مشاوره، تحقیقات، طرح و اجرای شبکه های ارتباطی

و برگزارکننده دوره های آموزشی

CCNA Security

CCNA Security 210-260

مدت(ساعت): ۴۰ | **پیش نیاز:** CCNA R&S | **اعتبار دهنده:** CISCO

معرفی دوره :

CCNA Security 210-260 که IINS نیز نامیده می شود، تأییدی بر توان فرد در برقراری امنیت شبکه های مبتنی بر سیسکو می باشد. به منظور دستیابی به این مدرک، داوطلب باید دانش و مهارت لازم را به منظور ایمن ساختن زیرساخت شبکه و نیز شناسایی و مقابله با حملات و خطراتی که شبکه را تهدید می کنند، بدست آورد. مفاد این دوره بر شناخت مفاهیم امنیت، پیاده سازی، مدیریت، نگهداری و عیب یابی امنیت شبکه تأکید دارد.این مدرک تایید میکند شما دانش و مهارت لازم برای تامین امنیت شبکه های سیسکو را دارید. همچنین بیانگر این است که شما توانایی شناسایی انواع حملات و تهدید های شبکه را دارید می توانید از شبکه خود در مقابل آنها محافظت نمایید. استاندارد آموزشی این دوره شامل تکنولوژی های امنیتی ،نصب و عیب یابی و مانیتورینگ تجهیزات شبکه جهت اعمال availability Confidentiality Integrity, داده ها و تجهیزات شبکه می باشد، جهت دریافت این مدرک آزمون IINS 260-210 را باید گذراند.

امتیازات دوره :

- اعطای مدرک فارسی و انگلیسی با مجوز رسمی از :
  - سازمان مدیریت و برنامه ریزی کشور (معاونت توسعه مدیریت و سرمایه انسانی رئیس جمهوری سابق)
  - مجوز از اداره کل نظام مدیریت امنیت اطلاعات (نما)
  - شورای عالی انفورماتیک
  - قابلیت ترجمه وتایید قوه قضاییه وامور خارجه
- بهره گیری از لابراتوارسخت افزاری ونرم افزاری مجهز
- بهره گیری از اساتید مجرب و تأیید شده با سابقه حضور در پروژه‌های ملی

اهداف دوره :

- آشنایی با مفاهیم اولیه امنیت
- آشنایی با امنیت روتر های سیسکو
- اشنایی با سوییچ های سیسکو
- آشنایی با فایروال های سیسکو
- آشنایی با IPS های سیسکو

مخاطبان دوره :

- مدیران، کارشناسان، دانشجویان فعال در حوزه فناوری اطلاعات

تهران : خیابان ملاصدرا، بعد از خیابان شیخ بهائی ، ساختمان فردوس ، پلاک ۲۴۲ تلفن مستقیم آموزش: ۸۸۰۶۲۲۰۳،۸ فاکس :۸۸۰۶۵۲۲۲

مشاوره، تحقیقات، طرح و اجرای شبکه های ارتباطی

و برگزارکننده دوره های آموزشی

Course Outline :	محتوای دوره :
1.0 Security Concepts 1.1 Common security principles 1.1.a Describe confidentiality, integrity, availability (CIA) 1.1.b Describe SIEM technology 1.1.c Identify common security terms 1.1.d Identify common network security zones 1.2 Common security threats 1.2.a Identify common network attacks 1.2.b Describe social engineering 1.2.c Identify malware 1.2.d Classify the vectors of data loss/exfiltration 1.3 Cryptography concepts 1.3.a Describe key exchange 1.3.b Describe hash algorithm 1.3.c Compare and contrast symmetric and asymmetric encryption 1.3.d Describe digital signatures, certificates, and PKI 1.4 Describe network topologies 1.4.a Campus area network (CAN) 1.4.b Cloud, wide area network (WAN) 1.4.c Data center 1.4.d Small office/home office (SOHO) 1.4.e Network security for a virtual environment **2.0 Secure Access** 2.1 Secure management 2.1.a Compare in-band and out of band 2.1.b Configure secure network management 2.1.c Configure and verify secure access through SNMP v3 using an ACL 2.1.d Configure and verify security for NTP 2.1.e Use SCP for file transfer 2.2 AAA concepts 2.2.a Describe RADIUS and TACACS+ technologies 2.2.b Configure administrative access on a Cisco router using TACACS+ 2.2.c Verify connectivity on a Cisco router to a TACACS+ server 2.2.d Explain the integration of Active Directory with AAA 2.2.e Describe authentication and authorization using ACS and ISE 2.3 802.1X authentication	2.3.a Identify the functions 802.1X components 2.4 BYOD 2.4.a Describe the BYOD architecture framework 2.4.b Describe the function of mobile device management (MDM) **3.0 VPN** 3.1 VPN concepts 3.1.a Describe IPsec protocols and delivery modes (IKE, ESP, AH, tunnel mode, transport mode) 3.1.b Describe hairpinning, split tunneling, always-on, NAT traversal 3.2 Remote access VPN 3.2.a Implement basic clientless SSL VPN using ASDM 3.2.b Verify clientless connection 3.2.c Implement basic AnyConnect SSL VPN using ASDM 3.2.d Verify AnyConnect connection 3.2.e Identify endpoint posture assessment 3.3 Site-to-site VPN 3.3.a Implement an IPsec site-to-site VPN with pre-shared key authentication on Cisco routers and ASA firewalls 3.3.b Verify an IPsec site-to-site VPN **4.0 Secure Routing and Switching** 4.1 Security on Cisco routers 4.1.a Configure multiple privilege levels 4.1.b Configure Cisco IOS role-based CLI access 4.1.c Implement Cisco IOS resilient configuration 4.2 Securing routing protocols 4.2.a Implement routing update authentication on OSPF 4.3 Securing the control plane 4.3.a Explain the function of control plane policing 4.4 Common Layer 2 attacks 4.4.a Describe STP attacks 4.4.b Describe ARP spoofing 4.4.c Describe MAC spoofing 4.4.d Describe CAM table (MAC address table) overflows 4.4.e Describe CDP/LLDP reconnaissance 4.4.f Describe VLAN hopping

