

امنیت شبکه

گام اول

تام توماس

ترجمہ و تالیف: علی مختار پور



مقدمه مترجم

شرکت سیسکو سیستم (Cisco System) یکی از بزرگترین تولید کنندگان وسایل شبکه‌های کامپیوتری است؛ مدارک آموزشی این شرکت که از ارزش و اعتبار جهانی برخوردار هستند، به عنوان تایید صلاحیت تکنسین‌های آموزش دیده، برای کار و پیکربندی انواع شبکه‌های رایانه‌ای و ارتباطی ارائه می‌گردند.

ضرورت یادگیری و کاربرد تجهیزات شبکه، با توجه به رشد و گسترش این صنعت و کاربری آن در بین صنایع دیگر، به وجود آمد. در ایران آموزش مجموعه‌های CCNA و CCNP، برای متقاضیان یادگیری شبکه‌های کامپیوتری و ادوات آنها تدریس و آموزش داده می‌شود؛ که این مجموعه کتاب‌ها برای آماده سازی امتحانات و اخذ مدارک این شرکت تهیه و تدوین شده‌اند.

علاوه بر این مجموعه کتاب‌ها، به تازگی شرکت سیسکو اقدام به انتشار مجموعه کتاب‌هایی با عنوان "گام اول" (First Step) کرده است. این کتاب‌ها اصول و مبانی شبکه‌های کامپیوتری را به شیوه‌ای ساده و آسان بیان می‌کنند تا افراد علاقمند به یادگیری این رشته، با کمترین اطلاعات از دنیای کامپیوتر بتوانند با اصول شبکه و استانداردهای آن آشنا شده و آنها را به کار بندند. در این کتاب‌ها به روشی ساده اصول کار با شبکه‌های کامپیوتری، تجهیزات و وسایل آن، همراه با مثال‌هایی عامیانه تشریح و توضیح داده شده‌اند.

کتاب‌های گام اول، در هفت شاخه مختلف تالیف شده‌اند:

- امنیت شبکه (Network Security)
- صوت بر روی IP (Voice over IP)
- سوئیچینگ (Switching)
- شبکه‌های کامپیوتری (Computer Networking)
- مسیریابی (Routing)
- ارتباطات بدون سیم (Wireless)
- TCP/IP



در ترجمه این کتاب‌ها سعی شده است همزمان با به کارگیری معادل فارسی کلمات تخصصی، معادل انگلیسی کلمات نیز همواره در جلوی چشم خواننده قرار گیرند؛ تا علاوه بر درک بهتر متن، ذهن هم به صورت ناخودآگاه کلمات را بیاموزد. چون دانستن کلمات انگلیسی در اینترنت، پیکربندی تجهیزات و شبکه‌های کامپیوتری ضروری می‌باشد.

کتاب "امنیت شبکه؛ گام اول"، آخرین کتاب از مجموعه کتاب‌های گام اول می‌باشد که در اختیار علاقمندان و دانشجویان این رشته قرار می‌گیرد. پیش از این، کتاب‌های "مسیریابی؛ گام اول"، "شبکه‌های کامپیوتری؛ گام اول"، "سوئیچینگ LAN؛ گام اول"، "TCP/IP؛ گام اول"، "صوت بر روی IP؛ گام اول" و "شبکه‌های بی‌سیم؛ گام اول" به چاپ رسیده و در دسترس شما قرار گرفته‌اند. لازم به توضیح است که این سری از کتاب‌ها هیچ گونه توالی ندارند و هرکدام به تنهایی تمامی اطلاعات لازم برای درک صحیح مطالب را در خود داشته و به خواننده منتقل می‌کنند.

در اینجا لازم است تا از کلیه دوستان و عزیزانی که با همراهی و راهنمایی‌های موثر خود در انجام این کار مرا یاری و مساعدت کردند، سپاسگزاری کنم؛ به خصوص سرکار خانم یگانه عسگری که در صورت نبود ایشان، این مجموعه نیز به سرانجام نمی‌رسید. تمام موفقیت این مجموعه را نتیجه زحمات ایشان می‌دانم.

علی مختارپور

درباره نویسنده

تام توماس (Tom Thomas) می‌گوید او هرگز کار نمی‌کند، زیرا عاشق کاری است که انجام می‌دهد.

