

زیرساخت امنیت اینترنت

تالیف و تدوین:

دکتر ناصر مدیری

مهندس احسان یزدان پرست



Publication

Mehregane Ghalam

سرشناسه : مدیری، ناصر، ۱۳۴۱
 عنوان و نام پدیدآور : زیرساخت امنیت اینترنت/ تالیف و تدوین ناصر مدیری_ احسان یزدانپرست.
 مشخصات نشر : تهران: مهرگان قلم، ۱۳۹۶.
 مشخصات ظاهری : [۳۲۸] ص.
 شابک : ۹۷۸-۶۰۰-۶۲۳۶-۹۷-۱
 وضعیت فهرست نویسی : فیا.
 موضوع : تکنولوژی اطلاعات و ارتباطات
 موضوع : اینترنت — تدابیر ایمنی
 موضوع : شبکه‌های کامپیوتری — تدابیر ایمنی
 موضوع : کامپیوترها — ایمنی اطلاعات
 شناسه افزوده : یزدانپرست، احسان، ۱۳۵۸
 رده بندی کنگره : T۵۸/۵/م۴ز۹ ۱۳۹۶
 رده بندی دیویی : ۳۰۳/۴۸۳۳
 حاره کتابشناسی ملی : ۴۵۸۷۱۵۲

نام کتاب : زیر ساخت امنیت اینترنت

مولف : ناصر مدیری-احسان یزدانپرست

ناشر: مهرگان قلم

نوبت چاپ اول: زمستان ۹۵

شابک: ۹۷۸-۶۰۰-۶۲۳۶-۹۷-۱

تیراژ: ۵۰۰

قیمت: ۳۵۰۰۰ تومان



Mehregane Ghalam

مرکز بخش

انتشارات مهرگان قلم:

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

تلفن تماس: ۵-۶۶۴۷۷۲۲۴ - ۵۸-۹۱۲۳۱۴۶۰

ن وَالْقَلَمِ وَمَا يَسْطُرُونَ

حضرت حق را سپاس که با الطاف بیکران خود این توفیق را بر ما ارزانی داشت تا کتابی را جهت یکی از اساسی‌ترین مباحث مهندسی کامپیوتر و در راه ارتقای دانش و فرهنگ این مرز و بوم به تألیف برسانیم.

در دوران جالبی زندگی می‌کنیم. برهه‌ای از زمان که عده‌ای نام عصر اطلاعات به آن داده‌اند و گروهی دیگر نام عصر ارتباطات را بر آن نهاده‌اند. هر چند که این دو واژه از لحاظ مفهومی بسیار با یکدیگر تفاوت هستند، لیکن نامیدن این دوره از زمان به عصر اطلاعات، به این علت است که فناوری‌های ارتباطی بسیار پیشرفت کرده‌اند. آنچه که در این کتاب به بررسی آن خواهیم پرداخت آشنایی با مکانیزم‌های اطلاعاتی و ارتباطی است. مدیریت شبکه، روش آدرس‌دهی، نام‌های اختصاصی و آدرس‌های اختصاصی را نیز به بحث خواهیم نشست. از طرفی آنچه را که معمولاً کاربران عادی اطلاع ندارند، یعنی همان سامانه‌های کنترل فضای سایبری و ... را نیز ارائه خواهیم داد.

در فصل اول این کتاب که با عنوان «شبکه اینترنت» آمده است، تاریخچه‌ای از اینترنت ارائه شده که بررسی می‌کند این پدیده هزاره سوم که جهان را در اختیار خود گرفته است چه سرگذشتی را پشت سر نهاده تا به اینجا رسیده است. پدیدآورندگان اینترنت از دیگر مطالب مهم این فصل است. چگونگی گردش داده‌ها در اینترنت و حرکت یک بسته داده‌ای از مبدأ به مقصد و عبور از مسیرهای بین راه بخشی دیگر است. خانه الکترونیکی یا همان وب سایت همراه با نگرش دولت‌ها به اینترنت از دیگر مطالبی است که در این فصل مشاهده خواهید کرد. در پایان بررسی روند توسعه اینترنت و چگونگی به وجود آمدن ترافیک و نحوه برطرف شدن آن مطالب مفیدی است که ملاحظه خواهید کرد.

در فصل دوم این کتاب که با عنوان «زیر شبکه‌های اینترنت» آمده است، توضیحاتی درباره NSF¹ اولین شبکه‌ای که گسترش یافت و ماهیت اینترنت را به وجود آورد ارائه شده است. از جمله مطالب مهم دیگر این فصل راجع به شرکت تله‌گلوب و فلگ است که جزء بک‌بن‌های اصلی اینترنت هستند و مسیرهای عبور خطوط فیبرنوری آنها نیز بررسی شده است. مبحث مهم پایانی درباره اینترنت II است که به واسطه پشتیبانی سرعت بیشتر، نوع خدمات متفاوتی را ارائه می‌کند.

