

12/1/99

الحمد لله

پیداوار غیر عامل شبکه

تأليف و تدوين:
دکتر ناصر مدیری
مهندس منیر سادات شاه ولایتی



Publication

Mehregane Ghalam

[illegible]

پوشناسه	مدیری، ناصر، ۱۳۴۱ -
عنوان و نام پدیدآور	پدافند غیرعامل شبکه/ مولف ناصر مدیری، منیر سادات شاه ولایتی.
مشخصات نشر	تهران: مهرگان قلم،
مشخصات ظاهری	۲۸۰ص: مصور.
شابک	۳-۰۴-۸۷۲۶-۶۰۰-۹۷۸:
وضعیت فهرست نویسی	فیفا
یادداشت	کتابنامه.
موضوع	شبکه های کامپیوتری -- تدابیر ایمنی
موضوع	COMPUTER NETWORKS -- SECURITY MEASURES :
موضوع	کامپیوترها -- ایمنی اطلاعات -- مدیریت
موضوع	COMPUTER SECURITY -- MANAGEMENT :
موضوع	جرایم کامپیوتری -- پیشگیری
موضوع	COMPUTER CRIMES -- PREVENTION :
شناسه افزوده	شاه ولایتی، منیر سادات، ۱۳۵۳ -
رده بندی کنگره	۱۳۹۵ پ ۴م / ۵۹ / ۵۱۰۵ TK
رده بندی دیسی	۰۰۵/۸ :
شمار کتابشناسی ملی	۴۶۱۲۷۲۴ :

تکثیر تمام یا قسمتی از اثر بدون
مجوز کتبی ناشر ممنوع است و
متخلفان به موجب قانون حمایت
حقوق مولفان، مصنفان و
هنرمندان تحت پیگرد قانونی قرار
دهند گفت.



Mehregan Ghalam

نام کتاب: پدافند غیر عامل شبکه

مولف: ناصر مدیری - منیر سادات شاه ولایتی

ناشر: مهرگان قلم

نوبت چاپ اول: زمستان ۹۵

شابک: ۳-۰۴-۸۷۲۶-۶۰۰-۹۷۸

تیراژ: ۵۰۰

قیمت: ۲۸۰۰۰ تومان

مرکز پخش

انتشارات مهرگان قلم:

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

تلفن تماس: ۵-۶۶۴۷۷۲۲۴ - ۵۸-۰۹۱۲۳۱۴۶

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 از اساسی‌ترین مباحث مهندسی کامپیوتر و در راه ارتقای دانش و فرهنگ این مرز و بوم به تألیف برسانیم. فضای سایر شامل اینترنت و دیگر شبکه‌های مبتنی بر کامپیوتر در حال تبدیل شدن به یکی از مهمترین تاسیسات زیربنایی است که اجتماعات مدرن را توصیف می‌نماید. در میان این شبکه‌ها، سیستم‌هایی وجود دارد که کنترل و مدیریت سایر تاسیسات زیربنایی مانند بانکها، سرویس‌های حیاتی و اورژانس، انتقال انرژی و خیلی از سیستم‌های نظامی را بر عهده دارند و خیلی از مراکز اقتصادی، سیاسی و اجتماعی نیز ممکن است به این شبکه‌ها وابسته باشند. از طرفی اینترنت به عنوان دنیایی که نسخه دیجیتالی شده دنیای واقعی است، محیطی را ایجاد کرده است که در آن می‌توان انواع و اقسام جرایم را شاهد بود. البته محصور بودن دنیای واقعی نسبت به آن شود فرآیند کنترل در آن امکان‌پذیر باشد، ولی از آنجایی که محیط مجازی هیچ مرزی ندارد، مشکلات فراوانی پیش روی قانون‌گذار وجود خواهد داشت. بنابراین نیاز است، علاوه بر برقرار کردن حفاظت‌های تکنیکی در شبکه، هوشیاری و آگاهی کاملی نسبت به همه کاربران و خطرات همراه آنها در استفاده از سیستم‌ها، مستلزم به شبکه، وجود داشته باشد. نکته حیاتی در استراتژی‌های دفاعی نظارت مداوم بر شبکه و همچنین نوآوری در ایجاد تکنیک‌های جدید نظارتی به منظور به حداقل رساندن عوامل ایجاد خطرات است. در هر صورت در هر استراتژی دفاعی که فی‌نفسه یک سیستم پیچیده است، باید مراحل وجود داشته باشد که باعث پیشگیری یا کاهش اثرات حملات گردد. این مراحل می‌تواند شامل مدیریت وقایع موجود در سازمان، بازسازی، جداسازی از وقوع حمله و بهبود بخشیدن کارایی دفاعی، بوسیله تحلیل و طراحی مجدد المان‌هایی که مورد سوءاستفاده جهت ایجاد نفوذ قرار گرفته‌اند باشد و قبل از وقوع حملات باید پیش‌بینی گردند.

