امنیت شبکه‌های کامپیوتری

(جلد اول)

آشنایی با مفاهیم و معرفی روش‌ها

مسعود بیکی اشکذری

سرشناسه ..... بیکی اشکذری، مسعود، ۱۳۴۴
عنوان و نام پدیدآور ..... امنیت شبکه‌های کامپیوتری/ جلداول/ آشنایی با مفاهیم و معرفی روش‌ها/
عنوان و نام پدیدآور ..... /مسعود بیکی اشکذری؛ ویراستار فاطمه حبیبی
مشخصات نشر ..... تهران؛ خط میخی ، ۱۴۰۳
مشخصات ظاهری ..... ۱ج، ۲۳*۲۹س‌م
شابک .....دوره: ۲-۱-۹۲۲۵۹-۶۲۲-۹۷۸؛ جلد۱: ۹-۲-۹۲۲۵۹-۶۲۲-۹۷۸
وضعیت فهرست نویسی ..... فیپا
یادداشت .....کتابنامه
موضوع ..... امنیت شبکه
رایانه، فناوری اطلاعات
Computer Network Security
هک‌کردن - پیشگیری
رده بندی کنگره .....TK ۵۱۰۹/۵۹
رده بندی دیویی ۰۰۵/۸
شماره کتابشناسی ملی ۹۹۵۹۱۱۹
اطلاعات رکورد کتابشناسی .....فیپا

امنیت شبکه های کامپیوتری

(جلد اول)

آشنایی با مفاهیم و معرفی روش‌ها

نویسنده: .....مسعودبیکی اشکذری
طراح جلد ..... فاطمه حبیبی
ویراستار..... فاطمه حبیبی
ناشر..... نشر خط میخی
قطع ..... رحلی
چاپ ..... گیلان
نوبت چاپ .....چاپ اول ۱۴۰۳
شمارگان .....۲۰۰ نسخه
قیمت .....۲۰۰ هزارتومان

شابک دوره ۲-۱-۹۲۲۵۹-۶۲۲-۹۷۸
شابک جلد اول ۹-۲-۹۲۲۵۹-۶۲۲-۹۷۸

STD_MBEIKI@ALUMNI.KHU.AC.IR

انتشارات خط میخی

تهران، خیابان انقلاب
روبروی دانشگاه تهران
پلاک ۱۲۰۲، طبقه ۴
شمالی، نشر خط میخی
تلفن: ۶۶۴۹۰۲۵۳

امنیت شبکه های کامپیوتری

(جلد اول)

آشنایی با مفاهیم و معرفی روش‌ها

پیشگفتار

در دنیای دیجیتال امروز، امنیت اطلاعات به عنوان یکی از حیاتی‌ترین و پیچیده‌ترین مباحث در عرصه فناوری اطلاعات شناخته می‌شود. با افزایش روزافزون استفاده از شبکه‌های کامپیوتری و اینترنت در زندگی روزمره، تهدیدات و حملات سایبری نیز به طرز چشم‌گیری در حال افزایش هستند. این وضعیت نه تنها امنیت داده‌ها و اطلاعات شخصی را به خطر می‌اندازد، بلکه همچنین می‌تواند به کسب‌وکارها و نهادهای دولتی آسیب‌های جبران‌ناپذیری وارد کند. از این رو، درک عمیق از مفاهیم امنیت شبکه و آشنایی با روش‌های مختلف برای حفاظت از زیرساخت‌ها و اطلاعات، از اهمیت ویژه‌ای برخوردار است.

با ظهور تکنیک‌ها و فناوری‌های جدید در زمینه امنیت سایبری، نیاز به آموزش و بروز رسانی مستمر در این حوزه به مراتب افزایش یافته است. به عنوان مثال، استفاده از هوش مصنوعی و یادگیری ماشین برای شناسایی تهدیدات، به تازگی به یکی از ابزارهای کلیدی در عرصه امنیت شبکه تبدیل شده است. همچنین، فناوری‌های بلاک‌چین نیز به عنوان یک راه‌کار جدید برای تأمین امنیت داده‌ها مورد توجه قرار گرفته‌اند.