در فصل سوم این کتاب که با عنوان «مراکز اصلی اینترنت» آمده است، توضیحاتی درباره اینترنتیک بین‌المللی و ماهیت کار آن ارائه شده، علت راه‌اندازی و جوانب دیگر آن بررسی شده است. از طرفی مراکز اصلی نگهدارنده آدرس وب‌سایت‌ها که همان DNS²ها هستند نیز بخشی از مطالب مهم این فصل را به خود اختصاص داده. مطلب دیگر، NOC³ یا مرکز کنترل عملیات شبکه است که به تفصیل به آن پرداخته شده است. نحوه مدیریت شبکه و مقوله NSA که شاید تعداد زیادی از افراد جامعه به آن بی‌توجه باشند نیز در حمله مطالب مفید این فصل است.

در فصل چهارم این کتاب که با عنوان «مراکز دسترسی به اینترنت» آمده است، ماهیت مراکز خادم⁴ اینترنت یا همان ISP⁵ها به تفصیل ارائه شده است. نحوه راه‌اندازی ISP، شیوه اداره کردن آن، ملاکهای انتخاب یک خادم خوب اینترنت، راهکارهای مدیریت و ... سایر موارد لازم بحث شده است. از طرفی مبحث تامین کنندگان اینترنت برای ISP⁶ها، یا همان ICPها نیز بررسی شده است. در فصل پنجم این کتاب که با عنوان «امنیت شبکه‌های رایانه‌ای» آمده است، امنیت شبکه با نگرش لایه‌بندی شامل پیرامون، شبکه، میزبان، برنامه کاربردی و داده به صورت مشروح بررسی شده است. در بخشی دیگر از این فصل امنیت تجهیزات شبکه از بعد فیزیکی و منطقی همراه با ملزومات آن ارائه شده است. بررسی خواص شبکه‌های امن به صورت مورد به مورد از دیگر مطالب مهم این فصل است. خاتمه دهنده مطالب پراهمیت این فصل بررسی بحث امنیت شبکه ایران است.

¹ National Science Foundation

² Domain Name Server

³ Network Operation Center

⁴ Server

⁵ Internet Service Provider

⁶ Internet Connection Provider

در فصل ششم این کتاب که با عنوان «هکرها» آمده است، معرفی ماهیت هکرها توضیح داده شده طبق یک گروه‌بندی عمومی دسته‌های آنها شرح داده شده و تفاوت‌های آنها بررسی شده است. راه‌کارهای تامین امنیت برای سامانه‌های رایانه‌ای از دیگر مطالب مهم این فصل است. ارائه یک دسته‌بندی از حملاتی که به رایانه‌های می‌شود و چگونگی انجام این حمله همراه با تجزیه و تحلیل آن بحث مفیدی است که در این فصل مطرح شده است.

در فصل هفتم این کتاب که با عنوان «روش‌های هک» آمده است، مطالب این فصل به 3 دسته اصلی: بسیار مهم تقسیم شده‌اند. ارائه اطلاعات کاملی راجع به IP Spoofing شامل ماهیت عمل آن، چگونگی انجام، اثرات برجای مانده و نحوه مقابله بخش اول این مطالب است. در بخش بعدی بحث Port Sniffing به طور کامل بررسی و تحلیل شده است. در بخش پایانی نیز مباحث مفیدی درباره Smart Mail شده که می‌تواند کاربردهای فراوانی داشته باشد. امید است که مطالب طرح شده برای علاقمندان مفید بوده و راه‌های تحقیقات علمی را نمایان کرده باشد.

در خاتمه بر خود لازم می‌دانم از همه میزبانانی که به نوعی در گردآوری مطالب این کتاب ما را یاری رساندند مخصوصاً خانم زهرا سرمست شوشتری کمال تشکر و قدردانی را بعمل آوریم. بی‌صبرانه منتظر نظرات، انتقادات و پیشنهادات شما هستیم. پست الکترونیکی انعکاس نظرات و سایت پیگیری: info@27000.ir

info@27000.ir
www.27000.ir

ناصر مدیری - احسان یزدان‌پور

فهرست

فصل 1

14	1. شبکه اینترنت
14	1.1. خلاصه فصل
15	1.2. مقدمه
16	1.3. تاریخچه اینترنت
19	1.4. پدیدآورندگان اینترنت
23	1.5. گردش داده‌ها در اینترنت
28	1.6. خانه الکترونیکی
29	1.7. اهمیت اینترنت
33	1.8. ناتیس
36	1.9. جهانی کردن اینترنت
44	1.10. اینترنت و رسانه‌ها
49	1.11. پیامدهای منفی اینترنت
53	1.12. دولت‌ها و اینترنت
54	1.13. نگاهی گذرا به روند اینترنت
57	1.14. ترافیک اینترنت
64	1.15. نتیجه‌گیری
64	1.16. سؤالات متداول
65	1.17. منابعی برای مطالعه بیشتر

