

آشنایی با مبانی امنیت شبکه



مؤلفین:

مهندس اشکان قنبری

باشگاه پژوهشگران جوان و نخبگان، واحد تهران شمال، دانشگاه آزاد اسلامی، تهران، ایران

مهندس مهران نیکو

باشگاه پژوهشگران جوان و نخبگان، واحد تهران شمال، دانشگاه آزاد اسلامی، تهران، ایران

سرشناسه	: قنبری، اشکان، ۱۳۶۳ -
عنوان و نام پدیدآور	: آشنایی با مبانی امنیت شبکه/مؤلفین اشکان قنبری، مهران نیکو.
مشخصات نشر	: قم: آثار نفیس، ۱۳۹۳.
مشخصات ظاهری	: ۹۰ ص.: مصور، جدول، نمودار.
شابک	: ۱۰۰۰۰۰ ریال: 978-600-5299-85-4
وضعیت فهرست نویسی	: فیبا
یادداشت	: کتابنامه.
موضوع	: شبکه‌های کامپیوتری -- تدابیر ایمنی
موضوع	: کامپیوترها -- ایمنی اطلاعات
شناسه افزوده	: نیکو، مهران، ۱۳۵۸ -
رده بندی کنگره	: ۱۳۹۳ ق ۵۱۰۵/۵۱۰۵ TK۵۹
رده بندی دیویی	: ۰۰۵/۸
شماره کتابشناسی ملی	: ۲۵۸۳۸۴۴



ISBN- 978-600-5299-85-4

نام کتاب: آشنایی با مبانی امنیت شبکه

مؤلفین: مهندس اشکان قنبری و مهندس مهران نیکو

چاپ اول: ۱۳۹۳

ناشر: انتشارات آثار نفیس

شابک::

تیراژ: ۵۰۰ جلد

قیمت: ۱۰۰۰۰۰ ریال

کلیه حقوق برای مؤلف محفوظ می‌باشد.

سخن مولفین:

اینترنت یک شبکه عظیم اطلاع‌رسانی و یک بانک وسیع اطلاعاتی است که در آینده نزدیک دسترسی به آن برای تک‌تک افراد ممکن خواهد شد. کارشناسان ارتباطات، بهره‌گیری از این شبکه را یک ضرورت در عصر اطلاعات می‌دانند. این شبکه که از هزاران شبکه کوچکتر تشکیل شده، فارغ از مرزهای جغرافیایی، سراسر جهان را به هم مرتبط ساخته است. طبق آخرین آمار بیش از ششصد میلیون رایانه از تمام نقاط جهان در این شبکه گسترده به یکدیگر متصل شده‌اند که اطلاعات بی‌شماری را در تمامی زمینه‌ها از هر سنخ و نوعی به اشتراک گذاشته‌اند. گفتنی می‌شود نزدیک به یک میلیارد صفحه اطلاعات با موضوعات گوناگون از سوی افراد حقیقی و حقوقی روی این شبکه قرار داده شده است. این اطلاعات با سرعت تمام در بزرگراه‌های اطلاعاتی به کاربران رد و بدل می‌شود و تقریباً هیچ گونه محدودیت و کنترلی بر وارد کردن یا دریافت کردن داده‌ها اعمال نمی‌شود. حمایت از جریان آزاد اطلاعات، گسترش روزافزون فناوری اطلاعات و بستن بزرگ‌ترین شکاف بین اتصال به شبکه‌های اطلاع‌رسانی شعار دولتهاست. این در حالی است که گستردگی و تنوع اطلاعات آلوده روی اینترنت، موجب بروز نگرانی در بین کشورهای مختلف شده است. انحصار تصویر مستهجن، ایجاد پایگاه‌هایی با مضامین پورنوگرافی و سایتهای سوءاستفاده از کودکان را انحاء مختلف در کشورهای پیشرفته صنعتی بخصوص در خاستگاه این شبکه جهانی، کارشناسان اجتماعی را بشدت نگران کرده، به گونه‌ای که هیأت حاکمه را مجبور به تصویب قوانینی مبنی بر کنترل این شبکه در سطح جهان نموده است. هشدار، جریمه و بازداشت برای برپاکندگانی پایگاههای مخرب و فسادانگیز تدابیری است که کشورهای مختلف جهان برای مقابله با آثار سوء این شبکه اتخاذ کرده‌اند. ترس و بیم از تخریب مبانی اخلاقی و اجتماعی، ناشی از هجوم اطلاعات آلوده و مخرب از طریق اینترنت، واکنشی منطقی است، زیرا هر جامعه‌ای چارچوبهای اطلاعاتی خاص خود را دارد و طبیعی است که هر نوع اطلاعاتی که این حد و مرزها را بشکند می‌تواند سلامت و امنیت جامعه را به خطر اندازد. علی‌الرغم وجود جنبه‌ای مثبت شبکه‌های جهانی، سوء استفاده از این شبکه‌های رایانه‌ای توسط افراد بزهکار، امنیت ملی را در کشورهای مختلف با خطر روبرو ساخته است. از این رو بکارگیری فیلترها و فایر وال‌های مختلف و در برقراری امنیت شبکه برای پیشگیری از نفوذ داده‌های مخرب و مضر و گزینش اطلاعات سالم در این شبکه‌ها رو به افزایش است. خوشبختانه با وجود هیاهوی بسیاری که شبکه اینترنت را غیرقابل کنترل

