بسم الله الرحمن الرحیم

امنیت شبکه

تألیف و تدوین:
دکتر ناصر مدیری
مهندس مهرداد جنگجو

Publication Mehregane Ghalam

شابک : ۹۷۸-۶۰۰-۸۷۲۶-۰۹-۸؛
شماره کتابشناسی ملی : ۴۶۱۹۹۶۳
عنوان و نام پدیدآور : امنیت شبکه/ تالیف و تدوین ناصر مدیری، مهرداد جنگجو.
مشخصات نشر : تهران: مهرگان قلم.
مشخصات ظاهری : ۲۹۶ ص.: مصور.
یادداشت : کتابنامه.
موضوع : شبکه‌های کامپیوتری -- تدابیر ایمنی
موضوع : Computer networks -- Security measures
موضوع : کامپیوترها -- ایمنی اطلاعات
موضوع : Computer security
رده بندی دیویی : ۰۰۵/۸
رده بندی کنگره : ۱۳۹۵ ۸الف۴م/۵۹/TK۵۱۰
شناسه : مدیری، ناصر، ۱۳۴۱ -
شناسه افزوده : جنگجو، مهرداد، ۱۳۶۳ -
وضعیت فهرست نویسی : فیپا

نام کتاب : امنیت شبکه

مولف : ناصر مدیری - مهرداد جنگجو

ناشر: مهرگان قلم

نوبت چاپ اول: زمستان ۹۵

شابک: ۹۷۸-۶۰۰-۸۷۲۶-۰۹-۸

تیراژ: ۵۰۰

قیمت: ۳۰۰۰۰ تومان

Mehregane Ghalam

مرکز پخش

انتشارات مهرگان قلم:
تهران - میدان انقلاب - خیابان کارگرجنوبی - بعد از خیابان وحید نظری - کوچه گشتاب-پلاک۷ واحد۲
تلفن تماس: ۵-۶۶۴۷۷۲۲۴ - ۰۹۱۲۳۱۴۶۰۵۸

WWW.MEHREGANEGHALAM.COM

پیشگفتار

ن و القَلَمِ وَ ما یَسطُرُونَ

سه دشواری در کار تالیف وجود دارد:

نوشتن چیزی که قابل نشر باشد،

یافتن مرد شریفی که آنرا نشر دهد،

پیدا کردن مردان و زنان حساس و نکته سنجی که آنرا بخوانند!!

((کولتون))

به نام هستی بخش دانا

تاکنون کتب متعددی در زمینه امنیت شبکه های کامپیوتری در کشور تالیف و ترجمه شده است ولی تا به امروز کتابی که کلیه مباحث پیشرفته در امنیت شبکه های کامپیوتری را به طور جامع شامل شود و مطالب را با علم روز دنیا نیز باشد در دسترس نبوده است. پرداختن به مطالب کلیدی و به روز در زمینه امنیت شبکه های کامپیوتری به نحوی که خواننده را به طریقی کاملا ساده، روان و تخصصی تا انتها همراه خود کند از هم دغدغه های مولفین این کتاب بوده است.

فصول کتاب " مهندسی امنیت شبکه های کامپیوتری" در راستای نیل به اهداف ذکر شده به نحوی کاملا مستقل و در عین حال از نظر مفهوم به هم پیوسته مطرح شده است.

چارچوب کتاب حاضر بگونه ای سازماندهی شده است که:

1- تهدیدات، نفوذپذیری و حملات در شبکه های کامپیوتری را بررسی می کند.

2- ویروس ها، کرم ها و بد افزارها در شبکه های کامپیوتری را مطرح می کند.

3- تجهیزات تامین امنیت IDS, IPS, Firewall, UTM و ... و در شبکه های کامپیوتری شرح می دهد.

این کتاب شامل سیزده فصل و چهار ضمیمه است که با رویکردی خلاقانه جهت فراگیری مباحث مربوط به حوزه‌ی مهندسی امنیت شبکه های کامپیوتری گردآوری شده است. در فصول اولیه‌ی این کتاب، سعی بر آن شده است تا انواع تهدیدات در شبکه های کامپیوتری و مدیریت آن تشریح شود.