بدین منظور این کتاب در یازده فصل تهیه گردیده است:

- در فصل اول با نام بررسی امنیت و تاثیرات اجتماعی آن، جرائم کامپیوتری تعریف شده و به بررسی نقش فن‌آوری‌های نوین و رایانه‌ها در جرائم کامپیوتری پرداخته شده است.
- در فصل دوم با عنوان شناخت استانداردهای امنیتی شبکه‌ها، به بررسی سیستم مدیریت امنیت اطلاعات یا ISMS و مراحل اجرای نظام مدیریت امنیت اطلاعات پرداخته شده و استانداردهای مدیریت امنیت اطلاعات مورد بررسی قرار گرفته و فوائد استاندارد BS7799 و لزوم پیاده‌سازی

- آن ذکر شده است.
- در فصل سوم با عنوان معرفی و مدیریت شبکه های کامپیوتری، به معرفی مفاهیم شبکه، انواع شبکه به لحاظ محدوده جغرافیایی، تقسیم بندی شبکه ها و کاربرد مدیریت شبکه در ایجاد امنیت پرداخته شده است.
- در فصل چهارم با عنوان روشهای حمله به شبکه های کامپیوتری، انواع حملات در محیط های کامپیوتری توضیح داده شده و اقدامات مؤثر برای کاهش تهدید پذیری در برابر حملات سایر عنوان گردیده و در ادامه راهکارهای پیشگیری از حملات در محیط های IT مورد بررسی قرار گرفته است.
- در فصل پنجم با نام نفوذگرهای شبکه های کامپیوتری، به بررسی سناریوی کلی نفوذ و دستورالعملهای پیشگیرانه و کاهنده پدافند غیرعامل جهت تامین امنیت پرداخته شده و مراحل اجرای تست نفوذ پذیر، ایمنی تست نفوذ پذیری و انواع روش های تست نفوذ پذیری بررسی شده اند.
- در فصل ششم با عنوان امنیت فیزیکی شبکه ها، به بررسی شرایط مورد نیاز برای برقراری امنیت فیزیکی و ساختمانی شبکه ها پرداخته شده است.
- در فصل هفتم با نام تهدیدات در شبکه های کامپیوتری، به تعاریف مختلف از نفوذپذیری و طبقه بندی جامع نفوذپذیری ها پرداخته شده و لیست کامل نفوذپذیری ها به زبان لاتین ذکر گردیده است.
- در فصل هشتم با عنوان تهدیدات سایتهای، سایت کامپیوتری، سایت اطلاع رسانی و انواع سایتهای و خدمات قابل ارائه در آنها معرفی شده و همچنین به بررسی پروتکلها و استانداردهای مدیریت سایت و سطوح امنیت در سایت بر اساس قواعد کلی CISCO پرداخته شده است.
- در فصل نهم با نام روشهای شناسایی شبکه های کامپیوتری، به شناسایی روشهای Port Scanning پرداخته شده و نرم افزار Nmap برای شناسایی شبکه های کامپیوتری معرفی شده است.
- در فصل دهم با نام چیدمان شبکه های کامپیوتری، طرح امنیتی Cisco برای تأسیس شبکه های سازمانی (SAFE)، که برای طراحی و پیاده سازی شبکه های کامپیوتری امن می باشد معرفی شده و جزئیات این پیاده سازی مورد بررسی قرار گرفته است.
- در فصل یازدهم با عنوان پدافند غیرعامل در محیط های کامپیوتری، مفهوم پدافند غیرعامل،

ضرورت وجود پدافند غیر عامل و پدافند غیر عامل در محیط IT معرفی شده و با تقسیم بندی محیط‌های کامپیوتری، به تقسیم بندی تدابیر ایمنی پدافند غیر عامل متناسب با هر یک از این محیط‌ها پرداخته شده است.

