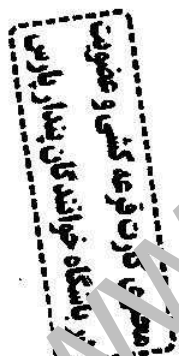


فیلم‌نگار آموزش عملی

CCNP Security (300-206)

آموزش گام به گام از روی فیلم‌های آموزشی Keith Barker

شرکت CBT Nuggets



تألیف: مهندس مهران تاجبخش

انتشارات پندار پارس

سرشناسه	: تاجبخش، مهران، ۱۳۴۷ -
عنوان و نام پدیدآور	: فیلم‌نگار آموزش عملی (300-206) CCNP Security: آموزش گام به گام از روی فیلم‌های آموزشی Keith Barker شرکت CBT Nuggets / تالیف مهران تاجبخش.
مشخصات نشر	: تهران: پندار پارس، ۱۳۹۶.
مشخصات ظاهری	: ۴۲۶ ص.: مصور. + لوح فشرده.
شابک	: 978-600-8201-27-4 : ۲۳۰۰۰۰ ریال: با لوح فشرده
وضعیت فهرست نویسی	: فیا.
موضوع	: شبکه‌های کامپیوتری -- تدابیر ایمنی -- آزمون‌ها -- راهنمای مطالعه
موضوع	: Computer networks -- Security measures -- Examinations -- Study guides
موضوع	: مهندسان مخابرات -- گواهی و گواهی‌نامه‌ها -- آزمون‌ها -- راهنمای مطالعه
موضوع	: Telecommunications engineers -- Certification -- Examinations -- Study guides
موضوع	: اکسترانته (شبکه‌های کامپیوتری)
موضوع	: Extranets (Computer networks)
رده بندی نکره	: ۱۳۹۶ فی ۹/۲/۵۹/۵۱۰۵ TK
رده بندی دیویی	: ۰۰۵/۸۰۷۶
شماره کتابشناسی ملی	: ۲۵۹ ۳۳

Telegram Channel: @PendarePars

انتشارات پندارپارس

دفتر فروش: انقلاب، ابتدای کارگر جنوبی، کوی شنج، شماره ۱۴، واحد ۱۶

تلفن: ۶۶۵۷۲۳۳۵ - تلفکس: ۶۶۹۲۶۵۷۸ همراهِ ۳۷۱۰ ۰۹۲۱

info@pendarepars.com

www.pendarepars.com

نام کتاب : فیلم‌نگار آموزش عملی (300-206) CCNP Security

ناشر : انتشارات پندار پارس

تألیف : مهران تاجبخش

چاپ نخست : بهمن ماه ۹۵

شمارگان : ۵۰۰ نسخه

طرح جلد : رامین شکرالهی

چاپ، صحافی : روز

شابک : ۹۷۸-۶۰۰-۸۲۰۱-۲۷-۴

قیمت : ۳۳۰۰۰ تومان به همراه DVD

* هرگونه کپی برداری، تکثیر و چاپ کاغذی یا الکترونیکی از این کتاب بدون اجازه ناشر تخلف بوده و پیگرد قانونی دارد *

پیش گفتار.....	۱
فصل ۱: مقابله با تهدیدها - ۲۵%	۵
درس ۱: کنترل لایه داده IPv4 با استفاده از فهرست کنترل دسترسی.....	۶
نام فیلم: Controlling the IPv4 Data-plane with ACL.....	۶
درس ۲: پیاده سازی فناوری PAT/ NAT.....	۱۵
نام فیلم: NAT and PAT.....	۱۵
درس ۳: فناوری فیلترینگ باتنت ها.....	۴۹
نام فیلم: Botnet Filtering.....	۴۹
درس ۴: فایروال های محتوا.....	۶۴
نام فیلم: Content-based Firewall.....	۶۴
درس ۵: فناوری های برابری امنیت سطح ۲ شبکه.....	۸۷
نام فیلم: VACLs, pACLs, and MACsec.....	۸۷
درس ۶: فناوری های کنترل آدرس مبدا.....	۹۳
نام فیلم:.....	۹۳
فصل ۲: رابط گرافیکی و مدیریت خط فرمان امن تجهیزات سیسکو - ۲۵%	۹۹
درس ۱: فهرست کنترل دسترسی در فایروال ASA.....	۱۰۰
نام فیلم: ASA ACLs.....	۱۰۰
درس ۲: ابزارهای محافظت لایه مدیریت مسیرباب.....	۱۱۲
نام فیلم: Tools to Protect Management-plane.....	۱۱۲
درس ۳: مدیریت فایروال ASA با استفاده از ASDM.....	۱۳۴
نام فیلم: (ASA Firewall).....	۱۳۴
درس ۴: مدیریت فایروال ASA با نرم افزار ASDM در شبیه ساز GNS3.....	۱۶۱
نام فیلم: ASA and ASDM working in GNS3.....	۱۶۱
فصل ۳: مدیریت سرویس ها در تجهیزات سیسکو - ۱۲%	۱۷۳