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 مثالهای ملموس جهت درک بهتر مفاهیم در هر مبحث است.

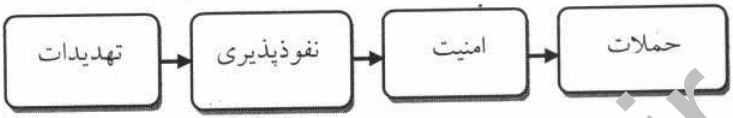
مطالب مطرح شده در هر فصل:

- *فصل اول*، معرفی انواع تهدیدات علیه امنیت شبکه‌های کامپیوتری و روشهای مقابله با این آسیب پذیری ها را بررسی کرده است.
- *فصل دوم*، انواع حملات هکرها و ابزارهای تست نفوذپذیری شبکه‌های کامپیوتری شرح داده می شود.
- *فصل سوم*، مفاهیم امنیت شبکه و راهکارهای امنیتی را معرفی کرده است.
- *فصل چهارم*، انواع حملات در شبکه‌های کامپیوتری و پورتهای استفاده شده در حملات DOS مورد بررسی قرار می گیرد.
- *فصل پنجم*، ویروس‌ها، شبکه‌های کامپیوتری و ترفند های افزایش امنیت سیستم را معرفی می کنیم.
- *فصل ششم*، اسبهای تراوا و راه های ورود آنها و خسارت های وارده به سیستم توسط آنها به طور کامل بررسی می شود.
- *فصل هفتم*، خطرناک ترین کرم‌ها و روش های مقابله با انتشار آنها بیان گردیده است.
- *فصل هشتم*، جاسوس افزارها و چگونگی سرقت اطلاعات شما توسط بد افزارها معرفی شده است.
- *فصل نهم*، طرز کار ضد ویروسها و ویژگی های یک ضد ویروس خوب تحت شبکه بیان شده است.
- *فصل دهم*، انواع دیواره آتش، وظایف کلی آنها و روشهای پیاده سازی آنها در شبکه‌های کامپیوتری گرداوری شده است.
- *فصل یازدهم*، انواع UTM، ویژگی های یک UTM خوب، سخت افزار و سیستم عامل آنها مطرح می شود.
- *فصل دوازدهم*، انواع رمزنگاری و تفاوت رمزنگاری با امضاء دیجیتال و... را مورد بررسی قرار می دهد.

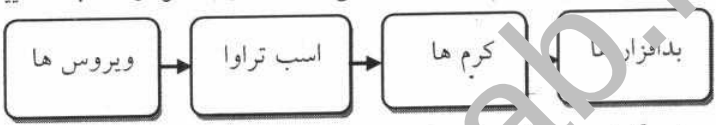
- *فصل سیزدهم*، معماری و ساختمان HONEY POT و مزایا و معایب آن را شرح داده شده است.

راهنمایی جهت مطالعه کتاب:

برای آشنایی با مفاهیم امنیت، فصل‌ها را مطابق با نمودار 1 دنبال نمایید.



برای آشنایی با مفاهیم بدافزارها، فصل‌ها را مطابق با نمودار 2 دنبال نمایید.



برای آشنایی با پارامترهای این امنیت، فصل‌ها را مطابق با نمودار 3 دنبال نمایید.

امید است این کتاب بتواند در خدمت دانشجویان رشته‌های مختلف علوم کامپیوتر قرار گیرد.

همچنین لازم می دانیم از سرکار خانم الهام حسن‌عامری و سرکار خانم فریده لطفی که زحمات آماده سازی این کتاب را برعهده گرفتند تشکر نمایم. 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
www.27000.Ir
ناصر مدیری – مهرداد جنگجو