فصل 2

68	2. زیرشبکه‌های اینترنت
68	2.1. خلاصه فصل

69	2.2 ماهیت اینترنت
76	2.3 شبکه NSF
78	2.4 گسترش NSF
81	2.5 پروژه فلگ
84	2.6 تله گلوب
89	2.7 ماهواره ها در ارائه اینترنت
92	2.8 زمان های ارتباطات ماهواره ای
94	2.9 ماهواره ها، زیربنای ارتباطاتی
97	2.10 اینترنت II
104	2.11 جایگزین اینترنت
107	2.12 نتیجه گیری
108	2.13 سؤالات متداول
108	2.14 منابعی برای مطالعه بیشتر

فصل 3

12	3 مراکز اصلی اینترنت
112	3.1 خلاصه فصل
113	3.2 InterNIC
114	3.3 DNS
118	3.4 مدل خادم - مخدوم DNS
119	3.5 معماری های خادم
123	3.6 بهینه سازی کارایی DNS
126	3.7 خلاصه سازی نامها و DNS
127	3.8 NOC
131	3.9 تقسیم بندی کلی NOC

135	3.10 مدیریت شبکه
138	3.11 وظایف مهندس NOC
140	3.12 NSA
144	3.13 نتیجه گیری
145	3.14 سؤالات متداول
145	3.15 منابعی برای مطالعه بیشتر
▼ فصل 4	
148	4. مراکز دسترسی به اینترنت
148	4.1 خلاصه فصل
149	4.2 مقدمه
150	4.3 چگونگی کار ISPها
154	4.4 انتخاب یک ISP
156	4.5 ارائه دهنده خدمات اینترنت
160	4.6 راه های ارتباط ISPها با اینترنت
162	4.7 نرم افزارهای کنترل شبکه ISP
175	4.8 شرکتها ICP
177	4.9 وب هاستینگ
181	4.10 نتیجه گیری
181	4.11 سؤالات متداول
182	4.12 منابعی برای مطالعه بیشتر
▼ فصل 5	
185	5. امنیت شبکه های رایانه ای
185	5.1 خلاصه فصل
186	5.2 مقدمه

86	5.3 مفاهیم اولیه امنیت شبکه
90	5.4 امنیت شبکه لایه بندی شده
192	5.4.1 سطح ۱: امنیت پیرامون
195	5.4.2 سطح ۲: امنیت شبکه
199	5.4.3 سطح ۳: امنیت میزبان
201	5.4.4 سطح ۴: امنیت برنامه کاربردی
203	5.4.5 سطح ۵: امنیت داده
205	5.5 انواع در مقابل تهدیدها و حملات معمول
206	5.6 امنیت تجهیزات شبکه
206	5.6.1 امنیت فیزیکی
210	5.6.2 امنیت منطقی
212	5.6.3 ملزومات امنیتی خادمان
214	5.7 خواص شبکه های امن
216	5.8 10 نکته برای حفظ امنیت
220	5.9 امنیت شبکه ایران
221	5.10 نتیجه گیری
222	5.11 سؤالات متداول
222	5.12 منابعی برای مطالعه بیشتر
	 فصل 6
25	6 هکرها
225	6.1 خلاصه فصل
226	6.2 مقدمه
228	6.3 گروه بندی هکرها
233	6.4 راه کارهای تامین امنیت
241	6.5 انواع حملات هکرها

251	6.6. شبه حملات
254	6.7. نتیجه گیری
255	6.8. سؤالات متداول
255	6.9. منابعی برای مطالعه بیشتر

فصل 7

257	7. روش های هک
257	7.1. خلاصه فصل
258	7.2. مقدمه
259	7.3. IP Spoofing
264	7.4. حملات TCP SYN Flooding
270	7.5. انواع حملات Spoofing
276	7.6. کم کردن پکت های IP Spoofed
279	7.7. Packet Sniffer
282	7.8. نحوه عمل Sniffing
285	7.9. روش های کشف Sniffer ها
289	7.10. Snort
294	7.11. مدل شناسایی ورود بدون مجوز به شبکه
299	7.12. عنوان های قوانین
307	7.13. نتیجه گیری
308	7.14. سؤالات متداول
308	7.15. منابعی برای مطالعه بیشتر
311	ضمیمه اول: استانداردها و مراکز اینترنت
314	ضمیمه دوم: واژه نامه انگلیسی به فارسی