درس-۱: تأیید هویت پروتکل SSH با استفاده از فناوری RSA ۱۷۴

نام فیلم: RSA SSH Authentication ۱۷۴

درس-۲: پروتکل مدیریت شبکه SNMPv3 ۱۸۳

نام فیلم: SNMPv3 - CPr ۱۸۳

درس-۳: ابزار رصد و مانیتورینگ شبکه NetFlow ۱۹۷

نام فیلم: NetFlow ۱۹۷

درس-۴: فناوری AAA در فایروال ASA ۲۰۵

نام فیلم: AAA on the ASA ۲۰۵

درس-۵: موانع مسیریاب شبکه ۲۲۷

نام فیلم: Fortifying the Local Router ۲۲۷

فصل ۴: اشکالیابی، مانیتورینگ و ابزارهای تولید گزارش - ۱۰% ۲۳۷

درس-۱: اشکالیابی شبکه VPN مبتنی بر پروتکل SSL و با استفاده از نرم افزار AnyConnect ۲۳۸

نام فیلم: Troubleshooting Any connect Clients SSL VPNs ۲۳۸

درس-۲: اشکالیابی شبکه VPN مبتنی بر پروتکل SSL و مرورگر وب ۲۵۴

نام فیلم: Troubleshooting Clientless SSL VPNs ۲۵۴

فصل ۵: ساختارهای مقابله با تهدید - ۱۶% ۲۷۱

درس-۱: مروری بر فایروال منطقه ای ۲۷۲

نام فیلم: ZBF Firewall Review ۲۷۲

نام درس-۲: پیاده سازی فایروال منطقه ای ۲۸۴

نام فیلم: Zone Based Firewalls Implementation ۲۸۴

درس-۳: مبانی جست و جوی سرویس دهنده DHCP ۲۹۹

نام فیلم: DHCP Snooping Concepts ۲۹۹

نام درس-۴: پیاده سازی جست و جوی سرویس دهنده DHCP ۳۰۵

نام فیلم: DHCP Snooping Implementation ۳۰۵

درس-۵: مبانی تجسس پویای پروتکل ARP ۳۱۳

نام فیلم: DAI Concepts ۳۱۳

درس-۶: پیاده‌سازی تجسس پویای ARP ۳۱۷

نام فیلم: (DAI Implementation) ۳۱۷

درس-۷: فایروال (فعال / در حال انتظار/بازیابی خطا) ۳۳۴

نام فیلم: Firewall (Active / Standby / Failover) ۳۳۴

نام درس-۸: فایروال‌های مجازی پشتیبان ۳۵۲

نام فیلم: (Active-Active Failover) ۳۵۲

نام درس-۹: فایروال نامرئی ۳۷۷

نام فیلم: Transparent Firewall ۳۷۷

فصل ۶: اجزای امنیت و نکات مربوط به آن ۱۲% ۴۰۳

نام درس-۱۰: فناوری iACL ۴۰۴

نام فیلم: iACL ۴۰۴

نام درس-۲: فناوری URP ۴۰۹

نام فیلم: uRPF ۴۰۹

پیش گفتار

در طی سالیان گذشته تا به امروز همواره محصولات شرکت سیسکو در زمینه تجهیزات ساختاری شبکه (Routers / Switches) در صدر فروش قرار داشته و همواره بالاترین سهم بازار را به خود اختصاص داده‌اند.

کیفیت و قابلیت‌های موجود در تجهیزات سخت‌افزاری و نرم‌افزارهای مورد استفاده در این تجهیزات باعث شده است که از بالاترین سطح کارایی، اطمینان‌پذیری و کیفیت برخوردار باشند. آن‌چنانکه طبق آخرین گزارش منتشر شده توسط مؤسسه معتبر تحقیقاتی گارتنر در شش حوزه مورد بررسی فناوری‌های شبکه، محصولات و خدمات شرکت سیسکو توانسته‌اند رتبه نخست را در سال ۲۰۱۶ به خود اختصاص دهند. این موارد عبارتند از:

- Unified Communications
- Corporate Telephony
- Video Conferencing
- Web Conferencing
- Customer Care
- Communications for Midsize Enterprises

امروزه در اغلب شبکه‌های حساس و مهم از لحاظ کسب و کار، کارایی و همچنین امنیت و اطمینان‌پذیری استفاده از تجهیزات و فناوری‌های ارائه شده در حوزه شبکه، شرکت سیسکو در اولویت انتخاب قرار دارند. بدون تردید بخشی از این کارایی و قابلیت‌ها به فناوری‌های سخت‌افزاری و نرم‌افزاری در حوزه امنیت مربوط می‌باشند.