فهرست مطالب

۱. تهدیدات در شبکه‌های کامپیوتری 20
1.1.خلاصه فصل 20
1.2.مقدمه 20
1.3.مروری بر مدل TCP/IP 21
1.4.تهدیدات علیه امنیت شبکه 21
1.5.راهکارهای امنیتی 22
1.6.الگوی امنیتی 27
1.6.1.الگوریتم جهت تهیه الگوی امنیتی شبکه 27
1.6.2.امنیت کاربردها 28
1.6.3.طبقه‌بندی اطلاعات 28
1.6.4.ایمن‌سازی اطلاعات 29
1.6.5.رمزنگاری اطلاعات شبکه 29
1.6.6.افزونگی اطلاعات 29
1.6.7.رمزنگاری سخت دیسک 30
1.6.8.تصدیق هویت 30
1.7.امن‌سازی نرم‌افزار 30
1.8.امن‌سازی هسته سیستم‌عامل 31
1.8.1.امنیت مجوزها 31
1.8.2.مدیریت به روز رسانی‌های امنیتی 31
1.8.3.ممیزی و نظارت بر حوادث امنیتی سیستم‌عامل 32
1.9.مقابله با آسیب‌پذیری‌های امنیت سازمانی 32
1.9.1.برنامه‌ای برای حفاظت از فضای امنیت سازمانی 32
1.9.2.پیشگیری 32
1.9.3.تشخیص 33

1.9.4.واکنش 33
1.9.5.بازیابی 33
1.10.نتیجه گیری 33
1.11.سؤالات متداول 34
1.12.منابعی برای مطالعه بیشتر 34
۲. نفوذ پذیری شبکه های کامپیوتری 38
2.1.خلاصه فصل 38
2.2.مقدمه 39
2.3.معرفی 40
2.4.دسته‌بندی هکر 40
2.5.حملات هکرها 41
2.6.موارد مورد نیاز هکر 41
2.7.تست نفوذپذیری 42
2.7.1.چرا تست نفوذپذیری 43
2.7.2.تفاوت بین تست‌ها 43
2.8.ابزارهای تست نفوذپذیری 47
2.8.1.Flexible 47
2.8.2.POWERFUL 47
2.8.3.Portable 48
2.8.4.Easy 48
2.8.5.Free 48
2.8.6.Nmap 48
2.8.7.Noise (excess traffic) 48
2.9.نتیجه گیری 49
2.10.سوالات متداول 49

2.11.منابعی برای مطالعه بیشتر 49

۳. امنیت شبکه های کامپیوتری 52

3.1.خلاصه فصل 52

3.2.مقدمه 53

3.3.مفاهیم امنیت شبکه 53

3.3.1.منابع شبکه 54

3.3.2.حمله 54

3.3.3.تحلیل خطر 55

3.3.4.سیاست امنیتی 56

3.3.5.طرح امنیت شبکه 56

3.3.6.نواحی امنیتی 57

3.4.راهکارهای امنیتی 58

3.5.نتیجه گیری 59

3.6.سؤالات متداول 60

3.7.منابعی برای مطالعه بیشتر 60

۴. حملات در شبکه های کامپیوتری 62

4.1.خلاصه فصل 62

4.2.مقدمه 62

4.3.وظیفه یک سرویس دهنده 64

4.4.سرویس‌های حیاتی و موردنیاز 65

4.5.پروتکل‌های مورد نیاز 66

4.6.غیرفعال نمودن پروتکل‌ها و سرویس‌های غیرضروری 67

4.7.حملات 68

4.8.مجاور 69

4.9.خودی 69
4.10.توزیعی 69
4.11.حملات فعال و غیر فعال 70
4.12.متداولترین پورت‌های استفاده شده در حملات DoS 74
4.13.حملات از نوع Back door 74
4.14.نتیجه گیری 76
4.15.سؤالات متداول 78
4.16.منابعی برای مطالعه بیشتر 78
۵. ویروس های شبکه‌های کامپیوتری 80
5.1.خلاصه فصل 80
5.2.مقدمه 80
5.3.تروجان Zlob-IO 80
5.4.تروجان Harnig-S 82
5.5.تروجان Dloadr-UP 83
5.6.کرم Rbot-DDJ 84
5.7.تروجان Kango-C 86
5.8.کرم W32/Sdbot-TB 88
5.9.ترفند افزایش امنیت سیستم 90
5.10.نتیجه گیری 99
5.11.سؤالات متداول 100
5.12.منابعی برای مطالعه بیشتر 100
۶. اسب های تراوا شبکه های کامپیوتری 102
6.1.خلاصه فصل 102
6.2.مقدمه 102