تام در سراسر سال‌هایی که در صنایع شبکه گذرانده است، به انسان‌های زیادی شبکه را آموخته است. او نویسنده و یا دستیار نویسنده ۱۷ کتاب در زمینه شبکه است. به غیر از نویسندگی، تام مهارت‌های کامپیوتر و شبکه را به عنوان یک آموزگار به افراد زیادی آموخته است.

تام گواهینامه Cisco Certified Internetwork Expert (CCIE No. 9360) (بالاترین مدرک شبکه) را دارد. او همچنین دارای گواهینامه‌های CCNP، CCDA و CCNA شرکت سیسکو است و آموزگار رسمی Cisco Systems می‌باشد. این گواهینامه‌ها مهارت او را در رهبری فنی شرکت‌ها و مشاغل در استفاده و کار درست با منابع IT خود، نشان می‌دهد.

تام موسس NetCerts.com (با آدرس فعلی CCPrep.com) است و در حال حاضر مالک اصلی و موسس Granite Systems, Inc. (www.GraniteSystems.net)، یک فراهم کننده IT برای مشاغل متوسط می‌باشد. در آنجا، او مسئول ساختار شرکت، اجراهای امنیت، و ساخت سرویس‌های محصولات جدید مثل ground-breaking IP Telephony Management System a.k.a. Bedrock است.

درباره مترجم

علی مختارپور دارای دانشنامه لیسانس دانشگاه صنعتی شریف می‌باشد. وی دارای یازده سال سابقه در امور شبکه‌های کامپیوتری و سابقه تدریس دروس شبکه در شاخه‌های Cisco/ CCNA-CCNP-CCSP-VoIP، Network Essentials و MCP-MCSE/ Microsoft است؛ و از سوابق شغلی ایشان می‌توان به مسئولیت فنی شبکه در سازمان مدیریت صنعتی، و مدیریت شبکه دفتر مطالعات سیاسی وزارت امور خارجه، و مدیریت بخش‌های VoIP، ISP و مسیریابی شرکت آریا رسانه تدبیر (شاتل) و ... اشاره کرد.

مطالعات تخصصی ایشان در زمینه شبکه و زیرشاخه‌های آن، بر روی پروتکل‌های مسیریابی، امنیت، VoIP و Wireless تجهیزات سیسکو متمرکز بوده است.



مطالب کتاب در یک نگاه

مقدمه iii

فصل ۱ اینجا هکر دارد! ۲

فصل ۲ سیاست‌ها و پاسخگویی‌های امنیتی ۵۰

فصل ۳ بررسی تکنولوژی‌های امنیت ۹۰

فصل ۴ پروتکل‌های امنیت ۱۳۴

فصل ۵ دیوارهای آتش ۱۶۶

فصل ۶ امنیت مسیریاب ۱۹۸

فصل ۷ شبکه‌های خصوصی مجازی IPSec ۲۴۲

فصل ۸ امنیت بی‌سیم ۲۸۸

فصل ۹ شناسایی تهاجم و ظرف‌های غسل ۳۳۲

فصل ۱۰ ابزارهای تجارت ۳۶۶

پیوست الف ۴۰۸

واژه‌نامه ۴۲۸

فهرست لغات ۴۵۰

فهرست

مقدمه iii

فصل ۱	اینجا هکر دارد! / ۲
	گام اول: جستجوی هدف / ۳
	هک کردن اطلاعات بی ضرر / ۵
	هدف‌های ناگهانی / ۸
	آیا شما یک هدف ناگهانی هستید؟ / ۱۰
	هدف برگزیده / ۱۱
	آیا شما یک هدف برگزیده هستید؟ / ۱۲
	مراحل یک حمله / ۱۴
	شناسایی و ردیابی (پوشش اتصال – Casing the Joint) / ۱۴
	وارسی / ۲۰
	تعیین شماره / ۲۴
	تعیین شماره ویندوز / ۲۵
	کسب دسترسی / ۲۸
	حملات سیستم عامل / ۲۹
	حملات برنامه کاربردی / ۳۰
	حملات پیکربندی غلط / ۳۰
	حمله کُد / ۳۱
	زیاد کردن امتیازات / ۳۳
	پوشاندن ردپاها / ۳۴
	حمله‌ها از کجا می‌آیند؟ / ۳۶
	شرکت‌های امنیت شبکه / ۳۷
	مرکز هماهنگی CERT / ۳۸
	SANS / ۳۹
	مرکز امنیت اینترنت (CIS) / ۳۹
	SCORE / ۳۹
	مرکز طوفان اینترنتی / ۴۰



