CCNA SECURITY SYLLABUS

Best CCNA Security Training in PUNE & Best CCNA Security Training Institute in MAHARASHTRA

RAHITECH is the biggest CCNA Security training center in PUNE with high tech infrastructure and lab facilities and the options of opting for multiple courses at PUNE Location. RAHITECH in PUNE prepares thousands of aspirants for CCNA Security at reasonable fees that is customized keeping in mind training and course content requirement of each attendee. CCNA Security training course involves "Learning by Doing" using state-of-the-art infrastructure for performing hands-on exercises and real-world simulations. This extensive hands-on experience in CCNA Security training ensures that you absorb the knowledge and skills that you will need to apply at work after your placement in an MNC.

IMPORTANCE OF CCNA SECURITY :-

For network engineers who need to increase their value to employers and stay current with advances in networking knowledge and skills, the cisco CCNA Security certification program provides the education and training required for installing, monitoring, and troubleshooting network infrastructure products designed by the industry leader in IP networking.

The CCNA Security certification validates the ability to install, configure, operate, and troubleshoot medium-size routed and switched networks. CCNA Security certified professionals have the knowledge and skills to make connections to remote sites via a WAN, and mitigate basic security threats. CCNA Security training covers (but is not limited to) the use of these topics: Layer 2 Security, IPS/IDS, IP Security, Private VLANs, VACLs, Cisco Licensing for firewall features, AAA, Context Based Access Control (CBAC), Zone Based Firewall (ZBF),IPSEC VPNs – Site-to-Site, Remote access, SSL Clientless and Full client VPN on ASA. CCNA Security Routing and Switching certifications are valid for three years. The CCNA Security curriculum emphasizes core security technologies, the installation, troubleshooting and monitoring of network devices to maintain integrity, confidentiality and availability of data and devices, and competency in the technologies that Cisco uses in its security structure.

CCNA SECURITY SYLLABUS

Topic
Security Concepts Common security principles Describe confidentiality, integrity, availability (CIA) Describe SIEM technology Identify common security terms Identify common network security zones Common security threats Identify common network attacks Describe social engineering Identify malware Classify the vectors of data loss/exfiltration Cryptography concepts Describe key exchange Describe hash algorithm Compare and contrast symmetric and asymmetric encryption Describe digital signatures, certificates, and PKI Describe network topologies Campus area network (CAN) Cloud, wide area network (WAN) 1.4.c Data center Small office/home office (SOHO) Network security for a virtual environment **Secure Access** Secure management Compare in-band and out-of band 2.1.b Configure secure network management Configure and verify secure access through SNMP v3 using an ACL Configure and verify security for NTP Use SCP for file transfer AAA concepts Describe RADIUS and TACACS+ technologies Configure administrative access on a Cisco router using TACACS+ 2.2.c Verify connectivity on a Cisco router to a TACACS+ server Explain the integration of Active Directory with AAA Describe authentication and authorization using ACS and ISE 802.1X authentication Identify the functions 802.1X components BYOD Describe the BYOD architecture framework Describe the function of mobile device management (MDM)

CCNA SECURITY SYLLABUS

VPN

VPN concepts
Describe IPsec protocols and delivery modes (IKE, ESP, AH, tunnel mode, transport mode)
Describe hairpinning, split tunneling, always-on, NAT traversal
Remote access VPN
Implement basic clientless SSL VPN using ASDM Verify clientless connection
Implement basic AnyConnect SSL VPN using ASDM Verify AnyConnect connection
Identify endpoint posture assessment
Site-to-site VPN
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

Secure Routing and Switching

Security on Cisco routers
Configure multiple privilege levels
Configure Cisco IOS role-based CLI access Implement Cisco IOS resilient configuration
Securing routing protocols
Implement routing update authentication on OSPF
Securing the control plane
Explain the function of control plane policing
Common Layer 2 attacks 4.4.a Describe STP attacks 4.4.b Describe ARP spoofing 4.4.c Describe MAC spoofing
Describe CAM table (MAC address table) overflows Describe CDP/LLDP reconnaissance
Describe VLAN hopping Describe DHCP spoofing
Mitigation procedures
Implement DHCP snooping
Implement Dynamic ARP Inspection Implement port security
Describe BPDU guard, root guard, loop guard Verify mitigation procedures
VLAN security
Describe the security implications of a PVLAN
Describe the security implications of a native VLAN

Cisco Firewall Technologies

Describe operational strengths and weaknesses of the different firewall technologies Proxy firewalls
Application firewall Personal firewall
Compare stateful vs. stateless firewalls Operations
Function of the state table
Implement NAT on Cisco ASA Static

Dynamic PAT
Policy NAT
Verify NAT operations
Implement zone-based firewall Zone to zone
Self-zone
Firewall features on the Cisco Adaptive Security Appliance (ASA) 9.x Configure ASA access management
Configure security access policies
Configure Cisco ASA interface security levels
Configure default Cisco Modular Policy Framework (MPF)
Describe modes of deployment (routed firewall, transparent firewall) Describe methods of implementing high availability
Describe security contexts Describe firewall services

IPS

Describe IPS deployment considerations Network-based IPS vs. host-based IPS
Modes of deployment (inline, promiscuous - SPAN, tap) Placement (positioning of the IPS within the network)
False positives, false negatives, true positives, true negatives
Describe IPS technologies Rules/signatures
Detection/signature engines
Trigger actions/responses (drop, reset, block, alert, monitor/log, shun) Blacklist (static and dynamic)

Content and Endpoint

Security
Describe mitigation technology for email-based threats
SPAM filtering, anti-malware filtering, DLP, blacklisting, email encryption
Describe mitigation technology for web-based threats Local and cloud-based web proxies
Blacklisting, URL filtering, malware scanning, URL categorization, web
Application filtering, TLS/SSL decryption
Describe mitigation technology for endpoint threats Anti-virus/anti-malware
Personal firewall/HIPS
Hardware/software encryption of local data

RAHITECH Trainer's Profile for CCNA Security Training in PUNE RAHITECH'S CCNA Security Trainers are:

 Are truly expert and fully up-to-date in the subjects they teach because they continue to spend time working on real-world industry applications.

CCNA SECURITY SYLLABUS

□ Have received awards and recognition from our partners and various recognized IT Organizations.
□ Are working professionals working in multinational companies.
□ Are certified Professionals with 7+ years of experience, Are Well connected with Hiring HRs in multinational companies.

Placement Assistance after CCNA Security Training in PUNE RAHITECH'S Placement Assistance

□ RAHITECH is the leader in offering placement to the students, as it has a dedicated placement wing which caters to the needs of the students during placements.
□ RAHITECH helps the students in the development of their RESUME as per current industry standards.
□ RAHITECH conducts Personality Development sessions including Spoken English, Group Discussions, Mock Interviews, Presentation skills to prepare students to face challenging interview situation with ease.
□ RAHITECH has prepared its students to get placed in top IT FIRMS like HCL, TCS, Infosys, Wipro, Syntel, Accenture and many more.

RAHITECH Course duration for CCNA Security Training in PUNE

Pre-requisite :- Any valid Cisco CCENT, CCNA Routing and Switching

Exam Code : - 210-260 IINS (Implementing Cisco IOS Network Security)

Global Exam Fee :-$325 (USA Dollar)

Certification Validity : - 3 Years

Training Duration : - Regular: 1 Month and 15 Days | 2 hrs. a Day

Weekend :- 6 Weekends | 4 hrs. Daily

Salary Offered :-CCNA Certified candidates are offered minimum 12000-18,000/- per month salary as per the company standards.