این کتاب به عنوان یک منبع آموزشی برای دانشجویان و علاقمندان در زمینه امنیت شبکه‌های کامپیوتری طراحی شده است. هدف اصلی این کتاب، آشنا کردن خوانندگان با مفاهیم پایه و روش‌های اصلی حفظ امنیت در شبکه‌ها است. به خصوص برای دانشجویانی که قبلاً درس مبانی شبکه‌های کامپیوتری را گذرانده‌اند، این کتاب می‌تواند ابزاری ارزشمند برای درک عمیق‌تر از مسائل امنیتی شبکه‌ها باشد. با ارائه مطالب به صورت ساده و قابل فهم، تلاش شده است تا خوانندگان بتوانند به راحتی و بدون دردسر موضوعات پیچیده امنیت اطلاعات را درک کنند.

این کتاب نه تنها شامل مطالب نظری است، بلکه مثال‌های عملی و موردپژوهی‌های مرتبط نیز به کار گرفته شده‌اند تا درک بهتر و عمیق‌تری از این مفاهیم فراهم شود. آشنایی با چالش‌های واقعی امنیت شبکه که بسیاری از متخصصان امروز با آن‌ها دست و پنجه نرم می‌کنند، می‌تواند به خوانندگان این امکان را بدهد که در دنیای واقعی مشکلات امنیتی را شناسایی و حل کنند.

در این زمینه، نام برخی از شخصیت‌های مطرح بین‌المللی در حوزه امنیت شبکه و سایبری به عنوان منبع الهام و تخصص به چشم می‌خورد. افرادی همچون «بروس اشنیر[1]»، مشاور امنیتی و نویسنده

[1] Bruce Schneier(1963), USA

کتاب‌های مشهور در این حوزه، که با انتشار آثار خود به آگاهی جامعه نسبت به تهدیدات سایبری کمک کرده است. افراد زیادی هستند که با تحقیقات و پروژه‌های خود در زمینه امنیت شبکه‌های کامپیوتری، تحولاتی چشم‌گیر ایجاد کرده‌اند.

کتاب پیش رو به بررسی مفاهیم و اصول امنیت شبکه می‌پردازد. از رمزنگاری گرفته تا کنترل‌های دسترسی و روش‌های پیشگیری از حملات، هر بخش از کتاب به گونه‌ای طراحی شده است که خوانندگان بتوانند با مفاهیم مختلف آشنا شوند و در زمینه امنیت شبکه توانمندی‌های متناسب با سطح مورد نظر را کسب کنند. مفاهیمی همچون امنیت زیرساخت‌های شبکه، تجزیه و تحلیل رفتارهای شبکه، و روش‌های شناسایی و پاسخ به تهدیدات جزء مهم‌ترین مباحثی هستند که در این کتاب به آن‌ها خواهیم پرداخت.

با توجه به اهمیت و گستردگی مسائل امنیتی در دنیای امروز، هدف ما در این کتاب، حتی فراتر از معرفی مفاهیم، فراهم کردن راهکارهایی عملی برای مقابله با تهدیدات و حملات سایبری است. در هر فصل، به تحلیل موردی و بررسی استراتژی‌های امنیتی موجود پرداخته خواهد شد تا خوانندگان بتوانند تجربیات و دانش خود را در عمل به کار گیرند. همچنین، خوانندگان با روش‌های نوین مانند ارزیابی ریسک، مدیریت حوادث، و توسعه سیاست‌های امنیتی آشنا خواهند شد. این موارد به آن‌ها کمک خواهد کرد تا از مهارت‌های خود در زمینه امنیت شبکه به بهترین نحو استفاده کرده و به عنوان متخصصان توانمند در این حوزه شناخته شوند.