۴۰ / ICAT Metabase

کانون امنیت / ۴۰

یادگیری از سازمان‌های امنیت شبکه / ۴۱

مروری بر حمله‌ها و استثماری‌های عمومی / ۴۱

خلاصه فصل / ۴۶

پرسش‌های دوره‌ای فصل / ۴۷

فصل ۲ سیاست‌ها و پاسخگویی‌های امنیتی / ۵۰

تعریف اعتماد / ۵۶

سیاست‌گذاری قابل قبول / ۵۹

بازبینی سیاست‌گذاری / ۶۰

هدف / ۶۰

چشم‌انداز / ۶۱

مالکیت و استفاده کلی / ۶۱

امنیت و مالکیت اطلاعات / ۶۲

استفاده غیر مجاز / ۶۵

فعالیت‌های شبکه و سیستم / ۶۵

فعالیت‌های ارتباطات و نامه الکترونیکی / ۶۷

اقدامات تنبیهی / ۶۸

نتیجه‌گیری / ۶۸

سیاست‌گذاری رمز عبور / ۶۹

بررسی اجمالی / ۶۹

هدف / ۷۰

چشم‌انداز / ۷۰

راهنمای ساخت رمز کلی / ۷۲

استانداردهای محافظت از رمز عبور / ۷۴

اقدامات تنبیهی / ۷۵

نتیجه‌گیری / ۷۵

سیاست امنیت VPN / ۷۶

هدف / ۷۷

چشم‌انداز / ۷۸

سیاست‌گذاری / ۷۸

نتیجه‌گیری / ۸۰

سیاست‌گذاری اتصال extranet / ۸۰

هدف / ۸۱

چشم انداز / ۸۲
بررسی امنیت / ۸۲
قرارداد اتصال شخص ثالث / ۸۲
مدرک شغلی / ۸۳
نقطه ارتباط / ۸۳
برقراری ارتباط / ۸۳
اصلاح یا تغییر اتصال و دسترسی / ۸۳
دسترسی پایان پذیر / ۸۳
نتیجه گیری / ۸۴
گواهی ISO و امنیت / ۸۵
سیاست گذاری‌های امنیتی نمونه در اینترنت / ۸۷
خلاصه فصل / ۸۸
پرسش‌های دوره‌ای فصل / ۸۹

فصل ۳	بررسی تکنولوژی‌های امنیت / ۹۰
	مفاهیم طراحی اولیه امنیت / ۹۱
	فیلتر کردن بسته‌ها از طریق فهرست‌های کنترل دسترسی / ۹۵
	مثال فهرست خرید / ۹۷
	محدودیت‌های فیلتر کردن بسته / ۱۰۲
	بازرسی کامل بسته / ۱۰۲
	بررسی جزئیات جریان بسته‌ها با استفاده از SPI / ۱۰۴
	محدودیت‌های بازرسی کامل بسته / ۱۰۶
	انتقال آدرس شبکه / ۱۰۶
	افزایش امنیت شبکه / ۱۱۰
	محدودیت‌های NAT / ۱۱۰
	حفاظت سطح برنامه کاربردی و Proxyها / ۱۱۲
	محدودیت‌های Proxy / ۱۱۵
	فیلترهای محتوا / ۱۱۶
	محدودیت‌های فیلتر کردن محتوا / ۱۲۰
	زیرساخت کلید عمومی / ۱۲۰
	محدودیت‌های PKI / ۱۲۲
	تکنولوژی‌های AAA / ۱۲۳
	تائید اعتبار / ۱۲۴
	مجوز / ۱۲۵
	حسابداری / ۱۲۶
	RADIUS / ۱۲۷



