خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ - ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

دوره جامع امنیت سیسکو از CCNA Security تا CCIE Security

شرح مختصر

دوره جامع امنیت سیسکو از CCNA Security تا CCIE Security

مروری بر دوره

مروری بر دوره

دوره Cisco Security Pack یک پکیج کامل در حوزه امنیت تجهیزات سیسکو می باشد. از آنجایی که امنیت برای هر سازمانی مهم و ضروری می باشد لذا افراد دارای مهارت های کافی در این حوزه با تقاضای قابل توجهی مواجه هستند. طراحی این دوره به گونه ای انجام شده است که دانشجو پس از آشنایی با مباحث اولیه امنیت در فصل های آغازین دوره CCNA Security، وارد دوره های CCNP Security شده و به صورت جامع و حرفه ای با مهارت های کار با فایروال های سیسکو و سنسور های سیسکو و ISE و ACS و .... بر طبق آخرین سیلابس سیسکو آشنا می شود. از مهمترین جذابیت های این دوره ارائه فیلم جلسات آموزشی به همراه جزوات فارسی به دانشجویان خواهد بود.

سرفصل ها (حضوری)

سرفصل ها

۲۱۰-۲۶۰ IINS

۱.۱ Common security principles

- ۱.۱.a Describe confidentiality, integrity, availability (CIA)
- ۱.۱.b Describe SIEM technology
- ۱.۱.c Identify common security terms
- ۱.۱.d Identify common network security zones

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

۱.۲ Common security threats

- ۱.۲.a Identify common network attacks
- ۱.۲.b Describe social engineering
- ۱.۲.c Identify malware
- ۱.۲.d Classify the vectors of data loss/exfiltration

۱.۳ Cryptography concepts

- ۱.۳.a Describe key exchange
- ۱.۳.b Describe hash algorithm
- ۱.۳.c Compare and contrast symmetric and asymmetric encryption
- ۱.۳.d Describe digital signatures, certificates, and PKI

۱.۴ Describe network topologies

- ۱.۴.a Campus area network (CAN)
- ۱.۴.b Cloud, wide area network (WAN)
- ۱.۴.c Data center
- ۱.۴.d Small office/home office (SOHO)
- ۱.۴.e Network security for a virtual environment

۳۰۰-۲۰۸ SISAS

۱.۱ Implement device administration

- ۱.۱.a Compare and select AAA options

خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

- ۱.۱.b TACACS+
- ۱.۱.c RADIUS
- ۱.۱.d Describe Native AD and LDAP

۱.۲ Describe identity management

- ۱.۲.a Describe features and functionality of authentication and authorization
- ۱.۲.b Describe identity store options (i.e., LDAP, AD, PKI, OTP, Smart Card, local)
- ۱.۲.c Implement accounting

۱.۳ Implement wired/wireless ۸۰۲.۱X

- ۱.۳.a Describe RADIUS flows
- ۱.۳.b AV pairs
- ۱.۳.c EAP types
- ۱.۳.d Describe supplicant, authenticator, and server
- ۱.۳.e Supplicant options
- ۱.۳.f ۸۰۲.۱X phasing (monitor mode, low impact, closed mode)
- ۱.۳.g AAA server
- ۱.۳.h Network access devices

۱.۴ Implement MAB

- ۱.۴.a Describe the MAB process within an ۸۰۲.۱X framework
- ۱.۴.b Flexible authentication configuration
- ۱.۴.c ISE authentication/authorization policies

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

- ۱.۴.d ISE endpoint identity configuration
- ۱.۴.e Verify MAB Operation

۱.۵ Implement network authorization enforcement

- ۱.۵.a dACL
- ۱.۵.b Dynamic VLAN assignment
- ۱.۵.c Describe SGA
- ۱.۵.d Named ACL
- ۱.۵.e CoA

۱.۶ Implement Central Web Authentication (CWA)

- ۱.۶.a Describe the function of CoA to support web authentication
- ۱.۶.b Configure authentication policy to facilitate CWA
- ۱.۶.c URL redirect policy
- ۱.۶.d Redirect ACL
- ۱.۶.e Customize web portal
- ۱.۶.f Verify central web authentication operation

۱.۷ Implement profiling

- ۱.۷.a Enable the profiling services
- ۱.۷.b Network probes
- ۱.۷.c IOS Device Sensor
- ۱.۷.d Feed service
- ۱.۷.e Profiling policy rules
- ۱.۷.f Utilize profile assignment in authorization policies

