Carrier Digit
کاریار ارقام

مشاوره، تحقیقات، طرح و اجرای شبکه های ارتباطی

و برگزار کننده دوره های آموزشی

CCNA Security & CCNP Security

Pack CCNA Security & New CCNP Security Part II

مدت(ساعت): ۷۰ | **پیش نیاز:** CCNP Security Part I | **اعتبار دهنده:** CISCO

معرفی دوره :

در بخش دوم از امنیت سیسکو بعد از گذراندن فصول باقیمانده از CCNA Security دو دوره SIMOS و SITCS ارائه خواهد شد.

در گذشته مدرک CCNP Security بر اساس تجهیزات امنیتی مانند Firewall و IPS طراحی شده بود اما در ویرایش جدید آن شرکت سیسکو اقدام به طراحی این دوره به تفکیک تکنولوژی های امنیتی بکار رفته در بلاک های مختلف شبکه کرده است.

این دوره شامل چهار کتاب زیر است:

- **SENSS :** در این کتاب افراد با مفاهیم و تکنولوژی های بکار رفته در لبه شبکه شامل DHCP Snooping , Dynamic ARP Inspection و... آشنا خواهند شد. شرکت سیسکو توصیه به گذراندن دوره FIREWALL در حین گذراندن این کتاب کرده است که مطالب آن در این پک گنجانده شده است.
- **SISAS :** در این کتاب مفاهیم و تکنولوژی های بکار رفته در بلاک دسترسی شبکه شامل آشنایی با پروتکل 802.1x و با پیاده سازی قابلیت های Cisco ISE آشنا خواهند شد.
- **SIMOS :** در این کتاب مفاهیم و تکنولوژی Nهای VPN هم بر روی تجهیز ASA و هم بر روی Router های سیسکو را پوشش خواهد داد. این کتاب ترکیبی از دو کتاب SECURE و FIREWALL است.
- **SITCS :** در این کتاب افراد با فایروال های نسل بعدی سیسکو و سرویس های بکار رفته بر روی آن و تجهیز IPS آشنا خواهند شد همچنین با سامانه های امنیتی Cloud Web Security و WSA و ESA آشنا خواهند شد.

این دوره کاملا بر اساس سرفصل های ارائه شده توسط شرکت سیسکو طراحی شده است و به صورتی است که افراد پس از گذراندن این دوره توانایی شرکت در آزمون رسمی شرکت سیسکو را خواهند داشت.

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 تکنولوژی های VPN شامل Site to Site VPN و Remote Access
- آشنایی با طراحی تکنولوژی های مختلف VPN و پیاده سازی
- آشنایی و پیاده سازی فایروال های Next Generation
- آشنایی و پیاده سازی تجهیزات IPS
- آشنایی و پیاده سازی اولیه سامانه WSA
- آشنایی و پیاده سازی اولیه سامانه ESM

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

EC-Council

Course Outline :

محتوای دوره :

CCNA Security 210-260 Part II

Virtual Private Networks (VPN)
- Fundamentals of VPN Technology and Cryptography
- Fundamentals of IP Security
- Implementing IPsec Site-to-Site VPNs
- Implementing SSL VPNs Using Cisco ASA

Cisco Firewall Technologies and Intrusion Prevention Systems
- Understanding Firewall Fundamentals
- Implementing Cisco IOS Zone-Based Firewalls
- Configuring Basic Firewall Policies on Cisco ASA
- Cisco IDS/IPS Fundamentals

Content and Endpoint Security
- Mitigation Technologies for E-mail-Based and Web-Based Threats
- Mitigation Technologies for Endpoint Threats

CCNP Security Part II

• Implementing Cisco Secure Mobility Solutions (SIMOS 300-209)

Secure Communications
Site-to-site VPNs on routers and firewalls
- Describe GETVPN
- Implement IPsec
- mplement DMVPN
- Implement FlexVPN

Implement remote access VPNs
- Implement AnyConnect IKEv2 VPNs on ASA and routers
- Implement AnyConnect SSLVPN on ASA and routers
- Implement clientless SSLVPN on ASA and routers
- Implement FLEX VPN on routers

Troubleshooting, Monitoring, and Reporting Tools
Troubleshoot VPN using ASDM & CLI
- Troubleshoot IPsec
- Troubleshoot DMVPN
- Troubleshoot FlexVPN
- Troubleshoot AnyConnect IKEv2 and SSL VPNs on ASA and routers
- Troubleshoot clientless SSLVPN on ASA and routers

Secure Communications Architectures
Design site-to-site VPN solutions
- Identify functional components of GETVPN, FlexVPN, DMVPN, and IPsec
- High availability considerations
- Identify VPN technology based on configuration output

Design remote access VPN solutions
- Identify functional components of FlexVPN, IPsec, and Clientless SSL
- VPN technology considerations based on functional requirements
- High availability considerations
- Identify VPN technology based on configuration output
- Identify AnyConnect client requirements
- Clientless SSL browser and client considerations/ requirements
- Identify split tunneling requirements

Describe encryption, hashing, and Next Generation Encryption (NGE)
- Compare and contrast Symmetric and asymmetric key algorithms
- Identify and describe the cryptographic process in VPNs
- Describe PKI components and protection methods
- Describe Elliptic Curve Cryptography (ECC)
- Compare and contrast SSL, DTLS, and TLS

• Implementing Cisco Threat Control Solutions (CITCS 300-207)

Content Security
- Cisco ASA 5500-X NGFW Security Services
- Cisco Cloud Web Security
- Cisco WSA
- Cisco ESA

Threat Defense
- Network IPS
- Configure device hardening per best practices

Device GUIs and Secured CLI
- Content Security

Troubleshooting, Monitoring, and Reporting Tools
- Configure IME and IP logging for IPS
- Content Security
- Monitor Cisco Security IntelliShield

Threat Defense Architectures
- Design IPS solution

Content Security Architectures
- Design Web Security solution
- Design Email Security solution
- Design Application Security solution

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