امنیت اطلاعات

محمدتقی روغنی

سرشناسه : روغنی، محمدتقی، ۱۳۶۰-
عنوان و نام پدیدآور : امنیت اطلاعات/ محمد تقی‌روغنی
مشخصات نشر : تهران: انتشارات ناقوس، ۱۳۹۳.
مشخصات ظاهری : ۴۴۸ ص.: مصور، جدول.
شابک : ۹۷۸-۹۶۴-۳۷۷-۷۳۲-۶ بها : ۲۵۰.۰۰۰ ریال
وضعیت فهرست‌نویسی : فیپا
موضوع : تکنولوژی اطلاعات—تدابیر ایمنی—استانداردها
موضوع : شبکه‌های کامپیوتری -تدابیر ایمنی—استانداردها
موضوع : کامپیوترها—ایمنی اطلاعات—دستنامه‌ها
موضوع : حفاظت اطلاعات—استانداردها
رده بندی کنگره : ۱۳۹۳ ۸الف۸۷ر/T۵۸/۵
رده بندی دیویی : ۳۰۳/۴۸۳۳
شمارهٔ کتابشناسی ملی : ۳۶۸۵۵۶۶

انتشارات ناقوس
NAGHOOS PUBLICATION

نام کتاب : امنیت اطلاعات
ناشر : انتشارات ناقوس
مؤلف : محمدتقی روغنی
چاپ اول : ۱۳۹۳
تیراژ : ۱۰۰۰ جلد
چاپ و صحافی : نارنجستان
قیمت : ۲۵۰.۰۰۰ ریال
شابک : ۹۷۸-۹۶۴-۳۷۷-۷۳۲-۶
ISBN : 978-964-377-732-6

چاپ اول

مراکز پخش:
۱- انتشارات ناقوس: میدان انقلاب، خیابان کارگرجنوبی، خیابان روانمهر، کوچه دولتشاهی، پلاک ۲
تلفن و فاکس: ۶۶۴۳۰۸۵۲۰ – ۶۶۴۳۰۱۷۹۸ – ۶۶۴۱۷۰۷۲ – ۶۶۴۶۶۷۹۳
۲- کتابفروشی گلریزان، ضلع جنوب‌شرقی میدان انقلاب، پلاک ۱۱ تلفن: ۶۶۹۷۶۲۳۰
۳- کتابفروشی الیاس: خیابان انقلاب، نبش فروردین تلفن: ۶۶۴۰۵۰۸۴

مقدمه مؤلف:

خداوند حکیم را شاکرم که عنایت خویش را برای نگارش کتابی جدید شامل حال بنده نمود، تا بتوانم گام کوچک دیگری در راستای ارتقای علمی فناوری اطلاعات هموطنان عزیزم بردارم.

تعاملات بین مشتریان و سازمان‌ها از طریق سرویس‌های فناوری اطلاعات، روزبه‌روز بیشتر شده و سازمان‌ها را مجبور می‌نماید که برای رفع نیاز مشتریان، دیتای بیشتری را بر روی سرویس‌دهنده‌های خود قرار دهند. هرقدر فناوری اطلاعات در کسب‌وکار سازمان‌ها بیشتر وارد شده و باعث تسهیل امور می‌شود، در مقابل ریسک سازمان در حفاظت از دارایی‌های اطلاعاتی را بالا می‌برد. از طرف دیگر وابستگی ادامه حیات کسب‌وکار سازمان، بیشتر به سرویس‌های فناوری اطلاعات گره می‌خورد.

در این سیرِ رو به رشد استفاده از سرویس‌های فناوری اطلاعات، متأسفانه بحث امنیت بسیار مهجور و یا مغفول مانده است. مخصوصاً در بین شرکت‌ها و سازمان‌های ایرانی آن‌چنان‌که بایدوشاید به بحث امنیت توجه نمی‌شود.

بعضی از سازمان‌ها برای مباحث امنیتی ارزش خاصی قائل نشده و تا روز بروز مصیبت، هیچ قدمی در جهت محافظت از دارایی‌های اطلاعاتی سازمان خود برنمی‌دارند. بعضی دیگر، امنیت را به خرید چند محصول امنیتی مثل فایروال و آنتی‌ویروس، محدود کرده و تصور می‌کنند که باوجود این محصولات، امنیت را در سازمان خود برقرار نموده‌اند.

توجه داشته باشید که امنیت صرفاً با خرید چند محصول امنیتی، برقرار نمی‌شود. اگر امنیت را یک فرآیند در نظر بگیریم، محصولات امنیتی تنها بخشی از آن فرآیند خواهند بود. در این فرآیند امنیتی، طراحی و ایجاد سیاست‌های امنیتی در سطح مدیران ارشد سازمان، باید به‌عنوان یکی از مؤلفه‌های مهم در نظر گرفته شود.