تهران : خیابان ملاصدرا، بعد از خیابان شیخ بهائی ، ساختمان فردوس ، پلاک ۲۴۲ تلفن مستقیم آموزش: ۸۸۰۶۲۲۰۳،۸ فاکس :۸۸۰۶۵۲۲۲

Course Outline :	محتوای دوره :
4.4.g Describe DHCP spoofing 4.5 Mitigation procedures 4.5.a Implement DHCP snooping 4.5.b Implement Dynamic ARP Inspection 4.5.c Implement port security 4.5.d Describe BPDU guard, root guard, loop guard 4.5.e Verify mitigation procedures 4.6 VLAN security 4.6.a Describe the security implications of a PVLAN 4.6.b Describe the security implications of a native VLA **5.0 Cisco Firewall Technologies** 5.1 Describe operational strengths and weaknesses of the different firewall technologies 5.1.a Proxy firewalls 5.1.b Application firewall 5.1.c Personal firewall 5.2 Compare stateful vs. stateless firewalls 5.2.a Operations 5.2.b Function of the state table 5.3 Implement NAT on Cisco ASA 9.x 5.3.a Static 5.3.b Dynamic 5.3.c PAT 5.3.d Policy NAT 5.3 e Verify NAT operations 5.4 Implement zone-based firewall 5.4.a Zone to zone 5.4.b Self zone 5.5 Firewall features on the Cisco Adaptive Security Appliance (ASA) 9.x 5.5.a Configure ASA access management 5.5.b Configure security access policies 2015 Cisco Systems, Inc. This document is Cisco Public. Page 4 5.5.c Configure Cisco ASA interface security levels 5.5.d Configure default Cisco Modular Policy Framework (MPF)	5.5.e Describe modes of deployment (routed firewall, transparent firewall) 5.5.f Describe methods of implementing high availability 5.5.g Describe security contexts 5.5.h Describe firewall services **6.0 IPS** 6.1 Describe IPS deployment considerations 6.1.a Network-based IPS vs. host-based IPS 6.1.b Modes of deployment (inline, promiscuous - SPAN, tap) 6.1.c Placement (positioning of the IPS within the network) 6.1.d False positives, false negatives, true positives, true negatives 6.2 Describe IPS technologies 6.2.a Rules/signatures 6.2.b Detection/signature engines 6.2.c Trigger actions/responses (drop, reset, block, alert, monitor/log, shun) 6.2.d Blacklist (static and dynamic) **7.0 Content and Endpoint Security** 7.1 Describe mitigation technology for email-based threats 7.1.a SPAM filtering, anti-malware filtering, DLP, blacklisting, email encryption 7.2 Describe mitigation technology for web-based threats 7.2.a Local and cloud-based web proxies 7.2.b Blacklisting, URL filtering, malware scanning, URL categorization, web application filtering, TLS/SSL decryption 7.3 Describe mitigation technology for endpoint threats 7.3.a Anti-virus/anti-malware 7.3.b Personal firewall/HIPS 7.3.c Hardware/software encryption of local data

Accredited by CARRIER DIGIT Computer Software LLC
EC-Council
تهران : خیابان ملاصدرا، بعد از خیابان شیخ بهائی ، ساختمان فردوس ، پلاک ۲۴۲ تلفن مستقیم آموزش: ۸۸۰۶۲۲۰۳،۸ فاکس :۸۸۰۶۵۲۲۲