6.3.تاریخچه تروجان‌ها 103
6.4.اسب تروا (تروجان)..... 104
6.5.اسب تراوای ثروتمند 105
6.6.راههای ورود اسب تراوا 105
6.7.خسارت‌ها وآسیب‌های وارده به سیستم توسط اسب‌های تراوا..... 106
6.8.چگونگی آلودگی به اسب‌های تراوا..... 106
6.9.اسب‌های تروا چگونه کار می‌کنند؟ 107
6.10.راههای مقابله با اسب‌های تراوا..... 110
6.11.نتیجه گیری..... 113
6.12.سؤالات متداول 114
6.13.منابعی برای مطالعه بیشتر 114

۷. کرم های شبکه های کامپیوتری..... 116
7.1.خلاصه فصل 116
7.2.مقدمه 117
7.3.کرم چیست؟..... 118
7.4.تبدیل یک کرم به پول..... 118
7.5.فرشته کرم‌ها، کرم‌هایی با اهداف خوب 119
7.6.خطرناک‌ترین و شایع‌ترین کرم‌ها 119
7.7.پیشگیری از آلودگی به کرم‌های کامپیوتری خطرناک 121
7.8.گسترش کرم اینترنتی 121
7.9.سیر و تحولات در مسیرکرم‌های آلوده‌کننده رایانه‌ای 122
7.10.معیارهای مؤثر بر سرعت انتشار کرم‌ها 126
7.11.تأثیر تعداد سیستم‌های آلوده‌ی اولیه..... 126
7.12.کم کردن مهلت‌های زمانی 127

7.13.قابلیت پردازش موازی 127
7.14.ترکیب پردازش موازی و کاهش مهلت زمانی 128
7.15.روشی برای مقابله با انتشار کرم‌ها 128
7.16.مدل‌های قدیمی انتشار کرم‌ها 130
7.17.روش قرنطینه‌ی پویا 131
7.18.نتیجه گیری 133
7.19.سؤالات متداول 134
7.20.منابعی برای مطالعه بیشتر 134

8. بدافزارها در شبکه های کامپیوتری 136
8.1.خلاصه فصل 136
8.2.مقدمه 136
8.3.جاسوس‌افزارها اطلاعات شما را سرقت می‌کنند 137
8.4.Scarewareها، باج‌گیرهای اینترنتی 138
8.5.اسب‌های تروجان 138
8.6.کرم‌های شبکه 139
8.7.ویروس 140
8.8.ویروس‌ها چگونه کار می کنند 140
8.9.نتیجه‌گیری 145
8.10.سؤالات متداول 149
8.11.منابعی برای مطالعه بیشتر 149

9. ضد ویروس ها در شبکه های کامپیوتری 152
9.1.خلاصه فصل 152
9.2.مقدمه 153
9.3.طرز کار آنتی ویروس 153

9.4.ویژگی‌های یک آنتی‌ویروس خوب تحت شبکه 154
9.5.شناسایی ویروس‌ها 155
9.6.چه موقع ویروس‌ها را شناسایی می‌کند؟ 156
9.7.تکنیک‌های عمومی نرم‌افزارهای آنتی‌ویروس 157
9.8.تکنیک حفاظت از ارتباطات اینترنتی 159
9.9.آنتی‌ویروس‌های قلابی 160
9.10.برنامه‌های ضد ویروس 161
9.10.1 ESAFE DESKTOP 161
9.10.2 COMMAND ANTIVIRUS 161
9.10.3 MCAFEE VIRUSSCAN 162
9.10.4 SOPHOS ANTI-VIRUS 163
9.10.5 SYMANTEC NORTON 164
9.10.6 TREND MICRO PC-CILLIN 164
9.10.7 Kaspersky Small Office Security 165
9.11.نتیجه گیری 167
9.12.سؤالات متداول 167
9.13.منابعی برای مطالعه بیشتر 168

۱۰. دیوار آتش در شبکه های کامپیوتری 170
10.1.خلاصه فصل 170
10.2.مقدمه 170
10.3.دیواره آتش 172
10.4.تاریخچه دیواره‌های آتش 173
10.5.وظایف کلی دیواره آتش 177
10.6.توانایی‌های دیواره‌های آتش 178

