



سرشناسه : مدیری، ناصر، ۱۳۴۱ -  
 عنوان و نام پدیدآور : امنیت سایت شبکه / تالیف و تدوین ناصر مدیری، فرشته جدیدی میاندشتی.  
 مشخصات نشر : تهران: مهرگان قلم، ۱۳۹۵.  
 مشخصات ظاهری : ۲۰۶ ص.؛ مصور.  
 شابک : ۹۷۸-۶۰۰-۶۲۳۶-۹۲-۶  
 وضعیت فهرست نویسی: فیا  
 یادداشت : کتاب حاضر اولین بار تحت عنوان "مهندسی امنیت سایت های کامپیوتری : مرجعی برای درس شبکه های کامپیوتری" توسط همین انتشارات در سال ۱۳۹۱ منتشر شده است.  
 یادداشت : واژه نامه.  
 یادداشت : کتابنامه.  
 عنوان دیگر : مهندسی امنیت سایت های کامپیوتری : مرجعی برای درس شبکه های کامپیوتری .  
 موضوع : شبکه های کامپیوتری — تدابیر ایمنی  
 نوع : Computer networks — Security measures  
 شتاد افزوده : جدیدی میاندشتی، فرشته، ۱۳۴۸ -  
 بندی کنگره : TK۵۱۰/۵۹/م۴م۹ ۱۳۹۵  
 رده بندی دیسی : ۰۰۵/۸  
 شماره کتبشناسی : ۴۵۸۶۰۷۳

نام کتاب : امنیت سایت شبکه

مولف : ناصر مدیری - فرشته جدیدی میاندشتی

ناشر: مهرگان قلم

نوبت چاپ اول: زمستان ۹۵

شابک: ۹۷۸-۶۰۰-۶۲۳۶-۹۲-۶

تیراژ: ۵۰۰

قیمت: ۲۱۰۰۰ تومان



Mehregane Ghalam

مرکز پخش

انتشارات مهرگان قلم:

تهران - میدان انقلاب - خیابان کارگر جنوبی - بعد از خیابان وحید نظری - کوچه گشتاب - پلاک ۷ واحد ۲

تلفن تماس: ۰۹۱۲۳۱۴۶۰۵۸ - ۶۶۴۷۷۲۲۴-۵

پیشگفتار

ن وَالْقَلَمِ وَمَا يَسْطُرُونَ

حضرت حق را سپاس که با الطاف بیکران خود این توفیق را بر ما ارزانی داشت تا کتابی را در جهت یکی اساسی‌ترین مباحث مهندسی کامپیوتر و در راه ارتقای دانش و فرهنگ این مرز و بوم به تألیف برسانیم. در سال‌های نه چندان دور، کمتر کسی می‌توانست توصیفی از مفهوم "شبکه‌های کامپیوتری" ارائه دهد و پیش‌بینی این موضوع بسیار دشوار بود که بعد از مدتی، شبکه‌های کامپیوتری به عنصر حیاتی و کلیدی در زندگی بشر تبدیل شوند.

اهمیت شبکه‌های زمانی احساس می‌شود که، این سوال پیش بیاید که با قدرت امروزی کامپیوترهای شخصی ما چرا شبکه‌ها ساخته می‌کنیم؟ جواب این سوال در یک جمله می‌تواند خلاصه شود: افزایش بهروری و کاهش هزینه‌ها. برای حصول این اطمینان نیازمند بکارگیری در تمام مراحل کار جهت اطلاع از چگونگی روند پیشرفت و تولید محصولی با کیفیت داریم. هزینه کمتر هستیم. هدف شبکه‌های کامپیوتری امروزی، بیشتر به اشتراک گذاشتن اطلاعات و ایجاد امکان کارگروهی است و لذا علاوه بر صرفه جویی در هزینه، در وقت نیز صرفه جویی شده و حس یگانگی گروهی را در مسیر اهداف مشخص در سازمان به وجود می‌آورد.

این کتاب شامل هفده فصل و پنج مجیم است که با رویکردی خلاقانه جهت فراگیری مباحث مربوط به شبکه‌های کامپیوتری گردآوری شده است.