پس از بحث مدیران ارشد، یکی دیگر از مشکلات در زمینه امنیت، ناآگاهی مدیران و کارشناسان IT نسبت به مفاهیم امنیت اطلاعات است. بسیاری از کارشناسان، پیکربندی تجهیزات را صرفاً به‌صورت تجربی و بدون اطلاع از نحوه عملکرد پروتکل‌ها انجام می‌دهند. لذا در اکثر مواقع پیکربندی درستی با توجه به نیازهای سازمان انجام نمی‌پذیرد.

در این کتاب سعی شده بجای یک محصول امنیتی خاص، به مفاهیم اساسی امنیت پرداخته شود. زمانی که یک مدیر یا کارشناس IT و امنیت، آگاهی درستی از مفاهیم امنیتی داشته باشد، توان تجزیه‌وتحلیل بهتری نسبت به فرآیندهای امنیتی پیداکرده و بالطبع در زمان طراحی سیاست‌های امنیتی و یا پیکربندی تجهیزات، عملکرد بهتری خواهد داشت.

مطالب این کتاب در چهار بخش تقسیم‌بندی شده است. در بخش اول به استاندارد سیستم مدیریت امنیت اطلاعات پرداخته‌شده است. قطعاً زمانی که وارد بحث امنیت اطلاعات می‌شویم، یکی از مهم‌ترین مواردی که باید در نظر گرفته شود، استانداردهای مربوطه است. اصلی‌ترین استاندارد درزمینه امنیت اطلاعات، استاندارد خانواده ISMS است. در فصل اول و دوم کتاب، استانداردهای ISO 27000، ISO 27001 و ISO 27002 به‌صورت اجمالی بررسی‌شده است.

در بخش دوم، به یکی از ارکان امنیت اطلاعات، یعنی رمزنگاری، پرداخته‌شده است. نحوه عملکرد الگوریتم‌های مهم رمزنگاری مثل DES، 3DES، AES، RSA و SHA شرح داده‌شده است. همچنین کاربرد این الگوریتم‌ها در برقراری سرویس‌های امنیتی مثل محرمانگی، احرازهویت، صحت، امضای دیجیتال و عدم انکار، تشریح شده است.

در بخش سوم این کتاب، مباحث امنیت شبکه مورد بررسی قرارگرفته است. با توجه به گسترش شبکه‌های ارتباطی، یکی از دغدغه‌های اصلی مدیران و کارشناسان، امنیت شبکه است. در فصول این بخش به مفاهیم امنیتی و تکنولوژی‌های مورداستفاده در امنیت شبکه ازجمله فایروال، IDS، IPS و هانی‌پات پرداخته شده است. در آخر این بخش نیز نحوه برقراری امنیت در ارتباطات شبکه‌ای با استفاده از IPsec و VPN، مورد بررسی قرار گرفته است.

در بخش چهارم، به امنیت سایر سرویس‌هایی که بیشتر مورداستفاده قرار می‌گیرند، پرداخته‌شده است. ازجمله تشریح پروتکل HTTPS برای امنیت وب، پروتکل PGP برای امنیت پست الکترونیک، بهترین شیوه‌های امنیت سیستم‌عامل و بررسی تهدیدات برتر دیتابیس و نحوه مقابله با آن‌ها، در فصول این بخش گنجانده شده است.

هرچند این کتاب توسط اساتید و کارشناسان امنیت مورد بازخوانی و رفع اشکال قرارگرفته، اما نمی‌توان آن را خالی از نقصان دانست. لذا خواهشمندم هرگونه انتقاد و پیشنهاد مدنظر خود را از طریق پست الکترونیک MTRoghani@Gmail.com، برای بنده ارسال نمایید.

در پایان امیدوارم که این کتاب بتواند نقشی هرچند کوچک، در افزایش آگاهی مدیران و کارشناسان IT و امنیت اطلاعات ایفا نماید. در ضمن از تمام اساتید و کارشناسان عزیزی که از راهنمایی‌های خود در نگارش این کتاب دریغ نکرده‌اند، صمیمانه سپاسگزاری می‌نمایم.

با احترام

محمدتقی روغنی

پاییز ۱۳۹۳

فهرست مطالب:

مقدمه مؤلف ۵

بخش اول استاندارد ISMS ۲۳

فصل اول مرور کلی استاندارد ISMS و الزامات آن ۲۵

مبحث اول؛ مرور استاندارد ISO/IEC 27000:2014 ۲۷

استانداردهای خانواده ISMS ۲۸

مروری بر استانداردهای خانواده ISMS ۲۹

۱- استاندارد ISO/IEC 27000 (همین استاندارد) ۲۹

۲- استاندارد ISO/IEC 27001 ۲۹

۳- استاندارد ISO/IEC 27006 ۲۹

۴- استاندارد ISO/IEC 27002 ۳۰

۵- استاندارد ISO/IEC 27003 ۳۰

۶- استاندارد ISO/IEC 27004 ۳۱

۷- استاندارد ISO/IEC 27005 ۳۱

۸- استاندارد ISO/IEC 27007 ۳۱

۹- استاندارد ISO/IEC TR 27008 ۳۱

۱۰- استاندارد ISO/IEC 27013 ۳۲

۱۱- استاندارد ISO/IEC 27014 ۳۲

۱۲- استاندارد ISO/IEC TR 27016 ۳۳

۱۳- استاندارد ISO/IEC 27010 ۳۳

۱۴- استاندارد ISO/IEC 27011 ۳۳

۱۵- استاندارد ISO/IEC TR 27015 ۳۴

۱۶- استاندارد ISO/IEC 27799 ۳۴

اصطلاحات و تعاریف ۳۵

مروری بر ISMS ۳۷

اصول PDCA ۳۹

برقراری، نظارت، نگهداری و بهبود عملکرد ISMS ۴۰

مبحث دوم؛ مرور استاندارد ISO/IEC 27001:2013 ۴۱

تعیین چارچوب سیستم مدیریت امنیت اطلاعات ۴۱

رهبری و تعهد ۴۲

سیاست‌گذاری و خط‌مشی ۴۲
نقش‌های سازمانی، مسئولیت‌ها و اختیارات ۴۳
برنامه‌ریزی ۴۳
ارزیابی ریسک امنیت اطلاعات ۴۳
مقابله با ریسک امنیت اطلاعات ۴۴
اهداف امنیت اطلاعات و برنامه‌ریزی برای دستیابی به آن‌ها ۴۴
صلاحیت و آگاهی ۴۵
ارتباط ۴۵
مستندسازی ۴۵
برنامه‌ریزی و کنترل عملیاتی ۴۶
ارزیابی کارایی ۴۶
بهبود ۴۷
نمودار کلی استاندارد ISO/IEC 27001:2013 ۴۷

فصل دوم دستورالعمل مدیریت امنیت اطلاعات ۴۹

مبحث اول؛ مرور استاندارد ISO/IEC 27002:2013 ۵۱

ساختار استاندارد ISO/IEC 27002 ۵۱
۵ - ماده ۱: سیاست‌های امنیت اطلاعات ۵۲
خط‌مشی امنیت اطلاعات ۵۲
۶ - ماده ۲: امنیت اطلاعات سازمان ۵۳
نقش‌ها و مسئولیت‌های امنیت اطلاعات ۵۳
خط‌مشی تجهیزات همراه ۵۲
دورکاری ۵۵
۷ - ماده ۳: امنیت منابع انسانی ۵۶
قوانین و شرایط استخدام ۵۶
۸ - ماده ۴: مدیریت دارایی ۵۷
فهرست دارایی‌ها ۵۷
طبقه‌بندی اطلاعات ۵۸
اداره دارایی ۵۹
مدیریت رسانه‌های قابل‌حمل ۶۰
دفع رسانه ۶۱
۹ - ماده ۵: کنترل دسترسی ۶۱
سیاست‌های کنترل دسترسی ۶۱
دسترسی به شبکه و سرویس‌های شبکه ۶۳
ثبت و لغو کاربر ۶۴
محدودیت دسترسی به اطلاعات ۶۵

سیستم مدیریت رمزعبور ۶۵
۱۰ - ماده ۶: رمزنگاری ۶۶
سیاست استفاده از کنترل‌های رمزنگاری ۶۶
مدیریت کلید رمزنگاری ۶۸
۱۱ - ماده ۷: امنیت محیطی و فیزیکی ۶۸
امنیت فیزیکی محیط پیرامونی ۶۸
کنترل ورود فیزیکی ۶۹
حفاظت در مقابل تهدیدات بیرونی و زیست‌محیطی ۷۰
امنیت کابل‌کشی ۷۰
۱۲ - ماده ۸: امنیت عملیات ۷۱
مستندسازی دستورالعمل عملیاتی ۷۱
مدیریت تغییر ۷۲
کنترل در برابر بدافزارها ۷۳
پشتیبان‌گیری ۷۴
ثبت رویداد ۷۵
نصب نرم‌افزار بر روی سیستم‌عامل ۷۶
محدودیت در نصب نرم‌افزار ۷۷
۱۳ - ماده ۹: امنیت ارتباطات ۷۸
کنترل شبکه ۷۸
سیاست‌ها و دستورالعمل انتقال اطلاعات ۷۹
۱۴ - ماده ۱۰: کسب، توسعه و نگهداری سیستم ۸۰
محافظت از نرم‌افزار خدمات معاملات ۸۰
سیاست توسعه امن نرم‌افزار ۸۱
دستورالعمل کنترل تغییرات سیستم ۸۲
۱۵ - ماده ۱۱: ارتباط با تأمین‌کنندگان ۸۳
سیاست‌های امنیت اطلاعات برای ارتباط با تأمین‌کنندگان ۸۳
۱۶ - ماده ۱۲: مدیریت حوادث امنیت اطلاعات ۸۵
مسئولیت‌ها و دستورالعمل‌ها ۸۵
گزارش رویداد امنیت اطلاعات ۸۶
گزارش ضعف‌های امنیت اطلاعات ۸۷
واکنش به حوادث امنیت اطلاعات ۸۸
۱۷ - ماده ۱۳: جنبه‌های امنیت اطلاعات در مدیریت تداوم کسب‌وکار ۸۹
برنامه‌ریزی تداوم امنیت اطلاعات ۸۹
دسترس‌پذیر بودن امکانات پردازش اطلاعات ۸۹
۱۸ - ماده ۱۴: انطباق ۹۰
انطباق با استانداردها و سیاست‌های امنیتی ۹۰
بررسی انطباق فنی ۹۱