10.7.ناتوانی‌های دیواره های آتش 180
10.8.انواع دیواره‌های آتش 182
10.9.روشهای مختلف پیادهسازی دیواره آتش 184
10.10.فیلتر بستهها 184
10.11.بررسی Stateful 185
10.12.فیلتر در سطح برنامههای کاربردی 185
10.13.مشکلات Packet Filter 186
10.14.Circuit-Level Gateways 186
10.15.Application Proxies 187
10.16.NAT 188
10.17.چند نکته درباره امنیت دیواره آتش 188
10.18.دیواره آتش لینوکس 191
10.19.نتیجه‌گیری 195
10.20.سؤالات متداول 195
10.21.منابعی برای مطالعه بیشتر 196

۱۱. UTM در شبکه های کامپیوتری 198
11.1.خلاصه فصل 198
11.2.مقدمه 198
11.3.مدل امنیت لایه‌بندی شده 200
11.4.UTM 201
11.5.مشخصه های یک UTM خوب 202
11.6.Firewall 202
11.7.Intrusion Detection/Prevention 204
11.8.شبکه اختصاصی مجازی 204

11.9.آنتی‌ویروس 205
11.10.آنتی اسپم 206
11.11.فیلترینگ 207
11.12.مدیریت پهنای باند 207
11.13.Web Caching 207
11.14.سیستم‌عامل UTM 208
11.15.سخت‌افزار تشکیل دهنده UTM 208
11.16.نتیجه گیری 209
11.17.سؤالات متداول 210

۱۲. رمزنگاری در شبکه‌های کامپیوتری 212
12.1.خلاصه فصل 212
12.2.مقدمه 212
12.3.رمزنگاری 213
12.4.تفاوت رمزنگاری با امضای دیجیتال 213
12.5.نحوه عملکرد رمزنگاری 214
12.5.1. الگوریتم‌ها 215
12.5.2. کلیدها در رمزنگاری 219
12.6.شکستن کلیدهای رمزنگاری 221
12.7.حملات متداول و راه‌حل‌های ممکن 222
12.8.خطرات تحمیلی رمزها 223
12.9.متداول‌ترین خطاها در پشتیبانی رمزها 226
12.10.چگونه یک رمز ایمن را انتخاب کنید؟ 227
12.11.چگونه رمزها را حفظ کنیم؟ 228
12.12.راه‌حلهای ممکن 229

12.12.1 الگوریتم MD5 231
12.12.2. پروتکل SSL 234
12.13.نتیجه گیری 239
12.14.سؤالات متداول 239
12.15.منابعی برای مطالعه بیشتر 240

۱۳. HONEY POT در شبکه های کامپیوتری 242
13.1 خلاصه فصل 242
13.2 مقدمه 242
13.3.مضرات Honey pot ها 243
13.4.چرا Honeypots 245
13.5.معماری HONEYPOT 246
13.6.ساختمان HONEYPOT 248
13.7.استفاده از تحقیقات با HONEYPOTS 249
13.8.مزایای استفاده از HONEYPOTS 249
13.9.معایب HONEYPOTS 250
13.10.مسائل حقوقی مربوط به HONEYPOTS 250
13.11. TARPITS 252
13.12.نشانه‌های Honey pot: 252
13.13.کار آینده 252
13.14.جایگاه Honeypot ها 257
13.15.پیشگیری 263
13.16.کشف یا شناسایی 263
13.17.Research Honeypot 264
13.۱۸. نتیجه گیری 267

13.19.سؤالات متداول 268
13.20.منابعی برای مطالعه بیشتر 268
ضمیمه اول 270
کنفرانس های سالانه امنیت شبکه 270
ضمیمه دوم 271
نمونه سؤالات گواهی مهندسی امنیت 271
ضمیمه سوم 277
نمونه پروژه های تحقیقاتی 277
ضمیمه چهارم 279
واژگان و عبارات 279
ضمیمه پنجم 289
فهرست علائم اختصاری 289