در فصول اولیه‌ی این کتاب، سعی بر آن شده است که مفاهیم، اصول، پیش‌نیاز و تکنیک‌های مورد نیاز و دلایل نیازمندی به علم شبکه‌های کامپیوتری بپردازیم. با توجه به توجهی دامنه‌ی کاری شبکه‌ها، یکی از دغدغه‌های اغلب سازمان‌ها ایجاد هماهنگی بین انواع سیستم‌های موجود و انتقال مسترده از شبکه‌ها در تمامی کارهای سازمانی اداری می‌باشد. از این رو در فصول بعد مباحث محوری از جمله انتقال داده‌ها، امنیت شبکه‌ها، امنیت داده‌ها، اطلاعات و مدیریت شبکه‌های کامپیوتری و... مطرح شده است.

سرفصل‌های این کتاب بگونه‌ای است که دانشجویان بتوانند مطالب مربوط به امنیت سایه‌های کامپیوتری را فرا گرفته و از مقالات متعددی در این زمینه بهره برده و تحقیقات خود را در صورت تمایل آغاز نمایند.

با توجه به گستردگی این مباحث، در پایان هر فصل منابعی جهت مطالعه‌ی بیشتر آورده شده است. خصوصیت بارز این کتاب، سادگی بیان به همراه استفاده از شکل‌ها و جداول و طرح سوالاتی برای سنجش میزان یادگیری خود در جهت درک بهتر مفاهیم هر بحث است.

مطالب مطرح شده در هر فصل:

- فصل اول، دیدگاهی کلی از فضای سایبر، جنگ سایبر و ویژگیهای آن را به همراه راهکارهای پیشنهادی برای حفظ امنیت این فضا، بیان کرده است.
- فصل دوم، به بیان مفاهیم پایه‌ای مربوط به ویروس‌ها و عوامل انتقال و راههای تشخیص و مقابله با آنها (بدون عنوان یکی از عوامل تهدید کننده سایت‌ها) پرداخته است.
- فصل سوم، قوانین طلایی طراحی یک شبکه امن را برشمرده است.

- فصل چهارم، حاوی نکاتی پیرامون ایمن سازی اطلاعات و شبکه‌های کامپیوتری می‌باشد.
  - فصل پنجم، روشهای افزایش امنیت در سیستم عامل Windows (به عنوان پر کاربردترین سیستم عامل) را شامل می‌شود.
  - فصل ششم، در این فصل معیارهای انتخاب مناسب تجهیزات مورد استفاده در سایت مطرح شده است. تجهیزاتی از قبیل: روترها، سوئیچ ها، سرورها و دیوارهای آتش.
  - فصل هفتم، در این فصل روش‌های مختلف تهاجم به یک سیستم انواع حملات DoS و راه‌های پیشگیری از بروز آن مطرح شده است.
  - فصل هشتم، به امنیت مراکز سرور توجه کرده است و بحث آن پیرامون تهدیدات مراکز سرور، مراحل برقراری امنیت، تدابیر پیشگیرانه و مفهوم پدافند غیرعامل می‌باشد.
  - فصل نهم، وابستگی پیرامون امنیت فیزیکی سایت ارائه شده است.
- امید است این کتاب بتواند به حرمت دانشجویان رشته‌های مختلف علوم کامپیوتر قرار گیرد. در خاتمه بر خود لازم می‌دانیم از تمامی عزیزانی که به نوعی در گردآوری مطالب این کتاب ما را یاری رساندند کمال تشکر و قدردانی را بعمل آوریم. بی‌صبرانه منتظر نظرات، انتقادات و پیشنهادات شما هستیم. پست الکترونیکی انعکاس نظرات:

[info@27000.Ir](mailto:info@27000.Ir)

[www.27000.Ir](http://www.27000.Ir)