VIII

معرفی می‌کند، فناوری لازم برای کنترل این شبکه و انتخاب اطلاعات سالم و برقراری امنیت در این شبکه روبه گسترش و تکامل است. در این کتاب یک بررسی کلی از اصول برقراری امنیت در شبکه خواهد شد. موضوعات اساسی امنیت شبکه نظیر معماری امنیت، استانداردهای امنیتی، سرویس‌ها، مکانیزم‌ها، توابع مدیریتی، تهدیدات، مخاطرات، رخنه‌های امنیتی و الگوریتم‌های امنیتی مانند رمز نگاری، احراز هویت، امضاهای دیجیتالی و... بررسی خواهند شد. در نهایت تکنولوژی‌های موجود و جدید برای ارتقاء امنیت شبکه‌ها مورد بحث قرار خواهد گرفت. این مجموعه می‌تواند به عنوان یک منبع در زمینه یکی از تکنولوژی‌های بروز مربوط به مخابرات رمز و کامپیوتر شناخته و در اختیار علاقمندان مخصوصاً دانشجویان کارشناسی، کارشناسی ارشد و مهندسی سخت افزار، نرم افزار و مهندسی برق با گرایش شبکه و رمز نگاری قرار گیرد. در ادامه لازم می‌دانیم از تمامی کسانی که ما را در تکمیل و نشر این کتاب یاری رسانند مخصوصاً دوست و همراه بسیار عزیزمان جناب آقای مهندس جواد شکوری کمال تشکر و قدردانی را داشته باشیم.

با آرزوی توفیق الهی

مهندس اشکان قنبری

(عضو باشگاه پژوهشگران جوان و نخبگان)

مهندس مهران نیکو

(عضو باشگاه پژوهشگران جوان و نخبگان)

VII فهرست

صفحه	عنوان
VII	سخن مولفین
۱	فصل اول
۱	بررسی کلیات کتاب و برخی مفاهیم موجود در امنیت شبکه
۳	۱-۱- مقدمه
۳	۱-۱-۱- مفهوم امنیت
۴	۱-۱-۲- اهمیت امنیت شبکه
۴	۲-۱- تاریخچه امنیت شبکه:
۵	۳-۱- تهدیدها و حمله‌ها به شبکه
۵	۱-۳-۱- تهدید
۶	۲-۳-۱- حمله:
۹	فصل دوم
۹	معماری امنیت برای ارتباط بین سیستم‌های باز براساس توصیف نامه X.800
۱۱	۱-۲- تعریف توصیف نامه X.800
۱۱	۱-۲-۲- سرویس‌های امنیتی
۱۳	۲-۲-۲- مکانیزم‌های امنیتی
۱۶	۳-۲- رابطه‌ی سرویس‌ها، مکانیزم‌ها و لایه‌ها
۱۶	۱-۳-۲- اصول لایه‌بندی امنیتی
۱۶	۲-۳-۲- قرارگیری سرویس‌ها و مکانیزم‌های امنیتی در شبکه
۲۰	۴-۲- مدیریت امنیت OSI (ارتباط سیستم‌های باز)
۲۱	۱-۴-۲- گروه‌های مدیریت امنیت OSI
۲۲	۲-۴-۲- فعالیت‌های مدیریتی امنیت سیستم خاص
۲۳	۳-۴-۲- توابع مدیریت مکانیزم امنیتی