x

۱۲۹ / TACACS

مقایسه RADIUS و TACACS+ / ۱۳۱

خلاصه فصل / ۱۳۱

پرسش‌های دوره‌ای فصل / ۱۳۲

فصل ۴

پروتکل‌های امنیت / ۱۳۴

رمزنگاری DES / ۱۳۷

قدرت رمزنگاری / ۱۳۹

محدودیت‌های DES / ۱۴۰

رمزنگاری DES سه‌گانه / ۱۴۱

نقطه قوت رمزنگاری / ۱۴۲

محدودیت‌های 3DES / ۱۴۲

الگوریتم Message Digest 5 / ۱۴۳

MD5 Hash در عمل / ۱۴۵

PPTP / ۱۴۶

عملکرد PPTP / ۱۴۷

محدودیت‌های PPTP / ۱۴۸

L2TP / ۱۵۰

مقایسه L2TP و PPTP / ۱۵۱

مزایای L2TP / ۱۵۲

عملکرد L2TP / ۱۵۳

SSH / ۱۵۶

مقایسه SSH و Telnet / ۱۵۷

عملکرد SSH / ۱۶۰

تونل زنی و ارسال درگاه / ۱۶۱

محدودیت‌های SSH / ۱۶۳

خلاصه فصل / ۱۶۴

پرسش‌های دوره‌ای فصل / ۱۶۵

فصل ۵

دیوارهای آتش / ۱۶۶

سوالات متداول در مورد دیواره آتش / ۱۶۹

چه کسی به دیواره آتش نیاز دارد؟ / ۱۶۹

چرا به دیواره آتش احتیاج داریم؟ / ۱۶۹

آیا چیز ارزشمندی برای محافظت داریم؟ / ۱۷۰

- یک دیواره آتش چگونه عمل می‌کند؟ / ۱۷۱
- دیواره‌های آتش "سیاست‌گذاری امنیت" هستند / ۱۷۳
- خلاصه عملکرد دیواره آتش / ۱۷۶
- دیواره آتش در عمل / ۱۷۸
- نصب یک دیواره آتش /
- تعیین سیاست دسترسی به داخل / ۱۸۰
- تعیین سیاست دسترسی به خارج / ۱۸۲
- ملزومات اولیه: زندگی در DMZ / ۱۸۵
- بررسی‌های موردی / ۱۸۷
- بررسی موردی: DMZ. بودن یا نبودن؟ / ۱۸۷
- بررسی موردی: پیکربندی دیواره آتش با سرور پست الکترونیکی حفاظت شده (داخلی) / ۱۸۸
- بررسی موردی: پیکربندی دیواره آتش با سرور پست الکترونیکی در DMZ / ۱۹۱
- خلاصه فصل / ۱۹۵
- پرسش‌های دوره‌ای فصل / ۱۹۶

فصل ۶

امنیت مسیریاب / ۱۹۸

- مسیریاب Edge با نقش یک نقطه انسداد / ۲۰۳
- محدودیت‌های مسیریاب‌های نقطه انسداد / ۲۰۶
- مسیریاب Edge به عنوان یک بازرسی بسته / ۲۰۷
- مزایای FFS / ۲۰۹
- بازرسی بسته مبتنی بر محتوا / ۲۱۳
- شناسایی نفوذ با استفاده از Cisco IOS / ۲۱۹
- چه موقع باید از FFS IDS استفاده کنیم / ۲۲۱
- مرور عملکرد FFS IDS / ۲۲۱
- محدودیت‌های FFS / ۲۲۵
- الگوی IOS امن / ۲۲۶
- خلاصه فصل / ۲۴۰
- پرسش‌های دوره‌ای فصل / ۲۴۱

فصل ۷

شبکه‌های خصوصی مجازی IPSec / ۲۴۲

- مقایسه: VPN‌ها به شکلی امن با LAN‌ها ارتباط برقرار می‌کنند / ۲۴۶
- نمای کلی از VPN / ۲۴۸
- مزایا و اهداف VPN‌ها / ۲۵۱
- استراتژی‌های به کارگیری VPN / ۲۵۳