بطور کلی، امید است که این کتاب نه تنها به درک عمیق‌تر خوانندگان از امنیت شبکه‌های کامپیوتری کمک کند، بلکه آن‌ها را برای اقدام و اقدام‌پذیری در برابر تهدیدات سایبری توانمند سازد. از همه دانشجویان و فعالان این حوزه دعوت می‌شود تا با مطالعه و یادگیری در این حوزه، توانایی‌های خود را در مقابله با چالش‌های امنیتی تقویت کرده و در این مسیر گام بردارند. در دنیای پیچیده امروز، آگاهی و آموزش مستمر تنها راه پیشگیری و مقابله با تهدیدات سایبری است و این کتاب می‌تواند به عنوان نقطه شروعی برای ورود به این دنیای جذاب و چالش‌برانگیز قلمداد شود.

فهرست مندرجات

مقدمه

امنیت شبکه‌های کامپیوتری امروزه به عنوان یک نیاز اساسی نه تنها به لحاظ علمی بلکه به عنوان یک ضرورت اجتماعی و اقتصادی شناخته می‌شود. با پیشرفت سریع فناوری اطلاعات و افزایش وابستگی به داده‌ها و اطلاعات دیجیتال، اهمیت به‌کارگیری لایه‌های امنیتی مناسب در شبکه‌ها به وضوح نمایان می‌شود. در دنیای امروز، اطلاعات حساس و حیاتی، از اطلاعات مالی تا داده‌های شخصی، به طور روزانه و به صورت آنلاین مبادله می‌شوند. عدم امنیت کافی می‌تواند نتایج وخیمی به همراه داشته باشد، از جمله سرقت هویت، از دست دادن داده‌های حیاتی و آسیب‌های مالی هنگفت. از این رو، هدف اصلی این کتاب، فراهم آوردن دانش و مهارت‌های لازم برای شناسایی تهدیدات، آسیب‌پذیری‌ها و مدیریت امنیت شبکه است. طی این کتاب، ما به بررسی عوامل مختلفی خواهیم پرداخت که بر امنیت شبکه تأثیر می‌گذارند و راهکارهای مؤثری برای حفاظت از این شبکه‌ها ارائه خواهیم کرد.

در سال‌های اخیر، با گسترش وب، به خصوص وب ۲.۰ و انتقال به سمت ابری، تهدیدات و حملات سایبری به شدت افزایش یافته است. بر اساس گزارشی از مرکز امنیت اینترنتی، تعداد حملات سایبری در سطح جهانی در حال افزایش است و پیش‌بینی می‌شود که هرسال این آمار افزایش یابد. این شرایط باعث شده است که سازمان‌ها و افراد نه تنها نسبت به تهدیدات موجود حساس‌تر شوند، بلکه در تلاش باشند تا روش‌های نوآورانه‌ای برای مقابله با این تهدیدات پیدا کنند. به همین دلیل، آگاهی و دانش در حوزه امنیت شبکه بیش از پیش ضرورت یافته است.

این کتاب به‌عنوان یک منبع آموزشی برای دانشجویان و فعالان در زمینه امنیت شبکه‌های کامپیوتری طراحی شده است. امید ما این است که محتوای این کتاب به خوانندگان کمک کند تا درک عمیق‌تری از مسائل امنیتی کسب کرده و توانمندی‌های لازم برای پیشگیری، شناسایی و پاسخ به تهدیدات امنیتی را به دست آورند.

فصول کتاب

این کتاب شامل نه فصل است که هر فصل به موضوعات خاصی در زمینه امنیت شبکه می‌پردازد:

فصل اول: مقدمه‌ای بر درس امنیت شبکه

در این فصل، ما به معرفی کلی امنیت شبکه خواهیم پرداخت و اهمیت آن را در دنیای دیجیتال توصیف خواهیم کرد. به طور خاص، مفاهیم پایه‌ای امنیت شبکه شامل محرمانگی، تمامیت و دسترسی‌پذیری را بررسی خواهیم کرد. این مفاهیم، پایه‌گذاری اصول برای امنیت شبکه را تشکیل می‌دهند و فهم آن‌ها ضروری است.

فصل دوم: معرفی اصطلاحات فنی امنیت شبکه

در این فصل، به بررسی اصطلاحات فنی مرتبط با امنیت شبکه خواهیم پرداخت. این اصطلاحات شامل فایروال، رمزنگاری، احراز هویت و سیستم‌های مدیریت امنیت اطلاعات هستند. درک این اصطلاحات به خوانندگان کمک می‌کند تا درک بهتری از مباحث فنی و تخصصی امنیت شبکه پیدا کنند.