ناصر مدیری - فرشته جدیدی می‌اندشتی

|    |                                               |
|----|-----------------------------------------------|
| 14 | 1. فضای سایبر                                 |
| 14 | 1.1. خلاصه فصل                                |
| 15 | 1.2. فضای سایبر                               |
| 15 | 1.3. ویژگی‌های فضای سایبر                     |
| 16 | 1.3.1. تعریف جنگ سایبر                        |
| 17 | 1.3.2. جنگ‌های اطلاعاتی نهفته در جنگ سایبر    |
| 17 | 1.3.3. اهداف و محصولات عملیات سایبری          |
| 18 | 1.3.4. نفوذگران و اهداف آنها                  |
| 19 | 1.3.5. تاثیرات جنگ‌های سایبری                 |
| 19 | 1.3.6. نمونه جنگ‌های سایبر                    |
| 21 | 1.4. ملزومات امنیت فضای سایبر                 |
| 22 | 1.5. چالش‌های ناشی از تهدیدات فضای سایبر      |
| 23 | 1.6. دلایل نفوذپذیری سایت‌ها                  |
| 25 | 1.7. راهکارهای پیشنهادی برای امنیت فضای سایبر |
| 27 | 1.8. سوالات متداول                            |
| 28 | 1.9. منابعی برای مطالعه بیشتر                 |
| 30 | 2. تاثیر ویروس‌های کامپیوتری                  |
| 30 | 2.1. خلاصه فصل                                |
| 31 | 2.2. مقدمه                                    |
| 34 | 2.3. برنامه‌های مخرب                          |
| 35 | 2.4. تاریخچه ویروس                            |
| 38 | 2.5. انواع ویروس‌ها                           |
| 39 | 2.6. افسانه ویروس‌های مثبت                    |
| 40 | 2.7. عوامل انتقال ویروس                       |
| 41 | 2.8. شناسایی و مقابله با ویروس‌ها             |
| 42 | 2.9. راه‌های تشخیص به آلودگی ویروس            |
| 42 | 2.10. راه‌های جلوگیری از ابتلا به ویروس       |
| 45 | 2.11. سوالات متداول                           |
| 45 | 2.12. منابعی برای مطالعه بیشتر                |

|    |                                               |
|----|-----------------------------------------------|
| 48 | 3. قوانین طلایی طراحی شبکه‌های محلی کامپیوتری |
| 48 | 3.1 خلاصه فصل                                 |
| 49 | 3.2 مقدمه                                     |
| 49 | 3.3 ویژگی‌های عمومی یک شبکه خوب               |
| 49 | 3.3.1 تامین نیازمندیها                        |
| 51 | 3.3.2 کارآیی                                  |
| 51 | 3.3.3 انعطاف پذیری                            |
| 52 | 3.3.4 قابلیت رشد و تغییر                      |
| 53 | 3.3.5 قابلیت مدیریت                           |
| 53 | 3.3.6 امنیت                                   |
| 53 | 3.3.7 برهم خرابیها                            |
| 54 | 3.3.8 ترمیم آسیب‌های جدی                      |
| 55 | 3.3.9 هزینه                                   |
| 55 | 3.4 پارامترهای طراحی                          |
| 55 | 3.4.1 نوع خدمات                               |
| 56 | 3.4.2 استراژی‌ها                              |
| 57 | 3.4.3 پارامترهای کمی                          |
| 59 | 3.5 روش طراحی شبکه                            |
| 62 | 3.6 تجهیزات                                   |
| 63 | 3.7 سوالات متداول                             |
| 63 | 3.8 منابعی برای مطالعه بیشتر                  |
| 66 | 4. ایمن‌سازی اطلاعات و شبکه‌های کامپیوتری     |
| 66 | 4.1 خلاصه فصل                                 |
| 67 | 4.2 تهدیدات امنیتی                            |
| 67 | 4.3 مراحل پیاده سازی امنیت                    |
| 68 | 4.4 تشکیلات اجرایی امنیت                      |
| 70 | 4.5 راهکارهای امنیتی                          |
| 70 | 4.5.1 سرویس‌های امنیتی                        |
| 70 | 4.5.2 مکانیزم‌های امنیتی                      |
| 70 | 4.5.3 تجهیزات امنیتی                          |