تونل‌زنی دوگانه / ۲۵۵
نمای کلی از VPN‌های IPSec / ۲۵۶
معتبر سازی و یکپارچگی داده / ۲۵۹
تونل‌زنی داده / ۲۶۰
حالت‌های رمزنگاری / ۲۶۲
حالت تونل / ۲۶۲
حالت حمل / ۲۶۳
پروتکل‌های IPSec / ۲۶۴
مشارکت‌های امنیتی / ۲۶۴
تبادل کلید اینترنت (IKE) / ۲۶۶
نمای کلی ISAKMP / ۲۶۸
بررسی عملکرد IPSec / ۲۶۸
IKE فاز یک / ۲۶۹
IKE فاز دو / ۲۷۰
الگوریتم Diffi-Hellman / ۲۷۱
تنظیم مسیریاب به عنوان یک عضو VPN / ۲۷۳
تنظیم ISAKMP / ۲۷۴
کلیدهای از پیش تقسیم شده / ۲۷۶
تنظیم دسته محافظتی ISAKMP / ۲۷۶
تنظیم کلید RSAKMP / ۲۷۷
تنظیم IPSec / ۲۷۸
گام 1: ایجاد ACL بسط یافته / ۲۷۸
گام 2: ایجاد انتقال IPSec / ۲۷۹
گام 3: ایجاد نقشه سری / ۲۸۰
گام 4: اعمال نقشه سری در یک رابط / ۲۸۲
تنظیم VPN دیواره آتش برای دسترسی کاربر / ۲۸۲
خلاصه فصل / ۲۸۶
پرسش‌های دوره‌ای فصل / ۲۸۶

فصل ۸

امنیت بی‌سیم / ۲۸۸
اولین ملزومات: LAN‌های بی‌سیم / ۲۹۱
Wi-Fi چیست؟ / ۲۹۳
بی‌سیم برابر با فرکانس رادیویی / ۲۹۴
شبکه بی‌سیم / ۲۹۵

حالت‌های عملکرد	۲۹۶
پوشش	۲۹۷
در دسترس بودن پهنای باند	۲۹۸
بازی‌های جنگی به شکل بی‌سیم	۲۹۹
نشانه‌گذاری جنگی	۳۰۰
رانندگی جنگی	۳۰۲
پرواز جنگی	۳۰۵
ارسال پیام جنگی	۳۰۵
جاسوسی جنگی	۳۰۶
تهدیدهای بی‌سیم	۳۰۷
ورود به استراق سمع	۳۰۸
حملات Denial of Service	۳۱۰
نقاط دسترسی غیر قانونی	۳۱۱
راهنمایی‌های به کارگیری AP غیرمجاز مهاجمان	۳۱۳
نقاط دسترسی درست تنظیم نشده	۳۱۴
استفاده نادرست از شبکه	۳۱۴
امنیت بی‌سیم	۳۱۵
شناسه‌گر مجموعه خدمات (SSID)	۳۱۵
مشارکت نقاط دسترسی و تجهیزات	۳۱۷
Wired Equivalent Privacy – WEP	۳۱۷
محدودیت‌ها و ضعف‌های WEP	۳۱۸
فیلتر کردن آدرس MAC	۳۱۹
Extensible Authentication Protocol (EAP)	۳۲۰
EAP-CD5	۳۲۱
(EAP-CISCO) LEAP	۳۲۱
EAP-TLS	۳۲۲
EAP-TTLS	۳۲۳
افزایش امنیت بی‌سیم	۳۲۳
ملزومات اولیه: ابزارهای نفوذ بی‌سیم	۳۲۵
برهم‌زننده‌های تعادل شبکه	۳۲۵
Packet Snifferهای بی‌سیم	۳۲۸
ردیابی در هوا	۳۲۹
خلاصه فصل	۳۳۰
پرسش‌های دوره‌ای فصل	۳۳۰



فصل ۹

- شناسایی تهاجم و طرف‌های عسل / ۳۳۲
- ملزومات اولیه: شناسایی حمله / ۳۳۶
- نگاهی بر عملکرد IDS / ۳۴۰
- سیستم شناسایی حملات شبکه‌ای (NIDS) / ۳۴۳
- سیستم شناسایی حمله مبتنی بر میزبان (HIDS) / ۳۴۵
- حملات چگونه شناسایی می‌شوند؟ / ۳۴۶
- بازسازی مجدد جریان ارتباطی / ۳۴۷
- تحلیل پروتکل / ۳۴۷
- شناسایی نامحسوس / ۳۴۷
- همخوانی الگو/ امضا / ۳۴۸
- تحلیل گزارش (Log) / ۳۴۹
- ترکیب روش‌ها / ۳۵۰
- جلوگیری از حمله / ۳۵۰
- عملکردها و پاسخ‌های IPS / ۳۵۱
- محصولات IDS / ۳۵۲
- ۳۵۳ / Snort
- محدودیت‌های IDS / ۳۵۶
- ملزومات اولیه: طرف‌های عسل / ۳۵۹
- سیاست‌های طراحی ظرف عسل / ۳۶۳
- محدودیت‌های ظرف عسل / ۳۶۳
- خلاصه فصل / ۳۶۴
- پرسش‌های دوره‌ای فصل / ۳۶۴