بخش دوم رمزنگاری ۹۳
فصل سوم مفاهیم رمزنگاری ۹۵
مبحث اول؛ مفاهیم و اصطلاحات رمزنگاری ۹۷
تعریف رمزنگاری ۹۷
اصطلاحات رمزنگاری ۹۸
انواع رمزنگاری ۱۰۰
انواع حملات به سیستم رمزنگاری ۱۰۱
انواع حملات کشف رمز ۱۰۱
اصول انتخاب سیستم رمزنگاری ۱۰۲
شروط شانون ۱۰۲
پنهان‌کاری (Steganography) ۱۰۳
رمزنگاری و فشرده‌سازی ۱۰۳
مبحث دوم؛ مفاهیم رمزنگاری متقارن ۱۰۴
اصول کلی رمزگذاری ۱۰۵
تقسیم‌بندی الگوریتم‌های جایگزینی ۱۰۵
رمزنگاری کلاسیک و مدرن ۱۰۶
انواع رمزنگاری کلاسیک ۱۰۶
۱. الگوریتم رمز سزار (Caesar Cipher) ۱۰۷
۲. الگوریتم رمز Playfair ۱۰۸
۳. الگوریتم رمز ویجنر (Vigenère Cipher) ۱۰۹
۴. الگوریتم رمز نرده راه‌آهن (Rail Fence) ۱۱۱
کلیدهای One-Time Pad ۱۱۲
مبحث سوم؛ مفاهیم رمزنگاری نامتقارن ۱۱۳
ویژگی‌های الگوریتم رمزنگاری نامتقارن ۱۱۵
مقایسه رمزنگاری متقارن با رمزنگاری نامتقارن ۱۱۶
محرمانگی و احرازهویت ۱۱۶
کاربردهای سیستم رمزنگاری کلیدعمومی ۱۱۷
الزامات رمزنگاری نامتقارن ۱۱۸
مبحث چهارم؛ مفاهیم توابع درهم‌سازی ۱۱۹
اصطلاحات توابع درهم‌سازی ۱۲۰
خواص توابع درهم‌سازی ۱۲۰
کاربرد Hash در بررسی صحت پیام ۱۲۱
کاربرد توابع درهم‌سازی ۱۲۲
امنیت توابع درهم‌سازی ۱۲۴
مقایسه توابع درهم‌سازی ۱۲۵

فصل چهارم الگوریتم‌های رمزنگاری متقارن ۱۲۷
مبحث اول: الگوریتم DES ۱۲۹
الگوریتم فایستل ۱۲۹
رمزگذاری و رمزگشایی در فایستل ۱۳۰
پارامترها و ویژگی‌های طراحی فایستل ۱۳۲
الگوریتم DES ۱۳۲
رمزگذاری در DES ۱۳۳
جایگشت اولیه (Initial Permutation) ۱۳۵
جزئیات یک دور (Round) از الگوریتم ۱۳۶
رمزگشایی در DES ۱۳۹
بررسی قدرت DES ۱۳۹
مبحث دوم: الگوریتم AES ۱۴۱
گالوا فیلد ۱۴۲
عملیات جمع در AES ۱۴۲
عملیات ضرب در AES ۱۴۲
ساختار کلی AES ۱۴۳
جزئیات ساختار AES ۱۴۵
جزئیات عملیات هر دور AES ۱۴۸
ویژگی‌های کلیدرمز در AES ۱۵۱
مبحث سوم: الگوریتم Triple DES ۱۵۲
3DES با دو کلید متفاوت ۱۵۲
3DES با سه کلید متفاوت ۱۵۴
مبحث چهارم: روش‌های عملیاتی رمزنگاری بلوکی ۱۵۵
روش Electronic Codebook (ECB) ۱۵۶
روش Cipher Block Chaining (CBC) ۱۵۷
روش Cipher Feedback (CFB) ۱۵۸
روش Output Feedback (OFB) ۱۶۰
روش Counter (CTR) ۱۶۲
مزایای روش CTR ۱۶۳
فصل پنجم الگوریتم‌های رمزنگاری نامتقارن ۱۶۵
مبحث اول: الگوریتم RSA ۱۶۷
تشریح الگوریتم RSA ۱۶۸
محاسبه کلید عمومی و خصوصی در RSA ۱۶۸
مثال محاسبه کلید خصوصی و عمومی ۱۶۹
تولید کلید ۱۷۲