سرفصل‌های این کتاب بگونه‌ای است که بتوان مطالب مربوط به مفاهیم پایه‌ای و دلیل استفاده گسترده از شبکه‌ها فرا گرفته شود و از مقالات متعددی در این زمینه بهره برده و تحقیقات خود را در صورت تمایل آغاز نمایند.

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

در خاتمه بر خود لازم می‌دانیم انتمای عزیزانی که به نوعی در گردآوری مطالب این کتاب ما را یاری رساندند کمال تشکر و قدردانی را عمل آوریم.

بی‌صبرانه منتظر نظرات، انتقادات و پیشنهاد شما هستیم.

پست الکترونیکی انعکاس نظرات:

info@27000.ir

www.27000.ir

ناصر مدیری - منیر سادات شاه‌ولایتی

فهرست مطالب

13	فصل اول
15	1. بررسی تأثیرات اجتماعی امنیت
15	1.1. خلاصه فصل
16	1.2. مقدمه
17	1.3. جرائم کامپیوتری
19	1.4. نقش رایانه‌ها در جرائم
19	1.5. نقش فن آوری نوین در جرائم رایانه‌ای
20	1.6. انواع جرائم رایانه‌ای
21	1.7. امنیت فضای سایر
23	1.8. راهکارهای امنیت فضای سایر
26	1.9. منابعی برای مطالعه بیشتر
27	فصل دوم
29	2. استانداردهای امنیتی شبکه‌های کامپیوتری
29	2.1. خلاصه فصل
29	2.2. مقدمه
30	2.3. استانداردهای مدیریت امنیت اطلاعات
36	2.4. استاندارد BS7799 و لزوم پیاده سازی
37	2.5. سیستم مدیریت امنیت اطلاعات ISMS
40	2.6. تعاریف
41	2.7. مراحل اجرای نظام مدیریت امنیت اطلاعات
47	2.8. الزامات مستند سازی
48	2.9. مسئولیتهای مدیریتی
50	2.10. ممیزی داخلی ISMS

51	2.11. بازنگری مدیریتی ISMS
52	2.12. بهینه سازی ISMS
53	2.13. کنترلها و تعاریف A مربوط به ISMS
74	2.14. منابعی برای مطالعه بیشتر
77	فصل سوم
79	3. مدیریت شبکه های کامپیوتری
79	3.1. خلاصه فصل
79	3.2. مقدمه
81	3.3. اصول طراحی شبکه و ایمن بندی
81	3.4. تجهیزات شبکه
84	3.5. تقسیم بندی شبکه ها
84	3.6. طراحی و پیاده سازی مبتنی بر سر و ...
87	3.7. کاربرد مدیریت شبکه
88	3.8. سطوح مدیریتی
91	3.9. منابعی برای مطالعه بیشتر
93	فصل چهارم
95	4. روشهای حمله به شبکههای کامپیوتری
95	4.1. خلاصه فصل
95	4.2. مقدمه
97	4.3. انواع حملات در محیطهای کامپیوتری
107	4.4. راهکارهای پیشگیری از حملات
108	4.5. منابعی برای مطالعه بیشتر
109	فصل پنجم