فصل ۱۰

- ابزارهای تجارت / ۳۶۶
- ملزومات اولیه: تحلیل آسیب پذیری / ۳۶۹
- حملات اصلی / ۳۷۰
- رهگیری IP / سرقت جلسه / ۳۷۰
- ابزارهای رهگیری IP / سرقت جلسه / ۳۷۱
- پیشگیری / ۳۷۲
- ۳۷۲ / Packet Sniffer
- حملات DOS (Denial of Service) / ۳۷۳
- حمله PING/ICMP / ۳۷۴
- حمله طغیان SYN (Flood SYN) / ۳۷۶
- جلوگیری از حمله‌های DoS / ۳۷۶
- حمله Man-in- the Middle / ۳۷۶

- ۳۷۶ / ARP Spoofing
- ۳۷۷ / Man in The Middle در حمله IP رهگیری نقش
- درهای پشتی (Back Doors) / ۳۷۷
- حملات متفرقه / ۳۷۸
- حملات زمینی (Land Attacks) / ۳۷۸
- حملات درخت کریسمس (Xmas Tree Attack) / ۳۷۹
- حمله قطره اشک (Teardrop Attack) / ۳۷۹
- حمله پینگ پنگ (Ping Pong Attack) / ۳۷۹
- ۳۸۰ / Ping of Death
- طغیان SYN (حمله نیمه باز) / ۳۸۰
- ۳۸۰ / Fire walking
- ارزیابی امنیت و آزمایش نفوذ پذیری / ۳۸۱
- ارزیابی نفوذ و آسیب پذیری داخلی / ۳۸۲
- روش ارزیابی / ۳۸۲
- ارزیابی نفوذ پذیری و آسیب پذیری خارجی / ۳۸۳
- روش ارزیابی / ۳۸۴
- ارزیابی امنیت فیزیکی / ۳۸۵
- روش ارزیابی / ۳۸۶
- ارزیابی‌های متفرقه / ۳۸۷
- ارائه دهندگان خدمات ارزیابی / ۳۸۸
- اسکنرهای آسیب پذیری / ۳۸۹
- ویژگی‌ها و مزایای اسکنرهای آسیب‌پذیری / ۳۸۹
- ۳۹۰ / Nessus
- دقت اسکن و شناسایی / ۳۹۱
- مستند سازی و پشتیبانی / ۳۹۱
- گزارش‌دهی / ۳۹۲
- به روز رسانی آسیب پذیری / ۳۹۳
- ۳۹۴ / Retina
- دقت اسکن و شناسایی / ۳۹۵
- مستند سازی و پشتیبانی / ۳۹۵
- گزارش‌دهی / ۳۹۶
- به روز رسانی آسیب پذیری / ۳۹۷
- محصولات آزمایش نفوذ / ۳۹۸
- دقت اسکن و شناسایی / ۳۹۹
- مستند سازی و پشتیبانی / ۴۰۰
- گزارش‌دهی / ۴۰۰



به روز رسانی آسیب پذیری / ۴۰۱

Core Impact در عمل / ۴۰۱

خلاصه فصل / ۴۰۶

پرسش‌های دوره‌ای فصل / ۴۰۷

پیوست الف / ۴۰۸

واژه‌نامه / ۴۲۸

فهرست لغات / ۴۵۰

مقدمه

این کتاب به منظور بیان ملزومات افزایش درک امنیت شبکه نوشته شده است. متون زیادی در رابطه با این موضوع وجود دارد، و با ارزش هستند. افراد و شرکت‌های زیادی در حال حاضر قصد دارند که امنیت شبکه خود را افزایش دهند. از کجا شروع می‌کنید؟ شاید می‌خواهید شبکه بی‌سیم (wireless) بسازید و لازم است که از امن بودن آن خاطر جمع باشید. چه منبع واحدی می‌تواند امنیت لازم را در شبکه شما ایجاد کند؟ این کتاب اطلاعات کافی را در مورد امنیت در اختیارتان قرار می‌دهد تا بتوانید طبق صلاحدید خود، امنیت را برای شرکت‌تان پیاده سازی کنید.