VIII

فصل سوم	۲۷
معماری امنیت برای سیستم‌های فراهم کننده ارتباطات سراسری (end to end)	۲۷
بر اساس توصیف نامه X.805	۲۷
۱-۳- تعریف معماری امنیت	۲۹
۲-۳- ابعاد امنیتی	۲۹
۱-۲-۳- بعد امنیتی کنترل دسترسی	۳۰
۲-۲-۳- بعد امنیتی احراز هویت	۳۰
۳-۲-۳- بعد امنیتی نفی انکار	۳۰
۴-۲-۳- بعد امنیتی محرمانه نگه داشتن اطلاعات	۳۱
۵-۲-۳- بعد برقراری امنیت مخابراتی	۳۱
۶-۲-۳- بعد امنیتی سلامت داده	۳۱
۷-۲-۳- بعد امنیتی دسترس پذیری	۳۱
۸-۲-۳- بعد امنیتی اختفای پیام	۳۱
۳-۳- لایه های امنیتی	۳۱
۱-۳-۳- لایه امنیت پایه	۳۲
۲-۳-۳- لایه امنیت سرویس	۳۲
۳-۳-۳- لایه امنیت برنامه‌های کاربردی	۳۲
۴-۳- صفحه‌های امنیتی	۳۳
۱-۴-۳- صفحه امنیت مدیریت	۳۳
۲-۴-۳- صفحه امنیت کنترل	۳۴
۳-۴-۳- صفحه امنیت کاربر نهایی	۳۴
۵-۳- مقابله با تهدید ها	۳۵
۶-۳- راه های مقابله با مخاطره ها درخصوص امنیت اطلاعات	۳۶
۱-۶-۳- لغو خطر	۳۷

IX

۳۷	۳-۶-۲- انتقال خطر
۳۸	۳-۶-۳- کاهش خطر
۳۹	۳-۶-۴- پذیرفتن خطر
۴۱	فصل چهارم
۴۱	الگوریتم‌های امنیتی
۴۳	۴-۱- رمزنگاری
۴۴	۴-۱-۱- رمزنگاری جانشینی
۴۵	۴-۱-۲- رمزنگاری جایگشتی
۴۶	۴-۱-۳- رمزگذاری کلید عمومی
۵۱	۴-۲- احراز هویت
۵۴	۴-۳- امضاهای دیجیتالی
۵۵	۴-۳-۱- امضای دیجیتالی با کلید سری
۵۶	۴-۳-۲- امضای دیجیتالی با کلید عمومی
۵۹	فصل ۵
۵۹	بررسی روش‌های ارتقاء امنیتی شبکه
۶۱	۵-۱- تعریف راه‌های ارتقاء امنیت
۶۴	۵-۲-۱- مبانی طراحی دیوار آتش
۶۸	۵-۲-۲- اجزای جانبی یک دیوار آتش
۶۹	۵-۳- سیستم‌های آشکار سازی نفوذ (IDS)
۶۹	۵-۳-۱- وظایف IDS
۷۰	۵-۳-۲- آسیب پذیری‌ها
۷۲	۵-۴- تکنولوژی TNC-UTM
۷۳	۵-۴-۱- تکنولوژی امنیتی TNC
۷۴	۵-۴-۲- تکنولوژی امنیتی UTM

۷۵..... استفاده از TNC-UTM ۵-۴-۳.....

۷۷..... فصل ششم

۷۷..... نتیجه گیری

۸۱..... واژه نامه

۸۷..... منابع و مآخذ