فصل سوم: آشنایی با سرویس‌های امنیت شبکه

فصل سوم به معرفی خدمات مختلف امنیتی اختصاص دارد که شبکه‌ها را در برابر تهدیدات محافظت می‌کنند. در این فصل، خدماتی مانند VPN (شبکه خصوصی مجازی)، IDS/IPS (سیستم‌های تشخیص و جلوگیری از نفوذ) و آنتی‌ویروس‌ها را معرفی خواهیم کرد و بر اهمیت آن‌ها در حفظ امنیت شبکه تأکید می‌کنیم.

فصل چهارم: آشنایی با نفوذ (هک) و انواع نفوذگرها (هکرها)

در این فصل به معرفی انواع نفوذگرها و روش‌های نفوذ آن‌ها خواهیم پرداخت. همچنین به توضیح روش‌های مختلف هک، از جمله حملات فیشینگ، حملات مهندسی اجتماعی و ابزارهای مورد استفاده آن‌ها خواهیم پرداخت. درک این روش‌ها به خوانندگان کمک خواهد کرد تا بهتر بتوانند از شبکه خود در برابر این تهدیدات دفاع کنند.

فصل پنجم: آشنایی با حملات، دسته‌بندی حملات و معرفی حملات مهم

در این فصل به بررسی انواع حملات سایبری خواهیم پرداخت و آن‌ها را به دسته‌های مختلف مانند حملات DoS، DDoS، و حملات Man-in-the-Middle تقسیم‌بندی خواهیم کرد. همچنین حملات مهم مانند SQL Injection و Cross-Site Scripting را مورد بررسی قرار خواهیم داد. این شناخت از انواع حملات و نحوه کار آن‌ها، به مخاطبان کمک می‌کند تا تمهید هایی برای پیشگیری و پاسخ به این حملات بیاندیشند و راهبردهای مؤثری برای دفاع مدنظر قرار دهند.

فصل ششم: آشنایی با مفاهیم رمزنگاری و معرفی انواع روش‌های رمزنگاری

فصل ششم به بررسی مفاهیم اولیه رمزنگاری اختصاص یافته است. رمزنگاری به عنوان یکی از مؤثرترین روش‌ها برای محافظت از اطلاعات در حال انتقال و ذخیره‌سازی، نقش اساسی دارد. در این فصل، دو نوع اصلی رمزنگاری، یعنی رمزنگاری متقارن و نامتقارن را معرفی خواهیم کرد و به بررسی الگوریتم‌های

مختلفی مانند AES (رمزنگاری پیشرفته) و RSA (رمزنگاری کلید عمومی) می‌پردازیم. همچنین، در این بخش به اصول کلیدی مانند کلیدهای رمزنگاری و مدیریت آن‌ها اشاره خواهیم کرد تا خوانندگان بتوانند از این نرم‌افزارهای رمزنگاری به بهترین شکل ممکن استفاده کنند.

فصل هفتم: آشنایی و معرفی روش‌های دفاعی در مقابل حملات بر اساس لایه‌های TCP/IP

فصل هفتم به بررسی روش‌های دفاعی طی لایه‌های مختلف مدل TCP/IP خواهد پرداخت. در این فصل، خواهیم گفت که چگونه می‌توان با استفاده از فایروال‌های لایه کاربرد، IDS/IPS و VPNها از اطلاعات در برابر تهدیدات محافظت کنیم. با اشاره به ابزارهای موجود در بازار و همچنین بهترین شیوه‌های پیاده‌سازی این تجهیزات، خوانندگان می‌توانند آموخته‌های خود را به یک استراتژی امنیتی کلی تبدیل کنند.

