امنیت شبکه‌های کامپیوتری و داده کاوی

تالیف:
یگانه حسن‌زاده کان‌اسماعیل‌کهریز
مریم طاهرلو

انتشارات خط آخر
۱۴۰۰

سرشناسه	:	حسن‌زاده کان اسماعیل کهریز، یگانه، ۱۳۷۲-
عنوان و نام پدیدآور	:	امنیت شبکه‌های کامپیوتری و داده‌کاوی/ تالیف یگانه حسن‌زاده‌کان‌اسماعیل‌کهریز، مریم طاهرلو.
مشخصات نشر	:	تهران: خط آخر، ۱۴۰۰.
مشخصات ظاهری	:	۱۱۸ ص.: مصور (رنگی).
شابک	:	۹۷۸-۶۲۲-۹۸۳۰۴-۴-۴
وضعیت فهرست نویسی	:	فیپا
یادداشت	:	کتابنامه: ص. ۱۱۵.
موضوع	:	شبکه‌های کامپیوتری -- تدابیر ایمنی
موضوع	:	Computer networks -- Security measures
موضوع	:	کامپیوترها -- ایمنی اطلاعات
موضوع	:	Computer security
موضوع	:	داده‌کاوی -- تدابیر ایمنی
موضوع	:	Data mining -- Security measures
موضوع	:	حفاظت داده‌ها
موضوع	:	Data protection
شناسه افزوده	:	طاهرلو، مریم، ۱۳۷۲-
رده بندی کنگره	:	TK۵۱۰۵/۵۹
رده بندی دیویی	:	۰۰۵/۸
شماره کتابشناسی ملی	:	۸۶۳۴۱۱۱
اطلاعات رکورد کتابشناسی	:	فیپا

انتشارات خط آخر

تهران - میدان انقلاب اسلامی

شماره تماس: ۰۹۰۱۰۳۵۶۱۰۵

وب سایت: www. ketab30.ir

ایمیل: khate.akhar.book@gmail.com

انتشارات خط آخر

نام کتاب	امنیت شبکه‌های کامپیوتری و داده کاوی
مولف	یگانه حسن‌زاده کان‌اسماعیل‌کهریز، مریم طاهرلو
ناشر	خط آخر
صفحه آرایی	رضا کاوه
طراح جلد	رضا کاوه
نوبت چاپ	اول، ۱۴۰۰
تیراژ	۱۰۰۰ نسخه
قیمت	۳۵۰۰۰ تومان

ISBN: 978-622-98304-4-4

فهرست مطالب

پیشگفتار

لازمه‌های امنیت اطلاعات در درون یک سازمان، در طی دهه‌های اخیر دو تغییر عمده یافته است. قبل از استفاده گسترده از تجهیزات پردازش داده‌ها، امنیت اطلاعاتی که ازنظر یک سازمان ارزشمند تلقی می‌شد عمدتاً از طریق روش‌های فیزیکی و مدیریتی فراهم می‌گردید. با ورود رایانه، نیاز به لوازم خودکاربرای حفاظت از پَرونَجاها و سایر اطلاعات ذخیره‌شده در رایانه آشکار گردید. این موضوع علی‌الخصوص در مورد یک سیستم به اشتراک گذاشته‌شده همانند یک سیستم اشتراک زمانی جدی‌تر بوده و حتی در مورد سیستم‌هایی که از طریق شبکه تلفنی، شبکه داده، و یا اینترنت قابل‌دستیابی هستند حیاتی‌تر است. نام کلی مجموعه لوازمی که برای حفاظت داده‌ها و خنثی کردن نیات بداندیشان طراحی‌شده است، امنیت رایانه است. تغییر عمده دیگر که امنیت را تحت تأثیر قرار داده است، ورود سیستم‌های توزیع‌شده و استفاده از تسهیلات شبکه‌ای و ارتباطی برای حمل داده‌ها بین پایانه و رایانه، و بین رایانه و رایانه است. معیارهای امنیت شبکه برای حفاظت از داده‌ها در هنگام انتقال آن‌ها ضروری است. درواقع اصطلاح امنیت شبکه تا حدودی گمراه‌کننده است زیرا تمام مشاغل، دولت و سازمان‌های آموزشی، تجهیزات پردازش دیتای خود را با مجموعه‌ای از

شبکه‌های متعامل به هم وصل کرده‌اند. چنین مجموعه‌ای را اغلب اینترنت نامند و در رابطه با آن، اصطلاح امنیت اینترنت و یا امنیت بین شبکه‌ای بکار می‌رود.

در این عصر اتصال الکترونیکی جهان، عصر ویروس‌ها و هَکرها، عصر استراق سمع الکترونیک و عصر فریب الکترونیک، واقعاً زمانی قابل‌تصور نیست که در آن امنیت مطرح نباشد. یک، رشد انفجارآمیز سیستم‌های کامپیوتری و اتصال آن‌ها از طریق شبکه‌ها، وابستگی هم سازمان‌ها و هم افراد به اطلاعات ذخیره‌شده و مبادله شده با استفاده از این سیستم‌ها را افزایش داده است. این امر به‌نوبه‌ی خود هوشیاری کاربران نسبت به لزوم محافظت داده و منابع اطلاعاتی از افشا، تضمین موثق بودن داده‌ها و پیام‌ها، و محافظت سیستم‌ها از حملات مبتنی بر شبکه را ارتقاء بخشیده است. دو، مقوله‌های مرتبط با رمزنگاری و امنیت شبکه کمال بیشتری یافته و منجر به ایجاد کاربردهای عملی‌تر و آماده‌تری برای اعمال امنیت شبکه شده‌اند.

ازآنجایی‌که ازنظر تکنیکی ایجاد سیستم‌های کامپیوتری بدون نقاط ضعف و شکست امنیتی عملاً غیرممکن است. تشخیص نفوذ در سیستم‌های کامپیوتری بااهمیت خاصی دنبال می‌شود. روش‌های جدید در حملات به سیستم‌های کامپیوتری توجه محققین را به خود جلب نموده است. سیستم تشخیص نفوذ تلاشی است در جهت کشف حمله‌کننده و یافتن روش‌هایی که این‌گونه افراد در جهت نفوذ به اطلاعات کامپیوتری بکار می‌گیرند.

ازنظر کلی این مورد بسیار اهمیت دارد که در برابر چنین حملات و تهاجماتی ایستادگی نمود. ولیکن بدون طراحی بنیادین یک راه‌حل مبتنی بر این سیستم جهت جستجوی حملات امکان‌پذیر نیست. هدف سیستم‌های تشخیص نفوذ، کشف و احتمالاً شناسایی حملات و تشخیص مشکلات امنیتی در سیستم یا شبکه کامپیوتری است. سیستم‌های تشخیص نفوذ به همراه دیوارهای آتش مکمل هم عمل می‌کنند.