امنیت RSA ۱۷۳
الف) حملات تهدیدکننده RSA ۱۷۳
ب) اقدامات متقابل با حملات RSA ۱۷۴
مبحث دوم: الگوریتم دیفی‌هلمن ۱۷۶
تشریح الگوریتم دیفی‌هلمن ۱۷۶
مثال محاسبه کلید دیفی‌هلمن ۱۷۸
حمله مردمیانی ۱۸۰
سیستم رمزنگاری الجمل ۱۸۱

فصل ششم توابع درهم‌سازی و کاربردها ۱۸۵
مبحث اول: تصدیق پیام ۱۸۷
روش اول: تصدیق پیام به‌علاوه محرمانگی ۱۸۷
روش دوم: تصدیق پیام بدون محرمانگی ۱۸۸
روش سوم: تصدیق پیام بدون استفاده از الگوریتم متقارن ۱۸۸
روش چهارم: تصدیق پیام با مقدار S به‌علاوه محرمانگی ۱۸۹
الگوریتم MAC ۱۹۰
توابع HMAC ۱۹۲
مبحث دوم: امضای دیجیتال ۱۹۳
روش اول: امضای دیجیتال ۱۹۳
روش دوم: امضای دیجیتال به‌علاوه محرمانگی با رمزنگاری متقارن ۱۹۵
روش سوم: امضای دیجیتال به‌علاوه محرمانگی با رمزنگاری نامتقارن ۱۹۶
الزامات امضای دیجیتال ۱۹۷
ویژگی عدم‌انکار ۱۹۷
استاندارد امضای دیجیتال (DSS) ۱۹۸
الگوریتم DSA ۲۰۰
تابع Signature ۲۰۱
تابع Verification ۲۰۲
مبحث سوم: الگوریتم SHA ۲۰۴
الگوریتم SHA-512 ۲۰۵
جزئیات یک دور (Round) از SHA ۲۰۹
جزئیات Message Schedule ۲۱۱

بخش سوم امنیت شبکه ۲۱۳
فصل هفتم مفاهیم امنیت شبکه ۲۱۵
مبحث اول: مفاهیم امنیتی ۲۱۷

مثلث امنیت اطلاعات ۲۱۹
محرمانگی (Confidentiality) ۲۱۹
صحت و تمامیت (Integrity) ۲۱۹
دسترس‌پذیری (Availability) ۲۲۰
طبقه‌بندی آسیب‌پذیری ۲۲۱
اصول اساسی امنیت ۲۲۱
مبحث دوم؛ انواع تهدیدات ۲۲۳
مالکیت معنوی ۲۲۴
حملات نرم‌افزاری ۲۲۵
ویروس ۲۲۵
کرم ۲۲۶
اسب تراوا ۲۲۶
بمب‌های منطقی ۲۲۶
درب پشتی ۲۲۶
تهدیدات چندشکلی ۲۲۶
مضرات آنتی‌ویروس‌ها ۲۲۷
تنزل در کیفیت خدمات ۲۲۷
جاسوسی یا تجاوز ۲۲۷
بلایای طبیعی ۲۲۸
خطاهای انسانی ۲۲۹
اخاذی اطلاعاتی ۲۲۹
سیاست یا برنامه‌ریزی سازمانی ناقص، ناکافی و یا گمشده ۲۲۹
کنترل‌های ناقص، ناکافی و یا گمشده ۲۳۰
کارشکنی یا خرابکاری ۲۳۰
سرقت ۲۳۰
خطاها و شکست سخت‌افزاری ۲۳۰
خطاها و شکست فنی نرم‌افزار ۲۳۱
منسوخ‌شدن تکنولوژی ۲۳۱
مبحث سوم؛ انواع حملات ۲۳۲
روش‌های حمله ۲۳۳
شناسایی ۲۳۳
مهندسی اجتماعی ۲۳۳
افزایش حق دسترسی ۲۳۳
درب پشتی(Back Door) ۲۳۴
کانال پنهان (Covert channel) ۲۳۴
حملات داخلی ۲۳۴