112	5. نفوذگرهای شبکه های کامپیوتری
112	5.1. خلاصه فصل
112	5.2. مقدمه
113	5.3. سناریوی کلی نفوذ
115	5.4. دستورالعملهای پیشگیرانه برای مقابله با نفوذگران
129	5.5. مفهوم تست نفوذ پذیری
131	ابزار تست نفوذ پذیری به صورت Black Box
134	5.6. دستورالعملهای کاهش نفوذ
135	5.7. منابعی برای مطالعه بیشتر
135	فصل ششم
138	6. امنیت فیزیکی شبکه های کامپیوتری
138	6.1. خلاصه فصل
138	6.2. امنیت فیزیکی و ساختمانی شبکهها
146	6.3. منابعی برای مطالعه بیشتر
145	فصل هفتم
150	7. طبقه بندی و شناخت کاستیهای شبکههای کامپیوتری
150	7.1. خلاصه فصل
150	7.2. مقدمه
151	7.3. نفوذپذیری
152	7.4. طبقه بندی نفوذپذیریها
164	7.5. آمار نفوذپذیریها
165	7.6. طبقه بندی شرکت CISCO از نفوذپذیریها
166	7.7. منابعی برای مطالعه بیشتر
167	فصل هشتم

170	8. تهدیدات سایتهای کامپیوتری
170	8.1. خلاصه فصل
170	8.2. مقدمه
171	8.3. طراحی سایت اطلاع رسانی
173	8.4. انواع سایتها و خدمات قابل ارائه
177	8.5. ضرورت تامین امنیت در محیط سایتها
178	8.6. تعریف سایتهای امنیتی شبکه
181	8.7. استراتژی طرح سایت
182	8.8. هدایت و کنترل سایت
182	8.9. پروتکلهای و استانداردهای مدیریت سایت
184	8.10. سطوح امنیت در سایتهای ارائه خدمات کلی CISCO
186	8.11. گسترش سیاست های امنیت یک سایت
187	8.12. پشتیبانی سایت و تجهیزات
188	8.13. مراحل پیاده سازی امنیت
193	8.14. منابعی برای مطالعه بیشتر
193	فصل نهم
196	9. روشهای شناسایی شبکه های کامپیوتری
196	9.1. خلاصه فصل
197	9.2. مقدمه
197	9.3. پورت چیست
198	9.4. عمل Port Scanning
200	9.5. روشهای Port Scanning
203	9.6. نرم افزارهای Port Scanning
203	9.7. Port Scanning در مقابل Firewall
204	9.8. نرم افزار Nmap

205	9.9. منابعی برای مطالعه بیشتر.....
207	فصل دهم.....
209	10. چیدمان شبکه های کامپیوتری.....
209	10.1. خلاصه فصل.....
210	10.2. مقدمه.....
211	10.3. دیدگاه معماری (overview).....
215	10.4. قواعد کلی SAE.....
223	10.5. ماژول طرح.....
224	10.6. Enterprise Campus.....
225	10.7. ماژول مدیریت.....
228	10.8. ماژول هسته.....
229	10.9. ساختمان ماژول توزیع.....
230	10.10. ماژول ساختمان.....
231	10.11. ماژول سرور.....
232	10.12. ماژول توزیع حاشیه ای.....
234	10.13. Enterprise edge.....
235	10.14. ماژولهای متحد اینترنتی.....
238	10.15. ماژولهای دسترسی از راه دور و VPN.....
239	10.16. ماژول شبکه گسترده.....
240	10.17. تهدیدات کاهش داده شده.....
240	10.18. ماژول تجارت الکترونیکی.....
242	10.19. منابعی برای مطالعه بیشتر.....
243	فصل یازدهم.....
246	11. پدافند غیرعامل در شبکه های کامپیوتری.....

246	11.1. خلاصه فصل
246	11.2. مقدمه
248	11.3. ضرورت وجود پدافند غیر عامل
248	11.4. قابلیت های پدافند غیر عامل
249	11.5. اصول پدافند غیر عامل
249	11.6. اهداف کلان
250	11.7. راهبردها
251	11.8. پدافند غیر عامل در محیط IT
252	11.9. تقسیم بندی تدابیر امنیتی پدافند غیر عامل در زمینه IT
272	11.10. استراتژی ایمن سازی فضای سایر
273	11.11. منابعی برای مطالعه بیشتر
275	ضمیمه اول
275	نمونه سؤالات مهندسی امنیت