# امنیت شبکه

# گام اول

تام توماس

ترجمه و تالیف: علی مختارپور

## 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 شیوه‌ایی 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"، "شبکه‌های‌کامپیوتری؛ 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 Essentionals و Microsoft/ MCP-MCSE 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 ISP، VoIP 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

# فهرست

## 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 خاطرجمع 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 تصوری 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 به‌سادگی 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 مسیریاب 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. هکرها 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 گیج کردن هکر با استفاده از honeypot را خـواهیم گفـت، و خواننـده نقـش هـر ابزار را خواهد دانست.

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

## شکل‌های استفاده شده در این کتاب