فهرست

پیشگفتار

با توسعهٔ فناوری اطلاعات و پیاده‌سازی سیستم‌های اطلاعاتی در سراسر دنیا، تأمین امنیت آن بهعنوان دغدغه‌ای مهم در مجامع علمی، دولتی و خصوصی مطرح شده است. از آنجا که شبکه به‌عنوان بستری اساسی برای انتقال اطلاعات به حالتی فراگیر نزدیک می‌شود، حفظ امنیت در انتقال اطلاعات و عدم نفوذپذیری از طریق شبکه، به‌عنوان حالت خاصی از امنیت اطلاعات، نیاز به بررسی بسیار دارد و البته کارهای ارزشمندی هم در این زمینه انجام گرفته و محصولات مختلفی ارائه شده است. آشنایی مدیران سازمان‌ها، مراکز دولتی، نظامی، تجاری و هر جایی که امنیت اطلاعات برای آنها مطرح است، با مبانی امنیت شبکه، مخاطرات امنیتی، راه‌حل‌ها و نحوهٔ سیاست‌گذاری صحیح برای این موضوع، امری اجتناب ناپذیر محسوب می‌شود. اگر همچنین مدیران شبکه، به مسایل امنیتی شبکهٔ خود آگاه نباشند، ممکن است به صورت‌های مختلفی مورد حملهٔ افراد نفوذگر قرار گیرند.

این کتاب سعی دارد با ارائهٔ مفاهیم بنیادی امنیت شبکه، مدیران سطح بالا را با مسایل مطرح در امنیت شبکه آشنا سازد تا بدین‌وسیله قادر به وضع سیاست‌های خاص برای حفظ امنیت اطلاعات و به‌طور خاص امنیت شبکه، شناسایی افراد خاطی و برخورد با آنها باشند. همچنین، در سطحی پیش‌رفته‌تر و البته نه صرفاً تکنیکی،

مسؤولین شبکه‌های شرکت‌ها و سازمان‌ها را با امنیت شبکه و تجهیزات آن، مخاطرات امنیتی، راه‌حل‌ها و سایر مسائل مربوط به امنیت یک شبکه در مقابله با نفوذگران داخلی و خارجی آشنا می‌گرداند. گفتنی است که مطالعهٔ کامل این کتاب نیاز به آشنایی با مفاهیم شبکه و دانستن اطلاعات پایه‌ای در زمینه امنیت شبکه دارد.

در این کتاب، منظور از "شبکهٔ داخلی"، شبکهٔ (محلی) مورد اعتماد ماست که در مقابل عبارت "شبکهٔ خارجی" که قابل اعتماد نیست به‌کار می‌رود.

فصل اول این کتاب، به معرفی مسایل عمومی امنیت شبکه، شامل وضع سیاست امنیتی، حملات شبکه‌ای و آشنایی مختصری با شبکه‌های بی‌سیم و امنیت آن (از آن جهت که جامعیت این مستند، حفظ شود) می‌پردازد. در فصل دوم، معرفی مسیریاب، مخاطرات امنیتی و مسائل مربوط به بالا بردن سطح امنیتی مسیریاب و با استفاده از آن، بهبود امنیت شبکه داخلی خود (با تأکید بر مسیریاب‌های سیسکو) در رأس مطالب قرار دارد. فصل سوم، بحثی کلی و جامع در مورد دروازه‌های امنیتی و دیوار آتش، انواع آن، معماری‌ها، سرویس‌های پیش‌رفتهٔ امنیتی ارائه شده در دیوار آتش و معرفی چند محصول را در این زمینه شامل می‌شود. در نهایت در فصل چهارم، سیستم‌های شناسایی نفوذ و نفوذگر موسوم به IDS[1] را مورد بحث قرار خواهیم داد که معرفی نفوذ ونفوذگر، سیستم‌های شناسایی نفوذ، انواع آن، سیستم‌های فریب و به دام انداختن نفوذگر و معرفی چندین محصول موجود در بازار امروز دنیا در این زمینه، رئوس مطالب را تشکیل می‌دهد.

---

[1]. Intrusion Detection System