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

- ۱.۷.g Verify profiling operation

۱.۸ Implement guest services

- ۱.۸.a Managing sponsor accounts
- ۱.۸.b Sponsor portals
- ۱.۸.c Guest portals
- ۱.۸.d Guest Policies
- ۱.۸.e Self registration
- ۱.۸.f Guest activation
- ۱.۸.g Differentiated secure access
- ۱.۸.h Verify guest services operation

۱.۹ Implement posture services

- ۱.۹.a Describe the function of CoA to support posture services
- ۱.۹.b Agent options
- ۱.۹.c Client provisioning policy and redirect ACL
- ۱.۹.d Posture policy
- ۱.۹.e Quarantine/remediation
- ۱.۹.f Verify posture service operation

۱.۱۰ Implement BYOD access

- ۱.۱۰.a Describe elements of a BYOD policy
- ۱.۱۰.b Device registration
- ۱.۱۰.c My devices portal
- ۱.۱۰.d Describe supplicant provisioning

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

۲.۱ Describe TrustSec Architecture

- ۲.۱.a SGT Classification – dynamic/static
- ۲.۱.b SGT Transport – inline tagging and SXP
- ۲.۱.c SGT Enforcement – SGACL and SGFW
- ۲.۱.d MACsec

۳.۱ Troubleshoot identity management solutions

- ۳.۱.a Identify issues using authentication event details in Cisco ISE
- ۳.۱.b Troubleshoot using Cisco ISE diagnostic tools
- ۳.۱.c Troubleshoot endpoint issues
- ۳.۱.d Use debug commands to troubleshoot RADIUS and ۸۰۲.۱X on IOS switches and wireless controllers
- ۳.۱.e Troubleshoot backup operations

۴.۱ Design highly secure wireless solution with ISE

- ۴.۱.a Identity Management
- ۴.۱.b ۸۰۲.۱X
- ۴.۱.c MAB
- ۴.۱.d Network authorization enforcement
- ۴.۱.e CWA

خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

- ۴.۱.f Profiling
- ۴.۱.g Guest Services
- ۴.۱.h Posture Services
- ۴.۱.i BYOD Access

۵.۱ Device administration

۵.۲ Identity Management

۵.۳ Profiling

۵.۴ Guest Services

۵.۵ Posturing Services

۵.۶ BYOD Access

۳۰۰-۲۰۶ SENSS

۱.۱ Implement firewall (ASA or IOS depending on which supports the implementation)

- ۱.۱.a Implement ACLs
- ۱.۱.b Implement static/dynamic NAT/PAT
- ۱.۱.c Implement object groups
- ۱.۱.d Describe threat detection features

- ۱.۱.e Implement botnet traffic filtering
- ۱.۱.f Configure application filtering and protocol inspection
- ۱.۱.g Describe ASA security contexts

۱.۲ Implement Layer ۲ Security

- ۱.۲.a Configure DHCP snooping
- ۱.۲.b Describe dynamic ARP inspection
- ۱.۲.c Describe storm control
- ۱.۲.d Configure port security
- ۱.۲.e Describe common Layer ۲ threats and attacks and mitigation
- ۱.۲.f Describe MACSec
- ۱.۲.g Configure IP source verification

۱.۳ Configure device hardening per best practices

- ۱.۳.a Routers
- ۱.۳.b Switches
- ۱.۳.c Firewalls

۲.۱ Implement SSHv۲, HTTPS, and SNMPv۳ access on the network devices

۲.۲ Implement RBAC on the ASA/IOS using CLI and ASDM

۲.۳ Describe Cisco Prime Infrastructure

- ۲.۳.a Functions and use cases of Cisco Prime

خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

- ۲.۳.b Device Management

۲.۴ Describe Cisco Security Manager (CSM)

- ۲.۴.a Functions and use cases of CSM
- ۲.۴.b Device Management

۲.۵ Implement Device Managers

- ۲.۵.a Implement ASA firewall features using ASDM

۳.۱ Configure NetFlow exporter on Cisco Routers, Switches, and ASA

۳.۲ Implement SNMPv۳

- ۳.۲.a Create views, groups, users, authentication, and encryption

۳.۳ Implement logging on Cisco Routers, Switches, and ASA using Cisco best practices

۳.۴ Implement NTP with authentication on Cisco Routers, Switches, and ASA

۳.۵ Describe CDP, DNS, SCP, SFTP, and DHCP

- ۳.۵.a Describe security implications of using CDP on routers and switches
- ۳.۵.b Need for dnssec