فصل هشتم: معرفی ابزارها و تکنیک‌های امنیتی

این فصل به معرفی ابزارها و تکنیک‌های امنیتی مختلف خواهد پرداخت. این ابزارها شامل اسکنرهای امنیتی، ابزارهای مانیتورینگ شبکه و سیستم‌های امنیتی زائد (SIEM) هستند. خوانندگان با آشنایی به این ابزارها می‌توانند نقش آن‌ها را در شناسایی و جلوگیری از تهدیدات بهتر درک کنند و بیاموزند چگونه می‌توانند از این ابزارها برای بهبود امنیت شبکه خود استفاده کنند.

فصل نهم: معرفی مدل‌های استقرار امنیت شبکه

در فصل پایانی، ما به بررسی مدل‌های مختلف استقرار امنیت شبکه خواهیم پرداخت. این مدل‌ها شامل مدل‌های امنیتی مبتنی بر لایه‌ها، مدل‌های مبتنی بر نقش‌ها و مدل‌های ترکیبی هستند. همچنین، ما به بهترین شیوه‌های پیاده‌سازی این مدل‌ها خواهیم پرداخت و بر نیاز به رویکردهای مناسب امنیتی در هر سازمان تأکید خواهیم کرد.

***روش‌شناسی و استناد به منابع**

در تالیف این کتاب، از منابع معتبر علمی و پژوهشی بین‌المللی بهره‌برداری شده است. این منابع شامل کتب، مقالات و تحقیقات به‌روز شده بر اساس آخرین یافته‌های علمی در حوزه امنیت شبکه است. تمامی منابع طبق فرمت استاندارد APA در تمام فصل‌ها ذکر شده است و به خوانندگان این امکان را می‌دهد

تا برای مطالعه عمیق‌تر در مورد هر موضوع از منابع اولیه بهره‌مند شوند. این شیوه، به اعتبار محتوای کتاب افزوده و کارشناسان و دانشجویان را به تعمیق در شناخت مطالب تشویق می‌کند.

هدف از نگارش این کتاب

هدف از تهیه این کتاب توانمندسازی دانشجویان رشته مهندسی کامپیوتر و سایر رشته‌های مرتبط با امنیت سایبری است. ما به دنبال فراهم‌آوردن محتوایی هستیم که به درک عمیق‌تر مفاهیم کلیدی این حوزه کمک کند و آنان را در مسیر حرفه‌ای‌شان یاری رساند. با توجه به رشد روزافزون تهدیدات سایبری و اهمیت امنیت در دنیای فناوری اطلاعات، به دانشجویان و حرفه‌ای‌های این حوزه آموخته می‌شود که چگونه با چالش‌های امنیتی مقابله کنند و بتوانند به عنوان متخصصان مؤثر در شرایط حساس عمل کنند.

امید داریم که محتوای ارائه شده در این کتاب، به عنوان یک منبع مفید و کاربردی در مسیر یادگیری و توسعه حرفه‌ای خوانندگان باشد و به آنها در تربیت نسل بعدی متخصصان نرم‌افزار و امنیت سایبری گردد. با تجهیز شدن به دانش و مهارت‌های لازم، آن‌ها می‌توانند به بهبود امنیت شبکه‌ها و اطلاعات کمک کنند و در مواجهه با تهدیدات سایبری، یک راهبرد سریع و مؤثر را پیاده‌سازی نمایند. در دنیای پیچیده و پرسرعت امروزی، آگاهی و آموزش مستمر، تنها راه پیشگیری و مقابله با تهدیدات سایبری است و این کتاب می‌تواند به عنوان یک نقطه شروع برای ورود به این دنیای جذاب و چالش‌برانگیز محسوب شود.

با در نظر گرفتن این موضوعات، امید است که خوانندگان با بررسی دقیق محتوای این کتاب، ابزارهای لازم برای مقابله با چالش‌های امنیتی را در اختیار داشته باشند و قادر باشند که به محیط‌های کاری خود ارزش افزوده‌ای بیفزایند. در عمل، این کتاب می‌تواند راهی برای تبدیل شدن به یک متخصص امنیت شبکه کارآمد فراهم کند و به افراد این توان را بدهد که در علیه هر گونه تهدید سایبری به نقشی فعال و مؤثر دست یابند.