نقطه نظر من این است که همه خوانندگان به امنیت احتیاج دارند، اما واقعا درک درستی از خطرات، تکنیک‌ها، و امکانات موجود ندارند. بنابراین، در هر فصل یک جنبه از مدل کلی امنیت لایه‌ای را تشریح خواهیم کرد و این امکان را به شما می‌دهیم که ببینید و بدانید که چرا امنیت برای هر فضایی لازم است، باید به چه چیزهایی توجه کنید، و چگونه باید اقدام کنید.

هدف‌ها و روش‌ها

هدف از این کتاب فراهم کردن یک مرجع برای هرکسی است که نگران امنیت می‌باشد. برای استفاده از این کتاب نیازی نیست که خوانندگان، متخصص شبکه یا CIO باشند. این آرزوی من است که همه خوانندگان، از دانش‌آموزان تا متخصصین، از این کتاب استفاده ببرند.

روش من این است که هریک از اجزاء شبکه را در نظر گرفته و چگونگی اجرای امن آن را بررسی می‌کنم. وقتی با تکنولوژی‌ها یا راهکارهای امنیت مواجه می‌شویم، با مثال‌های واقعی و مقایسه‌های عملی شرح داده می‌شوند. این کتاب عناوین مهم را پوشش می‌دهد، اما باید مفرح باشد و خواندن آن نیز ساده باشد. من تلاش کرده‌ام که به این هدف دست یابم.

چه کسی باید این کتاب را بخواند

این کتاب با فرض داشتن مخاطبان زیاد نوشته شده است. تعداد دانش‌آموزانی را تصور کنید که درباره اهمیت امنیت شبکه شنیده‌اند و تصور کنید که همه آنها بر روی این موضوع متمرکز شوند. این کتاب به آنها در درک همه مفاهیم اصلی امن ساختن شبکه کمک می‌کند. شاید شما یک متخصص شبکه با تخصصی ژرف در مسیریابی و سوئیچینگ هستید، و حالا از شما خواسته شده است که یک



شبکه بی‌سیم (امن) را پیاده‌سازی کنید. این کتاب اطلاعاتی بنیادین در مورد امنیت در اختیار شما می‌گذارد، تا نیازهای خود را برای رسیدن به هدف خود پیدا کنید. حتی ممکن است شما یک CIO باشید، کسی که از او خواسته شده تا نیازهای امنیتی شبکه را تشخیص دهد.

System (IDS): شاید لازم است بدانید که چرا لازم هستند، چگونه کار می‌کنند، و کی/کجا باید استفاده شوند.

صرفنظر از تخصص شما و یا نقش‌تان در صنعت IT، این کتاب برای شما مفید خواهد بود؛ برای فهم بهتر، مفاهیم را ساده‌تر کرده و به شما تصویری از مفهوم امنیت می‌دهد. اینکه از این اطلاعات چه استفاده‌ای می‌کنید، به خودتان بستگی دارد. این کتاب ممکن است به شما چیزی را که لازم دارید بدهد، یا ممکن است اولین گام در راه رشد شما باشد.

این کتاب چگونه سازمان‌دهی شده است

با اینکه می‌توانید این کتاب را از ابتدا تا انتها به صورت مرتب بخوانید، اما این کتاب قابل انعطاف طراحی شده و به شما امکان می‌دهد که به سادگی بتوانید بین فصل‌ها و بخش‌ها حرکت کرده تا مواردی را که به آنها نیاز دارید، بخوانید. اگر قصد دارید همه کتاب را بخوانید، به شما توصیه می‌کنم که آن را به ترتیب بخوانید.