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

۴.۱ Monitor firewall using analysis of packet tracer, packet capture, and syslog

- ۴.۱.a Analyze packet tracer on the firewall using CLI/ASDM
- ۴.۱.b Configure and analyze packet capture using CLI/ASDM
- ۴.۱.c Analyze syslog events generated from ASA

۵.۱ Design a Firewall Solution

- ۵.۱.a High-availability
- ۵.۱.b Basic concepts of security zoning
- ۵.۱.c Transparent & Routed Modes
- ۵.۱.d Security Contexts

۵.۲ Layer ۲ Security Solutions

- ۵.۲.a Implement defenses against MAC, ARP, VLAN hopping, STP, and DHCP rogue attacks
- ۵.۲.b Describe best practices for implementation
- ۵.۲.c Describe how PVLANs can be used to segregate network traffic at Layer ۲

۶.۱ Describe security operations management architectures

- ۶.۱.a Single device manager vs. multi-device manager

۶.۲ Describe Data Center security components and considerations

خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

- ۶.۲.a Virtualization and Cloud security

۶.۳ Describe Collaboration security components and considerations

- ۶.۳.a Basic ASA UC Inspection features

۶.۴ Describe common IPv۶ security considerations

- ۶.۴.a Unified IPv۶/IPv۴ ACL on the ASA

۳۰۰-۲۰۹ SIMOS

۱.۱ Site-to-site VPNs on routers and firewalls

- ۱.۱.a Describe GETVPN
- ۱.۱.b Implement IPsec (with IKEv۱ and IKEv۲ for both IPV۴ & IPV۶)
- ۱.۱.c Implement DMVPN (hub-Spoke and spoke-spoke on both IPV۴ & IPV۶)
- ۱.۱.d Implement FlexVPN (hub-Spoke on both IPV۴ & IPV۶) using local AAA

۱.۲ Implement remote access VPNs

- ۱.۲.a Implement AnyConnect IKEv۲ VPNs on ASA and routers
- ۱.۲.b Implement AnyConnect SSLVPN on ASA and routers
- ۱.۲.c Implement clientless SSLVPN on ASA and routers
- ۱.۲.d Implement FLEX VPN on routers

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

۲.۱ Troubleshoot VPN using ASDM & CLI

- ۲.۱.a Troubleshoot IPsec
- ۲.۱.b Troubleshoot DMVPN
- ۲.۱.c Troubleshoot FlexVPN
- ۲.۱.d Troubleshoot AnyConnect IKEv۲ and SSL VPNs on ASA and routers
- ۲.۱.e Troubleshoot clientless SSLVPN on ASA and routers

۳.۱ Design site-to-site VPN solutions

- ۳.۱.a Identify functional components of GETVPN, FlexVPN, DMVPN, and IPsec
- ۳.۱.b VPN technology considerations based on functional requirements
- ۳.۱.c High availability considerations
- ۳.۱.d Identify VPN technology based on configuration output

۳.۲ Design remote access VPN solutions

- ۳.۲.a Identify functional components of FlexVPN, IPsec, and Clientless SSL
- ۳.۲.b VPN technology considerations based on functional requirements
- ۳.۲.c High availability considerations
- ۳.۲.d Identify VPN technology based on configuration output
- ۳.۲.e Identify AnyConnect client requirements
- ۳.۲.f Clientless SSL browser and client considerations/requirements
- ۳.۲.g Identify split tunneling requirements

۳.۳ Describe encryption, hashing, and Next Generation Encryption (NGE)

خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

- ۳.۳.a Compare and contrast Symmetric and asymmetric key algorithms
- ۳.۳.b Identify and describe the cryptographic process in VPNs – Diffie-Hellman, IPsec – ESP, AH, IKEv۱, IKEv۲, hashing algorithms MD۵ and SHA, and authentication methods
- ۳.۳.c Describe PKI components and protection methods
- ۳.۳.d Describe Elliptic Curve Cryptography (ECC)
- ۳.۳.e Compare and contrast SSL, DTLS, and TLS

SITCS (۳۰۰-۲۱۰)

۱.۱ Cisco Cloud Web Security (CWS)

- ۱.۱.a Describe the features and functionality
- ۱.۱.b Implement the IOS and ASA connectors
- ۱.۱.c Implement the Cisco AnyConnect web security module
- ۱.۱.d Implement web usage control
- ۱.۱.e Implement AVC
- ۱.۱.f Implement antimalware
- ۱.۱.g Implement decryption policies