با توجه به اهمیت این موضوع، شرکت سیسکو به موازات توسعه راه‌های جدید در زمینه‌های سخت‌افزاری و نرم‌افزاری شبکه، اقدام به تدوین و ارائه دوره‌های آموزشی تخصصی مبنی بر شبکه در سه حوزه‌ی ساختار و تجهیزات و نقاط استفاده (CCNA Security) و ارتباط بین شبکه‌ای و شبکه‌های خصوصی مجازی و امنیت سیستم‌های همراه و مدیریت و برخورد با تهدیدها (CCNP Security) و ساماندهی امنیت در معماری و ساختار شبکه متوسط و بزرگ (CCIE Security) نموده است.

با توجه به اهمیتی که موضوع پیاده‌سازی امنیت در ساختارهای مختلف شبکه، به‌ویژه شبکه‌های بی‌سیم و همراه و همچنین ارتباط از راه دور و ارتباط بین شبکه‌ها و کنترل و مقابله با تهدیدها دارد، شرکت سیسکو دوره‌های بین‌المللی خود را که در یک گروه با عنوان CCNP Security ارائه می‌داد، در اواخر سال ۲۰۱۴ با توجه به گسترش فناوری‌ها و نیازهای روز افزون به آشنایی تخصصی‌تر و جزئی‌تر در موضوعات ذکر شده بالا، اقدام به به‌روزرسانی دوره‌های بین‌المللی خود در این حوزه کرد و هم‌اینک دوره بین‌المللی CCNP Security از چهار بخش به شرح زیر تشکیل شده است:

- 300-208 SISAS – Implementing Cisco Secure Access Solutions

(فناوری سیسکو برای دسترسی امن)

- 300-206 SENSS – Implementin Cisco Edge Netwrok Security Solutions
(فناوری های سیسکو برای ایجاد ارتباط امن بین شبکه با ایمن سازی تجهیزات مورد استفاده در این بخش، از جمله سوئیچ ها، مسیریاب ها، فایروال ها و ...)
- 300-209 SIMOS – Implementing Cisco Secure Mobility Solutions
(فناوری های سیسکو برای ایمن سازی شبکه های همراه و ارتباط های بی سیم)
- 300-210 SITCS – Implementing Cisco Threat Control Solutions
(فناوری های سیسکو برای کنترل و مقابله با تهدیدها، اعم از بدافزارها، ساختاری و منطقی و کاربران)

این کتاب مربوط به دوره آموزشی (SENSS) 300-206 شرکت سیسکو است که بر اساس فیلم های آموزشی ارائه شده توسط آقای کیت بارکر از شرکت CBT Nuggets تألیف و تدوین شده است. گفتنی است که این کتاب پس از (CCNA Security 11.4S2 0-200)، دومین تجربه تألیف محتوای آموزشی به صورت فیلم نگار است.

با توجه به اینکه این نوع ارائه آموزشی در قالب کتاب برای نخستین بار انجام شده است، قطعاً جا دارد تا در مجموعه های آینده بهبود یافته و نقاط ضعف آن تا حد امکان برطرف شود.

این کتاب در یک فاصله زمانی حدود یک ماه از کتاب نخست در این مجموعه (CCNA Security) ارائه می شود، میزان استقبال و همچنین نظرات ارسال شده در این فاصله زمانی کوتاه، من را بر آن داشت تا برای ارائه مجموعه هایی از این دست (فیلم نگار)، در موضوعات تخصصی دیگر همچون مجازی سازی VMware و همچنین پیاده سازی و ایمن سازی فضاهای پردازش ابری و راکر داده، برنامه ریزی های لازم را انجام دهم که امیدوارم در آینده نزدیک، اخبار مربوط به آنها را به آگاهی شما برسانم.

در نگارش این کتاب از ۲۹ فیلم آموزشی به مدت زمان بیش از ۱۰ ساعت استفاده شده است. برای استفاده بهینه تر و کارآمدتر از کتاب، آن را به همراه یک لوح فشرده حاوی آرایه وجود در کتاب با کیفیت خوب و فیلم های آموزشی اصلی به تفکیک فصل های کتاب عرضه کرده ایم.