|     |                                                       |
|-----|-------------------------------------------------------|
| 71  | 4.6 معماری امنیتی                                     |
| 71  | 4.7 استاندارد BS7799                                  |
| 73  | 4.8 نتیجه گیری                                        |
| 73  | 4.9 سوالات متداول                                     |
| 74  | 4.10 منابعی برای مطالعه بیشتر                         |
| 76  | <b>5_ افزایش امنیت سیستم عامل WINDOWS</b>             |
| 76  | 5.1 خلاصه فصل                                         |
| 77  | 5.2 فعال سازی مرکز امنیت در Windows                   |
| 77  | 5.2.1 به روز رسانی Windows                            |
| 78  | 5.2.2 Window Firewall                                 |
| 78  | 5.2.3 استفاده از نرم افزار آنتی ویروس                 |
| 79  | 5.3 آشکار کردن حساب های کاربری معین                   |
| 80  | 5.4 کلمه عبور محرمانه به صورت خودکار                  |
| 80  | 5.5 دسترسی به برنامه های محدود شده از سایر حساب ها    |
| 80  | 5.6 اجرای برنامه ها با مجوز Administrator             |
| 81  | 5.7 امن کردن فایل سیستم                               |
| 82  | 5.8 خطرهای پنهان. (Alternate Data Stream) ADS         |
| 83  | 5.9 رمزنگاری                                          |
| 84  | 5.10 تنظیم کلمه عبور در Screen Saver                  |
| 84  | 5.11 تنظیم سرویس گیرنده زمان                          |
| 84  | 5.12 SCM                                              |
| 85  | 5.13 افزایش اندازه فایل ثبت رویدادها                  |
| 86  | 5.14 کنترل فایل ها و پوشه های به اشتراک گذاشته شده    |
| 86  | 5.15 تنظیمات امنیتی برای Client                       |
| 109 | 5.16 چند قانون امنیتی                                 |
| 111 | 5.17 نتیجه گیری                                       |
| 111 | 5.18 سوالات متداول                                    |
| 112 | 5.19 منابعی برای مطالعه بیشتر                         |
| 114 | <b>6_ شاخص ها و معیارهای انتخاب تجهیزات سرمایه ای</b> |
| 114 | 6.1 خلاصه فصل                                         |

|     |                                                   |
|-----|---------------------------------------------------|
| 115 | 6.2 شاخص ها و معیارهای انتخاب روتر                |
| 115 | 6.2.1 پروتکل ها و الگوریتمهای مسیریابی            |
| 118 | 6.2.2 مدل سلسله مراتبی Cisco برای Internetworking |
| 119 | 6.2.3 مزایای مدل سلسله مراتبی                     |
| 120 | 6.3 شاخص ها و معیارهای انتخاب سوئیچ               |
| 123 | 6.4 شاخص ها و معیارهای انتخاب سرور                |
| 126 | 6.5 شاخص ها و معیارهای انتخاب دیوار آتش           |
| 130 | 6.6 سوالات متداول                                 |
| 130 | 6.7 منابعی برای مطالعه بیشتر                      |
| 132 | 7. روند حملات نایبر: DOS                          |
| 132 | 7.1 خلاصه فصل                                     |
| 133 | 7.2 مقدمه                                         |
| 134 | 7.3 حملات                                         |
| 135 | 7.4 حملات DoS و DDoS                              |
| 136 | 7.5 انواع حملات DoS                               |
| 138 | 7.6 هدف از این نوع حملات                          |
| 140 | 7.7 حملات DoS یا DDoS                             |
| 140 | 7.8 نحوه پیشگیری از حملات                         |
| 140 | 7.9 ابزارهای پیشگیری از حملات DoS                 |
| 141 | 7.10 عملیاتی بعد از بروز تهاجم                    |
| 141 | 7.11 حملات DoS                                    |
| 142 | 7.12 نتیجه گیری                                   |
| 142 | 7.13 سوالات متداول                                |
| 143 | 7.14 منابعی برای مطالعه بیشتر                     |
| 146 | 8. تهدیدات مراکز سرور                             |
| 146 | 8.1 خلاصه فصل                                     |
| 147 | 8.2 تهدیدات مراکز سرور                            |
| 147 | 8.3 مراحل برقراری امنیت                           |
| 148 | 8.4 امنیت مراکز سرور                              |
| 148 | 8.5 امنیت دسترسی فیزیکی                           |