کشف کلمه عبور ۲۳۵
Botnet ۲۳۵
حملات امنیتی ۲۳۶
حملات غیرفعال (Passive Attack) ۲۳۶
حملات فعال (Active Attack) ۲۳۷
حقه‌بازی (Spoofing) ۲۳۹
حمله مردمیانی ۲۳۹
هرزنامه (Spam) ۲۳۹
استراق سمع (Sniff) ۲۳۹
مبحث چهارم؛ سرویس‌ها و مکانیسم‌های امنیتی ۲۴۰
الف) سرویس‌های امنیتی ۲۴۰
احراز هویت (Authentication) ۲۴۰
کنترل دسترسی (Access Control) ۲۴۱
محرمانگی اطلاعات (Data Confidentiality) ۲۴۱
صحت اطلاعات (Data Integrity) ۲۴۱
انکارناپذیری (Non-repudiation) ۲۴۲
ب) مکانیسم‌های امنیتی ۲۴۲
رمزگذاری (Encipherment) ۲۴۲
مکانیسم امضای دیجیتال (Digital Signature) ۲۴۳
مکانیسم کنترل دسترسی (Access Control) ۲۴۳
مکانیسم‌های صحت دیتا ۲۴۴
مکانیسم تبادل احراز هویت ۲۴۵
مکانیسم توسعه ترافیک (Traffic padding mechanism) ۲۴۶
مکانیسم کنترل مسیریابی ۲۴۶
مکانیسم گواهی رسمی (Notarization mechanism) ۲۴۶

فصل هشتم تکنولوژی‌ها و ابزارهای امنیتی ۲۴۷

مبحث اول؛ کنترل دسترسی ۲۴۹
۱. کنترل دسترسی اجباری (Mandatory Access Controls) ۲۴۹
۲. کنترل دسترسی غیراختیاری (Non-discretionary control) ۲۵۰
۳. کنترل دسترسی اختیاری (Discretionary Access Control) ۲۵۰
مکانیسم‌های کنترل دسترسی ۲۵۰
شناسایی ۲۵۰
احرازهویت ۲۵۱
مجوزدهی ۲۵۲

پاسخگویی ۲۵۳
پروتکل AAA ۲۵۳
پروتکل کربروس (Kerberos) ۲۵۴
مبحث دوم؛ فایروال ۲۵۵
گروه اول؛ روش‌های پردازش فایروال ۲۵۵
۱. فایروال فیلترینگ بسته‌ها ۲۵۶
۲. دروازه برنامه ۲۵۹
۳. دروازه مدار ۲۶۰
۴. فایروال لایه MAC ۲۶۰
۵. فایروال چندگانه ۲۶۰
گروه دوم؛ تقسیم‌بندی بر اساس دوران توسعه ۲۶۱
Next-Generation Firewall ۲۶۲
گروه سوم؛ تقسیم‌بندی بر اساس ساختار ۲۶۲
انواع مناطق در شبکه ۲۶۳
۱. منطقه قابل‌اطمینان (Trusted Zone) ۲۶۳
۲.منطقه غیرقابل‌اطمینان (Untrusted Zone) ۲۶۳
۳.منطقه کمتر حفاظت‌شده (Demilitarized Zone) ۲۶۴
۴.منطقه سرورها (Server Zone) ۲۶۴
بهترین شیوه پیکربندی فایروال ۲۶۶
مبحث سوم؛ IDS/IPS ۲۶۸
وظایف کلیدی تکنولوژی IDPS ۲۷۰
روش‌های تشخیص ۲۷۲
۱. تشخیص مبتنی امضا (Signature-Based Detection) ۲۷۲
۲. تشخیص مبتنی بر رفتار خلاف قاعده (Anomaly-Based Detection) ۲۷۲
۳. تحلیل وضعیت پروتکل (Stateful Protocol Analysis) ۲۷۳
انواع تکنولوژی IDPS ۲۷۵
۱. مبتنی بر شبکه (Network-Based) ۲۷۵
۲. بی‌سیم (Wireless) ۲۷۵
۳. تحلیل رفتار شبکه (Network Behavior Analysis) ۲۷۵
۴. مبتنی بر میزبان (Host-Based) ۲۷۶
اجزای IDPS ۲۷۶
۱. سنسور یا عامل (Sensor or Agent) ۲۷۶
۲. سرور مدیریت (Management Server) ۲۷۶
۳. سرور دیتابیس (Database Server) ۲۷۷
۴. کنسول (Console) ۲۷۷
قابلیت‌های امنیتی IDPS ۲۷۷