با آزمون بین المللی CCNP Security (300-206 SENSS) بیشتر آشنا شوید

سرفصل و محتوای آموزشی و همچنین شرایط و قالب برگزاری آزمون بین المللی آن توسط شرکت سیسکو اعلام می گردد. این دوره آموزشی از دسامبر سال ۲۰۱۴ با کد جدید (CCNP Security – 300-206 SENSS) ارائه شد. آزمون بین المللی این دوره آموزشی از ۶۵ تا ۷۵ سؤال تشکیل شده است که مدت پاسخگویی به سوالات نیز ۹۰ دقیقه است. این آزمون در سطح بین المللی توسط موسسه Pearson VUE برگزار می شود.

محتوای موضوعی آزمون بین المللی CCNP Security (300-206 SENSS)

- مقابله با تهدید: ۲۵ درصد
- ابزارهای مدیریت سیسکو در خط فرمان و رابط کاربری گرافیکی: ۲۵ درصد
- مدیریت سرویس ها در تجهیزات سیسکو: ۱۲ درصد

- ابزارهای کنترل و نظارت و اشکال‌یابی و تهیه گزارش: ۱۹ درصد
- معماری‌های مقابله با تهدید: ۱۶ درصد
- اجزا و نکات مربوط به امنیت: ۱۲ درصد

چه مطالبی را در این کتاب خواهید آموخت

موضوعات ارائه شده در این کتاب بر محور امن‌سازی تجهیزات ارتباطی بین شبکه‌ها و دسترسی امن آنها با یکدیگر متمرکز شده است. در بخش نخست این کتاب با معماری و عملکرد انتقال ترافیک در لایه دوم و سوم شبکه و تهدیدهای موجود، و نیز روش‌های شناسایی و مقابله با آنها آشنا خواهید شد و در ادامه با ابزارهای مدیریتی در خط فرمان، و همچنین دارای رابط کاربری گرافیکی برای کنترل و نظارت و همچنین پیکربندی امنیت تجهیزات سیسکو آشنا می‌شوید و در بخش دیگری از این کتاب با سرویس‌های رمزنگار و کنترل و تأیید هویت در تجهیزات سیسکو برای برقراری ارتباط راه دور امن به منظور مدیریت و راهبری آنها آشنا خواهید شد و در ادامه، برار باد که برای نظارت و کنترل و شناسایی اشکال‌ها و تهیه گزارش از عملکردهای تجهیزات ارتباطی در شبکه مورد دارند، آشنا می‌شوید و سرانجام با ساختارهای مقابله با تهدید همچون ایجاد لایه میانی و استفاده از فایروال، سیستم تشخیص و مقابله با خرابی و فایروال‌های نامرئی و ... آشنا می‌شوید.

این کتاب برای چه کسانی است

موضوعات مورد بحث در این کتاب، به طوری که به طرز مشخص به ایمن‌سازی لایه‌های ارتباطی بین شبکه‌ای و تجهیزات مورد استفاده در آن می‌پردازد. بنابراین، این کتاب برای شبکه‌ازمان‌ها و مراکز داده می‌تواند از مطالب و فناوری‌هایی که در این فیلم نگار به آنها پرداخته شده است به منظور پیکربندی و مدیریت تجهیزات ارتباطی شبکه‌های مورد استفاده خود همچون سوئیچ‌ها و سیریاها و فایروال‌ها و همچنین سرورهای پروکسی و ابزارهای تشخیص و جلوگیری از نفوذ غیرمجاز (IDS/IPS) استفاده کنند.

در باره نویسنده

با بیش از ۲۶ سال سابقه تدریس در حوزه فناوری اطلاعات و شبکه در ... و ... است که به طور تخصصی در حوزه آموزش، مشاوره و اجرای پروژه‌های مربوط به امنیت شبکه و ... و ... و تست نفوذ و ادله الکترونیک و ارائه خدمات آموزش و مشاوره در حوزه پیاده‌سازی سیستم مدیریت امنیت اطلاعات (ISO27001) فعالیت داشته و دارای مدارک بین‌المللی فراوانی در حوزه شبکه، امنیت شبکه و تست نفوذ است که عبارتند از:

Network+, CCNA, CCNP, CCNA Security, CCNP Security, Security+, CIW security Professional, ISO27001 Lead Auditor.

برای برقراری ارتباط با نویسنده می‌توانید از طریق رایانامه زیر اقدام نمایید:

info@mehrantajbakhsh.com