فصلهای ۱ تا ۱۰، سرفصل‌های زیر را پوشش می‌دهند:

- **فصل ۱ "اینجا هکر دارد!":** در این فصل نگاه اجمالی به تفکر و انگیزه‌های افراد ماهری که قصد حمله به سیستم شما را دارند خواهیم داشت. این فصل ابزارها، تکنیک‌ها، و حمله‌ها را پوشش می‌دهد.
- **فصل ۲ "سیاست‌ها و پاسخگویی‌های امنیتی":** این فصل با مفهوم محافظت لایه‌ای، با ساختار امن ساختن شبکه آغاز می‌شود؛ سیاست‌گذاری امنیتی در این فصل بررسی می‌-

گردد. هنگامی که این فصل را به پایان می‌رسانید، نقشی را که سیاست‌گذاری ایفا می‌کند و یکی از راه‌های نوشتن آن را خواهید آموخت.

- **فصل ۳ "بررسی تکنولوژی‌های امنیت":** این فصل به بررسی نکات اصلی استفاده از تکنولوژی‌های امنیت، از ابتدایی‌ترین فهرست‌های کنترل دسترسی موجود در هر مسیر یاب گرفته تا برنامه‌های کلی، مثل PKI می‌پردازد. بسیاری از این تکنولوژی‌ها امروزه بدون اینکه شما بدانید، مورد استفاده قرار می‌گیرند. بعد از خواندن این فصل مزایای این تکنولوژی‌ها، کجا استفاده می‌شوند، و ریسک‌های مربوط به آنها را خواهید شناخت.
- **فصل ۴ "پروتکل‌های امنیت":** این فصل نگاهی دارد به پروتکل‌های امنیت و رمزنگاری، که برای امن ساختن شبکه استفاده می‌شوند. به علاوه، محدودیت‌های هر پروتکل امنیت نیز شرح داده می‌شود، زیرا هیچ چیز کامل نیست.
- **فصل ۵ "دیواره آتش":** این فصل، دیواره‌های آتش و عملکرد آنها را توضیح می‌دهد. این فصل بررسی می‌کند که چه کسی به دیواره آتش نیاز دارد و چرا دیواره آتش جزء ضروری محافظت از شبکه شماست.
- **فصل ۶ "امنیت مسیریاب":** اگر یک شبکه دارید، یک مسیریاب نیز دارید؛ آنها در طول سال‌ها رشد کرده‌اند و حالا دارای این قابلیت هستند که ابزارهای امنیتی موثری باشند. این فصل توانایی‌های گسترده مسیریاب‌ها را شرح خواهد داد.
- **فصل ۷ "شبکه‌های خصوصی مجازی IPSec":** این فصل نقش VPN‌ها را شرح می‌دهد و بیان می‌کند که آنها اینترنت عمومی را تغییر می‌دهند، و همه اطلاعات اینترنت را رمزنگاری می‌کنند. این شامل مشخصات عملی و پارامترهای موثر می‌شود.
- **فصل ۸ "امنیت بی‌سیم":** این فصل داغترین تکنولوژی، بی‌سیم، را شرح داده و توضیح می‌دهد که در این دنیای IT خوب نیستند. هرکس اینجا نیز می‌آیند، و تجهیزات کاملی را همراه خود خواهند آورد. بسیاری از مردم فکر می‌کنند که شبکه بی‌سیم امن و راحت است؛ این فصل بیان می‌کند که این افراد دچار مشکل امنیتی خواهند شد.
- **فصل ۹ "شناسایی تهاجم و ظرف‌های عسل":** در این فصل خواهیم گفت که چگونه تلاش‌های هکر برای دسترسی به شبکه خود را توسط IDS تشخیص دهید. به علاوه، یکی



از راه‌های گنج کردن هکر با استفاده از honeypot را خواهیم گفت، و خواننده نقش هر ابزار را خواهد دانست.

- فصل ۱۰ "ابزارهای تجارت": در این فصل ابزارهای امنیت استفاده شده توسط هکرها را معرفی می‌کنیم تا خوانندگان بدانند که با چه چیزهایی روبرو هستند. سپس در این فصل ابزارهای موجود برای تشخیص ضعف شبکه و بازرسی آناتومی امنیت را معرفی می‌کنیم، تا به وسیله آنها اطمینان حاصل کنید که شبکه شما امن است.

شکل‌های استفاده شده در این کتاب