|     |                                                              |
|-----|--------------------------------------------------------------|
| 150 | 8.5.1 امنیت محلی                                             |
| 151 | 8.5.2 امنیت شبکه                                             |
| 152 | 8.5.3 ساختار امنیتی سایت و مراکز سرور                        |
| 153 | 8.5.4 Protocol Analyzers                                     |
| 154 | 8.5.5 Routing                                                |
| 155 | 8.5.6 دیوار آتش                                              |
| 157 | 8.5.7 AntiSniffing                                           |
| 158 | 8.5.8 سیستم عامل                                             |
| 159 | 8.5.9 AntiSniffing                                           |
| 161 | 8.5.10 Web Operating System                                  |
| 161 | 8.5.11 Encryption                                            |
| 163 | 8.5.12 تاثیر روال ادارتی بر امنیت سایت                       |
| 164 | 8.6 تشکیلات اجرایی امنیت                                     |
| 166 | 8.7 تدابیر پیشگیرانه                                         |
| 166 | 8.7.1 طراحی ایمن مراکز داده                                  |
| 168 | 8.8 پدافند غیرعامل                                           |
| 169 | 8.8.1 ضرورت وجود پدافند غیرعامل                              |
| 169 | 8.8.2 پدافند غیرعامل در محیط IT                              |
| 170 | 8.8.3 تدابیر فیزیکی پدافند غیرعامل در محیط سایتهای کلاه سفید |
| 174 | 8.9 سوالات متداول                                            |
| 174 | 8.10 منابعی برای مطالعه بیشتر                                |
| 176 | 9. امنیت فیزیکی سایت                                         |
| 176 | 9.1 خلاصه فصل                                                |
| 177 | 9.2 مقدمه                                                    |
| 177 | 9.3 ضوابط امنیتی در ساختار سایت، تجهیزات و منابع             |
| 177 | 9.4 انتخاب صحیح محل ساختمان مرکز داده                        |
| 178 | 9.4.1 تدابیر امنیتی در ساختمان سایت                          |
| 179 | 9.4.2 خنک سازی، تهویه هوا و رطوبت                            |
| 180 | 9.4.3 کشف و اطفاء حریق                                       |
| 180 | 9.4.4 منبع تغذیه و برق                                       |

|     |                                                        |
|-----|--------------------------------------------------------|
| 182 | 9.4.5 استفاده از سیستم‌های نظارتی                      |
| 182 | 9.4.6 محافظت در برابر سیل                              |
| 182 | 9.4.7 امنیت کابل‌ها                                    |
| 183 | 9.4.8 امنیت Rack                                       |
| 183 | 9.5 تامین امنیت فیزیکی توسط افراد                      |
| 183 | 9.5.1 ابزارهای کنترل دسترسی                            |
| 185 | 9.5.2 دسترسی مجاز و سطوح آن                            |
| 186 | 9.5.3 دادن آگاهی امنیتی به کارکنان در حدود وظایف هر یک |
| 186 | 9.5.4 ممانعت از ورود مواد غذایی به مرکز داده           |
| 186 | 9.5.5 تمیز کردن بیت                                    |
| 188 | 9.5.6 پاکسازی رسانه‌ها و اسناد، قبل از انهدام          |
| 188 | 9.5.7 تهیه و نگهداری نسخه پشتیبان در مکانی امن         |
| 189 | 9.6 سوالات متداول                                      |
| 189 | 9.7 منابعی برای مطالعه بیشتر                           |
| 191 | ضمائم                                                  |
| 192 | ضمیمه اول                                              |
| 192 | واژگان و عبارات                                        |
| 197 | ضمیمه دوم                                              |
| 197 | فهرست علائم اختصاری                                    |