, transport mode) b Describe hairpinning, split tunneling, always-on, NAT traversal • Remote access VPN a Implement basic clientless SSL VPN using ASDM b Verify clientless connection c Implement basic AnyConnect SSL VPN using ASDM d Verify AnyConnect connection e Identify endpoint posture assessment • Site-to-site VPN a 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	Theory and Lecture	
	Summary challenge advance lap for Router secure access and VPN	(Lab 1) Configure SNMPv3 and controller access via ACL (Lab 2) Configure secure-NTP (Lab 3) Configure site-to-site VPN (Lab 4) Configure SSL VPN	(Lab 1 and Lab 2) **Real Devices** Switch 2960 1 Unit Switch 3650 1unit ISR router 4300 1 unit ASA 5506 1 Unit	(Lab 3 and Lab 4) **Real Devices** Switch 2960 1 Unit Switch 3650 1unit ISR router 4300 1 unit ASA 5506 1 Unit Anyconnect software ASDM software

Day 3

Item	Subject	Details	Trainee Lab and devices	Workgroup Lab and devices
4	Secure Routing and Switching	• Security on Cisco routers a Configure multiple privilege levels b Configure Cisco IOS role-based CLI access c Implement Cisco IOS resilient configuration • Securing routing protocols a Implement routing update authentication on OSPF • Securing the control plane a Explain the function of control plane policing	Theory and Lecture	
		Break		
		• Common Layer 2 attacks a Describe STP attacks b Describe ARP spoofing c Describe MAC spoofing d Describe CAM table (MAC address table) overflows e Describe CDP/LLDP reconnaissance f Describe VLAN hopping g Describe DHCP spoofing • Mitigation procedures a Implement DHCP snooping b Implement Dynamic ARP Inspection c Implement port security d Describe BPDU guard, root guard, loop guard e Verify mitigation procedures • VLAN security a Describe the security implications of a PVLAN b Describe the security implications of a native VLAN	Theory and Lecture	
	Summary challenge advance lap for Access control , Private VLAN and switch security Feature	(Lab 1) Configure IOS RBAC via CLI (Lab 2) Configure Private VLAN (Lab 3) Configure Port Security feature and error-disable state (Lab 4) Configure DHCP snooping	(Lab 1, 2, and 3) **Real Devices** Switch 2960 1 Unit Switch 3560 1 unit ISR router 4300 1 unit	(Lab 4) **Real Devices** Switch 2960 1 Unit Switch 3560 1 unit ISR router 4300 1 unit

Day 4

Item	Subject	Details	Personal Lab and devices	Workgroup Lab and devices
5	Cisco Firewall Technologies	• Describe operational strengths and weaknesses of the different firewall technologies a Proxy firewalls b Application firewall c Personal firewall • Compare stateful vs. stateless firewalls a Operations b Function of the state table • Implement NAT on Cisco ASA 9.x a Static b Dynamic c PAT d Policy NAT e Verify NAT operation	Theory and Lecture	
		Break		
		• Implement zone-based firewall a Zone to zone b Self zone • Firewall features on the Cisco Adaptive Security Appliance (ASA) 9.x a Configure ASA access management b Configure security access policies c Configure Cisco ASA interface security levels d Configure default Cisco Modular Policy Framework (MPF) e Describe modes of deployment (routed firewall, transparent firewall) f Describe methods of implementing high availability g Describe security contexts h Describe firewall services	Theory and Lecture	
	Summary challenge advance lab for NAT and Firewall feature	(Lab 1) ASA basic configuration and verify (Lab 2) Configure NAT on ASA (Lab 3) Configure zone-base firewall with IOS Firewall (Lab 4) Configure CBAC firewall with IOS Firewall	(Lab 1 and Lab 2) **Real Devices** Switch 2960 1 Unit Switch 3650 1unit ISR router 4300 1 unit ASA 5506 1 Unit	(Lab 3 and Lab 4) **Real Devices** Switch 2960 1 Unit Switch 3650 1unit ISR router 4300 1 unit

Day 5

Item	Subject	Details	Personal Lab and devices	Workgroup Lab and devices
6	IPS	• Describe IPS deployment considerations a Network-based IPS vs. host-based IPS b Modes of deployment (inline, promiscuous - SPAN, tap) c Placement (positioning of the IPS within the network) d False positives, false negatives, true positives, true negatives • Describe IPS technologies a Rules/signatures b Detection/signature engines c Trigger actions/responses (drop, reset, block, alert, monitor/log, shun) d Blacklist (static and dynamic)\	Theory and Lecture	
		Break		
7	Content and Endpoint Security	• Describe mitigation technology for email-based threats a SPAM filtering, anti-malware filtering, DLP, blacklisting, email encryption • Describe mitigation technology for web-based threats a Local and cloud-based web proxies b Blacklisting, URL filtering, malware scanning, URL categorization, web application filtering, TLS/SSL decryption • Describe mitigation technology for endpoint threats a Anti-virus/anti-malware b Personal firewall/HIPS c Hardware/software encryption of local data	Theory and Lecture	
	Summary challenge advance lab for IOS IPS and Dynamic ACL	(Lab 1) Enabling and fine tune IOS IPS on router (Lab 2) Configure Dynamic ACL and secure access	(Lab 1) **Real Devices** Switch 2960 1 Unit Switch 3650 1unit ISR router 4300 1 unit	(Lab 2) **Real Devices** Switch 2960 1 Unit Switch 3650 1unit ISR router 4300 1 unit

Course Post-Test

Not Required

Course Materials

Not include in this class training (but you can requested from sale team)

Course Devices Training (Per 1 Personal)

Cisco Catalyst 3650-CX

Cisco Router ISR 4321

Cisco ASA 5506

Cisco Catalyst 2960

CISCO

CCNA Security