۱. قابلیت جمع‌آوری اطلاعات (Information Gathering Capabilities) ۲۷۷
۲. قابلیت واقعه‌نگاری (Logging Capabilities) ۲۷۷
۳. قابلیت تشخیص (Detection Capabilities) ۲۷۸
۴. قابلیت پیشگیری (Prevention Capabilities) ۲۸۰
معماری شبکه و محل قرارگیری سنسور ۲۸۰
۱. برخط (Inline) ۲۸۱
۲. منفعل (Passive) ۲۸۲
مبحث چهارم؛ هانی‌پات ۲۸۳
مزایا و معایب هانی‌پات ۲۸۴
۱. مزایای استفاده از هانی‌پات ۲۸۴
۲. معایب استفاده از هانی‌پات ۲۸۴
انواع هانی‌پات ۲۸۵
۱. کم‌تعامل (Low-Interaction) ۲۸۵
۲. پرتعامل (High-Interaction) ۲۸۵
فصل نهم ارتباطات امن شبکه ۲۸۷
مبحث اول؛ IPsec ۲۸۹
کاربردهای IPsec ۲۹۰
مزایای استفاده از IPsec ۲۹۲
پروتکل‌های مورداستفاده در IPsec ۲۹۳
۱. Authentication Header (AH) ۲۹۳
۲. Encapsulating Security Payload (ESP) ۲۹۳
حالت‌های استفاده از پروتکل‌های AH و ESP ۲۹۳
۱. Transport Mode ۲۹۴
۲. Tunnel Mode ۲۹۴
سیاست امنیت IP (IP Security Policy) ۲۹۵
Security Association (SA) ۲۹۵
Security Association Database (SAD) ۲۹۶
Security Policy Database (SPD) ۲۹۸
انتخاب نوع پردازش ۲۹۹
پروتکل Encapsulating Security Payload (ESP) ۳۰۰
حالت‌های ESP ۳۰۰
فرآیند رمزنگاری در ESP ۳۰۱
فرآیند حفاظت از صحت (تمامیت) در ESP ۳۰۱
ساختار بسته ESP ۳۰۲
پروتکل IKE ۳۰۳
فاز اول IKE ۳۰۵

۱. روش Main Mode ۳۰۵
۲. روش Aggressive Mode ۳۰۸
فاز دوم IKE ۳۰۹
مبحث دوم؛ شبکه خصوصی مجازی ۳۱۱
انواع VPN ۳۱۲
انواع VPN بر اساس تکنولوژی ۳۱۲
انواع VPN بر اساس پروتکل ۳۱۲
انواع VPN بر اساس لایه OSI ۳۱۲
انواع اتصال در VPN ۳۱۳
۱. Remote Access VPN ۳۱۳
۲. Site to Site VPN ۳۱۳
مزایای استفاده از VPN ۳۱۴
پروتکل PPTP ۳۱۵
پروتکل PAP ۳۱۶
پروتکل CHAP ۳۱۶
پروتکل MS-CHAP ۳۱۶
پروتکل MPPE ۳۱۷
پروتکل L2TP ۳۱۷
پروتکل IPsec ۳۱۸
پروتکل SSL VPN ۳۱۹
۱. SSL Portal VPN ۳۲۰
۲. SSL Tunnel VPN ۳۲۰
بخش چهارم امنیت سیستم‌ها و سرویس‌ها ۳۲۱
فصل دهم امنیت وب ۳۲۳
مبحث اول؛ پروتکل SSL/TLS ۳۲۵
معماری SSL ۳۲۵
مفاهیم Session و Connection در SSL ۳۲۶
پارامترهای تعیین وضعیت Session ۳۲۷
پارامترهای تعیین وضعیت Connection ۳۲۸
پروتکل SSL Record ۳۲۹
پروتکل Change Cipher Spec ۳۳۱
پروتکل Alert ۳۳۱
پروتکل Handshake ۳۳۳
فاز اول پروتکل Handshake؛ برقراری قابلیت‌های امنیتی ۳۳۵
فاز دوم پروتکل Handshake؛ احرازهویت سرور و تبادل کلید ۳۳۷

فاز سوم پروتکل Handshake؛ احرازهویت کلاینت و تبادل کلید ۳۳۸
فاز چهارم پروتکل Handshake؛ پایان ۳۳۹
مبحث دوم؛ پروتکل HTTPS ۳۴۱
ملاحظات امنیتی وب ۳۴۲
تهدیدات امنیتی وب ۳۴۳
روش‌های امنیت ترافیک وب ۳۴۴
پروتکل HTTPS ۳۴۵
شروع اتصال ۳۴۵
بستن اتصال ۳۴۷
فصل یازدهم امنیت پست الکترونیک ۳۴۹
مبحث اول؛ پروتکل PGP ۳۵۲
نشانه‌گذاری ۳۵۳
تشریح عملیات PGP ۳۵۴
احرازهویت در PGP ۳۵۵
محرمانگی در PGP ۳۵۶
احراز هویت به همراه محرمانگی در PGP ۳۵۷
فشرده‌سازی در PGP ۳۵۸
سازگاری با پست الکترونیک ۳۵۸
کلیدهای رمزنگاری و دسته‌کلیدها ۳۵۹
مولد کلید نشست (Session Key Generation) ۳۶۰
شناسه کلید ۳۶۱
دسته‌کلید ۳۶۴
تولید پیام در PGP ۳۶۷
دریافت پیام در PGP ۳۶۸
مبحث دوم؛ پروتکل S/MIME ۳۷۱
استاندارد RFC 5322 ۳۷۱
پروتکل MIME ۳۷۳
انواع محتوا در MIME ۳۷۴
کدگذاری انتقال در MIME ۳۷۵
پروتکل S/MIME ۳۷۶
الگوریتم‌های رمزنگاری در S/MIME ۳۷۶
پیام S/MIME ۳۷۹
Enveloped Data ۳۸۰
Signed Data ۳۸۰
پردازش گواهینامه در S/MIME ۳۸۱