۱.۲ Cisco Web Security Appliance (WSA)

- ۱.۲.a Describe the features and functionality
- ۱.۲.b Implement data security
- ۱.۲.c Implement WSA identity and authentication, including transparent

user identification

- ۱.۲.d Implement web usage control
- ۱.۲.e Implement AVC
- ۱.۲.f Implement antimalware and AMP
- ۱.۲.g Implement decryption policies
- ۱.۲.h Implement traffic redirection and capture methods (explicit proxy vs. transparent proxy)

۱.۳ Cisco Email Security Appliance

- ۱.۳.a Describe the features and functionality
- ۱.۳.b Implement email encryption
- ۱.۳.c Implement antispam policies
- ۱.۳.d Implement virus outbreak filter
- ۱.۳.e Implement DLP policies
- ۱.۳.f Implement antimalware and AMP
- ۱.۳.g Implement inbound and outbound mail policies and authentication
- ۱.۳.h Implement traffic redirection and capture methods
- ۱.۳.i Implement ESA GUI for message tracking

۲.۱ Cisco Next-Generation Firewall (NGFW) Security Services

- ۲.۱.a Implement application awareness
- ۲.۱.b Implement access control policies (URL-filtering, reputation based, file filtering)
- ۲.۱.c Configure and verify traffic redirection

خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

- ۲.۱.d Implement Cisco AMP for Networks

۲.۲ Cisco Advanced Malware Protection (AMP)

- ۲.۲.a Describe cloud detection technologies
- ۲.۲.b Compare and contrast AMP architectures (public cloud, private cloud)
- ۲.۲.c Configure AMP endpoint deployments
- ۲.۲.d Describe analysis tools
- ۲.۲.e Describe incident response functionality
- ۲.۲.f Describe sandbox analysis
- ۲.۲.g Describe AMP integration

۳.۱ Configurations

۳.۲ Describe traffic redirection and capture methods

- ۳.۲.a Describe preprocessors and detection engines
- ۳.۲.b Implement event actions and suppression thresholds
- ۳.۲.c Implement correlation policies
- ۳.۲.d Describe SNORT rules
- ۳.۲.e Implement SSL decryption policies

۳.۳ Deployments

- ۳.۳.a Deploy inline or passive modes
- ۳.۳.b Deploy NGIPS as appliance, virtual appliance, or module within an ASA
- ۳.۳.c Describe the need for traffic symmetry

- ۳.۳.d Compare inline modes: inline interface pair and inline tap mode

۴.۱ Design a web security solution

- ۴.۱.a Compare and contrast Cisco FirePOWER NGFW, WSA, and CWS
- ۴.۱.b Compare and contrast physical WSA and virtual WSA
- ۴.۱.c Describe the available CWS connectors

۴.۲ Design an email security solution

- ۴.۲.a Compare and contrast physical ESA and virtual ESA
- ۴.۲.b Describe hybrid mode

۴.۳ Design Cisco FirePOWER solutions

- ۴.۳.a Configure the virtual routed, switched, and hybrid interfaces
- ۴.۳.b Configure the physical routed interfaces

۵.۱ Design a web security solution

- ۵.۱.a Compare and contrast FirePOWER NGFW, WSA, and CWS
- ۵.۱.b Compare and contrast physical WSA and virtual WSA
- ۵.۱.c Describe the available CWS connectors

۵.۲ Cisco Web Security Appliance (WSA)

خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

- ۵.۲.a Implement the WSA Policy Trace tool
- ۵.۲.b Describe WSA reporting functionality
- ۵.۲.c Troubleshoot using CLI tools

۵.۳ Cisco Email Security Appliance (ESA)

- ۵.۳.a Implement the ESA Policy Trace tool
- ۵.۳.b Describe ESA reporting functionality
- ۵.۳.c Troubleshoot using CLI tools

۵.۴ Cisco FirePOWER

- ۵.۴.a Describe the Cisco FirePOWER Management Center dashboards and reports
- ۵.۴.b Implement health policy
- ۵.۴.c Configure email, SNMP, and syslog alerts
- ۵.۴.d Troubleshoot NGIPS using CLI tools

CCIE Security v۵

- Perimeter Security and Intrusion Prevention
- Advanced Threat Protection and Content Security
- Secure Connectivity and Segmentation
- Identity Management , Information Exchange and Access
- Infrastructure Security, Virtualization and Automation
- Evolving Technologies

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

مخاطبان دوره

مخاطبان دوره

- افراد علاقه مند به کسب تجربه و کار در حوزه امنیت سیسکو

پیش نیاز ها

پیش نیازها

- دوره CCNA Routing & Switching