نقش کاربر ۳۸۱
گواهینامه VeriSign ۳۸۱

فصل دوازدهم امنیت سیستم‌عامل ۳۸۳

مبحث اول: بهترین شیوه‌های مدیریت امن سیستم ۳۸۶
امنیت فیزیکی سیستم و کنسول ۳۸۶
نصب سیستم با حداقل برنامه‌ها ۳۸۸
رمزعبور مدیر سیستم ۳۸۸
محول کردن وظایف مدیریتی ۳۸۹
رمزعبور کاربران ۳۹۰
سیستم کاربر ۳۹۱
محدود کردن کاربر ۳۹۲
آموزش کاربران ۳۹۲
به‌روزرسانی سیستم‌ها ۳۹۳
آزمون آسیب‌پذیری ۳۹۴
مانیتورینگ سیستم ۳۹۵
مستندسازی پیکربندی ۳۹۵
پشتیبان‌گیری و بازیابی فاجعه ۳۹۶
آنتی‌ویروس ۳۹۷
مبحث دوم: سطوح امنیتی در سیستم‌عامل ۳۹۸
۱. Trusted Computing Base (TCB) ۳۹۹
۲. Automatic Data Processing (ADP) ۳۹۹
بخش D: محافظت حداقلی (Minimal Protection) ۳۹۹
بخش C: محافظت اختیاری (Discretionary Protection) ۳۹۹
• کلاس C1: Discretionary Security Protection ۳۹۹
• کلاس C2: Controlled Access Protection ۴۰۱
بخش B: محافظت اجباری (Mandatory Protection) ۴۰۳
• کلاس B1: Labeled Security Protection ۴۰۳
• کلاس B2: Structured Protection ۴۰۵
• کلاس B3: Security Domains ۴۰۷
بخش A: محافظت تأییدشده (Verified Protection) ۴۰۹
• کلاس A1: Verified Design ۴۰۹
انواع کنترل دسترسی ۴۱۱
• کنترل دسترسی اختیاری (DAC) ۴۱۱
• کنترل دسترسی اجباری (MAC) ۴۱۲
• کنترل دسترسی بر مبنای نقش (Role-Based Access Control) ۴۱۲

• کنترل دسترسی بر مبنای شبکه (Lattice-Based Access Control) ۴۱۲
• کنترل دسترسی بر مبنای خصوصیت(Attribute-Based Access Control) ۴۱۳
مبحث سوم؛ بهترین شیوه‌های امنیت سیستم‌عامل ۴۱۴
۱. نصب وصله‌ها و به‌روزرسانی سیستم‌عامل ۴۱۵
۲. مقاوم‌سازی و ایمن‌سازی پیکربندی سیستم‌عامل ۴۱۶
حذف یا غیرفعال کردن سرویس‌ها، برنامه‌ها و پروتکل‌های شبکه غیرضروری۴۱۶
پیکربندی احرازهویت کاربر در سیستم‌عامل ۴۱۷
پیکربندی کنترل‌های منابع ۴۲۰
۳. نصب و پیکربندی کنترل‌های امنیتی اضافی ۴۲۰
۴. آزمون امنیت سیستم‌عامل ۴۲۲
فصل سیزدهم امنیت دیتابیس ۴۲۳
مبحث اول؛ ده تهدید برتر دیتابیس ۴۲۶
۱. امتیازات بیش‌ازحد و استفاده‌نشده ۴۲۶
۲. سوءاستفاده از امتیازات ۴۲۷
۳. تزریق وروده‌ی (SQL Injection سابق) ۴۲۷
۴. بدافزار ۴۲۸
۵. دنباله میزی ضعیف ۴۲۸
۶. در معرض خطر قرار گرفتن رسانه‌های ذخیره‌سازی ۴۲۹
۷. بهره‌برداری از آسیب‌پذیری‌ها و اشتباهات پیکربندی دیتابیس ۴۲۹
۸. دیتای حساس مدیریت نشده ۴۳۰
۹. منع خدمت ۴۳۰
۱۰. تخصص و آموزش امنیتی محدود ۴۳۱
مبحث دوم؛ روش‌های مقابله با تهدیدات ۴۳۲
استراتژی دفاعی چندلایه برای امنیت دیتابیس ۴۳۲
۱. کشف و ارزیابی (Discovery and Assessment) ۴۳۴
۲. مدیریت حقوق کاربر (User Rights Management) ۴۳۶
۳. نظارت و مسدودسازی (Monitoring and Blocking) ۴۳۷
۴. حسابرسی (Auditing) ۴۳۹
۵. حفاظت از اطلاعات (Data Protection) ۴۳۹
۶. امنیت غیر فنی (Non-Technical Security) ۴۴۰
بخش پایانی ضمائم ۴۴۱
منابع ۴۴۳
معرفی کتاب ۴۴۵